TREND MICRO™

2.5 TREND MICRO™ TippingPoint™ Advanced Threat Protection for Email

Installation and Deployment Guide

Advanced Protection Against Targeted Email Threats

Endpoint Security

Network Security

Protected Cloud

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

Document Part No.: APEM27285/151229

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

Chapter 4: Using the Command Line Interface

Chapter 5: Technical Support

Appendix A: Getting Started

Index

Preface

Preface

Topics include:

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

Chapter 1

Introduction

Topics include:

About TippingPoint Advanced Threat Protection for Email

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

What's New

TABLE 1-1. New Features in ATP Email 2.5

FEATURE	DESCRIPTION
Domain-based email delivery	ATP Email routes email messages to specified servers based on domains and email addresses.
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.
URL rewriting	ATP Email prevents connections to suspicious URLs and instead redirects users to custom warning or blocking pages.
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.
TippingPoint Advanced Threat Protection Analyzer integration	ATP Email can send objects to TippingPoint Advanced Threat Protection Analyzer for better processing performance.
Smart Protection Server integration	ATP Email integrates with Smart Protection Server for web reputation data.

Feature	Description
Enhanced Control Manager integration	ATP Email sends suspicious objects to and receives exceptions from Control Manager.
Enhanced syslog integration	ATP Email sends logs for detections, analysis, alerts, and system events to up to three syslog servers.
Advanced Threat Indicators widget	The Advanced Threat Indicators widget shows the type, count, and risk level of advanced threat indicators in all email messages.
Support of high-end hardware modules	ATP Email supports the high level hardware module, ATP Email 9100.

Chapter 2

Deployment

Topics include:

Deployment Overview

The following procedure provides an overview for planning the deployment and installing TippingPoint Advanced Threat Protection for Email.

Procedure

1. Decide the deployment mode.

   See *Network Topology Considerations on page 2-2*.

2. Review the system requirements.

   See *System Requirements on page 3-2*.

3. Install TippingPoint Advanced Threat Protection for Email.

   See *Installing TippingPoint Advanced Threat Protection for Email on page 3-6*.

4. Complete the getting started tasks.

   See *Getting Started Tasks on page A-2*.

Network Topology Considerations

Deploy TippingPoint Advanced Threat Protection for Email between the anti-spam gateway and the network's internal mail servers.

Deploying TippingPoint Advanced Threat Protection for Email behind the anti-spam gateway improves performance and reduces false positives by reducing the total email messages required to investigate.

Make sure that the management interface eth0 (on the back of the appliance) is accessible via TCP port 22 for the Command Line Interface (SSH) and TCP port 443 for the management console (HTTPS).

BCC Mode

While in BCC mode, TippingPoint Advanced Threat Protection for Email acts as an out-of-band appliance that does not interfere with network traffic. TippingPoint Advanced Threat Protection for Email discards all replicated email messages after they are checked for threats. No replicated email messages are delivered to the recipients.

Use BCC mode to understand how TippingPoint Advanced Threat Protection for Email processes email messages and identifies risks before fully deploying the product as an MTA. Configure an upstream MTA to mirror email traffic and handle message delivery. TippingPoint Advanced Threat Protection for Email sends alert notifications whenever a suspicious email message passes through the network, but does not deliver email messages.

The following figure shows how an email message passes through a network with TippingPoint Advanced Threat Protection for Email deployed in BCC mode. The email message enters the network and routes through the anti-spam gateway. The anti-spam gateway sends the email message through the network to the recipient and sends a copy of the email message to TippingPoint Advanced Threat Protection for Email.

TippingPoint Advanced Threat Protection for Email investigates and then discards the email message.

