Best Practice Guide for Advanced Malware Protection (AMP) on Cisco Email Security

Contents

Introduction
Verify Feature Keys
Enable Advanced Malware Protection (AMP)
Customize Advanced Malware Protection (AMP) global settings
File Analysis threshold setting
Integrate ESA with AMP for Endpoints Console
Enable Mailbox Auto Remediation (MAR)
Configure Advanced Malware Protection (AMP) in mail policy
Integrate SMA with Cisco Threat Response (CTR)
Conclusion

Introduction

Advanced Malware Protection (AMP) is a comprehensive solution that enables malware detection and blocking, continuous analysis and retrospective alerting. Taking advantage of AMP with Cisco Email Security allows superior protection across the attack continuum – before, during, and after an attack with the most cost-effective, easily deployed approach to advanced malware defense.

This best practice document will cover the key features of AMP on the Cisco Email Security Appliance (ESA) as listed below:

- **File Reputation** - captures a fingerprint of each file as it traverses the ESA and sends it to AMP's cloud-based intelligence network for a reputation verdict. Given these results, you can automatically block malicious files and apply administrator-defined policy.
- **File Analysis -** provides the ability to analyze unknown files that are traversing the ESA. A highly secure sandbox environment enables AMP to glean precise details about the file's behavior and to combine that data with detailed human and machine analysis to determine the file's threat level. This disposition is then fed into AMP cloud-based intelligence network and used to dynamically update and expand the AMP cloud data set for enhanced protection.
- **Mailbox Auto Remediation (MAR)** – for Microsoft Office 365 and Exchange 2013/2016 automates the removal of emails with files that become malicious after the initial point of inspection. This saves administrators hours of work and helps contain a threat's impact.
- **Cisco AMP Unity** – is the capability that allows an organization to register its AMP-enabled device including ESA with AMP subscription in the AMP for Endpoints Console. With such integration, Cisco Email Security can be seen and queried for sample observations the same way the AMP for Endpoints console already offers for endpoints and allows correlating file propagation data across all of the threat vectors in a single user interface.
- **Cisco Threat Response** – is an orchestration platform that brings together security-related information from Cisco and third-party sources into a single, intuitive investigation and response console. It does so through a modular design that serves as an integration

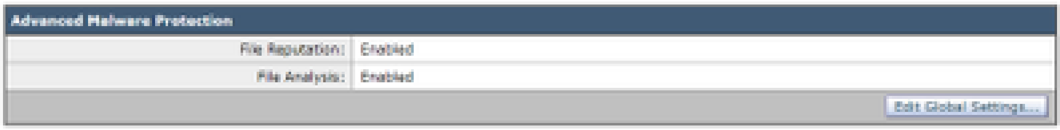
framework for event logs and threat intelligence. Modules allow for the rapid correlation of data by building relationship graphs that in turn, enable security teams to obtain a clear view of the attack, as well as to quickly make effective response actions.

Verify Feature Keys

- On the ESA, navigate to **System Administration**> **Feature Keys**
- Look for File Reputation and File Analysis feature keys and make sure the statuses are **Active**

Enable Advanced Malware Protection (AMP)

- On the ESA, navigate to **Security Services** >**Advanced Malware Protection – File Reputation and Analysis**
- Click the **Enable** button on **Advanced Malware Protection** Global Settings:



Advanced Malware Protection

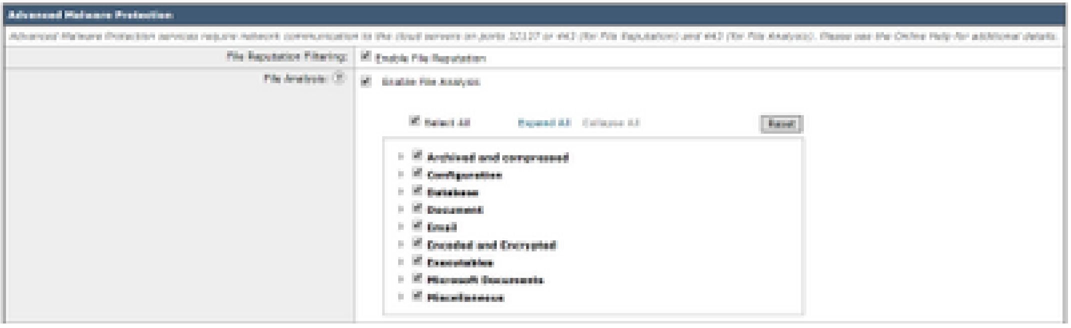
File Reputation: Enabled

File Analysis: Enabled

- **Commit** your changes.

