

**Enabling AMP on Content  
Security Products (ESA/WSA)**  
January 2017  
Version 2.2



Bill Yazji  
[byazji@cisco.com](mailto:byazji@cisco.com)

## CONTENT SECURITY – AMP BEST PRACTICES

### Overview:

The vast majority of threats, attacks and nuisances faced by an organization often come through email in the form of spam, malware and blended attacks, as well as via normal every day web browsing.

Cisco's Email Security Appliances and Web Security Appliances include several different technologies and features to cut these threats off at the gateway, *before* they enter the organization, and this document will describe the best practice approaches to configuring our Advanced Malware Protection (AMP) feature.

Advanced Malware Protection – AMP is provided to detect and act upon known, unknown, zero day or targeted attacks. – including a File Reputation SHA lookup, automated cloud sandboxing of files, and retrospective alerting and detection of changes in the threat level of a file after it has left the email chain, or after the file is downloaded to the end user's workstation. The File Reputation and File Analysis Criteria for AMP for Cisco Content Security Products can be found [here](#).

This guide covers configuration and best practices on both the ESA and WSA products, along with general tips towards the end of the document.

## CONFIGURING AMP ON EMAIL SECURITY APPLIANCE (ESA)

### Email Security Appliance (ESA) Code Requirements:

- **Minimum ESA Version 9.7.2-065**
- **Current Recommendation v10.0.0-203**

### Security Management Appliance (SMA) Code Requirements:

- **Minimum SMA Version 10.0.0-055**
- **Current Recommendation v10.0.0-096**

While AMP has been supported on ESA on releases since v8.5.5, there has been significant reporting and functionality enhancements since the original release. Customers are strongly recommended to follow the above recommendations for an optimal experience.

When using a SMA for centralized reporting and message tracking, ensure the appropriately paired SMA release for the ESA release. You may reference the compatibility matrix [here](#).

### Confirming Advanced Malware Protection (AMP) Licensing

Confirm you have the appropriate licensing by navigating to *System Administration > Feature Keys*. You will need to have the File Reputation and File Analysis Keys listed and Active.

Description	Status	Time Remaining	Expiration Date
File Reputation	Active	333 days	19 Sep 2017 15:28 (GMT -07:00)
File Analysis	Active	333 days	19 Sep 2017 15:28 (GMT -07:00)

### Configuring Advanced Malware Protection (AMP)

Once the keys are confirmed, navigate to *Security Services > File Reputation and Analysis*

Under “Advanced Malware Protection,” click “Edit the Global Settings”

You will want to Enable File Reputation, and Enable File Analysis. Cisco recommends enabling file analysis for all File Types.

Advanced Malware Protection	
<small>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.</small>	
File Reputation Filtering:	<input checked="" type="checkbox"/> Enable File Reputation
File Analysis: ?	<input checked="" type="checkbox"/> Enable File Analysis
	File Types: <input checked="" type="checkbox"/> Adobe Portable Document Format (PDF) <input checked="" type="checkbox"/> Microsoft Office 2007+ (Open XML) <input checked="" type="checkbox"/> Microsoft Office 97-2004 (OLE) <input checked="" type="checkbox"/> Microsoft Windows / DOS Executable <input checked="" type="checkbox"/> Other potentially malicious file types
▸ Advanced Settings for File Reputation	<small>Advanced settings for File Reputation</small>
▸ Advanced Settings for File Analysis	<small>Advanced settings for File Analysis</small>

## AMP INSTALLATION AND BEST PRACTICES

By default, File Reputation communicates on port tcp/32137. As many customer environments do not have this port open, it may be required check the “Use SSL” checkbox under *Advanced Settings for File Reputation*. This will ensure communication over tcp/443, which is more commonly permitted. Additionally, you can configure the File Reputation query over a proxy in this same configuration area.

