TREND MICRO

2.6

# TREND MICRO™ TippingPoint™ Advanced Threat Protection for Email

## Administrator's Guide

Advanced Protection Against Targeted Email Threats

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-for-email.aspx

Trend Micro, the Trend Micro t-ball logo, OfficeScan, Control Manager, and TippingPoint 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.: APEM27712/170215

Release Date: May 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 ..... ix
Documentation ..... x
Audience ..... xi
Document Conventions ..... xi
About Trend Micro ..... xii

## Chapter 1: Introduction

About TippingPoint Advanced Threat Protection for Email ..... 1-2
What's New ..... 1-2
Features and Benefits ..... 1-5
A New Threat Landscape ..... 1-7
Spear-Phishing Attacks ..... 1-7
C&C Callback ..... 1-8
A New Solution ..... 1-8
Virtual Analyzer ..... 1-9
Advanced Threat Scan Engine ..... 1-10
Web Reputation Services ..... 1-11
Social Engineering Attack Protection ..... 1-11
Trend Micro Control Manager ..... 1-11

## Chapter 2: Getting Started

Getting Started Tasks ..... 2-2
Configuring Management Console Access ..... 2-4
Opening the Management Console ..... 2-6
System Requirements ..... 2-7
Management Console Navigation ..... 2-8

## Chapter 3: Dashboard

Dashboard Overview ..... 3-2

Tabs ..... 3-3
- Predefined Tabs ..... 3-3
- Tab Tasks ..... 3-4
- New Tab Window ..... 3-4

Widgets ..... 3-6
- Adding Widgets to the Dashboard ..... 3-6
- Widget Tasks ..... 3-6
- Threat Monitoring ..... 3-8
- Trends ..... 3-15
- System Status ..... 3-20
- Virtual Analyzer ..... 3-24
- Control Manager ..... 3-28

## Chapter 4: Detections

Detected Risk ..... 4-2
- Email Message Risk Levels ..... 4-2
- Virtual Analyzer Risk Levels ..... 4-4

Threat Type Classifications ..... 4-5

Exporting Search Results ..... 4-6

Detected Messages ..... 4-7
- Viewing Detected Messages ..... 4-7
- Investigating a Detected Message ..... 4-11
- Viewing Affected Recipients ..... 4-13
- Viewing Attack Sources ..... 4-14
- Viewing Senders ..... 4-16
- Viewing Email Subjects ..... 4-17

Suspicious Objects ..... 4-18
- Viewing Suspicious Hosts ..... 4-19
- Viewing Suspicious URLs ..... 4-20
- Viewing Suspicious Files ..... 4-21

Quarantine ..... 4-22
- Viewing Quarantined Messages ..... 4-22

Investigating a Quarantined Email Message ..... 4-24

## Chapter 5: Policy

Policy Overview ..... 5-2
Configuring the Actions ..... 5-2
Recipient Notification ..... 5-4
Configuring the Recipient Notification ..... 5-4
Message Tags ..... 5-5
Specifying Message Tags ..... 5-5
Redirect Pages ..... 5-6
Customizing the Redirect Pages ..... 5-6
Policy Exceptions ..... 5-7
Configuring Message Exceptions ..... 5-8
Managing Object Exceptions ..... 5-8
Configuring URL Keyword Exceptions ..... 5-12

## Chapter 6: Alerts and Reports

Alerts ..... 6-2
Critical Alerts ..... 6-2
Important Alerts ..... 6-3
Informational Alerts ..... 6-4
Configuring Alert Notifications ..... 6-5
Viewing Triggered Alerts ..... 6-5
Alert Notification Parameters ..... 6-7
Reports ..... 6-22
Scheduling Reports ..... 6-22
Generating On-Demand Reports ..... 6-23

## Chapter 7: Logs

Email Message Tracking ..... 7-2
Querying Message Tracking Logs ..... 7-2
MTA Events ..... 7-6
Querying MTA Event Logs ..... 7-6

System Events ..... 7-7
Querying System Event Logs ..... 7-8

Time-Based Filters and DST ..... 7-9

## Chapter 8: Administration

Component Updates ..... 8-2
Components ..... 8-2
Update Source ..... 8-3
Updating Components ..... 8-4
Rolling Back Components ..... 8-5
Scheduling Component Updates ..... 8-5

Product Updates ..... 8-6
System Updates ..... 8-6
Managing Patches ..... 8-7
Upgrading Firmware ..... 8-7

System Settings ..... 8-9
Network Settings ..... 8-9
Operation Modes ..... 8-11
Configuring Proxy Settings ..... 8-13
Configuring the Notification SMTP Server ..... 8-14
Configuring System Time ..... 8-16
SNMP ..... 8-17

Mail Settings ..... 8-22
Message Delivery ..... 8-22
Configuring SMTP Connection Settings ..... 8-23
Configuring Message Delivery Settings ..... 8-26
Configuring Limits and Exceptions ..... 8-28
Configuring the SMTP Greeting Message ..... 8-30

Integrated Products/Services ..... 8-30
Control Manager ..... 8-30
Deep Discovery Director ..... 8-35
Threat Intelligence Sharing ..... 8-38
Auxiliary Products/Services ..... 8-40
Microsoft Active Directory ..... 8-65
Log Settings ..... 8-66

SFTP ..... 8-68

Scanning / Analysis ..... 8-69
Email Scanning ..... 8-70
Virtual Analyzer ..... 8-70
File Passwords ..... 8-85
Smart Protection ..... 8-88
Smart Feedback ..... 8-91
YARA Rules ..... 8-92

System Maintenance ..... 8-97
Backing Up or Restoring a Configuration ..... 8-97
Configuring Storage Maintenance ..... 8-101
Debug Logs ..... 8-103
Testing Network Connections ..... 8-104

Accounts / Contacts ..... 8-104
Managing Accounts ..... 8-105
Changing Your Password ..... 8-109
Managing Contacts ..... 8-110

License ..... 8-110

About TippingPoint Advanced Threat Protection for Email ..... 8-110

## Chapter 9: Maintenance

Maintenance Agreement ..... 9-2

Activation Codes ..... 9-2

Product License Description ..... 9-3

Product License Status ..... 9-3

Viewing Your Product License ..... 9-4

Managing Your Product License ..... 9-5

## Chapter 10: Technical Support

Troubleshooting Resources ..... 10-2
Using the Support Portal ..... 10-2
Threat Encyclopedia ..... 10-2

Contacting Trend Micro TippingPoint Support ..... 10-3

Sending Suspicious Content to Trend Micro ..... 10-4
Email Reputation Services ..... 10-4
File Reputation Services ..... 10-4
Web Reputation Services ..... 10-4

Other Resources ..... 10-5
Download Center ..... 10-5
Documentation Feedback ..... 10-5

# Appendices

## Appendix A: Transport Layer Security

About Transport Layer Security ..... A-2

Deploying TippingPoint Advanced Threat Protection for Email in TLS Environments ..... A-2

Prerequisites for Using TLS ..... A-3

Configuring TLS Settings for Incoming Messages ..... A-4

Configuring TLS Settings for Outgoing Messages ..... A-5

Creating and Deploying Certificates ..... A-6

## Appendix B: Using the Command Line Interface

Using the CLI ..... B-2

Entering the CLI ..... B-2

Command Line Interface Commands ..... B-3

## Appendix C: Notification Message Tokens

Recipient Notification Message Tokens ..... C-2

Alert Notification Message Tokens ..... C-3

## Appendix D: Connections and Ports

Service Addresses and Ports ..... D-2

Ports Used by the Appliance ..... D-3

## Appendix E: SNMP Object Identifiers

SNMP Query Objects ..... E-2
SNMP Traps ..... E-18
Registration Objects ..... E-27

## Appendix F: IPv6 Support in TippingPoint Advanced Threat Protection for Email

Configuring IPv6 Addresses ..... F-3
Configurable IPv6 Addresses ..... F-3

## Appendix G: System Event Logs

## Appendix H: Glossary

## Index

Index ..... IN-1

# Preface

## Preface

Topics include:


- *Documentation on page x*
- *Audience on page xi*
- *Document Conventions on page xi*
- *About Trend Micro on page xii*

# Documentation

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

**TABLE 1. Product Documentation**

| DOCUMENT | DESCRIPTION |
|---|---|
| Administrator's Guide | PDF documentation provided with the product or downloadable from the Trend Micro website.<br><br>The Administrator's Guide contains detailed instructions on how to deploy, configure and manage ATP Email, and provides explanations on ATP Email concepts and features. |
| Installation and Deployment Guide | PDF documentation provided with the product or downloadable from the Trend Micro website.<br><br>The Installation and Deployment Guide discusses requirements and procedures for installing and deploying ATP Email. |
| Syslog Content Mapping Guide | The Syslog Content Mapping Guide contains information on event logging formats supported by ATP Email. |
| Quick Start Card | The Quick Start Card provides user-friendly instructions on connecting ATP Email 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. |
| Online Help | Web-based documentation that is accessible from the ATP Email management console.<br><br>The Online Help contains explanations of ATP Email components and features, as well as procedures needed to configure ATP Email. |

| Document | Description |
| --- | --- |
| Support Portal | The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website:<br><br>http://esupport.trendmicro.com |

View and download ATP Email documentation from the Trend Micro Documentation Center:

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

# Audience

The TippingPoint Advanced Threat Protection for Email 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
- Email routing
- SMTP

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

# Document Conventions

The documentation uses the following conventions:

**TABLE 2. Document Conventions**

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

# 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

Topics include:


- *About TippingPoint Advanced Threat Protection for Email on page 1-2*
- *A New Threat Landscape on page 1-7*
- *A New Solution on page 1-8*

# About TippingPoint Advanced Threat Protection for Email

TippingPoint Advanced Threat Protection for Email stops sophisticated targeted attacks and cyber threats by scanning, simulating, and analyzing suspicious links and attachments in email messages before they can threaten your network. Designed to integrate into your existing anti-spam/antivirus network topology, TippingPoint Advanced Threat Protection for Email can act as a Mail Transfer Agent in the mail traffic flow or as an out-of-band appliance silently monitoring your network for cyber threats.

## What's New

**TABLE 1-1. New Features in ATP Email 2.6**

| FEATURE | DESCRIPTION |
|---|---|
| Auxiliary product integration | TippingPoint Advanced Threat Protection for Email integrates with the following products to provide effective detection and blocking at the perimeter:<br>• Check Point Open Platform for Security (OPSEC)<br>• TippingPoint Security Management System (SMS)<br>• IBM Security Network Protection (XGS)<br>• Palo Alto Panorama and Firewalls |
| Threat intelligence sharing | TippingPoint Advanced Threat Protection for Email can share suspicious object information with third-party products (such as Blue Coat ProxySG) through HTTP/HTTPS web services. |
| Microsoft Active Directory integration | TippingPoint Advanced Threat Protection for Email integrates with Microsoft Active Directory to allow web console logon using Active Directory credentials. |

| Feature | Description |
|---|---|
| New components | TippingPoint Advanced Threat Protection for Email integrates the following components:<br>• Network Content Inspection Engine (NCIE)<br>• Network Content Inspection Pattern (NCIP)<br>• Deep Discovery Trusted Certificate Authorities<br>• Virtual Analyzer Configuration Pattern |
| Enhanced component management | TippingPoint Advanced Threat Protection for Email improves component management by providing the option to roll back component versions. |
| YARA rule support | TippingPoint Advanced Threat Protection for Email 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. |
| Exception list management | TippingPoint Advanced Threat Protection for Email can import or export exception lists through HTTPS web service. |
| Enhanced Virtual Analyzer | The internal Virtual Analyzer has been enhanced to include proxy configuration. |

| Feature | Description |
|---|---|
| Improved detection capability | TippingPoint Advanced Threat Protection for Email provides increased protection by improving its detection capabilities. This release supports the following:<br>• Deployment of sandbox images running Windows 10 Threshold 2 (B1511), Windows Server 2012, and Windows Server 2012 R2 operating systems<br>• Support Microsoft Office 2016 application for Office file analysis in sandbox images<br>• New file types (Microsoft Publisher 2016, Microsoft Windows Command Script file, Microsoft Windows Batch file, and Scalable Vector Graphics) for file submission filters<br>• File SHA-256 and vulnerability information in analysis reports<br>• Decrypt password-protected PDF and Microsoft Office files in archive files<br>• Extract files in archive files with multiple compression layers |
| SFTP upload for detection logs | TippingPoint Advanced Threat Protection for Email can upload Virtual Analyzer detection logs to a secure FTP (SFTP) server. |
| Enhanced SMTP notifications | The enhanced SMTP notifications feature includes the following features:<br>• Support for SMTP server authentication<br>• Option to test connection to SMTP server |
| High memory usage alert | TippingPoint Advanced Threat Protection for Email can send alert notifications when the high memory usage threshold is reached. |

| Feature | Description |
|---|---|
| Management console enhancements | Administrators can view the following information on the management console:<br>• System information (system time, appliance IP address, and network throughput) in the top banner<br>• Additional email header information in detected messages |
| Enhanced credential management | TippingPoint Advanced Threat Protection for Email implements stricter system access credential checks to strengthen product security. |

## Features and Benefits

The following sections describe the TippingPoint Advanced Threat Protection for Email features and benefits.

### Advanced Detection

TippingPoint Advanced Threat Protection for Email advanced detection technology discovers targeted threats in email messages, including spear-phishing and social engineering attacks.

- Reputation and heuristic technologies catch unknown threats and document exploits
- Detects threats hidden in password-protected files and shortened URLs

### Visibility, Analysis, and Action

TippingPoint Advanced Threat Protection for Email provides real-time threat visibility and analysis in an intuitive, multi-level format. This allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures.

## Flexible Deployment

TippingPoint Advanced Threat Protection for Email integrates into your existing anti-spam/antivirus network topology by acting as a Mail Transfer Agent in the mail traffic flow or as an out-of-band appliance monitoring your network for cyber threats.

## Light-weight Policy Management

TippingPoint Advanced Threat Protection for Email simplifies preventative actions with a streamlined policy structure.

- Block and quarantine suspicious email messages
- Allow certain email messages to pass through to the recipient
- Strip suspicious attachments
- Redirect suspicious links to blocking or warning pages
- Tag the email subject or body with a customized string
- Send email notifications

## Custom Threat Simulation Sandbox

The Virtual Analyzer sandbox environment opens files, including password-protected archives and document files, and URLs to test for malicious behavior. Virtual Analyzer is able to find exploit code, Command & Control (C&C) and botnet connections, and other suspicious behaviors or characteristics.

## Email Attachment Analysis

TippingPoint Advanced Threat Protection for Email utilizes multiple detection engines and sandbox simulation to investigate file attachments. Supported file types include a wide range of executable, Microsoft Office, PDF, web content, and compressed files.

### Embedded URL Analysis

TippingPoint Advanced Threat Protection for Email utilizes reputation technology, direct page analysis, and sandbox simulation to investigate URLs embedded in an email message.

### Social Engineering Attack Protection

Social Engineering Attack Protection detects suspicious behavior related to social engineering attacks in email messages. When Social Engineering Attack Protection is enabled, TippingPoint Advanced Threat Protection for Email scans for suspicious behavior in several parts of each email transmission, including the email header, subject line, body, attachments, and the SMTP protocol information.

### Password Derivation

TippingPoint Advanced Threat Protection for Email decrypts password-protected archives and document files using a variety of heuristics and customer-supplied keywords.

# A New Threat Landscape

Where once attackers were content to simply deface a website or gain notoriety through mass system disruption, they now realize that they can make significant money, steal important data, or interfere with major infrastructure systems via cyber warfare instead.

A targeted attack is a long-term cyber-espionage campaign against a person or organization to gain persistent access to the target network. This allows them to extract confidential company data and possibly damage the target network. These compromised networks can be used for attacks against other organizations, making it harder to trace the attack back to its originator.

## Spear-Phishing Attacks

Spear-phishing attacks combine phishing attacks and targeted malware. Attackers send spear-phishing messages to a few targeted employees with crafted email messages

masquerading as legitimate recipients, possibly a boss or colleague. These spear-phishing messages likely contain a link to a malicious website or a malicious file attachment. A file attachment can exploit vulnerabilities in Microsoft™ Word™, Excel™, and Adobe™ products. The file attachment can also be a compressed archive containing executable files. When a recipient opens the file attachment, malicious software attempts to exploit the system. Often, to complete the ruse, the malicious software launches an innocuous document that appears benign.

Once the malicious software runs, it lies dormant on a system or attempts to communicate back to a command-and-control (C&C) server to receive further instructions.

## C&C Callback

The following actions usually occur when malicious software installs and communicates back to a C&C server:

- Software called a "downloader" automatically downloads and installs malware.
- A human monitoring the C&C server (attacker) responds to the connection with an action. Software called a "remote access Trojan" (RAT) gives an attacker the ability to examine a system, extract files, download new files to run on a compromised system, turn on a system's video camera and microphone, take screen captures, capture keystrokes, and run a command shell.

Attackers will attempt to move laterally throughout a compromised network by gaining additional persistent access points. Attackers will also attempt to steal user credentials for data collection spread throughout the network. If successful, collected data gets exfiltrated out of the network to another environment for further examination.

Attackers move at a slow pace to remain undetected. When a detection occurs, they will temporarily go dormant before resuming activity. If an organization eradicates their presence from the network, the attackers will start the attack cycle all over again.

# A New Solution

TippingPoint Advanced Threat Protection for Email prevents spear-phishing attacks and cyber threats by investigating suspicious links, file attachments, and social engineering

attack patterns in email messages before they can threaten your network. Designed to integrate into your existing anti-spam/antivirus network topology, TippingPoint Advanced Threat Protection for Email can act as a mail transfer agent in the mail traffic flow (MTA mode) or as an out-of-band appliance monitoring your network for cyber threats (BCC mode or SPAN/TAP mode).

Whichever deployment method is chosen, TippingPoint Advanced Threat Protection for Email investigates email messages for suspicious file attachments, embedded links (URLs), and characteristics. If an email message exhibits malicious behavior, TippingPoint Advanced Threat Protection for Email can block the threat and notify security administrators about the malicious activity.

After TippingPoint Advanced Threat Protection for Email scans an email message for known threats in the Trend Micro Smart Protection Network, it passes suspicious files and URLs to the Virtual Analyzer sandbox environment for simulation. Virtual Analyzer opens files, including password-protected archives and document files, and accesses URLs to test for exploit code, Command & Control (C&C) and botnet connections, and other suspicious behaviors or characteristics.

After investigating email messages, TippingPoint Advanced Threat Protection for Email assesses the risk using multi-layered threat analysis. TippingPoint Advanced Threat Protection for Email calculates the risk level based on the highest risk assigned between the TippingPoint Advanced Threat Protection for Email email scanners and Virtual Analyzer.

TippingPoint Advanced Threat Protection for Email acts upon email messages according to the assigned risk level and policy settings. Configure TippingPoint Advanced Threat Protection for Email to block and quarantine the email message, allow the email message to pass to the recipient, strip suspicious file attachments, redirect suspicious links to blocking or warning pages, or tag the email message with a string to notify the recipient. While TippingPoint Advanced Threat Protection for Email monitors your network for threats, you can access dashboard widgets and reports for further investigation.

## Virtual Analyzer

Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, and administrators and investigators (through SSH).

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.

## Advanced Threat Scan Engine

The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and heuristic scanning to detect document exploits and other threats used in targeted attacks.

Major features include:

- Detection of zero-day threats
- Detection of embedded exploit code
- Detection rules for known vulnerabilities

- Enhanced parsers for handling file deformities

## Web Reputation Services

With one of the largest domain-reputation databases in the world, Trend Micro web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis, such as phishing scams that are designed to trick users into providing personal information. To increase accuracy and reduce false positives, Trend Micro Web Reputation Services assigns reputation scores to specific pages or links within sites instead of classifying or blocking entire sites, since often, only portions of legitimate sites are hacked and reputations can change dynamically over time.

## Social Engineering Attack Protection

Social Engineering Attack Protection detects suspicious behavior related to social engineering attacks in email messages. When Social Engineering Attack Protection is enabled, TippingPoint Advanced Threat Protection for Email scans for suspicious behavior in several parts of each email transmission, including the email header, subject line, body, attachments, and the SMTP protocol information.

## Trend Micro Control Manager

Trend Micro Control Manager™ is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. The Control Manager web-based management console provides a single monitoring point for managed products and services throughout the network.

Control Manager allows system administrators to monitor and report on activities such as infections, security violations, or virus entry points. System administrators can download and deploy components throughout the network, helping ensure that protection is consistent and up-to-date. Control Manager allows both manual and pre-scheduled updates, and the configuration and administration of products as groups or as individuals for added flexibility.

# Chapter 2

# Getting Started

Topics include:


- *Getting Started Tasks on page 2-2*
- *Configuring Management Console Access on page 2-4*
- *Opening the Management Console on page 2-6*

# Getting Started Tasks

Getting Started Tasks provides a high-level overview of all procedures required to get TippingPoint Advanced Threat Protection for Email up and running as quickly as possible. Each step links to more detailed instructions later in the document. The getting started process is the same for BCC, SPAN/TAP and MTA modes.

**Procedure**

1. Configure network settings to access the management console.

   For details, see *Configuring Management Console Access on page 2-4*.

2. Open the management console.

   For details, see *Opening the Management Console on page 2-6*.

3. Activate the TippingPoint Advanced Threat Protection for Email product license.

   For details, see *Managing Your Product License on page 9-5*.

4. Configure the system time.

   For details, see *Configuring System Time on page 8-16*.

5. Configure network settings.

   For details, see *Configuring Network Settings on page 8-9*.

6. Configure the operation mode.

   For details, see *Operation Modes on page 8-11*.

7. Configure the SMTP server.

   For details, see *Configuring the Notification SMTP Server on page 8-14*.

8. Configure the mail limits and exceptions.

   For details, see *Configuring Limits and Exceptions on page 8-28*.

9. Configure Virtual Analyzer network settings.

   For details, see *Configuring Virtual Analyzer Network and Filters on page 8-77*.

10. Import Virtual Analyzer images.

    For details, see *Importing Virtual Analyzer Images on page 8-74*.

> **Important**
>
> At least one Virtual Analyzer image is required to perform analysis.

11. Configure the password to open archive files and document files.

    For details, see *Adding File Passwords on page 8-86*.

12. Configure email routing for downstream MTAs.

    For details, see *Configuring Message Delivery Settings on page 8-26*.

13. Add at least one notification recipient to all critical and important alerts.

    For details, see *Alerts on page 6-2*.

14. (Optional) Configure policy rules.

    For details, see *Configuring the Actions on page 5-2*.

15. (Optional) Configure policy exceptions.

    For details, see *Policy Exceptions on page 5-7*.

16. (Optional) Register with Trend Micro Control Manager for central management.

    For details, see *Control Manager on page 8-30*.

17. Configure upstream MTAs or SPAN/TAP devices.

    a. If TippingPoint Advanced Threat Protection for Email is operating in BCC or MTA mode, configure the upstream MTAs to route email traffic to TippingPoint Advanced Threat Protection for Email.

**Note**

Configuring the upstream MTA requires different settings for MTA mode and BCC mode. See the supporting documentation provided by the MTA server manufacturer for instructions about configuring MTA settings.

- In MTA mode, configure the MTA to forward email traffic to TippingPoint Advanced Threat Protection for Email.
- In BCC mode, configure the MTA to copy email traffic to TippingPoint Advanced Threat Protection for Email.

b. If TippingPoint Advanced Threat Protection for Email is operating in SPAN/TAP mode, configure the SPAN/TAP device to mirror traffic to TippingPoint Advanced Threat Protection for Email.

**Note**

See the supporting documentation provided by the SPAN/TAP device manufacturer for instructions about configuring settings.

# Configuring Management Console Access

After completing the installation, the server restarts and loads the Command Line Interface (CLI). Configure TippingPoint Advanced Threat Protection for Email network settings to gain access to the management console.

The following procedure explains how to log on to the CLI and configure the following required network settings:

- Management IP address and netmask
- Host name
- DNS
- Gateway

**Procedure**

1. Log on to the CLI with the default credentials.
   - User name: `admin`
   - Password: `ddei`
2. At the prompt, type `enable` and press Enter to enter privileged mode.
3. Type the default password, `trend#1`, and then press Enter.

   The prompt changes from > to #.
4. Configure network settings with the following command:

   ```
   configure network basic
   ```
5. Configure the following network settings and press Enter after typing each setting.

   **Note**

   IPv6 settings are optional.

   - Host name
   - IPv4 address
   - Subnet mask
   - IPv4 gateway
   - Preferred IPv4 DNS
   - Alternate IPv4 DNS
   - IPv6 address
   - Prefix length
   - IPv6 gateway
   - Preferred IPv6 DNS

- Alternate IPv6 DNS

6. Type `Y` to confirm settings and restart.

   TippingPoint Advanced Threat Protection for Email implements specified network settings and then restarts all services.

The initial configuration is complete and the management console is accessible.

**Note**

You can log on to the CLI later to perform additional configuration, troubleshooting, or maintenance tasks. For details about the CLI, see *Using the Command Line Interface on page B-1*.

# Opening the Management Console

TippingPoint Advanced Threat Protection for Email provides a built-in management console that you can use to configure and manage the product.

View the management console using any supported web browser. For information about supported browsers, see *System Requirements on page 2-7*.

For information about configuring required network settings before accessing the management console, see *Configuring Management Console Access on page 2-4*.

**Procedure**

1. In a web browser, type the IP address of the TippingPoint Advanced Threat Protection for Email server.

   **Note**

   The default management console IP address / subnet mask is `192.168.252.1` / `255.255.0.0`.

   The logon screen appears.

2. Specify the logon credentials (user name and password).

**Note**

Use the default administrator logon credentials when logging on for the first time:

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

3. Click **Log On**.

The management console **Dashboard** appears.

For details about the dashboard, see *Dashboard on page 3-1*.

**Important**

Trend Micro recommends changing the password to prevent unauthorized changes to the management console.

For details, see *Changing Your Password on page 8-109*.

## System Requirements

Trend Micro provides the TippingPoint Advanced Threat Protection for Email appliance hardware. No other hardware is supported.

TippingPoint Advanced Threat Protection for Email is a self-contained, purpose-built, and performance-tuned Linux operating system. A separate operating system is not required.

**Note**

Trend Micro recommends viewing the console using a monitor that supports 1280 x 1024 resolution or greater.

The following table lists the minimum software requirements to access the Command Line Interface and the management console that manage TippingPoint Advanced Threat Protection for Email.

**TABLE 2-1. Minimum Software Requirements**

| APPLICATION | REQUIREMENTS | DETAILS |
|---|---|---|
| SSH client | SSH protocol version 2 | Set the Command Line Interface terminal window size to 80 columns and 24 rows. |
| Internet Explorer™ | Versions 9, 10, 11 | Use only a supported browser to access the management console.<br>Using the data port IP address you set during the initial configuration, specify the following URL:<br>`https://[Appliance_IP_Address]:443` |
| Microsoft Edge™ | Windows 10 | |
| Mozilla Firefox™ | Version 50 or later | |
| Google Chrome™ | Version 54 or later | |

**Note**

By default, SSH service is disabled and is not started when enabled. To enable SSH service, see *configure service ssh enable on page B-11*. To start SSH service, see *start service ssh on page B-25*.

## Management Console Navigation

The management console consists of the following elements:

**TABLE 2-2. Management Console Elements**

| SECTION | DETAILS |
|---|---|
| Banner | The management console banner contains:<br>• Product logo and name: Click to go to the dashboard. For details, see *Dashboard Overview on page 3-2*.<br>• Name of the user currently logged on: Click and select **Change password** to change the account password (see *Changing Your Password on page 8-109*) or select **Log off** to log out of the management console.<br>• System time: Displays the current system time and time zone.<br>• Appliance IP address: Displays the IP address of the TippingPoint Advanced Threat Protection for Email appliance.<br>• Network traffic: Displays the incoming and outgoing network throughput. |
| 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. |
| Context-sensitive Help | Use **Help** to find more information about the screen that is currently displayed. |

# Chapter 3

# Dashboard

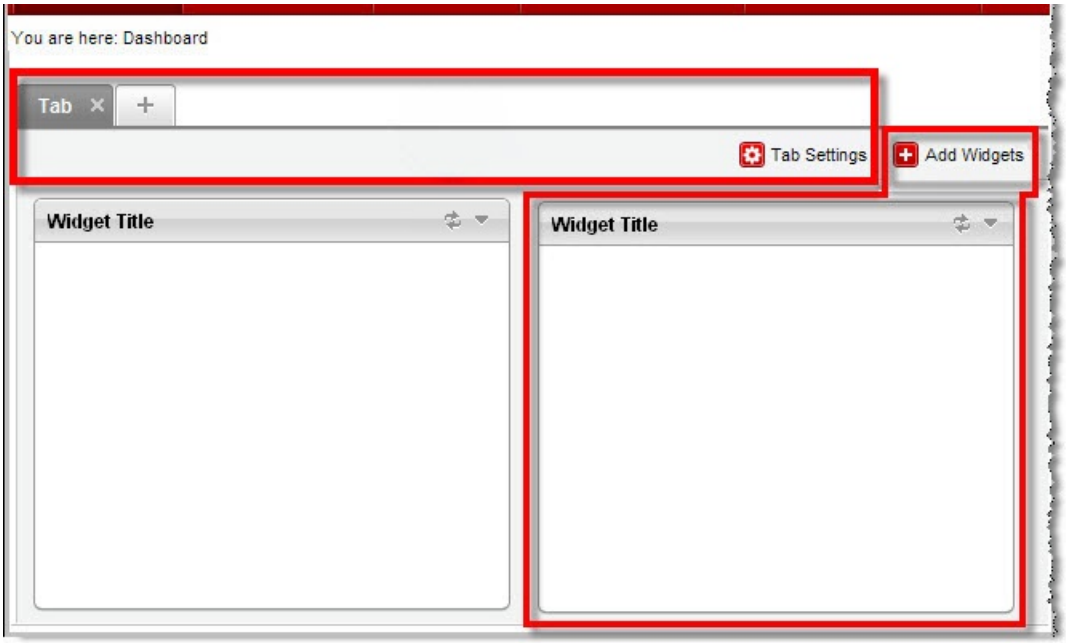
Topics include:


- *Dashboard Overview on page 3-2*
- *Tabs on page 3-3*
- *Widgets on page 3-6*

# 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.<br>For details, see *Tabs on page 3-3*. |
| Widgets | Widgets represent the core dashboard components.<br>For details, see *Widgets on page 3-6*. |

**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 provide a container for widgets. For details, see *Tabs on page 3-3*.
- Widgets represent the core dashboard components. For details, see *Widgets on page 3-6*.

**Note**

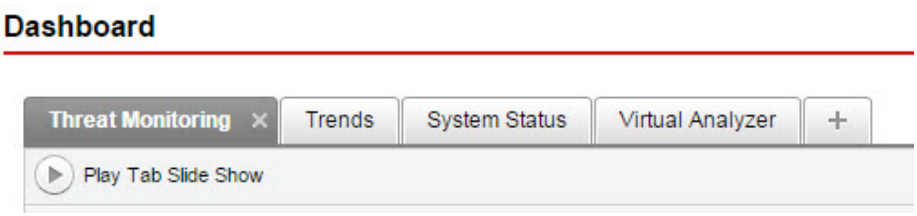
Click **Play Tab Slide Show** to show a dashboard slide show.

# Tabs

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

## Predefined Tabs

The dashboard comes with predefined tabs, each with a set of widgets. You can rename, delete, and add widgets to these tabs.




The predefined tabs include:

- **Threat Monitoring**

- **Trends**
- **System Status**
- **Virtual Analyzer**

## 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.<br>For information about this window, 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:

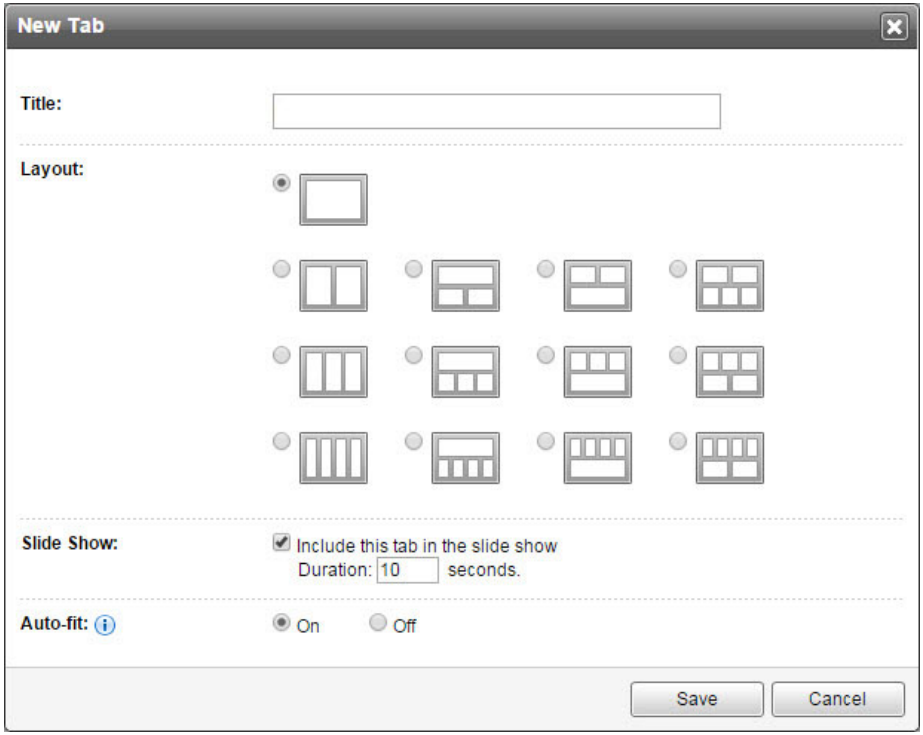



**TABLE 3-1. New Tab Tasks**

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

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

# Widgets

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

## 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**.

## Widget Tasks

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

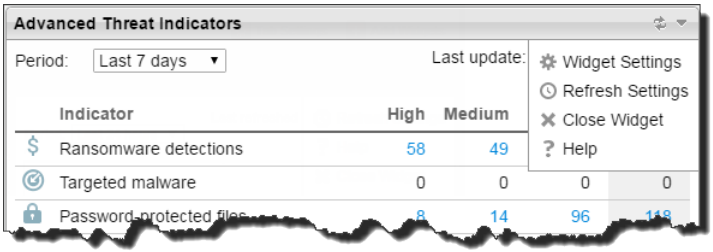
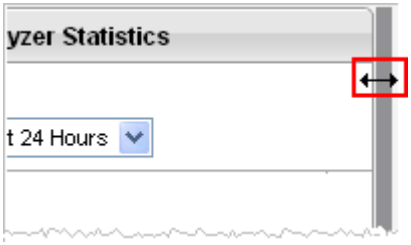
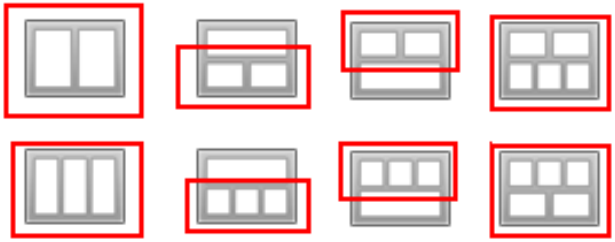



**TABLE 3-2. Widget Options Menu**

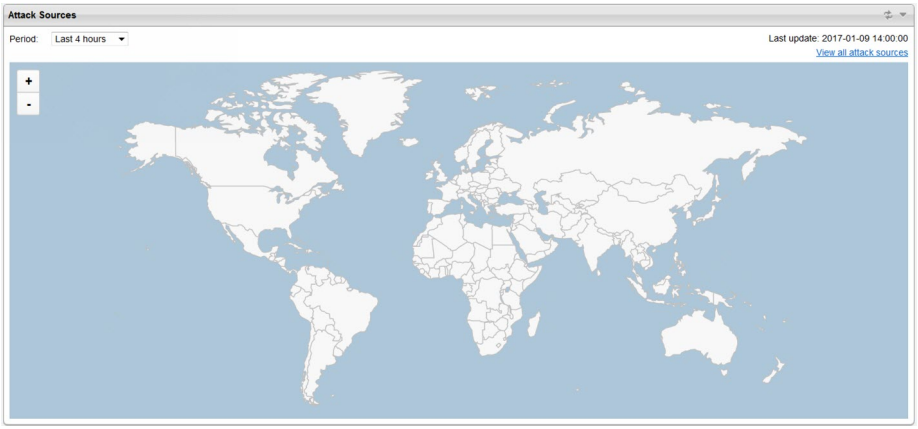
| TASK | STEPS |
|---|---|
| Access widget options | Click the options icon ( ) at the widget's top-right corner to view the menu options. |
| Edit a widget | Click the edit icon ( ) to change settings. |
| Refresh widget data | Click the refresh icon ( ) to refresh widget data.<br><br>Click the refresh settings icon ( ) to set the frequency that the widget refreshes or to automatically refresh widget data. |
| Get help | Click the question mark icon ( ) to get help. The online help appears explaining how to use the widget. |
| 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. |
| Move a widget within the same tab | Use drag-and-drop to move the widget to a different location within the tab. |
| Move a widget to a different tab | Use drag-and-drop to move the widget to the tab title. An option appears to either copy or move the widget to the destination tab location. |

| 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.<br>  <br><br>You can resize any widget within a multi-column tab (red squares). These tabs have any of the following layouts.<br>  |
| Change period | If available, click the **Period** drop-down menu to select the time period. |

## Threat Monitoring

View **Threat Monitoring** widgets to understand incoming suspicious messages, attack sources, affected recipients, and which messages were quarantined.

## Attack Sources Widget




The **Attack Sources** widget shows an interactive map representing all source MTAs that routed suspicious email traffic.

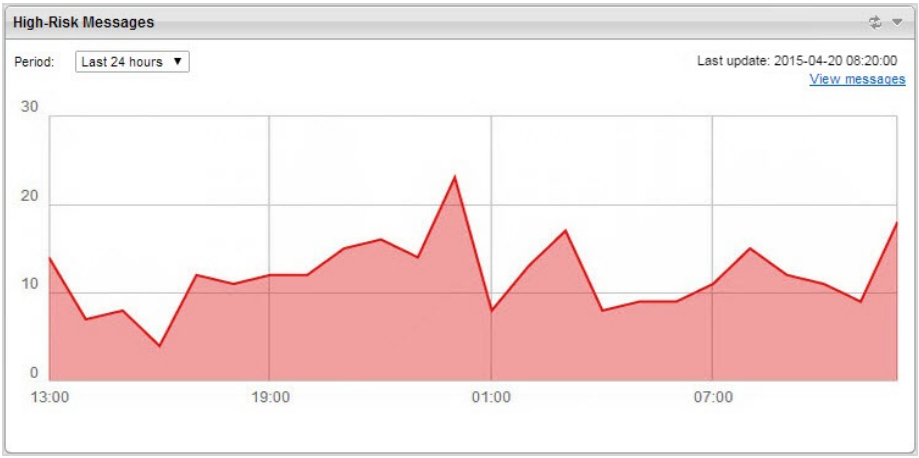
An attack source is the first MTA with a public IP address that routes a suspicious message. For example, if a suspicious message travels the following route: IP1 (sender) > IP2 (MTA: 225.237.59.52) > IP3 (company mail gateway) > IP4 (recipient), TippingPoint Advanced Threat Protection for Email identifies 225.237.59.52 (IP2) as the attack source. By studying attack sources, you can identify regional attack patterns or attack patterns that involve the same mail server.

Mouse-over any point on the map to learn about the events that came from the attack source location.

Click any highlighted region on the map to learn more about attacks originating from that region.

Click **View all attack sources** in the top-right corner to go to the **Attack Sources** screen.

## High-Risk Messages Widget



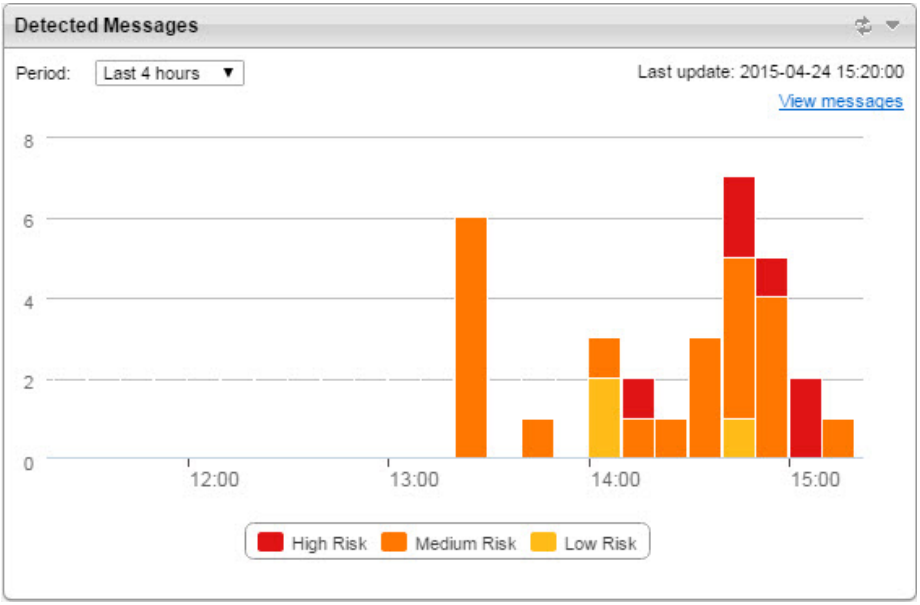

The **High-Risk Messages** widget shows all incoming malicious messages. High-risk messages have malware communications, malicious contact destinations, malicious behavior patterns, or strings that definitively indicate compromise.

The graph is based on the selected period. The Y-axis represents the email message count. The X-axis represents the period. Mouse-over a point on the graph to view the number of high risk messages and the period.

Click **View messages** to view all high-risk detections.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Detected Messages Widget




The **Detected Messages** widget shows all email messages with malicious and suspicious characteristics. Suspicious characteristics includes anomalous behavior, false or misleading data, suspicious and malicious behavior patterns, and strings that indicate system compromise but require further investigation.

**Note**

A similar widget called Email Messages with Advanced Threats is available in Control Manager, which aggregates data from several TippingPoint Advanced Threat Protection for Email appliances. For details, see *Control Manager on page 3-28*.

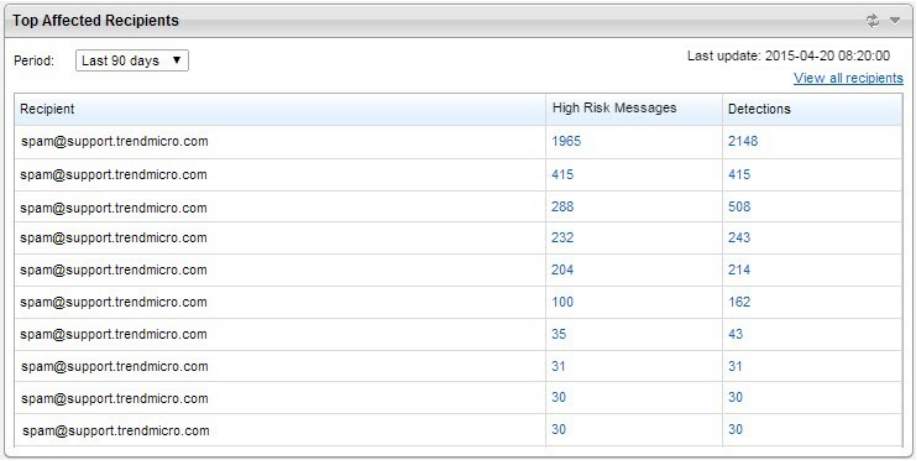
The graph is based on the selected period. The Y-axis represents the email message count. The X-axis represents the period. Mouse-over a point on the graph to view the number of high risk messages and the period.

