

Integrate Secure Endpoint Private Cloud with Secure Web and Email

Contents

[Introduction](#)

[Prerequisites](#)

[Components Used](#)

[Verification checks before proceeding with integration](#)

[Procedure](#)

[Configure the Secure Endpoint private cloud](#)

[Configure the Secure Web Appliance](#)

[Configure the Cisco Secure Email](#)

[The steps to fetch AMP logs from Secure Web and Email](#)

[Testing the integration between Secure Web Appliance and Secure Endpoint private cloud.](#)

[SWA Access Logs](#)

[SWA AMP Logs](#)

Introduction

This document describes the steps required to integrate Secure Endpoint private cloud with Secure Web Appliance (SWA) and Secure Email Gateway (ESA).

Prerequisites

Cisco recommends that you have knowledge of these topics:

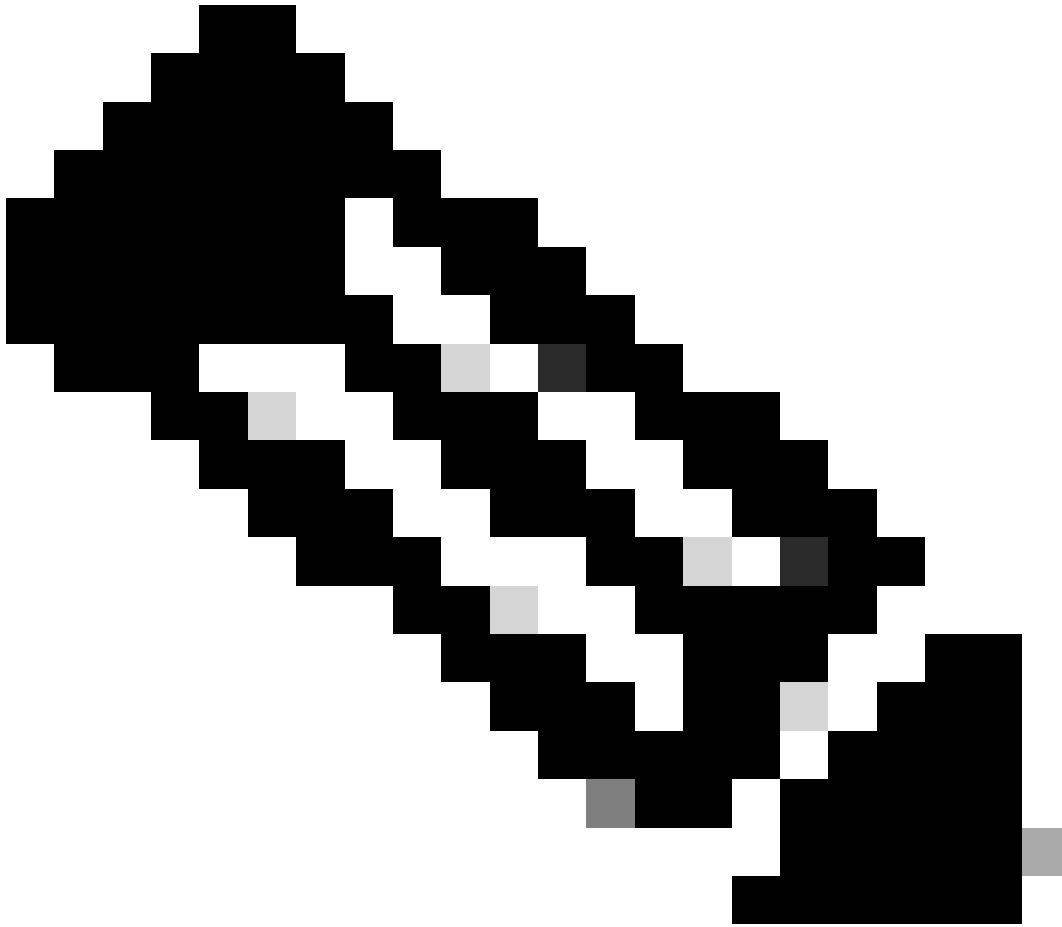
- Secure Endpoint AMP Virtual Private Cloud
- Secure Web Appliance(SWA)
- Secure Email Gateway

Components Used

SWA (Secure Web Appliance) 15.0.0-322

AMP virtual private cloud 4.1.0_202311092226

Secure Email Gateway 14.2.0-620



Note: The documentation is valid for both physical and virtual variations of all the products involved.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Verification checks before proceeding with integration

1. Verify if the **Secure Endpoint Private Cloud/SWA/Secure Email Gateway** has the required licenses. You can verify the feature key on **SWA/Secure Email** or check that the smart license is enabled.
2. **HTTPS Proxy** must be enabled on **SWA** if you are planning to inspect the **HTTPS** traffic. You need to decrypt the **HTTPS** traffic in order to do any file reputation checks.
3. The **AMP Private Cloud/Virtual Private Cloud** appliance and all the necessary certificates must be configured. Please refer to the **VPC certificate** guide for verification.