▼ Advanced Settings for File Reputation	Cloud Domain:	<input type="text" value="a.immunet.com"/>
	File Reputation Server:	AMERICAS (cloud-sa.amp.sourcefire.com) ▼
	SSL Communication for File Reputation:	<input checked="" type="checkbox"/> Use SSL (Port 443) Tunnel Proxy (Optional): Server: <input type="text"/>

The final configuration item would be to ensure all of the ESA devices are configured with the same Reporting Group ID. This permits a SMA to review all the File Analysis reports for all of the ESA’s sending files for File Analysis. Without this, you can only access the File Analysis reports via the ESA that submitted the file.

It is recommended to use something like COMPANYNAME-AMP. Despite the value recommendation below of a CCO ID, this is not an optimal item to use. If your organization already utilizes Threat Grid, and have access to use panacea.threatgrid.com, the naming should be based on the Organization name from panacea.threatgrid.com. This is found from looking at the User > My Account option on the Threat Grid portal. ***It is critical that every ESA has the same value in this space and that this matches what is configured on the SMA.***

In the event your organization has purchased a full ThreatGRID subscription, you are able to tie the samples from your ESA/SMA to this account. This can be achieved by opening a case with ThreatGRID support ([support@threatgrid.com](mailto:support@threatgrid.com)) and providing the Device IDs and Serial Numbers (or VLN) of your ESA/SMA architecture. More information can be found [here](#). Please take note to understand that if using a virtual ESA (ESAv), that the VLN is part of the ID used for the integration with the full ThreatGRID subscription. If the VLN license file changes and the VLN changes, this needs to be updated with ThreatGRID support.

Configuration on ESA: *Security Services > File Reputation and Analysis*. **Note:** It is critical to do this configuration at the machine level, not the cluster level.

Configuration on SMA: *Management Appliance > Centralized Services > Security Appliances*

Appliance Grouping for File Analysis Cloud Reporting

File Analysis Cloud Reporting Group ID: File Analysis Cloud Reporting Group ID Not Initialized

You can use any appliance in a group to view detailed File Analysis results in the cloud for files uploaded from any appliance in the group.

ID:

- Typically, this value will be your Cisco Connection Online ID (CCO ID).
- This ID is case-sensitive
- It must be configured identically on each appliance in the File Analysis Cloud Reporting Group. An appliance can belong to only one group per server.

This change will take effect immediately, without Commit. Once initialized, this value can only be reset by Cisco support.

[Add Appliance to Group](#)

## AMP INSTALLATION AND BEST PRACTICES

Once the above items are completed. Click Submit at the bottom of the screen, then Commit the changes.

The AMP configuration is now complete on the Email Security Appliance. Now, we must enable AMP services for the Incoming Mail flow. Note that AMP is not available for Outgoing Mail Policies.

Navigate to *Mail Policies > Incoming Mail Policies*. For the Incoming Mail Policy, the following settings are recommended.

Advanced Malware Protection Settings	
Policy:	DEFAULT
Enable Advanced Malware Protection for This Policy:	<input checked="" type="radio"/> Enable File Reputation <input checked="" type="checkbox"/> Enable File Analysis <input type="radio"/> No
<b>Message Scanning</b>	
	<input checked="" type="checkbox"/> (recommended) Include an X-header with the AMP results in messages
<b>Unscannable Attachments:</b>	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: ATTACHMENT UNSCANNED]
Advanced	Optional settings for custom header.
<b>Messages with Malware Attachments:</b>	
Action Applied to Message:	Drop Message
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Drop Malware Attachments:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: MALWARE DETECTED]
Advanced	Optional settings for custom header.
<b>Messages with File Analysis Pending:</b>	
Action Applied to Message:	Quarantine
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append [WARNING: ATTACHMENT(S) MAY CONTAIN
Advanced	Optional settings for custom header.

Cancel Submit

Incoming emails with a file attachment will be first checked with the File Reputation Services of AMP. The SHA256 hash for the file is queried to the AMP cloud. If the file is known “malicious” – the configuration section “Messages with Malware Attachments” [above] will be followed. The configuration above will have any email with a known malware attachment dropped.