Click an item in the widget legend to show or hide data related to that metric.

Click **View messages** to view all high-risk detections.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Top Affected Recipients Widget



Top Affected Recipients

Period: Last 90 days

Last update: 2015-04-20 08:20:00

View all recipients

| Recipient | High Risk Messages | Detections |
|---|---|---|
| spam@support.trendmicro.com | 1965 | 2148 |
| spam@support.trendmicro.com | 415 | 415 |
| spam@support.trendmicro.com | 288 | 508 |
| spam@support.trendmicro.com | 232 | 243 |
| spam@support.trendmicro.com | 204 | 214 |
| spam@support.trendmicro.com | 100 | 162 |
| spam@support.trendmicro.com | 35 | 43 |
| spam@support.trendmicro.com | 31 | 31 |
| spam@support.trendmicro.com | 30 | 30 |
| spam@support.trendmicro.com | 30 | 30 |

The **Top Affected Recipients** widget shows the recipients who received the highest volume of suspicious messages.

**Note**

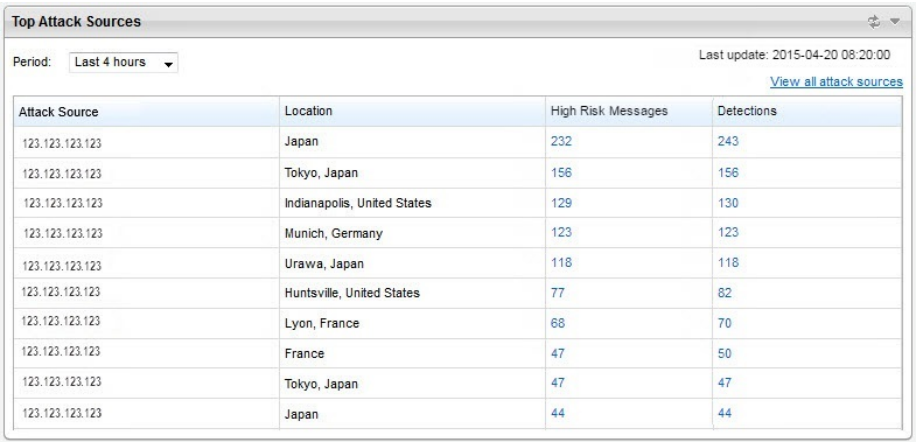
A similar widget called Top Email Recipients of Advanced Threats is available in Control Manager, which aggregates data from several TippingPoint Advanced Threat Protection for Email appliances. For details, see *Control Manager on page 3-28*.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

Click **View all recipients** to see all recipients affected by suspicious messages.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Top Attack Sources Widget




| Attack Source | Location | High Risk Messages | Detections |
|---|---|---|---|
| 123.123.123.123 | Japan | 232 | 243 |
| 123.123.123.123 | Tokyo, Japan | 156 | 156 |
| 123.123.123.123 | Indianapolis, United States | 129 | 130 |
| 123.123.123.123 | Munich, Germany | 123 | 123 |
| 123.123.123.123 | Urawa, Japan | 118 | 118 |
| 123.123.123.123 | Huntsville, United States | 77 | 82 |
| 123.123.123.123 | Lyon, France | 68 | 70 |
| 123.123.123.123 | France | 47 | 50 |
| 123.123.123.123 | Tokyo, Japan | 47 | 47 |
| 123.123.123.123 | Japan | 44 | 44 |

The **Top Attack Sources** widget shows the most active IP addresses attacking your network.

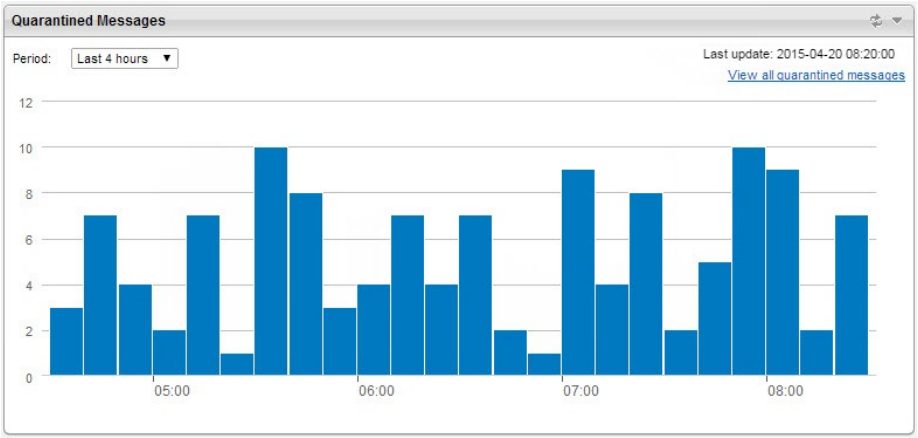
An attack source is the first MTA with a public IP address that routes a suspicious message. For example, if a suspicious message travels the following route: IP1 (sender) > IP2 (MTA: 225.237.59.52) > IP3 (company mail gateway) > IP4 (recipient), TippingPoint Advanced Threat Protection for Email identifies 225.237.59.52 (IP2) as the attack source. By studying attack sources, you can identify regional attack patterns or attack patterns that involve the same mail server.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

Click **View all attack sources** to see all detected attack sources over the selected time period.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Quarantined Messages Widget




The **Quarantined Messages** widget shows all email messages that TippingPoint Advanced Threat Protection for Email quarantined based on how the message characteristics matched policy rule criteria. For details about configuring the policy, see *Policy on page 5-1*.

The graph is based on the selected period. The Y-axis represents the email message count. The X-axis represents the period. Mouse-over a point on the graph to view the number of high risk messages and the period.

Click **View all quarantined messages** to see the quarantine.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Advanced Threat Indicators

**Advanced Threat Indicators**

Period: Last 7 days

Last update: 15/06/2016 09:20:00

| Indicator | High | Medium | Low | Total |
|---|---|---|---|---|
| Ransomware detections | 58 | 48 | 0 | 106 |
| Targeted malware | 0 | 0 | 0 | 0 |
| Password-protected files | 8 | 14 | 95 | 117 |
| Documents with exploit code | 6 | 0 | 0 | 6 |
| Files with spoofed names | 21 | 0 | 0 | 21 |
| C&C callback (upon execution) | 6 | 0 | 0 | 6 |
| Unknown malicious links in message body | 0 | 65 | 38 | 103 |
| Unknown malicious links in attachments | 0 | 0 | 0 | 0 |

The **Advanced Threat Indicators** widget shows the type, amount, and risk level of advanced threat indicators detected in all email messages.

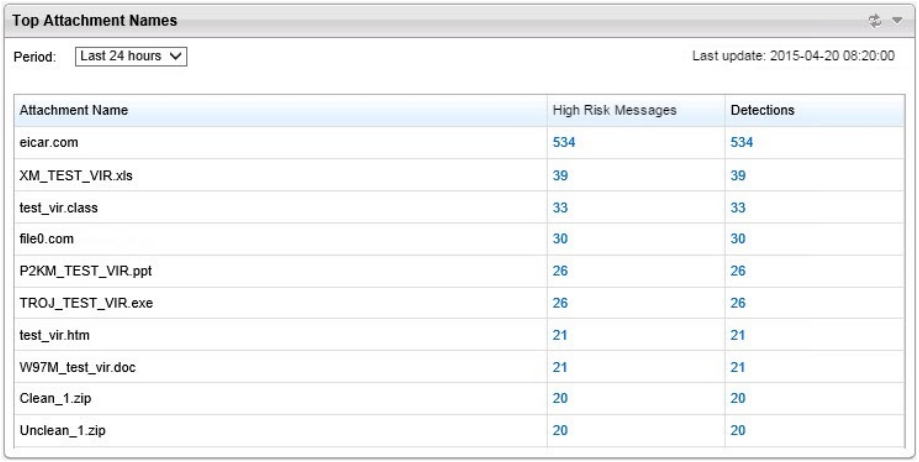
The table shows detections based on the selected time period. Click a number under **High**, **Medium**, **Low**, or **Total** to learn more about the detections.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Trends

View **Trends** widgets to understand the top activity in your network, including suspicious message content and callback destinations, to understand the threat characteristics affecting your network.

## Top Attachment Names Widget



Top Attachment Names

Period: Last 24 hours

Last update: 2015-04-20 08:20:00

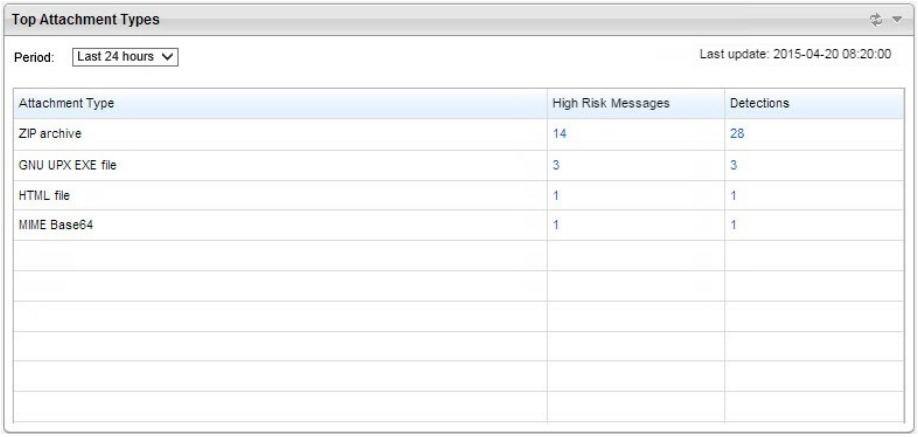
| Attachment Name | High Risk Messages | Detections |
|---|---|---|
| eicar.com | 534 | 534 |
| XM_TEST_VIR.xls | 39 | 39 |
| test_vir.class | 33 | 33 |
| file0.com | 30 | 30 |
| P2KM_TEST_VIR.ppt | 26 | 26 |
| TROJ_TEST_VIR.exe | 26 | 26 |
| test_vir.htm | 21 | 21 |
| W97M_test_vir.doc | 21 | 21 |
| Clean_1.zip | 20 | 20 |
| Unclean_1.zip | 20 | 20 |

The **Top Attachment Names** widget shows the most common file attachments contained in suspicious and high-risk email messages.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Top Attachment Types Widget

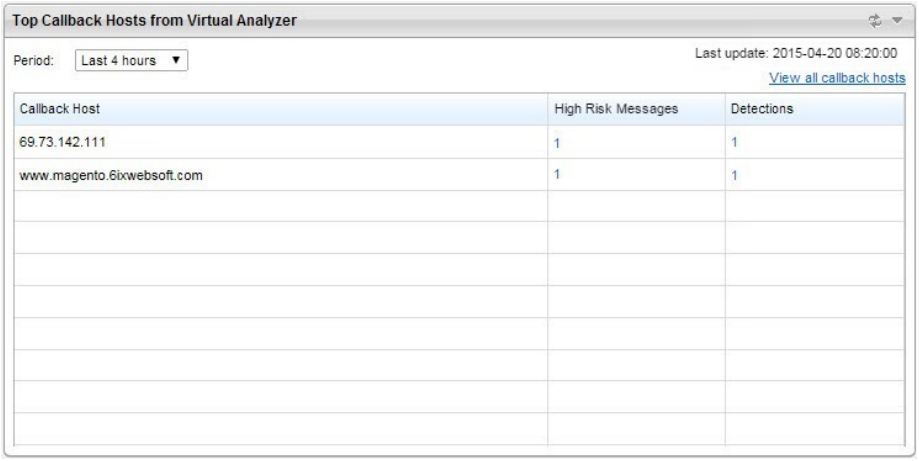



The **Top Attachment Types** widget shows the most common attachment file types contained in detected messages.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Top Callback Hosts from Virtual Analyzer Widget




The **Top Callback Hosts from Virtual Analyzer** widget shows the most common callback hosts contained in suspicious and high-risk email messages. A callback host is the IP address or host name of a C&C server.

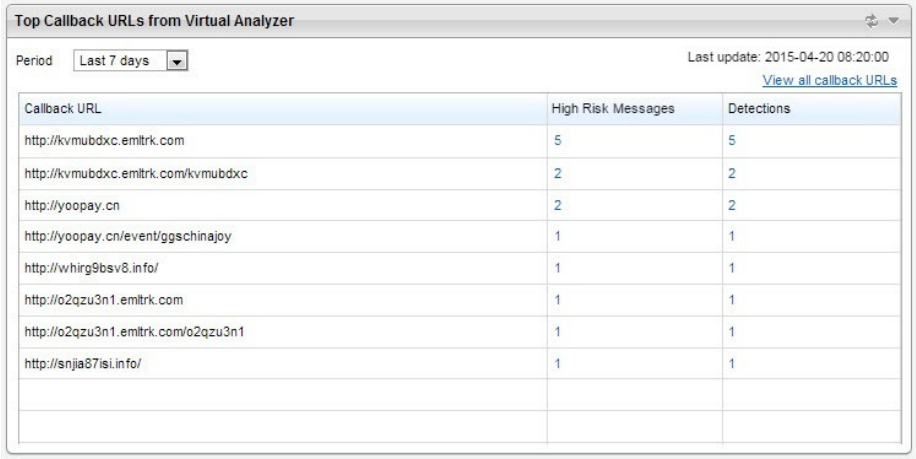
When Virtual Analyzer receives an object (file or URL) from the TippingPoint Advanced Threat Protection for Email email scanners, Virtual Analyzer observes whether the object connects to an external network address. A high-risk object attempts to perform a callback to a known C&C server host. Virtual Analyzer reports all connections (URLs, IP addresses, and host names) made by submitted samples, including possible malware callback and other suspicious connections.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

Click **View all callback hosts** to see all suspicious host objects found during analysis.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Top Callback URLs from Virtual Analyzer Widget




The **Top Callback URLs from Virtual Analyzer** widget shows the most common callback URLs contained in suspicious and high-risk email messages. A callback URL is the web address of a C&C server.

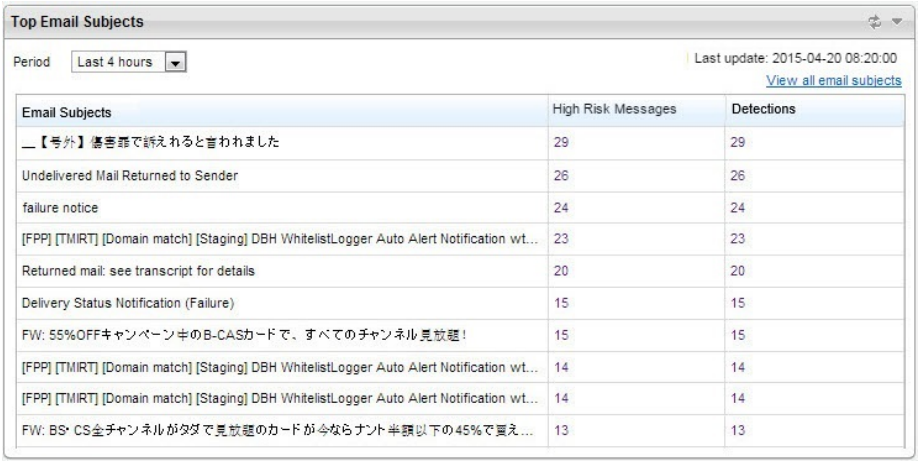
When Virtual Analyzer receives an object (file or URL) from the TippingPoint Advanced Threat Protection for Email email scanners, Virtual Analyzer observes whether the object connects to an external network address. A high-risk object attempts to perform a callback to a known C&C server host. Virtual Analyzer reports all connections (URLs, IP addresses, and host names) made by submitted samples, including possible malware callback and other suspicious connections.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

Click **View all callback URLs** to see all suspicious URL objects found during analysis.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Top Email Subjects Widget




| Email Subjects | High Risk Messages | Detections |
|---|---|---|
| __【号外】傷害罪で訴えれると言われました | 29 | 29 |
| Undelivered Mail Returned to Sender | 26 | 26 |
| failure notice | 24 | 24 |
| [FPP] [TMIRT] [Domain match] [Staging] DBH WhitelistLogger Auto Alert Notification wt... | 23 | 23 |
| Returned mail: see transcript for details | 20 | 20 |
| Delivery Status Notification (Failure) | 15 | 15 |
| FW: 55%OFFキャンペーン中のB-CASカードで、すべてのチャンネル見放題！ | 15 | 15 |
| [FPP] [TMIRT] [Domain match] [Staging] DBH WhitelistLogger Auto Alert Notification wt... | 14 | 14 |
| [FPP] [TMIRT] [Domain match] [Staging] DBH WhitelistLogger Auto Alert Notification wt... | 14 | 14 |
| FW: BS・CS全チャンネルがタダで見放題のカードが今ならナント半額以下の45%で買え... | 13 | 13 |

The **Top Email Subjects** widget shows the most common email message subjects contained in suspicious and high-risk email messages.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

Click **View all email subjects** to see the email subjects in detected messages during the selected time period.

For general widget tasks, see *Widget Tasks on page 3-6*.

# System Status

View **System Status** widgets to understand overall email message processing volume during different time periods for different risk levels and the current TippingPoint Advanced Threat Protection for Email appliance hardware status. The widgets graphically show how system performance affects message delivery.

## Processed Messages by Risk Widget

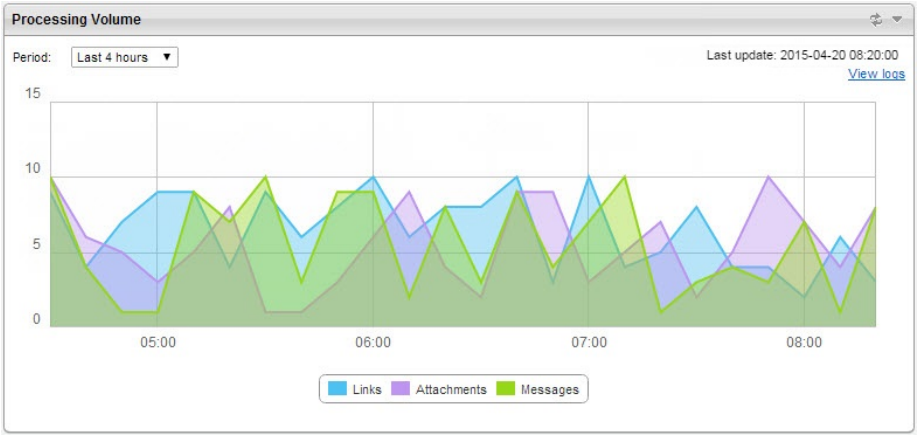
The **Processed Messages by Risk** widget shows all the email messages that TippingPoint Advanced Threat Protection for Email investigated and assigned a risk level. Email messages meeting policy exception and quarantine criteria do not appear in the widget.

The graph is based on the selected time period and represents each risk level as a separate bar. Mouse-over an area to learn more about the detections.

Click **View logs** to view the message tracking logs.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Processing Volume Widget




The **Processing Volume** widget shows all email messages, file attachments, and embedded links that TippingPoint Advanced Threat Protection for Email investigated.

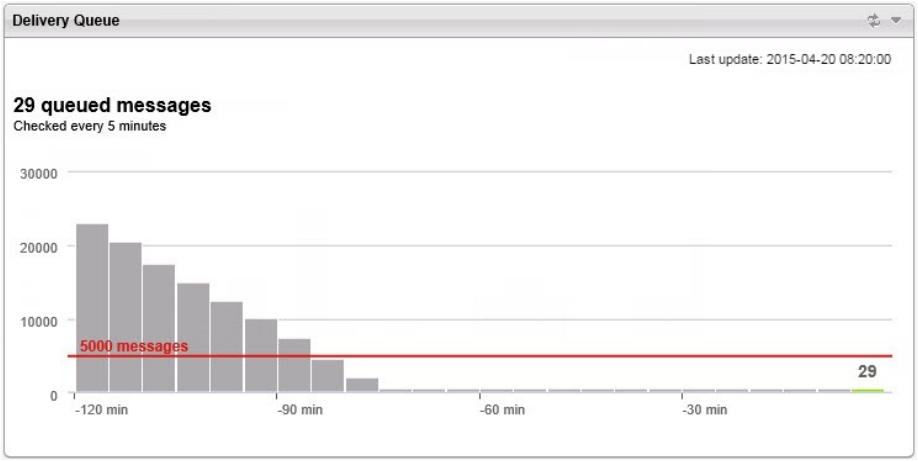
The graph is based on the selected period. The Y-axis represents the total number of processed email messages, attachments, or embedded links. The X-axis represents the period. Mouse-over a point on the graph to view the number of high risk messages and the period. Click on an item in the legend to toggle it on or off in the graph.

Click an item in the widget legend to show or hide data related to that metric.

Click **View logs** to view the message tracking logs.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Delivery Queue Widget

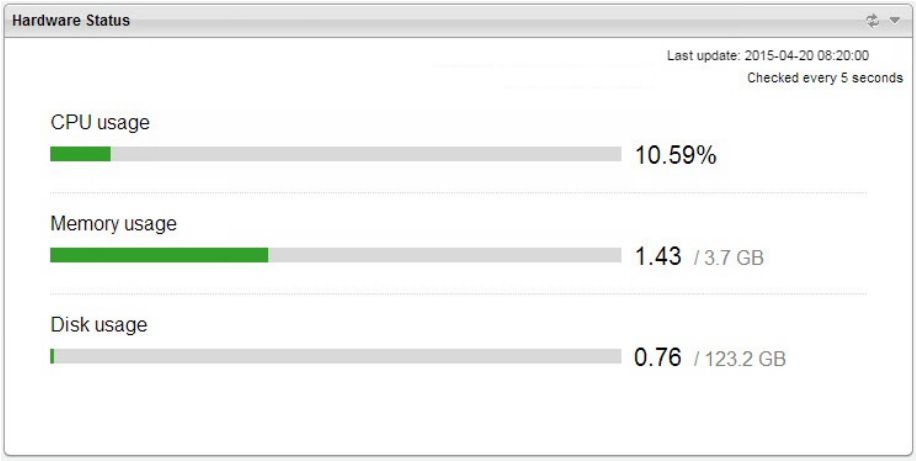



The **Delivery Queue** widget shows all email messages that TippingPoint Advanced Threat Protection for Email investigated, deemed safe, and delivers to the intended recipients.

The graph is based on the selected period. The Y-axis represents the email message count. The X-axis represents the period. Mouse-over a point on the graph to view the number of high risk messages and the period.

For general widget tasks, see *Widget Tasks on page 3-6*.

### Hardware Status Widget




The **Hardware Status** widget shows the TippingPoint Advanced Threat Protection for Email appliance's current CPU, memory, and disk usage within the last 5 seconds.

**Note**

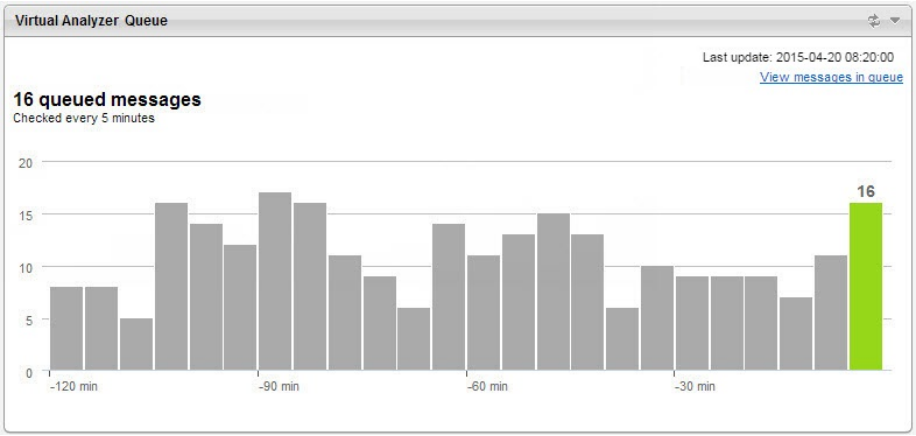
"Disk usage" refers to the amount of data stored on the disk partition.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Virtual Analyzer

View **Virtual Analyzer** widgets to assess Virtual Analyzer performance based on processing time, queue size, and the volume of suspicious objects discovered during analysis.

## Virtual Analyzer Queue Widget



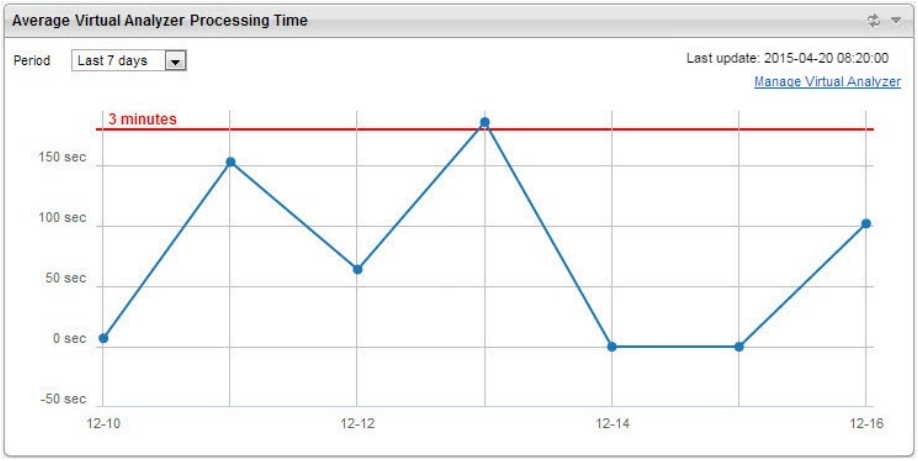

The **Virtual Analyzer Queue** widget shows all email messages queued in Virtual Analyzer, including email messages with attachments or links undergoing analysis.

The graph is based on the selected period. The Y-axis represents the email message count. The X-axis represents the period. Mouse-over a point on the graph to view the number of high risk messages and the period.

Click **View messages in queue** to view email messages currently undergoing analysis.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Average Virtual Analyzer Processing Time Widget



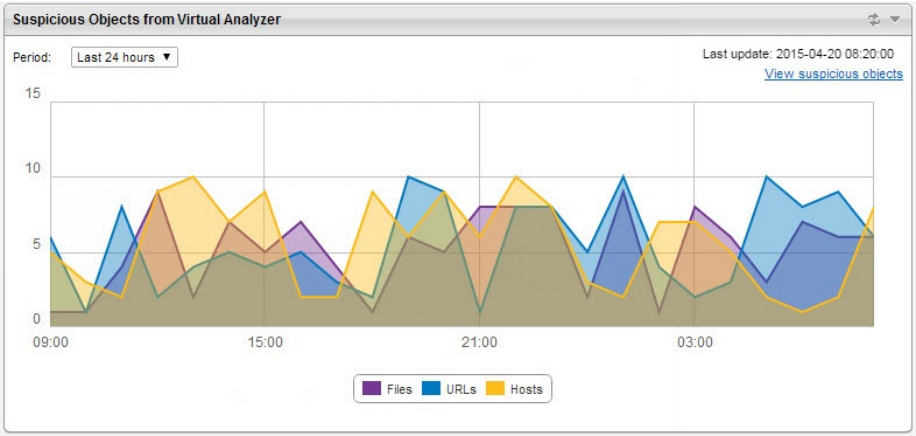

The **Average Virtual Analyzer Processing Time** widget shows the average time in seconds between when Virtual Analyzer receives an object and completes analysis.

The graph is based on the selected period. The Y-axis represents the average length of time required to analyze the object. The X-axis represents the period. Mouse-over a point on the graph to view the number of high risk messages and the period.

Click **Manage Virtual Analyzer** to reallocation instances, to add or remove images, or to make other changes to Virtual Analyzer settings.

For general widget tasks, see *Widget Tasks on page 3-6*.

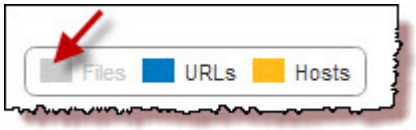
## Suspicious Objects from Virtual Analyzer Widget




The **Suspicious Objects from Virtual Analyzer** widget shows the suspicious objects found in Virtual Analyzer. Suspicious objects are objects with the potential to expose systems to danger or loss. Virtual Analyzer detects and analyzes suspicious IP addresses, host names, files, and URLs.

The graph is based on the selected period. The Y-axis represents the number of suspicious object detected. The X-axis represents the period. Mouse-over a point on the graph to view the number of high risk messages and the period.

Click an item in the widget legend to show or hide data related to that metric.




Click **View suspicious objects** to view suspicious objects affecting your network.

For general widget tasks, see *Widget Tasks on page 3-6*.

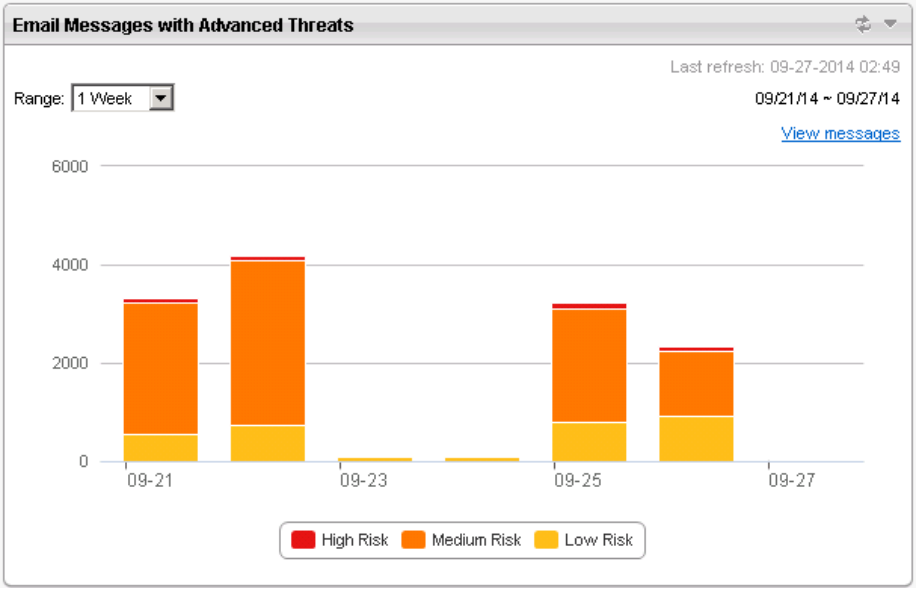
## Control Manager

In addition to widgets available through the TippingPoint Advanced Threat Protection for Email dashboard, Control Manager provides widgets that aggregate information about threatening mail traffic collected from all registered TippingPoint Advanced Threat Protection for Email appliances.

**Note**

Use the Control Manager management console to view Control Manager widgets. Control Manager widgets cannot be viewed through the TippingPoint Advanced Threat Protection for Email management console. For information about viewing widgets on the Control Manager management console, see the *Control Manager Administrator's Guide*.

### Email Messages with Advanced Threats Widget




The **Email Messages with Advanced Threats** widget shows all email messages with malicious and suspicious behavior. Suspicious behavior includes anomalous behavior,

false or misleading data, suspicious and malicious behavioral patterns, and strings that indicate system compromise but require further investigation to confirm.

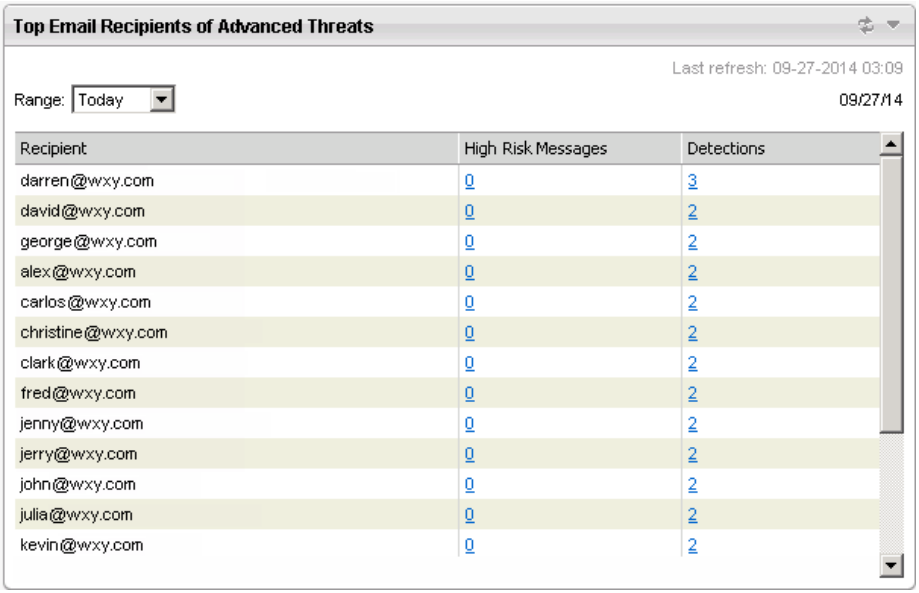
The graph is based on the selected period. The Y-axis represents the email message count. The X-axis represents the period. Mouse-over a point on the graph to view the number of high risk messages and the period.

Click an item in the widget legend to show or hide data related to that metric.

Click **View messages** to view all high-risk detections.

For general widget tasks, see *Widget Tasks on page 3-6*.

## Top Email Recipients of Advanced Threats Widget




| Recipient | High Risk Messages | Detections |
|---|---|---|
| darren@wxy.com | 0 | 3 |
| david@wxy.com | 0 | 2 |
| george@wxy.com | 0 | 2 |
| alex@wxy.com | 0 | 2 |
| carlos@wxy.com | 0 | 2 |
| christine@wxy.com | 0 | 2 |
| clark@wxy.com | 0 | 2 |
| fred@wxy.com | 0 | 2 |
| jenny@wxy.com | 0 | 2 |
| jerry@wxy.com | 0 | 2 |
| john@wxy.com | 0 | 2 |
| julia@wxy.com | 0 | 2 |
| kevin@wxy.com | 0 | 2 |

The **Top Email Recipients of Advanced Threats** widget shows the recipients who received the highest volume of suspicious messages.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

For general widget tasks, see *Widget Tasks on page 3-6*.

# Chapter 4

# Detections

Topics include:


- *Detected Risk on page 4-2*
- *Threat Type Classifications on page 4-5*
- *Detected Messages on page 4-7*
- *Suspicious Objects on page 4-18*
- *Quarantine on page 4-22*

# Detected Risk

Detected risk is potential danger exhibited by a suspicious email message.

TippingPoint Advanced Threat Protection for Email assesses email message risk using multi-layered threat analysis. Upon receiving an email message, TippingPoint Advanced Threat Protection for Email email scanners check the email message for known threats in the Trend Micro Smart Protection Network and Trend Micro Advanced Threat Scanning Engine. If the email message has unknown or suspicious characteristics, the email scanners send file attachments and embedded URLs to Virtual Analyzer for further analysis. Virtual Analyzer simulates the suspicious file and URL behavior to identify potential threats. TippingPoint Advanced Threat Protection for Email assigns a risk level to the email message based on the highest risk assigned between the TippingPoint Advanced Threat Protection for Email scanners and Virtual Analyzer.

For details about how TippingPoint Advanced Threat Protection for Email investigates email messages, see *A New Solution on page 1-8*.

## Email Message Risk Levels

The following table explains the email message risk levels after investigation. View the table to understand why an email message was classified as high, medium, or low risk.

**TABLE 4-1. Email Message Risk Definitions**

| RISK LEVEL | DESCRIPTION |
|---|---|
| High | A high-risk email message contains:<br>• Attachments with unknown threats detected as high risk by Virtual Analyzer<br>• Attachments detected as high risk based on YARA rules<br>• Attachments detected as high risk based on suspicious file matching |

| Risk Level | Description |
|---|---|
| Medium | A medium-risk email message contains:<br>• Known malware<br>• Known dangerous links<br>• Attachments detected as medium risk based on YARA rules<br>• Links detected as medium risk based on suspicious URL matching |
| Low | A low-risk email message contains:<br>• Known highly suspicious or suspicious links (Aggressive mode)<br>• Links detected as low risk by Virtual Analyzer<br>• Attachments detected as low risk by Virtual Analyzer<br>• Attachments detected as low risk based on YARA rules<br>• Links detected as low risk based on suspicious URL matching |
| No risk | A no-risk email message:<br>• Contains no suspicious attachments or links<br>• Contains known highly suspicious or suspicious links (Standard mode)<br>• Matches policy exception criteria |

| Risk Level | Description |
|---|---|
| Unrated | An unrated email message falls under any of the following categories:<br>• Bypassed scanning: Contains an attachment with a compression layer greater than 20 (the file has been compressed over twenty times)<br>• Unscannable archive: Contains a password-protected archive that could not be extracted and scanned using the password list or heuristically obtained passwords<br>• Unscannable message or attachment: Matches any of the following criteria:<br>  • Malformed email format<br>  • A system timeout occurred when Virtual Analyzer attempted to analyze the message<br>  • A system timeout occurred when Virtual Analyzer attempted to analyze some of the attachments or links and no other risks were detected<br>  • Virtual Analyzer was unable to analyze all of the attachments or links and no other risks were detected |

## Virtual Analyzer Risk Levels

The following table explains the Virtual Analyzer risk levels after object analysis. View the table to understand why a suspicious object was classified as high or low risk.

| Risk Level | Description |
|---|---|
| High | The object exhibited highly suspicious characteristics that are commonly associated with malware.<br>Examples:<br>• Malware signatures; known exploit code<br>• Disabling of security software agents<br>• Connection to malicious network destinations<br>• Self-replication; infection of other files<br>• Dropping or downloading of executable files by documents |
| Low | The object exhibited mildly suspicious characteristics that are most likely benign. |
| No Risk | The object did not exhibit suspicious characteristics. |

# Threat Type Classifications

The following table explains the threat types detected during scanning or analysis. View the table to understand the malicious activity affecting your network.

**Table 4-2. Email Message Threat Types**

| Threat Type | Classification |
|---|---|
| Targeted Malware | Malware made to look like they come from someone a user expects to receive email messages from, possibly a boss or colleague |
| Malware | Malicious software used by attackers to disrupt, control, steal, cause data loss, spy upon, or gain unauthorized access to computer systems |
| Malicious URL | A hyperlink embedded in an email message that links to a known malicious website |

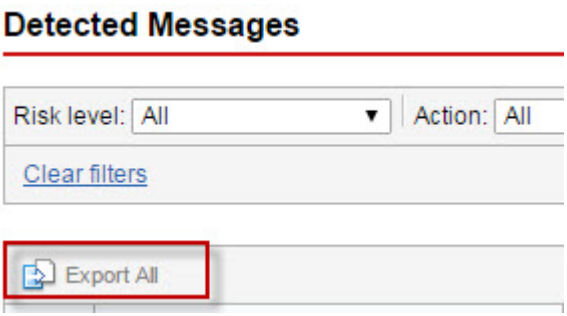
| THREAT TYPE | CLASSIFICATION |
|---|---|
| Suspicious File | A file that exhibits malicious characteristics<br><br>**Important**<br>Always handle suspicious files with caution. |
| Suspicious URL | A hyperlink embedded in an email message that links to an unknown malicious website |

# Exporting Search Results

You can export the search results for detected messages and suspicious objects.

**Procedure**

- Click **Export All** above the search results.




The search results download as a CSV file.

**Note**

Only the first 50000 entries in the query results are included in the CSV file.

# Detected Messages

Detected messages are email messages that contain malicious or suspicious content, embedded links, attachments, or social engineering attack related characteristics. TippingPoint Advanced Threat Protection for Email assigns a risk rating to each email message based on the investigation results.

Query detected messages to:

- Better understand the threats affecting your network and their relative risk
- Find senders and recipients of detected messages
- Understand the email subjects of detected messages
- Research attack sources that route detected messages
- Discover trends and learn about related detected messages
- See how TippingPoint Advanced Threat Protection for Email handled the detected message

## Viewing Detected Messages

Gain intelligence about the context of a spear-phishing attack by investigating a wide array of information facets. Review the email headers to quickly verify the email message origin and how it was routed. Investigate attacks trending on your network by correlating common characteristics (examples: email subjects that appear to be your Human Resource department or fake internal email addresses). Based on the detections, change your policy configuration and warn your users to take preventive measures against similar attacks.

---

**Procedure**

1. Go to **Detections** > **Detected Messages**.
2. Specify the search criteria.

   See *Detected Message Search Filters on page 4-9*.

3. Press ENTER.

   All email messages matching the search criteria appear.

4. View the results.

| HEADER | DESCRIPTION |
|---|---|
| ▸ | Investigate the email message to learn more about potential threats.<br><br>For details, see *Investigating a Detected Message on page 4-11*. |
| Detected | View the date and time that the suspicious email message was first detected in TippingPoint Advanced Threat Protection for Email.<br><br>**Note**<br>There is a short delay between when TippingPoint Advanced Threat Protection for Email receives an email message and when the email message appears on the **Detected Messages** screen. |
| Risk Level | View the level of potential danger exhibited in a suspicious email message. For details, see *Detected Risk on page 4-2*. |
| Recipients | View the detected message recipient email addresses. |
| To | View the primary recipient email address in the email header. |
| Sender | View the sending email address of the detected message. |
| From | View the author email address in the email header. |
| Email Subject | View the email subject of the suspicious email message. |
| | View the number of email messages with embedded malicious links. |
| | View the number of email messages with malicious file attachments. |
| Threat | View the name and classification of the discovered threat. For details, see *Threat Type Classifications on page 4-5*. |

| Header | Description |
|---|---|
| Action | View the final result after scanning and analyzing the email message. The result is the executed policy action.<br><br>**Note**<br>In BCC mode and SPAN/TAP mode, the action is always **Monitoring only**. |

## Detected Message Search Filters

The following table explains the basic search filters for querying suspicious messages. To view the detected messages, go to **Detections** > **Detected Messages**.

**Note**

Search filters do not accept wildcards. TippingPoint Advanced Threat Protection for Email uses fuzzy logic to match search criteria to email message data.

| Filter | Description |
|---|---|
| Risk level | Select **All** or the email message risk level. |
| Action | Select an action from the list.<br><br>For details, see *Configuring the Actions on page 5-2*.<br><br>**Note**<br>In BCC mode and SPAN/TAP mode, the action is always **Monitoring only**. |
| Recipients | Specify one or more recipient email addresses. Use a semicolon to separate multiple recipients. |
| Period | Select a predefined time range or specify a custom range. |

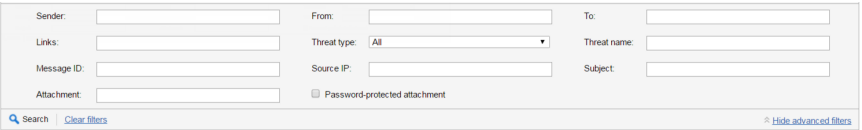
## Applying Advanced Filters

In addition to basic filters, you can apply advanced filters to query suspicious messages.

### Procedure

1. Click **Show advanced filters**.

   The advanced filters appear.