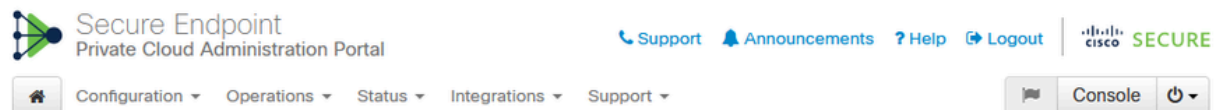
<https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/214326-how-to-generate-and-add-certificates-tha.html>

4. All hostnames of the products must be DNS resolvable. This is to avoid any connectivity issues or cert issues while integrating. On the Secure Endpoint private cloud, the Eth0 interface is for Admin access and Eth1 must be able to connect with integrating devices.

Procedure

Configure the Secure Endpoint private cloud

1. Log in to the Secure Endpoint VPC admin portal.
2. Go to “Configuration” > “Services” > “Disposition Server” > Copy the disposition server hostname (This can be also fetched from the third step) .
3. Navigate to “Integrations” > “Web Security Appliance”.
4. Download the “Disposition Server Public Key” & “Appliance Certificate Root” .
5. Navigate to “Integrations” > “Email Security Appliance”.
6. Select the version of your ESA and download the “Disposition Server Public Key” and “Appliance Certificate Root”.
7. Please keep both the cert and key safe. This must be uploaded to SWA/Secure Email later.



Connect Cisco Web Security Appliance to Secure Endpoint Appliance

Step 1: Web Security Appliance Setup

1. Go to the Web Security Appliance Portal.
2. Navigate to `Security Services > Anti-Malware and Reputation > Edit Global Settings...`
3. Enable the checkbox for Enable File Reputation Filtering.
4. Click `Advanced > Advanced Settings for File Reputation` and select Private Cloud under File Reputation Server.
5. In the Server field paste the Disposition Server hostname: `disposition.vpc1.nanganath.local`.
6. Upload your Disposition Server Public Key found below and select the Upload Files button.

Disposition Server Public Key Download

Step 2: Proxy Setting

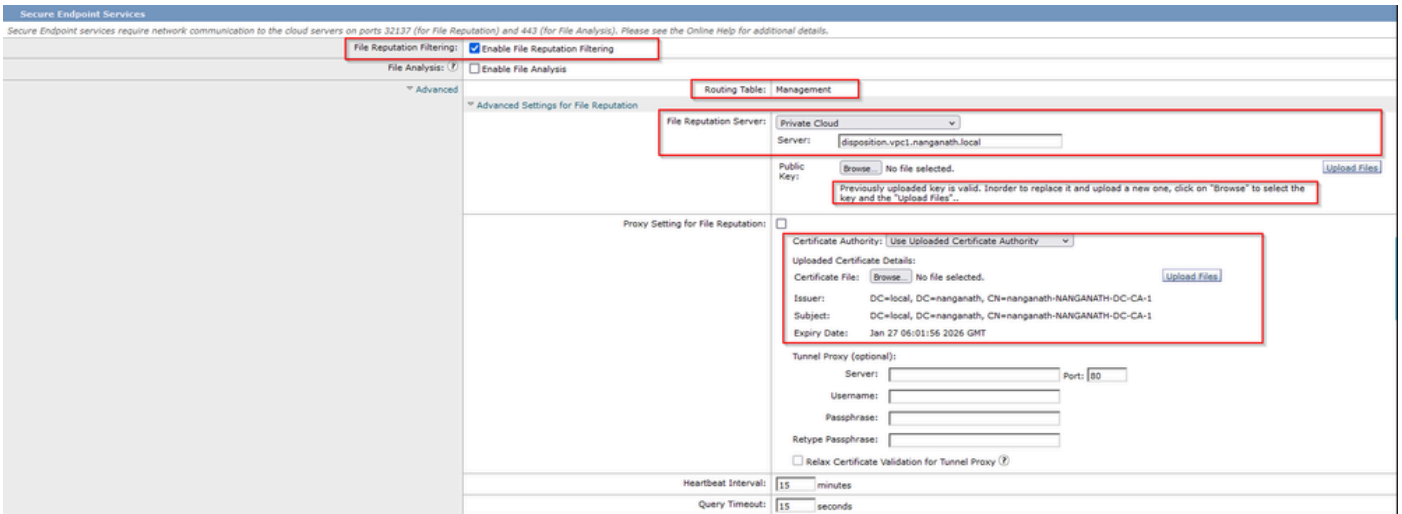
1. Continuing from Step 1 above, find the Proxy Setting for File Reputation section.
2. Choose Use Uploaded Certificate Authority from the Certificate Authority drop down.
3. Upload your Appliance Certificate Root found below and select the Upload Files button.
4. Click the Submit button to save all changes.