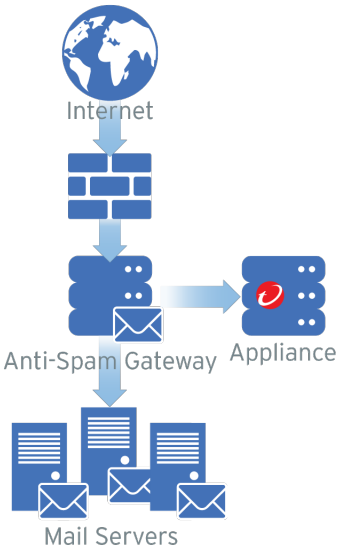


FIGURE 2-1. BCC Mode

MTA Mode

While in MTA mode, TippingPoint Advanced Threat Protection for Email serves as a Message Transfer Agent (MTA) in the line of the mail traffic flow. In a typical configuration, TippingPoint Advanced Threat Protection for Email receives email messages from an upstream MTA, such as an anti-spam gateway, and delivers the email messages to a downstream MTA.

The following figure shows how an email message passes through a network with TippingPoint Advanced Threat Protection for Email configured in MTA mode. The email message enters the network and routes through the anti-spam gateway to TippingPoint Advanced Threat Protection for Email. If the email message passes inspection, TippingPoint Advanced Threat Protection for Email routes the email message to downstream MTAs. Based on the policy configuration, TippingPoint

Advanced Threat Protection for Email performs user-configured actions on messages that contain malicious file attachments, embedded URLs, or suspicious message characteristics. TippingPoint Advanced Threat Protection for Email then notifies recipients.

FIGURE 2-2. MTA Mode

SPAN/TAP Mode

While in SPAN/TAP mode, TippingPoint Advanced Threat Protection for Email acts as an out-of-band appliance that does not interfere with network traffic. TippingPoint Advanced Threat Protection for Email discards all replicated email messages after they are checked for threats. No replicated email messages are delivered to the recipients.

Configure a switch or network tap to send mirrored traffic to TippingPoint Advanced Threat Protection for Email. TippingPoint Advanced Threat Protection for Email sends alert notifications whenever a suspicious email message passes through the network, but does not deliver email messages.

The following figure shows how an email message passes through a network with TippingPoint Advanced Threat Protection for Email deployed in SPAN/TAP mode. The email message enters the network and routes through the switch or network tap. The switch or network tap sends the email message through the network to the recipient and sends a copy of the email message to TippingPoint Advanced Threat Protection for Email. TippingPoint Advanced Threat Protection for Email investigates and then discards the email message.

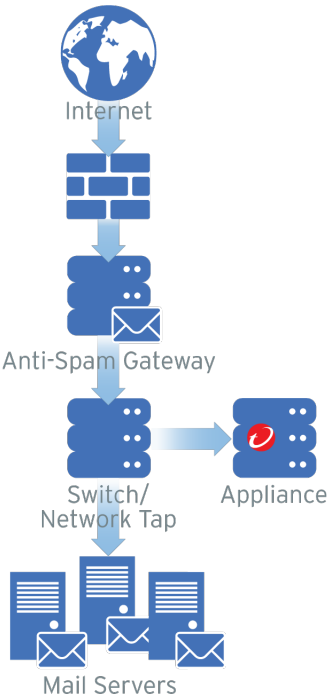


FIGURE 2-3. SPAN/TAP Mode

Control Manager Deployment

In a network topology containing multiple TippingPoint Advanced Threat Protection for Email appliances, Control Manager can aggregate log and suspicious objects data, generate reports, and update product components. Optionally single sign-on (SSO) through Control Manager to the management console of any registered TippingPoint Advanced Threat Protection for Email appliance.

The following figure shows how an email message passes through a network with multiple TippingPoint Advanced Threat Protection for Email appliances configured in MTA mode and registered to Control Manager. Each TippingPoint Advanced Threat

Protection for Email appliance independently processes email messages as an MTA while management is centralized through Control Manager.