2. Specify the information to filter.

| FILTER | DESCRIPTION |
|---|---|
| Sender | Specify the sender email address. |
| From | Specify the author email address in the email header. |
| To | Specify a primary recipient email address in the email header. |
| Links | Specify a URL. |
| Threat type | Select a threat type from the list. For details, see *Threat Type Classifications on page 4-5*. |
| Message ID | Specify the unique message ID.<br>Example: `20160603021433.F0304120A7A@example.com` |

| FILTER | DESCRIPTION |
|---|---|
| Source IP | Specify the MTA IP address nearest to the email sender. The source IP is the IP address of the attack source, compromised MTA, or a botnet with mail relay capabilities.<br><br>A compromised MTA is usually a third-party open mail relay used by attackers to send malicious email messages or spam without detection.<br><br>**Note**<br>**Source IP** is the only search filter that requires an exact-string match. TippingPoint Advanced Threat Protection for Email does not use fuzzy logic to match search results for the source IP address. |
| Threat name | Specify the threat name provided by Trend Micro. The dashboard widgets and the **Detections** tab provide information about threat names.<br><br>For information about threat discovery capabilities, see *Scanning / Analysis on page 8-69*. |
| Subject | Specify the email message subject. |
| Attachment | Specify an attachment file name. |
| Password-protected attachment | Select email messages that contain a password-protected file. |

3. Click **Search**.

## Investigating a Detected Message

### Procedure

1. Search for the email message.

   See *Viewing Detected Messages on page 4-7*.

2. Click the arrow next to the email message in the table.

   The table row expands with more information.

3. Discover the email message details.

   See *Email Message Details on page 4-12*.

## Email Message Details

The following table explains the email message details viewable after expanding the search results.

| FIELD | DESCRIPTION |
|---|---|
| Overview | View the message ID, recipients, and source IP address of the email message to understand where the message came from and other tracking information. |
| Attachments | Get information about any files attached to the email message, including the file name, password, file type, risk level, the scan engine that identified the threat, and the name of detected threats. |
| Global Intelligence | Click **View in Threat Connect** to get correlated information about suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network, which provides relevant and actionable intelligence. |
| Links | Get information about any embedded suspicious URLs that appeared in the email message, including the URL, site category, risk level, the scan engine that identified the threat, and the name of detected threats. |
| Analysis Reports | View and in-depth PDF or HTML analysis report about this email message, including suspicious attachments or links, notable characteristics, callback destinations, and dropped or downloaded files. |

| FIELD | DESCRIPTION |
|---|---|
| Forensics | Get more information about this email message for further analysis. Download the email message or safely download the email message as an image.<br><br>For an email messages with one or more embedded suspicious URLs, you can download the email message and detection details log in a password-protected zip archive for further investigation. |
| Message Source | View the email message header content. |

## Viewing Affected Recipients

Affected recipients are recipients of malicious or suspicious email messages. Gain intelligence about who in your network is targeted by spear-phishing attacks or social engineering attacks and understand the attack behavior in related messages. Learn if your executive is targeted by the attacks and then raise his/her awareness about the attack pattern. Discovering a community of affected recipients belonging to the same department can indicate that the attacker has access to your company address book.

---

**Procedure**

1. Go to **Detections** > **Recipients**.
2. Specify the search criteria.
   - **Recipient** (email address)
   - **Period**
3. Press ENTER.

   All email messages matching the search criteria appear.
4. View the results.

| HEADER | DESCRIPTION |
|---|---|
| Recipient | View the detected message recipient email addresses. |

| HEADER | DESCRIPTION |
|---|---|
| Detections | View the email messages with malicious or suspicious characteristics. Signature-based detection involves searching for known patterns of data within executable code or behavior analysis. Click the number to see more information about the suspicious message. |
| High Risk | View the detected messages with malicious characteristics. |
| Medium Risk | View the detected messages with characteristics that are most likely malicious. |
| Low Risk | View the detected messages with suspicious characteristics. |
| | View the number of email messages with embedded malicious links. |
| | View the number of email messages with malicious file attachments. |
| Latest Detection | View the most recent occurrence of the detected message. |

## Viewing Attack Sources

An attack source is the first MTA with a public IP address that routes a suspicious message. For example, if a suspicious message travels the following route: IP1 (sender) > IP2 (MTA: 225.237.59.52) > IP3 (company mail gateway) > IP4 (recipient), TippingPoint Advanced Threat Protection for Email identifies 225.237.59.52 (IP2) as the attack source. By studying attack sources, you can identify regional attack patterns or attack patterns that involve the same mail server.

Gain intelligence about the prevalence of the attack detections and their relative risk to your network. Learn about the location of the attack, especially whether the attack source is an MTA in your organization or in a region where your organization does not operate.

**Procedure**

1. Go to **Detections** > **Attack Sources**.
2. Specify the search criteria.
   - **Attack source** (IP address)
   - **Country**
3. Select the **Period**.
4. Press ENTER.

   All email messages matching the search criteria appear.
5. View the results.

| HEADER | DESCRIPTION |
|---|---|
| Attack Source | View the IP address of the attack source. |
| Country | View the country where the attack source is located. |
| City | View the city where the attack source is located. |
| Detections | View the email messages with malicious or suspicious characteristics. Signature-based detection involves searching for known patterns of data within executable code or behavior analysis. Click the number to see more information about the suspicious message. |
| High Risk | View the detected messages with malicious characteristics. |
| Medium Risk | View the detected messages with characteristics that are most likely malicious. |
| Low Risk | View the detected messages with suspicious characteristics. |
| | View the number of email messages with embedded malicious links. |
| | View the number of email messages with malicious file attachments. |

| Header | Description |
|---|---|
| Latest Detection | View the most recent occurrence of the detected message. |

## Viewing Senders

Suspicious senders are senders of malicious or suspicious email messages. Find patterns in spoofed sender addresses and learn which social engineering techniques are employed. For example, the sender's email address appears as internal addresses, financial services (PayPal, banks), or other services (Gmail, Taobao, Amazon). Check the sender domain addresses and associated risk level to change policy settings or settings on the anti-spam gateway to block the suspicious sender email addresses at your mail gateway.

**Procedure**

1. Go to **Detections** > **Senders**.
2. Specify the search criteria.
   - **Sender** (email address)
   - **Period**
3. Press ENTER.

   All email messages matching the search criteria appear.
4. View the results.

| Header | Description |
|---|---|
| Sender | View the sending email address of the detected message. |
| Detections | View the email messages with malicious or suspicious characteristics. Signature-based detection involves searching for known patterns of data within executable code or behavior analysis. Click the number to see more information about the suspicious message. |

| Header | Description |
|---|---|
| High Risk | View the detected messages with malicious characteristics. |
| Medium Risk | View the detected messages with characteristics that are most likely malicious. |
| Low Risk | View the detected messages with suspicious characteristics. |
| | View the number of email messages with embedded malicious links. |
| | View the number of email messages with malicious file attachments. |
| Latest Detection | View the most recent occurrence of the detected message. |

## Viewing Email Subjects

Suspicious subjects are the email subjects of malicious or suspicious email messages. Find trends in common keywords or other social engineering techniques. Pretexting is the most common way to engage a victim. Look for email subjects that appear familiar to targeted recipients (examples: holiday party invitation, bank statement, or a common subject used in department newsletters) that can trick your users into opening the email message. If users trust the email subject, there is more chance that they will download a malicious attachment or follow a phishing link that appears to be a legitimate request for their domain credentials or customer information.

**Procedure**

1. Go to **Detections** > **Subjects**.
2. Specify the search criteria.
   - **Email subject**
   - **Period**
3. Press ENTER.

   All email messages matching the search criteria appear.

4. View the results.

| Header | Description |
|---|---|
| Email Subject | View the email subject of the suspicious email message. |
| Detections | View the email messages with malicious or suspicious characteristics. Signature-based detection involves searching for known patterns of data within executable code or behavior analysis. Click the number to see more information about the suspicious message. |
| High Risk | View the detected messages with malicious characteristics. |
| Medium Risk | View the detected messages with characteristics that are most likely malicious. |
| Low Risk | View the detected messages with suspicious characteristics. |
| | View the number of email messages with embedded malicious links. |
| | View the number of email messages with malicious file attachments. |
| Latest Detection | View the most recent occurrence of the detected message. |

# Suspicious Objects

Suspicious objects are objects with the potential to expose systems to danger or loss.

Query Suspicious Objects to:

- Better understand the threats affecting your network and their relative risk
- Assess the prevalence of suspicious hosts, URLs, and files
- Learn whether email messages contain embedded links or callback addresses
- Find infected endpoints in your network

- Proactively contain or block infections

## Viewing Suspicious Hosts

A suspicious host is an IP address or host name with the potential to expose systems to danger or loss. View suspicious hosts to understand your risk, find related messages, and assess the relative prevalence of the suspicious host.

---

**Procedure**

1. Go to **Detections** > **Suspicious Objects** > **Hosts**.
2. Specify the search criteria.
   - **Host** (IP address or host name)
   - **Period**
3. Press ENTER.

   All suspicious objects matching the search criteria appear.
4. View the results.

| HEADER | DESCRIPTION |
|---|---|
| Host | View the IP address or host name used by the suspicious object. |
| Port | View the port number used by the suspicious object. |
| Risk Level | View the level of potential danger in a sample after Virtual Analyzer executes the file or opens the URL. |
| Related Messages | View the messages containing the same suspicious object. |
| Last Message Recipients | View the most recent recipients of the email message containing suspicious objects. |

| HEADER | DESCRIPTION |
|---|---|
| Last Detection | View the date and time Virtual Analyzer last found the suspicious object in a submitted object. |

## Viewing Suspicious URLs

A suspicious URL is a web address with the potential to expose systems to danger or loss . View suspicious URLs to understand your risk, find related messages, and see the most recent occurrences.

**Procedure**

1. Go to **Detections** > **Suspicious Objects** > **URLs**.
2. Specify the search criteria.
   - **URL**
   - **Period**
3. Press ENTER.

   All suspicious objects matching the search criteria appear.
4. View the results.

| HEADER | DESCRIPTION |
|---|---|
| URL | View the web address of the suspicious object. |
| Risk Level | View the level of potential danger in a sample after Virtual Analyzer executes the file or opens the URL. |
| Related Messages | View the messages containing the same suspicious object. |
| Last Message Recipients | View the most recent recipients of the email message containing suspicious objects. |

| Header | Description |
|---|---|
| Last Detection | View the date and time Virtual Analyzer last found the suspicious object in a submitted object. |

## Viewing Suspicious Files

A suspicious file is the associated SHA-1 hash value with the potential to expose systems to danger or loss. View suspicious files to understand your risk, find related messages, and assess the relative prevalence of the suspicious file.

**Procedure**

1. Go to **Detections** > **Suspicious Objects** > **Files**.
2. Specify the search criteria.
   - **File SHA-1**
   - **Period**
3. Press ENTER.

   All suspicious objects matching the search criteria appear.
4. View the results.

| Header | Description |
|---|---|
| File SHA-1 | View the 160-bit hash value that uniquely identifies a file. |
| Related Messages | View the messages containing the same suspicious object. |
| Last Message Recipients | View the most recent recipients of the email message containing suspicious objects. |
| Last Detection | View the date and time Virtual Analyzer last found the suspicious object in a submitted object. |

# Quarantine

TippingPoint Advanced Threat Protection for Email quarantines suspicious email messages that meet certain policy criteria. View details about an email message before deciding whether to delete the email message or release it to the intended recipients.

Before deciding which action to perform, query the email messages that TippingPoint Advanced Threat Protection for Email quarantined.

Perform any of the following actions:

- Search for quarantined messages based on a variety of criteria
- Learn more about malicious file attachments and URLs
- Release or delete quarantined messages

## Viewing Quarantined Messages

**Procedure**

1. Go to **Detections** > **Quarantine**.
2. Specify the search criteria.

   See *Quarantine Search Filters on page 4-23*.
3. Press ENTER.

   All email messages matching the search criteria appear.
4. View the results.

| HEADER | DESCRIPTION |
|---|---|
| ▸ | Investigate the email message to learn more about potential threats.<br>For details, see *Investigating a Quarantined Email Message on page 4-24*. |

| Header | Description |
|---|---|
| Detected | View the date and time that the suspicious email message was first detected and quarantined in TippingPoint Advanced Threat Protection for Email.<br><br>**Note**<br>There is a short delay between when TippingPoint Advanced Threat Protection for Email receives an email message and when the email message appears on the **Quarantine** screen. |
| Risk Level | View the level of potential danger exhibited in a suspicious email message. For details, see *Detected Risk on page 4-2*. |
| Recipients | View the detected message recipient email addresses. |
| To | View the primary recipient email address in the email header. |
| Sender | View the sending email address of the detected message. |
| From | View the author email address in the email header. |
| Email Subject | View the email subject of the suspicious email message. |
| | View the number of email messages with embedded malicious links. |
| | View the number of email messages with malicious file attachments. |
| Threat | View the name and classification of the discovered threat. For details, see *Threat Type Classifications on page 4-5*. |

## Quarantine Search Filters

The following table explains the basic search filters for querying the quarantined email messages. To apply advanced filters, see *Applying Advanced Filters on page 4-10*.

To view the quarantine, go to **Detections** > **Quarantine**.

**Note**

Search filters do not accept wildcards. TippingPoint Advanced Threat Protection for Email uses fuzzy logic to match search criteria to email message data.

| FILTER | DESCRIPTION |
|---|---|
| Risk level | Select **All** or the email message risk level. |
| Recipient | Specify one or more recipient email addresses. Use a semicolon to separate multiple recipients. |
| Period | Select a predefined time range or specify a custom range. |

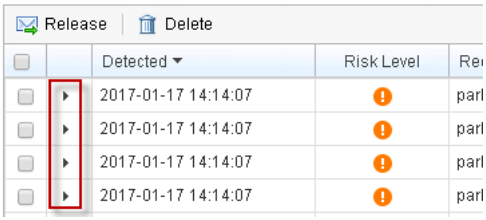
## Investigating a Quarantined Email Message

**Procedure**

1. Search for the email message.

   See *Viewing Quarantined Messages on page 4-22*.

2. Click the arrow next to the email message in the table.




   The table row expands with more information.

3. Discover the email message details.

   See *Quarantined Message Details on page 4-25*.

4. Take action upon the quarantined message.

   - Leave the message in the quarantine.

     **Note**

     Quarantined messages purge based on the settings configured on the **Storage Maintenance** screen.

     For details, see *Configuring Storage Maintenance on page 8-101*.

   - Click **Delete** to purge the email message from the quarantine.
   - Click **Release** to deliver the email message.

## Quarantined Message Details

The following table explains the email message details viewable after expanding the search results.

| FIELD | DESCRIPTION |
|---|---|
| Overview | View the message ID, recipients, and source IP address of the email message to understand where the message came from and other tracking information. |
| Attachments | Get information about any files attached to the email message, including the file name, password, file type, risk level, the scan engine that identified the threat, and the name of detected threats. |
| Links | Get information about any embedded suspicious URLs that appeared in the email message, including the URL, site category, risk level, the scan engine that identified the threat, and the name of detected threats. |
| Analysis Reports | View and in-depth PDF or HTML analysis report about this email message, including suspicious attachments or links, notable characteristics, callback destinations, and dropped or downloaded files. |

| Field | Description |
|---|---|
| Forensics | Get more information about this email message for further analysis. Download the email message or safely download the email message as an image. |
| Global Intelligence | Click **View in Threat Connect** to get correlated information about suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network, which provides relevant and actionable intelligence. |
| Message Source | View the email message header content. |

# Chapter 5

# Policy

Topics include:


- *Policy Overview on page 5-2*
- *Recipient Notification on page 5-4*
- *Message Tags on page 5-5*
- *Redirect Pages on page 5-6*
- *Policy Exceptions on page 5-7*

# Policy Overview

The streamlined policy architecture provides security controls that ensure protection against threats without complex policy rules.

Policy controls determine the action applied to detected threats. By default, the policy actions block and quarantine high-risk messages. You can fine-tune policy actions, notifications, message tags, and redirect pages to customize traffic handling behavior.

Policy exceptions reduce false positives. Configure exceptions to classify certain email messages as safe. Specify the safe senders, recipients, and X-header content, or add files, URLs, IP addresses and domains, and URL keywords. Safe email messages are discarded (BCC and SPAN/TAP mode) or delivered to the recipient (MTA mode) without further investigation.

## Configuring the Actions

**Procedure**

1. Go to **Policy** > **Policy** > **Actions**.
2. In **Actions by Risk Level**, configure the settings for High, Medium, and Low risk messages.
   a. Specify the **Action**.

| OPTION | ACTIONS TAKEN |
|---|---|
| Block and quarantine | • Does not deliver the email message<br>• Stores a copy in the quarantine area |
| Strip attachments, redirect links to blocking page, and tag | • Delivers the email message to the recipient<br>• Replaces suspicious attachments with a text file<br>• Redirects suspicious links to a blocking page<br>• Tags the email message subject with a string to notify the recipient |

| Option | Actions Taken |
|---|---|
| Strip attachments, redirect links to warning page, and tag | • Delivers the email message to the recipient<br>• Replaces suspicious attachments with a text file<br>• Redirects suspicious links to a warning page<br>• Tags the email message subject with a string to notify the recipient |
| Pass and tag | • Delivers the email message to the recipient<br>• Tags the email message subject with a string to notify the recipient |
| Pass with no action | • Delivers the email message to the recipient |

b. (Optional) Select **Notify recipients** to inform recipients about the applied policy action.

**Important**

TippingPoint Advanced Threat Protection for Email only sends recipient notifications when you select **Notify recipients**.

c. (Optional) In the **Subject tag** field, specify the string to insert in the subject of email messages.

d. (Optional) In the **X-Header** field, specify the string to add to the X-header.

3. In **Other Actions**, configure the following:

a. (Optional) Select **Quarantine a copy of the original message when stripping attachments or redirecting links** to store the email message with the attachment and URL in the quarantine for further investigation.

b. (Optional) Select **Apply action to messages with unscannable attachments** to apply either **Block and quarantine** or **Pass and tag** policy actions. These actions apply to password-protected archives that could not be extracted and scanned using the password list or heuristically obtained passwords.

| OPTION | ACTIONS TAKEN |
|---|---|
| Block and quarantine | • Does not deliver the email message<br>• Stores a copy in the quarantine area |
| Pass and tag | • Delivers the email message to the recipient<br>• Tags the email message subject with a string to notify the recipient |

c. (Optional) Select **Notify recipients** to inform recipients about the applied policy action.

**Important**

TippingPoint Advanced Threat Protection for Email only sends recipient notifications when you select **Notify recipients**.

d. If required, specify the string to insert into the subject of the email messages.

4. Click **Save**.

# Recipient Notification

A message is sent to notify recipients that an email message was processed and contained suspicious or malicious content. After investigation, TippingPoint Advanced Threat Protection for Email assigns a risk level to suspicious email messages.

## Configuring the Recipient Notification

**Procedure**

1. Go to **Policy** > **Policy** > **Recipient Notification**.
2. Configure the email notification sent to the recipient after TippingPoint Advanced Threat Protection for Email investigates and acts upon an email message.

Use the provided tokens to customize your message. For details, see *Recipient Notification Message Tokens on page C-2*.

3. Click **Save**.

# Message Tags

Message tags are sent to notify a recipient that the email message was processed and contained suspicious or malicious content. After investigation, TippingPoint Advanced Threat Protection for Email assigns a risk level to suspicious email messages. Configure unique message tags for different policy actions based on the risk level.

Message tags include the following items:

- A file that replaces a stripped suspicious attachment
- Text appended to the end of the message

**Note**

For information about how TippingPoint Advanced Threat Protection for Email assigns the risk level, see *Detected Risk on page 4-2*.

## Specifying Message Tags

**Procedure**

1. Go to **Policy** > **Policy** > **Message Tags**.
2. Specify the message tag settings.

| Option | Description |
|---|---|
| Attachment | Upload a file to replace an attachment stripped from the email message. |
| End Stamp | Specify the message to append to all processed email messages. |

3. Click **Save**.

# Redirect Pages

TippingPoint Advanced Threat Protection for Email uses policy actions to determine if a redirect page blocks or warns users from opening suspicious links. You can customize the redirect pages with your own logo, message body, and administrator contact information.

## Customizing the Redirect Pages

When using built-in redirect pages, ensure that the message recipients can open the redirect pages. If the redirect pages cannot be opened, check your network configuration or use external redirect pages.

**Procedure**

1. Go to **Policy** > **Policy** > **Redirect Pages**.
2. Select whether to use external or built-in redirect pages.
   - **Use external redirect pages**: Type the page URL of the **Blocking page** to use
   - **Use built-in redirect pages**: Select to show the **Warning page** or **Blocking page**.

     Do the following to edit the redirect page:

     - Select **Use host name in link. Configure the host name to enable this setting.**.

       **Tip**

       Trend Micro recommends enabling this setting to prevent users from accidentally visiting the malicious website.

- Click **host name** to redirect to the **System Settings** screen where you can view or change the **Host name** setting under **Host Name / Gateway / DNS**.

  **Note**

  Save any changes before navigating away from the **Policy** screen.

- Click the **Replace image** ( ) icon to browse and select an image file.

  **Important**

  Images must be 500x60 pixels and in GIF, JPEG, or PNG format.

- Click the **Edit** ( ) icon to open the field for editing.
- Click the **Enable** hyperlink to open the **Administrator Contact Information** fields for editing.

3. Click **Save**.

# Policy Exceptions

Policy exceptions reduce false positives. Configure exceptions to classify certain email messages as safe. Specify the safe senders, recipients, and X-header content, or add files, URLs, IP addresses and domains, and URL keywords. Safe email messages are discarded (BCC and SPAN/TAP mode) or delivered to the recipient (MTA mode) without further investigation.

**Note**

If TippingPoint Advanced Threat Protection for Email is registered to Control Manager, TippingPoint Advanced Threat Protection for Email synchronizes object exceptions from Control Manager every 10 minutes.

## Configuring Message Exceptions

TippingPoint Advanced Threat Protection for Email considers specified senders, recipients, or X-header content in the exceptions list safe.

**Procedure**

1. Go to **Policy** > **Exceptions** > **Messages**.
2. Specify email message exception criteria.
   - **Senders**
   - **Recipients**
   - **X-header**

   **Note**

   TippingPoint Advanced Threat Protection for Email ignores case-sensitivity for X-header exceptions.

   TippingPoint Advanced Threat Protection for Email supports the use of the wildcard asterisk (*) character to specify an entire domain. For example, to create a **Senders** exception for the domain `abc.com`, type the following:

   ```
   *@abc.com
   ```

3. Click **Save**.

## Managing Object Exceptions

Perform any of the following tasks to manage object exceptions.

**Procedure**

- Specify search filters to control the display and to view existing exceptions.

  The following table describes the **Source** filter options.

| Option | Description |
|---|---|
| Local | Displays object exception that are added manually on TippingPoint Advanced Threat Protection for Email. |
| Control Manager | Displays object exceptions that are synchronized from Control Manager.<br><br>**Note**<br>If TippingPoint Advanced Threat Protection for Email is registered to Control Manager, TippingPoint Advanced Threat Protection for Email synchronizes object exceptions from Control Manager every 10 minutes. |
| Web service | Displays object exceptions that are imported through the HTTP web service. |

- Modify the objects considered safe.

  The following table describes the actions on object exceptions.

| Action | Description |
|---|---|
| Add | Add a new object to the exceptions list. Optionally include a note to help you better understand the object exception.<br><br>For more information, see *Adding Object Exceptions on page 5-11*. |

| Action | Description |
|---|---|
| Import | Select the CSV file to import.<br>The format for each line is:<br><type>,<object>,[source],[notes]<br>• <type> values: IP address, Domain, URL, Files<br>• <object> values: IP address, domain, URL, or SHA-1 hash value<br>• (Optional) [source] values: Control Manager, Local, web service<br>• (Optional) [notes]: Any additional information in any format<br>Valid CSV examples:<br>• Links,www.example.com,local,customer can view this site<br>• IP address,10.10.10.10,,HR address<br>• Files, 3395856CE81F2B7382DEE72602F798B642F14140, Control Manager,SHA-1 of CA certificate<br>• Domain,example.com,,Added<br>For more information, see *Importing Object Exceptions on page 5-12*. |
| Delete | Delete the selected objects. |
| Delete All | Delete all objects. |
| Export | Export the selected objects. |
| Export All | Export the entire exceptions list to a CSV file. |

## Adding Object Exceptions

TippingPoint Advanced Threat Protection for Email passes email messages containing only safe files, URLs, IP addresses, and domains without further investigation. If an email message contains one safe URL and another unknown URL, TippingPoint Advanced Threat Protection for Email investigates the unknown URL. Virtual Analyzer also ignores safe files and URLs during sandbox analysis.

**Procedure**

1. Go to **Policy** > **Exceptions** > **Objects**.
2. Click **Add**.
3. Specify file, URL, IP address, or domain exception criteria.
   - For files, select **File** for the type and then specify the SHA-1 hash value.

     **Note**

     Threat Connect correlates suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network to provide relevant and actionable intelligence.

   - For URLs, select **URL** for the type and then specify the web address.

     **Note**

     Specify a complete URL or use a wildcard (*) for subdomains.

   - For IP addresses, select **IP address** for the type and then specify the web address.
   - For domains, select **Domain** for the type and then specify the web address.
4. (Optional) Specify a note.
5. (Optional) Click **Add more** to specify multiple file, URL, IP address, or domain exception criteria at the same time.
   a. Specify file, URL, IP address, or domain exception criteria.

b. Click **Add to List**. The criterion is added to the object list.

6. Click **Add**.

## Importing Object Exceptions

You can import exceptions from a properly-formatted CSV file.

**Procedure**

1. Go to **Policy** > **Exceptions** > **Objects**.
2. Click **Import**.
3. Do one of the following:
   - 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.
4. Click **Import**.

   The imported exceptions display in the list with **Web service** as the source.

# Configuring URL Keyword Exceptions

URLs that contain any of the specified keywords are considered one-click URLs and will not be accessed by TippingPoint Advanced Threat Protection for Email.

**Procedure**

1. Go to **Policy** > **Exceptions** > **URL Keywords**.
2. Specify URL keywords.

**Note**

Specify one keyword per line.

3. Click **Save**.

# Chapter 6

# Alerts and Reports

Topics include:


- *Alerts on page 6-2*
- *Reports on page 6-22*

# Alerts

Alerts provide immediate intelligence about the state of TippingPoint Advanced Threat Protection for Email. Alerts are classified into three categories:

- Critical alerts are triggered by events that require immediate attention
- Important alerts are triggered by events that require observation
- Informational alerts are triggered by events that require limited observation (most likely benign)

The threshold to trigger each alert is configurable.

**Note**

For information about available message tokens in alert notifications, see *Alert Notification Message Tokens on page C-3*.

## Critical Alerts

The following table explains the critical alerts triggered by events requiring immediate attention. TippingPoint Advanced Threat Protection for Email considers malfunctioning sandboxes, stopped services, unreachable relay MTAs, and license expiration as critical problems.

**TABLE 6-1. Critical Alerts**

| NAME | CRITERIA (DEFAULT) | CHECKING INTERVAL (DEFAULT) |
|---|---|---|
| Virtual Analyzer Stopped | Virtual Analyzer encountered an error and was unable to recover<br><br>**Note**<br>This alert is only available when using a local Virtual Analyzer. | Immediate |

| Name | Criteria (Default) | Checking Interval (Default) |
|---|---|---|
| Service Stopped | A service has stopped and cannot be restarted | Immediate |
| Relay MTAs Inaccessible | TippingPoint Advanced Threat Protection for Email sent 10 email messages to the domain relay MTA without a reply | Once every 5 minutes |
| License Expiration | The TippingPoint Advanced Threat Protection for Email license is about to expire or has expired | Immediate |

## Important Alerts

The following table explains the important alerts triggered by events that require observation. TippingPoint Advanced Threat Protection for Email considers traffic surges, suspicious message detections, hardware capacity changes, certain sandbox queue activity, and component update issues as important events.

**Table 6-2. Important Alerts**

| Name | Criteria (Default) | Checking Interval (Default) |
|---|---|---|
| Suspicious Messages Identified | 1 or more messages detected with threats | Once every 5 minutes |
| Watchlisted Recipients at Risk | 1 or more messages detected with threats sent to watchlist recipients | Once every 5 minutes |
| Quarantined Messages | At least 10 messages detected and quarantined | Once every 30 minutes |
| Long Message Delivery Queue | At least 500 messages in delivery queue | Once every 5 minutes |
| High CPU Usage | CPU usage is at least 90% | Once every 5 minutes |

| Name | Criteria (Default) | Checking Interval (Default) |
|---|---|---|
| Long Virtual Analyzer Queue | At least 20 messages in Virtual Analyzer queue | Immediate |
| Long Virtual Analyzer Processing Time | Average Virtual Analyzer processing time is greater than 15 minutes | Once every hour |
| Low Free Disk Space | Disk space is 5GB or less | Once every 30 minutes |
| Component Update/ Rollback Unsuccessful | An update/rollback was not successful | Immediate |
| Email Messages Timed Out Without Analysis Results | At least 1 email message timed out without analysis results | Once every 5 minutes |
| Low Free Quarantine Disk Space | Free quarantine disk space left is 10% or less | Once every 30 minutes |
| High Memory Usage | Memory usage is at least 90% | Once every 5 minutes |

## Informational Alerts

The following table explains the alerts triggered by events that require limited observation. Surges in detection and processing, and completed updates are most likely benign events.

**Table 6-3. Informational Alerts**

| Name | Criteria (Default) | Checking Interval (Default) |
|---|---|---|
| Detection Surge | At least 10 messages detected | Once every hour |
| Processing Surge | At least 20,000 messages processed | Once every hour |

| NAME | CRITERIA (DEFAULT) | CHECKING INTERVAL (DEFAULT) |
|---|---|---|
| Component Update/ Rollback Successful | An update/rollback was successfully completed | Immediate |

## Configuring Alert Notifications

Add at least one notification recipient for all critical and important alerts.

**Note**

Configure the SMTP server to send notifications. For details, see *Configuring the Notification SMTP Server on page 8-14*.

**Procedure**

1. Go to **Alerts / Reports** > **Alerts** > **Rules**.
2. Click the name of an alert under the **Rule** column.

   The alert rule configuration screen appears.
3. Configure the alert parameters.

   For details, see *Alert Notification Parameters on page 6-7*.
4. Click **Save**.
5. Click **Back** to return to the **Alert Rules** screen.

## Viewing Triggered Alerts

**Procedure**

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

2. Specify the search criteria.
   - **Level**
   - **Type**
   - **Rule Name**
   - **Period**
3. View alert details.

| HEADER | DESCRIPTION |
|---|---|
| Triggered | The date and time when the alert occurred |
| Level | The importance of the alert: critical, important, or informational |
| Rule | The name of the alert rule |
| Criteria | The alert rule criteria that triggered the alert |
| Detections | The triggered alert occurrences |
| Notification Recipients | The most recent alert notification recipients |
| Notification Subject | The most recent alert notification subject |

## Managing Alerts

Perform any of the following tasks to manage alerts.

**Procedure**

- Specify search filters to control the display and view existing exceptions.
- Export or purge triggered alerts after review.

| OPTION | DESCRIPTION |
|---|---|
| Delete | Delete the selected alerts. |
| Export | Export up to 50000 alerts to a CSV file. |

## Alert Notification Parameters

All triggered alert rules can notify recipients with a custom email message. Some alerts have additional parameters, including message count, checking interval, or risk level.

### Critical Alert Parameters

**Note**

For explanations about available message tokens in each alert, see *Alert Notification Message Tokens on page C-3*.

**TABLE 6-4. Virtual Analyzer Stopped**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |

| Parameter | Description |
|---|---|
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%DateTime%`<br>• `%DeviceIP%`<br>• `%DeviceName%` |

**Table 6-5. Service Stopped**

| Parameter | Description |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%DateTime%`<br>• `%DeviceIP%`<br>• `%DeviceName%`<br>• `%ServiceName%` |

**Table 6-6. Relay MTAs Inaccessible**

| Parameter | Description |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |

| Parameter | Description |
|---|---|
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%DateTime%`<br>• `%DeviceName%`<br>• `%DeviceIP%`<br>• `%MessageList%`<br>• `%MTAList%` |

**Table 6-7. License Expiration**

| Parameter | Description |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |

| PARAMETER | DESCRIPTION |
|---|---|
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%DateTime%`<br>• `%DaysBeforeExpiration%`<br>• `%DeviceName%`<br>• `%DeviceIP%`<br>• `%ExpirationDate%`<br>• `%LicenseStatus%`<br>• `%LicenseType%` |

## Important Alert Parameters

**Note**

For explanations about available message tokens in each alert, see *Alert Notification Message Tokens on page C-3*.

**TABLE 6-8. Suspicious Messages Identified**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Email messages | Select the detections threshold that will trigger the alert. |
| Risk level | Select the risk level that will trigger the alert. |
| Alert frequency | View the time interval that TippingPoint Advanced Threat Protection for Email checks for the alert rule criteria. |

| Parameter | Description |
|---|---|
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%DateTime%`<br>• `%DeviceIP%`<br>• `%DeviceName%`<br>• `%MessageList%` |

**Table 6-9. Watchlisted Recipients at Risk**

| Parameter | Description |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Recipient watchlist | Add recipients to the watchlist. The alert triggers when any watchlist recipient receives a suspicious or malicious email message. |
| Email messages | Select the detections threshold that will trigger the alert. |
| Risk level | Select the risk level that will trigger the alert. |
| Alert frequency | View the time interval that TippingPoint Advanced Threat Protection for Email checks for the alert rule criteria. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |

| Parameter | Description |
|---|---|
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%DateTime%`<br>• `%DeviceIP%`<br>• `%DeviceName%`<br>• `%MessageList%` |

**Table 6-10. Long Message Delivery Queue**

| Parameter | Description |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Email messages | Select email message threshold that will trigger the alert. |
| Alert frequency | View the time interval that TippingPoint Advanced Threat Protection for Email checks for the alert rule criteria. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%DateTime%`<br>• `%DeliveryQueue%`<br>• `%DeviceIP%`<br>• `%DeviceName%`<br>• `%QueueThreshold%` |

**TABLE 6-11. High CPU Usage**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Average CPU usage | Specify the threshold for the average CPU usage that will trigger the alert. |
| Alert frequency | View the time interval that TippingPoint Advanced Threat Protection for Email checks for the alert rule criteria. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%CPUThreshold%`<br>• `%CPUUsage%`<br>• `%DateTime%`<br>• `%DeviceIP%`<br>• `%DeviceName%` |

**TABLE 6-12. Long Virtual Analyzer Queue**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Submissions | Select email message threshold that will trigger the alert. |
| Alert frequency | View the time interval that TippingPoint Advanced Threat Protection for Email checks for the alert rule criteria. |

| Parameter | Description |
|---|---|
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%DateTime%`<br>• `%DeviceIP%`<br>• `%DeviceName%`<br>• `%SandboxQueue%`<br>• `%SandboxQueueThreshold%` |

**Table 6-13. Long Virtual Analyzer Processing Time**

| Parameter | Description |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Average processing time | Select the average time threshold required to process samples in the sandbox queue during the past hour that will trigger the alert. |
| Alert frequency | View the time interval that TippingPoint Advanced Threat Protection for Email checks for the alert rule criteria. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |

| Parameter | Description |
|---|---|
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%AveSandboxProc%`<br>• `%DateTime%`<br>• `%DeviceIP%`<br>• `%DeviceName%`<br>• `%SandboxProcThreshold%` |

**Table 6-14. Low Free Disk Space**

| Parameter | Description |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Free Disk space | The lowest disk space threshold in GB that triggers the alert. |
| Alert frequency | View the time interval that TippingPoint Advanced Threat Protection for Email checks for the alert rule criteria. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%DateTime%`<br>• `%DeviceIP%`<br>• `%DeviceName%`<br>• `%DiskSpace%` |

**TABLE 6-15. Component Update/Rollback Unsuccessful**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%ComponentList%`<br>• `%DateTime%`<br>• `%DeviceIP%`<br>• `%DeviceName%` |

**TABLE 6-16. Email Messages Timed Out Without Analysis Results**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Email messages | Select email message threshold that will trigger the alert. |
| Alert frequency | View the time interval that TippingPoint Advanced Threat Protection for Email checks for the alert rule criteria. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |

| Parameter | Description |
|---|---|
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%MessageList%`<br>• `%DateTime%`<br>• `%DeviceName%`<br>• `%DeviceIP%`<br>• `%ConsoleURL%` |

**Table 6-17. Low Free Quarantine Disk Space**

| Parameter | Description |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Free quarantine disk space | The lowest disk space threshold that triggers the alert.<br>**Note**<br>**Free quarantine disk space** refers to the percentage of space remaining on the disk partition. |
| Alert frequency | View the time interval that TippingPoint Advanced Threat Protection for Email checks for the alert rule criteria. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |

| Parameter | Description |
|---|---|
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%DiskSpace%`<br>• `%DateTime%`<br>• `%DeviceName%`<br>• `%DeviceIP%`<br>• `%ConsoleURL%` |

**Table 6-18. Quarantined Messages**

| Parameter | Description |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Quarantined messages | Specify the quarantine message threshold that will trigger the alert. |
| Risk level | Select the risk level that will trigger the alert. |
| Alert frequency | View the time interval that TippingPoint Advanced Threat Protection for Email checks for the alert rule criteria. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |
| Message | Use the following tokens to customize your message:<br>• `%MessageList%`<br>• `%DateTime%`<br>• `%DeviceName%`<br>• `%DeviceIP%`<br>• `%ConsoleURL%` |

**TABLE 6-19. High Memory Usage**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Average memory usage | Select the threshold for avergae memory usage that will trigger the alert.<br><br>**Note**<br>**Free disk space** refers to the amount of space remaining on the disk partition. |
| Alert frequency | View the time interval that TippingPoint Advanced Threat Protection for Email checks for the alert rule criteria. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |
| Message | Specify the body of the triggered alert email message.<br><br>Use the following tokens to customize your message:<br><br>• `%MemoryThreshold%`<br>• `%MemoryUsage%`<br>• `%DateTime%`<br>• `%DeviceIP%`<br>• `%DeviceName%`<br>• `%ConsoleURL%` |

## Informational Alert Parameters

**Note**

For explanations about available message tokens in each alert, see *Alert Notification Message Tokens on page C-3*.

**TABLE 6-20. Detection Surge**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Detected messages | Select the detections threshold that will trigger the alert. |
| Alert frequency | View the time interval that TippingPoint Advanced Threat Protection for Email checks for the alert rule criteria. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%DateTime%`<br>• `%DetectionCount%`<br>• `%DetectionThreshold%`<br>• `%DeviceIP%`<br>• `%DeviceName%`<br>• `%Interval%` |

**TABLE 6-21. Processing Surge**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Processed messages | The email message threshold that triggers the alert. |

| Parameter | Description |
|---|---|
| Alert frequency | View the time interval that TippingPoint Advanced Threat Protection for Email checks for the alert rule criteria. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%DateTime%`<br>• `%DeviceIP%`<br>• `%DeviceName%`<br>• `%Interval%`<br>• `%ProcessingCount%`<br>• `%ProcessingThreshold%` |

**Table 6-22. Component Update/Rollback Successful**

| Parameter | Description |
|---|---|
| Status | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages. |
| Recipients | Specify the recipients who will receive the triggered alert email message. |
| Subject | Specify the subject of the triggered alert email message. |

| PARAMETER | DESCRIPTION |
|---|---|
| Message | Specify the body of the triggered alert email message.<br>Use the following tokens to customize your message:<br>• `%ConsoleURL%`<br>• `%ComponentList%`<br>• `%DateTime%`<br>• `%DeviceIP%`<br>• `%DeviceName%` |

# Reports

TippingPoint Advanced Threat Protection for Email provides reports to assist in mitigating threats and optimizing system settings. Generate reports on demand or set a daily, weekly, or monthly schedule. TippingPoint Advanced Threat Protection for Email offers flexibility in specifying the content for each report.

The reports generate in PDF format.

## Scheduling Reports

Scheduled reports automatically generate according to the configured schedules.

**Note**

Configure the SMTP server to send notifications. For details, see *Configuring the Notification SMTP Server on page 8-14*.

**Procedure**

1. Go to **Alerts / Reports** > **Reports** > **Schedules**.
2. Enable a scheduled report by selecting the associated interval.

- **Generate daily report**
- **Generate weekly report**
- **Generate monthly report**

3. Specify when to generate the report.

> **Note**
> When a monthly report schedule is set to generate reports on the 29th, 30th, or 31st day, the report generates on the last day of the month for months with fewer days. For example, if you select 31, the report generates on the 28th (or 29th) in February, and on the 30th in April, June, September, and November.

4. Specify the recipients.

> **Note**
> Separate multiple recipients with a semicolon.

5. Optional: Select the **Include detailed information** check box to include a list containing the high-risk messages, alerts, and suspicious objects found during analysis.
6. Click **Save**.

## Generating On-Demand Reports

**Procedure**

1. Go to **Alerts / Reports** > **Reports** > **On Demand** .
2. Configure report settings.

| Option | Description |
|---|---|
| Period | Select the scope and start time for report generation. |

| OPTION | DESCRIPTION |
|---|---|
| Include detailed information | Optional: Select the check box to include a list containing the high-risk messages, alerts, and suspicious objects found during analysis. |
| Recipients | Specify the recipients. Separate multiple recipients with a semicolon. |

3. Click **Generate**.

   The report generates and the following actions occur:

   - The report appears at **Alerts / Reports** > **Reports** > **Generated Reports**.
   - Report notifications are sent to recipients.

# Chapter 7

# Logs

Topics include:


- *Email Message Tracking on page 7-2*
- *MTA Events on page 7-6*
- *System Events on page 7-7*
- *Time-Based Filters and DST on page 7-9*

# Email Message Tracking

Track any email message that passed through TippingPoint Advanced Threat Protection for Email, including blocked and delivered messages. TippingPoint Advanced Threat Protection for Email records message details, including the sender, recipients, and the taken policy action.

Message tracking logs indicate if an email message was received or sent by TippingPoint Advanced Threat Protection for Email. Message tracking logs also provide evidence about TippingPoint Advanced Threat Protection for Email investigating an email message.

## Querying Message Tracking Logs

**Procedure**

1. Go to **Logs** > **Message Tracking**.
2. Specify the search criteria.

**Note**

No wildcards are supported. TippingPoint Advanced Threat Protection for Email uses fuzzy logic to match search results.

| FILTER | DESCRIPTION |
|---|---|
| Period | Select a predefined time range or specify a custom range. |
| Recipients | Specify a recipient email address. Only one address is allowed. |
| To | Specify a primary recipient email address in the email header. |
| Sender | Specify the sender email address. |
| From | Specify the author email address in the email header. |
| Subject | Specify the email message subject. |

| FILTER | DESCRIPTION |
|---|---|
| Message ID | Specify the unique message ID.<br><br>Example: `20160603021433.F0304120A7A@example.com` |
| Source IP | Specify the MTA IP address nearest to the email sender. The source IP is the IP address of the attack source, compromised MTA, or a botnet with mail relay capabilities.<br><br>A compromised MTA is usually a third-party open mail relay used by attackers to send malicious email messages or spam without detection. |
| Risk level | Select **All** or the email message risk level. |
| Latest status | Select any of the following check boxes:<br><br>• **Deleted from quarantine**: Messages that were manually deleted from the **Quarantine**.<br><br>• **Delivered/Processing completed**: Messages that were delivered. In BCC mode and SPAN/TAP mode, email messages with this status are discarded.<br><br>• **Delivery unsuccessful**: Messages that could not be delivered. In BCC mode and SPAN/TAP mode, email messages are never delivered.<br><br>• **Quarantined**: Messages that were quarantined in keeping with your TippingPoint Advanced Threat Protection for Email policies. In BCC mode and SPAN/TAP mode, email messages are never quarantined.<br><br>• **Queued for delivery**: Messages that are pending delivery. In BCC mode and SPAN/TAP mode, email messages with this status are queued to be discarded.<br><br>• **Queued for sandbox analysis**: Messages that are pending analysis. |

3. Click **Query**.

   Logs matching the search criteria appear in the table. The query results include message ID, recipients, sender, subject, risk level, latest status, and received timestamp.

