TREND MICRO™

2.5

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/home.aspx

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

Document Part No.: APEM27307/160118

Release Date: December 2016

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

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

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

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

Evaluate this documentation on the following site:

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

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 1-4
A New Threat Landscape 1-6
Spear-Phishing Attacks 1-6
C&C Callback 1-7
A New Solution 1-7
Virtual Analyzer 1-8
Advanced Threat Scan Engine 1-9
Web Reputation Services 1-9
Social Engineering Attack Protection 1-10
Trend Micro Control Manager 1-10

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
Configuring Internet Explorer 2-8

Chapter 3: Dashboard

Dashboard Overview 3-2

Tabs 3-3
- Predefined Tabs 3-3
- Tab Tasks 3-3
- New Tab Window 3-5

Widgets 3-6
- Adding Widgets to the Dashboard 3-6
- Widget Tasks 3-7
- Threat Monitoring 3-9
- Trends 3-16
- System Status 3-21
- Virtual Analyzer 3-25
- Control Manager 3-29

Chapter 4: Detections

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

Threat Type Classifications 4-5

Detected Messages 4-5
- Viewing Detected Messages 4-6
- Investigating a Detected Message 4-9
- Viewing Affected Recipients 4-11
- Viewing Attack Sources 4-13
- Viewing Senders 4-14
- Viewing Email Subjects 4-15
- Exporting Detections 4-17

Suspicious Objects 4-17
- Viewing Suspicious Hosts 4-18
- Viewing Suspicious URLs 4-19
- Viewing Suspicious Files 4-20

Quarantine 4-21
- Viewing Quarantined Messages 4-21

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 5-7
Adding Object Exceptions 5-8
Managing Object Exceptions 5-9
Configuring URL Keyword Exceptions 5-10

Chapter 6: Alerts and Reports

Alerts 6-2
Critical Alerts 6-2
Important Alerts 6-3
Informational Alerts 6-4
Configuring Critical Alert Notifications 6-5
Viewing Triggered Alerts 6-6
Alert Notification Parameters 6-7
Reports 6-20
Scheduling Reports 6-20
Generating On-Demand Reports 6-21

Chapter 7: Logs

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

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
Scheduling Component Updates 8-4
Rolling Back Components 8-5
Updating Your Product License 8-5

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

System Settings 8-8
Network Settings 8-8
Control Manager Settings 8-14
Configuring System Time 8-18
SNMP 8-18

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

Log Settings 8-30
Syslog 8-30

Scanning / Analysis 8-32
Email Scanning 8-32
Configuring Virtual Analyzer Network and Filters 8-32
Virtual Analyzer Overview 8-38
Virtual Analyzer Images 8-40
Configuring an External Virtual Analyzer 8-44

File Passwords 8-45
Smart Protection 8-48
Smart Feedback 8-52

System Maintenance 8-53
Backing Up or Restoring a Configuration 8-53
Configuring Storage Maintenance 8-56
Exporting Debugging Files 8-57
Configuring Log Level 8-57

Accounts / Contacts 8-58
Managing Accounts 8-58
Changing Your Password 8-61
Managing Contacts 8-61

License 8-62

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

Contacting Trend Micro TippingPoint Support 10-3

Sending Suspicious Content to Trend Micro 10-4

Other Resources 10-5

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
Obtaining a Digital Certificate A-3
Ensure that the Certificate Format is Valid A-4

Configuring TLS Settings for Incoming Messages A-4

Configuring TLS Settings for Outgoing Messages A-5

Creating and Deploying Certificates A-6
Creating the Certificate Authority Key and Certificate A-6
Creating the TippingPoint Advanced Threat Protection for Email Private Key and Certificate A-8
Creating the Keys and Certificates for Other Servers A-9
Signing the TippingPoint Advanced Threat Protection for Email Certificate A-10
Uploading Certificates A-13

Appendix B: Using the Command Line Interface

Using the CLI B-2

Entering the CLI B-2

Command Line Interface Commands B-3
Entering Privileged Mode B-4
CLI Command Reference B-4

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 TippingPoint Advanced Threat Protection for Email .. D-3

Appendix E: IPv6 Support in TippingPoint Advanced Threat Protection for Email

Configuring IPv6 Addresses E-2

Configurable IPv6 Addresses E-2
Management Console IPv6 Addresses E-3
CLI IPv6 Addresses E-3

Appendix F: 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. 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. 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. 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: 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 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 details, 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 1-6*
- *A New Solution on page 1-7*

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 TippingPoint Advanced Threat Protection for Email (ATP Email) 2.5

FEATURE	DESCRIPTION
Domain-based email delivery	ATP Email routes email messages to specified servers based on domains and email addresses. For details, see *Message Delivery on page 8-22*
Simple Network Management Protocol (SNMP) support	ATP Email sends SNMP trap messages to notify administrators about events that require attention, and listens to SNMP manager requests for system information, status updates, and configuration. For details, see *SNMP on page 8-18*
URL rewriting	ATP Email prevents connections to suspicious URLs and instead redirects users to custom warning or blocking pages. For details, see *Redirect Pages on page 5-6*

Feature	Description
Analysis of password-protected and macro-enabled files	ATP Email uses user-specified passwords to open protected documents prior to analysis and force-analyzes macro-enabled Microsoft Office files. For details, see *Virtual Analyzer File Submission Filters on page 8-35*
TippingPoint Advanced Threat Protection Analyzer integration	ATP Email can send objects to TippingPoint Advanced Threat Protection Analyzer for better processing performance. For details, see *Configuring an External Virtual Analyzer on page 8-44*
Smart Protection Server integration	ATP Email integrates with Smart Protection Server for web reputation data. For details, see *Setting Up Smart Protection Server on page 8-50*
Enhanced Control Manager integration	ATP Email sends suspicious objects to and receives exceptions from Control Manager. For details, see *Control Manager Settings on page 8-14*
Enhanced syslog integration	ATP Email sends logs for detections, analysis, alerts, and system events to up to three syslog servers. For details, see *Syslog on page 8-30*
Advanced Threat Indicators widget	The Advanced Threat Indicators widget shows the type, count, and risk level of advanced threat indicators in all email messages. For details, see *Advanced Threat Indicators on page 3-16*
Support of high-end hardware modules	ATP Email supports the high level hardware module, ATP Email 9100.

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

ATP 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

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, ATP 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. 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, ATP 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 8-18*.

5. Configure network settings.

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

6. Configure the notification SMTP server.

   For details, see *Configuring the Notification SMTP Server on page 8-12*.

7. Configure the mail limits and exceptions.

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

8. Configure Virtual Analyzer custom network settings.

   For details, see *Configuring Virtual Analyzer Network and Filters on page 8-32*.

9. Import Virtual Analyzer images.

   For details, see *Importing Virtual Analyzer Images on page 8-40*.

Important

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

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

    For details, see *Adding File Passwords on page 8-46*.

11. Configure email routing for downstream MTAs.

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

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

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

13. (Optional) Configure policy rules.

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

14. (Optional) Configure policy exceptions.

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

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

    For details, see *Control Manager Settings on page 8-14*.

16. 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 8-61*.

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.

Application	Requirements	Details
Internet Explorer™	Versions 9, 10, 11	Use only a supported browser to access the management console. Using the data port IP address you set during the initial configuration, specify the following URL: `https://[Appliance_IP_Address]:443`
Microsoft Edge™	Windows 10	
Mozilla Firefox™	Version 26 or later	
Google Chrome™	Version 31 or later	

Note

- SSH service is disabled by default when using the SSH client. To enable SSH service, see *configure service ssh enable on page B-12*.
- Internet Explorer requires additional configuration. For details, see *Configuring Internet Explorer on page 2-8*.

Configuring Internet Explorer

Disable Protected Mode if you are accessing the management console from Internet Explorer.

Procedure

1. From the Internet Explorer menu, go to **Tools** > **Internet Options** > **Security**.
2. Click **Internet**.
3. Clear **Enable Protected Mode**.

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. For details, see *Tabs on page 3-3*.
Widgets	Widgets represent the core dashboard components. For more information, 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

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 tab-related tasks:

TASK	STEPS
Add a tab	Click the plus icon (+) on top of the dashboard. The **New Tab** window appears. For information about this window, see *New Tab Window on page 3-5*.
Edit tab settings	Click **Tab Settings**. The **Tab Settings** window appears. The settings are similar to adding a new tab.
Move tab	Use drag-and-drop to change a tab's position.
Delete tab	Click the delete icon ( ) next to the tab title. Deleting a tab also removes all widgets in the tab.

New Tab Window

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

FIGURE 3-1. New Tab Window

TABLE 3-1. New Tab Configuration

CONFIGURATION	DESCRIPTION
Title	Specify the name of the tab.
Layout	Select an available layout.
Slide Show	Select whether to include the tab in the slide show that appears if you click **Play Tab Slide Show** on the dashboard.

Configuration	Description
Auto-fit	Select whether the tab automatically scales widgets to fit the page.

Widgets

Widgets represent the core components of the dashboard. Widgets contain visual charts and graphs that allow you to track threats and associate them with the logs accumulated from log sources.

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:

Task	Steps
Reduce the widgets that appear	Click a category from the left side.
Search for a widget	Specify the widget name in the **Search** text box at the top.
Change the widget count per page	Select a number from the **Records** drop-down menu.
Switch between the Detailed and Summary views	Click the display icons ( ) at the top right.
Select the widget to add the dashboard	Select the check box next to the widget's title.
Add 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. 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. You can resize any widget within a multi-column tab (red squares). These tabs have any of the following layouts.
Change the period	If available, click the **Period** drop-down menu to select the 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 3-7*.

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 3-29*.

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 3-7*.

Top Affected Recipients Widget

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 3-29*.

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 3-7*.

Top Attack Sources Widget

Top Attack Sources

Period: Last 4 hours

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

View all attack sources

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 3-7*.

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 3-7*.

Advanced Threat Indicators

Indicator	High	Medium	Low	Total
Targeted malware	0	0	0	0
Password-protected files	49	55	3	107
Documents with exploit code	0	0	0	0
Files with spoofed names	0	0	0	0
C&C callback (upon execution)	100	2	0	102
Unknown malicious links in message body	0	1457	85	1542
Unknown malicious links in attachments	0	0	0	0
Ransomware Detections	0	11	0	11

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 3-7*.

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 3-7*.

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 3-7*.

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 3-7*.

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 3-7*.

Top Email Subjects Widget

Top Email Subjects

Period Last 4 hours

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

View all email subjects

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 3-7*.

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 3-7*.

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 3-7*.

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 3-7*.