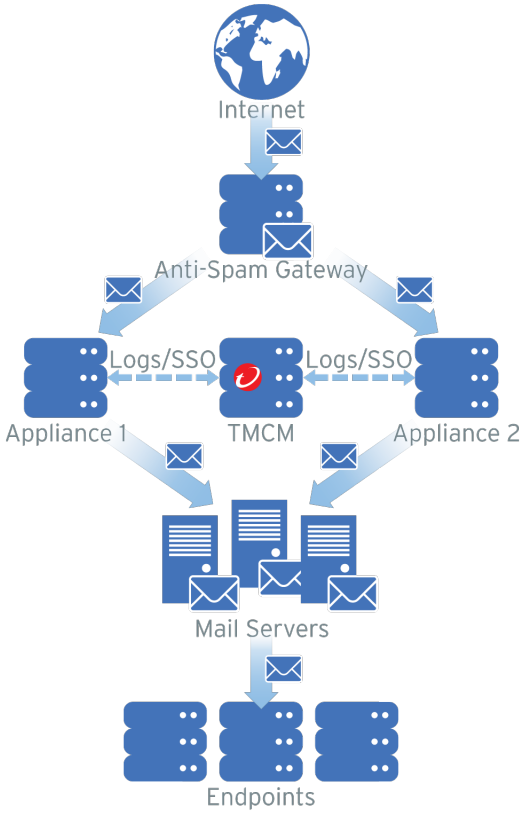


FIGURE 2-4. Control Manager Deployment

For details about configuring Control Manager settings, see *TippingPoint Advanced Threat Protection for Email Administrator's Guide*.

Recommended Network Environment

TippingPoint Advanced Threat Protection for Email requires connection to a **management network**. After deployment, administrators can perform configuration tasks from any computer on the management network.

Connection to a **custom network** is recommended to simulate malware behavior when connecting to the Internet. For best results, Trend Micro recommends an Internet connection without proxy settings, proxy authentication, and connection restrictions.

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

Typically, the management network is the organization's Intranet, while the custom network is an environment isolated from the Intranet, such as a test network with Internet connection.

Items to Prepare

Requirement	Details
Activation Code	Obtain from Trend Micro
Monitor and VGA cable	Connects to the VGA port of the appliance
USB keyboard	Connects to a USB port of the appliance
USB mouse	Connects to a USB port of the appliance
Ethernet cables	Connect to the management and data ports • Required: Management port (eth0) of the appliance to the management network • Recommended: Data port (eth1, eth2, or eth3) connects to the custom network • Optional: Unused data ports connect to the mail network for mail routing and monitoring

Requirement	Details
Internet-enabled computer	Access to the management console from a computer with the following software installed: A supported web browser: • Microsoft Internet Explorer® 9, 10, 11 • Microsoft Edge™ • Google Chrome™ 32 or later • Mozilla Firefox® 24 or later
IP addresses	• Required: One IPv4 address in the management network • Recommended: One IPv4 address for the custom network • Optional: Two IPv4 addresses for the mail network and one IPv6 address for the management network
Third party software licenses	Licenses for all third party software installed on sandbox images

Chapter 3

Installation

Topics include:

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 3-1. Minimum Software Requirements

APPLICATION	REQUIREMENTS	DETAILS
SSH client	SSH protocol version 2	Set the Command Line Interface terminal window size to 80 columns and 24 rows.
Internet Explorer™	Versions 9, 10, 11	Use only a supported browser to access the management console. 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 4-12*.
- Internet Explorer requires additional configuration. For details, see *Configuring Internet Explorer on page 3-3*.

Control Manager System Requirements

Control Manager is a separately licensed product. For information about Control Manager system requirements, go to:

http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx

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**.

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 3-2. 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.

Installing TippingPoint Advanced Threat Protection for Email

Important

The TippingPoint Advanced Threat Protection for Email appliance comes with the appliance software installed. The following procedure provides a reference for fresh installs only.

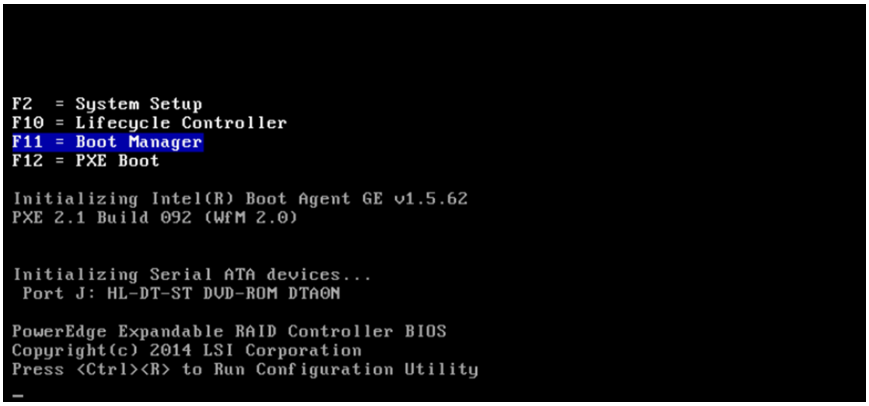
Trend Micro provides the TippingPoint Advanced Threat Protection for Email appliance hardware. No other hardware is supported. For information about software requirements, see *System Requirements on page 3-2*.