**Note**

You can clear the search criteria by clicking **Clear filters**.

4. View the results.

- Click the ▷ icon next to a row to view detailed information about the email message.

| FIELD | DESCRIPTION |
|---|---|
| Message details | Source IP: Displays the MTA IP address nearest to the email message sender.<br><br>Example: `123.123.123.123`. |
| Processing history | View how TippingPoint Advanced Threat Protection for Email processed the email message. The following are the possible processing actions:<br><br>• **Action set to 'pass'**:<br>  • The **Pass** policy action was applied to the email message.<br>  • A copy of the email message was released by the user. This only applies if the **Strip attachments, redirect links to blocking page, and tag** and **Strip attachments, redirect links to warning page, and tag** policies were applied to the original email message.<br><br>• **Deleted**: The email message was deleted from the **Quarantine** folder.<br><br>• **Delivered**: The email message was delivered.<br><br>• **Not analyzed**: Virtual Analyzer was unable to complete the analysis for the reason specified.<br><br>• **Processing completed**: Analysis was completed and the email message was discarded. This is the final status in BCC and SPAN/TAP mode.<br><br>• **Quarantined**: The email message was quarantined in keeping with your TippingPoint |

| FIELD | DESCRIPTION |
|---|---|
| | Advanced Threat Protection for Email policies. In BCC mode and SPAN/TAP mode, email messages are never quarantined.<br>• **Queued for delivery**: The email message is pending delivery. In BCC mode and SPAN/TAP mode, email messages with this status are queued to be discarded.<br>• **Received**: The email message was received by TippingPoint Advanced Threat Protection for Email.<br>• **Sent for analysis**: The email message was sent to Virtual Analyzer for analysis.<br>• **Stripped**: Attachments were stripped from the email message and it was passed for delivery. |
| Action | Do any of the following:<br>Quarantined Message:<br>• **View in Quarantine**<br>• **Release from Quarantine**<br>• **View in Threat Messages**<br>Non-Quarantined Message, with high/medium/low risk level:<br>**View in Threat Messages**<br>No Risk Message:<br>**No Action Links** |

**Note**

TippingPoint Advanced Threat Protection for Email sorts logs using **UTC 0** time, even if the display is in local time.

5. Perform additional actions.

   - Click **Export** to save the query results in a CSV file.

**Note**

Only the first 50000 entries in the query results are included in the CSV file.

- 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.

# MTA Events

View connection details about Postfix and SMTP activity on your network.

**Note**

TippingPoint Advanced Threat Protection for Email automatically purges logs when there are a total of 100 log files that are each 51200KB. The most recent 10 logs can be queried.

## Querying MTA Event Logs

**Procedure**

1. Go to **Logs** > **MTA**.
2. Specify the time range to query logs.
3. Click **Query**.

   All logs matching the time criteria appear in the table.
4. View the results.

| FIELD | DESCRIPTION |
|---|---|
| Timestamp | The date and time when the event occurred |
| Description | The log event description |

**Note**

TippingPoint Advanced Threat Protection for Email sorts logs using **UTC 0** time, even if the display is in local time.

5. Perform additional actions.
   - Click **Export** to save the query results in a CSV file.
   - 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.

# System Events

View details about user access, policy modification, network setting changes, and other events that occurred using the TippingPoint Advanced Threat Protection for Email management console.

TippingPoint Advanced Threat Protection for Email maintains two system event log types:

- **Update events**: All component update events
- **Audit logs**: All user access events

**Note**

- Logs purge based on the settings configured on the **Storage Maintenance** screen.

  For details, see *Configuring Storage Maintenance on page 8-101*.
- For a list of system event logs available, see *System Event Logs on page G-1*.

## Querying System Event Logs

**Procedure**

1. Go to **Logs** > **System**.
2. Specify the time range to query logs.
3. Click **Query**.

   All logs matching the time criteria appear in the table.
4. View the results.

| FIELD | DESCRIPTION |
|---|---|
| Timestamp | The date and time when the event occurred |
| Event Type | TippingPoint Advanced Threat Protection for Email records two system event log types:<br>• Update events<br>• Audit logs |
| Description | The log event description |

**Note**

TippingPoint Advanced Threat Protection for Email sorts logs using **UTC 0** time, even if the display is in local time.

5. Perform additional actions.
   - From the **Show** drop-down menu at the top-right side, select an event type to filter the results.
   - Click **Export** to save the query results in a CSV file.
   - 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.

# Time-Based Filters and DST

When querying logs using time-based filters, the query assumes that the selected time range is based on the current Daylight Savings Time (DST) status. For example, if the time shifts from 2 a.m. back to 1 a.m. for DST and you query 0100-0159 after DST, the query matches the logs from the new 0100-0159 after the shift. Even though the local times match, the query results do not show logs matching the pre-DST time.

# Chapter 8

# Administration

Topics include:


- *Component Updates on page 8-2*
- *Product Updates on page 8-6*
- *System Settings on page 8-9*
- *Mail Settings on page 8-22*
- *Integrated Products/Services on page 8-30*
- *Scanning / Analysis on page 8-69*
- *System Maintenance on page 8-97*
- *Accounts / Contacts on page 8-104*
- *License on page 8-110*
- *About TippingPoint Advanced Threat Protection for Email on page 8-110*

# Component Updates

Download and deploy product components used to investigate threats. Because Trend Micro frequently creates new component versions, perform regular updates to address the latest spear-phishing attacks and social engineering attack patterns.

## Components

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

**TABLE 8-1. Components**

| COMPONENT | DESCRIPTION |
|---|---|
| Advanced Threat Scan Engine<br><br>Advanced Threat Scan Engine (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. |
| Deep Discovery Malware Pattern | The Deep Discovery Malware Pattern contains the detection routines for virus and malware scanning. Trend Micro updates the Deep Discovery Malware Pattern regularly with detection routines for new identified threats. |
| 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 | The Network Content Inspection Engine is used to perform network scanning. |

| COMPONENT | DESCRIPTION |
|---|---|
| Network Content Inspection Pattern | The Network Content Inspection Pattern is used by the Network Content Inspection Engine to perform network scanning. |
| Script Analyzer Engine | The Script Analyzer Engine analyzes web page scripts to identify malicious code. |
| Script Analyzer Pattern | The Script Analyzer Pattern is used during analysis of web page scripts to identify malicious code. |
| Spyware/Grayware Pattern | The Spyware/Grayware Pattern identifies unique patterns of bits and bytes that signal the presence of certain types of potentially undesirable files and programs, such as adware and spyware, or other grayware. |
| Virtual Analyzer Sensors | The Virtual Analyzer Sensors are a collection of utilities used to execute and detect malware and to record behavior in Virtual Analyzer. |
| Virtual Analyzer Configuration Pattern | The Virtual Analyzer Configuration Pattern contains configuration information for Virtual Analyzer, such as supported threat types and supported file types. |

## Update Source

TippingPoint Advanced Threat Protection for Email downloads components from the Trend Micro ActiveUpdate server, the default update source. TippingPoint Advanced Threat Protection for Email can be configured to download components from another update source specifically set up in your organization.

**Note**

If TippingPoint Advanced Threat Protection for Email is registered to Control Manager, you can configure TippingPoint Advanced Threat Protection for Email to download directly from Control Manager. For details on how a Control Manager server can act as an update source, see the*Trend Micro Control Manager Administrator's Guide*.

## Configuring the Update Source

Frequently update components to receive protection from the latest threats. By default, components automatically receive updates from the Trend Micro ActiveUpdate server. Receive updates from another Internet location by configuring a different update source.

---

**Procedure**

1. Go to **Administration** > **Component Updates** > **Source**.
2. Configure the update source settings.
   - **Trend Micro ActiveUpdate server**

     Obtain the latest components from the Trend Micro ActiveUpdate server (default).
   - **Other update source**

     Specify a different update source location. The update source URL must begin with “http://” or “https//:”.

     Example: `http://update.mycompany.com`.

     **Note**

     The update source does not support UNC path format.
3. Click **Save**.

---

## Updating Components

Update components to immediately download the component updates from the update source server. For information about the update source, see *Configuring the Update Source on page 8-4*.

**Procedure**

1. Go to **Administration** > **Component Updates** > **Components**.
2. Select one or more components.
3. Click **Update**.
4. At the confirmation message, click **OK**.

## Rolling Back Components

Roll back components to revert all components to the most recent version.

**Procedure**

1. Go to **Administration** > **Component Updates** > **Components**.
2. Select one or more components.
3. Click **Roll Back**.

   The components revert to the most recent version.
4. At the confirmation message, click **OK**.

## Scheduling Component Updates

**Procedure**

1. Go to **Administration** > **Component Updates** > **Schedule**.

   The **Schedule** tab appears.
2. Enable the scheduled update.
3. Select the update interval.

4. Click **Save**.

# Product Updates

Use the **Product Updates** screen to apply hotfixes and patches, or perform a firmware upgrade to TippingPoint Advanced Threat Protection for Email.

## System Updates

After an official product release, Trend Micro releases system updates to address issues, enhance product performance, or add new features.

**TABLE 8-2. System Updates**

| 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.<br><br>**Note**<br>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. |

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

http://www.trendmicro.com/download

## Managing Patches

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

You can install a patch file on Trend Micro using one of the following methods:

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

---

**Procedure**

1. Go to **Administration** > **Product Updates** > **Hotfixes / Patches**.
2. Under **History**, verify the software version number.
3. Manage the product patch.
   - Upload a patch by browsing to the patch file provided by Trend Micro Support and then clicking **Install** under **Install Hotfix / Patch**.
   - Roll back a patch by clicking **Roll Back** under **History**. After rollback, TippingPoint Advanced Threat Protection for Email uses the most recent previous configuration. For example, rolling back patch 3 returns TippingPoint Advanced Threat Protection for Email to a patch 2 state.

---

## Upgrading Firmware

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

Updating the firmware ensures that TippingPoint Advanced Threat Protection for Email has access to new and improved security features when they become available.

**Note**

Ensure that you have finished all management console tasks before proceeding. The upgrade process may take some time to complete, and upgrading from TippingPoint Advanced Threat Protection for Email 2.5 or 2.5 SP1 to TippingPoint Advanced Threat Protection for Email 2.6 may take an hour or more. Trend Micro recommends starting the upgrade during off-peak office hours. Installing the update restarts TippingPoint Advanced Threat Protection for Email.

**Procedure**

1. Back up configuration settings.
2. Obtain the firmware image.
   - Download the TippingPoint Advanced Threat Protection for Email firmware image from the Trend Micro Download Center at:

     http://downloadcenter.trendmicro.com
   - Obtain the firmware package from your Trend Micro reseller or support provider.
3. Save the image to any folder on a computer.
4. Go to **Administration** > **Product Updates** > **Firmware**.
5. Next to **Software version**, verify your firmware version.
6. Browse for the firmware update package.
7. Click **Install**.

   **Tip**

   You can access the command line interface to view the installation process.

   After the installation is complete, TippingPoint Advanced Threat Protection for Email automatically restarts and the command line interface appears.
8. Perform the following post-installation steps:

- Clear the browser cache.
- Manually log onto the web console.

# System Settings

Topics include:


- *Network Settings on page 8-9*
- *Operation Modes on page 8-11*
- *Configuring Proxy Settings on page 8-13*
- *Configuring the Notification SMTP Server on page 8-14*
- *Configuring System Time on page 8-16*
- *SNMP on page 8-17*


## Network Settings

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

### Configuring Network Settings

Perform initial network configurations with the Command Line Interface (CLI). Use the management console to make changes to the network interface settings.

**Procedure**

1. Go to **Administration** > **System Settings** > **Network**.
2. Specify the host name.

3. Specify the network settings.

| OPTION | DESCRIPTION |
|---|---|
| IP address and Subnet mask / prefix length | Specify the network interface IP settings for the management network, custom network, and mail network.<br>• **Management network**: The management network handles the management console, SSH connections, and Trend Micro updates. Mail traffic can pass through the management network and by default it is the only network that routes mail. Use only the management port (eth0).<br>• **Custom network**: The custom network handles sandbox analysis. This network should be an isolated network without connection restrictions so that malicious samples do not affect other networks. Use any available network interface (eth1, eth2, or eth3) that is not configured for the mail network.<br>• **Mail network**: The mail network handles mail routing and monitoring. Use a network interface that is not configured for the custom network.<br>  • (Optional) For BCC or MTA mode, use any available network interface (eth1, eth2, or eth3).<br>  • For SPAN/TAP mode, use the eth2 or eth3 network interface.<br>**Note**<br>For information on operation mode configuration, see *Operation Modes on page 8-11*. |
| Gateway / DNS | Specify the general network settings that affect all interfaces, including the gateway and DNS settings. |

4. Click **Save**.

## Operation Modes

TippingPoint Advanced Threat Protection for Email can act as a Mail Transfer Agent (MTA mode), or as an out-of-band appliance (BCC mode or SPAN/TAP mode).

To configure the operation mode, go to **Administration** > **System Settings** > **Operation Mode**.

**Note**

The internal Postfix server cannot be used to send email notifications in BCC or SPAN/TAP mode.

For more information on specifying an external SMTP server, see *Configuring the Notification SMTP Server on page 8-14*.

**TABLE 8-3. Operation Modes**

| MODE | DESCRIPTION |
|---|---|
| MTA mode<br><br>(Default) | As an inline MTA, TippingPoint Advanced Threat Protection for Email protects your network from harm by blocking malicious email messages in the mail traffic flow. TippingPoint Advanced Threat Protection for Email delivers safe email messages to recipients. |
| BCC mode | As an out-of-band appliance, TippingPoint Advanced Threat Protection for Email receives mirrored traffic from an upstream MTA to monitor your network for cyber threats. TippingPoint Advanced Threat Protection for Email discards all replicated email messages without delivery. |
| SPAN/TAP mode | As an out-of-band appliance, TippingPoint Advanced Threat Protection for Email receives mirrored traffic from a SPAN/TAP device to monitor your network for cyber threats. TippingPoint Advanced Threat Protection for Email discards all replicated email messages without delivery.<br><br>If you select **SPAN/TAP mode**, you must add at least one monitoring rule. For more information, see *Monitoring Rules for SPAN/TAP Mode on page 8-12*. |

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

## Monitoring Rules for SPAN/TAP Mode

When SPAN/TAP mode is selected, you can add a maximum of 10 monitoring rules. The monitoring rules specify the SMTP traffic that TippingPoint Advanced Threat Protection for Email monitors for cyber threats.

### Adding a Monitoring Rule

**Procedure**

1. Go to **Administration** > **System Settings** > **Operation Mode**.
2. Click **Add Rule**.

   The **Add SPAN/TAP Mode Rule** window appears.
3. Type the **Source IP address**, **Destination IP address**, and **SMTP port** to monitor.

   **Note**

   If a field is empty, all SMTP traffic for that option is monitored.

   For example, when **Source IP address** is empty, SMTP traffic from all sources is monitored.
4. Click **Add**.

### Editing a Monitoring Rule

**Procedure**

1. Go to **Administration** > **System Settings** > **Operation Mode**.
2. Select a monitoring rule and click **Edit**.

   The **Edit SPAN/TAP Mode Rule** window appears.
3. Make the changes.

4. Click **Edit**.

### Deleting a Monitoring Rule

**Procedure**

1. Go to **Administration** > **System Settings** > **Operation Mode**.
2. Select a monitoring rule and click **Delete**.

## Configuring Proxy Settings

Configuring proxy settings affects:

- Certified Safe Software Service
- Community File Reputation
- Component updates (pattern files and scan engines)
- Product license registration
- Script Analyzer Engine
- Web Reputation queries
- Web Inspection Service

**Procedure**

1. Go to **Administration** > **System Settings** > **Proxy**.

   The **Proxy** screen appears.
2. Specify the proxy server settings.

| OPTION | DESCRIPTION |
|---|---|
| Check box | Select **Use a proxy server to connect to the Internet**. |
| **Type** | Select the proxy protocol:<br>• **HTTP**<br>• **SOCKS4**<br>• **SOCKS5** |
| **Server address** | Specify the proxy server host name or IP address. |
| **Port** | Specify the port that the proxy server uses to connect to the Internet. |
| **User name** | Optional: Specify the user name for administrative access to the proxy server. |
| **Password** | Optional: Specify the corresponding password. |

3. Click **Save**.

## Configuring the Notification SMTP Server

TippingPoint Advanced Threat Protection for Email uses the SMTP server settings to send alert notifications.

For details about processing SMTP traffic, see *Mail Settings on page 8-22*.

**Procedure**

1. Go to **Administration** > **System Settings** > **SMTP**.
2. Type the **Sender email address**.
3. Specify the SMTP server settings.

| Option | Description |
|---|---|
| Internal postfix server | Select this option to use the postfix server embedded in TippingPoint Advanced Threat Protection for Email as an SMTP server.<br><br>**Note**<br>Internal postfix is not available when operating in BCC mode and SPAN/TAP mode. |
| External SMTP server | Select this option to specify a standalone SMTP server, such as Microsoft Exchange. |
| Server address | Type the external SMTP server host name, IPv4 address or IPv6 address. |
| Port | Type the external SMTP server port number. |
| Connection security | Select a security protocol if required for the connection. |
| SMTP server requires authentication | Select this option if connection to the SMTP server requires authentication.<br><br>**Note**<br>• Make sure that you configure the user name and password correctly. An external SMTP server may refuse connection from TippingPoint Advanced Threat Protection for Email after the maximum number of unsuccessful authentication attempts has been reached.<br>• Clicking **Test Connection** checks the connection from TippingPoint Advanced Threat Protection for Email to the external SMTP server, but does not verify SMTP server authentication. |

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

4. Click **Save**.
5. (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 for Email does not send a test email message to the recipient.

## Configuring System Time

Network Time Protocol (NTP) synchronizes computer system clocks across the Internet. Configure NTP settings to synchronize the server clock with an NTP server, or manually set the system time. Specify the format to display the date and time in.

**Procedure**

1. Go to **Administration** > **System Settings** > **Time**.
2. Set the system time.
   - To synchronize with an NTP server, select **Synchronize appliance time with an NTP server** and then specify the domain name or IP address of the NTP server.
   - To manually set the system time, select **Set time manually** and then select the date and time or select the time zone.
   - To display the date and time in another format, select the format from the **Date and time format** drop-down list.
3. Click **Save**.

## SNMP

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 for Email, 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 8-18*.

- Configure the appliance to listen for manager requests

  For details, see *Configuring Manager Requests on page 8-20*.

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

| OPTION | DESCRIPTION |
|---|---|
| Security model | **Note**<br>This field is only available for SNMPv3.<br><br>Select the security model:<br>• No authentication or privacy<br>• Authenticated<br>• Authenticated with privacy |
| User name | **Note**<br>This field is only available for SNMPv3.<br><br>Specify the user name. |
| Password | **Note**<br>This field is only available for SNMPv3.<br><br>Specify the password. |
| Privacy passphrase | **Note**<br>This field is only available for SNMPv3.<br><br>Specify the 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 for Email supported SNMP object identifiers (OID), see *SNMP Object Identifiers on page E-1*.

## Configuring Manager Requests

SNMP managers can use SNMP protocol commands to request TippingPoint Advanced Threat Protection for Email 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:<br>• SNMPv1/SNMPv2c<br>• SNMPv3<br>If you use SNMPv3, configure the SNMP server as follows:<br>• Context Name: `""` (default context)<br>• Context Engine ID: `<Auto>`<br>• (Optional) MD5 Authentication protocol: `HMAC-MD5`<br>• (Optional) DES Privacy protocol: `CBC-DES` |
| Allowed community names | Specify a maximum of 5 community names. |

| OPTION | DESCRIPTION |
|---|---|
| Security model | **Note**<br>This field is only available for SNMPv3.<br><br>Select the security model:<br>• No authentication or privacy<br>• Authenticated<br>• Authenticated with privacy |
| User name | **Note**<br>This field is only available for SNMPv3.<br><br>Specify the user name. |
| Password | **Note**<br>This field is only available for SNMPv3.<br><br>Specify the password. |
| Privacy passphrase | **Note**<br>This field is only available for SNMPv3.<br><br>Specify the privacy passphrase. |
| Trusted manager server addresses | Specify a maximum of 5 trusted manager server addresses. |

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 for Email supported SNMP object identifiers (OID), see *SNMP Object Identifiers on page E-1*.

# Mail Settings

Topics include:


- *Message Delivery on page 8-22*
- *Configuring SMTP Connection Settings on page 8-23*
- *Configuring Message Delivery Settings on page 8-26*
- *Configuring Limits and Exceptions on page 8-28*
- *Configuring the SMTP Greeting Message on page 8-30*


## Message Delivery

TippingPoint Advanced Threat Protection for Email maintains a routing table based on domains and email addresses. TippingPoint Advanced Threat Protection for Email uses this routing table to route email messages (with matching recipient domains or email addresses) to specified destination servers or to destination servers that match specified mail exchanger records (MX records).

There are two message delivery methods:

- Look up MX record

  When delivering an email message using MX record lookup, TippingPoint Advanced Threat Protection for Email queries the specified MX record, and then delivers the email message to the destination server identified by the MX record.

- Specify servers

  When delivering an email message using specified servers, TippingPoint Advanced Threat Protection for Email first sends the email message to the destination server with the highest priority. If the server is unavailable, TippingPoint Advanced Threat Protection for Email chooses the remaining servers in descending order of their

priority. If multiple destination servers have the same priority, TippingPoint Advanced Threat Protection for Email randomly selects a server for message delivery.

Email messages destined to unspecified domains and email addresses are routed based on the records in the Domain Name Server (DNS). For example, if the delivery domain includes "example.com" and the associated SMTP server is `10.10.10.10` on port 25, then all email messages sent to "example.com" deliver to the SMTP server at `10.10.10.10` using port 25.

## Configuring SMTP Connection Settings

Configure SMTP connection settings to control which MTAs and mail user agents are allowed to connect to the server.

**Note**

Connection control settings take priority over mail relay settings.

**Procedure**

1. Go to **Administration** > **Mail Settings** > **Connections**.
2. Specify the **SMTP Interface** settings.

| OPTION | DESCRIPTION |
|---|---|
| Port | Specify the listening port of the SMTP service. |
| Disconnect after { } minutes of inactivity | Specify a time-out value. |
| Simultaneous connections | Click **No limit** or **Allow up to { } connections** and specify the maximum allowed connections. |

3. Specify the **Connection Control** settings.
   a. Select a connections "deny list" or "permit list".
      - Select **Accept all, except the following list** to configure the "deny list".

- Select **Deny all, except the following list** to configure the "permit list".

b. Select an option and then specify the IP addresses.

| OPTION | DESCRIPTION |
|---|---|
| Single computer | Specify an IPv4 or IPv6 address, and then click **[ >> ]** to add it to the list. |
| Group of computers | i. Select the IP version.<br>ii. Type the **Subnet address**.<br>iii. If IPv4 was selected, type the **Subnet mask**.<br>iv. Click **[ >> ]** to add it to the list. |
| Import from File | Click to import an IP list from a file. The following list shows sample content of an IP list text file:<br>192.168.1.1<br>192.168.2.0:255.255.255.0<br>192.168.3.1:255.255.255.128<br>192.168.4.100<br>192.168.5.32:255.255.255.192 |

4. Specify the **Transport Layer Security** settings.

   See *Configuring TLS Settings on page 8-24*.

5. Click **Save**.

## Configuring TLS Settings

Transport Layer Security (TLS) provides a secure communication channel between hosts over the Internet, ensuring the privacy and integrity of the data during transmission.

For details about TLS settings, see *Transport Layer Security on page A-1*.

**Procedure**

1. Go to **Administration** > **Mail Settings** > **Connections**.
2. Go to the bottom of the page to the section titled **Transport Layer Security**.
3. Select **Enable incoming TLS**.

   This option allows the TippingPoint Advanced Threat Protection for Email SMTP Server to provide Transport Layer Security (TLS) support to SMTP email relays, but does not require that email relays use TLS encryption to establish the connection.
4. Select **Only accept SMTP connections through TLS** for TippingPoint Advanced Threat Protection for Email to only accept secure incoming connections.

   This option enables the TippingPoint Advanced Threat Protection for Email SMTP server to accept messages only through a TLS connection.
5. Click a **Browse** button next to one of the following:

| Option | Description |
|---|---|
| CA certificate | The CA certificate verifies an SMTP email relay. However, TippingPoint Advanced Threat Protection for Email does not verify the email relay and only uses the CA certificate for enabling the TLS connection. |
| Private key | The SMTP email relay creates the session key by encrypting a random number using the TippingPoint Advanced Threat Protection for Email SMTP server's public key.<br><br>The TippingPoint Advanced Threat Protection for Email SMTP server then uses the private key to decrypt the random number in order to establish the secure connection.<br><br>This key must be uploaded to enable a TLS connection. |
| SMTP server certification | SMTP email relays can generate session keys with the TippingPoint Advanced Threat Protection for Email SMTP server public key.<br><br>Upload the key to enable a TLS connection. |

6. Select **Enable outgoing TLS**.
7. Click **Save**.

## Configuring Message Delivery Settings

The following procedure explains how to configure message delivery settings for downstream mail servers.

For more information about configuring connections, importing message delivery settings, and setting message rules, see *Mail Settings on page 8-22*.

Specify settings for email message delivery to TippingPoint Advanced Threat Protection for Email downstream mail servers. TippingPoint Advanced Threat Protection for Email checks the recipient domains or email addresses, determines destination servers, and sends the message to the next SMTP host for the matched domain or email address.

**Procedure**

1. Go to **Administration** > **Mail Settings** > **Message Delivery**.
2. Click **Add**.

   The **Add Delivery Profile** screen appears.
3. Select the status of the delivery profile.
4. Specify the recipient domain or email address. Type a wildcard (*) to manage email message delivery from a domain and any subdomains.
   - * (Include all domains)
   - `example.com` (Include only example.com)
   - `*.example.com` (Include example.com and any subdomains)
5. Select either of the following from the **Destination servers** drop-down list:
   - **Look up MX record**: Specify the MX record name, and a port number when connecting through a non-default port.

- **Specify server**: Specify the IP address or fully qualified domain name, port number, and priority to forward email messages.

**Note**

- The lower the priority value, the higher the priority.
- Optionally add multiple destination servers by clicking on **Add server**.
- To disable a destination server, click on the check mark for the server behind the **Priority** field. Then the check mark becomes a dash mark. To enable the server again, click the dash mark.

6. Click **Save**.

## Importing Message Delivery Settings

Use this option if you have a properly formatted `.xml` file containing message delivery settings. Optionally, export existing settings from the management console, or download a sample XML from the **Import Delivery Profiles** screen and generate a file according to the exported file.

Specify settings for email message delivery to TippingPoint Advanced Threat Protection for Email downstream mail servers. TippingPoint Advanced Threat Protection for Email checks the recipient domains or email addresses, determines destination servers, and sends the message to the next SMTP host for the matched domain or email address.

**Procedure**

1. Go to **Administration** > **Mail Settings** > **Message Delivery**.
2. Click **Import**.

   The **Import Delivery Profiles** screen appears.
3. Click **Browse** to locate the file to import.
4. Specify the import settings.

   - Merge with existing profiles: Merge the imported profiles to the existing message delivery list.

- Replace existing profiles: Overwrite all existing profiles with the profiles in the XML file.

5. Click **Continue**.

   The profiles are added to the **Message Delivery** list.

## Configuring Limits and Exceptions

Set limits on the email messages that TippingPoint Advanced Threat Protection for Email processes to:

- Improve performance by reducing the total number of email messages required to process
- Restrict senders of relayed messages to prevent TippingPoint Advanced Threat Protection for Email from acting as an open mail relay

**Note**

Connection control settings take priority over mail relay settings.

**Procedure**

1. Go to **Administration** > **Mail Settings** > **Limits and Exceptions**.
2. Specify the **Message Limits** settings:

| OPTION | DESCRIPTION |
|---|---|
| Maximum message size | Specify maximum message size from 1 to 2047 MB. |
| Maximum number of recipients | Specify number of recipients from 1 to 99,999. |

3. Specify the **Permitted Senders of Relayed Mail**.
   - **TippingPoint Advanced Threat Protection for Email only**
   - **Hosts in the same subnet**

- **Hosts in the same address class**

**Note**

When this option is selected, TippingPoint Advanced Threat Protection for Email will check if the IP address of TippingPoint Advanced Threat Protection for Email and hosts are in the same address class and subnet.

- TippingPoint Advanced Threat Protection for Email will only allow hosts to relay messages if they are in the same address class and subnet.

  For example:

  - Class A: The TippingPoint Advanced Threat Protection for Email IP address is 10.1.2.3, and the hosts' IP address is 10.1.2.x.

    Class B: The TippingPoint Advanced Threat Protection for Email IP address is 172.31.2.3, and the hosts' IP address is 172.31.x.x.

    Class C: The TippingPoint Advanced Threat Protection for Email IP address is 192.168.10.3, and the hosts' IP address is 192.168.10.x.

- TippingPoint Advanced Threat Protection for Email will not allow hosts to relay messages if they are in the same address class, but not in the same subnet.

  For example:

  - Class A: The TippingPoint Advanced Threat Protection for Email IP address is 10.1.2.3, and the hosts' IP address is 11.2.3.x.

    Class B: The TippingPoint Advanced Threat Protection for Email IP address is 172.31.2.3, and the hosts' IP address is 172.32.x.x.

    Class C: The TippingPoint Advanced Threat Protection for Email IP address is 192.168.10.3, and the hosts' IP address is 192.168.11.x.

- **Specified IP addresses**

**Note**

Import settings from a file by clicking **Import from a File**.

Export settings to a file by clicking **Export**.

4. Click **Save**.

## Configuring the SMTP Greeting Message

The SMTP greeting message presents to the mail relay whenever TippingPoint Advanced Threat Protection for Email establishes an SMTP session.

**Procedure**

1. Go to **Administration** > **Mail Settings** > **SMTP Greeting**
2. In the text box, specify a greeting message.
3. Click **Save**.

# Integrated Products/Services

TippingPoint Advanced Threat Protection for Email integrates with the following products and services:


- *Control Manager on page 8-30*
- *Deep Discovery Director on page 8-35*
- *Auxiliary Products/Services on page 8-40*
- *Threat Intelligence Sharing on page 8-38*
- *Microsoft Active Directory on page 8-65*
- *Log Settings on page 8-66*
- *SFTP on page 8-68*


## Control Manager

Trend Micro Control Manager is a software management solution that gives you the ability to control antivirus and content security programs from a central location,

regardless of the program's physical location or platform. This application can simplify the administration of a corporate antivirus and content security policy.

For details about Control Manager features, see *Control Manager Features on page 8-31*.

On TippingPoint Advanced Threat Protection for Email, use the **Administration** > **Integrated Products/Services** > **Control Manager** tab to perform the following tasks:

- Register to a Control Manager server.

  For details, see *Registering to Control Manager on page 8-33*.

- Check the connection status between TippingPoint Advanced Threat Protection for Email and Control Manager.

- Unregister from a Control Manager server.

  For details, see *Unregistering from Control Manager on page 8-35*.

- Synchronize suspicious objects with Control Manager.

**Note**

Ensure that both TippingPoint Advanced Threat Protection for Email and the Control Manager server belong to the same network segment. If TippingPoint Advanced Threat Protection for Email is not in the same network segment as Control Manager, configure the port forwarding settings for TippingPoint Advanced Threat Protection for Email.

## Control Manager Features

Control Manager offers the following features:

**TABLE 8-4. Control Manager Features**

| FEATURE | CONTROL MANAGER SCREEN |
|---|---|
| Log data aggregation | **Log Aggregation Settings** |
| Suspicious object data aggregation | **Suspicious Objects** |

| FEATURE | CONTROL MANAGER SCREEN |
|---|---|
| Reports | • One-time report: **One-time Reports**<br>• Scheduled report: **Scheduled Reports** |
| Notifications | **Event Notifications** |
| Single sign-on (SSO) | **Products** |
| Product component updates | **Products** |
| Exceptions | **Virtual Analyzer Objects** |

For details, see the *Trend Micro Control Manager Administrator's Guide*.

## Control Manager Components

**TABLE 8-5. Control Manager Components**

| COMPONENT | DESCRIPTION |
|---|---|
| Control Manager server | The computer upon which the Control Manager application is installed. This server hosts the web-based Control Manager product console |
| Management Communication Protocol (MCP) Agent | An application installed along with TippingPoint Advanced Threat Protection for Email that allows Control Manager to manage the product. The agent receives commands from the Control Manager server, and then applies them to TippingPoint Advanced Threat Protection for Email. It also collects logs from the product, and sends them to Control Manager. The Control Manager agent does not communicate with the Control Manager server directly. Instead, it interfaces with a component called the Communicator. |
| Entity | A representation of a managed product (such as TippingPoint Advanced Threat Protection for Email) on the Control Manager console's product directory tree. The product directory tree includes all managed entities. |

## Registering to Control Manager

### Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Control Manager**.
2. Configure **General** settings.
   - View the registration status.
   - Specify the display name that identifies TippingPoint Advanced Threat Protection for Email in the Control Manager Product Directory.

> **Tip**
> Use the host name or specify a unique and meaningful name to help you quickly identify TippingPoint Advanced Threat Protection for Email.

3. Configure **Server Settings**.

| OPTION | DESCRIPTION |
|---|---|
| Server address | Type the Control Manager server FQDN or IP address. |
| Port | Type the port number that the MCP agent uses to communicate with Control Manager.<br>Select **Use HTTPS** if the Control Manager security is set to medium or high.<br>Medium: Trend Micro allows HTTPS and HTTP communication between Control Manager and the MCP agent of managed products.<br>High: Trend Micro only allows HTTPS communication between Control Manager and the MCP agent of managed products. |
| User name and password | Type the logon credentials for the IIS server used by Control Manager if your network requires authentication. |
| Connect using a proxy server | Optionally select **Connect using a proxy server**.<br>For details, see *Configuring Proxy Settings on page 8-13*. |

4. (Optional) Configure **Incoming Connections from Control Manager** settings.
   a. Select **Receive connections through a NAT device** to use a NAT device.
   b. Type the IP address of the NAT device.
   c. Type the port number.
5. (Optional) Under **Suspicious Object Synchronization**, do the following:
   a. Select **Synchronize suspicious objects from Control Manager**.

   **Attention**

   You can only choose to synchronize suspicious objects with one source. If you enable TippingPoint Advanced Threat Protection for Email to synchronize with Control Manager, you will not receive suspicious objects from any other external sources.

   If you are using an external sandbox, verify that the external sandbox is configured to send suspicious objects to Control Manager before selecting this option.

   b. Type an API Key.

   **Note**

   Log on to Control Manager to obtain an API key.

   TippingPoint Advanced Threat Protection for Email synchronizes suspicious object lists from Control Manager every 20 seconds, and displays the time of the last synchronization.
6. Click **Save**.

TippingPoint Advanced Threat Protection for Email registers to Control Manager.

To verify the registration, on Control Manger go to **Directories** > **Products**.

## Unregistering from Control Manager

**Procedure**

1. Go to **Administration** > **Integrated Products/Services** > **Control Manager**.
2. Under **General**, click the **Unregister** button.

> **Note**
>
> Use this option to unregister ATP Email from Control Manager. After unregistering, ATP Email can register to another Control Manager.

ATP Email unregisters from Control Manager.

To verify the result, on Control Manger go to **Directories** > **Products**.

# Deep Discovery Director

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.

> **Note**
>
> TippingPoint Advanced Threat Protection for Email does not support integration with Deep Discovery Director.

The Deep Discovery Director screen displays the following information:

**TABLE 8-6. Deep Discovery Director Fields**

| FIELD | INFORMATION |
|---|---|
| Status | The following appliance statuses can be displayed:<br>• Not registered: The appliance is not registered to Deep Discovery Director.<br>• Registering: The appliance is registering to Deep Discovery Director.<br>• Registered \| Connected: The appliance is registered and connected to Deep Discovery Director.<br>• 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.<br>• Registered \| Untrusted fingerprint: The appliance is registered to Deep Discovery Director, but the connection was interrupted. To restore the connection, trust the new fingerprint.<br>• Unregistering: The appliance is unregistering from Deep Discovery Director. |
| 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. |
| Fingerprint (SHA-256) | The Deep Discovery Director fingerprint. |
| Connect using a proxy server | Select to use the system proxy settings to connect to Deep Discovery Director. |

## 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. Configure **Connection Settings**.

| OPTION | DESCRIPTION |
|---|---|
| Server address | Type the server address for Deep Discovery Director. |
| API key | Type the API key for Deep Discovery Director.<br>**Note**<br>You can find this information on the **Help** screen on the management console of Deep Discovery Director. |

3. (Optional) If you have configured proxy settings for TippingPoint Advanced Threat Protection for Email and want to use these settings for Deep Discovery Director connections, select **Connect using a proxy server**.

   **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**.

4. 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.

**Important**

Integration with Deep Discovery Director for Virtual Analyzer image deployment requires additional disk space. After registering TippingPoint Advanced Threat Protection for Email to Deep Discovery Director, configure TippingPoint Advanced Threat Protection for Email to delete logs when the total free disk space is less than 20%.

For more information, see *Configuring Storage Maintenance on page 8-101*.

## 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**.

# Threat Intelligence Sharing

TippingPoint Advanced Threat Protection for Email can share threat intelligence data (such as suspicious URLs) with other products or services (for example, a Blue Coat ProxySG device) through HTTP or HTTPS web service.

**Note**

When TippingPoint Advanced Threat Protection for Email is registered to Control Manager, TippingPoint Advanced Threat Protection for Email does not include user-defined suspicious objects synchronized from Control Manager in the shared threat intelligence data.

## Configuring Threat Intelligence Sharing Settings

**Procedure**

1. On the TippingPoint Advanced Threat Protection for Email management console, go to **Administration** > **Integrated Products/Services** > **Threat Intelligence Sharing**.
2. Select **Enable Threat Intelligence Sharing to allow integrated products/services to get information from TippingPoint Advanced Threat Protection for Email**.
3. Under **Criteria**, select the risk level of the objects to be included in the threat intelligence data file.
4. (Optional) By default, TippingPoint Advanced Threat Protection for Email shares threat intelligence data through HTTPS web service. You can also enable HTTP web service for data sharing. Under **Server Settings**, select **Share information using HTTP (in addition to HTTPS)** and specify the HTTP port number.
5. (Optional) Under **Schedule Settings**, select **Enabled** for **Scheduled file generation** and configure the schedule settings.
6. Click **Save**.
7. Click **Generate Now**.

   **Note**

   After the file generation is successfully, you can click the URL to download the threat intelligence data file to view the content.

8. Configure an integrated product/service (for example, Blue Coat ProxySG device) to obtain threat intelligence data from TippingPoint Advanced Threat Protection

for Email. For more information, see the documentation for the integrated product/service.

## Auxiliary Products/Services

To help provide effective detection and blocking at the perimeter, TippingPoint Advanced Threat Protection for Email can distribute Virtual Analyzer suspicious objects list to auxiliary products and services.

TippingPoint Advanced Threat Protection for Email integrates with the following solutions:

**TABLE 8-7. Supported Solutions**

| NAME | VERSIONS |
|---|---|
| Trend Micro TippingPoint Security Management System (SMS) | SMS 4.4.0.57192 or later |
| Check Point Open Platform for Security (OPSEC) | Check Point R77.20 or later |
| IBM Security Network Protection (XGS) | XGS 5.2 or later |
| Palo Alto Panorama | PAN-OS 7.0.1 or later |
| Palo Alto Firewalls | PAN-OS 4.1.0 or later |

**Note**

- TippingPoint Advanced Threat Protection for Email supports only one auxiliary product/service at a time.
- When TippingPoint Advanced Threat Protection for Email is registered to Control Manager, TippingPoint Advanced Threat Protection for Email does not distribute synchronized user-defined suspicious objects to an auxiliary product/service.
- When enabled, TippingPoint Advanced Threat Protection for Email distributes the list of selected suspicious object types every 10 minutes.

## Trend Micro TippingPoint Security Management System (SMS)

Both TippingPoint Advanced Threat Protection for Email and Trend Micro Control Manager can send suspicious objects to Trend Micro TippingPoint SMS. TippingPoint Advanced Threat Protection for Email sends each suspicious object with the following optional information:

- Risk level: Severity of each suspicious object attempt
- Product Name: Trend Micro TippingPoint Advanced Threat Protection for Email (not configurable)
- Appliance Host Name: Trend Micro TippingPoint Advanced Threat Protection for Email host name (not configurable)

Trend Micro TippingPoint SMS uses reputation filters to apply block, permit, or notify actions across an entire reputation group. For more information about reputation filters, refer to your Trend Micro TippingPoint documentation.

### Configuring Trend Micro TippingPoint Security Management System (SMS)

**Procedure**

1. On the TippingPoint Advanced Threat Protection for Email management console, go to **Administration** > **Integrated Products/Services** > **Auxiliary Products/Services**.
2. Select **Trend Micro TippingPoint Security Management System (SMS)**.
3. Under **Object Distribution**, select **Enable**.
4. Under **Server Settings**, provide the following information:
   - Server name

     **Note**

     The server name must be the IPv4 address of the auxiliary product.

- User name: Existing authentication credential
- Password: Existing authentication credential

**TABLE 8-8. Valid Character Sets**

| | USER NAME | PASSWORD |
|---|---|---|
| Minimum length | 1 character | 1 character |
| Maximum length | 15 characters | 15 characters |

5. (Optional) Click **Test Connection**.
6. To send object information from TippingPoint Advanced Threat Protection for Email to this product/service, configure the following criteria:
   - Object type:
     - Suspicious Object
       - IPv4 address
       - Domain
   - Risk level:
     - High only
     - High and medium
     - High, medium, and low
7. Click **Save**.

   The following table displays the mappings between the data columns in TippingPoint Advanced Threat Protection for Email and the tag categories in the TippingPoint reputation database.

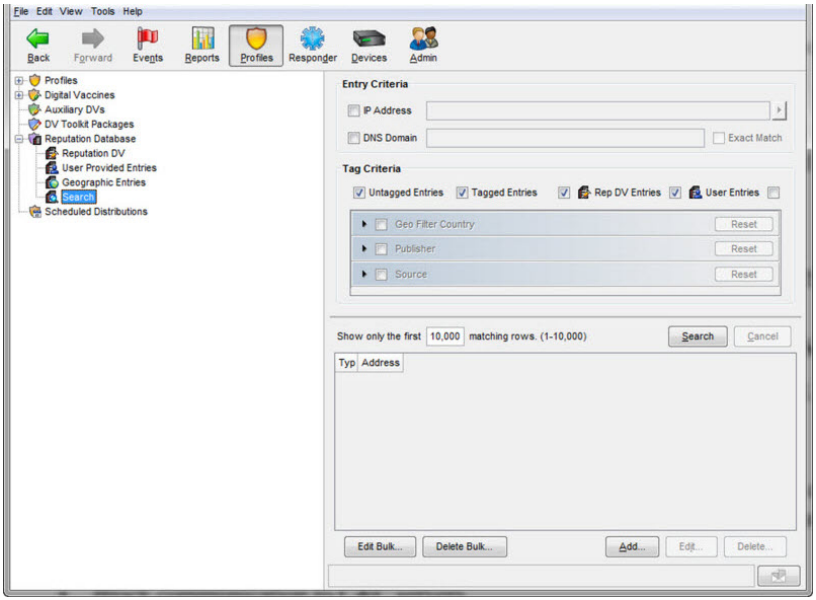
**TABLE 8-9. Tag categories added to the reputation database**

| COLUMN | TAG CATEGORY |
|---|---|
| Product Name | Trend Micro Publisher |

| Column | Tag Category |
|---|---|
| Appliance Host Name | Trend Micro Source |
| Object Type | Trend Micro Detection Category |
| Risk Level | Trend Micro Severity |

**8.** (Optional) To view distributed suspicious objects in Trend Micro TippingPoint SMS, do the following:

a. On the **Profile** tab, go to **Reputation Database** > **Search**.




b. On the **Entry Criteria** screen, type search parameters and then click **Search**.