In the event the File Reputation services determines the file is ‘unknown file,’ the ESA will determine if the file is a supported file type for File Analysis. Keep in mind that while File Reputation supports most file types for SHA lookup, File Analysis has a smaller subset of supported file types. If the file is a supported file type for File Analysis, and if the pre-classification engine on

## AMP INSTALLATION AND BEST PRACTICES

the ESA determines the file is one that could have malicious content, that file is sent to the cloud for File Analysis, and the configuration under “Messages with File Analysis Pending” [above] will be followed. The configuration above will have emails with files Pending Analysis be Quarantined based on the quarantine settings.

File Analysis quarantine settings are configured under:

*Monitor > Policy, Virus and Outbreak Quarantines* if on an ESA, and when using centralized quarantines on an SMA, under the Email Tab, then *Message Quarantine > Policy, Virus and Outbreak Quarantines*. Configuration of the File Analysis Quarantine is the same on either an ESA or SMA.

Click on the “File Analysis” Quarantine.

Policy, Virus and Outbreak Quarantines						
Add Policy Quarantine...		Search Across Quarantines				
Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
Bad Reputation Sender	Policy	1620	Retain 1 day 16 hours then Release	19 Oct 2016 13:30 (GMT -07:00)	497.9M	
DLP HIPAA	Policy	1	Retain 365 days then Delete	10 Jun 2016 13:37 (GMT -07:00)	67.48K	
DMARC_Quarantine	Policy	0	Retain 1 day 16 hours then Release	N/A	0	
File Analysis	Advanced Malware Protection	11	Retain 30 minutes then Release	19 Oct 2016 11:55 (GMT -07:00)	1.79M	

Cisco’s default Retention period is 1 hour, with a **minimum recommended** value of 30 minutes. Configuration is **not recommended** any shorter than 30 minutes. Once this time has expired, the Default Action will take place – either Delete or Release. The recommendation here is Release. If a customer chooses Delete, it is strongly recommended to have a longer Retention period.

Settings	
Quarantine Name:	File Analysis
Created On:	Not Available
Created by:	System
Size Used:	1.8M
Retention Period:	<input type="text" value="30"/> Minutes <input type="button" value="v"/>
Default Action:	<input type="radio"/> Delete <input checked="" type="radio"/> Release <input checked="" type="checkbox"/> Free up space by applying default action on messages upon space overflow Additional options to apply on Release action (when used for freeing up space) <ul style="list-style-type: none"> <li><input type="checkbox"/> Modify Subject</li> <li><input type="checkbox"/> Add X-Header</li> <li><input type="checkbox"/> Strip Attachments</li> </ul>
Local Users:	No users selected
Externally Authenticated Users:	External authentication is disabled. Go to System Administration > Users to enable external authentication.
Custom User Roles:	No roles selected

## Configuring AMP on Web Security Appliance (WSA)

### Web Security Appliance Code Requirements:

- **Minimum WSA Version v9.1.1-074**
- **Current Recommendation v9.1.1-074**

### Security Management Appliance (SMA) Code Requirements:

- **Minimum SMA Version 10.0.0-055**
- **Current Recommendation v10.0.0-096**

While AMP has been supported on WSA on releases since v8.0.5, there has been considerable reporting and functionality enhancements since the original release. Customers are strongly recommended to follow the above recommendations for an optimal experience.

When using a SMA for centralized reporting and message tracking, ensure the appropriately paired SMA release for the WSA release. You may reference the compatibility matrix [here](#).

### Confirming Advanced Malware Protection (AMP) Licensing

Confirm you have the appropriate licensing by navigating to *System Administration > Feature Keys*. You will need to have the File Reputation and File Analysis Keys listed and Active.