WARNING!

The installation deletes any existing data or partitions on the selected disk. Back up existing data before installing TippingPoint Advanced Threat Protection for Email.

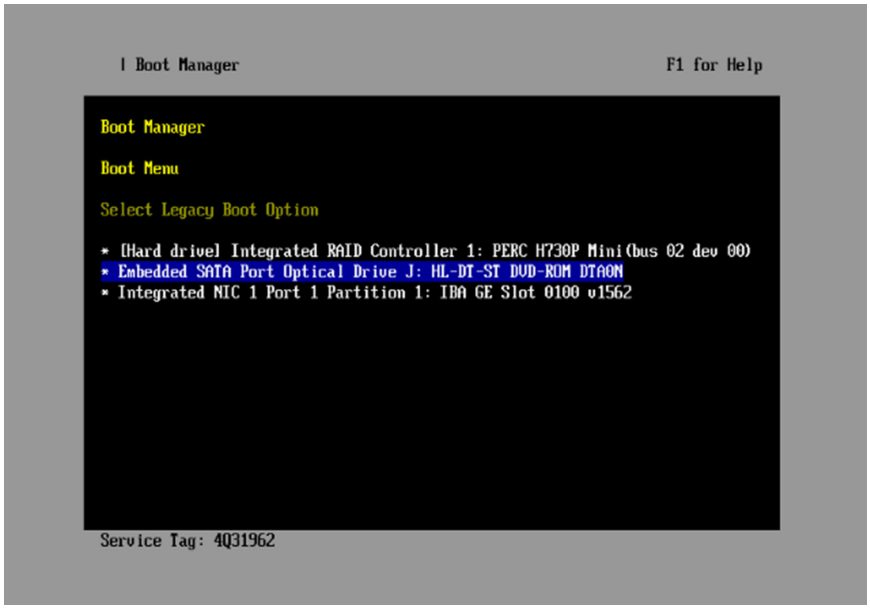
Procedure

1. Power on the server.
2. Insert the TippingPoint Advanced Threat Protection for Email Installation DVD into the optical disc drive.
3. Restart the server.
4. Press the F11 key.



5. Under **Boot Manager Main Menu**, select **BIOS Boot Manager** and then press ENTER.

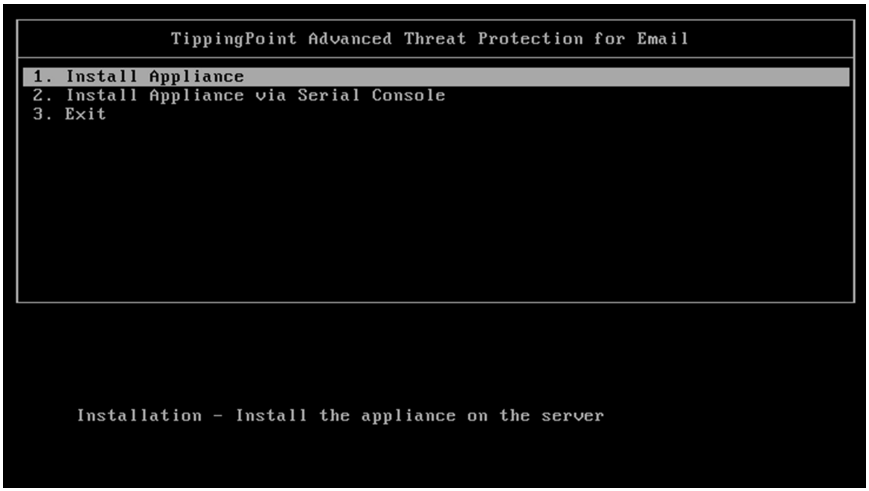
6. Select the optical disc drive that contains the Installation DVD and then press ENTER.