Suspicious objects distributed by TippingPoint Advanced Threat Protection for Email are displayed.

## Check Point Open Platform for Security (OPSEC)

Check Point Open Platform for Security (OPSEC) manages network security through an open, extensible management framework.

TippingPoint Advanced Threat Protection for Email integrates with Check Point OPSEC via the Suspicious Activities Monitoring (SAM) API.

The SAM API implements communications between the SAM client (TippingPoint Advanced Threat Protection for Email) and the Check Point firewall, which acts as a SAM Server. TippingPoint Advanced Threat Protection for Email uses the SAM API to request that the Check Point firewall take specified actions for certain connections.

For example, TippingPoint Advanced Threat Protection for Email may ask Check Point OPSEC to block a connection with a client that is attempting to issue illegal commands or repeatedly failing to log on.

### Configuring Check Point Open Platform for Security (OPSEC)

**Procedure**

1. On the TippingPoint Advanced Threat Protection for Email management console, go to **Administration** > **Integrated Products/Services** > **Auxiliary Products/Services**.
2. Select **Check Point Open Platform for Security (OPSEC)**.
3. Under **Object Distribution**, select **Enable**.
4. Under **Server Settings**, select a connection type.

**Note**

Ensure that your network configuration allows TippingPoint Advanced Threat Protection for Email to connect to the Check Point appliance.

TippingPoint Advanced Threat Protection for Email may connect to the Check Point appliance through the secured connection port or clear connection port that is configured on the Check Point appliance. TippingPoint Advanced Threat Protection for Email also pulls the certificate from the Check Point appliance through port 18210.

If you selected **Secured connection**, the **OPSEC application name** and **SIC one-time password** settings appear.

5. Type a server name.

> **Note**
> The server name must be the IPv4 address of the auxiliary product.

6. If you selected **Secured connection**, type the **OPSEC application name** and **SIC one-time password**.

   For more details, see *Configuring a Secured Connection on page 8-53*.

> **Note**
> If the one-time password is reset on the Check Point appliance, the new one-time password must be different than the previous one-time password.

7. Type the port.

> **Note**
> This port must be the same port that is configured on the security gateway. For details, see *Preconfiguring a Security Gateway on page 8-51*.

8. (Optional) Click **Test Connection**.
9. Click **Save**.
10. On your Check Point firewall appliance, preconfigure a security gateway. For details see *Preconfiguring a Security Gateway on page 8-51*.
11. On the Check Point SmartDashboard console, do the following to configure your Check Point appliance for deploying suspicious objects from TippingPoint Advanced Threat Protection for Email:

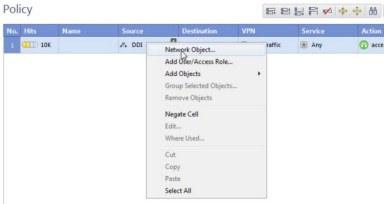
    a. On the **Firewall** tab, go to **Policy**.

    b. To add a rule, click the **Add Rule at the Top** icon.

c. To configure the new policy, right-click the action.

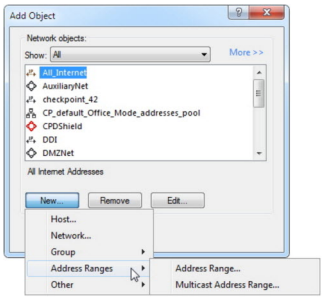
d. Change the action to **Accept**.

e. Right-click the source.




f. Select **Network Object...**.

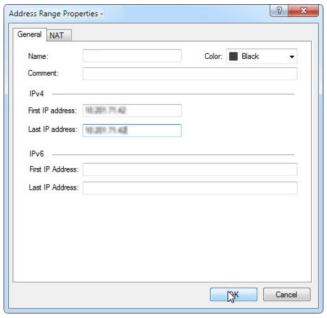
The **Add Object** window appears.




g. Click **New ...**.

h. Select **Address Ranges** > **Address Range...**.

The **Address Range Properties** window appears.




i. In **Name**, type `ATPE`.

j. In **First IP address**, type the TippingPoint Advanced Threat Protection for Email IP address.

k. In **Last IP address**, type the TippingPoint Advanced Threat Protection for Email IP address.

l. Click **OK**.

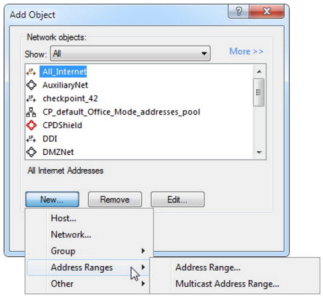
The **Add Object** window appears.

m. Select **ATPE** and then click **OK**.

n. Right-click the destination.

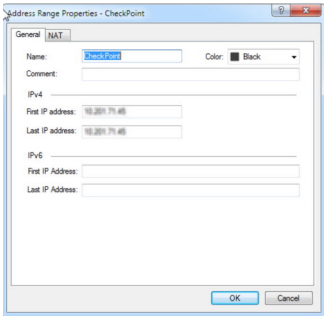
o. Select **Network Object...**.

The **Add Object** window appears.



p. Click **New ...**.

The **Address Range Properties** window appears.




q. Select **Address Ranges** > **Address Range...**.

r. In **Name**, type `CheckPoint`.

s. In **First IP address**, type the CheckPoint IP address.

t. In **Last IP address**, type the CheckPoint IP address.

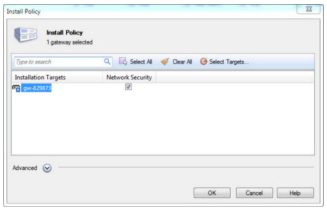
u. Click **OK**.

The **Add Object** window appears.

v. Select **CheckPoint** and then click **OK**.

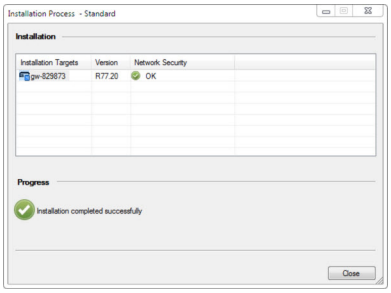
w. Click **Install Policy**.

The **Install Policy** window opens.



x. Select the target gateway and click **OK**.

The target gateway installs.




y. Click **Close**.

The Check Point appliance is enabled to receive suspicious objects from TippingPoint Advanced Threat Protection for Email.

**12.** On the TippingPoint Advanced Threat Protection for Email management console, configure the following criteria to send suspicious object information from TippingPoint Advanced Threat Protection for Email to this product/service:

- Object type:
  - Suspicious Object
    - IPv4 address
- Risk level:
  - High only
  - High and medium
  - High, medium, and low

**13.** Under **Advanced Settings**, click one of the following actions:

- **Reject**: Packets will be rejected and a notification sent to the communicating peer that the packet has been rejected.

- **Drop**: Packets will be dropped without sending the communicating peer a notification.
- **Notify**: A notification about the defined activity will be sent but the activity will not be blocked.

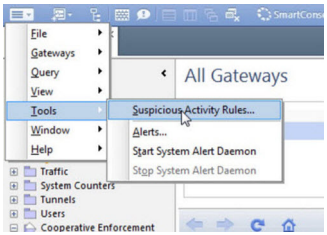
**14.** Click **Save**.

The **Distribute Now** option appears.

**15.** (Optional) Click **Distribute Now** to distribute suspicious objects to Check Point immediately.

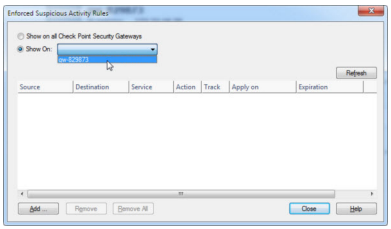
**16.** To view suspicious objects distributed by TippingPoint Advanced Threat Protection for Email on Check Point SmartView Monitor, do the following:

a. Click the **Launch Menu** icon and go to **Tools** > **Suspicious Activity Rules**.




The **Enforced Suspicious Activity Rules** window opens.

b. At **Show On**, select the target Check Point appliance name.



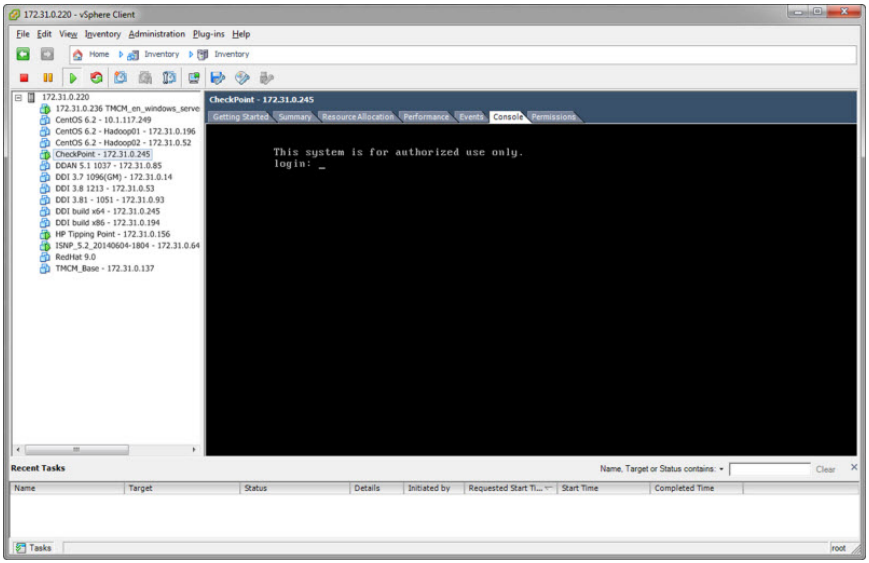
c. Click **Refresh**.

Suspicious objects distributed by TippingPoint Advanced Threat Protection for Email are displayed.

## Preconfiguring a Security Gateway

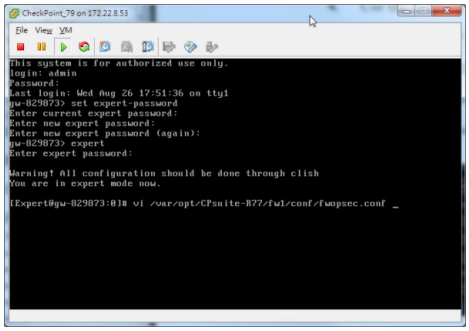
### Procedure

1. Log on to your Check Point appliance.

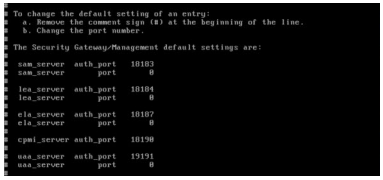



2. (Optional) Set a password for expert mode.

3. Type the password to enter expert mode.




4. Use the vi editor to open `/var/opt/CPsuite-R77/fw1/conf/fwopsec.conf`.




**Note**

The image of the default configuration is for reference only. The actual file contents may vary.

5. In `fwopsec.conf`, configure the SAM communication mode ports using one of the following options:

- Secured connection (default port)
  - No changes in `fwopsec.conf` are necessary. The default port 18183 is used for the **sam_server auth_port** setting.

**Note**

On TippingPoint Advanced Threat Protection for Email, verify that the **Check Point Open Platform for Security (OPSEC) Port** setting at **Administration** > **Integrated Products/Services** > **Auxiliary Products/Services** is also 18183.

- Secured connection (user-defined port)
  - In `fwopsec.conf`, remove the comment sign (#) from `sam_server auth_port: 18183` and then change the port number.

    **Note**

    Configure the same port in `fwopsec.conf` and in the **Check Point Open Platform for Security (OPSEC) Port** setting on TippingPoint Advanced Threat Protection for Email at **Administration** > **Integrated Products/Services** > **Auxiliary Products/Services**.

- Clear connection (user-defined port)
  - In `fwopsec.conf`, remove the comment sign (#) from `sam_server port: 0` and then change the port number.

    **Note**

    Configure the same port in `fwopsec.conf` and in the **Check Point Open Platform for Security (OPSEC) Port** setting on TippingPoint Advanced Threat Protection for Email at **Administration** > **Integrated Products/Services** > **Auxiliary Products/Services**.

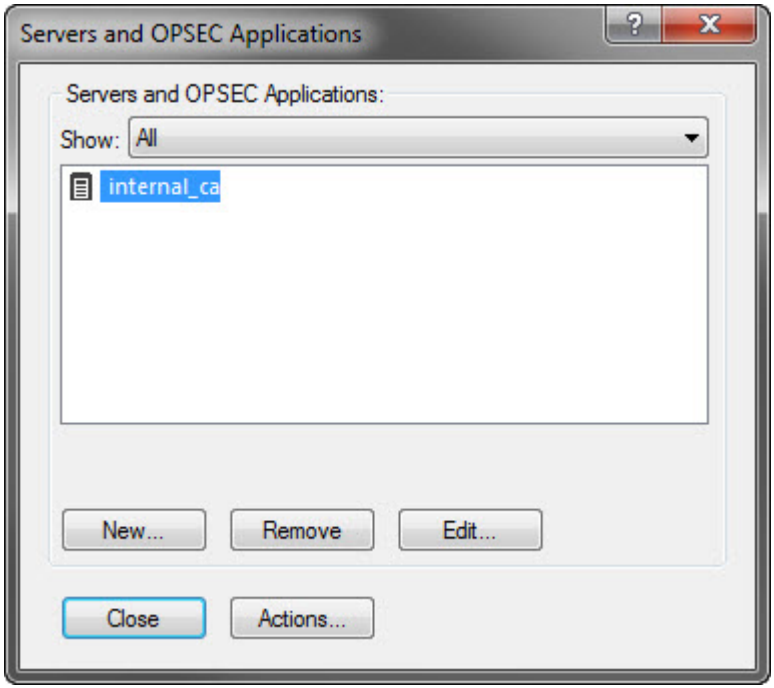
6. If changes were made to the `fwopsec.conf` file, save the `fwopsec.conf` file and restart your Check Point appliance.

## Configuring a Secured Connection

**Procedure**

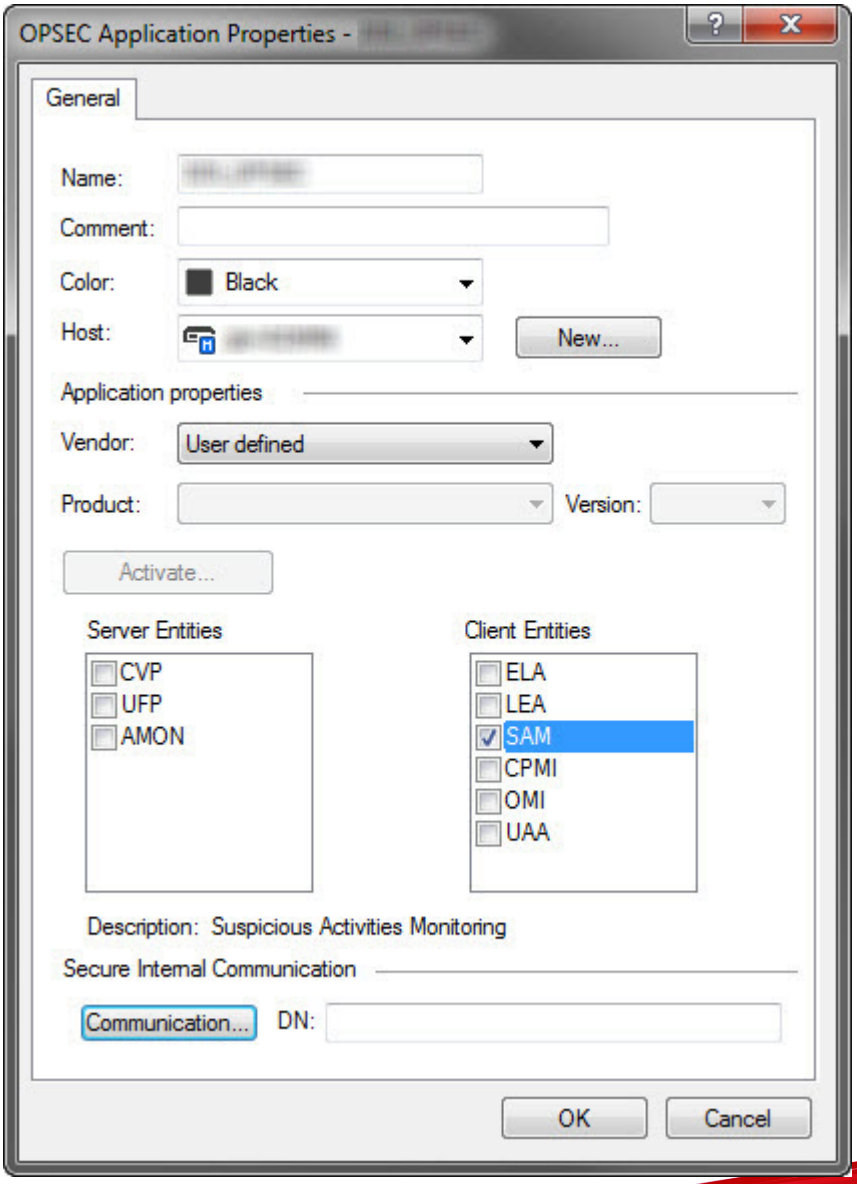
1. Open the Check Point SmartDashboard and then select **Manage** > **Servers and OPSEC Applications**.

The **Servers and OPSEC Applications** window appears.




2. Click **New** and then click **OPSEC Application...**.

The **OPSEC Application Properties** window appears.



3. Type a **Name**.

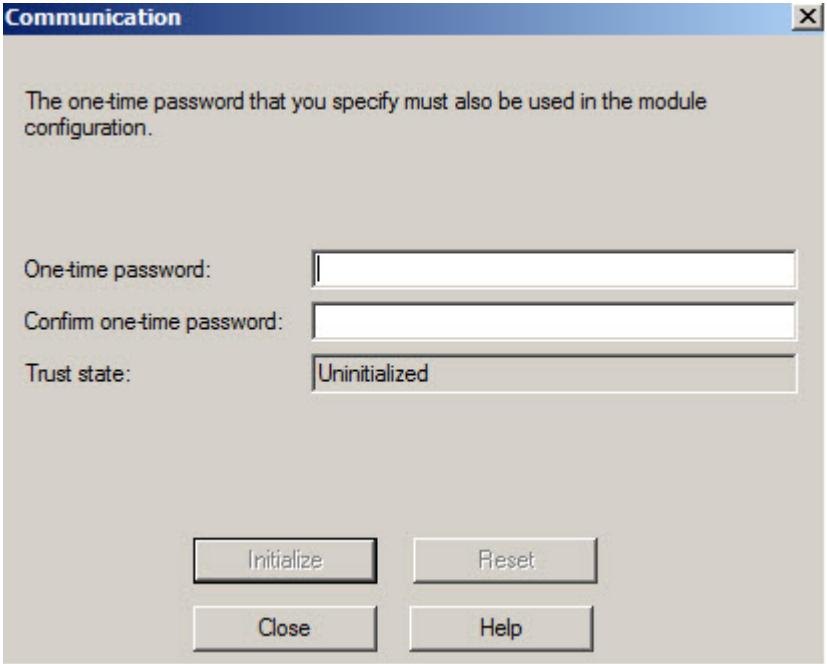
**Note**

Use this name as the **OPSEC application name** in TippingPoint Advanced Threat Protection for Email.

The application name must be less than 101 characters, start with an English alphabetical letter, and contain only English alphabetical letters, periods, underscores or dashes.

4. Select a **Host**.
5. Under **Client Entities**, select **SAM**.
6. Click **Communication...**.

   The **Communication** window appears.



7. Type a password in **One-time password** and type the same password in **Confirm one-time password**.

> **Note**
>
> Use this password as the **SIC one-time password** in TippingPoint Advanced Threat Protection for Email.

> **Note**
>
> If the one-time password is reset on the Check Point appliance, the new one-time password must be different than the previous one-time password.

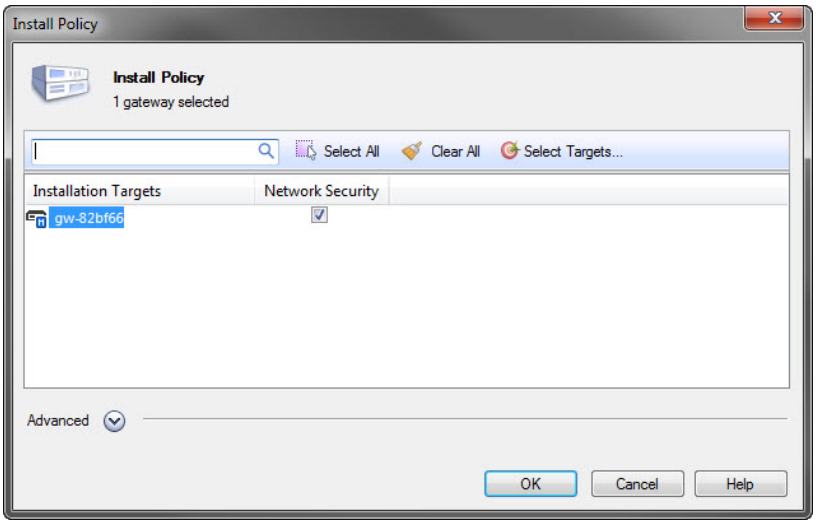
8. Click **Initialize**.

   The **Trust state** becomes **Initialized but trust not established**.

9. Install the policy.

   a. In the **Check Point SmartDashboard** main window, click **Install Policy**.

      The Install Policy window appears.



b. Choose the installation components and then click **OK**.

The policy starts installing.

## IBM Security Network Protection

IBM Security Network Protection (XGS), provides a web services API that enables third-party applications such as TippingPoint Advanced Threat Protection for Email to directly submit suspicious objects. IBM XGS can perform the following functions:

- Quarantine hosts infected with malware
- Block communication to C&C servers
- Block access to URLs found to be distributing malware

To integrate TippingPoint Advanced Threat Protection for Email with IBM XGS, configure a generic agent to do the following:

- Accept alerts that adhere to a specific schema
- Create quarantine rules based on a generic ATP translation policy

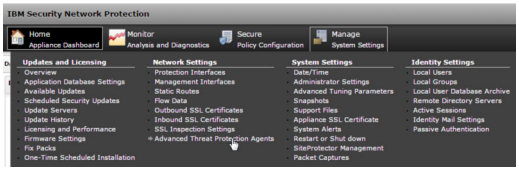
The ATP translation policy allows several categories of messages to take different actions on IBM XGS, including blocking and alerting.

### Configuring IBM Security Network Protection

**Procedure**

1. On the IBM XGS console, do the following to configure the generic agent:

   a. Go to **Manage System Settings** > **Network Settings** > **Advanced Threat Protection Agents**.



The **Advanced Threat Protection Agents** window opens.

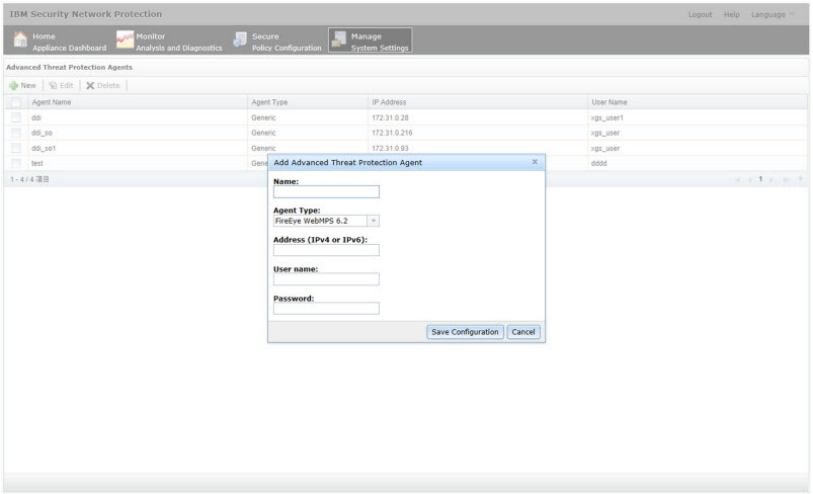
b. Click **New**.

c. Provide the following information:

- Name: Type a name
- Agent Type: Select **Generic**
- Address: TippingPoint Advanced Threat Protection for Email management port IP address in IPv4 or IPv6 format
- User name: Existing authentication credential
- Password: Existing authentication credential

**TABLE 8-10. Valid Character Sets**

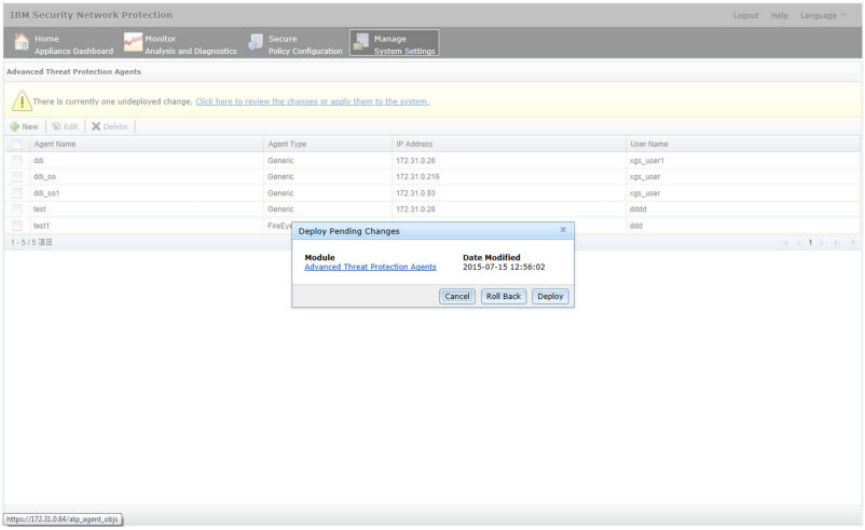
| | USER NAME | PASSWORD |
|---|---|---|
| Minimum length | 1 character | 1 character |
| Maximum length | 15 characters | 15 characters |



2. Click **Save Confirmation**.

   The **Deploy Pending Changes** window opens.

3. To apply changes to IBM XGS, click **Deploy**.




   The new agent appears in the **Advanced Threat Protection Agents** list.

4. On the TippingPoint Advanced Threat Protection for Email management console, go to **Administration** > **Integrated Products/Services** > **Auxiliary Products/Services**.

5. Select **Configuring IBM Security Network Protection (XGS)**.

6. Under **Object Distribution**, select **Enable**.

7. Under **Server Settings**, provide the following information:

   - Server name

   **Note**

   The server name must be the IPv4 address of the auxiliary product.

- User name: Existing authentication credential
- Password: Existing authentication credential

**TABLE 8-11. Valid Character Sets**

| | USER NAME | PASSWORD |
|---|---|---|
| Minimum length | 1 character | 1 character |
| Maximum length | 15 characters | 15 characters |

8. (Optional) Click **Test Connection**.
9. To send object information from TippingPoint Advanced Threat Protection for Email to this product/service, configure the following criteria:
   - Object type:
     - Suspicious Object
       - IPv4 address
       - URL
   - Risk level:
     - High only
     - High and medium
     - High, medium, and low
10. Click **Save**.
11. (Optional) On the IBM XGS console, go to **Secure Policy Configuration** > **Security Policies** > **Active Quarantine Rules** to view suspicious objects and C&C callback addresses sent by TippingPoint Advanced Threat Protection for Email to IBM XGS.

**Note**

Suspicious objects with a low risk level do not appear in the IBM XGS **Active Quarantine Rules**. To view all suspicious objects sent by TippingPoint Advanced Threat Protection for Email, go to **Security Policy Configuration** > **Advanced Threat Policy** and specify the following settings:

- **Agent Type**: **Generic**
- **Alert Type**: **Reputation**
- **Alert Severity**: **Low**

Suspicious objects and C&C callback addresses distributed by TippingPoint Advanced Threat Protection for Email are displayed.

## Palo Alto Panorama or Firewalls

Palo Alto Networks® firewalls identify and control applications, regardless of port, protocol, encryption (SSL or SSH) or evasive characteristics. Panorama™ is a centralized policy and device management system that allows administrators to control Palo Alto Networks firewalls.

TippingPoint Advanced Threat Protection for Email can send IPv4, domain, and URL suspicious objects to the URL category of Palo Alto Firewall or Palo Alto Panorama™ as match criteria allow for exception-based behavior.

Use URL categories in policies as follows:

- Identify and allow exceptions to general security policies for users who belong to multiple groups within Active Directory

  Example: Deny access to malware and hacking sites for all users, while allowing access to users that belong to the security group.

- Allow access to streaming media category, but apply quality of service policies to control bandwidth consumption

- Prevent file download and upload for URL categories that represent higher risks

  Example: Allow access to unknown sites, but prevent upload and download of executable files from unknown sites to limit malware propagation.

- Apply SSL decryption policies that allow encrypted access to finance and shopping categories, but decrypt and inspect traffic to all other URL categories.

## Configuring Palo Alto Panorama and Firewalls

**Procedure**

1. On the TippingPoint Advanced Threat Protection for Email management console, go to **Administration** > **Integrated Products/Services** > **Auxiliary Products/Services**.
2. Select **Palo Alto Panorama or Firewalls**.
3. Under **Object Distribution**, select **Enable**.
4. Under **Server Settings**, provide the following information:
   - Server name

     **Note**
     The server name must be the IPv4 address of the auxiliary product.

   - Server type
   - User name: Existing authentication credential
   - Password: Existing authentication credential

   **TABLE 8-12. Valid Character Sets**

| | USER NAME | PASSWORD |
|---|---|---|
| Minimum length | 1 character | 1 character |
| Maximum length | 15 characters | 15 characters |

5. (Optional) Click **Test Connection**.
6. To send object information from TippingPoint Advanced Threat Protection for Email to this product/service, configure the following criteria:

- Object type:
  - Suspicious Object
    - URL
    - IPv4 address
    - Domain
- Risk level:
  - High only
  - High and medium
  - High, medium, and low

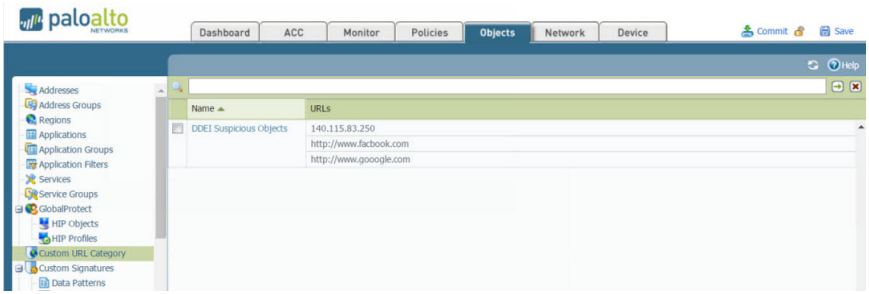
7. Under **Advanced Settings**, customize URL category names:

   URL category names must include a minimum of one character and a maximum of 31 characters, and may include the following characters:

   - Uppercase (A-Z)
   - Lowercase (a-z)
   - Numeric (0-9)
   - Special characters: - _
   - Space

8. Click **Save**.

9. (Optional) To view suspicious objects sent by TippingPoint Advanced Threat Protection for Email on the Palo Alto product console, go to **Objects** > **Custom URL Category** (or **Objects** > **Custom Objects** > **URL Category**).




Suspicious objects distributed by TippingPoint Advanced Threat Protection for Email are displayed.

## Microsoft Active Directory

Use the **Microsoft Active Directory** screen to integrate a Microsoft Active Directory server with ATP Email. ATP Email can then add Active Directory accounts to the list of accounts that can access the management console.

### Configuring Microsoft Active Directory Settings

**Procedure**

1. Obtain the information required to configure Microsoft Active Directory integration from the server administrator.
2. Go to **Administration** > **Integrated Products/Services** > **Microsoft Active Directory**.
3. Select **Use Microsoft Active Directory server**.
4. Select the server type that is integrating.
   - **Microsoft Active Directory**
   - **Microsoft AD Global Catalog**

5. Type the server address.
6. Select the encryption method.
   - **SSL**
   - **STARTTLS**
7. Type the port number.

**Note**

Trend Micro recommends using the following default ports:

- For Microsoft Active Directory:
  - **SSL**: 636
  - **STARTTLS**: 389
- For Microsoft AD Global Catalog:
  - **SSL**: 3269
  - **StartTLS**: 3268

8. Type the base distinguished name.
9. Type the user name.
10. Type the password.
11. (Optional) Click **Test Connection** to verify that a connection to the Microsoft Active Directory server can be established using the specified information.
12. (Optional) If your organization uses a CA certificate, select **Use CA certificate** and click **Select** to locate the CA certificate file.
13. Click **Save**.

## Log Settings

TippingPoint Advanced Threat Protection for Email maintains system logs that provide summaries of system events, including component updates and appliance restarts. Go to

**Administration** > **Integrated Products/Services** > **Log Settings** to configure TippingPoint Advanced Threat Protection for Email to send logs to a syslog server.

## Syslog

TippingPoint Advanced Threat Protection for Email can send logs to up to three syslog servers after saving the logs to its database. Only logs saved after enabling a syslog server will be sent to that server. Previous logs are excluded.

### Adding a Syslog Server

**Procedure**

1. Go to **Administration** > **Integrated Products/Services** > **Log Settings**.

   The **Log Settings** screen appears.

2. Click **Add**.

   The **Add Syslog Server Profile** settings appear.

3. Type a profile name for the syslog server.

4. Type the host name or IP address of the syslog server.

5. Type the port number.

6. Select the protocol to be used when transporting log content to the syslog server.

   - TCP
   - UDP
   - SSL

7. Select the format in which event logs should be 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 by Trend Micro and is used by Trend Micro products for reporting event information.

8. Select the scope of the data that will be logged.
   - **Detections**
   - **Alerts**
   - **Virtual Analyzer analysis logs**
   - **System events**
9. Click **Save**.

### Editing Syslog Server Profiles

**Procedure**

1. Go to **Administration** > **Integrated Products/Services** > **Log Settings**.

   The **Log Settings** screen appears.
2. Click a syslog server profile hyperlink.

   The **Edit Syslog Server Profile** screen appears.
3. Make the required changes.
4. Click **Save**.

## SFTP

You can configure TippingPoint Advanced Threat Protection for Email to send Virtual Analyzer detection information to a secure FTP (SFTP) server.

**Procedure**

1. Go to **Administration** > **Integrated Products/Services** > **SFTP**.
2. Select **Send detection information to SFTP server**.
3. Configure the following settings.

| FIELD | DESCRIPTION |
|---|---|
| Authentication method | Select an option from the drop-down list. |
| IP address / Domain | Type the server IP address or domain name. |
| Port | Type the port number. |
| User name | Type the user name to access the SFTP server. |
| Password | Type the password for the user account to access the SFTP server. |
| Path | Specify the directory on the SFTP server to upload files. |
| Encryption | Type the password to encrypt the ZIP file for upload. |
| Certificate | Click **Select** to locate and upload a certificate. |
| Passphrase | Type a passphrase to protect the certificate. |

4. Select one or more data types to upload.
5. Click **Save**.

# Scanning / Analysis

Use the **Scanning / Analysis** screen to configure settings for the following features:

- *Virtual Analyzer on page 1-9*
- *File Passwords on page 8-85*

- *Smart Protection on page 8-88*
- *Smart Feedback on page 8-91*
- *YARA Rules on page 8-92*


## Email Scanning

When an email message enters your network, TippingPoint Advanced Threat Protection for Email gathers security intelligence from several Trend Micro Smart Protection Network services to investigate the email message's risk level.

- Analyzing file attachments

  See *Advanced Threat Scan Engine on page 1-10*.

- Analyzing embedded links (URLs)

  See *Web Reputation Services on page 1-11*.

- Social Engineering Attack Protection

  See *Social Engineering Attack Protection on page 1-7*.

After scanning the email message for suspicious files, URLs, and characteristics, TippingPoint Advanced Threat Protection for Email correlates the results to either assign a risk level and immediately execute a policy action based on the risk level, or send the file, URL and message samples to Virtual Analyzer for further analysis.

**Note**

The file password settings affect both TippingPoint Advanced Threat Protection for Email email scanners and Virtual Analyzer.

## Virtual Analyzer

Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, and administrators and investigators (through SSH). 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.

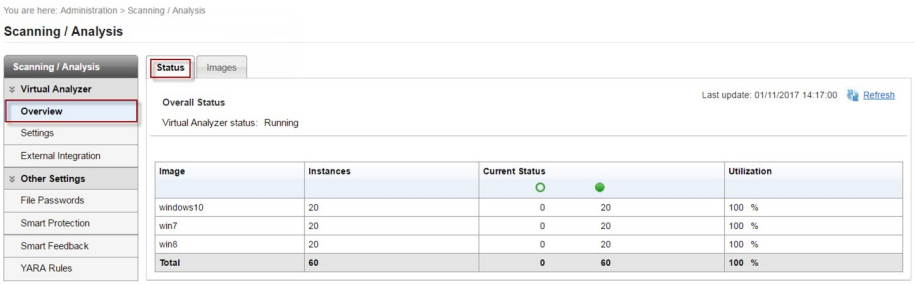
## Virtual Analyzer Overview

The **Overview** screen varies depending on whether TippingPoint Advanced Threat Protection for Email is configured to use the internal or external Virtual Analyzer sandbox environment.

If TippingPoint Advanced Threat Protection for Email is using an external Virtual Analyzer, you can configure the integration settings and check the status of the external Virtual Analyzer sandbox environment on the **External Integration** screen.

If TippingPoint Advanced Threat Protection for Email is using an internal Virtual Analyzer, click **Status** to check the status of the Virtual Analyzer sandbox environment.

View the table to understand the real-time status of Virtual Analyzer and the sandbox images.




## Virtual Analyzer Statuses

The following table describes the Virtual Analyzer statuses.

**TABLE 8-13. Virtual Analyzer Statuses**

| STATUS | DESCRIPTION |
|---|---|
| Initializing... | Virtual Analyzer is preparing the sandbox environment. |
| Starting... | Virtual Analyzer is starting all sandbox instances. |
| Stopping... | Virtual Analyzer is stopping all sandbox instances. |
| Running | Virtual Analyzer is analyzing samples. |
| No images | No images have been imported into Virtual Analyzer. |
| Modifying instances... | Virtual Analyzer is increasing or decreasing the number of instances for one or more images. |
| Importing images... | Virtual Analyzer is importing an image. |

## Overall Status Table

The Virtual Analyzer **Overall Status** table shows the allocated instances, status (busy or idle), and the utilization information for each sandbox image.

**TABLE 8-14. Overall Status Table Descriptions**

| HEADER | 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 |

## Virtual Analyzer Images

Virtual Analyzer does not contain any images by default. You must import an image before Virtual Analyzer can analyze samples.

Virtual Analyzer supports Open Virtualization Format Archive (OVA) files.

**Note**

Before importing custom images, verify that you have secured valid licenses for all included platforms and applications.

Use the Image Preparation Tool to check that an image has the correct virtual machine settings, supported platforms and required applications before importing the image to Virtual Analyzer. For details about the Image Preparation Tool, see the *Virtual Analyzer Image Preparation User's Guide* at http://docs.trendmicro.com/en-us/enterprise/virtual-analyzer-image-preparation.aspx.

### Virtual Analyzer Image Preparation

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 Virtual Analyzer Images

Virtual Analyzer supports OVA files between 1GB and 20GB in size.

**Note**

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

If TippingPoint Advanced Threat Protection for Email is registered to Deep Discovery Director, you can also import an image to TippingPoint Advanced Threat Protection for Email through image deployment from Deep Discovery Director.

**Procedure**

1. Go to **Administration** > **Scanning / Analysis** > **Virtual Analyzer** > **Overview** > **Images**.
2. Click **Import**.

   The **Import Image** screen appears.
3. Specify a name in the **Image** field.
4. Specify the number of instances for this image.
5. Select an image source and configure the applicable settings.
   - **Local or network folder**

     See *Importing an Image from a Local or Network Folder on page 8-75*.
   - **HTTP or FTP server**

     See *Importing an Image from an HTTP or FTP Server on page 8-76*.

### Importing an Image from a Local or Network Folder

The following procedure explains how to import an image into Virtual Analyzer from a local or network folder. Before importing an image, verify that your computer has established a connection to TippingPoint Advanced Threat Protection for Email. From the **Images** screen, check the connection status under **Step 1** on the management console.

---

**Procedure**

1. Select **Local or network folder**.
2. Specify an image name with a maximum of 260 characters/bytes.
3. Click **Connect**.
4. Once connected, import the image using the Virtual Analyzer Image Import Tool.
   a. Click **Download Image Import Tool**.
   b. Open the file `VirtualAnalyzerImageImportTool.exe`.
   c. Specify the TippingPoint Advanced Threat Protection for Email management IP address.

   **Note**

   For information about configuring the TippingPoint Advanced Threat Protection for Email management IP address, see *Configuring Network Settings on page 8-9*.

   d. Click **Browse** and select the image file.
   e. Click **Import**.

   The import process will stop if:

   - The connection to the device was interrupted
   - Memory allocation was unsuccessful
   - Windows socket initialization was unsuccessful

- The image file is corrupt

5. Wait for import to complete.

**Note**

Virtual Analyzer deploys the imported image to sandbox instances immediately after the image uploads.

### Importing an Image from an HTTP or FTP Server

The following procedure explains how to import an image into Virtual Analyzer from an HTTP or FTP server. For information about adding images, see *Importing Virtual Analyzer Images on page 8-74*.

**Procedure**

1. Select **HTTP or FTP server**.
2. Specify the HTTP or FTP URL settings.

| Option | Description |
|---|---|
| URL | Specify the HTTP or FTP URL.<br>Example: `ftp://custom_ftp:1080/tmp/test.ova` |
| User name | Optional: Specify the user name if authentication is required. |
| Password | Optional: Specify the password if authentication is required. |
| Anonymous Login | Optional: Select to disable the user name and password, and authenticate anonymously. |

3. Click **Import**.
4. Wait for deployment to complete.

**Note**

Virtual Analyzer deploys instances immediately.

## Deleting Virtual Analyzer Images

**Procedure**

1. Go to **Administration** > **Scanning / Analysis** > **Virtual Analyzer** > **Overview** > **Images**
2. Select an image by selecting the box in the left column.
3. Click **Delete**.

   The image is removed.

## Modifying Instances

**Procedure**

1. Go to **Administration** > **Scanning / Analysis** > **Virtual Analyzer** > **Overview** > **Images**.
2. Click **Modify**.

   The **Modify Instances** screen appears.
3. Modify the instances allocated to any image.
4. Click **Save**.

# Configuring Virtual Analyzer Network and Filters

To reduce the number of files in the Virtual Analyzer queue, configure the file submission filters and enable exceptions.