Customize Advanced Malware Protection (AMP) global settings

- AMP is now enabled, click **Edit Global Settings** to customize the global settings.
- The list of file extensions will be automatically updated from time to time, so please always visit this setting and ensure all file extensions are selected:



Advanced Malware Protection

Advanced Malware Protection services require network communication to the cloud servers on ports 32137 or 443 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.

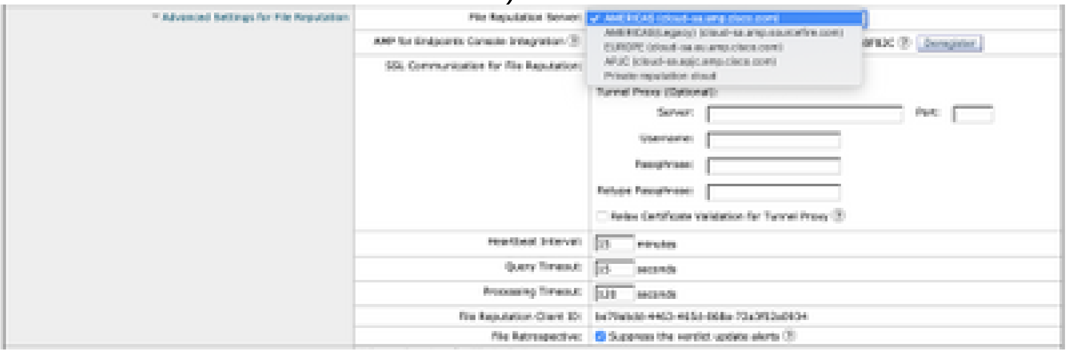
File Reputation Filtering: ☑ Enable File Reputation

File Analysis: ☑ Enable File Analysis

☑ Select All

- ☑ Archived and compressed
- ☑ Configuration
- ☑ Database
- ☑ Document
- ☑ Email
- ☑ Encoded and Encrypted
- ☑ Executables
- ☑ Microsoft Documents
- ☑ Miscellaneous

- Expand **Advanced settings for File Reputation**
- The default selection for File Reputation Server is **AMERICA (cloud-sa.amp.cisco.com)**
- Click the drop-down menu and choose the nearest File Reputation Servers (especially for APJC and EUROPE customers):



▾ Advanced Settings for File Reputation

File Reputation Server: ✓ AMERICAS (cloud-sa.amp.cisco.com)

AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com)
EUROPE (cloud-sa.eu.amp.cisco.com)
APJC (cloud-sa.apjc.amp.cisco.com)
Private reputation cloud
Deregister

AMP for Endpoints Console Integration: [illegible]

SSL Communication for File Reputation:

Tunnel Proxy (Optional):

Server: Port:

Username:

Passphrase:

Retype Passphrase:

□ Relax Certificate Validation for Tunnel Proxy

Heartbeat Interval: 15 minutes

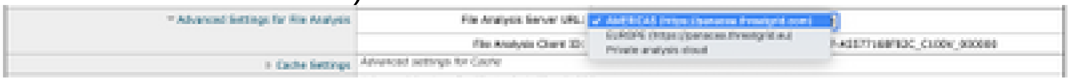
Query Timeout: 15 seconds

Processing Timeout: 120 seconds

File Reputation Client ID: [illegible]

File Retrospective: ☑ Suppress the verdict update alerts

- Expand **Advanced settings for File Analysis**
- The default selection for the File Analysis Server URL is **AMERICAS (https://panacea.threatgrid.com)**
- Click the drop-down menu and choose the nearest File Reputation Servers (especially for EUROPE customers):



▾ Advanced Settings for File Analysis

File Analysis Server URL: ✓ AMERICAS (https://panacea.threatgrid.com)
EUROPE (https://panacea.threatgrid.eu)
Private analysis cloud

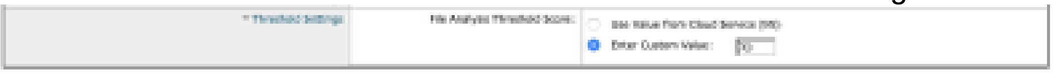
File Analysis Client ID: …-4157716BF82C_C100V_000000

▸ Cache Settings
Advanced settings for Cache

File Analysis threshold setting

(Optional) You are allowed to set the upper threshold limit for the acceptable file analysis score. The files that are blocked based on Threshold Settings are displayed as Custom Threshold in the Incoming Malware Threat Files section of the Advanced Malware Protection report.