The server boots from the TippingPoint Advanced Threat Protection for Email Installation DVD and the installation begins.

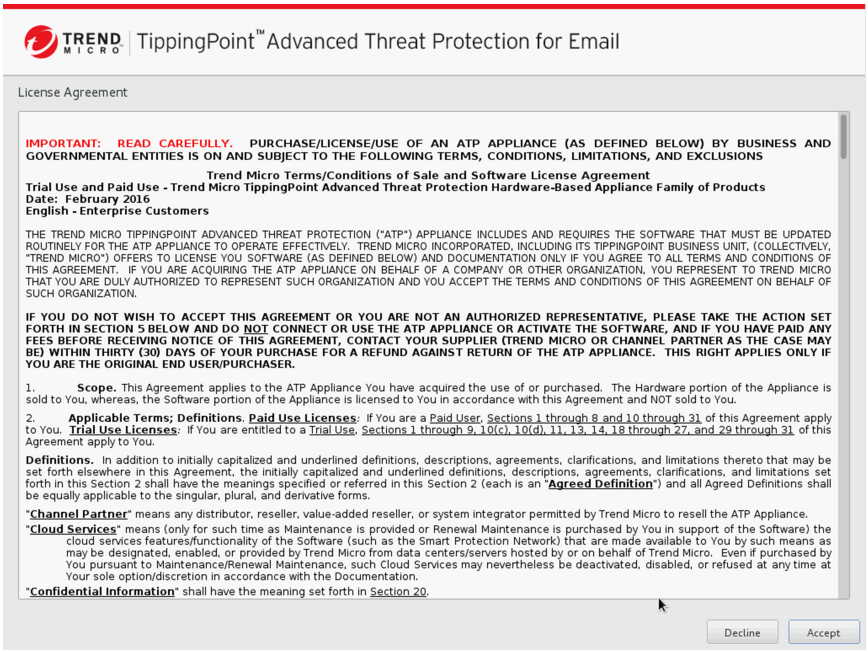
The **TippingPoint Advanced Threat Protection for Email Installation Menu** screen appears.

7. Select **Install Appliance**.

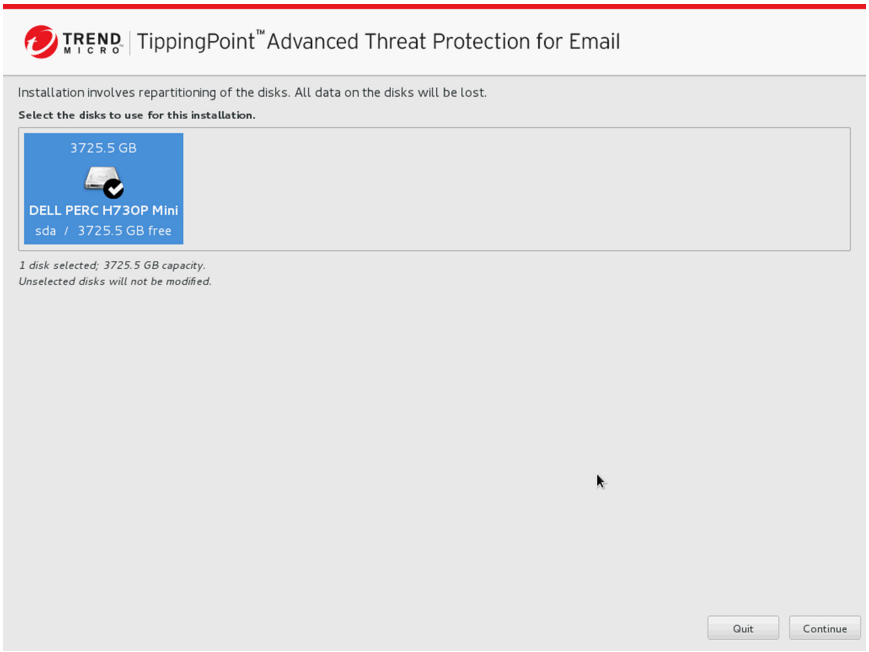


After the setup initializes, the **License Agreement** screen appears.