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 3-7*.

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 3-7*.

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 3-7*.

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 3-7*.

Control Manager

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

Note

Use the Control Manager management console to view Control Manager widgets. Control Manager widgets cannot be viewed through the ATP 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 3-7*.

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 3-7*.

Chapter 4

Detections

Topics include:

- *Detected Risk on page 4-2*
- *Threat Type Classifications on page 4-5*
- *Detected Messages on page 4-5*
- *Suspicious Objects on page 4-17*
- *Quarantine on page 4-21*

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 1-7*.

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 attachments with unknown threats detected as high risk by Virtual Analyzer
Medium	A medium-risk email message contains: • Known malware • Known dangerous links • Links detected as medium risk by Virtual Analyzer • Attachments detected as medium risk by Virtual Analyzer

Risk Level	Description
Low	A low-risk email message contains: • Known highly suspicious or suspicious links (Aggressive mode) • Links detected as low risk by Virtual Analyzer • Attachments detected as low risk by Virtual Analyzer
No risk	A no-risk email message: • Contains no suspicious attachments or links • Contains known highly suspicious or suspicious links (Standard mode) • Matches policy exception criteria

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

Risk Level	Description
High	The object exhibited highly suspicious characteristics that are commonly associated with malware. Examples: • Malware signatures; known exploit code • Disabling of security software agents • Connection to malicious network destinations • Self-replication; infection of other files • Dropping or downloading of executable files by documents
Medium	The object exhibited moderately suspicious characteristics that are also associated with benign applications. Examples: • Modification of startup and other important system settings • Connection to unknown network destinations; opening of ports • Unsigned executable files • Memory residency • Self-deletion
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
Suspicious File	A file that exhibits malicious characteristics **Important** Always handle suspicious files with caution.
Suspicious URL	A hyperlink embedded in an email message that links to an unknown malicious website

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 4-7*.

3. Click **Search**.

   All email messages matching the search criteria appear.

4. View the results.

HEADER	DESCRIPTION
▶	Investigate the email message to learn more about potential threats. For details, see *Investigating a Detected Message on page 4-9*.

Header	Description
Received	View the date and time that the suspicious email message first passes TippingPoint Advanced Threat Protection for Email. **Note** There is a short delay between when TippingPoint Advanced Threat Protection for Email receives an email message and when the email message appears in the **Detected Messages** tab.
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.
Sender	View the sending email address of the detected message.
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*.
Action	View the final result after scanning and analyzing the email message. The result is the executed policy action. **Note** In BCC mode and SPAN/TAP mode, the action is always **Monitoring only**.

Detected Message Search Filters

The following table explains the 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 the email message risk level. For details about risk levels, see *Email Message Risk Levels on page 4-2*.
Action	Select an action from the list. For details, see *Configuring the Actions on page 5-2*. **Note** In BCC mode and SPAN/TAP mode, the action is always **Monitoring only**.
Recipients	Specify recipient email addresses. Use a semicolon to separate multiple recipients.
Period	Select a predefined time range or specify a custom range.
Sender	Specify the sender email address. Only one address is allowed.
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. Example: `950124.162336@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. A compromised MTA is usually a third-party open mail relay used by attackers to send malicious email messages or spam without detection. **Note** **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. For information about threat discovery capabilities, see *Scanning / Analysis on page 8-32*.
Subject	Specify the email message subject.
Attachment	Specify attachment file names. Use a semicolon to separate multiple file names.
Password-protected file	Select email messages that contain a password-protected file.

Investigating a Detected Message

Procedure

1. Search for the email message.

   See *Viewing Detected Messages on page 4-6*.

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 4-10*.

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. 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.
Forensics	Get more information about this email message for further analysis. Download the email message or safely download the email message as an image.
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. Click **Search**.

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

HEADER	DESCRIPTION
Recipients	View the detected message recipient email addresses.
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. Click **Search**.

   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.

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 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. Click **Search**.

   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.
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. Click **Search**.

   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.

Exporting Detections

Procedure

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

The search results download as a CSV file.

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. Click **Search**.

   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.
Last Detected	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. Click **Search**.

   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.
Last Detected	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. Click **Search**.

   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. **Note** The SHA-1 hash value links to Threat Connect. 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.
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 Detected	View the date and time Virtual Analyzer last found the suspicious object in a submitted object.

Quarantine

TippingPoint Advanced Threat Protection for Email quarantines that suspicious email messages that meet certain policy criteria. View details about the 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. Click **Search**.

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

HEADER	DESCRIPTION
▸	Investigate the email message to learn more about potential threats. For details, see *Investigating a Quarantined Email Message on page 4-24*.
Received	View the date and time that the suspicious email message first passes TippingPoint Advanced Threat Protection for Email. **Note** There is a short delay between when TippingPoint Advanced Threat Protection for Email receives an email message and when the email message appears in the **Detected Messages** tab.
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.
Sender	View the sending email address of the detected message.
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*.
Password-protected attachment	Select to only show quarantined messages that have password-protected attachments.

Quarantine Search Filters

The following table explains the search filters for querying the quarantine. 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 the email message risk level. For details about risk levels, see *Email Message Risk Levels on page 4-2*.
Recipients	Specify recipient email addresses. Use a semicolon to separate multiple recipients.
Period	Select a predefined time range or specify a custom range.
Sender	Specify the sender email address. Only one address is allowed.
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. Example: `950124.162336@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. A compromised MTA is usually a third-party open mail relay used by attackers to send malicious email messages or spam without detection. **Note** **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.
Subject	Specify the email message subject.
Attachment	Specify attachment file names. Use a semicolon to separate multiple file names.
Password-protected attachment	Check if the attachement is password-protected.

Investigating a Quarantined Email Message

Procedure

1. Search for the email message.

   See *Viewing Quarantined Messages on page 4-21*.

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

Export All

Received	Risk Level	Recipients
2016-03-10 20:34:00	Medium	relay@njrelay.itlab.trendn
2016-03-10 20:34:00	Medium	relay@njrelay.itlab.trendn
2016-03-10 20:34:00	Medium	relay@njrelay.itlab.trendn
2016-03-10 20:34:00	Medium	relay@njrelay.itlab.trendn
2016-03-10 20:34:00	Medium	relay@njrelay.itlab.trendn
2016-03-10 20:34:00	Medium	relay@njrelay.itlab.trendn
2016-03-10 20:34:00	Medium	relay@njrelay.itlab.trendn
2016-03-10 20:34:00	Medium	relay@njrelay.itlab.trendn
2016-03-10 20:34:00	Medium	relay@njrelay.itlab.trendn

The table row expands with more information.

Received	Risk Level	Recipients	Sender	Email Subject			Threat	Action
2016-03-10 20:34:00	Medium	relay@njrelay.itlab.trendmicro	trendmicrotscases=trendmicro	NEW PSP CASE ALERT: 001	1	0	Malicious URL: EXPL_DRIVEBY.WR	Monitoring only
2016-03-10 20:34:00	Medium	relay@njrelay.itlab.trendmicro	trendmicrotscases=trendmicro	NEW PSP CASE ALERT: 001	1	0	Malicious URL: EXPL_DRIVEBY.WR	Monitoring only
2016-03-10 20:34:00	Medium	relay@njrelay.itlab.trendmicro	trendmicrotscases=trendmicro	NEW PSP CASE ALERT: 001	1	0	Malicious URL: EXPL_DRIVEBY.WR	Monitoring only
2016-03-10 20:34:00	Medium	relay@njrelay.itlab.trendmicro	trendmicrotscases=trendmicro	NEW PSP CASE ALERT: 001	1	0	Malicious URL: EXPL_DRIVEBY.WR	Monitoring only

Overview
Message ID: FzvpN00000000000000000000000000000000000000000...
Source IP: 204.14.232.72(San Francisco, United States)
Recipients: relay@njrelay.itlab.trendmicro.com

Attachments N/A

Links

URL	Site Category	Risk Level	Identified by	Threat	Global Intelligence
http://www.marioalons...	Disease Vector	Medium	Web Reputation Services	EXPL_DRIVEBY.WRS	View in Threat Connect

Analysis reports N/A

Forensics Download message (password: virus) | Screenshot

Message source

```
Received: from internalbeat (unknown [127.0.0.1])
        by internalbeat.tapping.ddei (Postfix) with ESMTP id 5DEDE5320B36
        for <relay@njrelay.itlab.trendmicro.com>; Thu, 10 Mar 2016 20:33:54 +0800 (CST)
Received: by sjdcintlab01.itlab.trendmicro.com (Postfix)
        id E8DE320500; Thu, 10 Mar 2016 04:33:46 -0800 (PST)
Delivered-To: internalbeta@itlab.trendmicro.com
Received: from sjdc-ittf-04.udc.trendmicro.com (sjdc-ittf-04.udc.trendmicro.com [66.180.82.132])
```

2016-03-10 20:34:00	Medium	relay@njrelay.itlab.trendmicro	trendmicrotscases=trendmicro	NEW PSP CASE ALERT: 001	1	0	Malicious URL: EXPL_DRIVEBY.WR	Monitoring only

3. Discover the email message details.

   See *Quarantined Message Details on page 4-26*.

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 8-56*.

- 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.
Message characteristics	Get information about any social engineering attack related characteristics that were detected in the email message, including the mail server reputation, gaps between transits, inconsistent recipient accounts, and forged sender addresses or unexpected relay servers.
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.
Message Source	View the email message header content.

Chapter 5

Policy

Topics include:

- *Policy Overview on page 5-2*
- *Message Tags on page 5-5*
- *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 • Stores a copy in the quarantine area
Strip attachment, redirect links to blocking page, and tag	• Delivers the email message to the recipient • Replaces suspicious attachments with a text file • Redirects suspicious links to a blocking page • Tags the email message subject with a string to notify the recipient

Option	Actions Taken
Strip attachment, redirect links to warning page, and tag	• Delivers the email message to the recipient • Replaces suspicious attachments with a text file • Redirects suspicious links to a warning page • Tags the email message subject with a string to notify the recipient
Pass and tag	• Delivers the email message to the recipient • 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) Specify the string to insert in the subject of email messages.

d. (Optional) In **X-Header**, 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 archives** 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 • Stores a copy in the quarantine area
Pass and tag	• Delivers the email message to the recipient • 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. (Optional) 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.

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 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**.

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

The SHA-1 hash value links to Threat Connect. 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**.

Managing Object Exceptions

Perform any of the following tasks to manage object exceptions. For details, see *Adding Object Exceptions on page 5-8*.

Procedure

- Specify search filters to control the display and to view existing exceptions.
- Modify the objects considered safe.