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

---

**Procedure**

1. Go to **Administration** > **Scanning / Analysis** > **Virtual Analyzer**.
2. Specify **Settings**.

| OPTION | DESCRIPTION |
|---|---|
| Network Connection | **Note**<br>This section is available when TippingPoint Advanced Threat Protection for Email is using an internal Virtual Analzyer.<br>When the internal Virtual Analyzer is set to connect to the Internet through a proxy server, reconfigure proxy settings after a configuration restore or firmware update on TippingPoint Advanced Threat Protection for Email.<br><br>From the **Network type** drop-down list, select how Virtual Analyzer connects to the network. For information about network types, see *Virtual Analyzer Network Types on page 8-80*.<br>If you select the **Custom Network** type, select a specific port for Virtual Analyzer traffic from the **Sandbox port** drop-down list and click **Configure IPv4 settings** to configure the network settings.<br>If a proxy server is required for the internal Virtual Analyzer to connect to the Internet, select **Use a dedicated proxy server** from the drop-down list and provide the following information:<br>• **Server address**<br>• **Port**<br>• **Proxy server requires authentication**: If authentication is required, select this check box and type the user name and password. |

| OPTION | DESCRIPTION |
|---|---|
| Submission Filters | **Files**: Select the file types to have Virtual Analyzer perform one of the following actions:<br>• Submit only highly suspicious files<br>• Submit highly suspicious files and force analyze all selected file types<br>**Exceptions**: Select Certified Safe Software Service to reduce the likelihood of false-positive detections.<br>For details, see *Certified Safe Software Service on page 8-79*. |
| Timeout Setting | Select how long Virtual Analyzer should wait before timing out a submitted object. Virtual Analyzer does not assign any risk level to objects that have time out. Timed out objects still receive risk levels from other scan engines. |

3. Click **Save**.

## Certified Safe Software Service

Certified Safe Software Service (CSSS) is the Trend Micro cloud database of known safe files. Trend Micro datacenters are queried to check submitted files against the database.

Enabling CSSS prevents known safe files from entering the Virtual Analyzer queue. This process:

- Saves computing time and resources
- Reduces the likelihood of false positive detections

**Tip**

CSSS is enabled by default. Trend Micro recommends using the default settings.

## Virtual Analyzer Network Types

When simulating file and URL behavior, Virtual Analyzer uses its own analysis engine to determine the risk of an object. The selected network type also determines whether submitted objects can connect to the Internet.

After configuring the network connection, click **Test Internet Connectivity** to verify that Virtual Analyzer can connect to the Internet.

**Note**

Internet access improves analysis by allowing samples to access C&C callback addresses or other external links.

| Network Type | Description |
|---|---|
| Management network | Direct Virtual Analyzer traffic through the management port.<br><br>**Important**<br>Enabling connections to the management network may result in malware propagation and other malicious activity in the network. |
| Custom network | Virtual Analyzer connects to the Internet using a port other than the management port.<br><br>**Note**<br>Trend Micro recommends using an environment isolated from the management network, such as a test network with Internet connection but without proxy settings, proxy authentication, and connection restrictions. |

| Network Type | Description |
|---|---|
| No network access | Isolate Virtual Analyzer traffic within the sandbox environment. The environment has no connection to an outside network.<br><br>**Note**<br>Virtual Analyzer has no Internet connection and relies only on its analysis engine.<br><br>No URLs are submitted for analysis. |

## Virtual Analyzer File Submission Filters

In addition to highly suspicious files, Virtual Analyzer can also scan for a variety of file types.

The following table shows the displayed file categories, contained full file types, and file extensions.

**Table 8-15. Virtual Analyzer File Submission Filters**

| Displayed File Category | Full File Type | Example File Extensions |
|---|---|---|
| Flash and other multimedia | Scalable Vector Graphics (SVG)<br>Adobe™ Shockwave™ Flash file<br>Apple QuickTime media | `.svg`<br>`.swf`<br>`.mov` |
| Java | Java Archive (JAR)<br>Java class file | `.jar`<br>`.class` |
| Office | Microsoft™ Word™ document<br>Microsoft™ OLE document<br>Microsoft™ Office Word™ (2007 or later) document<br>Microsoft™ Powerpoint™ presentation | `.doc`<br>`.dot`<br>`.docx`<br>`.dotx`<br>`.pps` |

| Displayed File Category | Full File Type | Example File Extensions |
|---|---|---|
| | Microsoft™ Office PowerPoint™ (2007 or later) presentation<br>Microsoft™ Excel™ spreadsheet<br>Microsoft™ Office Excel™ (2007 or later) spreadsheet<br>Microsoft™ Office™ 2003 XML file<br>Microsoft™ Word™ 2003 XML document<br>Microsoft™ Excel™ 2003 XML spreadsheet<br>Microsoft™ PowerPoint™ 2003 XML presentation<br>Microsoft™ Publisher 2016<br>Hancom™ Hancell spreadsheet<br>Hancom™ Hangul Word Processor (HWP) document<br>Hancom™ Hangul Word Processor (2014 or later) (HWPX) document<br>JustSystems™ Ichitaro™ document<br>JungUm™ Global document<br>Microsoft™ Outlook™ Item | .ppsx<br>.ppt<br>.pptx<br>.pub<br>.xla<br>.xls<br>.xlsx<br>.xlt<br>.xlm<br>.cell<br>.xml<br>.xlsb<br>.xltx<br>.hwp<br>.hwpx<br>.jtd<br>.gul<br>.msg |
| Office with Macros | Microsoft™ Office Word™ 2007 macro-enabled document<br>Microsoft™ Office PowerPoint™ 2007 macro-enabled presentation<br>Microsoft™ Office Excel™ 2007 macro-enabled spreadsheet | .docm<br>.dotm<br>.potm<br>.ppam<br>.ppsm<br>.pptm |

| Displayed File Category | Full File Type | Example File Extensions |
|---|---|---|
| | | .xlam<br>.xlsm<br>.xltm |
| Other document formats | Compiled HTML (CHM) help file<br>Microsoft™ Windows™ Shell Binary Link shortcut<br>Microsoft™ Rich Text Format (RTF) document | .chm<br>.lnk<br>.rtf |
| PDF | Adobe™ Portable Document Format (PDF) | .pdf |
| Scripts | Microsoft™ Windows™ Batch file<br>Microsoft™ Windows™ Command Script file<br>JavaScript™ file<br>JavaScript™ encoded script file<br>HTML Application file<br>Microsoft™ Windows™ PowerShell script file<br>Visual Basic™ encoded script file<br>Visual Basic™ script file<br>Microsoft™ Windows™ script file | .bat<br>.cmd<br>.js<br>.jse<br>.hta<br>.ps1<br>.vbe<br>.vbs<br>.wsf |
| Windows executables | AMD™ 64-bit DLL file<br>Microsoft™ Windows™ 16-bit DLL file<br>Microsoft™ Windows™ 32-bit DLL file<br>Executable file (EXE)<br>AMD™ 64-bit EXE file<br>DIET DOS EXE file<br>Microsoft™ DOS EXE file<br>IBM™ OS/2 EXE file | .cpl<br>.crt<br>.dll<br>.drv<br>.exe<br>.ocx<br>.scr<br>.sys |

| Displayed File Category | Full File Type | Example File Extensions |
|---|---|---|
| | LZEXE DOS EXE file | |
| | MIPS EXE file | |
| | MSIL Portable executable file | |
| | Microsoft™ Windows™ 16-bit EXE file | |
| | Microsoft™ Windows™ 32-bit EXE file | |
| | ARJ compressed EXE file | |
| | ASPACK 1.x compressed 32-bit EXE file | |
| | ASPACK 2.x compressed 32-bit EXE file | |
| | GNU UPX compressed 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 | |
| | PEPACK compressed executable | |
| | PKWARE™ PKLITE™ compressed DOS EXE file | |
| | PETITE compressed 32-bit executable file | |
| | PKZIP compressed EXE file | |
| | WWPACK compressed executable file | |

## Configuring an External Virtual Analyzer

You can configure TippingPoint Advanced Threat Protection for Email to integrate with TippingPoint Advanced Threat Protection Analyzer to perform suspicious object analysis.

**Procedure**

1. Go to **Administration** > **Scanning / Analysis** > **Virtual Analyzer** > **External Integration**.
2. From the **Source** drop-down list, select **External**.
3. In the **Server address** field, provide the IP address or FQDN of the TippingPoint Advanced Threat Protection Analyzer server.
4. If your company uses a proxy server, select **Connect using a proxy server**.

   **Note**

   For information about configuring proxy settings, see *Configuring Proxy Settings on page 8-13*.

5. Type the API key.
6. (Optional) Click **Test Connection** to verify the server settings.
7. Click **Save**.

## File Passwords

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 for Email can also heuristically discover passwords in email messages to extract files.

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

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

- 7z

- `zip`
- `tar`
- `arj`

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

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

**Note**

File passwords are stored as unencrypted text.

## Adding File Passwords

A maximum of 100 passwords is allowed.

**Procedure**

1. Go to **Administration** > **Scanning / Analysis** > **Other Settings** > **File Passwords**.
2. Click **Add password**.
3. Type a password with only ASCII characters.

**Note**

Passwords are case-sensitive and must not contain spaces.

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

## Importing File Passwords

A maximum of 100 passwords is allowed.

**Procedure**

1. Go to **Administration** > **Scanning / Analysis** > **Other Settings** > **File Passwords**.

   The **File Passwords** screen appears.

2. Click **Import passwords**.

   The **Import Passwords** window appears.

3. Browse and select the file to import.

   **Note**

   Click **Download sample file** to view a sample of a properly formatted file.

   The passwords are checked and any invalid or duplicate items are identified.

4. Click **Import**.

## Smart Protection

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 for Email can obtain reputation data for websites that users attempt to access. TippingPoint Advanced Threat Protection for Email 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 for Email does not use the File Reputation Service that is part of Smart Protection technology.

TippingPoint Advanced Threat Protection for Email 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 8-16. 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<br><br>To configure Smart Protection Network as source, see *Configuring Smart Protection Settings on page 8-90* . | Use as primary source and the Smart Protection Network as an alternative source<br><br>For guidelines on setting up Smart Protection Server and configuring it as source, see *Setting Up Smart Protection Server on page 8-90* and *Configuring Smart Protection Settings on page 8-90*. |

## 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 for Email. 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 for Email 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 for Email management console.

   For details, see *Configuring Smart Protection Settings on page 8-90*.

**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** > **Scanning / Analysis** > **Other Settings** > **Smart Protection**.
2. Select **Connect to Web Reputation Services using Smart Protection Server**.
3. Configure the Smart Protection Server.

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

      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. Select **Connect using a proxy server** if proxy settings for TippingPoint Advanced Threat Protection for Email 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 for Email directly.

c. Specify the port number.

4. Click **Test Connection** to verify that specified Smart Protection Server can connect to global services.

> **Important**
>
> TippingPoint Advanced Threat Protection for Email only supports global services when connecting using Smart Protection Server version 3.0 Patch 2.

5. (Optional) Select **Connect to global services using Smart Protection Server** to configure TippingPoint Advanced Threat Protection for Email to query global Smart Protection services.

   - If your organization uses a CA certificate, select **Use certificate** and click **Browse** to select the certificate file; then, click **Import** to import the certificate file.

     - If your organization uses a Certificate Revocation List (CRL), select **Use CRL** and click **Browse** to select the CRL file; then, click **Import** to import the Certificate Revocation List file.

6. Click **Save**.

## Smart Feedback

TippingPoint Advanced Threat Protection for Email integrates the new Trend Micro Feedback Engine. This engine sends threat information to the Trend Micro Smart Protection Network, which allows Trend Micro to identify and protect against new

threats. Participation in Smart Feedback authorizes Trend Micro to collect certain information from your network, which is kept in strict confidence.

Information collected by Smart Feedback:

- 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 **Administration** > **Scanning / Analysis** > **Other Settings** > **Smart Feedback**.
2. Select Smart Feedback settings.
   - Select **Enable Smart Feedback (recommended)** to send anonymous information to Trend Micro from your network.
   - Select **Send suspicious executable files to Trend Micro** to send suspicious files found as high-risk in Virtual Analyzer to Trend Micro for further investigation.

     For details about detected risk levels, see *Virtual Analyzer Risk Levels on page 4-4*.
3. Click **Save**.

## YARA Rules

TippingPoint Advanced Threat Protection for Email 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 for Email supports a maximum of 5,000 enabled YARA rules regardless of the number of YARA rule files. On the top-right

corner of the YARA rule table, the **Rules in use** field indicates the number of YARA rules currently enabled in the system.

The following table shows information about YARA rule files.

**TABLE 8-17. YARA Rules**

| FIELD | DESCRIPTION |
|---|---|
| File name | Name of the YARA rule file. |
| Risk level | Risk level of the YARA rules. |
| 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. |
| Status | Toggle to enable or disable the YARA rule file. |

## Creating a YARA Rule File

TippingPoint Advanced Threat Protection for Email 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 8-18. 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:<br>• 1 to 9 = Low risk<br>• 10 = High risk<br>**Note**<br>The weight value does not correspond to the risk level assigned by TippingPoint Advanced Threat Protection for Email. |
| 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. Go to **Administration** > **Scanning / Analysis** > **Other Settings** > **YARA Rules**.
2. Click **Add** to add a YARA rule file.

   The **Add YARA Rule File** window appears.
3. In the new window that opens, configure the following:

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

   b. **Risk level**: Select the detection risk level for the YARA rules in the file.

   c. **Files to analyze**: Type or select file types that Virtual Analyzer processes specific to this YARA rule file.
4. 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 8-93*.

## Editing a YARA Rule File

**Procedure**

1. Go to **Administration** > **Scanning / Analysis** > **Other Settings** > **YARA Rules**.
2. Click a file name to edit a YARA rule file.

   The **Edit YARA Rule File** window appears.
3. Make changes to the settings.
4. Click **Save**.

## Deleting a YARA Rule File

**Procedure**

1. Go to **Administration** > **Scanning / Analysis** > **Other Settings** > **YARA Rules**.
2. Select one or several YARA rule files to remove.
3. Click **Delete**.

## Exporting a YARA Rule File

**Procedure**

1. Go to **Administration** > **Scanning / Analysis** > **Other Settings** > **YARA Rules**.
2. Select a YARA rule file to export.

**Note**

You can export only one YARA rule at a time.

3. Click **Export**.

# System Maintenance

Go to the **System Maintenance** screen to perform the following operations:

- *Backing Up or Restoring a Configuration on page 8-97*
- *Configuring Storage Maintenance on page 8-101*
- *Debug Logs on page 8-103*
- *Testing Network Connections on page 8-104*

## Backing Up or Restoring a Configuration

Export settings from the management console to back up the TippingPoint Advanced Threat Protection for Email configuration. If a system failure occurs, you can restore the settings by importing the configuration file that you previously backed up.

**Important**

TippingPoint Advanced Threat Protection for Email only supports restoring configurations from other TippingPoint Advanced Threat Protection for Email servers running the same version. For example, you cannot restore a server running version 2.6 with a configuration file backed up from a server running version 2.5.

**Note**

When exporting/importing your settings, the database will be locked. Therefore, all TippingPoint Advanced Threat Protection for Email actions that depend on database access will not function.

Trend Micro recommends:

- Backing up the current configuration before each import operation
- Performing the operation when TippingPoint Advanced Threat Protection for Email is idle. Importing and exporting affects TippingPoint Advanced Threat Protection for Email performance.

Back up settings to create a copy of TippingPoint Advanced Threat Protection for Email appliance configuration to restore the configuration in another TippingPoint Advanced Threat Protection for Email appliance or to revert to the backup settings at a later time. Replicate a configuration across several TippingPoint Advanced Threat Protection for Email appliances by restoring the same configuration file into each appliance.

## Backup Recommendations

Trend Micro recommends exporting your settings to:

- Keep a backup

  If TippingPoint Advanced Threat Protection for Email cannot recover from a critical problem, import your configuration backup after restoring the device to automatically implement the pre-failure configuration.

- Replicate settings across several devices

  If you have several devices on your network, you do not need to separately configure most settings.

## Backing Up a Configuration

During export, do not:

- Access other management console screens or modify any settings
- Perform any database operations
- Start/stop any services on the device or in the group to which the device belongs
- Launch other export or import tasks

You can back up settings from the screens and tabs listed in the following table.

**TABLE 8-19. Backed up configuration settings**

| SCREEN | TAB |
|---|---|
| **Dashboard** | Not applicable (all widgets and settings) |
| **Policy** > **Policy** | **Actions** |
| | **Recipient Notification** |
| | **Message Tags** |
| | **Redirect Pages** |
| **Policy** > **Exceptions** | **Messages** |
| | **Objects** |
| | **URL Keywords** |
| **Alerts / Reports** > **Alerts** | **Rules** |
| **Alerts / Reports** > **Reports** | **Schedules** |
| **Administration** > **Component Updates** | **Schedule** |
| | **Source** |
| **Administration** > **System Settings** | **Operation Mode** |
| | **Proxy** |
| | **SMTP** |
| | **Time** |
| | **SNMP** |
| **Administration** > **Mail Settings** | **Connections** |
| | **Message Delivery** |
| | **Limits and Exceptions** |
| | **SMTP Greeting** |

| Screen | Tab |
|---|---|
| **Administration** > **Integrated Products/ Services** | **Log Settings** |
| | **Microsoft Active Directory** |
| | **SFTP** |
| **Administration** > **Scanning / Analysis** | **Settings** |
| | **File Passwords** |
| | **Smart Protection** |
| | **Smart Feedback** |
| | **YARA Rules** |
| **Administration** > **System Maintenance** | **Storage Maintenance** |
| **Administration** > **Accounts / Contacts** | **Accounts** |
| | **Contacts** |

**Procedure**

1. Go to **Administration** > **System Maintenance** > **Back Up / Restore**.
2. Next to **Configuration Settings Backup**, click **Export**.

   A **File Download** window appears.
3. Click **Save** to save the configuration file to local storage.

## Restoring a Configuration

Restoring TippingPoint Advanced Threat Protection for Email settings replaces the original settings and rules, such as message delivery settings, with the imported configuration.

During import, do not:

- Access other management console screens or modify any settings.
- Perform any database operations.
- Start/stop any services on the device or in the group to which the device belongs.
- Launch other export or import tasks.

**Note**

For information on the settings that you can restore, see *Backing Up a Configuration on page 8-98*.

**Procedure**

1. Go to **Administration** > **System Maintenance** > **Back Up / Restore**.
2. Next to **Restore Configuration Settings**, click **Choose File** or **Browse** and locate the file.
3. Click **Restore**.

   All services restart. It can take up to two minutes to restart services after applying imported settings and rules.

## Configuring Storage Maintenance

Storage Maintenance allows you to control the size of your quarantine folder and the amount of log data that the system saves.

**Procedure**

1. Go to **Administration** > **System Maintenance** > **Storage Maintenance**.
2. Specify the quarantine settings.
   - **Quarantine size**: Specify the size of the quarantine folder in GB

**Note**

Depending on your version of the TippingPoint Advanced Threat Protection for Email appliance, configure the quarantine size as follows:

- TippingPoint Advanced Threat Protection for Email 7100: The quarantine size must be a value between 1 and 100
- TippingPoint Advanced Threat Protection for Email 9100: The quarantine size must be a value between 1 and 400

- **Delete message attachments, links, and analysis reports when the free quarantine space is equal to or lower than**: Specify the quarantine space threshold for automatic file deletion

**Note**

The threshold value must be between 10 and 50.

TippingPoint Advanced Threat Protection for Email purges 10% more than the specified percentage.

3. Specify the log settings.

- **Delete logs older than**: Specify the number of days to keep logs

**Note**

The specified value must be between 3 and 366.

- **Delete logs when the total free disk space is equal to or lower than**: Specify the disk space threshold for automatic log deletion

**Note**

The threshold value must be between 10 and 50.

TippingPoint Advanced Threat Protection for Email purges 10% more than the specified percentage.

**Important**

Integration with Deep Discovery Director for Virtual Analyzer image deployment requires additional disk space. After registering TippingPoint Advanced Threat Protection for Email to Deep Discovery Director, configure TippingPoint Advanced Threat Protection for Email to delete logs when the total free disk space is less than 20%.

4. Click **Save**.

# Debug Logs

TippingPoint Advanced Threat Protection for Email creates debug logs that include information Trend Micro Support uses to troubleshoot problems.

## Exporting Debugging Files

Export your debugging file to provide information to Trend Micro Support for troubleshooting a problem.

**Procedure**

1. Go to **Administration** > **System Maintenance** > **Debug Logs** .
2. Select the number of days to export.
3. Click **Export**.
4. Wait for the export to complete. The time required depends on the amount of data to export.

## Configuring Log Level

Configure the log level to save information that you can provide to Trend Micro Support for troubleshooting a problem.

**Procedure**

1. Go to **Administration** > **System Maintenance** > **Debug Logs** .
2. Select the log level.
   - Debug
   - Error
3. Click **Apply**.

## Testing Network Connections

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

**Procedure**

1. Go to **Administration** > **System Maintenance** > **Network Services Diagnostics**.
2. 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.

# Accounts / Contacts

TippingPoint Advanced Threat Protection for Email uses role-based administration to grant and control access to the management console. Use this feature to assign specific management console privileges to the accounts and present them with only the tools and permissions necessary to perform specific tasks. Each account is assigned a specific role. A role defines the level of access to the management console. Users log on to the management console using custom user accounts.

# Managing Accounts

Delegate tasks to different security and network administrators to reduce bottlenecks in TippingPoint Advanced Threat Protection for Email administration. The default administrator account ("admin") has full access to TippingPoint Advanced Threat Protection for Email.

**Note**

An account with the administrator role can add new administrator accounts.

## Account Role Classifications

| Role | Description |
|---|---|
| Administrator | Users have complete access to the features and settings contained in the menu items.<br>• **Dashboard**<br>• **Detections**<br>• **Policy**<br>• **Alerts / Reports**<br>• **Logs**<br>• **Administration**<br>• **Help** |

| Role | Description |
|---|---|
| Investigator | Users can view certain features and settings contained in the menu items, but cannot make any administrative modifications.<br>• **Dashboard**<br>• **Detections**<br>• **Alerts / Reports** > **Reports** > **Generated Reports**<br>• **Alerts / Reports** > **Alerts** > **Triggered Alerts**<br>• **Logs**<br>• **Help** |
| Operator | Users can view certain features and settings contained in the menu items, but cannot make any administrative modifications.<br>• **Dashboard**<br>• **Detections** (no access to message body)<br>• **Alerts / Reports** > **Reports** > **Generated Reports**<br>• **Alerts / Reports** > **Alerts** > **Triggered Alerts**<br>• **Logs**<br>• **Help** |

## Adding a Local User Account

**Procedure**

1. Go to **Administration** > **Accounts / Contacts** > **Accounts**.
2. Click **Add**.

   The **Add Account** screen appears.
3. Toggle the **Status** of this account.
4. Select **Local user** from the **Type** drop-down list.

5. Specify the account user name and password.
6. Select a **Role** for this account. The role determines the level of access this account has.

   See *Account Role Classifications on page 8-105*.

7. Click **Save**.

   The new account is added to the **Accounts** list.

## Adding an Active Directory User Account or Group

**Note**

Microsoft Active Directory Integration has to be configured before an Active Directory user account or group can be added.

For details, see *Microsoft Active Directory on page 8-65*.

**Procedure**

1. Go to **Administration** > **Accounts / Contacts** > **Accounts**.
2. Click **Add**.

   The **Add Account** screen appears.

3. Toggle the **Status** of this account.
4. Select **Active Directory user or group** as the **Type** of this account.
5. Type a user or group name and click **Search** to search the Active Directory for matching user accounts or groups.

   Matching user accounts and groups are displayed in the results table.

**Note**

User accounts are not displayed in the results table if:

- The user account's User Principle Name (UPN) is not specified on the Active Directory server
- The user account is disabled on the Active Directory server

6. Select the Active Directory user account or group to add.
7. Select a **Role** for this account. The role determines the level of access this account has.

   See *Account Role Classifications on page 8-105*.

8. Click **Save**.

   The new account is added to the **Accounts** list.

## Editing Accounts

Change account permissions to adjust settings for a role revision or other organizational changes.

**Procedure**

1. Go to **Administration** > **Accounts / Contacts** > **Accounts**.
2. Click the account name hyperlink.
3. Make the required changes.
4. Click **Save**.

## Deleting Accounts

Delete accounts to adjust settings for a role revision or other organizational changes.

**Note**

You can only delete custom accounts. You cannot delete the default TippingPoint Advanced Threat Protection for Email administrator account.

**Procedure**

1. Go to **Administration** > **Accounts / Contacts** > **Accounts**.
2. Select the account to remove.
3. Click **Delete**.
4. At the confirmation message, click **OK**.

## Changing Your Password

**Note**

The passwords of Microsoft Active Directory accounts and Trend Micro Control Manager single sign-on (SSO) accounts cannot be changed from the management console.

**Procedure**

1. On the management console banner, click your account name.

   The **Change Password** screen appears.
2. Specify password settings.
   - **Old password**
   - **New password**
   - **Confirm password**
3. Click **Save**.

## Managing Contacts

Type the email addresses of notification contacts that are sent alert notifications and reports.

For details, see *Scheduling Reports on page 6-22* and *Configuring Alert Notifications on page 6-5*.

# License

For information about managing your product license, see *Maintenance on page 9-1*.

# About TippingPoint Advanced Threat Protection for Email

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

# Chapter 9

# Maintenance

Topics include:


- *Maintenance Agreement on page 9-2*
- *Activation Codes on page 9-2*
- *Product License Description on page 9-3*
- *Product License Status on page 9-3*
- *Viewing Your Product License on page 9-4*
- *Managing Your Product License on page 9-5*

# Maintenance Agreement

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration 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.

Typically, 90 days before the Maintenance Agreement expires, you will be alerted of the pending discontinuance. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Microsales, or on the Trend Micro Online Registration URL:

https://olr.trendmicro.com/registration/

# Activation Codes

Use a valid Activation Code to enable your product. A product will not be operable until activation is complete. An Activation Code has 37 characters (including the hyphens) and appears as follows:

xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

If you received a Registration Key instead of an Activation Code, use it to register the product at:

https://olr.trendmicro.com/registration/

A Registration Key has 22 characters (including the hyphens) and appears as follows:

xx-xxxx-xxxx-xxxx-xxxx

After registration, your Activation Code is sent via email.

# Product License Description

The following table describes your product license. Make an informed decision about your Maintenance Agreement with Trend Micro. For information about viewing the product license, see *Viewing Your Product License on page 9-4*.

| ITEM | DESCRIPTION |
|---|---|
| **Product Details** | |
| Product | The product name is TippingPoint Advanced Threat Protection for Email. |
| Version | The product version is associated with the Activation Code and product license. The product version is helpful for troubleshooting an issue. |
| **License Details** | |
| Activation Code | The Activation Code has 37 characters (including the hyphens) and appears as follows:<br>xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx<br>For details, see *Activation Codes on page 9-2*. |
| Type | The license type includes full and trial licenses. The Maintenance Agreement defines the available license type. |
| Status | The current state of your product license. For information about the product license statuses, see *Product License Status on page 9-3*. |
| Expires on | The date that the license expires. |

# Product License Status

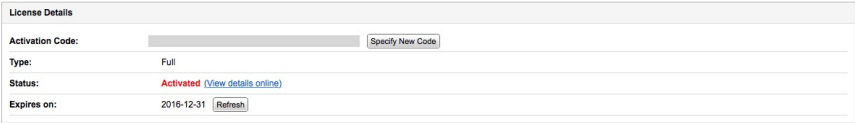
Your product license status changes from when you first acquire the product to when you must renew the license. Some of these statuses require intervention in order to maintain all product functionality. You can evaluate the product without activating a product license.

| Status | Description |
|---|---|
| Evaluation | TippingPoint Advanced Threat Protection for Email has full product functionality for a limited trial period. The trial period is based on the Maintenance Agreement. |
| Not Activated | Technical support and component updates are not available. TippingPoint Advanced Threat Protection for Email passes all email messages without investigation until the product license is activated. |
| Activated | TippingPoint Advanced Threat Protection for Email has full product functionality and component updates for the license period. Technical Support is available based on the Maintenance Agreement. |
| Expired | The license is no longer valid. After the grace period lapses, product functionality is limited.<br>• For evaluation licenses, component updates and scanning are not available.<br>• For full licenses, technical support and component updates are not available. Scanning is maintained with outdated components.<br>**WARNING!**<br>Outdated components significantly reduce product detection capabilities. |

# Viewing Your Product License

**Procedure**

1. Go to **Administration** > **License**.




2. Under **License Details**:

- Click **View details online** to display the Trend Micro Online Registration website.
- Click **Refresh** to manually synchronize the license expiration date.

# Managing Your Product License

**Procedure**

1. Go to **Administration** > **License**.
2. Click **Specify New Code**.

   The **Activation Code** screen displays.
3. Specify the new Activation Code.
4. Read the license agreement and select **I have read and accept the terms of the Trend Micro License Agreement**.
5. Click **Apply**.

   The TippingPoint Advanced Threat Protection for Email activates.
6. View your product license.

   See *Viewing Your Product License on page 9-4*.

# Chapter 10

# Technical Support

Learn about the following topics:


- *Troubleshooting Resources on page 10-2*
- *Contacting Trend Micro TippingPoint Support on page 10-3*
- *Sending Suspicious Content to Trend Micro on page 10-4*
- *Other Resources on page 10-5*

# 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 TippingPoint Support

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

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

- Visit us online at:

  http://www.trendmicro.com/tippingpoint

- Trend Micro product documentation:

  http://docs.trendmicro.com

# 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

# Appendices

## Appendices

# Appendix A

## Transport Layer Security

Topics include:


- *About Transport Layer Security on page A-2*
- *Deploying TippingPoint Advanced Threat Protection for Email in TLS Environments on page A-2*
- *Prerequisites for Using TLS on page A-3*
- *Configuring TLS Settings for Incoming Messages on page A-4*
- *Configuring TLS Settings for Outgoing Messages on page A-5*
- *Creating and Deploying Certificates on page A-6*

# About Transport Layer Security

Transport Layer Security (TLS) provides a secure communication channel between hosts over the Internet, ensuring the privacy and integrity of the data during transmission.

Two hosts (the TippingPoint Advanced Threat Protection for Email appliance and the email relay) establish a TLS session as follows:

1. The sending host requests a secure connection with the receiving host by sending a cipher list.
2. The two hosts establish a connection.
3. The receiving host selects one cipher and replies with its digital certificate signed by a Certificate Authority (CA).
4. The sending host verifies the identity with the trusted CA certificate and generates the session keys by encrypting a message using a public key.
5. The receiving host decrypts the message using the corresponding private key.
6. The sending host's identity verifies when the receiving host can decrypt the message with the private key.
7. The TLS session establishes and email messages passed between the hosts are encrypted.

**Tip**

By default, TippingPoint Advanced Threat Protection for Email does not apply TLS or email encryption, nor does it verify email relay host identities. Enable TLS for TippingPoint Advanced Threat Protection for Email to encrypt incoming email messages.

# Deploying TippingPoint Advanced Threat Protection for Email in TLS Environments

Enable the TLS settings for messages entering and exiting TippingPoint Advanced Threat Protection for Email.

**Procedure**

1. Review the prerequisites.

   See *Prerequisites for Using TLS on page A-3*.

2. Enable incoming TLS.

   See *Configuring TLS Settings for Incoming Messages on page A-4*.

3. Enable outgoing TLS.

   See *Configuring TLS Settings for Outgoing Messages on page A-5*.

# Prerequisites for Using TLS

Establishing the TLS infrastructure requires that the organization has its own Certificate Authority (CA) key or is able to sign all generated certificate requests by an external CA. Private keys and certificate requests must be generated for each SMTP server in the network. The certificate requests should be signed by the CA.

## Obtaining a Digital Certificate

To obtain a digital certificate,apply for the certificate and public/private key pairs from a certificate authority.

**Note**

TippingPoint Advanced Threat Protection for Email provides a default certificate and key file.

## Ensure that the Certificate Format is Valid

- TippingPoint Advanced Threat Protection for Email only supports the PEM certificate format.

- Ensure that the signed certificate contains both the private key and certificate information.

# Configuring TLS Settings for Incoming Messages

TippingPoint Advanced Threat Protection for Email applies TLS to messages that enter and exit the server where TippingPoint Advanced Threat Protection for Email is installed. Message traffic exits TippingPoint Advanced Threat Protection for Email to downstream MTA that deliver the email messages to recipients.

**Procedure**

1. Go to **Administration** > **Mail Settings** > **Connections**.
2. Go to the bottom of the page to the section titled **Transport Layer Security**.
3. Select **Enable Incoming TLS**.

   This option allows the TippingPoint Advanced Threat Protection for Email SMTP Server to provide Transport Layer Security (TLS) support to SMTP email relays, but does not require that email relays use TLS encryption to establish the connection.
4. Select **Only accept SMTP connections through TLS** for TippingPoint Advanced Threat Protection for Email to only accept secure incoming connections.

   This option enables the TippingPoint Advanced Threat Protection for Email SMTP server to accept messages only through a TLS connection.
5. Click a **Browse** button next to one of the following:

| Option | Description |
|---|---|
| CA certificate | The CA certificate verifies an SMTP email relay. However, TippingPoint Advanced Threat Protection for Email does not verify the email relay and only uses the CA certificate for enabling the TLS connection. |
| Private key | The SMTP email relay creates the session key by encrypting a random number using the TippingPoint Advanced Threat Protection for Email SMTP server's public key.<br><br>The TippingPoint Advanced Threat Protection for Email SMTP server then uses the private key to decrypt the random number in order to establish the secure connection.<br><br>This key must be uploaded to enable a TLS connection. |
| SMTP server certification | SMTP email relays can generate session keys with the TippingPoint Advanced Threat Protection for Email SMTP server public key.<br><br>Upload the key to enable a TLS connection. |

6. Click **Save**.

## Configuring TLS Settings for Outgoing Messages

TippingPoint Advanced Threat Protection for Email applies TLS to messages that enter and exit TippingPoint Advanced Threat Protection for Email. Message traffic exits TippingPoint Advanced Threat Protection for Email to downstream MTAs that deliver the email messages to recipients.

**Procedure**

1. Go to **Administration** > **Mail Settings** > **Connections**.
2. Go to the bottom of the page to the section titled **Transport Layer Security**.

3. Select **Enable outgoing TLS**.
4. Click **Save**.

# Creating and Deploying Certificates

This section introduces how to create and deploy certificates in TippingPoint Advanced Threat Protection for Email for Transport Layer Security (TLS) environments.

**Important**

Create the certificate on a separate machine running Linux, not on the TippingPoint Advanced Threat Protection for Email appliance. After creating the certificate, upload the certificate through the TippingPoint Advanced Threat Protection for Email management console at **Administration** > **Mail Settings** > **Connections** in the **Transport Layer Security** section.

## Creating the Certificate Authority Key and Certificate

Organizations that do not have existing CA infrastructure can obtain a CA private key and certificate through a well-known, external service, such as VeriSign™, or execute the following procedure to generate their own CA private key and certificate.

```
# openssl req -x509 -days 365 -newkey rsa:1024 -keyout /tmp/
root_key.pem -out /tmp/root_req.pem

Generating a 1024 bit RSA private key

...................++++++

..............++++++

writing new private key to '/tmp/root_key.pem'

Enter PEM pass phrase:Trend

-----
```

```
You are about to be asked to enter information that will be
incorporated into your certificate request.

What you are about to enter is what is called a Distinguished
Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [GB]:DE

State or Province Name (full name) [Berkshire]:Bavaria

Locality Name (eg, city) [Newbury]:Munich

Organization Name (eg, company) [My Company Ltd]: Trend Micro

Organizational Unit Name (eg, section) []:Global Training

Common Name (eg, your name or your server's host name) []:EF

Email Address []:email@domain.com
```

After the completion of this procedure, the `/tmp/root_key.pem` file contains the private key encrypted with the "Trend" password. The `/tmp/root_key.pem` file contains the self-signed certificate that must be distributed to all clients and servers. Both are stored in the PEM-format.

**WARNING!**

The Organization (O) field for the CA and key owners must be the same.

After obtaining a CA private key and certificate:

- Deploy the CA certificate on all servers.
- Have all certificates issued in your organization signed by the CA.

## Creating the TippingPoint Advanced Threat Protection for Email Private Key and Certificate

Create the TippingPoint Advanced Threat Protection for Email private key and certificate to secure the communication channel.

```
# openssl genrsa -out /tmp/ddei_key.pem

Generating RSA private key, 1024 bit long modulus

.....................++++++

....++++++

e is 65537 (0x10001)

# openssl req -new -key /tmp/ddei_key.pem -out /tmp/ddei_req.pem

You are about to be asked to enter information that will be
incorporated into your certificate request.

What you are about to enter is what is called a Distinguished
Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [GB]:DE

State or Province Name (full name) [Berkshire]:Bavaria

Locality Name (eg, city) [Newbury]:Munich

Organization Name (eg, company) [My Company Ltd]:Trend Micro

Organizational Unit Name (eg, section) []:Global Training

Common Name (eg, your name or your server's host name)
[]:linux.course.test
```

```
Email Address []:<Enter>

Please enter the following 'extra' attributes to be sent with
your certificate request

A challenge password []:<Enter>

An optional company name []:<Enter>
```

After completing this procedure, the `/tmp/ddei_key.pem` file contains the TippingPoint Advanced Threat Protection for Email (`linux.course.test`) private key in PEM-format. The `/tmp/ddei_req.pem` file contains the unsigned certificate (certificate request) in the PEM-format.

**WARNING!**

The Common Name (CN) field for the key owner must be equal to the FQDN or be the same as the name specified in the domain-based delivery.

## Creating the Keys and Certificates for Other Servers

Keys and certificates for other communicating servers must be created if they do not exist. The following procedure describes the key and certificate generation for host `linux.course.test`.

```
# openssl genrsa -out /tmp/linux_key.pem 1024

Generating RSA private key, 1024 bit long modulus

.....................................++++++

................++++++

e is 65537 (0x10001)

# openssl req -new -key /tmp/linux_key.pem -out /tmp/linux_req.pem

You are about to be asked to enter information that will be
incorporated into your certificate request.

What you are about to enter is what is called a Distinguished
Name or a DN.
```

```
There are quite a few fields but you can leave some blank

For some fields there will be a default value

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [GB]:DE

State or Province Name (full name) [Berkshire]:Bavaria

Locality Name (eg, city) [Newbury]:Munich

Organization Name (eg, company) [My Company Ltd]:Trend Micro

Organizational Unit Name (eg, section) []:Global Training

Common Name (eg, your name or your server's host name)
[]:linux.course.test

Email Address []:<Enter>

Please enter the following 'extra' attributes to be sent with
your certificate request

A challenge password []:<Enter>

An optional company name []:<Enter>
```

After completing this procedure, the `/tmp/linux_key.pem` file contains the linux.course.test private key in PEM-format. The `/tmp/linux_req.pem` file contains the unsigned certificate (certificate request) in the PEM-format.

## Signing the TippingPoint Advanced Threat Protection for Email Certificate

Signing the certificate is optional. The certificate must be signed if you do not want to distribute all the certificates on systems and only distribute the CA certificate. To confirm that the TippingPoint Advanced Threat Protection for Email certificate is trusted by the CA, you need to sign the TippingPoint Advanced Threat Protection for Email certificate request by the CA private key (`/tmp/root_key.pem`) but before doing this you need to set up the OpenSSL environment for CA:

**Procedure**

1. Update the OpenSSL configuration file `/etc/pki/tls/openssl.cnf`.

   Find the definition of the [ CA_default ]/ dir parameter and change it to `/etc/pki/CA`:

   ```
   [ CA_default ]
   dir = /etc/pki/CA # Where everything is kept
   ```

2. Create the empty index.txt file in the `/etc/pki/CA` directory:

   ```
   # touch /etc/pki/CA/index.txt
   ```

3. Create the serial file with initial content in the `/etc/pki/CA` directory:

   ```
   # echo "01" > /etc/pki/CA/serial
   ```

4. Sign the certificate:

   ```
   # openssl ca -days 365 -cert /tmp/root_req.pem -keyfile /tmp/
   root_key.pem -in /tmp/ddei_req.pem -out /tmp/ddei_cert.pem -
   outdir /tmp
   Using configuration from /etc/pki/tls/openssl.cnf
   Enter pass phrase for /tmp/root_key.pem:Trend
   Check that the request matches the signature
   Signature ok
   Certificate Details:
   Serial Number: 1 (0x1)
   Validity
   Not Before: Oct 22 09:35:52 2010 GMT
   Not After : Oct 22 09:35:52 2011 GMT
   Subject:
   countryName = DE
   ```

```
stateOrProvinceName = Bavaria

organizationName = Trend Micro

organizationalUnitName = Global Training

commonName = ddei.course.test

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

Netscape Comment:

X509v3 Subject Key Identifier:

82:15:B8:84:9C:40:8C:AB:33:EE:A4:BA:9C:2E:F6:7E:C0:DC:E8:1C
X509v3

Authority Key Identifier:

keyid:5B:B4:06:4D:8D:12:D0:B3:36:A7:6B:
3A:FD:F2:C8:83:4A:DD:AA: BD

Certificate is to be certified until Oct 22 09:35:52 2011
GMT (365 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated

#
```

The file contains the TippingPoint Advanced Threat Protection for Email certificate signed by the CA. You need to distribute this file to all servers and clients communicating with TippingPoint Advanced Threat Protection for Email.

## Uploading Certificates

The TLS support provided by TippingPoint Advanced Threat Protection for Email uses the same set of keys for upstream and downstream directions. The CA certificate can be one of the following:

- The real CA certificate used to sign all public keys of all email relays communicating with TippingPoint Advanced Threat Protection for Email.
- Individual certificates of all email relays communicating with TippingPoint Advanced Threat Protection for Email.

---

**Procedure**

1. Go to **Administration** > **Mail Settings** > **Connections**.
2. Under **Transport Layer Security**, do the following:
   a. Select **Enable incoming TLS**.
   b. Click **Choose File** or **Browse** next to the type of certificate to upload.
   c. Click **Upload**.
3. Click **Save**.

---

# Appendix B

## Using the Command Line Interface

Topics include:


- *Using the CLI on page B-2*
- *Entering the CLI on page B-2*
- *Command Line Interface Commands on page B-3*

# Using the CLI

Use the Command Line Interface (CLI) perform the following tasks:

- Configure initial settings, such as the device IP address and host name
- Restart the device
- View device status
- Debug and troubleshoot the device

**Note**

Do not enable scroll lock on your keyboard when using HyperTerminal. If scroll lock is enabled, you cannot enter data.

# Entering the CLI

To log on to the CLI, either connect directly to the server or connect using SSH.

**Procedure**

- To connect directly to the server:
  a. Connect a monitor and keyboard to the server.
  b. Log on to the CLI.

  **Note**

  The default credentials are:

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

- If the SSH service is enabled, do the following to connect using SSH:

a. Verify the computer you are using can ping TippingPoint Advanced Threat Protection for Email's IP address.

b. Use an SSH client to connect to TippingPoint Advanced Threat Protection for Email's IP address and TCP port 22.

**Note**

The default IP address / subnet mask is `192.168.252.1` / `255.255.0.0`.

# Command Line Interface Commands

The TippingPoint Advanced Threat Protection for Email CLI commands are separated into two categories: normal and privileged commands. Normal commands are basic commands to obtain system information and to perform simple tasks. Privileged commands provide full configuration control and advanced monitoring and debugging features. Privileged commands are protected by the **`enable`** command and password.

## Entering Privileged Mode

**WARNING!**

Enter the shell environment only if your support provider instructs you to perform debugging operations.

**Procedure**

1. Log on to the CLI.

   See *Entering the CLI on page B-2*.