- In the AMP global setting page, expand **Threshold** Settings.
- The default value from the cloud service is **95**.
- Choose the radio button of **Enter Custom Value** and change the value (for example 70):



▾ Threshold Settings

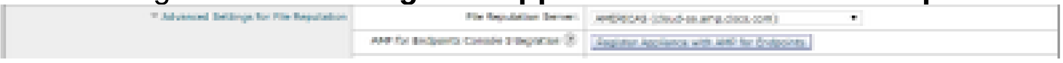
File Analysis Threshold Score:
○ Use Value From Cloud Service (95)
● Enter Custom Value: 70

- Click **Submit andCommit** your changes

Integrate ESA with AMP for Endpoints Console

(Only for AMP for Endpoints customer) A unified custom file Blocklist (or a file Allowlist) can be created through the AMP for Endpoints console and can seamlessly distribute the containment strategy across the security architecture including the ESA.

- In the AMP global setting page, expand **Advanced settings for File Reputation**
- Clicking the button – **Register Appliance with AMP for Endpoints**:

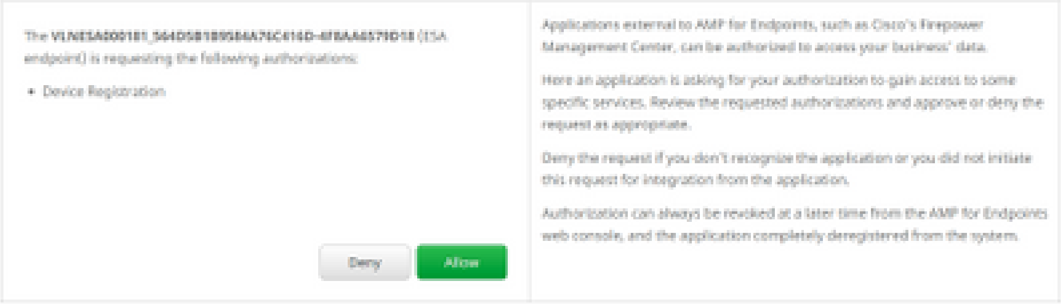


▾ Advanced Settings for File Reputation

File Reputation Server: AMERICAS (cloud-sa.amp.cisco.com)

AMP for Endpoints Console Integration ?: Register Appliance with AMP for Endpoints

- Click **OK** to redirect to the AMP for Endpoints console site to complete the registration.
- Log in to the AMP for Endpoints console with your user credential
- Click **Allow** authorizing the ESA registration:



The **VLNESA000181_564D5B1B9584A76C416D-4F8AA6579D18** (ESA endpoint) is requesting the following authorizations:

- Device Registration

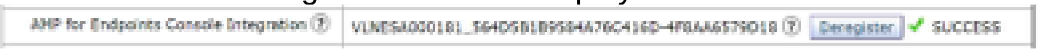
Applications external to AMP for Endpoints, such as Cisco's Firepower Management Center, can be authorized to access your business' data.

Here an application is asking for your authorization to gain access to some specific services. Review the requested authorizations and approve or deny the request as appropriate.

Deny the request if you don't recognize the application or you did not initiate this request for integration from the application.

Authorization can always be revoked at a later time from the AMP for Endpoints web console, and the application completely deregistered from the system.

- The AMP for Endpoints console automatically pivots the page back to ESA.
- Make sure the registration status display as **SUCCESS**:



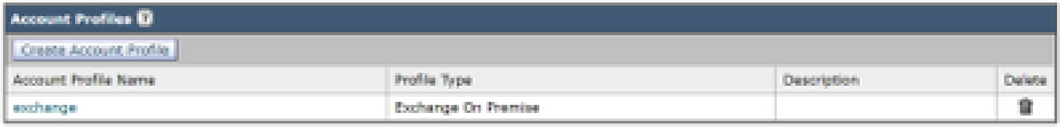
AMP for Endpoints Console Integration ?: VLNESA000181_564D5B1B9584A76C416D-4F8AA6579D18 ? Deregister ✓ SUCCESS

- Click **Submit** and **Commit** your changes

Enable Mailbox Auto Remediation (MAR)

If you have O365 mailboxes or Microsoft Exchange 2013/2016, Mailbox Auto Remediation (MAR) feature will allow the action to be taken when the file reputation verdict change from Clean/Unknown to Malicious.