OPTION	DESCRIPTION
Add	Add a new object to the exceptions list. Optionally include a note to help you better understand the object exception.
Import	Select the CSV file to import. The format for each line is: <object>,<type>,[source],[notes] • <object> values: IP address or hyphenated IP range, domain, URL, or SHA-1 hash value • <type> values: IP address, Domain, Links, Files • (Optional) [source] values: Control Manager, local • (Optional) [notes]: Any additional information in any format Valid CSV examples: • www.example.com, Links, local, customer can view this site • 10.10.10.10, IP address, , HR address • 3395856CE81F2B7382DEE72602F798B642F14140, Files, Control Manager, SHA-1 of CA certificate • example.com, Domain, ,
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.

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 6-20*

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 **Note** 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)
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
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
Long Virtual Analyzer Queue	At least 20 messages in the Virtual Analyzer queue	Immediate

Name	Criteria (Default)	Checking Interval (Default)
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 Unsuccessful	Update has failed	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

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
Component Update Successful	An update was successfully completed	Immediate

Configuring Critical Alert Notifications

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

Note

Configure the notification SMTP server to send notifications. For details, see *Configuring the Notification SMTP Server on page 8-12*.

Procedure

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

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

Option	Description
Enable alert	Enable the selected alert.
Recipients	Specify the recipients who receive an email message when the alert triggers.
Subject	Specify the subject of the triggered alert email message.
Message	Specify the body of the triggered alert email message.

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

Viewing Triggered Alerts

Procedure

1. Go to **Alerts / Reports** > **Alerts** > **Triggered Alerts** .
2. Specify the search criteria.
   - **Alert level**
   - **Alert type**
   - **Search alert rule**
   - **Period**
3. View alert details.

HEADER	DESCRIPTION
Alert Level	The importance of the alert: critical, important, or informational
Alert 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
Triggered	The date and time when the alert occurred

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 All	Export all 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
Enable	Enable the selected alert.
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. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceIP%` • `%DeviceName%`

Table 6-5. Service Stopped

Parameter	Description
Enable	Enable the selected alert.
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. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceIP%` • `%DeviceName%` • `%ServiceName%`

Table 6-6. Relay MTAs Inaccessible

Parameter	Description
Enable	Enable the selected alert.
Recipients	Specify the recipients who will receive the triggered alert email message.

Parameter	Description
Subject	Specify the subject of the triggered alert email message.
Message	Specify the body of the triggered alert email message. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%MessageList%` • `%MTAList%`

Table 6-7. License Expiration

Parameter	Description
Enable	Enable the selected alert.
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. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DaysBeforeExpiration%` • `%DeviceName%` • `%DeviceIP%` • `%ExpirationDate%` • `%LicenseStatus%` • `%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
Enable	Enable the selected alert.
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.
Message	Specify the body of the triggered alert email message. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceIP%` • `%DeviceName%` • `%MessageList%`

TABLE 6-9. Watchlisted Recipients at Risk

PARAMETER	DESCRIPTION
Enable	Enable the selected alert.

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

Table 6-10. Long Message Delivery Queue

Parameter	Description
Enable	Enable the selected alert.
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. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeliveryQueue%` • `%DeviceIP%` • `%DeviceName%` • `%QueueThreshold%`

Table 6-11. High CPU Usage

Parameter	Description
Enable	Enable the selected alert.
Average CPU usage	Select the threshold for 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.

Parameter	Description
Message	Specify the body of the triggered alert email message. Use the following tokens to customize your message: • `%ConsoleURL%` • `%CPUThreshold%` • `%CPUUsage%` • `%DateTime%` • `%DeviceIP%` • `%DeviceName%`

Table 6-12. Long Virtual Analyzer Queue

Parameter	Description
Enable	Enable the selected alert.
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.
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. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceIP%` • `%DeviceName%` • `%SandboxQueue%` • `%SandboxQueueThreshold%`

TABLE 6-13. Long Virtual Analyzer Processing Time

PARAMETER	DESCRIPTION
Enable	Enable the selected alert.
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.
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. Use the following tokens to customize your message: • `%ConsoleURL%` • `%AveSandboxProc%` • `%DateTime%` • `%DeviceIP%` • `%DeviceName%` • `%SandboxProcThreshold%`

TABLE 6-14. Low Free Disk Space

PARAMETER	DESCRIPTION
Enable	Enable the selected alert.
Free disk space	The lowest disk space threshold in GB that triggers the alert. **Note** **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.

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. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceIP%` • `%DeviceName%` • `%DiskSpace%`

Table 6-15. Component Update Unsuccessful

Parameter	Description
Enable	Enable the selected alert.
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. Use the following tokens to customize your message: • `%ConsoleURL%` • `%ComponentList%` • `%DateTime%` • `%DeviceIP%` • `%DeviceName%`

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

PARAMETER	DESCRIPTION
Enable	Enable the selected alert.
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. Use the following tokens to customize your message: • `%MessageList%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%ConsoleURL%`

TABLE 6-17. Low Free Quarantine Disk Space

PARAMETER	DESCRIPTION
Enable	Enable the selected alert.
Free quarantine disk space	The lowest disk space threshold that triggers the alert. **Note** **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.

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. Use the following tokens to customize your message: • `%DiskSpace%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%ConsoleURL%`

Informational Alert Parameters

Note

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

Table 6-18. Detection Surge

Parameter	Description
Enable	Enable the selected alert.
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.

Parameter	Description
Message	Specify the body of the triggered alert email message. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DetectionCount%` • `%DetectionThreshold%` • `%DeviceIP%` • `%DeviceName%` • `%Interval%`

Table 6-19. Processing Surge

Parameter	Description
Enable	Enable the selected alert.
Processed messages	The email message threshold 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.

Parameter	Description
Message	Specify the body of the triggered alert email message. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceIP%` • `%DeviceName%` • `%Interval%` • `%ProcessingCount%` • `%ProcessingThreshold%`

Table 6-20. Component Update Successful

Parameter	Description
Enable	Enable the selected alert.
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. Use the following tokens to customize your message: • `%ConsoleURL%` • `%ComponentList%` • `%DateTime%` • `%DeviceIP%` • `%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 notification SMTP server to send notifications. For details, see *Configuring the Notification SMTP Server on page 8-12*.

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 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.
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.
Custom range	Specify a starting and ending time range.
Recipients	Specify recipient email addresses. Use a semicolon to separate multiple recipients.
Sender	Specify sender email addresses. Use a semicolon to separate multiple senders.
Subject	Specify the email message subject.

Filter	Description
Message ID	Specify the unique message ID. Example: `950124.162336@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. 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 the email message risk level. For details about risk levels, see *Email Message Risk Levels on page 4-2*.
Latest status	Select any of the following check boxes: • **Deleted from quarantine**: Messages that were manually deleted from the **Quarantine**. • **Delivered/Processing completed**: Messages that were delivered. In BCC mode and SPAN/TAP mode, email messages with this status are discarded. • **Delivery unsuccessful**: Messages that could not be delivered. In BCC mode and SPAN/TAP mode, email messages are never delivered. • **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. • **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. • **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.

4. View the results.

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

Field	Description
Source IP	View the MTA IP address nearest to the email message sender. Example: `123.123.123.123`.

Field	Description

Processing history	View how TippingPoint Advanced Threat Protection for Email processed the email message. The following are the possible processing actions:
	• **Action set to 'pass'**:
	  • The **Pass** policy action was applied to the email message.
	  • A copy of the email message was released by the user. This only applies if the **Strip attachments and tag** policy was applied to the original email message.
	• **Deleted**: The email message was deleted from the **Quarantine** folder.
	• **Delivered**: The email message was delivered.
	• **Not analyzed**: Virtual Analyzer was unable to complete the analysis for the reason specified.
	• **Processing completed**: Analysis was completed and the email message was discarded. This is the final status in BCC and SPAN/TAP mode.
	• **Quarantined**: The email message was quarantined in keeping with your TippingPoint Advanced Threat Protection for Email policies. In BCC mode and SPAN/TAP mode, email messages are never quarantined.
	• **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.
	• **Received**: The email message was received by ATP Email.
	• **Sent for analysis**: The email message was sent to Virtual Analyzer for analysis.
	• **Stripped**: Attachments were stripped from the email message and it was passed for delivery.

Field	Description
Action	Do any of the following: Quarantined Message: • **View in Quarantine** • **Release from Quarantine** • **View in Threat Messages** Non-Quarantined Message, with high/medium/low risk level: **View in Threat Messages** No Risk Message: **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.
   - From the bottom-right of the control panel, select the results to show per page or view the next results page.

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.
   - From the bottom-right of the control panel, select the results to show per page or view the next results page.

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 8-56*.

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: • Update events • 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.
   - From the bottom-right of the control panel, select the results to show per page or view the next results page.

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 8-8*
- *Mail Settings on page 8-22*
- *Log Settings on page 8-30*
- *Scanning / Analysis on page 8-32*
- *System Maintenance on page 8-53*
- *Accounts / Contacts on page 8-58*
- *License on page 8-62*

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 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.
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	Network Content Correlation Pattern implements detection rules defined by Trend Micro.
Script Analyzer Engine	The Script Analyzer Engine analyzes web page scripts to identify malicious code.
Script Analyzer Pattern	The Script Analyzer Pattern is used during analysis of web page scripts to identify malicious code.
Spyware/Grayware Pattern	The Spyware/Grayware Pattern identifies unique patterns of bits and bytes that signal the presence of certain types of potentially undesirable files and programs, such as adware and spyware, or other grayware.

Component	Description
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 Virus Pattern contains the detection routines for virus and malware scanning. Trend Micro updates the Virus Pattern regularly with detection routines for new identified threats.

Update Source

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

Note

If ATP Email is registered to Control Manager, you can configure ATP 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 8-3*.

Procedure

1. Go to **Administration** > **Component Updates** > **Components**.
2. Click **Update**.

   The components update.
3. 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**.

Rolling Back Components

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

Procedure

1. Go to **Administration** > **Component Updates** > **Components**.
2. Click **Rollback**.

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

Updating Your Product License

A license to Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support ("Maintenance") for one year from the date of purchase. After the first year, Maintenance must be renewed annually at Trend Micro's current Maintenance fees.

Procedure

- See *Maintenance Agreement on page 9-2*.

Product Updates

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

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

http://downloadcenter.trendmicro.com

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.

Procedure

1. Go to **Administration** > **Product Updates** > **Hot Fixes / 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 Hot Fix / Patch**.
   - Roll back a patch by clicking **Roll Back** under **History**. After rollback, ATP Email uses the most recent previous configuration. For example, rolling back patch 3 returns ATP 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. 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.