2. At the prompt, type `enable` and press ENTER to enter privileged mode.

3. Type the default password, `trend#1`, and then press ENTER.

The prompt changes from > to #.

## CLI Command Reference

The following tables explain the CLI commands.

**Note**

CLI commands require privileged mode. For details, see *Entering Privileged Mode on page B-3*.

### configure product management-port

**TABLE B-1. configure product management-port**

| | |
|---|---|
| Set the management port IP address | |
| **Syntax**:<br>`configure product management-port [ipv4 \| ipv6] <ip> <mask>` | |
| **View** | Privileged |
| **Parameters** | **ipv4**: Configure IPv4 settings<br>**ipv6**: Configure IPv6 settings<br>**<ip>**: IP address for the interface<br>**<mask>**: Network mask for the NIC |
| **Example**: | |
| To set the management port IPv4 address:<br>`configure product management-port ipv4 192.168.10.21 255.255.255.0` | |

### configure product operation-mode

**TABLE B-2. configure product operation-mode**

| |
|---|
| Set the TippingPoint Advanced Threat Protection for Email operation mode |

| | |
|---|---|
| **Syntax**:<br>`configure product operation-mode [BCC \| MTA \| TAP]` | |
| **View** | Privileged |
| **Parameters** | **BCC**: Deploy in BCC mode<br>**MTA**: Deploy in MTA mode<br>**TAP**: Deploy in SPAN/TAP mode |
| **Example**: | |
| To deploy in BCC mode:<br>`configure product operation-mode BCC` | |

## configure network basic

**TABLE B-3. configure network basic**

| | |
|---|---|
| Configures basic network settings, including host name, IP address, subnet mask, gateway, and DNS. | |
| **Syntax**:<br>`configure network basic` | |
| **View** | Privileged |
| **Parameters** | None |
| **Examples**: | |

```
***Network Configuration***

Specify value for each item and press ENTER. Settings apply to the
management port (Eth0) and require a restart.

Host name: mail.com

IPv4 address: 10.64.70.151

Subnet mask: 255.255.254.0

IPv4 gateway: 10.64.70.1

Preferred IPv4 DNS: 10.64.1.55

Alternate IPv4 DNS: 10.64.1.54

IPv6 address:

Prefix length:

IPv6 gateway:

Preferred IPv6 DNS:

Alternate IPv6 DNS:

Confirm changes and restart (Y/N):
```

## configure network dns

**TABLE B-4. configure network dns**

| | |
|---|---|
| Configures DNS settings for the TippingPoint Advanced Threat Protection for Email device. | |
| **Syntax**:<br>`configure network dns [ipv4 \| ipv6] <dns1> <dns2>` | |
| **View** | Privileged |

| | |
|---|---|
| **Parameters** | **ipv4**: Configure IPv4 settings<br>**ipv6**: Configure IPv6 settings<br>**<dns1>**: Primary DNS server<br>**<dns2>**: Secondary DNS server<br>**Note**<br>Use a space to separate the primary and secondary DNS value. |
| **Examples**: | |
| To configure the primary DNS with an IP address of 192.168.10.21:<br>`configure network dns ipv4 192.168.10.21` | |
| To configure the primary and secondary DNS with the following values:<br>• Primary DNS: `192.168.10.21`<br>• Secondary DNS: `192.168.10.22`<br>`configure network dns ipv4 192.168.10.21 192.168.10.22` | |

## configure network hostname

**TABLE B-5. configure network hostname**

| | |
|---|---|
| Configures the host name for the TippingPoint Advanced Threat Protection for Email device. | |
| **Syntax**:<br>`configure network hostname <hostname>` | |
| **View** | Privileged |
| **Parameters** | **<hostname>**: The host name or fully qualified domain name (FQDN) for the TippingPoint Advanced Threat Protection for Email device |
| **Examples**: | |

| |
|---|
| To change the host name of the TippingPoint Advanced Threat Protection for Email device to test.host.com:<br>`configure network hostname test.example.com` |

## configure network interface

**TABLE B-6. configure network interface**

| | |
|---|---|
| Configures the IP address for the network interface card (NIC). | |
| **Syntax**:<br>`configure network interface [ipv4 \| ipv6] <interface> <ip> <mask>` | |
| **View** | Privileged |
| **Parameters** | **ipv4**: Configure IPv4 settings<br>**ipv6**: Configure IPv6 settings<br>**<interface>**: NIC name<br>**<ip>**: IP address for the interface<br>**<mask>**: Network mask for the NIC |
| **Example**: | |
| To configure an NIC with the following values:<br>• Interface: `eth0`<br>• IPv4 address: `192.168.10.10`<br>• IPv4 subnet mask: `255.255.255.0`<br>`configure network interface ipv4 eth0 192.168.10.10 255.255.255.0` | |

## configure network route add

**TABLE B-7. configure network route add**

| |
|---|
| Adds a new route entry |

| | |
|---|---|
| **Syntax**:<br>`configure network route add [ipv4 \| ipv6] <ip_prefixlen> <via> <dev>` | |
| **View** | Privileged |
| **Parameters** | **ipv4**: Configure IPv4 settings<br>**ipv6**: Configure IPv6 settings<br>**<ip_prefixlen>**: Destination network ID with format IP_Address/Prefixlen<br>**<via>**: IP address of the next hop<br>**<dev>**: Device name |
| **Example**: | |
| To add a new route entry:<br>`configure network route add ipv4 172.10.10.0/24 192.168.10.1 eth1` | |

## configure network route default

**TABLE B-8. configure network route default**

| | |
|---|---|
| Sets the default route | |
| **Syntax**:<br>`configure network route default [ipv4 \| ipv6] <gateway>` | |
| **View** | Privileged |
| **Parameter** | **ipv4**: Configure IPv4 settings<br>**ipv6**: Configure IPv6 settings<br>**<gateway>**: IP address of default gateway |
| **Example**: | |
| To set the default route for the TippingPoint Advanced Threat Protection for Email appliance:<br>`configure network route default ipv4 192.168.10.1` | |

## configure network route del

**TABLE B-9. configure network route del**

| | |
|---|---|
| Deletes a route | |
| **Syntax**:<br>`configure network route del [ipv4 \| ipv6] <ip_prefixlen> <via> <dev>` | |
| **View** | Privileged |
| **Parameters** | **ipv4**: Configure IPv4 settings<br>**ipv6**: Configure IPv6 settings<br>**<ip_prefixlen>**: Destination network ID with format IP_Address/Prefixlen<br>**<via>**: IPv4 address of the next hop<br>**<dev>**: Device name |
| **Example**: | |
| To delete a route for the TippingPoint Advanced Threat Protection for Email appliance:<br>`configure network route del ipv4 172.10.10.0/24 192.168.10.1 eth1` | |

## configure network route del default/default ipv6

**TABLE B-10. configure network route del default/default ipv6**

| | |
|---|---|
| Deletes the default IPv6 gateway | |
| **Syntax**:<br>`configure network route del default ipv6 <gateway> <device>` | |
| **View** | Privileged |
| **Parameters** | gateway: IPv6 Address of the default gateway<br>device: Link local to IPv6 default gateway |

| |
|---|
| **Example**:<br>To delete the default IPv6 gateway fe80::20c:29ff:fe75:b579 on device eth0: `configure network route del default ipv6 fe80::20c:29ff:fe75:b579 eth0` |

## configure service ssh disable

**TABLE B-11. configure service ssh disable**

| | |
|---|---|
| Disables SSH on all network interface cards (NIC). | |
| **Syntax**:<br>`configure service ssh disable` | |
| **View** | Privileged |
| **Parameters** | None |
| **Examples**: | |
| To disable SSH on all NICs:<br>`configure service ssh disable` | |

## configure service ssh enable

**TABLE B-12. configure service ssh enable**

| | |
|---|---|
| Enables SSH on one specific network interface card (NIC). | |
| **Syntax**:<br>`configure service ssh enable` | |
| **View** | Privileged |
| **Parameters** | None |
| **Examples**: | |
| To enable SSH:<br>`configure service ssh enable` | |

## configure service ssh port

**TABLE B-13. configure service ssh port**

| | |
|---|---|
| Change SSH service port. | |
| **Syntax**:<br>`configure service ssh port <port>` | |
| **View** | Privileged |
| **Parameters** | port: configure the SSH service port<br><port>: SSH service port number |
| **Example**:<br>To change the SSH service port to 56743: `configure service ssh port 56743` | |

## configure service ntp

**TABLE B-14. configure service ntp**

| | |
|---|---|
| Synchronize the TippingPoint Advanced Threat Protection for Email system time with an NTP server. | |
| **Syntax**:<br>`configure service ntp [enable \| disable \| server-address <address>]` | |
| **View** | Privileged |
| **Parameters** | **enable**: Enable NTP<br>**disable**: Disable NTP<br>**server-address**: Configure the NTP server address<br>**<address>**: Specify the FQDN or IP address of the NTP server |
| **Examples**: | |
| To configure the NTP server address as 192.168.10.21:<br>`configure service ntp server-address 192.168.10.21` | |

| |
|---|
| To enable synchronization with the NTP server:<br>`configure service ntp enable` |

## configure system date

**TABLE B-15. configure system date**

| | |
|---|---|
| Configures the time and date and saves the data in CMOS. | |
| **Syntax**:<br>`configure system date <date> <time>` | |
| **View** | Privileged |
| **Parameters** | **<date>**: Set the date using the following format: **yyyy-mm-dd**<br>**<time>**: Set the time with the following format: **hh:mm:ss** |
| **Example**: | |
| To set the date to August 12, 2010 and the time to 3:40 PM:<br>`configure system date 2010-08-12 15:40:00` | |

## configure system password enable

**TABLE B-16. configure system password enable**

| | |
|---|---|
| To change the password required to enter Privileged mode. | |
| **Syntax**:<br>`configure system password enable` | |
| **View** | Privileged |
| **Parameters** | None |
| **Examples**: | |

| |
|---|
| To change the password required to enter Privileged mode:<br>`configure system password enable` |

## configure system timezone

**TABLE B-17. configure system timezone**

| | |
|---|---|
| Configures the time zone used by TippingPoint Advanced Threat Protection for Email. | |
| **Syntax**:<br>`configure system timezone <region> <city>` | |
| **View** | Privileged |
| **Parameters** | **<region>**: Region name<br>**<city>**: City name |
| **Example**: | |
| To configure the TippingPoint Advanced Threat Protection for Email appliance to use the time zone for the following location:<br>Region: America<br>City: New York<br>`configure system timezone America New_York` | |

**TABLE B-18. Time Zone Setting Examples**

| REGION/COUNTRY | CITY |
|---|---|
| Africa | Cairo |
| | Harare |
| | Nairobi |

| Region/Country | City |
|---|---|
| America | Anchorage |
| | Bogota |
| | Buenos_Aires |
| | Caracas |
| | Chicago |
| | Chihuahua |
| | Denver |
| | Godthab |
| | Lima |
| | Los_Angeles |
| | Mexico_City |
| | New_York |
| | Noronha |
| | Phoenix |
| | Santiago |
| | St_Johns |
| | Tegucigalpa |

| Region/Country | City |
|---|---|
| Asia | Almaty |
| | Baghdad |
| | Baku |
| | Bangkok |
| | Calcutta |
| | Colombo |
| | Dhaka |
| | Hong_Kong |
| | Irkutsk |
| | Jerusalem |
| | Kabul |
| | Karachi |
| | Katmandu |
| | Krasnoyarsk |
| | Kuala_Lumpur |
| | Kuwait |
| | Magadan |
| | Manila |
| | Muscat |
| | Rangoon |
| | Seoul |
| | Shanghai |

| Region/Country | City |
|---|---|
| Asia (Continued) | Singapore |
| | Taipei |
| | Tehran |
| | Tokyo |
| | Yakutsk |
| Atlantic | Azores |
| Australia | Adelaide |
| | Brisbane |
| | Darwin |
| | Hobart |
| | Melbourne |
| | Perth |
| Europe | Amsterdam |
| | Athens |
| | Belgrade |
| | Berlin |
| | Brussels |
| | Bucharest |
| | Dublin |
| | Moscow |
| | Paris |

| REGION/COUNTRY | CITY |
|---|---|
| Pacific | Auckland |
| | Fiji |
| | Guam |
| | Honolulu |
| | Kwajalein |
| | Midway |
| US | Alaska |
| | Arizona |
| | Central |
| | East-Indiana |
| | Eastern |
| | Hawaii |
| | Mountain |
| | Pacific |

## enable

**TABLE B-19. enable**

| | |
|---|---|
| Enters privileged mode so privileged commands can be provided. | |
| **Syntax**:<br>`enable` | |
| **View** | Normal |
| **Parameters** | None |
| **Example**: | |

| |
|---|
| To enter privileged mode:<br>`enable` |

## exit

**TABLE B-20. exit**

| | |
|---|---|
| Exits privileged mode.<br>Exits the session for those not in privileged mode. | |
| **Syntax**:<br>`exit` | |
| **View** | Normal |
| **Parameters** | None |
| **Example**: | |
| To exit privileged mode or to exit the session when not in privileged mode:<br>`exit` | |

## help

**TABLE B-21. help**

| | |
|---|---|
| Displays the CLI help information. | |
| **Syntax**:<br>`help` | |
| **View** | Normal |
| **Parameters** | None |
| **Example**: | |

| |
|---|
| To display the CLI help information:<br>`help` |

## history

**TABLE B-22. history**

| | |
|---|---|
| Displays the current session's command line history. | |
| **Syntax**:<br>`history [limit]` | |
| **View** | Normal |
| **Parameters** | **[limit]**: Specifies the size of the history list for the current session<br>Specifying "0" retains all commands for the session. |
| **Example**: | |
| To specify six commands for the size of the history list:<br>`history 6` | |

## logout

**TABLE B-23. logout**

| | |
|---|---|
| Logs out of the current CLI session. | |
| **Syntax**:<br>`logout` | |
| **View** | Normal |
| **Parameters** | None |
| **Example**: | |

| |
|---|
| To logout from the current session:<br>`logout` |

## ping

**TABLE B-24. ping**

| | |
|---|---|
| Pings a specified host. | |
| **Syntax**:<br>`ping [-c num_echos] [-i interval] <dest>` | |
| **View** | Normal |
| **Parameters** | **[-c num_echos]**: Specifies the number of echo requests to be sent. Default value is 5.<br>**[-i interval]**: Specifies the delay interval in seconds between each packet. Default value is 1 second.<br>**<dest>**: Specifies the destination host name or IP address |
| **Examples**: | |
| To ping the IP address 192.168.1.1:<br>`ping 192.168.1.1` | |
| To ping the host remote.host.com:<br>`ping remote.host.com` | |

## ping6

**TABLE B-25. ping6**

| |
|---|
| Pings a specified IPv6 host through interface eth0. |
| **Syntax**:<br>`ping6 [-c num_echos] [-i interval] <dest>` |

| | |
|---|---|
| **View** | Normal |
| **Parameters** | **[-c num_echos]**: Specifies the number of echo requests to be sent. Default value is 5.<br><br>**[-i interval]**: Specifies the delay interval in seconds between each packet. Default value is 1 second.<br><br>**<dest>**: Specifies the destination host name or IP address |
| **Examples**: | |
| To ping the IPv6 address fe80::21a:a5ff:fec1:1060:<br><br>`ping6 fe80::21a:a5ff:fec1:1060` | |
| To ping the host remote.host.com:<br><br>`ping6 remote.host.com` | |

## start task postfix drop

**TABLE B-26. start task postfix drop**

| | |
|---|---|
| Deletes a specified message or all messages in the email message queue. | |
| **Syntax**:<br><br>`start task postfix drop { <mail_id> \| all }` | |
| **View** | Privileged |
| **Parameters** | **<mail_id>**: Specifies the message ID in the postfix queue to delete |
| **Examples**: | |
| To delete email message D10D4478A5 from the email message queue:<br><br>`start task postfix drop D10D4478A5` | |
| To delete all email messages from the email message queue:<br><br>`start task postfix drop all` | |

## start task postfix flush

**TABLE B-27. start task postfix flush**

| | |
|---|---|
| Attempts to deliver all queued email messages. | |
| **Syntax**:<br>`start task postfix flush` | |
| **View** | Privileged |
| **Parameters** | None |
| **Example**: | |
| To deliver all queued email messages:<br>`start task postfix flush` | |

## start task postfix queue

**TABLE B-28. start task postfix queue**

| | |
|---|---|
| Displays all email messages queued in Postfix. | |
| **Syntax**:<br>`start task postfix queue` | |
| **View** | Privileged |
| **Parameters** | None |
| **Example**: | |
| To display all Postfix queued email messages:<br>`start task postfix queue` | |

## start service postfix

**TABLE B-29. start service postfix**

| | |
|---|---|
| Starts the Postfix mail system | |
| **Syntax**:<br>`start service postfix` | |
| **View** | Privileged |
| **Parameters** | None |
| **Example**: | |
| To start the Postfix mail system:<br>`start service postfix` | |

## start service product

**TABLE B-30. start service product**

| | |
|---|---|
| Starts the Product service system. | |
| **Syntax**:<br>`start service product` | |
| **View** | Privileged |
| **Parameters** | None |
| **Example**: | |
| To start the Product service system:<br>`start service product` | |

## start service ssh

**TABLE B-31. start service ssh**

| | |
|---|---|
| Starts the ssh service system. | |
| **Syntax**:<br>`start service ssh` | |
| **View** | Privileged |
| **Parameters** | None |
| **Example**: | |
| To start the ssh service system:<br>`start ssh service` | |

## stop process core

**TABLE B-32. stop process core**

| | |
|---|---|
| Stops a running process and generates a core file. | |
| **Syntax**:<br>`stop process core <pid>` | |
| **View** | Privileged |
| **Parameters** | **<pid>**: The process ID |
| **Example**: | |
| To stop a process with ID 33:<br>`stop process core 33` | |

## stop service postfix

**TABLE B-33. stop service postfix**

| | |
|---|---|
| Stops the Postfix mail system. | |
| **Syntax**:<br>`stop service postfix` | |
| **View** | Privileged |
| **Parameters** | None |
| **Example**: | |
| To stop the Postfix mail system:<br>`stop service postfix` | |

## stop service product

**TABLE B-34. stop service product**

| | |
|---|---|
| Stops the Product service system. | |
| **Syntax**:<br>`stop service product` | |
| **View** | Privileged |
| **Parameters** | None |
| **Example**: | |
| To stop the Product service system:<br>`stop service product` | |

## stop service ssh

**TABLE B-35. stop service ssh**

| | |
|---|---|
| Stops the ssh service system. | |
| **Syntax**:<br>`stop service ssh` | |
| **View** | Privileged |
| **Parameters** | None |
| **Example**: | |
| To stop the ssh service system:<br>`stop ssh service` | |

## reboot

**TABLE B-36. reboot**

| | |
|---|---|
| Reboots the TippingPoint Advanced Threat Protection for Email appliance immediately or after a specified delay. | |
| **Syntax**:<br>`reboot [time]` | |
| **View** | Privileged |
| **Parameters** | **[time]**: Specifies the delay, in minutes, to reboot the TippingPoint Advanced Threat Protection for Email appliance |
| **Examples**: | |
| To reboot the TippingPoint Advanced Threat Protection for Email appliance immediately:<br>`reboot` | |
| To reboot the TippingPoint Advanced Threat Protection for Email appliance after 5 minutes:<br>`reboot 5` | |

## resolve

**TABLE B-37. resolve**

| | |
|---|---|
| Resolves an IPv4 address from a host name or resolves a host name from an IPv4 address. | |
| **Syntax**:<br>`resolve <dest>` | |
| **View** | Privileged |
| **Parameter** | **<dest>**: Specifies the IPv4 address or host name to resolve |
| **Examples**: | |
| To resolve the host name from IP address 192.168.10.1:<br>`resolve 192.168.10.1` | |
| To resolve the IP address from host name parent.host.com:<br>`resolve parent.host.com` | |

## show storage statistic

**TABLE B-38. show storage statistic**

| | |
|---|---|
| Displays the file system disk space usage. | |
| **Syntax**:<br>`show storage statistic [partition]` | |
| **View** | Normal |
| **Parameters** | **[partition]**: Specify a partition. This is optional. |
| **Example**: | |
| To display the file system disk space usage of the TippingPoint Advanced Threat Protection for Email appliance:<br>`show storage statistic` | |

## show network

**TABLE B-39. show network**

| | |
|---|---|
| Displays various TippingPoint Advanced Threat Protection for Email network configurations. | |
| **Syntax**:<br>`show network [arp <address> \| connections \| dns \| dns ipv6\| hostname \| interface \| route \| route ipv4 \| route default ipv4 \| route default ipv6]` | |
| **View** | Normal |
| **Parameters** | **arp**: Displays the value returned by the Address Resolution Protocol (ARP) for the given address.<br>**<address>**: FQDN or IP address that will be resolved with the Address Resolution Protocol (ARP).<br>**connections**: Displays the current network connections of the TippingPoint Advanced Threat Protection for Email appliance.<br>**dns**: Displays the DNS IP address of the TippingPoint Advanced Threat Protection for Email appliance.<br>**dns ipv6**: Displays system DNS configuration for IPv6.<br>**hostname**: Displays the host name of the TippingPoint Advanced Threat Protection for Email appliance.<br>**interface**: Displays the network interface card (NIC) status and configuration.<br>**route**: Displays IP address route table.<br>**route ipv4**: Displays system IPv4 route table.<br>**route default ipv4**: Displays default IPv4 route table.<br>**route default ipv6**: Display default IPv6 route table. |
| **Examples**: | |
| To display the ARP information for the address 10.2.23.41:<br>`show network arp 10.2.23.41` | |

| |
|---|
| To display the current network connections of the TippingPoint Advanced Threat Protection for Email appliance:<br>`show network connections` |
| To display the DNS configuration:<br>`show network dns` |
| To display system DNS configuration for IPv6:<br>`show network dns ipv6` |
| To display the host name of the TippingPoint Advanced Threat Protection for Email appliance:<br>`show network hostname` |
| To display the NIC status and configuration:<br>`show network interface` |
| To display the IP address route table:<br>`show network route` |
| To display system IPv4 route table:<br>`show network route ipv4` |
| To display system default IPv4 gateway:<br>`show network route default ipv4` |
| To display system default IPv6 gateway:<br>`show network route default ipv6` |

## show kernel

**TABLE B-40. show kernel**

| |
|---|
| Displays the OS kernel information of the TippingPoint Advanced Threat Protection for Email appliance. |

| | |
|---|---|
| **Syntax**:<br>`show kernel {messages \| modules \| parameters \| iostat}` | |
| **View** | Normal |
| **Parameters** | **messages**: Displays kernel messages.<br>**modules**: Displays kernel modules.<br>**parameters**: Displays kernel parameters.<br>**iostat**: Displays CPU statistics and I/O statistics for devices and partitions. |
| **Examples**: | |
| To display the OS kernel's messages:<br>`show kernel messages` | |
| To display the OS kernel's modules:<br>`show kernel modules` | |
| To display the OS kernel's parameters:<br>`show kernel parameters` | |
| To display the CPU statistics and I/O statistics:<br>`show kernel iostat` | |

## show service

**TABLE B-41. show service**

| | |
|---|---|
| Displays the TippingPoint Advanced Threat Protection for Email service status. | |
| **Syntax**:<br>`show service [ntp <enabled \| server-address> \| ssh]` | |
| **View** | Normal |

| | |
|---|---|
| **Parameters** | **ntp enabled**: Displays the system NTP service status.<br>**ntp server-address**: Displays the system NTP service server address.<br>**ssh**: Displays the status of SSH. |
| **Examples**: | |
| To display the NTP service status:<br>`show service ntp` | |
| To display the SSH status:<br>`show service ssh` | |

## show memory

**TABLE B-42. show memory**

| | |
|---|---|
| Displays the system memory information. | |
| **Syntax**:<br>`show memory [vm \| statistic]` | |
| **View** | Normal |
| **Parameters** | **vm**: Displays virtual memory statistics<br>**statistic**: Displays system memory statistics |
| **Examples**: | |
| To display the virtual memory statistics:<br>`show memory vm` | |
| To display the system memory statistics:<br>`show memory statistic` | |

## show process

**TABLE B-43. showprocess**

| | |
|---|---|
| Displays the status of the processes that are currently running. | |
| **Syntax**:<br>`show process [top \| stack \| itrace \| trace] [pid]` | |
| **View** | Normal |
| **Parameters** | **top**: Displays the status of the processes that are currently running and system related processes<br>**stack**: Print a stack trace of a running process<br>**itrace**: Trace the library call<br>**trace**: Trace system calls and signals<br>**pid**: The process id number |
| **Examples**: | |
| To display the status of the processes that are currently running:<br>`show process`<br>To display the stack trace of process 1233:<br>`show process stack 1233`<br>To display the system call of process 1233:<br>`show process trace 1233`<br>To display the library call of process 1233:<br>`show process itrace 1233` | |

## show product-info

**TABLE B-44. show product-info**

| |
|---|
| Displays the product information. |

| | |
|---|---|
| **Syntax**:<br>`show product-info [management-port \| operation-mode \| service-status \| version` | |
| **View** | Normal |
| **Parameters** | **management-port**: Displays the management port's IP address and subnet mask<br>**operation-mode**: Displays the operation mode of TippingPoint Advanced Threat Protection for Email<br>**service-status**: Displays the status of services<br>**version**: Displays the product version |
| **Examples**: | |
| To display the management port's IP address and mask: `show product-info management-port`<br>To display the operation mode: `show product-info operation-mode`<br>To display the status of the service: `show-product-info service-status`<br>To display the build version of TippingPoint Advanced Threat Protection for Email: `show product-info version` | |

## show system

**TABLE B-45. show system**

| | |
|---|---|
| Displays various system settings. | |
| **Syntax**:<br>`show system [date \| timezone [continent \| city \| country]\| uptime \| version]` | |
| **View** | Normal |

| | |
|---|---|
| **Parameters** | **date**: Displays the current time and date.<br>**timezone**: Displays the timezone settings. You can optionally specify the timezone information to view:<br>• **continent**: Displays the system continent<br>• **city**: Displays the system city<br>• **country**: Displays the system country<br>**uptime**: Displays how long the TippingPoint Advanced Threat Protection for Email appliance has been running.<br>**version**: Displays version number for the TippingPoint Advanced Threat Protection for Email appliance. |

**Examples**:

To display the current time and date of the TippingPoint Advanced Threat Protection for Email appliance:

```
show system date
```

To display the timezone settings:

```
show system timezone
```

To display the continent of the TippingPoint Advanced Threat Protection for Email appliance:

```
show system timezone continent
```

To display the city of the TippingPoint Advanced Threat Protection for Email appliance: device's city:

```
show system timezone city
```

To display the country of the TippingPoint Advanced Threat Protection for Email appliance:

```
show system timezone country
```

To display how long TippingPoint Advanced Threat Protection for Email has been running:

```
show system uptime
```

| |
|---|
| To display the version number of the TippingPoint Advanced Threat Protection for Email appliance:<br>`show system version` |

## shutdown

**TABLE B-46. shutdown**

| | |
|---|---|
| Specifies shutting down the TippingPoint Advanced Threat Protection for Email appliance immediately or after a specified delay. | |
| **Syntax**:<br>`shutdown [time]` | |
| **View** | Privileged |
| **Parameters** | **[time]**: Shuts down the TippingPoint Advanced Threat Protection for Email appliance after a specified delay in minutes. |
| **Examples**: | |
| To shut down the TippingPoint Advanced Threat Protection for Email appliance immediately:<br>`shutdown` | |
| To shut down the TippingPoint Advanced Threat Protection for Email appliance after a 5 minute delay:<br>`shutdown 5` | |

## traceroute

**TABLE B-47. traceroute**

| |
|---|
| Displays the tracking route to a specified destination. |
| **Syntax**:<br>`traceroute [-h hops] <dest>` |

| | |
|---|---|
| **View** | Normal |
| **Parameters** | **[-h hops]**: Specifies the maximum number of hops to the destination. The minimum number is 6.<br><br>**<dest>**: Specifies the remote system to trace |
| **Examples**: | |
| To display the route to IP address 172.10.10.1 with a maximum of 6 hops:<br><br>`traceroute 172.10.10.1` | |
| To display the route to IP address 172.10.10.1 with a maximum of 30 hops:<br><br>`traceroute -h 30 172.10.10.1` | |

# Appendix C

## Notification Message Tokens

Add message tokens to customize email message notifications.

Topics include:


- *Recipient Notification Message Tokens on page C-2*
- *Alert Notification Message Tokens on page C-3*

# Recipient Notification Message Tokens

TippingPoint Advanced Threat Protection for Email sends recipient notifications to inform recipients that an email message contained a detected threat. After acting upon an email message, TippingPoint Advanced Threat Protection for Email sends recipient notifications based on the detected risk level. Use the following table to customize your recipient notifications with message tokens.

**Note**

For information about configuring recipient notifications, see *Configuring the Actions on page 5-2*.

**TABLE C-1. Message Tokens**

| TOKEN | DESCRIPTION | EXAMPLE |
|---|---|---|
| `%Action%` | The action that TippingPoint Advanced Threat Protection for Email took on the processed message | • Block and quarantine<br>• Strip attachments, redirect links to blocking page, and tag<br>• Strip attachments, redirect links to warning page, and tag<br>• Pass and tag<br>• Pass with no action |
| `%DateTime%` | The date and time that the alert was triggered | 2014-03-21 03:34:09 |
| `%Risk%` | The email message's risk level | • High<br>• Medium<br>• Low<br>• Unscanned Attachments |
| `%Sender%` | The sending email address | senderemail@example.com |

| Token | Description | Example |
|---|---|---|
| `%Subject%` | The subject of the email message | Your dream job! |

# Alert Notification Message Tokens

The following table explains the tokens available for alert notifications. Use the table to customize your alert notifications with message tokens.

**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 6-7*.

**Table C-2. Message Tokens**

| Token | Description | Notes |
|---|---|---|
| `%AveSandboxProc%` | The average time in minutes it takes to queue and analyze messages in the past hour | Where allowed:<br>• System: Long Virtual Analyzer Processing Time<br>Examples:<br>• 3<br>• 2 |

| Token | Description | Notes |
|---|---|---|
| `%ComponentList%` | The list of components. | Where allowed:<br>• System: Component Update/Rollback Successful<br>• System: Component Update/Rollback Unsuccessful<br>Examples:<br>• Network Content Inspection Engine/ 0x48000204/ 9.862.1107<br>• Network Content Inspection Engine/ 0x48000204/ Unknown |
| `%ConsoleURL%` | The TippingPoint Advanced Threat Protection for Email management console URL. | Where allowed:<br>• All<br>Example:<br>• https://192.168.252.1/ loginPage.ddei |
| `%CPUThreshold%` | The maximum CPU usage as a percentage allowed before TippingPoint Advanced Threat Protection for Email sends an alert notification | Where allowed:<br>• System: High CPU Usage<br>Examples:<br>• 95<br>• 85 |
| `%CPUUsage%` | The total CPU utilization as a percentage | Where allowed:<br>• System: High CPU Usage<br>Examples:<br>• 80<br>• 65 |

| Token | Description | Notes |
|---|---|---|
| `%DateTime%` | The date and time that the TippingPoint Advanced Threat Protection for Email received the email message | Where allowed:<br>• All<br>Examples:<br>• 2014-03-21 03:34:09<br>• 2014-06-15 11:31:22 |
| `%DaysBeforeExpiration%` | The number of days before the product license expires | Where allowed:<br>• System: License Expiration<br>Examples:<br>• 4<br>• 123 |
| `%DeliveryQueue%` | The number of email messages in the delivery queue waiting for TippingPoint Advanced Threat Protection for Email to process. | Where allowed:<br>• System: Long Message Delivery Queue<br>Examples:<br>• 100<br>• 600 |
| `%DetectionCount%` | The number of messages detected with suspicious characteristics during the specified period of time | Where allowed:<br>• System: Detection Surge<br>Examples:<br>• 50<br>• 200 |

| Token | Description | Notes |
|---|---|---|
| `%DetectionThreshold%` | The maximum number of messages detected to have suspicious characteristics before TippingPoint Advanced Threat Protection for Email sends an alert notification | Where allowed:<br>• System: Detection Surge<br>Examples:<br>• 50<br>• 40 |
| `%DeviceIP%` | The IP address of the TippingPoint Advanced Threat Protection for Email appliance | Where allowed:<br>• All<br>Example:<br>• 123.123.123.123 |
| `%DeviceName%` | The host name of the TippingPoint Advanced Threat Protection for Email appliance | Where allowed:<br>• All<br>Example:<br>• example.com |
| `%DiskSpace%` | The lowest amount of disk space in GB before TippingPoint Advanced Threat Protection for Email send an alert notification | Where allowed:<br>• System: Low Free Disk Space<br>• System: Low Free Quarantine Disk Space<br>Examples:<br>• 2<br>• 30 |
| `%ExpirationDate%` | The date that the product license expires | Where allowed:<br>• System: License Expiration<br>Examples:<br>• 2014-03-21 03:34:09<br>• 2014-06-15 11:31:22 |

| Token | Description | Notes |
|---|---|---|
| `%Interval%` | The frequency that TippingPoint Advanced Threat Protection for Email checks the message processing volume in minutes | Where allowed:<br>• System: Detection Surge<br>• System: Processing Surge<br>Examples:<br>• 15<br>• 10 |
| `%LicenseStatus%` | The current status of the product license | Where allowed:<br>• System: License Expiration<br>Examples:<br>• Evaluation<br>• Not Activated<br>• Activated<br>• Expired<br>• Grace Period<br>For details, see *Product License Status on page 9-3*. |
| `%LicenseType%` | The product license type | Where allowed:<br>• System: License Expiration<br>Examples:<br>• Full<br>• Trial |
| `%MemoryThreshold%` | The maximum memory usage as a percentage allowed before TippingPoint Advanced Threat Protection for Email sends an alert notification. | Where allowed:<br>• System: High Memory Usage<br>Example: 90 |

| Token | Description | Notes |
|---|---|---|
| `%MemoryUsage%` | The total memory utilization as a percentage. | Where allowed:<br>• System: High Memory Usage<br>Example: 90 |

| Token | Description | Notes |
|---|---|---|
| %MessageList% | The list of detected messages, which includes the risk level, threat type, action taken, message ID, recipients, sender, recipient, subject, top three most risky attachment details, and when the message was received. | Where allowed:<br>• Security: Suspicious Message Identified<br>• Security: Watchlisted Recipients at Risk<br>• System: Quarantined Messages<br>• System: Email Messages Timed Out Without Analysis Results<br>• System: Relay MTAs Inaccessible<br>Examples:<br>• `==========`<br>`Risk: High (potentially malicious file)`<br>`Message ID: 20140610002704.EE9A5E0236@example.com`<br>`Recipients: john@example.com`<br>`Sender: louie@example.com`<br>`Subject: The latest report`<br>`Attachments: filename.pdf (PDF), anotherattachment.doc (Word), hello.exe (EXE)`<br>`Received: 2014-05-21 11:52:32`<br>• `==========`<br>`Risk: Medium (potentially malicious URL)`<br>`Message ID: 20140610002721.EE9A5E0236@example.com`<br>`Recipients: suzysmith@example.com, johnnycash@gmail.com, peterpaul@examplecom`<br>`Sender: johndoe@example.com`<br>`Subject: Bad story to report about the differences in world eating habits`<br>`Attachments: (Link only)`<br>`Received: 2014-05-21 11:48:32` |

| Token | Description | Notes |
|---|---|---|
| `%MTAList%` | The list of unreachable MTAs. Each MTA appears as an IP address and the port number. | Where allowed:<br>• System: Relay MTAs Inaccessible<br>Examples:<br>• [1.1.1.1]:99<br>• [7.7.7.7]:77 |
| `%ProcessingCount%` | The total number of processed messages over the specified period of time | Where allowed:<br>• System: Processing Surge<br>Examples:<br>• 50<br>• 200 |
| `%ProcessingThreshold%` | The maximum number of processed messages during the specified time frame before TippingPoint Advanced Threat Protection for Email sends an alert notification | Where allowed:<br>• System: Processing Surge<br>Examples:<br>• 100<br>• 40 |
| `%QueueThreshold%` | The maximum number of messages in the delivery queue before TippingPoint Advanced Threat Protection for Email sends an alert notification | Where allowed:<br>• System: Long Message Delivery Queue<br>Examples:<br>• 100<br>• 40 |

| Token | Description | Notes |
|---|---|---|
| `%SandboxProcThreshold%` | The maximum amount of time allocated for average sandbox processing before TippingPoint Advanced Threat Protection for Email sends an alert notification | Where allowed:<br>• System: Long Virtual Analyzer Processing Time<br>Examples:<br>• 15<br>• 30 |
| `%SandboxQueue%` | The email message count in the sandbox queue waiting to be analyzed by Virtual Analyzer | Where allowed:<br>• System: Long Virtual Analyzer Queue<br>Examples:<br>• 30<br>• 75 |
| `%SandboxQueueThreshold%` | The maximum number of messages in the sandbox queue before TippingPoint Advanced Threat Protection for Email sends an alert notification | Where allowed:<br>• System: Long Virtual Analyzer Queue<br>Examples:<br>• 100<br>• 75 |
| `%ServiceName%` | The stopped TippingPoint Advanced Threat Protection for Email service<br>Where allowed:<br>• System: Service Stopped | Where allowed:<br>• System: Service Stopped<br>Example:<br>• scanner |

# Appendix D

## Connections and Ports

# Service Addresses and Ports

TippingPoint Advanced Threat Protection for Email 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 D-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. | `http://atpe26-p.activeupdate.trendmicro.com:80/activeupdate` |
| Certified Safe Software Service (CSSS) | Verifies the safety of files. Certified Safe Software Service reduces false positives, and saves computing time and resources. | `https://grid-global.trendmicro.com:443/ws/level-0/files` |
| 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. | `atpe260-en.census.trendmicro.com:80` |
| Customer Licensing Portal | Manages your customer information, subscriptions, and product or service license. | `licenseupdate.trendmicro.com:80`<br>`clp.trendmicro.com:443` |

| Service | Description | Address and Port |
|---|---|---|
| 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. | `atpe260-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. | `atpe26-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. | `atpe2-6-en.url.trendmicro.com:80`<br>`atpe2-6-en-wis.trendmicro.com:443` |

# Ports Used by the Appliance

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

**TABLE D-2. Ports used by TippingPoint Advanced Threat Protection for Email**

| PORT | PROTOCOL | FUNCTION | PURPOSE |
|---|---|---|---|
| 22 | TCP | Listening | Endpoints connect to ATP Email through SSH. |
| 25 | TCP | Listening | MTAs and mail servers connect to ATP Email through SMTP. |
| 53 | TCP/UDP | Outbound | ATP Email uses this port for DNS resolution. |
| 80 | TCP | Listening and outbound | ATP Email connects to other computers and integrated Trend Micro products and hosted services through this port.<br>• Connect to the Customer Licensing Portal to manage the product license<br>• Connect to Community File Reputation services when analyzing file samples<br>• Connect to the Smart Protection Network and query Web Reputation Services<br>• Upload virtual analyzer images to ATP Email using the image import tool |
| 123 | UDP | Outbound | ATP Email connects to the NTP server to synchronize time. |
| 161 | TCP | Listening | ATP Email uses this port to listen for requests from SNMP managers. |
| 162 | TCP | Outbound | ATP Email connects to SNMP mangers to send SNMP trap messages. |

| Port | Protocol | Function | Purpose |
|---|---|---|---|
| 443 | TCP | Listening and outbound | TippingPoint Advanced Threat Protection for Email uses this port to:<br>• Access the management console with a computer through HTTPS<br>• Communicate with Trend Micro Control Manager<br>• Connect to the Smart Protection Network and query Web Reputation Services<br>• Connect to Trend Micro Threat Connect<br>• Send anonymous threat information to Smart Feedback<br>• Update components by connecting to the ActiveUpdate server<br>• Send product usage information to Trend Micro feedback servers<br>• Verify the safety of files through the Certified Safe Software Service<br>• Communicate with Deep Discovery Director<br>• Share threat intelligence information and exception list with other products |
| 636 | TCP | Outbound | ATP Email uses this port as the default port to connect to the Microsoft Active Directory server for third-party authentication. |

| Port | Protocol | Function | Purpose |
|---|---|---|---|
| 3269 | TCP | Outbound | ATP Email uses this port as the default port to connect to the Microsoft Active Directory server for LDAP query using Global Catalog. |
| 5274 | TCP | Outbound | ATP Email uses this port as the default port to connect to the Smart Protection Server for web reputation services. |
| User-defined | N/A | Outbound | ATP Email uses specified ports to:<br>• Send logs to syslog servers<br>• Share threat intelligence with integrated products/services<br>• Upload detection logs to SFTP servers<br>• Communicate with Check Point Open Platform for Security (OPSEC) |

# Appendix E

## SNMP Object Identifiers

Topics include:


- *SNMP Query Objects on page E-2*
- *SNMP Traps on page E-18*
- *Registration Objects on page E-27*

# SNMP Query Objects

**Table E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-18. dskAvail**

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

**TABLE E-19. dskUsed**

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

**TABLE E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-42. ssRawInterrupts**

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

**Table E-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 E-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 E-45. ssRawSwapIn**

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

**Table E-46. ssRawSwapOut**

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

**TABLE E-47. productVersion**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.1.1 |
| **Object name** | productVersion |
| **Description** | Returns the TippingPoint Advanced Threat Protection for Email version. |

**TABLE E-48. productBuild**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.1.2 |
| **Object name** | productBuild |
| **Description** | Returns the TippingPoint Advanced Threat Protection for Email build number. |

**TABLE E-49. productHotfix**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.1.3 |
| **Object name** | productHotfix |
| **Description** | Returns the TippingPoint Advanced Threat Protection for Email hotfix number. |

**TABLE E-50. patternIndex**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.2.1.1 |
| **Object name** | patternIndex |
| **Description** | Returns the pattern index. |

**TABLE E-51. patternID**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.2.1.2 |
| **Object name** | patternID |
| **Description** | Returns the pattern ID. |

**TABLE E-52. patternName**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.2.1.3 |
| **Object name** | patternName |
| **Description** | Returns the pattern name. |

**TABLE E-53. patternVersion**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.2.1.4 |
| **Object name** | patternVersion |
| **Description** | Returns the pattern version. |

**TABLE E-54. deliveryQueue**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.3.1 |
| **Object name** | deliveryQueue |
| **Description** | Returns the delivery queue number. |

**TABLE E-55. virtualAnalyzerQueue**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.3.2 |

| Item | Description |
|---|---|
| **Object name** | virtualAnalyzerQueue |
| **Description** | Returns the Virtual Analyzer queue number. |

**Table E-56. ifIndex**

| Item | Description |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.4.1.1 |
| **Object name** | ifIndex |
| **Description** | Returns the interface index. |

**Table E-57. ifDescr**

| Item | Description |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.4.1.2 |
| **Object name** | ifDescr |
| **Description** | Returns the interface description. |

**Table E-58. ifReceiveThroughput**

| Item | Description |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.4.1.3 |
| **Object name** | ifReceiveThroughput |
| **Description** | Returns the interface receiving throughput. |

**Table E-59. ifTransmitThroughput**

| Item | Description |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.4.1.4 |
| **Object name** | ifTransmitThroughput |
| **Description** | Returns the interface transmitting throughput. |

# SNMP Traps

**TABLE E-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 E-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 E-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 E-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 E-64. vaStoppedNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.1 |
| **Object name** | vaStoppedNotification |
| **Description** | Notification to indicate that Virtual Analyzer is not available. |