Appliance Certificate Root Download

Configure the Secure Web Appliance

1. Navigate to SWA GUI > “Security Services” > “Anti-Malware and Reputation” > Edit Global Settings
2. Under the section “Secure Endpoint Services” you can see the option “Enable File Reputation Filtering”, and "Check" this option shows a new field “Advanced”
3. Select “Private Cloud” in the File Reputation Server.
4. Provide the private cloud Disposition Server hostname as “Server”.
5. Upload the public key which you downloaded earlier. Click “Upload Files”.

6. There is an option to upload the Certificate Authority. Choose “Use Uploaded Certificate Authority” from the drop-down and upload the CA certificate that you downloaded earlier.
7. Submit the change
8. Commit the change

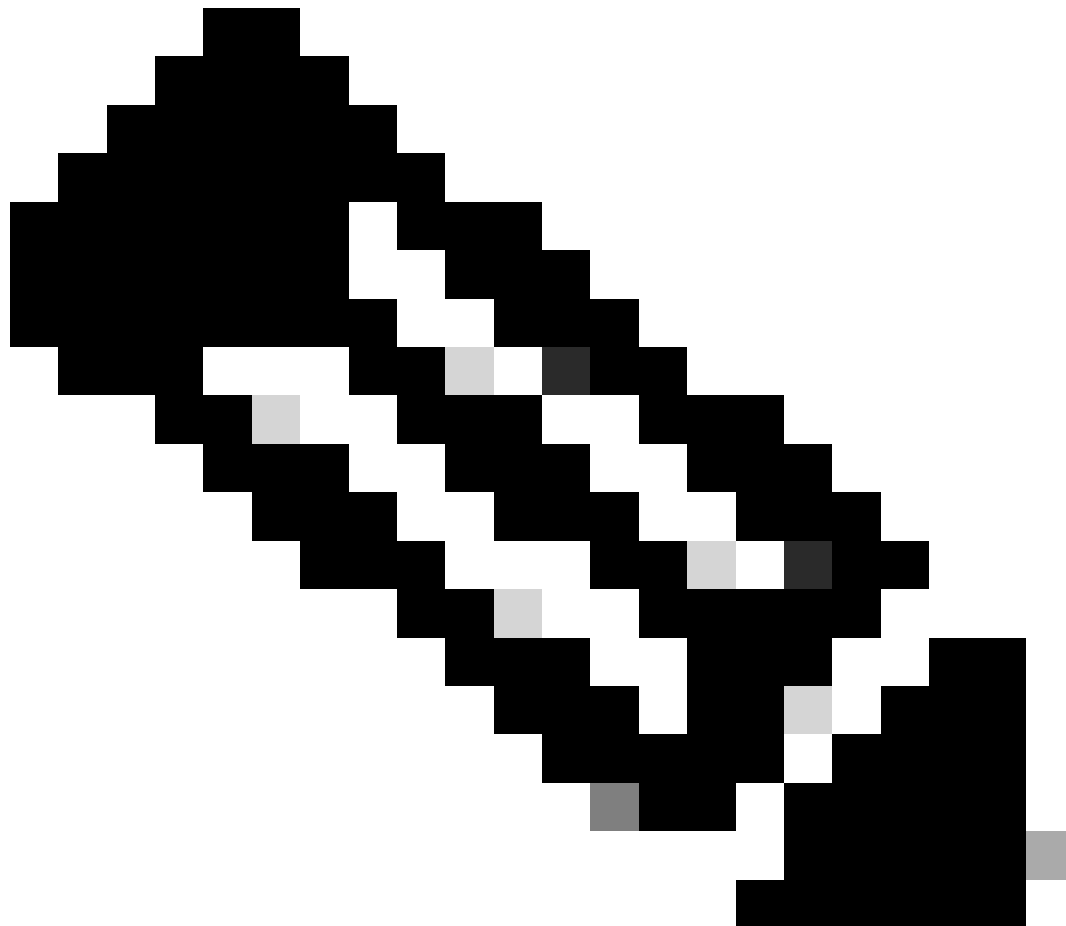


Configure the Cisco Secure Email

1. Navigate to Secure Email GUI > Security Services” > “File Reputation and Analysis” > Edit Global Settings > “Enable” or “Edit Global Settings”
2. Select “Private Cloud” in the File Reputation Server
3. Provide the private cloud Disposition Server hostname as “Server”.
4. Upload the public key which we downloaded earlier. Click “Upload Files”.
5. Upload the Certificate Authority. Choose “Use Uploaded Certificate Authority” from the drop-down and upload the CA certificate that you downloaded earlier.
6. Submit the change
7. Commit the change