   Backing Up or Restoring a Configuration on page 8-53

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**.

   After the installation completes, the command line interface appears.

8. Perform the following post-installation steps:
   - Clear the browser.
   - Manually log on to the console.

System Settings

Network Settings

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). The following table describes each operation mode.

TABLE 8-3. Operation Modes

MODE	DESCRIPTION
MTA mode (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.

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

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 and to select the TippingPoint Advanced Threat Protection for Email operation mode.

Procedure

1. Go to **Administration** > **System Settings** > **Network**.
2. 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.
	• **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).
	• **Custom network**: The custom network handles sandbox analysis. This network should be an isolated network without a proxy or connection restrictions so that malicious samples do not affect other networks. To enable Virtual Analyzer file and URL analysis, specify network settings for at least one network interface other than the management port. Use any available network interface (eth1, eth2, or eth3) that is not configured for the mail network.
	• **Mail network**: The mail network handles mail routing and monitoring. Use a network interface that is not configured for the custom network.
	  • (Optional) For BCC or MTA mode, use any available network interface (eth1, eth2, or eth3).
	  • For SPAN/TAP mode, use the eth2 or eth3 network interface.

Host Name / Gateway / DNS	Specify the general network settings that affect all interfaces, including the host name, gateway, and DNS settings. **Note** If Virtual Analyzer will connect to the Internet, specify at least one DNS server that is accessible from the Virtual Analyzer network.

Option	Description
Operation Mode (Optional)	Select the operation mode based on your deployment. MTA mode is the default. For more information, see *Operation Modes on page 8-8*. **Note** BCC mode and SPAN/TAP mode are not available when the notification SMTP server is configured as internal Postfix. For details, see *Configuring the Notification SMTP Server on page 8-12*.

3. Click **Save**.
4. If you select **SPAN/TAP mode**, you must add at least one monitoring rule.

   For details, see *Adding a Monitoring Rule on page 8-11*.

Adding a Monitoring Rule

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

Procedure

1. In **Operation Mode**, click **Add Rule**.

   The **Add SPAN/TAP Mode Rule** window appears.
2. 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.

3. Click **Add**.

Configuring the Notification SMTP Server

TippingPoint Advanced Threat Protection for Email uses the notification 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** > **Notification 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. **Note** 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 name or IP address	Type the external SMTP server host name, IPv4 address or IPv6 address.

Option	Description
SMTP server port	Type the external SMTP server port number.

4. Click **Save**.

Configuring Proxy Settings

Configuring proxy settings affects:

- Component updates (pattern files and scan engines)
- Product license registration
- Web Reputation queries
- Script Analyzer Engine

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**.
Proxy type	Select the proxy protocol: • **HTTP** • **SOCKS4** • **SOCKS5**
Proxy server	Specify the proxy server host name or IP address.
Port	Specify the port that the proxy server uses to connect to the Internet.

OPTION	DESCRIPTION
User name	Optional: Specify the user name for administrative access to the proxy server.
Password	Optional: Specify the corresponding password.

3. Click **Save**.

Control Manager Settings

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 8-15*.

On ATP Email, use the **Administration** > **System Settings** > **Control Manager** tab to perform the following tasks:

- Register to a Control Manager server.

  For details, see *Registering to Control Manager on page 8-16*.

- Check the connection status between ATP Email and Control Manager.

- Unregister from a Control Manager server.

  For details, see *Unregistering from Control Manager on page 8-17*.

Note

Ensure that both ATP Email and the Control Manager server belong to the same network segment. If ATP Email is not in the same network segment as Control Manager, configure the port forwarding settings for ATP 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**
Reports	• One-time report: **One-time Reports** • 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

Component	Description
Management Communication Protocol (MCP) Agent	An application installed along with ATP Email that allows Control Manager to manage the product. The agent receives commands from the Control Manager server, and then applies them to ATP 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 ATP Email) on the Control Manager console's directory tree. The directory tree includes all managed entities.

Registering to Control Manager

Procedure

1. Go to **Administration** > **System Settings** > **Control Manager**.
2. Configure **General** settings.
   - View the registration status.
   - Specify the display name that identifies ATP Email in the Control Manager Product Directory.

   Tip

   Use the host name or specify a unique and meaningful name to help you quickly identify ATP Email.

3. Configure **Server Settings**.

Option	Description
Server address	Type the Control Manager server FQDN or IP address.

Option	Description
Port	Type the port number that the MCP agent uses to communicate with Control Manager. Select **Use HTTPS** if the Control Manager security is set to medium or high. Medium: Trend Micro allows HTTPS and HTTP communication between Control Manager and the MCP agent of managed products. 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**. 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. Click **Save**.

ATP 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** > **System Settings** > **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**.

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 ATP 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 8-19*.

- 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 IP address.

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

4. Click **Save**.
5. (Optional) Click **Download MIB** to save these settings for reuse.

   Users can import the MIB settings file to the SNMP server.

Configuring Manager Requests

SNMP managers can use SNMP protocol commands to request TippingPoint Advanced Threat Protection for Emails 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 device location of ATP Email.
Administrator contact	Specify the administrator contact of ATP Email.
SNMP version	Select the SNMP version: • SNMPv1/SNMPv2c • SNMPv3 If you use SNMPv3, configure the SNMP server as follows: • Context Name: `""` (default context) • Context Engine ID: `<Auto>` • (Optional) MD5 Authentication protocol: `HMAC-MD5` • (Optional) DES Privacy protocol: `CBC-DES`
Allowed community names	Specify at least one community name.
Security model	Select the security model: • No authentication or privacy • Authenticated • Authenticated with privacy
User name	Specify the user name.
Password	Specify the password.

Option	Description
Privacy passphrase	Specify the privacy passphrase.
Trusted manager server addresses	Specify between 1 and 5 trusted manager server addresses.

4. Click **Save**.
5. (Optional) Click **Download MIB** to save these settings for reuse.

   Users can import the MIB settings file to the SNMP server.

Mail Settings

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. ii. Type the **Subnet address**. iii. If IPv4 was selected, type the **Subnet mask**. 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: 192.168.1.1 192.168.2.0:255.255.255.0 192.168.3.1:255.255.255.128 192.168.4.100 192.168.5.32:255.255.255.192

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 private key by encrypting a random number using the TippingPoint Advanced Threat Protection for Email SMTP server's public key and an encryption key to generate the session keys. 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. 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. 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. Specify the **Sender email address**.
3. Under **Greeting Message**, specify a greeting message.
4. Click **Save**.

Log Settings

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** > **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**.

Scanning / Analysis

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 1-9*.

- Analyzing embedded links (URLs)

  See *Web Reputation Services on page 1-9*.

- Social Engineering Attack Protection

  See *Social Engineering Attack Protection on page 1-5*.

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.

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	Select how Virtual Analyzer connects to the network. For information about network types, see *Virtual Analyzer Network Types on page 8-34*.
Submission Filters	**Files**: Submit only highly suspicious files or submit highly suspicious files and force analyze all selected file types. **Exceptions**: Select Certified Safe Software Service to reduce the likelihood of false-positive detections. For details, see *Certified Safe Software Service on page 8-33*.
Timeout Settings	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. Virtual Analyzer requires an Internet connection to query Trend Micro cloud services (examples: WRS, ERS, and CSSS) for available threat data. 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. **Important** Enabling connections to the management network may result in malware propagation and other malicious activity in the network.

Network Type	Description
Custom network	Virtual Analyzer connects to the Internet using a port other than the management port. 1. Select a specific port for Virtual Analyzer traffic. Make sure that the port is available and able to connect directly to an outside network. 2. Type the gateway that Virtual Analyzer will use to access outside networks. 3. Type the DNS address that Virtual Analyzer will use to access outside networks. **Note** 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.
No network access	Isolate Virtual Analyzer traffic within the sandbox environment. The environment has no connection to an outside network. **Note** Virtual Analyzer has no Internet connection and relies only on its analysis engine. 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 8-6. Virtual Analyzer File Submission Filters

DISPLAYED FILE CATEGORY	FULL FILE TYPE	EXAMPLE FILE EXTENSIONS
Flash and other multimedia	Adobe™ Shockwave™ Flash file Apple QuickTime media	.swf .mov
Java	Java™ Applet Java Archive (JAR)	.Applet .jApplet .awt .jar
Office	Microsoft™ Word™ document Microsoft™ Office Word™ 2007 document Microsoft™ Powerpoint™ presentation Microsoft™ Office PowerPoint™ 2007 presentation Microsoft™ Excel™ spreadsheet Microsoft™ Office Excel™ 2007 spreadsheet Microsoft™ Office™ 2003 XML file Microsoft™ Word™ 2003 XML document Microsoft™ Excel™ 2003 XML spreadsheet Microsoft™ PowerPoint™ 2003 XML presentation Hancom™ Hangul Word Processor (HWP) document JustSystems™ Ichitaro™ document JungUm™ Global document Microsoft™ Outlook™ Item	.doc .docx .ppt .pptx .xls .xlsx .cell .xml .hwp .jtd .gul .msg
Office with Macros	Microsoft™ Office Word™ 2007 macro-enabled document Microsoft™ Office PowerPoint™ 2007 macro-enabled presentation	.docm .pptm .xlsm

Displayed File Category	Full File Type	Example File Extensions
	Microsoft™ Office Excel™ 2007 macro-enabled spreadsheet	
Other document formats	Compiled HTML (CHM) help file Microsoft™ Windows™ Shell Binary Link shortcut Microsoft™ Rich Text Format (RTF) document Adobe™ Portable Document Format (PDF)	.chm .lnk .rtf .pdf
Scripts	Text file	.js .jse .vbe .vbs
Windows executables	AMD™ 64-bit DLL file Microsoft™ Windows™ 16-bit DLL file Microsoft™ Windows™ 32-bit DLL file Executable file (EXE) AMD™ 64-bit EXE file DIET DOS EXE file Microsoft™ DOS EXE file IBM™ OS/2 EXE file 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	.dll .exe

Displayed File Category	Full File Type	Example File Extensions
	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	

Virtual Analyzer Overview

The **Virtual Analyzer Status** screen is a window into the health and 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 8-7. 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 8-8. 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 Tool 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 Tool 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 Tool 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. All instances are also automatically redistributed whenever you add images.

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 8-41*.
   - **HTTP or FTP server**

     See *Importing an Image from an HTTP or FTP Server on page 8-43*.

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 8-40*.