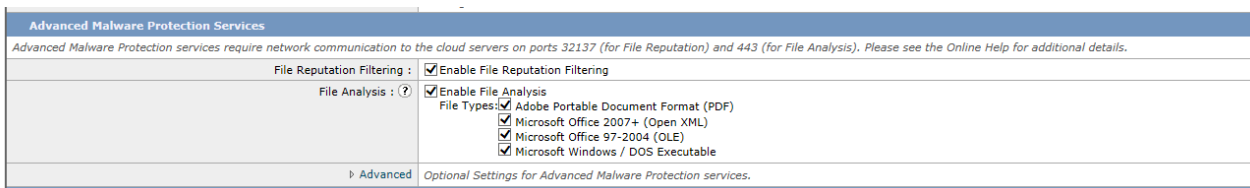
Description	Status	Time Remaining	Expiration Date
File Reputation	Active	333 days	19 Sep 2017 15:28 (GMT -07:00)
File Analysis	Active	333 days	19 Sep 2017 15:28 (GMT -07:00)

### Configuring Advanced Malware Protection (AMP)

Next, navigate to *Security Services > Anti-Malware and Reputation* in order to configure AMP.

Under “Advanced Malware Protection,” click “Edit the Global Settings”

You will want to Enable File Reputation, and Enable File Analysis. Cisco recommends enabling file analysis for all File Types.



By default, File Reputation communicates on port tcp/32137. As many customer environments do not have this port open, it may be required to check the “Use SSL” checkbox under *Advanced*

## AMP INSTALLATION AND BEST PRACTICES

*Settings for File Reputation.* This will ensure communication over tcp/443, which is more commonly permitted. Additionally, you can configure the File Reputation query over a proxy in this same configuration area.

Advanced	Routing Table:	Management
Advanced Settings for File Reputation		
File Reputation Server:	AMERICAS (cloud-sa.amp.sourcefire.com) ▼	
Cloud Domain:	cloud-sa.amp.sourcefire.com	
SSL Communication for File Reputation:	<input checked="" type="checkbox"/> Use SSL (Port 443)	
	Tunnel Proxy (optional):	
	Server:	Port: 80
	Username:	
	Passphrase:	
	Retype Passphrase:	
	<input type="checkbox"/> Relax Certificate Validation for Tunnel Proxy ?	

The final configuration item would be to ensure all of the WSA appliances are configured with the same Reporting Group ID. This permits a SMA to review all the File Analysis reports for all of the WSA's sending files for File Analysis. Without this, you can only access the File Analysis reports via the WSA that submitted the file.

It is recommended to use something like COMPANYNAME-AMP. Despite the value recommendation below of a CCO ID, this is not an optimal item to use. If your organization already utilizes Threat Grid, and have access to use panacea.threatgrid.com, the naming should be based on the Organization name from panacea.threatgrid.com. This is found from looking at the User > My Account option on the Threat Grid portal. ***It is critical that every WSA has the same value in this space and that this matches what is configured on the SMA.***

In the event your organization has purchased a full ThreatGRID subscription, you are able to tie the samples from your WSA/SMA to this account. This can be achieved by opening a case with ThreatGRID support ([support@threatgrid.com](mailto:support@threatgrid.com)) and providing the Device IDs and Serial Numbers (or VLN) of your WSA/SMA architecture. More information can be found [here](#). Please take note to understand that if using a virtual WSA (WSAv), that the VLN is part of the ID used for the integration with the full ThreatGRID subscription. If the VLN license file changes and the VLN changes, this needs to be updated with ThreatGRID support.

Configuration on WSA: *Security Services > File Reputation and Analysis*  
Configuration on SMA: *Management Appliance > Centralized Services > Security Appliances*

Appliance Grouping for File Analysis Cloud Reporting	
File Analysis Cloud Reporting Group ID:	File Analysis Cloud Reporting Group ID Not Initialized
	You can use any appliance in a group to view detailed File Analysis results in the cloud for files uploaded from any appliance in the group.
ID:	<input type="text"/>
	<ul style="list-style-type: none"><li>Typically, this value will be your Cisco Connection Online ID (CCO ID).</li><li>This ID is case-sensitive</li><li>It must be configured identically on each appliance in the File Analysis Cloud Reporting Group. An appliance can belong to only one group per server.</li></ul>
	<b>This change will take effect immediately, without Commit. Once initialized, this value can only be reset by Cisco support.</b>
	<a href="#">Add Appliance to Group</a>



## AMP INSTALLATION AND BEST PRACTICES

Once the above items are completed. Click Submit at the bottom of the screen, then Commit the changes.