8. Click **Accept**.



9. Select the device to install TippingPoint Advanced Threat Protection for Email.



10. Click **Continue**.

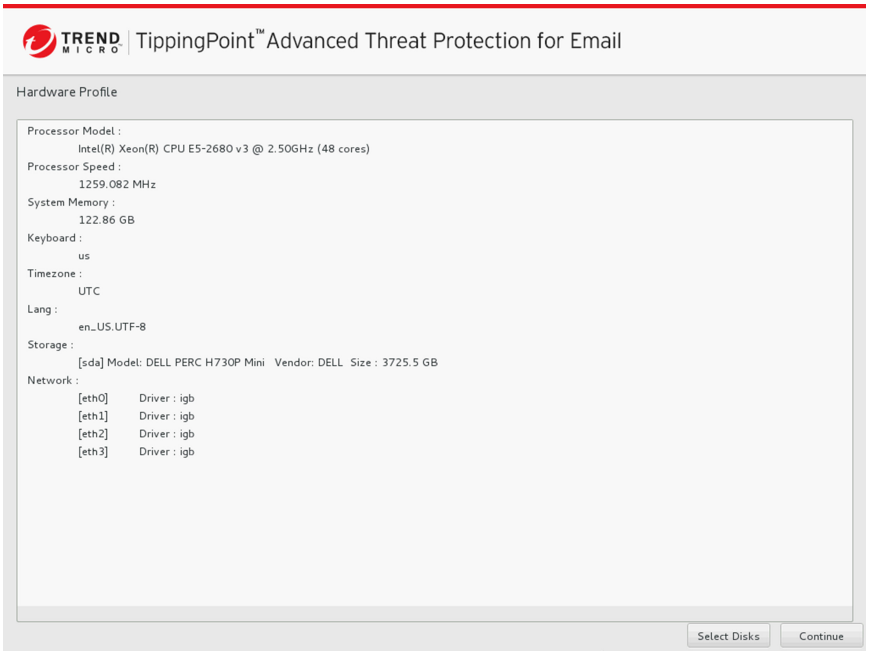
11. At the warning message, click **Yes** to continue.

    The TippingPoint Advanced Threat Protection for Email installer scans the hardware to determine that it meets the minimum specifications.

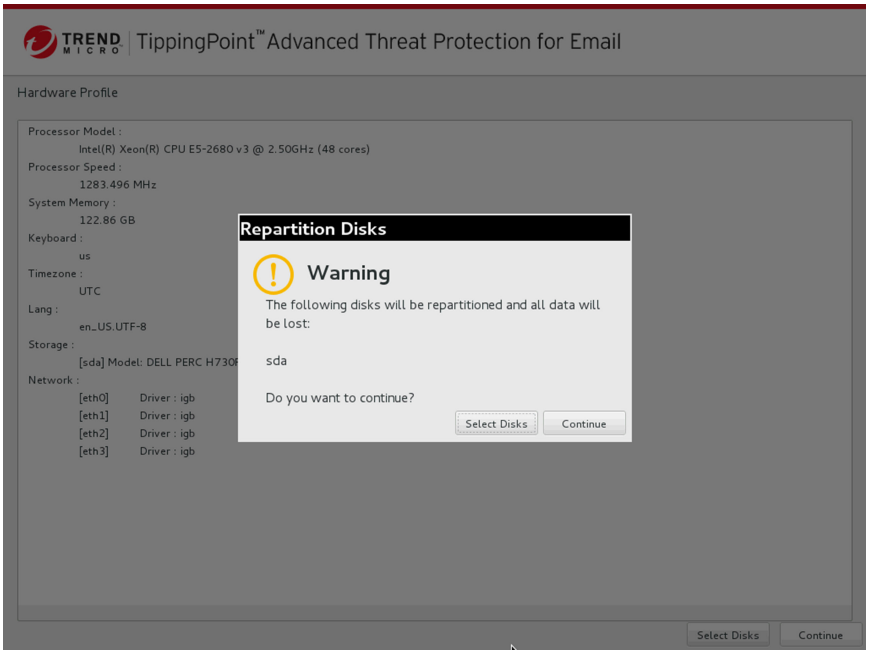
12. Click **Next**.