Procedure

1. Select **HTTP or FTP server**.
2. Specify the HTTP or FTP URL settings.

Option	Description
URL	Specify the HTTP or FTP URL. 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

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

Procedure

1. Go to **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

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

Procedure

1. Go to **Administration** > **Scanning / Analysis** > **Virtual Analyzer** > **Overview** > **Images**.
2. Click **Modify**.

   The **Modify Instances** screen appears.
3. Specify the number of instances for each image.
4. Click **Save**.

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. In the **Source** drop-down, 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.

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

Virtual Analyzer supports the following archive file types:

- `7z`
- `rar`
- `zip`

- bz2
- gzip
- tar
- arj
- zlib
- cab
- lha
- msg
- tnef
- ace

Virtual Analyzer 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 8-9. 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

Basis of Comparison	Trend Micro Smart Protection Network	Smart Protection Server
Administration	Hosted and maintained by Trend Micro	Installed and managed by Trend Micro product administrators
Connection protocol	HTTP	HTTP
Usage	Use if you do not plan to install Smart Protection Server To configure Smart Protection Network as source, see *Configuring Smart Protection Settings on page 8-50*.	Use as primary source and the Smart Protection Network as an alternative source For guidelines on setting up Smart Protection Server and configuring it as source, see *Setting Up Smart Protection Server on page 8-50*.

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.

CONSIDERATION	DESCRIPTION
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 8-50*, from Step 3.

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**
>
> ATP Email only supports global services when connecting using Smart Protection Server version 3.0 Patch 2 or later.

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

   - If your organization uses a CA certificate, select **Use certificate** and click **Import** to locate the certificate file.

     - If your organization uses a Certificate Revocation List, select **Use CRL** and click **Import** to locate 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**.

System Maintenance

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.

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

Note

You cannot back up the following settings:

- Control Manager settings
- Licenses and Activation Codes
- ActiveUpdate server information
- IP address and network settings

Procedure

1. Go to **Administration** > **System Maintenance** > **Back Up / Restore**.

2. Next to **Back up appliance configuration**, 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

You cannot restore the following settings:

- Control Manager settings
- Licenses and Activation Codes
- ActiveUpdate server information
- IP and network settings

Procedure

1. Go to **Administration** > **System Maintenance** > **Back Up / Restore**.
2. Next to **Restore the appliance configuration**, click **Choose File** and locate the file.
3. Click **Import**.

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 ATP 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.

     ATP 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.
>
> ATP Email purges 10% more than the specified percentage.

4. Click **Save**.

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**.

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

Only the default administrator account can add new administrator accounts. Custom accounts cannot do so even if you assign full permissions to the account.

Custom accounts with full administration rights can change only their own TippingPoint Advanced Threat Protection for Email passwords. Custom investigator and viewer accounts cannot change their own passwords. If you forget the default administrator account password, contact Trend Micro Support to reset the password.

Account Role Classifications

Role	Description
Administrator	Users have complete access to the features and settings contained in the menu items. • **Dashboard** • **Detections** • **Policy** • **Alerts / Reports** • **Logs** • **Administration** • **Help**
Investigator	Users can view certain features and settings contained in the menu items, but cannot make any administrative modifications. • **Dashboard** • **Detections** • **Alerts / Reports** > **Reports** > **Generated Reports** • **Alerts / Reports** > **Alerts** > **Triggered Alerts** • **Logs** > **MTA** • **Help**
Operator	Users can view certain features and settings contained in the menu items, but cannot make any administrative modifications. • **Dashboard** • **Detections** (no access to message body) • **Alerts / Reports** > **Reports** > **Generated Reports** • **Alerts / Reports** > **Alerts** > **Triggered Alerts** • **Logs** > **MTA** • **Help**

Adding Accounts

Procedure

1. Go to **Administration** > **Accounts / Contacts** > **Accounts**.
2. Click **Add**.

   The **Add Account** screen appears.
3. Select **Enabled**.
4. Specify the account user name and password.
5. Select the role.

   See *Account Role Classifications on page 8-59*.
6. Click **Save**.

   The new account is added to the **Admin 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

Procedure

1. Go to **Administration** > **Accounts / Contacts** > **Password**.

   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 6-20* and *Configuring Critical Alert Notifications on page 6-5*.

License

For information about managing your product license, see *Maintenance on page 9-1*.

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://clp.trendmicro.com/

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://clp.trendmicro.com/

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: xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx 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. • For evaluation licenses, component updates and scanning are not available. • For full licenses, technical support and component updates are not available. Scanning is maintained with outdated components. **WARNING!** 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** field 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://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware to learn more about:

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

Contacting Trend Micro TippingPoint Support

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

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

- Visit us online at:

  http://www.trendmicro.com/tippingpoint

- Trend Micro product documentation:

  http://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://ers.trendmicro.com

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

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

File Reputation Services

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

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

Record the case number for tracking purposes.

Web Reputation Services

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

http://global.sitesafety.trendmicro.com

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

Other Resources

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

Download Center

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

http://downloadcenter.trendmicro.com

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

Documentation Feedback

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

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

Appendix A

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, perform one of the following actions:

Procedure

- 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 private key by encrypting a random number using the TippingPoint Advanced Threat Protection for Email SMTP server's public key and an encryption key to generate the session keys. 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. 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. 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/key.pem

Generating RSA private key, 1024 bit long modulus

.....................++++++

....++++++

e is 65537 (0x10001)

# openssl req -new -key /tmp/key.pem -out /tmp/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/key.pem` file contains the TippingPoint Advanced Threat Protection for Email (`linux.course.test`) private key in PEM-format. The `/tmp/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/req.pem -out /tmp/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 = 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** 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`

- 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 specific low security risk information and to perform simple tasks. Privileged commands provide full configuration control and advanced monitoring and debugging features. Privileged commands are protected by an additional layer of credentials: the **Enable** account and password.

After you open the CLI menu, the screen appears.

0) **Exit**: Leaves the CLI.

1) **Device Information and Status**: Monitor hardware items, such as CPU usage, hard disk status, and disk space.

2) **Network Settings**: Modify the device host name, IP address, subnet mask, and the network default gateway address and DNS servers. You can also select the active data port.

3) **Maintenance**: Restarts the device, rescues the application, unregisters from the parent, or re-registers to the parent if the parent IP address was modified.

4) **Utility**: Modifies access to the management console and SSH access to the Data port. You can also enter the Linux-like shell environment for debugging and modify the device time zone, date, and time.

5) **Shutdown**: Reboots or powers off the device.

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-4*.

configure product management-port

TABLE B-1. configure product management-port

Set the management port IP address
Syntax: `configure product management-port [ipv4 | ipv6] <ip> <mask>`

View	Privileged
Parameters	**ipv4**: Configure IPv4 settings **ipv6**: Configure IPv6 settings **<ip>**: IP address for the interface **<mask>**: Network mask for the NIC
Example:	
To set the management port IPv4 address: `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: `configure product operation-mode [BCC | MTA | TAP]`	
View	Privileged
Parameters	**BCC**: Deploy in BCC mode **MTA**: Deploy in MTA mode **TAP**: Deploy in SPAN/TAP mode
Example:	
To deploy in BCC mode: `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: `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: `configure network dns [ipv4 | ipv6] <dns1> <dns2>`	
View	Privileged
Parameters	**ipv4**: Configure IPv4 settings **ipv6**: Configure IPv6 settings **<dns1>**: Primary DNS server **<dns2>**: Secondary DNS server **Note** 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: `configure network dns ipv4 192.168.10.21`	
To configure the primary and secondary DNS with the following values: • Primary DNS: `192.168.10.21` • Secondary DNS: `192.168.10.22` `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: `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: `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: `configure network interface [ipv4 | ipv6] <interface> <ip> <mask>`	
View	Privileged
Parameters	**ipv4**: Configure IPv4 settings **ipv6**: Configure IPv6 settings **<interface>**: NIC name **<ip>**: IP address for the interface **<mask>**: Network mask for the NIC

Example:
To configure an NIC with the following values: • Interface: `eth0` • IPv4 address: `192.168.10.10` • IPv4 subnet mask: `255.255.255.0` `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: `configure network route add [ipv4 | ipv6] <ip_prefixlen> <via> <dev>`	
View	Privileged
Parameters	**ipv4**: Configure IPv4 settings **ipv6**: Configure IPv6 settings **<ip_prefixlen>**: Destination network ID with format IP_Address/Prefixlen **<via>**: IP address of the next hop **<dev>**: Device name
Example:	
To add a new route entry: `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 for an TippingPoint Advanced Threat Protection for Email device	
Syntax: `configure network route default [ipv4 | ipv6] <gateway>`	
View	Privileged
Parameter	**ipv4**: Configure IPv4 settings **ipv6**: Configure IPv6 settings **<gateway>**: IP address of default gateway
Example:	
To set the default route for an TippingPoint Advanced Threat Protection for Email device: `configure network route default ipv4 192.168.10.1`	

configure network route del

TABLE B-9. configure network route del

Deletes a route for an TippingPoint Advanced Threat Protection for Email device	
Syntax: `configure network route del [ipv4 | ipv6] <ip_prefixlen> <via> <dev>`	
View	Privileged
Parameters	**ipv4**: Configure IPv4 settings **ipv6**: Configure IPv6 settings **<ip_prefixlen>**: Destination network ID with format IP_Address/Prefixlen **<via>**: IPv4 address of the next hop **<dev>**: Device name

Example:
To delete a route for an TippingPoint Advanced Threat Protection for Email device: `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 for a TippingPoint Advanced Threat Protection for Email device	
Syntax: `configure network route del default ipv6 <gateway> <device>`	
View	Privileged
Parameters	gateway: IPv6 Address of the default gateway device: Link local to IPv6 default gateway
Example: 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: `configure service ssh disable`	
View	Privileged
Parameters	None
Examples:	

To disable SSH on all NICs: `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: `configure service ssh enable`	
View	Privileged
Parameters	None
Examples:	
To enable SSH: `configure service ssh enable`	

configure service ssh port

TABLE B-13. configure service ssh port

Change SSH service port.	
Syntax: `configure service ssh <port>`	
View	Privileged
Parameters	port: configure the SSH service port <port>: port number
Example: 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: `configure service ntp [enable | disable | server-address <address>]`	
View	Privileged
Parameters	**enable**: Enable NTP **disable**: Disable NTP **server-address**: Configure the NTP server address **<address>**: Specify the FQDN or IP address of the NTP server
Examples:	
To configure the NTP server address as 192.168.10.21: `configure service ntp server-address 192.168.10.21`	
To enable synchronization with the NTP server: `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: `configure system date <date> <time>`	
View	Privileged
Parameters	**<date>**: Set the date using the following format: **yyyy-mm-dd** **<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: `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: `configure system password enable`	
View	Privileged
Parameters	None
Examples:	
To change the password required to enter Privileged mode: `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: `configure system timezone <region> <city>`	
View	Privileged
Parameters	**<region>**: Region name **<city>**: City name
Example:	