Edit File Reputation and Analysis Settings

Advanced Malware Protection	
Advanced Malware Protection services require network communication to the cloud servers on ports 443 (for File Reputation and File Analysis). Please see the Online Help for additional details.	
File Reputation Filtering:	<input checked="" type="checkbox"/> Enable File Reputation
File Analysis: (?)	<input type="checkbox"/> Enable File Analysis
Advanced Settings for File Reputation	
File Reputation Server:	Private reputation cloud
Server:	disposition.vpc1.nanganath.local
Public Key:	<input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload File"/>
A valid public key has already been uploaded. To upload a new one, click on "Browse" to select the key and then the "Upload File".	
SSL Communication for File Reputation:	Use SSL (Port 443)
Tunnel Proxy (Optional):	
Server:	<input type="text"/>
Port:	<input type="text"/>
Username:	<input type="text"/>
Passphrase:	<input type="text"/>
Retype Passphrase:	<input type="text"/>
<input type="checkbox"/> Relax Certificate Validation for Tunnel Proxy (?)	
Heartbeat Interval:	15 minutes
Query Timeout:	20 seconds
Processing Timeout:	120 seconds
File Reputation Client ID:	cb1b31fc-9277-4008-a396-6cd486ecc621
File Retrospective:	<input type="checkbox"/> Suppress the verdict update alerts (?)
Cache Settings	Advanced settings for Cache
Threshold Settings	Advanced Settings for File Analysis Threshold Score



Note: Cisco Secure Web Appliance & Cisco Secure Email Gateway are based on AsyncOS and share almost the same logs when the file reputation gets initialized. The AMP log can be observed in Secure Web Appliance or Secure Email Gateway AMP logs (Similar logs in both devices). This only indicates that the service is initialized on the SWA and Secure Email Gateway. It did not indicate the connectivity was fully successful. If there are any connectivity or certificate issues, then you can see errors after the "File Reputation initialized" message. Mostly it indicates an "Unreachable error" or "certificate Invalid" error.

The steps to fetch AMP logs from Secure Web and Email

1. Log in to the SWA/Secure Email Gateway CLI and type the command "grep"
2. Select "amp" or "amp_logs"
3. Leave all other fields as it is and type "Y" to tail the logs. Tail the logs to show the live events. If you are looking for old events, then you can type the date in "regular expression"

```
Tue Feb 20 18:17:53 2024 Info: connecting to /tmp/reporting_listener.sock.root [try #0 of 20]
Tue Feb 20 18:17:53 2024 Info: connected to /tmp/reporting_listener.sock.root [try #0 of 20]
Tue Feb 20 18:17:53 2024 Info: File reputation service initialized successfully
Tue Feb 20 18:17:53 2024 Info: The following file type(s) can be sent for file analysis: Executables, Document,
Microsoft Documents, Database, Miscellaneous, Encoded and Encrypted, Configuration, Email, Archived and compress
ed. To allow analysis of new file type(s), go to Security Services > File Reputation and Analysis.
```

Testing the integration between Secure Web Appliance and Secure Endpoint private cloud.

There is no direct option to test the connectivity from SWA. You must inspect the logs or alerts to verify if there are any issues.

For simplicity, we are testing an HTTP URL instead of HTTPS. Please note that you need to decrypt the HTTPS traffic for any file reputation checks.

Configuration is done in SWA access policy and enforced the AMP scanning.

Note: Please review the SWA [user guide](#) to understand how to configure the policies on Cisco Secure Web Appliance.

Access Policies

Policies									
Add Policy...									
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	AP.Users Identification Profile: ID.Users All identified users	(global policy)	(global policy)	Monitor: 342	(global policy)	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Disabled	(global policy)		

Access Policies: Anti-Malware and Reputation Settings: AP.Users

Web Reputation and Anti-Malware Settings

Define Web Reputation and Anti-Malware Custom Settings

Web Reputation Settings

Web Reputation Filters will automatically block transactions with a low Web Reputation score. For transactions with a higher Web Reputation score, scanning will be performed using the services selected by Adaptive Scanning.