- Navigate to **System Administration** > **Account Settings**
- Under **Account Profile**, click **Create Account Profile** to create an API connection profile with your Office 365 and/or Microsoft Exchange's mailboxes:



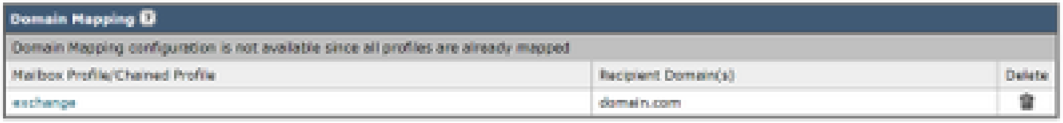
Account Profiles

Create Account Profile

Account Profile Name	Profile Type	Description	Delete
exchange	Exchange On Premise		🗑

- Click **Submit** and **Commit** your changes

- (Optional) Chained Profile is a collection of profiles, you only configure chained profile when accounts to be accessed reside across different tenants of different kinds of deployments.
- Click **Create Domain Mapping** button to map your account profile with the recipient domain. The recommended settings are shown below:



Domain Mapping

Domain Mapping configuration is not available since all profiles are already mapped

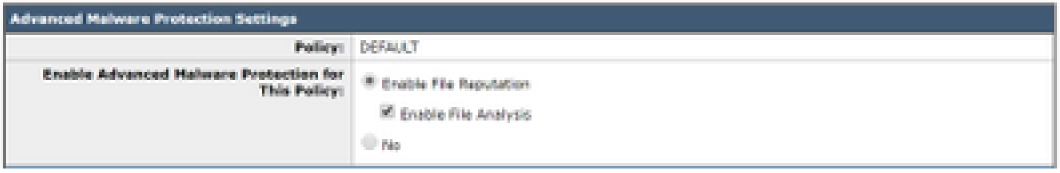
Mailbox Profile/Chained Profile	Recipient Domain(s)	Delete
exchange	domain.com	🗑

- Click **Submit** and **Commit** your changes

Configure Advanced Malware Protection (AMP) in mail policy

Once AMP and MAR have been configured globally, you can now enable the services to mail policies.

- Navigate to **Mail Policies** > **Incoming Mail Policies**
- Customize **Advanced Malware Protection** settings for an Incoming Mail Policy by clicking the blue link under **Advanced Malware Protection** for the policy you wish to customize.
- For the purposes of this best practice document, click the radio button next to **Enable File Reputation** and select **Enable File Analysis**:

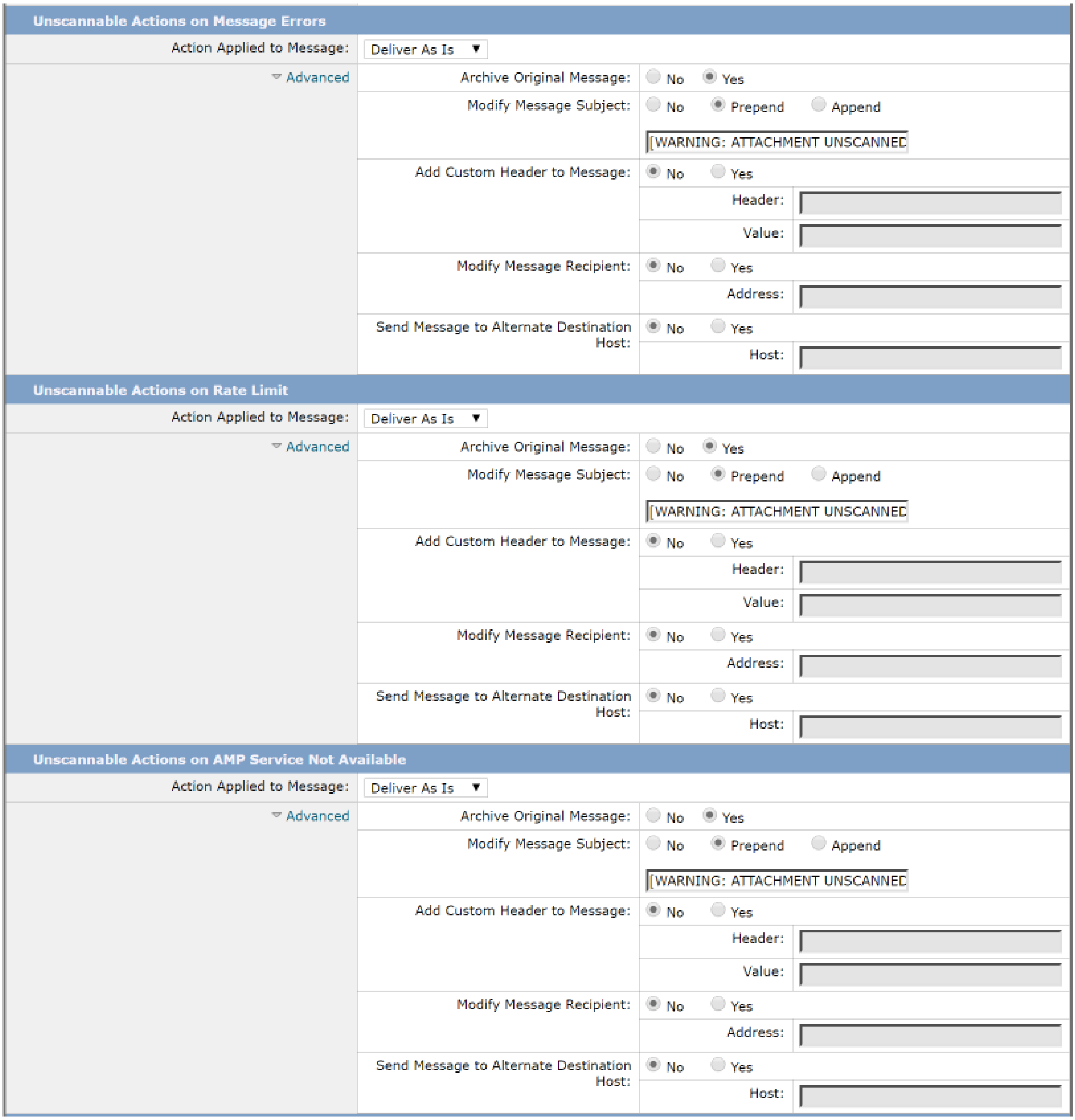


Advanced Malware Protection Settings

Policy: DEFAULT

Enable Advanced Malware Protection for This Policy:
● Enable File Reputation
☑ Enable File Analysis
○ No

- It is recommended to **include an X-header with the AMP result in a message**.
- The next three sections allow you to select the action that the ESA must perform if an attachment is considered as Unscannable due to message errors, rate limit or if the AMP service is not available. The recommended action is to **Deliver As-Is** with **warning text prepended on the message subject**:



Unscannable Actions on Message Errors

Action Applied to Message: Deliver As Is ▼

▿ Advanced

Archive Original Message: ○ No ● Yes

Modify Message Subject: ○ No ● Prepend ○ Append

[WARNING: ATTACHMENT UNSCANNED

Add Custom Header to Message: ● No ○ Yes

Header:

Value:

Modify Message Recipient: ● No ○ Yes

Address:

Send Message to Alternate Destination Host: ● No ○ Yes

Host:

Unscannable Actions on Rate Limit

Action Applied to Message: Deliver As Is ▼

▿ Advanced

Archive Original Message: ○ No ● Yes

Modify Message Subject: ○ No ● Prepend ○ Append

[WARNING: ATTACHMENT UNSCANNED

Add Custom Header to Message: ● No ○ Yes

Header:

Value:

Modify Message Recipient: ● No ○ Yes

Address:

Send Message to Alternate Destination Host: ● No ○ Yes

Host:

Unscannable Actions on AMP Service Not Available

Action Applied to Message: Deliver As Is ▼

▿ Advanced

Archive Original Message: ○ No ● Yes

Modify Message Subject: ○ No ● Prepend ○ Append

[WARNING: ATTACHMENT UNSCANNED

Add Custom Header to Message: ● No ○ Yes

Header:

Value:

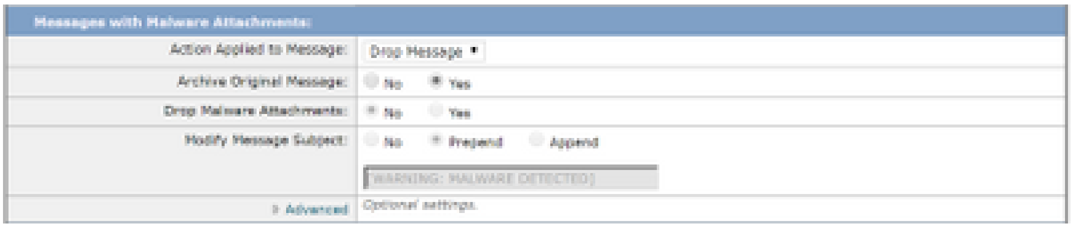
Modify Message Recipient: ● No ○ Yes

Address:

Send Message to Alternate Destination Host: ● No ○ Yes

Host:

- The next section will configure the ESA to drop the message if an attachment is considered malicious:



Messages with Malware Attachments:

Action Applied to Message: Drop Message ▼

Archive Original Message: ○ No ● Yes

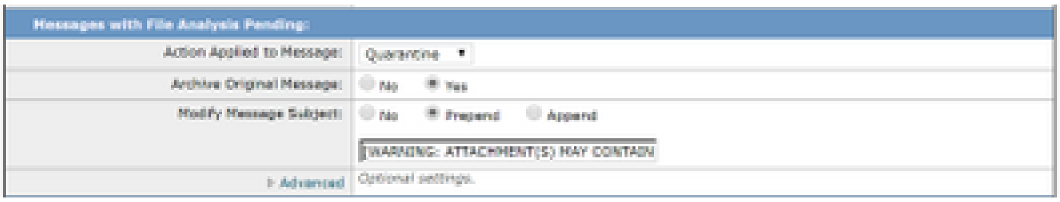
Drop Malware Attachments: ● No ○ Yes

Modify Message Subject: ○ No ● Prepend ○ Append

[WARNING: MALWARE DETECTED]

▹ Advanced Optional settings.

- The recommended action is to quarantine the message if the attachment is sent for File Analysis:



Messages with File Analysis Pending:

Action Applied to Message: Quarantine

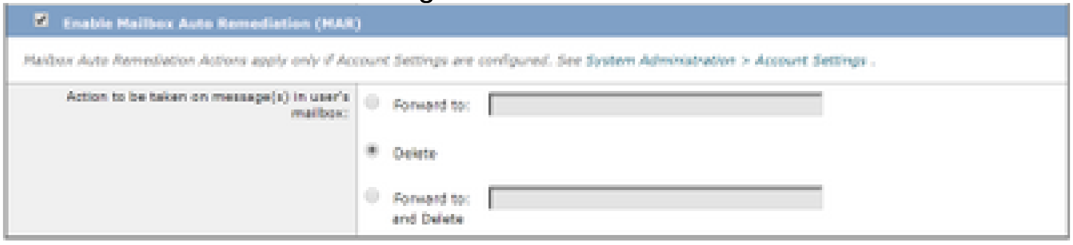
Archive Original Message: ○ No ● Yes

Modify Message Subject: ○ No ● Prepend ○ Append

[WARNING: ATTACHMENT(S) MAY CONTAIN

▸ Advanced Optional settings.

- (For incoming mail policy only) Configure the remedial actions to be performed on the message delivered to end-users when the threat verdict changes to malicious.
  The recommended settings are shown below:



☑ Enable Mailbox Auto Remediation (MAR)

Mailbox Auto Remediation Actions apply only if Account Settings are configured. See System Administration > Account Settings .