To configure the TippingPoint Advanced Threat Protection for Email device to use the time zone for the following location:

Region: America

City: New York

```
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: `enable`	
View	Normal
Parameters	None
Example:	

To enter privileged mode: `enable`

exit

TABLE B-20. exit

Exits privileged mode. Exits the session for those not in privileged mode.	
Syntax: `exit`	
View	Normal
Parameters	None
Example:	
To exit privileged mode or to exit the session when not in privileged mode: `exit`	

help

TABLE B-21. help

Displays the CLI help information.	
Syntax: `help`	
View	Normal
Parameters	None
Example:	

To display the CLI help information: `help`

history

TABLE B-22. history

Displays the current session's command line history.	
Syntax: `history [limit]`	
View	Normal
Parameters	**[limit]**: Specifies the size of the history list for the current session Specifying "0" retains all commands for the session.
Example:	
To specify six commands for the size of the history list: `history 6`	

logout

TABLE B-23. logout

Logs out of the current CLI session.	
Syntax: `logout`	
View	Normal
Parameters	None
Example:	

To logout from the current session: `logout`

ping

TABLE B-24. ping

Pings a specified host.	
Syntax: `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. **[-i interval]**: Specifies the delay interval in seconds between each packet. Default value is 1 second. **<dest>**: Specifies the destination host name or IP address
Examples:	
To ping the IP address 192.168.1.1: `ping 192.168.1.1`	
To ping the host remote.host.com: `ping remote.host.com`	

ping6

TABLE B-25. ping6

Pings a specified IPv6 host through interface eth0.
Syntax: `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. **[-i interval]**: Specifies the delay interval in seconds between each packet. Default value is 1 second. **<dest>**: Specifies the destination host name or IP address
Examples:	
To ping the IPv6 address fe80::21a:a5ff:fec1:1060: `ping6 fe80::21a:a5ff:fec1:1060`	
To ping the host remote.host.com: `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: `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: `start task postfix drop D10D4478A5`	
To delete all email messages from the email message queue: `start task postfix drop all`	

start task postfix flush

TABLE B-27. start task postfix flush

Attempts to deliver all queued email messages.	
Syntax: `start task postfix flush`	
View	Privileged
Parameters	None
Example:	
To deliver all queued email messages: `start task postfix flush`	

start task postfix queue

TABLE B-28. start task postfix queue

Displays all email messages queued in Postfix.	
Syntax: `start task postfix queue`	
View	Privileged
Parameters	None
Example:	
To display all Postfix queued email messages: `start task postfix queue`	

start service postfix

TABLE B-29. start service postfix

Starts the Postfix mail system	
Syntax: `start service postfix`	
View	Privileged
Parameters	None
Example:	
To start the Postfix mail system: `start service postfix`	

start service product

TABLE B-30. start service product

Starts the Product service system.	
Syntax: `start service product`	
View	Privileged
Parameters	None
Example:	
To start the Product service system: `start service product`	

start service ssh

TABLE B-31. start service ssh

Starts the ssh service system.	
Syntax: `start service ssh`	
View	Privileged
Parameters	None
Example:	
To start the ssh service system: `start ssh service`	

stop process core

TABLE B-32. stop process core

Stops a running process and generates a core file.	
Syntax: `stop process core <pid>`	
View	Privileged
Parameters	**<pid>**: The process ID
Example:	
To stop a process with ID 33: `stop process core 33`	

stop service postfix

TABLE B-33. stop service postfix

Stops the Postfix mail system.	
Syntax: `stop service postfix`	
View	Privileged
Parameters	None
Example:	
To stop the Postfix mail system: `stop service postfix`	

stop service product

TABLE B-34. stop service product

Stops the Product service system.	
Syntax: `stop service product`	
View	Privileged
Parameters	None
Example:	
To stop the Product service system: `stop service product`	

stop service ssh

TABLE B-35. stop service ssh

Stops the ssh service system.	
Syntax: `stop service ssh`	
View	Privileged
Parameters	None
Example:	
To stop the ssh service system: `stop ssh service`	

reboot

TABLE B-36. reboot

Reboots the TippingPoint Advanced Threat Protection for Email device immediately or after a specified delay.	
Syntax: `reboot [time]`	
View	Privileged
Parameters	**[time]**: Specifies the delay, in minutes, to reboot the TippingPoint Advanced Threat Protection for Email device
Examples:	
To reboot the TippingPoint Advanced Threat Protection for Email device immediately: `reboot`	
To reboot the TippingPoint Advanced Threat Protection for Email device after 5 minutes: `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: `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: `resolve 192.168.10.1`	
To resolve the IP address from host name parent.host.com: `resolve parent.host.com`	

show storage statistic

TABLE B-38. show storage statistic

Displays the file system disk space usage.	
Syntax: `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 device: `show storage statistic`	

show network

TABLE B-39. show network

Displays various TippingPoint Advanced Threat Protection for Email network configurations.	
Syntax: `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. **<address>**: FQDN or IP address that will be resolved with the Address Resolution Protocol (ARP). **connections**: Displays the TippingPoint Advanced Threat Protection for Email device's current network connections. **dns**: Displays the TippingPoint Advanced Threat Protection for Email device's DNS IP address. **dns ipv6**: Displays system DNS configuration for IPv6. **hostname**: Displays the TippingPoint Advanced Threat Protection for Email device's host name. **interface**: Displays the network interface card (NIC) status and configuration. **route**: Displays IP address route table. **route ipv4**: Displays system IPv4 route table. **route default ipv4**: Displays default IPv4 route table. **route default ipv6**: Display default IPv6 route table.
Examples:	
To display the ARP information for the address 10.2.23.41: `show network arp 10.2.23.41`	

To display the TippingPoint Advanced Threat Protection for Email device's current network connections: `show network connections`
To display the DNS configuration: `show network dns`
To display system DNS configuration for IPv6: `show network dns ipv6`
To display the host name of the TippingPoint Advanced Threat Protection for Email device: `show network hostname`
To display the NIC status and configuration: `show network interface`
To display the IP address route table: `show network route`
To display system IPv4 route table: `show network route ipv4`
To display system default IPv4 gateway: `show network route default ipv4`
To display system default IPv6 gateway: `show network route default ipv6`

show kernel

TABLE B-40. show kernel

Displays the TippingPoint Advanced Threat Protection for Email device's OS kernel information.

Syntax: `show kernel {messages | modules | parameters | iostat}`	
View	Normal
Parameters	**messages**: Displays kernel messages. **modules**: Displays kernel modules. **parameters**: Displays kernel parameters. **iostat**: Displays CPU statistics and I/O statistics for devices and partitions.
Examples:	
To display the OS kernel's messages: `show kernel messages`	
To display the OS kernel's modules: `show kernel modules`	
To display the OS kernel's parameters: `show kernel parameters`	
To display TippingPoint Advanced Threat Protection for Email device CPU statistics and I/O statistics: `show kernel iostat`	

show service

TABLE B-41. show service

Displays the TippingPoint Advanced Threat Protection for Email service status.	
Syntax: `show service [ntp <enabled | server-address> | ssh]`	
View	Normal

Parameters	**ntp enabled**: Displays the system NTP service status. **ntp server-address**: Displays the system NTP service server address. **ssh**: Displays the status of SSH.
Examples:	
To display the NTP service status: `show service ntp`	
To display the SSH status: `show service ssh`	

show memory

TABLE B-42. show memory

Displays the TippingPoint Advanced Threat Protection for Email device's system memory information.	
Syntax: `show memory [vm | statistic]`	
View	Normal
Parameters	**vm**: Displays virtual memory statistics **statistic**: Displays system memory statistics
Examples:	
To display TippingPoint Advanced Threat Protection for Email device virtual memory statistics: `show memory vm`	
To display TippingPoint Advanced Threat Protection for Email system memory statistics: `show memory statistic`	

show process

TABLE B-43. showprocess

Displays the status of TippingPoint Advanced Threat Protection for Email processes currently running.	
Syntax: `show process [top | stack | itrace | trace] [pid]`	
View	Normal
Parameters	**top**: Displays the status of TippingPoint Advanced Threat Protection for Email processes currently running and system related processes **stack**: Print a stack trace of a running process **itrace**: Trace the library call **trace**: Trace system calls and signals **pid**: The process id number
Examples:	

To display the status of TippingPoint Advanced Threat Protection for Email processes currently running:
`show process`
To display the stack trace of process 1233:
`show process stack 1233`
To display the system call of process 1233:
`show process trace 1233`
To display the library call of process 1233:
`show process itrace 1233`	

show product-info

TABLE B-44. show product-info

Displays the TippingPoint Advanced Threat Protection for Email product information.	
Syntax: `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 **operation-mode**: Displays the operation mode of TippingPoint Advanced Threat Protection for Email **service-status**: Displays the status of services **version**: Displays the product version
Examples:	
To display the management port's IP address and mask: `show product-info management-port` To display the operation mode: `show product-info operation-mode` To display the status of the service: `show-product-info service-status` 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 TippingPoint Advanced Threat Protection for Email system settings.
Syntax: `show system [date | timezone [continent | city | country]| uptime | version]`

View	Normal
Parameters	**date**: Displays the current time and date. **timezone**: Displays the TippingPoint Advanced Threat Protection for Email device's timezone settings. You can optionally specify the timezone information to view: • **continent**: Displays the system continent • **city**: Displays the system city • **country**: Displays the system country **uptime**: Displays how long the TippingPoint Advanced Threat Protection for Email device has been running. **version**: Displays version number for the TippingPoint Advanced Threat Protection for Email device.