You have successfully enabled the AMP services on the Web Security Appliance. Now, you must enable AMP services in the Access Policies. This configuration is quite simple.

Under *Web Security Manager > Access Policies* you will need to configure Advanced Malware Protection under the Anti-Malware and Reputation Column. Click on the blue “Advanced Malware Protection”

### Access Policies

Policies							
Add Policy...							
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	AP CEO Identification Profile: All	(global policy)	Block: 9 Warn: 5 Monitor: 75	(global policy)	(global policy)	(global policy)	
2	AP Finance Identification Profile: All 1 groups (AD CiscoSec\CISCOSEC\Finance)	(global policy)	Block: 9 Warn: 5 Monitor: 75	(global policy)	(global policy)	(global policy)	
3	AP Marketing Identification Profile: All 1 groups (AD CiscoSec\CISCOSEC\Marketing)	(global policy)	Block: 9 Warn: 5 Monitor: 75	(global policy)	(global policy)	(global policy)	
4	AP CentOS Identification Profile: Linux Generated Load All identified users	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	
	Global Policy Identification Profile: All	No blocked items	Block: 10 Warn: 6 Monitor: 67 Allow: 1 Redirect: 1	Monitor: 365	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Enabled Webroot: Enabled McAfee: Disabled Sophos: Enabled	

Edit Policy Order...

Once in the configuration, under “Advanced Malware Protection Settings” check the box to enable the “File Reputation and File Analysis” and configure the appliance to either Monitor or Block Known Malicious and High-Risk Files. Cisco recommends to Block these.

Advanced Malware Protection Settings		
<input checked="" type="checkbox"/> Enable File Reputation Filtering and File Analysis		
<i>File Reputation Filters will identify transactions containing known malicious or high-risk files. Files that are unknown may be forwarded to the cloud for File Analysis.</i>		
File Reputation	Monitor 	Block 
Known Malicious and High-Risk Files		

Downloaded files will be first checked with the File Reputation Services of AMP. The SHA256 hash for the file is queried to the AMP cloud. If the file is known “malicious” – the configuration section “Known Malicious and High-Risk Files” [above] will be followed. The configuration above will have any file with a known malware blocked from transfer to the end client.

In the event the File Reputation services determines the file is ‘unknown file,’ it will be passed to the end user. The WSA will determine if the file is a supported file type for File Analysis. Keep in mind that while File Reputation supports most file types for SHA lookup, File Analysis has a smaller subset of supported file types. The File Retrospection functionality will alert the administrator to any file that completes File Analysis with a “malicious” verdict. A report on the WSA (or SMA) will show what users downloaded these files for manual remediation.

## AMP INSTALLATION AND BEST PRACTICES

### Timing of Processes and Verdict Updates

- There is no Service Level Agreement for timing of AMP processes, all information here is best-effort based on current processing
- The File Analysis process can take between 10 minutes to 1 hour (estimated, with average being on the lower end). When File Analysis is complete, the updated disposition will be pushed to the AMP cloud
- After a verdict is updated in the cloud, it currently takes approximate an hour for the retrospective verdict to be reflected on your content security appliance.
- The ESA & SMA File Analysis Quarantine checks for File Analysis Completion every 5 minutes, upon updated verdict it will release/block the email per the quarantine configuration.
- The WSA & ESA File Retrospection process checks the AMP Cloud every 15 minutes for updated file disposition
- The WSA & ESA cache file dispositions and update via retrospective events. The cache lives forever unless we need to empty the space, in that event the least recently used are cleared.



---

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

## AMP INSTALLATION AND BEST PRACTICES