Action to be taken on message(s) in user's mailbox:

○ Forward to:

● Delete

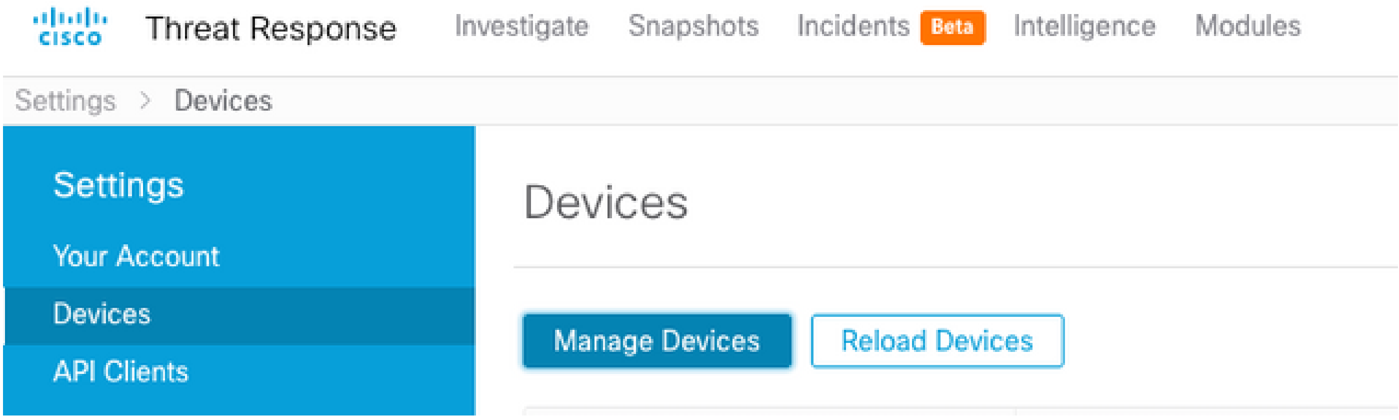
○ Forward to: and Delete

- Click **Submit** and **Commit** your changes

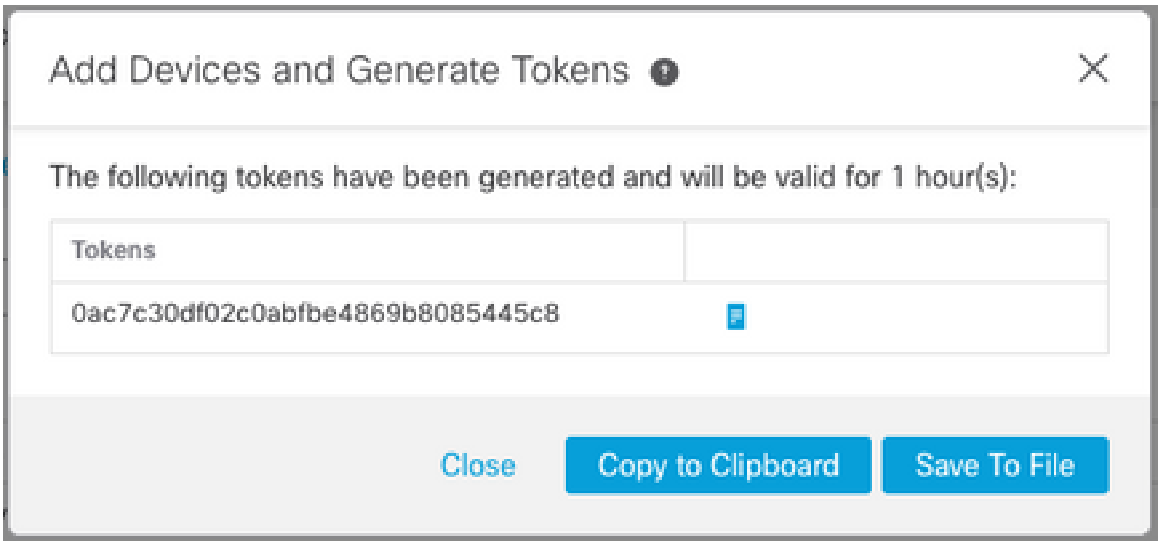
Integrate SMA with Cisco Threat Response (CTR)

The integration of an SMA Email module requires the use of the Security Services Exchange (SSE) via CTR. SSE allows an SMA to register with the Exchange and you provide explicit permission for Cisco Threat Response to access the registered devices. The process involves linking your SMA to SSE via a token that is generated when you are ready to link it.