**TABLE E-65. serviceStoppedNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.2 |
| **Object name** | serviceStoppedNotification |
| **Description** | Notification to indicate that a service has stopped and cannot be restarted. |

**TABLE E-66. unreachableMTANotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.3 |
| **Object name** | unreachableMTANotification |
| **Description** | Notification to indicate that relay MTAs for a domain cannot be reached. |

**TABLE E-67. suspiciousMsgNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.4 |
| **Object name** | suspiciousMsgNotification |
| **Description** | Notification to indicate that one or more email messages are detected with threats. |

**TABLE E-68. watchlistNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.5 |
| **Object name** | watchlistNotification |
| **Description** | Notification to indicate that one or more email messages detected with threats are sent to watchlist recipients. |

**TABLE E-69. deliveryQueueNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.6 |
| **Object name** | deliveryQueueNotification |
| **Description** | Notification to indicate that the number of email messages on the delivery queue has reached the maximum threshold. |

**TABLE E-70. cpuUsageNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.7 |
| **Object name** | cpuUsageNotification |
| **Description** | Notification to indicate that the CPU usage level has reached the maximum threshold. |

**TABLE E-71. vaQueueNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.8 |
| **Object name** | vaQueueNotification |
| **Description** | Notification to indicate that the number of email messages on the Virtual Analyzer queue has reached the maximum threshold. |

**TABLE E-72. vaProcessTimeNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.9 |
| **Object name** | vaProcessTimeNotification |
| **Description** | Notification to indicate that the average Virtual Analyzer processing time is greater than the maximum threshold. |

**TABLE E-73. diskSpaceNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.10 |
| **Object name** | diskSpaceNotification |
| **Description** | Notification to indicate that the available disk space is less than the minimum threshold. |

**TABLE E-74. updateFailedNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.11 |
| **Object name** | updateFailedNotification |
| **Description** | Notification to indicate that a component update was unsuccessful. |

**TABLE E-75. updateSuccessNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.12 |
| **Object name** | updateSuccessNotification |
| **Description** | Notification to indicate that a component update was successful. |

**TABLE E-76. ntpFailedNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.13 |
| **Object name** | ntpFailedNotification |
| **Description** | Notification to indicate that time synchronization with an NTP server is not successful. |

**TABLE E-77. vaProcessTimeoutNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.14 |
| **Object name** | vaProcessTimeoutNotification |
| **Description** | Notification to indicate that an analysis process has timed out with no analysis result. |

**TABLE E-78. quarantineDiskSpaceNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.15 |
| **Object name** | quarantineDiskSpaceNotification |
| **Description** | Notification to indicate that the available disk space for quarantined files has reached the minimum threshold. |

**TABLE E-79. msgQuarantinedNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.0.16 |
| **Object name** | msgQuarantinedNotification |
| **Description** | Notification to indicate that one or more email messages are quarantined. |

**TABLE E-80. memUsageNotification**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | 1.3.6.1.4.1.6101.3004.5.0.17 |
| **Object name** | memUsageNotification |
| **Description** | Notification to indicate that the memory usage level has reached the maximum threshold. |

**TABLE E-81. vaStoppedMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.1 |
| **Object name** | vaStoppedMsg |
| **Description** | Message to indicate that Virtual Analyzer is not available. |

**TABLE E-82. serviceStoppedMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.2 |
| **Object name** | serviceStoppedMsg |
| **Description** | Message to indicate that a service has stopped and cannot be restarted. |

**TABLE E-83. unreachableMTAMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.3 |
| **Object name** | unreachableMTAMsg |
| **Description** | Message to indicate that relay MTAs for a domain cannot be reached. |

**TABLE E-84. suspiciousMsgMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.4 |
| **Object name** | suspiciousMsgMsg |
| **Description** | Message to indicate that one or more email messages are detected with threats. |

**TABLE E-85. watchlistMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.5 |
| **Object name** | watchlistMsg |
| **Description** | Message to indicate that one or more email messages detected with threats are sent to watchlist recipients. |

**TABLE E-86. deliveryQueueMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.6 |
| **Object name** | deliveryQueueMsg |
| **Description** | Message to indicate that the number of email messages on the delivery queue has reached the maximum threshold. |

**TABLE E-87. cpuUsageMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.7 |
| **Object name** | cpuUsageMsg |
| **Description** | Message to indicate that the CPU usage level has reached the maximum threshold. |

**TABLE E-88. vaQueueMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.8 |
| **Object name** | vaQueueMsg |
| **Description** | Message to indicate that the number of email messages on the Virtual Analyzer queue has reached the maximum threshold. |

**TABLE E-89. vaProcessTimeMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.9 |
| **Object name** | vaProcessTimeMsg |
| **Description** | Message to indicate that the average Virtual Analyzer processing time is greater than the maximum threshold. |

**TABLE E-90. diskSpaceMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.10 |
| **Object name** | diskSpaceMsg |
| **Description** | Message to indicate that the available disk space is less than the minimum threshold. |

**TABLE E-91. updateFailedMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.11 |
| **Object name** | updateFailedMsg |
| **Description** | Message to indicate that a component update was unsuccessful. |

**TABLE E-92. updateSuccessMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.12 |
| **Object name** | updateSuccessMsg |
| **Description** | Message to indicate that a component update was successful. |

**TABLE E-93. ntpFailedMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.13 |
| **Object name** | ntpFailedMsg |
| **Description** | Message to indicate that time synchronization with an NTP server is not successful. |

**TABLE E-94. vaProcessTimeoutMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.14 |
| **Object name** | vaProcessTimeoutMsg |
| **Description** | Message to indicate that an analysis process has timed out with no analysis result. |

**TABLE E-95. quarantineDiskSpaceMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.15 |
| **Object name** | quarantineDiskSpaceMsg |
| **Description** | Message to indicate that the available disk space for quarantined files has reached the minimum threshold. |

**TABLE E-96. msgQuarantinedMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.16 |
| **Object name** | msgQuarantinedMsg |
| **Description** | Message to indicate that one or more email messages are quarantined. |

**TABLE E-97. memUsageMsg**

| ITEM | DESCRIPTION |
|---|---|
| **OID** | .1.3.6.1.4.1.6101.3004.5.1.17 |
| **Object name** | memUsageMsg |
| **Description** | Message to indicate that the memory usage level has reached the maximum 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 |

| OID | Description |
|---|---|
| .1.3.6.1.4.1.8072 | NET-SNMP-AGENT-MIB |
| .1.3.6.1.4.1.6101.999 | TMCM |
| .1.3.6.1.4.1.6101.3001 | TMTM |
| .1.3.6.1.4.1.6101.3004 | TippingPoint Advanced Threat Protection for Email |

# Appendix F

## IPv6 Support in TippingPoint Advanced Threat Protection for Email

This appendix is required reading for users who plan to deploy TippingPoint Advanced Threat Protection for Email in an environment that supports IPv6 addressing. This appendix contains information on the extent of IPv6 support in TippingPoint Advanced Threat Protection for Email.

TippingPoint Advanced Threat Protection for Email assumes that the reader is familiar with IPv6 concepts and the tasks involved in setting up a network that supports IPv6 addressing.

IPv6 support for TippingPoint Advanced Threat Protection for Email started in version 2.1. Earlier TippingPoint Advanced Threat Protection for Email versions do not support IPv6 addressing. IPv6 support is automatically enabled after installing or upgrading TippingPoint Advanced Threat Protection for Email.

The following TippingPoint Advanced Threat Protection for Email features support IPv6:

- Email message processing (receiving and delivering)
- Management console and CLI access
- Notification SMTP
- SPAN/TAP mode

- Syslog server

# Configuring IPv6 Addresses

The CLI and management console allow you to configure an IPv6 address. The following are some configuration guidelines.

- TippingPoint Advanced Threat Protection for Email accepts standard IPv6 address presentations.

  For example:

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

  `2001:db7:85a3::8a2e:370:7334`

  `::ffff:192.0.2.128`

  **Note**

  TippingPoint Advanced Threat Protection for Email does not accept link-local IPv6 addresses.

- When the IPv6 address is part of a URL, enclose the address in square brackets ([]).

# Configurable IPv6 Addresses

IPv6 addresses are configurable on the management console and CLI.

## Management Console IPv6 Addresses

IPv6 addresses are configurable on the following management console screens:

- **Administration** > **System Settings** > **Network**
- **Administration** > **System Settings** > **SMTP**
- **Administration** > **Mail Settings** > **Connections**

- **Administration** > **Mail Settings** > **Message Delivery**
- **Administration** > **Mail Settings** > **Limits and Exceptions**
- **Administration** > **Integrated Products/Services** > **Log Settings**
- **Administration** > **System Settings** > **Operation Mode** (SPAN/TAP mode rules)

## CLI IPv6 Addresses

IPv6 addresses are configurable using the following CLI commands:

- *configure product management-port on page B-4*
- *configure network basic on page B-5*
- *configure network dns on page B-6*
- *configure network interface on page B-8*
- *configure network route add on page B-8*
- *configure network route default on page B-9*
- *configure network route del on page B-10*

# Appendix G

## System Event Logs

The following table lists the system event logs in TippingPoint Advanced Threat Protection for Email.

**TABLE G-1. System event logs**

| ID | LOG TYPE | MESSAGE |
|---|---|---|
| 11001 | Update events | Product Updates: {USER} installed hot fix {VERSION} from {IP} |
| 11002 | Update events | Product Updates: {USER} rolled back hot fix {VERSION} from {IP} |
| 11003 | Update events | Product Updates: Appliance firmware upgraded by {USER} from {IP} |
| 12001 | Update events | Deep Discovery Director: Hotfix update successful |
| 12002 | Update events | Deep Discovery Director: Firmware update successful |
| 12003 | Update events | Deep Discovery Director: Virtual Analyzer image import successful |
| 12004 | Update events | Deep Discovery Director: Configuration update successful |

| ID | Log Type | Message |
|---|---|---|
| 130xx | Update events | ActiveUpdate: {COMPONENT} downloaded manually by {USER} from {IP} |
| 131xx | Update events | ActiveUpdate: {COMPONENT} unsuccessfully downloaded manually by {USER} from {IP} |
| 132xx | Update events | ActiveUpdate: {COMPONENT} downloaded by scheduled update |
| 133xx | Update events | ActiveUpdate: {COMPONENT} unsuccessfully downloaded by scheduled update |
| 134xx | Update events | ActiveUpdate: {COMPONENT} rolled back to version {VERSION} by {USER} from {IP} |
| 135xx | Update events | ActiveUpdate: {COMPONENT} unsuccessfully rolled back by {USER} from {IP} |
| 136xx | Update events | ActiveUpdate Exception - Apply {COMPONENT} {VERSION} to local scanner failed |
| 20101 | Audit log | System started |
| 20102 | Audit log | System stopped |
| 20201 | Audit log | Service started |
| 20202 | Audit log | Service stopped |
| 20301 | Audit log | License: Product license expired, grace period ends on {DATE} |
| 20302 | Audit log | License: Product license expired |
| 20303 | Audit log | License: Product license updated |
| 30101 | Audit log | Active update source setting was changed |
| 30102 | Audit log | Active update schecule setting was changed |
| 30201 | Audit log | System Settings: Host name saved as {NAME} by {USER} from {IP} |

| ID | Log Type | Message |
|---|---|---|
| 30202 | Audit log | System Settings: {INTERFACE} IPv4 address and subnet mask were saved as {SUBNET} by {USER} from {IP} |
| 30203 | Audit log | System Settings: {INTERFACE} IPv6 address and prefix length were saved as {IP}/{LENGTH} by {USER} from {IP} |
| 30204 | Audit log | System Settings: {INTERFACE} IPv4 gateway saved as {GATEWAY} by {USER} from {IP} |
| 30205 | Audit log | System Settings: {INTERFACE} IPv6 gateway saved as {GATEWAY} by {USER} from {IP} |
| 30206 | Audit log | System Settings: {INTERFACE} primary IPv4 DNS server saved as {IP} and secondary IPv4 DNS server saved as {IP} by {USER} from {IP} |
| 30207 | Audit log | System Settings: {INTERFACE} primary IPv6 DNS server saved as {IP} and secondary IPv6 DNS server saved as {IP} by {USER} from {IP} |
| 30301 | Audit log | System Settings: Operation mode saved as {MODE} by {USER} from {IP} |
| 30401 | Audit log | System Settings: Proxy settings modified by {USER} from {IP} |
| 30402 | Audit log | System Settings: Proxy settings unsuccessfully modified by {USER} from {IP} |
| 30501 | Audit log | System Settings: SMTP server settings modified by {USER} from {IP} |
| 30601 | Audit log | System Settings: System time zone saved as {ZONE} by {USER} from {IP} |
| 30602 | Audit log | System Settings: NTP server synchronization enabled by {USER} from {IP} |
| 30603 | Audit log | System Settings: NTP server synchronization disabled by {USER} from {IP} |
| 30604 | Audit log | System Settings: System time saved as {TIME} by {USER} from {IP} |

| ID | Log Type | Message |
|---|---|---|
| 30605 | Audit log | System Settings: Database time zone saved as {ZONE} by {USER} from {IP} |
| 30606 | Audit log | System Settings: NTP server saved as {NAME} by {USER} from {IP} |
| 30701 | Audit log | System Settings: SNMP settings modified by {USER} from {IP} |
| 30702 | Audit log | System Settings: SNMP MIB files downloaded by {USER} from {IP} |
| 30801 | Audit log | Mail Settings: SMTP Connection setting saved by {USER} from {IP} |
| 30802 | Audit log | Mail Settings: TLS certificate uploaded by {USER} from {IP} |
| 30803 | Audit log | Mail Settings: TLS certificate downloaded by {USER} from {IP} |
| 30901 | Audit log | Mail Settings: Delivery profiles exported by {USER} from {IP} |
| 30902 | Audit log | Mail Settings: Delivery profiles unsuccessfully exported by {USER} from {IP} |
| 30903 | Audit log | Mail Settings: Delivery profiles imported by {USER} from {IP} |
| 30904 | Audit log | Mail Settings: Delivery profiles unsuccessfully imported since total exceeds 256 |
| 30905 | Audit log | Mail Settings: Delivery profiles unsuccessfully imported by {USER} from {IP} |
| 30906 | Audit log | Mail Settings: Delivery profile added by {USER} from {IP} |
| 30907 | Audit log | Mail Settings: Delivery profile modified by {USER} from {IP} |
| 30908 | Audit log | Mail Settings: Delivery profile deleted by {USER} from {IP} |
| 31001 | Audit log | Mail Settings: Mail settings modified by {USER} from {IP} |

| ID | Log Type | Message |
|---|---|---|
| 31101 | Audit log | Mail Settings: SMTP server greeting saved by {USER} from {IP} |
| 31201 | Audit log | Log Settings: {NAME} syslog server profile created by {USER} from {IP} |
| 31202 | Audit log | Log Settings: {NAME} syslog server profile deleted by {USER} from {IP} |
| 31203 | Audit log | Log Settings: {NAME} syslog server profile modified by {USER} from {IP} |
| 31204 | Audit log | Log Settings: {NAME} enabled by {USER} from {IP} |
| 31205 | Audit log | Log Settings: {NAME} disabled by {USER} from {IP} |
| 31301 | Audit log | Integrated Products/Services: SFTP Upload settings modified by {USER} from {IP} |
| 31401 | Audit log | Integrated Products/Services: Microsoft Active Directory Integration settings modified by {USER} from {IP} |
| 31501 | Audit log | Integrated Products/Services: Threat Intelligent Sharing settings modified by {USER} from {IP} |
| 31502 | Audit log | Integrated Products/Services: {USER} generate suspicious objects list from {IP} |
| 31601 | Audit log | Integrated Products/Services:Auxiliary Products/Services settings modified by {USER} from {IP} |
| 31602 | Audit log | Integrated Products/Services: {USER} clicked Auxiliary Products/Services > Distribute Now from {IP} |
| 31701 | Audit log | Systems Settings: Control Manager settings modified by {USER} from {IP} |
| 31702 | Audit log | System Settings: Suspicious object synchronization enabled by {USER} from {IP} |
| 31703 | Audit log | System Settings: Suspicious object synchronization disabled by {USER} from {IP} |

| ID | Log Type | Message |
|---|---|---|
| 31801 | Audit log | System Settings: Proxy settings for Deep Discovery Director modified by {USER} by {IP} |
| 31802 | Audit log | System Settings: Registered to Deep Discovery Director by {USER} from {IP} |
| 31803 | Audit log | System Settings: Unregistered from Deep Discovery Director by {USER} from {IP} |
| 31804 | Audit log | System Settings: Deep Discovery Director fingerprint trusted by {USER} from {IP} |
| 31901 | Audit log | Scanning / Analysis: Image imported by {USER} from {IP} |
| 31902 | Audit log | Scanning / Analysis: Image deleted by {USER} from {IP} |
| 31903 | Audit log | Scanning / Analysis: Number of instances for each Virtual Analyzer image modified by {USER} from {IP} |
| 32001 | Audit log | Scanning / Analysis: Virtual Analyzer settings modified by {USER} from {IP} |
| 32101 | Audit log | Scanning / Analysis: {PRODUCT NAME} registered to the external Virtual Analyzer |
| 32102 | Audit log | Scanning / Analysis: Unable to register to the external Virtual Analyzer |
| 32103 | Audit log | Scanning / Analysis: {PRODUCT NAME} unregistered from the external Virtual Analyzer |
| 32104 | Audit log | Scanning / Analysis: Virtual Analyzer external integration settings modified by {USER} from "%s" |
| 32201 | Audit log | Scanning / Analysis: File Passwords setting was modified by {USER} from {IP} |
| 32301 | Audit log | Scanning / Analysis: Smart Protection settings modified by {USER} from {IP} |
| 32401 | Audit log | Scanning / Analysis: Smart Feedback settings modified by {USER} from {IP} |
| 32501 | Audit log | YARA Rules: {USER} added rule {NAME} from {IP} |

| ID | Log Type | Message |
|---|---|---|
| 32502 | Audit log | YARA Rules: {USER} modified rule {NAME} from {IP} |
| 32503 | Audit log | YARA Rules: {USER} deleted rule {NAME} from {IP} |
| 32504 | Audit log | YARA Rules: {USER} modified status for rule {NAME} from {IP} |
| 32601 | Audit log | System Maintenance: Configuration imported by {USER} from {IP} |
| 32602 | Audit log | System Maintenance: Configuration unsuccessfully imported by {USER} from {IP} |
| 32603 | Audit log | System Maintenance: Configuration exported by {USER} from {IP} |
| 32604 | Audit log | System Maintenance: Configuration unsuccessfully exported by {USER} from {IP} |
| 32701 | Audit log | System Maintenance: Data purge started automatically |
| 32702 | Audit log | System Maintenance: Data purge completed ({MIN} min {SEC} s) |
| 32703 | Audit log | System Maintenance: Storage maintenance setting modified by {USER} from {IP} |
| 32801 | Audit log | System Maintenance: System log level setting modified by {USER} from {IP} |
| 32901 | Audit log | Accounts / Contacts: {USER} created the account {NAME} from {IP} |
| 32902 | Audit log | Accounts / Contacts: {USER} deleted the account {NAME} from {IP} |
| 32903 | Audit log | Accounts / Contacts: {USER} modified the account {NAME} from {IP} |
| 33001 | Audit log | Logon: {USER} logged on as {ROLE} role from {IP} |
| 33002 | Audit log | Logon: {USER} logged off from {IP} |

| ID | Log Type | Message |
|---|---|---|
| 33003 | Audit log | Logon: Attempted log on with an invalid user name ({USER}) or password from {IP} |
| 33004 | Audit log | Logon: Attempted log on with a disabled user name ({USER}) from {IP} |
| 33101 | Audit log | Accounts / Contacts: Contacts for alert notifications and reports modified by {USER} from {IP} |
| 33201 | Audit log | Accounts / Contacts: {USER} modified the password for {NAME} from {IP} |
| 33301 | Audit log | License: Product registered by {USER} from {IP} |
| 33302 | Audit log | License: Unsuccessful registration using an invalid Activation Code by {USER} from {IP} |
| 33401 | Audit log | Policy: Policy setting changed by {USER} from {IP} |
| 33501 | Audit log | Policy: Policy exception settings modified by {USER} from {IP} |
| 33601 | Audit log | Alerts: Alert rule settings modified by {USER} from {IP} |
| 33701 | Audit log | Report: Report settings changed by {USER} from {IP} |
| 33801 | Audit log | Detected Messages: Message {NAME} downloaded by {USER} from {IP} |
| 33802 | Audit log | Detected Messages: Investigation package {NAME} downloaded by {USER} from {IP} |
| 33901 | Audit log | Quarantine: MsgID {ID} released by {USER} from {IP} |
| 33902 | Audit log | Quarantine: MsgID {ID} deleted by {USER} from {IP} |
| 34001 | Audit log | Unable to distribute suspicious objects to Check Point OPSEC. Verify that the Check Point OPSEC settings are correct and that no network problem exists. |
| 34002 | Audit log | Unable to distribute suspicious objects to Trend Micro TippingPoint SMS. Verify that the Trend Micro TippingPoint SMS settings are correct and that no network problem exists. |

| ID | Log Type | Message |
|---|---|---|
| 34003 | Audit log | Unable to distribute suspicious objects to IBM Security Network Protection XGS. Verify that the IBM Security Network Protection XGS settings are correct and that no network problem exists. |
| 34004 | Audit log | Unable to distribute suspicious objects to Palo Alto Panorama or Firewalls. Verify that the Palo Alto Panorama or Firewalls settings are correct and that no network problem exists. |
| 34005 | Audit log | Unable to generate suspicious objects list. Verify that the Threat Intelligence Sharing settings are correct. |

# Appendix H

## Glossary

| Term | Definition |
|---|---|
| ActiveUpdate Server | Provides updates for product components, including pattern files. Trend Micro regularly releases component updates through the Trend Micro ActiveUpdate server. |
| Advanced Threat Scan Engine<br><br>Advanced Threat Scan Engine (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. |
| Affected Recipient | A recipient of malicious or suspicious email messages. |

| TERM | DEFINITION |
|---|---|
| Alert | An occurrence of an event or set of events triggering a predefined condition.<br>Alerts have the following levels of importance:<br>• Critical Alert<br>A message about an event that requires immediate attention.<br>• Important Alert<br>A message about an event that does not require immediate attention, but should be observed.<br>• Informational Alert<br>A message about an event that is most likely benign. |
| Archive | A file composed of one or more files that have been concatenated, compressed, or encrypted for portability or storage.<br>An “archive” may also be called a “compressed file”. |
| Archive file password | A password to decrypt an archive. |
| Attack source | The first mail server with a public IP address that routes a suspicious message. For example, if a suspicious message routes from IP1 (sender) to IP2 (MTA: 225.237.59.52) to IP3 (company mail gateway) to IP4 (recipient), TippingPoint Advanced Threat Protection for Email identifies 225.237.59.52 (IP2) as the attack source. By studying attack sources, you can identify regional attack patterns or attack patterns that involve the same mail server. |
| Attacker | An individual, group, organization, or government that conducts or has the intent to conduct harmful activities. |

| Term | Definition |
|---|---|
| Authentication | The verification of the identity of a person or a process. Authentication ensures that the system delivers the digital data transmissions to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from).<br><br>The simplest form of authentication requires a user name and password to gain access to a particular account. Other authentication protocols are secret-key encryption, such as the Data Encryption Standard (DES) algorithm, or public-key systems using digital signatures. |
| Bot | A program that infects computers connected to the Internet, allowing them to be remotely controlled by an attacker. Bot-controlled computers become part of a network of compromised machines that are exploited by the attacker for malicious activities. |
| Botnet | A botnet (short for “bot network”) is a network of hijacked zombie computers controlled remotely by an attacker. The attacker uses the network to send spam and launch Denial of Service attacks, and may rent the network out to other cybercriminals. If one of the computers targeted becomes compromised, the attacker can often take control of that computer and add it to the botnet. |
| BCC mode | A TippingPoint Advanced Threat Protection for Email operation mode. TippingPoint Advanced Threat Protection for Email operates as an out-of-band appliance. TippingPoint Advanced Threat Protection for Email silently monitors mirrored email traffic received from an upstream mail server and notifies security administrators about discovered threats. |
| Callback address | An external IP address, host name, or URL that an object requests (“calls back to”) during scanning or analysis. Malware connected to a C&C server often sends requests to it in order to carry out harmful activities.<br><br>The host name or IP address that an object requests may be called a “callback host”. A URL that an object requests may be called a “callback URL”. |
| Command-and-Control (C&C) server | The central server (s) for a botnet or entire network of compromised devices used by a malicious bot to propagate malware and infect a host. |

| Term | Definition |
|---|---|
| Compromised MTA | A compromised MTA is usually a third-party open mail relay that attackers can use to send malicious email messages or spam without detection because the mail relay does not check the source or destination for known users. |
| Certified Safe Software Service (CSSS) | Verifies the safety of files. Certified Safe Software Service reduces false positives, and saves computing time and resources. |
| Communicator | The communications backbone of the Control Manager system. Communicator is part of the Control Manager Management Infrastructure. Commands from the Control Manager server to TippingPoint Advanced Threat Protection for Email, and status reports from TippingPoint Advanced Threat Protection for Email to the Control Manager server all pass through this component. |
| Data port | A hardware port that accesses resources available on a network. |
| Detection | A discovered event, file, or network address. Detections include unusual, undesired, suspicious, unknown, and malicious behaviors and connections. |
| Event | An observable, measurable occurrence in a system or network. |
| False positive | A detection that is determined to be high risk but is actually benign. |
| File submission rule | A set of criteria and conditions used to reduce the number of files in the Virtual Analyzer queue. File submission rules check files based on detection types, detection rules, and file properties. |
| IntelliTrap | A Trend Micro utility that helps reduce the risk of viruses entering the network by blocking real-time compressed executable files and pairing them with other malware characteristics. |
| 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. |
| Log | An official record of events occurring in a system or network. |

| Term | Definition |
|---|---|
| Management console | A web-based user interface for managing a product. |
| Management port | A hardware port that connects to the management network. |
| Message ID | A unique identifier for a digital message, most commonly a globally unique identifier used in email messages. Message IDs must have a specific format (subset of an email address) and be globally unique. A common technique used by many message systems is to use a time and date stamp along with the local host's domain same. |
| Message stamp | Text added at the beginning or end of the email message. |
| Message tag | Text added to the subject line of the email message. |
| MTA mode | A TippingPoint Advanced Threat Protection for Email operation mode. TippingPoint Advanced Threat Protection for Email can act as a Mail Transfer Agent (MTA) in the mail traffic flow. As an inline MTA, TippingPoint Advanced Threat Protection for Email directly protects your network from harm by blocking malicious email messages. |
| Notification | A message triggered by an event in an endpoint or network. |
| Permitted sender | An email sender approved by TippingPoint Advanced Threat Protection for Email as being safe. |
| Permitted sender of relayed mail | An endpoint permitted or denied connection to the appliance based on the IP address of a single endpoint or any endpoint in an IP address range. |
| Port | The following term has multiple definitions depending upon its context:<br>• Hardware<br>A socket on an endpoint to connect to a removable device, cable, or other external equipment.<br>• TCP/IP Networking<br>An access channel by which software applications can use hardware resources in parallel. |

| Term | Definition |
|---|---|
| Report | A compilation of data generated from selectable criteria, used to provide the user with needed information. |
| Sample | A potentially malicious file or URL submitted to Virtual Analyzer. Virtual Analyzer opens the file or accesses the link in the sample to analyze the risk level. If Virtual Analyzer finds any additional links or files while analyzing a sample, Virtual Analyzer also analyzes them.<br><br>Example: If a user submits an archive that contains multiple files to Virtual Analyzer, Virtual Analyzer will analyze the archive as well as all of the encrypted files. |
| Sandbox image | A template used to deploy sandbox instances in Virtual Analyzer. A sandbox image includes an operating system, installed software, and other settings necessary for that specific computing environment. |
| Sandbox instance | A single virtual machine based on a sandbox image. |
| Script Analyzer Engine<br><br>Script Analyzer Pattern | The Script Analyzer Pattern is used during analysis of web page scripts to identify malicious code. |
| 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. |
| Smart Protection Network | Rapidly and accurately identifies new threats, delivering global threat intelligence to all Trend Micro products and services. The Smart Protection Network cloud data mining framework advances in the depth and breadth allow Trend Micro to look in more places for threat data, and respond to new threats more effectively, to secure data wherever it resides. |

| Term | Definition |
|---|---|
| Social engineering | A form of attack to psychologically manipulate a person to perform actions or divulge confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme. |
| Source IP address | The IP address of the mail server nearest to the email sender.<br><br>Examples: gateway mail server, compromised mail server, botnet with mail relay capabilities |
| SPAN/TAP mode | A TippingPoint Advanced Threat Protection for Email operation mode. TippingPoint Advanced Threat Protection for Email operates as an out-of-band appliance. TippingPoint Advanced Threat Protection for Email silently monitors mirrored email traffic received from a switch or network tap and notifies security administrators about discovered threats. |
| Spear phishing | A type of targeted attack where an attacker sends an email message masquerading as a known or legitimate entity to gain personal information from a targeted person. Spear phishing significantly raises the chances that targets will read a message that will allow to compromise a target network. In many cases, spear-phishing emails use attachments made to appear as legitimate documents because sharing via email is a common practice among large enterprises and government organizations. |
| Spyware Pattern | The Spyware Pattern identifies spyware and grayware in messages and attachments. |
| 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. |
| Threat Knowledge Base | The Threat Knowledge Base provides information for threat correlation. |
| True file type | The kind of data stored in a file, regardless of the file extension.<br><br>Example: A text file may have an extension of HTML, CSV, or TXT, but its true file type remains the same. |

| Term | Definition |
|---|---|
| Unscannable Archive | A password-protected archive that cannot be extracted and scanned using a custom-defined password list or heuristically obtained passwords. |
| Viewer account | An account that can view detection and system information, but does not have access to most configuration screens on the management console. |
| 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. |
| 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. |
| Virus Pattern | The Trend Micro Virus Scan Engine protects against viruses and malware in files through heuristic, signature-based, and behavior-based detection. Trend Micro updates the virus pattern files as soon as detection routines for new threats are available. |
| 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. |
| Widget Framework | The Widget Framework provides the template for TippingPoint Advanced Threat Protection for Email widgets. |

# Index


**A**

about
- features, 1-5
- Maintenance Agreement, 9-2
- new threats, 1-7
- product overview, 1-8

Active Directory
- group, 8-107
- user account, 8-107
- User Principle Name (UPN), 8-107

add local user account, 8-106

admin accounts, 8-105, 8-106, 8-108

administration, 8-1, 8-2, 8-4–8-7, 8-9, 8-11, 8-13, 8-14, 8-17, 8-22, 8-23, 8-25–8-28, 8-30, 8-66, 8-68–8-72, 8-74–8-77, 8-80, 8-81, 8-84–8-87, 8-97, 8-98, 8-100, 8-101, 8-103–8-106, 8-108, 8-110
- account roles, 8-105, 8-106
- accounts, 8-104
- accounts / contacts, 8-104
- Active Directory group, 8-107
- Active Directory user account, 8-107
- admin account, 8-105, 8-108
- archive file passwords, 8-86, 8-87
- backup recommendations, 8-98
- back up settings, 8-97, 8-98, 8-100
- components, 8-2, 8-4, 8-5
- contacts, 8-104, 8-110
- email scanning, 8-70
- export debug file, 8-103
- file passwords, 8-85
- license, 8-110
- local user account, 8-106
- log level, 8-103
- log settings, 8-66
- mail settings, 8-22
- message delivery, 8-22
- network settings, 8-9
- operation mode, 8-11
- product upgrades, 8-6, 8-7
- proxy settings, 8-13
- restore settings, 8-97, 8-98, 8-100
- scanning / analysis, 8-69
- SFTP upload, 8-68
- SMTP, 8-28
- SMTP connections, 8-23
- SMTP greeting, 8-30
- SMTP routing, 8-26, 8-27
- SMTP server, 8-14
- storage management, 8-101
- system and accounts, 8-17
- system maintenance, 8-97
- system settings, 8-9
- TLS, 8-25
- unable to restore settings, 8-98, 8-100
- Virtual Analyzer, 8-71, 8-72, 8-74–8-77, 8-80, 8-81, 8-84

advanced detection, 1-5

Advanced Threat Scan Engine, 1-10, 8-2, 8-70, H-1
- about, 1-10

affected recipients, 4-13

alerts, 6-1–6-7, 6-10, 6-20
- critical alerts, 6-2
- delete, 6-6
- export, 6-6
- important alerts, 6-3
- informational alerts, 6-4
- manage, 6-6

notification parameters, 6-7, 6-10, 6-20
required settings, 6-5
alerts, 6-5
triggered alerts, 6-5
view, 6-5
analysis, 8-69, 8-70
atse, 8-70
ATSE, 1-10, 8-2, H-1
about, 1-10
attachment stripping, 5-5
attacker, 1-7, 1-8
attack sources, 4-14
average Virtual Analyzer queue time alert, 6-3

**B**

backup, 8-97, 8-98, 8-100
backup recommendations, 8-98
benefits, 1-5
block action, 5-2
blocking page, 5-6
built-in redirect pages, 5-6

**C**

C&C, 1-7, 1-8
callback, 1-8
Certified Safe Software Service, 8-79
change password, 8-109
CLI, B-1
command-and-control, 1-7, 1-8
command line interface
entering the shell environment, B-3
Command Line Interface, B-1
accessing, B-2
using, B-2
components, 8-2
rollback, 8-5
update components, 8-4
updates, 8-5
update source, 8-4
component updates, 8-1
configuration, 2-1, 8-1
local user account, 8-106
management console, 2-4, 2-6
overview, 2-2
policy, 5-2, 5-6
configure
import SMTP settings, 8-27
Messaged Delivery settings, 8-26, 8-27
message delivery settings, 8-25, 8-26, 8-28, 8-30
SMTP connections, 8-23
configure system time, 8-17
Control Manager
about, 8-30
unregister, 8-35
CPU usage alert, 6-3
create certificates, A-6, A-8–A-10
critical alerts, 6-2, 6-5, 6-7
CSSS, 8-79

**D**

dashboard, 3-1, 3-3, 3-6–3-28, 3-30
dashboard
tabs, 3-2
overview, 3-2
tabs, 3-3
widgets, 3-2, 3-6–3-28, 3-30
daylight savings time, 7-9
Deep Discovery Malware Pattern, 8-2
default admin, 8-105
delete admin accounts, 8-108
delete alerts, 6-6
delete image, 8-77
deploy certificates, A-6, A-8–A-10

deployment, 1-5
system requirements, 2-7
deploy TLS, A-2
detected message alert, 6-3
detected risk, 4-2
detections, 4-1
detected risk, 4-2
email message risk levels, 4-2
suspicious message, 4-7
suspicious messages, 4-6, 4-7, 4-9, 4-12–4-14, 4-16–4-25
threat types, 4-5
Virtual Analyzer risk levels, 4-4
detection surge alert, 6-4
digital certificates, A-3
disk space alert, 6-3
documentation feedback, 10-5
Download Center, 8-7
downloader, 1-8
DST, 7-9

## E

edit admin account, 8-108
email message tracking, 7-1, 7-2
query, 7-2
email scanning, 8-70
archive file passwords, 8-86, 8-87
file passwords, 8-85
email subjects, 4-17
end stamp, 5-5
enter CLI, B-1
exfiltrate, 1-8
export alerts, 6-6
export debug file, 8-103
export debugging files, 8-97
exporting detections, 4-6
export settings, 8-97, 8-98
external integration, 8-84
external redirect pages, 5-6

## F

features, 1-5
file passwords, 8-85
firmware update, 8-7

## G

getting started, 2-1
management console, 2-6
management console access, 2-4
summary, 2-2

## I

images, 8-72, 8-74–8-77
important alerts, 6-2, 6-3, 6-5, 6-10
import certificates, A-13
import settings, 8-97, 8-98, 8-100
informational alerts, 6-2, 6-20
installation
software requirements, 2-7
instances, 8-72
IntelliTrap Exception Pattern, 8-2, H-4
IntelliTrap Pattern, 8-2, H-4
internal postfix, 8-14
IPv6 support, F-1

## L

license expiration alert, 6-2
local user accounts, 8-106
log level, 8-103
logs, 7-1, 7-2, 7-6–7-9
email message tracking, 7-2
filters, 7-9
MTA events, 7-6
system, 7-7
system events, 7-8

log settings, 8-66
    syslog server, 8-67

**M**

mail settings, 8-22
maintenance agreement, 8-110
Maintenance Agreement
    about, 9-2
    expiration, 9-2
    renewal, 9-2
malicious URLs, 4-5
malware, 4-5
management console, 2-4, 2-6
    navigation, 2-8
management network, 8-80
management port, 8-9
message delivery, 8-22, 8-26, 8-27
message delivery alert, 6-3
message delivery domains, 8-22
message delivery settings, 8-26, 8-27
Message Delivery settings
    configure, 8-26, 8-27
message details, 4-25
message tags, 5-2, 5-5
message tokens, 6-2
Microsoft Active Directory, 8-107. *See also* Active Directory
minimum requirements, 2-7
modify image, 8-77
MTA events, 7-1, 7-6

**N**

Network Content Correlation Pattern, 8-2
Network Content Inspection Engine, 8-2
Network Content Inspection Pattern, 8-3
network settings, 8-1, 8-9
notification parameters, 6-7
notification SMTP server, 8-9

**O**

on-demand reports, 6-22, 6-23
operation mode
    BCC mode, 8-11
    MTA mode, 8-11
    SPAN/TAP mode, 8-11

**P**

pass action, 5-2
password, 8-109
password derivation, 1-5
patches, 8-7
permitted senders, 8-28
phishing, 1-7
policy, 1-5, 5-1, 5-2, 5-5, 5-6
    actions, 5-2, 5-5, 5-6
    configuration, 5-2, 5-6
    controls, 5-2
    exceptions, 5-2, 5-7, 5-8, 5-11, 5-12
        import, 5-12
    structure, 5-2
policy actions, 5-2, 5-5, 5-6
ports, D-3
processing surge alert, 6-4
product license, 8-1, 8-110
product updates, 8-1
product upgrade, 8-6, 8-7
proxy settings, 8-9, 8-13

**Q**

quarantine, 4-22
    investigate, 4-24
    message details, 4-25
    search filters, 4-23
    view, 4-22

quarantine action, 5-2
query logs, 7-2, 7-8

## R

RAT, 1-8
redirect pages, 5-6
report formats, 6-22
reports, 6-1, 6-22, 6-23
    on demand, 6-23
    scheduled, 6-22
requirements, 2-7
restore, 8-97, 8-98, 8-100
risk level, 4-2
risk levels, 4-2, 4-4
rollback, 8-5

## S

safe domains, 5-8, 5-11, 5-12
safe files, 5-8, 5-11, 5-12
safe IP addresses, 5-8, 5-11, 5-12
safe recipients, 5-2, 5-7, 5-8
safe senders, 5-2, 5-7, 5-8
safe URLs, 5-8, 5-11, 5-12
sandbox error alert, 6-2
sandbox images, 8-72
sandbox queue alert, 6-3
scanning, 8-69
scanning and analysis, 8-1
scheduled reports, 6-22
schedule reports, 6-22
schedule updates, 8-5
Script Analyzer Engine, 8-3
Script Analyzer Pattern, 8-3, H-6
search, 7-9
search filters, 4-23
service stopped alert, 6-2
SFTP upload, 8-68
shell environment, B-3
smart protection, 1-11
    Web Reputation Services, 1-11
SMTP connections, 8-23
SMTP greeting, 8-28, 8-30
SMTP routing, 8-22, 8-26, 8-27
SMTP server, 8-14
spear-phishing, 1-7
Spyware/Grayware Pattern, 8-3
Spyware Pattern, H-7
storage management, 8-101
supported file types, 8-81
suspicious files, 4-5, 4-21
suspicious hosts, 4-19
suspicious messages, 4-7
    affected recipients, 4-13
    attack sources, 4-14
    email subjects, 4-17
    exporting detections, 4-6
    message details, 4-12
    quarantine, 4-22–4-25
    search filters, 4-9
    suspicious objects, 4-18–4-21
    suspicious senders, 4-16
    viewing, 4-7
suspicious objects, 4-18
    files, 4-21
    hosts, 4-19
    URLs, 4-20
suspicious senders, 4-16
suspicious URLs, 4-5, 4-20
syslog, 8-66
syslog server, 8-67
system and accounts, 8-1
system events, 7-1, 7-7
    query, 7-8

system requirements, 2-7
system updates, 8-6

**T**

tabs, 3-3
    system status, 3-3
    threat monitoring, 3-3
    trends, 3-3
    Virtual Analyzer, 3-3
tag action, 5-2
targeted malware, 1-7, 4-5
Threat Knowledge Base, H-7
threat types, 4-5
time-based filters, 7-1, 7-9, 8-1
TippingPoint Advanced Threat Protection Analyzer integration, 8-84
TLS, 8-25, A-1
    about, A-2
    certificate format, A-3
    create CA, A-6
    deploy, A-2
    deploy certificates, A-6, A-9, A-10
    import certificates, A-13
    obtain digital certificate, A-3
    prerequisites, A-3
    private key, A-8
transport layer, 8-24
transport layer security, 8-25
Transport Layer Security, A-1
Trend Micro TippingPoint Security Management System (SMS)
    about, 8-41
    tag categories, 8-42
triggered alerts, 6-2, 6-5

**U**

unreachable relay MTA alert, 6-2
update completed surge, 6-4
update failed alert, 6-3
updates, 8-4
    components, 8-2
    source, 8-3
update source, 8-4
User Principle Name (UPN), 8-107
using CLI, B-1

**V**

viewer accounts, 8-105, 8-106
Virtual Analyzer, 8-69, 8-70, 8-86, 8-87
    archive file passwords, 8-86, 8-87
    exceptions, 8-77
    external integration, 8-84
    file types, 8-77, 8-80, 8-81
    images, 8-72, 8-74–8-77
    instances, 8-72
    network settings, 8-77
    network types, 8-80
    overall status, 8-72
    overview screen, 8-71
    risk levels, 4-4
    statuses, 8-72
Virtual Analyzer Configuration Pattern, 8-3
Virtual Analyzer Sensors, 8-3, H-8
VSAPI, 8-2

**W**

warning page, 5-6
watchlist alert, 6-3
web reputation, 1-11
Web Reputation Services, 8-70
Widget Framework, H-8
widgets, 3-6–3-28, 3-30
    add, 3-6
    analysis

top attachment names, 3-16
top attachment types, 3-17
top callback hosts from Virtual Analyzer, 3-18
top callback URLs from Virtual Analyzer, 3-19
top email subjects, 3-20
control manager, 3-28
email messages with advanced threats, 3-28
sandbox performance, 3-24
average sandbox processing time, 3-26
suspicious objects from sandbox, 3-27
Virtual Analyzer queue, 3-25
system performance
delivery queue, 3-23
hardware status, 3-24
processed messages by risk, 3-21
processing volume, 3-22
quarantined messages, 3-14
system status, 3-20
tasks, 3-7, 3-8
threat monitoring, 3-8
advanced threat indicators, 3-15
attack sources, 3-9
detected messages, 3-11
high-risk messages, 3-10
top affected recipients, 3-12, 3-30
top attack sources, 3-13
trends, 3-15
wrs, 8-70


## X


X-header, 5-2, 5-7, 5-8


## Y


YARA rule file
add, 8-95
create, 8-93
delete, 8-96
edit, 8-96
export, 8-96
requirements, 8-93
YARA rules, 8-92

**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: APEM27712/170215