Examples:	
To display the current time and date of the TippingPoint Advanced Threat Protection for Email device: `show system date`	
To display the TippingPoint Advanced Threat Protection for Email device's timezone settings: `show system timezone`	
To display the TippingPoint Advanced Threat Protection for Email device's continent: `show system timezone continent`	
To display the TippingPoint Advanced Threat Protection for Email device's city: `show system timezone city`	
To display the TippingPoint Advanced Threat Protection for Email device's country: `show system timezone country`	
To display how long TippingPoint Advanced Threat Protection for Email has been running: `show system uptime`	

To display TippingPoint Advanced Threat Protection for Email's version number: `show system version`

shutdown

TABLE B-46. shutdown

Specifies shutting down the TippingPoint Advanced Threat Protection for Email device immediately or after a specified delay.	
Syntax: `shutdown [time]`	
View	Privileged
Parameters	**[time]**: Shuts down the TippingPoint Advanced Threat Protection for Email device after a specified delay in minutes.
Examples:	
To shut down the TippingPoint Advanced Threat Protection for Email device immediately: `shutdown`	
To shut down the TippingPoint Advanced Threat Protection for Email device after a 5 minute delay: `shutdown 5`	

traceroute

TABLE B-47. traceroute

Displays the tracking route to a specified destination.	
Syntax: `traceroute [-h hops] <dest>`	
View	Normal

Parameters	**[-h hops]**: Specifies the maximum number of hops to the destination. The minimum number is 6. **<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: `traceroute 172.10.10.1`	
To display the route to IP address 172.10.10.1 with a maximum of 30 hops: `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 • Strip attachments, redirect links to blocking page, and tag • Strip attachments, redirect links to warning page, and tag • Pass and tag • Pass with no action
`%DateTime%`	The date and time that the alert initiated	2014-03-21 03:34:09
`%Risk%`	The email message's risk level	• High • Medium • Low • 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: • System: Average Sandbox Processing Time Examples: • 3 • 2
`%ComponentList%`	The list of components.	Where allowed: • System: Update Completed • System: Update Failed Examples: • Virus Pattern • Spyware Pattern • IntelliTrap Exception Pattern

Token	Description	Notes
`%CPUThreshold%`	The maximum CPU usage as a percentage allowed before TippingPoint Advanced Threat Protection for Email sends an alert notification	Where allowed: • System: CPU Usage Examples: • 95 • 85
`%CPUUsage%`	The total CPU utilization as a percentage	Where allowed: • System: CPU Usage Examples: • 80 • 65
`%DateTime%`	The date and time that the TippingPoint Advanced Threat Protection for Email received the email message	Where allowed: • All Examples: • 2014-03-21 03:34:09 • 2014-06-15 11:31:22
`%DaysBeforeExpiration%`	The number of days before the product license expires	Where allowed: • System: License Expiration Examples: • 4 • 123

Token	Description	Notes
`%DeliveryQueue%`	The number of email messages in the delivery queue waiting for TippingPoint Advanced Threat Protection for Email to process.	Where allowed: • System: Message Delivery Queue Examples: • /var/spool/postfix/active • /var/spool/postfix/incoming
`%DetectionCount%`	The number of messages detected with suspicious characteristics during the specified period of time	Where allowed: • System: Detection Surge Examples: • 50 • 200
`%DetectionThreshold%`	The maximum number of messages detected to have suspicious characteristics before TippingPoint Advanced Threat Protection for Email sends an alert notification	Where allowed: • System: Detection Surge Examples: • 50 • 40
`%DeviceIP%`	The IP address of the TippingPoint Advanced Threat Protection for Email appliance	Where allowed: • All Example: • 123.123.123.123
`%DeviceName%`	The host name of the TippingPoint Advanced Threat Protection for Email appliance	Where allowed: • All Example: • example.com

Token	Description	Notes
`%DiskSpace%`	The lowest amount of disk space in GB before TippingPoint Advanced Threat Protection for Email send an alert notification	Where allowed: • System: Disk Space Examples: • 2 • 30
`%DomainList%`	The list of unreachable domains	Where allowed: • System: Unreachable Relay MTAs Examples: • a9.dd.com • a9.bb.com
`%ExpirationDate%`	The date that the product license expires	Where allowed: • System: License Expiration Examples: • 2014-03-21 03:34:09 • 2014-06-15 11:31:22
`%Interval%`	The frequency that TippingPoint Advanced Threat Protection for Email checks the message processing volume in minutes	Where allowed: • System: Detection Surge • System: Processing Surge Examples: • 15 • 10

Token	Description	Notes
`%LicenseStatus%`	The current status of the product license	Where allowed: • System: License Expiration Examples: • Evaluation • Not Activated • Activated • Expired • Grace Period For details, see *Product License Status on page 9-3*.
`%LicenseType%`	The product license type	Where allowed: • System: License Expiration Examples: • Full • Trial

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:
		• Security: Message Detected
		• Security: Watchlist
		Examples:
		• `==========`
		`Risk: High (potentially malicious file)`
		`Message ID: 20140610002704.EE9A5E0236@example.com`
		`Recipients: john@example.com`
		`Sender: louie@example.com`
		`Subject: The latest report`
		`Attachments: filename.pdf (PDF), anotherattachment.doc (Word), hello.exe (EXE)`
		`Received: 2014-05-21 11:52:32`
		• `==========`
		`Risk: Medium (potentially malicious URL)`
		`Message ID: 20140610002721.EE9A5E0236@example.com`
		`Recipients: suzysmith@example.com, johnnycash@gmail.com, peterpaul@examplecom`
		`Sender: johndoe@example.com`
		`Subject: Bad story to report about the differences in world eating habits`
		`Attachments: (Link only)`
		`Received: 2014-05-21 11:48:32`

%MTAList%	The list of unreachable MTAs. Each MTA appears as an IP address and the port number.	Where allowed: • System: Unreachable Relay MTAs Examples: • [1.1.1.1]:99 • [7.7.7.7]:77

Token	Description	Notes
`%ProcessingCount%`	The total number of processed messages over the specified period of time	Where allowed: • System: Processing Surge Examples: • 50 • 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: • System: Processing Surge Examples: • 100 • 40
`%QueueThreshold%`	The maximum number of messages in the delivery queue before TippingPoint Advanced Threat Protection for Email sends an alert notification	Where allowed: • System: Message Delivery Queue • System: Sandbox Queue Examples: • 100 • 40
`%SandboxProcThreshold%`	The maximum amount of time allocated for average sandbox processing before TippingPoint Advanced Threat Protection for Email sends an alert notification	Where allowed: • System: Average Sandbox Processing Time Examples: • 15 • 30

Token	Description	Notes
`%SandboxQueue%`	The email message count in the sandbox queue waiting to be analyzed by Virtual Analyzer	Where allowed: • System: Sandbox Queue Examples: • 30 • 75
`%SandboxQueueThreshold%`	The maximum number of messages in the sandbox queue before TippingPoint Advanced Threat Protection for Email sends an alert notification	Where allowed: • System: Sandbox Queue Examples: • 100 • 75
`%ServiceName%`	The stopped TippingPoint Advanced Threat Protection for Email service Where allowed: • System: Service Stopped	Where allowed: • System: Service Stopped Example: • scanner

Appendix D

Connections and Ports

Service Addresses and Ports

ATP 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.	`atpe25-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.	`atpe250-en.census.trendmicro.com:80`
Customer Licensing Portal	Manages your customer information, subscriptions, and product or service license.	`licenseupdate.trendmicro.com:80` `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.	`atpe250-en.fbs20.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.	`atpe25-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.	`atpe25-en.url.trendmicro.com:80` `atpe25-en-wis.url.trendmicro.com:443`

Ports Used by TippingPoint Advanced Threat Protection for Email

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	Computer connects to TippingPoint Advanced Threat Protection for Email through SSH.
25	TCP	Listening	MTAs and mail servers connect to TippingPoint Advanced Threat Protection for Email through SMTP.
53	TCP/UDP	Outbound	TippingPoint Advanced Threat Protection for Email uses this port for DNS resolution.
80	TCP	Listening and outbound	TippingPoint Advanced Threat Protection for Email connects to other computers and integrated Trend Micro products and hosted services through this port. In particular, it uses this port to: • Connect to the Customer Licensing Portal to manage the product license • Connect to Community File Reputation services when analyzing file samples • Connect to the Smart Protection Network and query Web Reputation Services • Upload virtual analyzer images to TippingPoint Advanced Threat Protection for Email using the image import tool
123	UDP	Outbound	TippingPoint Advanced Threat Protection for Email connects to the NTP server to synchronize time.

Port	Protocol	Function	Purpose
161	TCP	Listening	TippingPoint Advanced Threat Protection for Email uses this port to listen for requests from SNMP managers.
162	TCP	Outbound	TippingPoint Advanced Threat Protection for Emailconnects to SNMP mangers to send SNMP trap messages.
443	TCP	Listening and outbound	TippingPoint Advanced Threat Protection for Email uses this port to: • Access the management console with a computer through HTTPS • Communicate with Trend Micro Control Manager • Connect to the Smart Protection Network and query Web Reputation Services • Connect to Trend Micro Threat Connect • Send anonymous threat information to Smart Feedback • Update components by connecting to the ActiveUpdate server • Send product usage information to Trend Micro feedback servers • Verify the safety of files through the Certified Safe Software Service
5274	TCP	Outbound	TippingPoint Advanced Threat Protection for Email uses this port as the default port to connect to the Smart Protection Server for web reputation services.

Port	Protocol	Function	Purpose
User-defined	N/A	Outbound	TippingPoint Advanced Threat Protection for Email uses the specified port to send logs to syslog servers.

Appendix E

IPv6 Support in TippingPoint Advanced Threat Protection for Email

This appendixsection 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.

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`

- TippingPoint Advanced Threat Protection for Email also accepts link-local IPv6 addresses, such as:

  fe80::210:5aff:feaa:20a2

  WARNING!

  Exercise caution when specifying a link-local IPv6 address because even though TippingPoint Advanced Threat Protection for Email can accept the address, it might not work as expected under certain circumstances. For example, TippingPoint Advanced Threat Protection for Email cannot update from an update source if the source is on another network segment and is identified by its link-local IPv6 address.

- 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 > Notification SMTP
- Administration > Mail Settings > Connections
- Administration > Mail Settings > Message Delivery
- Administration > Mail Settings > Limits and Exceptions
- Administration > Log Settings

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-6*
- *configure network dns on page B-7*
- *configure network interface on page B-8*
- *configure network route add on page B-9*
- *configure network route default on page B-10*
- *configure network route del on page B-10*

Appendix F

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 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. Alerts have the following levels of importance: • Critical Alert A message about an event that requires immediate attention. • Important Alert A message about an event that does not require immediate attention, but should be observed. • Informational Alert 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. 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). 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. 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: • Hardware A socket on an endpoint to connect to a removable device, cable, or other external equipment. • TCP/IP Networking 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 an object, Virtual Analyzer also analyzes them. 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 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. 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. 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 ATP Email widgets.

Index

A

about
- features, 1-4
- Maintenance Agreement, 9-2
- new threats, 1-6
- product overview, 1-7

add admin account, 8-60
admin accounts, 8-58–8-60
administration, 8-1–8-9, 8-12, 8-13, 8-18, 8-22, 8-23, 8-25–8-28, 8-30, 8-32, 8-34, 8-35, 8-38, 8-39, 8-41, 8-43–8-47, 8-53–8-62
- account roles, 8-59
- accounts, 8-58
- accounts / contacts, 8-58
- admin account, 8-58, 8-60
- archive file passwords, 8-46, 8-47
- backup recommendations, 8-54
- back up settings, 8-53–8-55
- change password, 8-61
- components, 8-2–8-5
- contacts, 8-58, 8-61
- email scanning, 8-32
- export debug file, 8-57
- file passwords, 8-45
- license, 8-62
- log level, 8-57
- log settings, 8-30
- mail settings, 8-22
- message delivery, 8-22
- network settings, 8-8, 8-9
- notification SMTP server, 8-12
- operation modes, 8-8
- product license, 8-5
- product upgrades, 8-6, 8-7
- proxy settings, 8-13
- restore settings, 8-53–8-55
- scanning / analysis, 8-32
- SMTP, 8-28
- SMTP connections, 8-23
- SMTP greeting, 8-30
- SMTP routing, 8-26, 8-27
- storage management, 8-56
- system and accounts, 8-18
- system maintenance, 8-53
- system settings, 8-8
- TLS, 8-25
- unable to restore settings, 8-54, 8-55
- Virtual Analyzer, 8-32, 8-34, 8-35, 8-38, 8-39, 8-41, 8-43, 8-44

advanced detection, 1-4
Advanced Threat Scan Engine, 1-9, 8-32
- about, 1-9

Advanced Threat Spam Engine, 8-2, F-1
affected recipients, 4-11
alerts, 6-1–6-7, 6-10, 6-17
- 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, 6-17
- required settings, 6-5
  - alerts, 6-5
- triggered alerts, 6-6
- view, 6-6

analysis, 8-32
atse, 8-32

ATSE, 1-9, 8-2, F-1
about, 1-9
attachment stripping, 5-5
attacker, 1-6, 1-7
attack sources, 4-13
average Virtual Analyzer queue time alert, 6-3

B

backup, 8-53–8-55
backup recommendations, 8-54
benefits, 1-4
block action, 5-2
blocking page, 5-6
built-in redirect pages, 5-6

C

C&C, 1-6, 1-7
callback, 1-7
Certified Safe Software Service, 8-33
change password, 8-61
CLI, B-1
command-and-control, 1-6, 1-7
command line interface
entering the shell environment, B-4
overview, B-3
Command Line Interface, B-1
accessing, B-2
using, B-2
components, 8-2
roll back, 8-5
update components, 8-4
updates, 8-4
update source, 8-3
component updates, 8-1
configuration, 2-1, 8-1
add admin account, 8-60
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, 8-18
contacting, 10-5
documentation feedback, 10-5
Control Manager
about, 8-14
unregister, 8-17
CPU usage alert, 6-3
create certificates, A-6, A-8–A-10
critical alerts, 6-2, 6-5, 6-7
CSSS, 8-33

D

dashboard, 3-1, 3-3, 3-5, 3-6, 3-8–3-29, 3-31
dashboard
tabs, 3-2
new tab, 3-5
overview, 3-2
tabs, 3-3
widgets, 3-2, 3-6, 3-8–3-29, 3-31
daylight savings time, 7-9
default admin, 8-58
delete admin accounts, 8-60
delete alerts, 6-6
delete image, 8-44
deploy certificates, A-6, A-8–A-10
deployment, 1-4
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, 4-5
    suspicious messages, 4-6, 4-7, 4-10, 4-11, 4-13–4-15, 4-17–4-21, 4-23, 4-24, 4-26
    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, 8-6, 8-7
downloader, 1-7
DST, 7-9

E

edit admin account, 8-60
email message tracking, 7-1, 7-2
    query, 7-2
email scanning, 8-32
    archive file passwords, 8-46, 8-47
    file passwords, 8-45
email subjects, 4-15
end stamp, 5-5
enter CLI, B-1
exfiltrate, 1-7
export alerts, 6-6
export debug file, 8-57
export debugging files, 8-53
exporting detections, 4-17
export settings, 8-53, 8-54
external integration, 8-44
external redirect pages, 5-6

F

features, 1-4
firmware update, 8-7

G

getting started, 2-1
    management console, 2-6
    management console access, 2-4
    summary, 2-2

I

images, 8-39, 8-41, 8-43, 8-44
important alerts, 6-2, 6-3, 6-5, 6-10
import certificates, A-13
import settings, 8-53, 8-55
informational alerts, 6-2, 6-17
installation
    software requirements, 2-7
instances, 8-39
IntelliTrap Exception Pattern, 8-2, F-4
IntelliTrap Pattern, 8-2, F-4
internal postfix, 8-12

L

license, 8-5
license expiration alert, 6-2
log level, 8-57
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, 8-30
    syslog server, 8-30

M

mail settings, 8-22

maintenance, 8-5
maintenance agreement, 8-62
Maintenance Agreement
    about, 9-2
    expiration, 9-2
    renewal, 9-2
malicious URLs, 4-5
malware, 4-5
management console, 2-4, 2-6
management network, 8-34
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, 4-26
message tags, 5-2, 5-5
message tokens, 6-2
minimum requirements, 2-7
modify image, 8-44
MTA events, 7-1, 7-6

N

network settings, 8-1, 8-8, 8-9
notification parameters, 6-7
notification SMTP server, 8-8, 8-12

O

on-demand reports, 6-20, 6-21
operation mode, 8-9
operation modes, 8-8
    BCC mode, 8-8
    MTA mode, 8-8
    SPAN/TAP mode, 8-8

P

pass action, 5-2
password, 8-61
password derivation, 1-4
patches, 8-7
permitted senders, 8-28
phishing, 1-6
policy, 1-4, 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, 5-7–5-9
    structure, 5-2
policy actions, 5-2, 5-5, 5-6
processing surge alert, 6-4
product license, 8-1, 8-5, 8-62
product updates, 8-1
product upgrade, 8-6, 8-7
proxy settings, 8-8, 8-13

Q

quarantine, 4-21
    investigate, 4-24
    message details, 4-26
    search filters, 4-23
    view, 4-21
quarantine action, 5-2
query logs, 7-2, 7-8

R

RAT, 1-7
redirect pages, 5-6
report formats, 6-20
reports, 6-1, 6-20, 6-21
    on demand, 6-21
    scheduled, 6-20
requirements, 2-7

restore, 8-53–8-55
risk level, 4-2
risk levels, 4-2, 4-4
roll back, 8-5

S

safe domains, 5-8, 5-9
safe files, 5-8, 5-9
safe IP addresses, 5-8, 5-9
safe recipients, 5-2, 5-7
safe senders, 5-2, 5-7
safe URLs, 5-8, 5-9
sandbox error alert, 6-2
sandbox images, 8-39
sandbox queue alert, 6-3
scanning, 8-32
scanning and analysis, 8-1
scheduled reports, 6-20
schedule reports, 6-20
schedule updates, 8-4
Script Analyzer Engine, 8-2
Script Analyzer Pattern, 8-2, F-6
search, 7-9
search filters, 4-23
service stopped alert, 6-2
shell environment, B-4
smart protection, 1-9
    Web Reputation Services, 1-9
SMTP connections, 8-23
SMTP greeting, 8-28, 8-30
SMTP routing, 8-22, 8-26, 8-27
SMTP server, 8-12
spear-phishing, 1-6
Spyware/Grayware Pattern, 8-2
Spyware Pattern, F-7
storage management, 8-56
supported file types, 8-35
suspicious files, 4-5, 4-20
suspicious hosts, 4-18
suspicious messages, 4-5
    affected recipients, 4-11
    attack sources, 4-13
    email subjects, 4-15
    exporting detections, 4-17
    message details, 4-10
    quarantine, 4-21, 4-23, 4-24, 4-26
    search filters, 4-7
    suspicious objects, 4-17–4-20
    suspicious senders, 4-14
    viewing, 4-6
suspicious objects, 4-17
    files, 4-20
    hosts, 4-18
    URLs, 4-19
suspicious senders, 4-14
suspicious URLs, 4-5, 4-19
syslog, 8-30
syslog server, 8-30
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
    tasks, 3-3
    threat monitoring, 3-3
    trends, 3-3
    Virtual Analyzer, 3-3
tag action, 5-2
targeted malware, 1-6, 4-5
Threat Knowledge Base, F-7

threat types, 4-5
time-based filters, 7-1, 7-9, 8-1
TippingPoint Advanced Threat Protection Analyzer integration, 8-44
TLS, 8-25, A-1
    about, A-2
    certificate format, A-4
    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 products
    services, D-2
triggered alerts, 6-2, 6-6

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, 8-3
using CLI, B-1

V

viewer accounts, 8-59
Virtual Analyzer, 8-32, 8-45–8-47
    archive file passwords, 8-46, 8-47
    exceptions, 8-32
    external integration, 8-44
    file passwords, 8-45
    file types, 8-32, 8-34, 8-35
    images, 8-39, 8-41, 8-43, 8-44
    instances, 8-39
    network settings, 8-32
    network types, 8-34
    overall status, 8-39
    overview screen, 8-38
    risk levels, 4-4
    statuses, 8-39
Virtual Analyzer Sensors, 8-3, F-8
Virus Pattern, 8-3
VSAPI, 8-3

W

warning page, 5-6
watchlist alert, 6-3
web reputation, 1-9
Web Reputation Services, 8-32
Widget Framework, F-8
widgets, 3-6, 3-8–3-29, 3-31
    add, 3-6
    analysis
        top attachment names, 3-17
        top attachment types, 3-18
        top callback hosts from Virtual Analyzer, 3-19
        top callback URLs from Virtual Analyzer, 3-20
        top email subjects, 3-21
    control manager, 3-29
        email messages with advanced threats, 3-29
    sandbox performance, 3-25
        average sandbox processing time, 3-27

suspicious objects from sandbox, 3-28
Virtual Analyzer queue, 3-26
system performance
delivery queue, 3-24
hardware status, 3-25
processed messages by risk, 3-22
processing volume, 3-23
quarantined messages, 3-15
system status, 3-21
tasks, 3-8, 3-9
threat monitoring, 3-9
advanced threat indicators, 3-16
attack sources, 3-10
detected messages, 3-12
high-risk messages, 3-11
top affected recipients, 3-13, 3-31
top attack sources, 3-14
trends, 3-16
wrs, 8-32

X

X-header, 5-2, 5-7

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

www.trendmicro.com

Item Code: APEM27307/160118