    The **Summary** screen appears.

13. Click **Continue** to begin the installation.



14. At the warning message, click **Continue**.



After formatting the disk, the program installs the operating system. The TippingPoint Advanced Threat Protection for Email appliance installs after the appliance restarts.

15. Remove the Installation DVD from the optical disc drive to prevent reinstallation.

Chapter 4

Using the Command Line Interface

Topics include:

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 4-2*.

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 4-4*.

configure product management-port

TABLE 4-1. 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 4-2. 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 4-3. 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 4-4. 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 4-5. 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 4-6. 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 4-7. 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 4-8. 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 4-9. 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 4-10. 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 4-11. 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 4-12. 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 4-13. 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 4-14. 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 4-15. 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 4-16. 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 4-17. 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 4-18. 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 4-19. enable

Enters privileged mode so privileged commands can be provided.	
Syntax: `enable`	
View	Normal
Parameters	None
Example:	

To enter privileged mode: `enable`

exit

TABLE 4-20. 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 4-21. help

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

To display the CLI help information: `help`

history

TABLE 4-22. 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 4-23. logout

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

To logout from the current session: `logout`

ping

TABLE 4-24. 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 4-25. 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 4-26. 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 4-27. 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 4-28. 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 4-29. 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 4-30. 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 4-31. 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 4-32. 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 4-33. 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 4-34. 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 4-35. 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 4-36. 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 4-37. 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 4-38. 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 4-39. 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 4-40. 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 4-41. 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 4-42. 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 4-43. 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 4-44. 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 4-45. 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 4-46. 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 4-47. 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`	

Chapter 5

Technical Support

Learn about the following topics:

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

1. Go to http://esupport.trendmicro.com.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** 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

Getting Started

Topics include:

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 A-4*.

2. Open the management console.

   For details, see *Opening the Management Console on page A-5*.

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

   For details, see *Managing Your Product License on page A-7*.

4. Configure the system time.

   For details, see *Configuring System Time on page A-7*.

5. Configure network settings.

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

6. Configure the notification SMTP server.

   For details, see *Configuring the Notification SMTP Server on page A-10*.

7. Configure the mail limits and exceptions.

   For details, see *Configuring Limits and Exceptions on page A-11*.

8. Configure Virtual Analyzer custom network settings.

   For details, see *Configuring Virtual Analyzer Network and Filters on page A-13*.

9. Import Virtual Analyzer images.

   For details, see *Importing Virtual Analyzer Images on page A-13*.

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 A-14*.

11. Configure email routing for downstream MTAs.

    For details, see *Configuring Message Delivery Settings on page A-15*.

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

    For details, see *Alerts on page A-16*.

13. (Optional) Configure policy rules.

    For details, see *Configuring the Actions on page A-16*.

14. (Optional) Configure policy exceptions.

    For details, see *Policy Exceptions on page A-18*.

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

    For details, see *Control Manager Settings on page A-19*.

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.

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 3-2*.

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

   Important

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

   For details, see the *TippingPoint Advanced Threat Protection for Email Administrator's Guide*.

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.

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**.

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.

For details about the available operating modes, see *Network Topology Considerations on page 2-2*.

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. **Note** BCC mode and SPAN/TAP mode are not available when the notification SMTP server is configured as internal Postfix.

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

   For details on adding a monitoring rule, see *TippingPoint Advanced Threat Protection for Email Administrator's Guide*.

Configuring the Notification SMTP Server

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

Procedure

1. Go to **Administration** > **System Settings** > **Notification SMTP**.
2. 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.

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

3. Click **Save**.

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**.

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. Select an image source and configure the applicable settings.
   - **Local or network folder**
   - **HTTP or FTP server**

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.
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.
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**.

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**.

Configuring Message Delivery Settings

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

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**.

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.

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
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**.

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.

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.

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

- Register to a Control Manager server.
- Check the connection status between ATP Email and Control Manager.
- Unregister from a Control Manager server.

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.

Index

TREND MICRO INCORPORATED

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

www.trendmicro.com

Item Code: APEM27308/160118