- On the CTR portal (https://visibility.amp.cisco.com), log in with your user credentials.
- CTR uses a module to integrate with other Cisco security products including ESA. Click the **Modules** tab.
- Choose **Devices** and click **Manage Devices:**



- CTR will pivot the page to SSE.
- Click the **+** icon to generate a new token and click **Continue**.
- Copy the new token before closing the box:

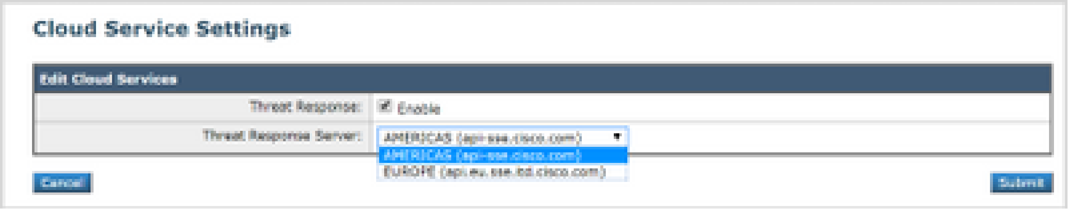


Add Devices and Generate Tokens

The following tokens have been generated and will be valid for 1 hour(s):

Tokens	
0ac7c30df02c0abfbe4869b8085445c8	

- On your SMA, navigate to **Management Appliances** tab > **Network** > **Cloud Service Settings**
- Click **Edit Setting** and make sure the Threat Response option is **Enable**.
- The default selection for Threat Response Server URL is **AMERICAS (api-sse.cisco.com).** For EUROPE customers, click the drop-down menu and choose **EUROPE (api.eu.sse.itd.cisco.com)**:



Cloud Service Settings

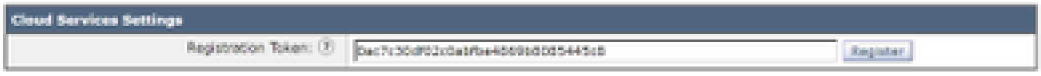
Edit Cloud Services

Threat Response: ☑ Enable

Threat Response Server: AMERICAS (api-sse.cisco.com)

AMERICAS (api-sse.cisco.com)
EUROPE (api.eu.sse.itd.cisco.com)
Cancel
Submit

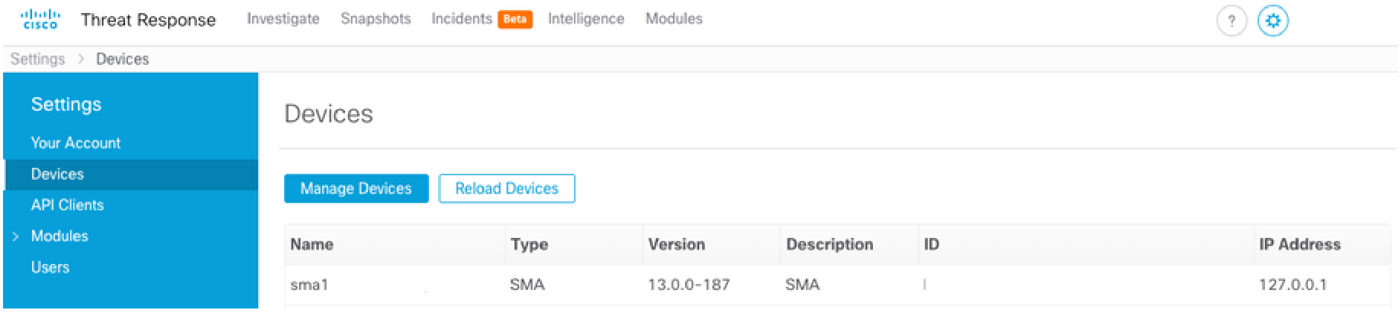
- Click **Submit** and **Commit** your changes
- Paste the token key (which you have generated from the CTR portal) in the Cloud Services Setting and click **Register**:



Cloud Services Settings

Registration Token: 0ac7c30df02c0abfbe4869b8085445c8

- It will take a while to complete the registration process, please navigate back to this page after a few minutes to check the status again.
- Return to **CTR** > **Modules** > **Device** and click the **Reload Device** button to make sure the SMA appears on the list:



Devices

Name	Type	Version	Description	ID	IP Address
sma1	SMA	13.0.0-187	SMA	I	127.0.0.1

Conclusion

This document aimed to describe the default or best practice configurations for Cisco Advanced Malware Protection (AMP) in the Email Security Appliance. Most of these settings are available on both the inbound and outbound email policies, and configuration and filtering are recommended in both directions.