If Web Reputation Filtering is disabled in this policy, transactions will not be automatically blocked based on low Web Reputation Score. Blocking of sites that contain malware or other high-risk content is controlled by the settings below.

Enable Web Reputation Filtering

Secure Endpoint Settings

Enable File Reputation Filtering and File Analysis

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.

File Reputation	Monitor	Block
<input checked="" type="checkbox"/> Known Malicious and High-Risk Files	<input type="checkbox"/>	<input checked="" type="checkbox"/>

An attempt was made to download a malicious file “Bombermania.exe.zip” from the internet through the Cisco secure web appliance. The log shows that the malicious file is BLOCKED.

SWA Access Logs

The Access logs can be fetched by these steps.

1. Log in to the SWA and type the command "grep"
2. Select "accesslogs"
3. If you would like to add any "regular expression" such as client IP, then please mention it.
4. Type "Y" to tail the log

```
1708320236.640 61255 10.106.37.205 TCP_DENIED/403 2555785 GET
http://static1.1.sqspcdn.com/static/f/830757/21908425/1360688016967/Bombermania.exe.zip?token=gsFKIOF
- DEFAULT_PARENT/bg111-lab-wsa-2.cisco.com application/zip BLOCK_AMP_RESP_12-AP.Users-
ID.Users-NONE-NONE-NONE-DefaultGroup-NONE <"IW_comp",3.7,1,"-,-,-,1,"-,-,-,"-1,-,"-,"-,-
,"IW_comp",-,"AMP High Risk","Computers and Internet",-,"Unknown","Unknown",-,"-","333.79,0,-"
"-
",37,"Win.Ransomware.Protected::Trojan.Agent.talos",0,0,"Bombermania.exe.zip","46ee42fb79a161bf3763e8
",-,-,-> -
```

TCP_DENIED/403 --> SWA denied this HTTP GET request.

BLOCK_AMP_RESP --> The HTTP GET request was blocked due to AMP response.

Win.Ransomware.Protected::Trojan.Agent.talos --> Threat Name

Bombermania.exe.zip --> File name which we tried to download

46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8 --> SHA value of the file

SWA AMP Logs

The AMP logs can be fetched by using these steps.

1. Log in to the SWA and type the command "grep"

2. Select "amp_logs"

3. Leave all other fields as it is and type "Y" to tail the logs. Tail the logs to show the live events. If you are looking for old events, then you can type the date in "regular expression"

'verdict_from': 'Cloud' This seems to be the same for private cloud and public cloud. Do not confuse it as a verdict from the public cloud.

```
Mon Feb 19 10:53:56 2024 Debug: Adjusted verdict - {'category': 'amp', 'spyname': 'Win.Ransomware.Protected::Trojan.Agent.talos', 'original_verdict': 'MALICIOUS', 'analysis_status': 18, 'verdict_num': 3, 'analysis_score': 0, 'uploaded': False, 'file_name': 'Bombermania.exe.zip', 'verdict_source': None, 'extract_file_verdict_list': '', 'verdict_from': 'Cloud', 'analysis_action': 2, 'file_type': 'application/zip', 'score': 0, 'upload_reason': 'File type is not configured for sandboxing', 'sha256': '46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8', 'verdict_str': 'MALICIOUS', 'malicious_child': None}
```

Secure Endpoint Private cloud event logs

The event logs are available under /data/cloud/log

You can search for the event either with the SHA256 or using the "File Reputation Client ID" of the SWA. "File Reputation Client ID" is present in the AMP configuration page of the SWA.

```
[root@fireamp log]# pwd
/data/cloud/log
[root@fireamp log]#
[root@fireamp log]# less eventlog | grep -E "46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8"
[09:33] ip:10.106.39.144 h:11 n:0 m:1 s:0 tvc:6 wct:1 d:2 app:1 cets:1788320235, tstr:1788370222, tsnr:1707403179, uu:"9a7a27a1-49aa-452f-a970-ed78e215b717" al:"1" aptus:"1344" ptus:"975590" spero:{"h":"00","fa":"0","ts":"0","hd":1} sha256:{"h":"46EE42FB79A161BF3763E8E34A047018BD16D8572F8D31C2CDECAE3D2E7A57A8" fa:"0",ts:"0",ft:"6",rd:"3",nord:"1",dn:"Win.Ransomware.Protected::Trojan.Agent.talos" url:"http://static1.1.saspcdn.com/static/1/7830/57/21988425713806888016957/Bombermania.exe.zip?token=g5FA1UFLQWMyjAM1328pg31jRwQ30" rd:"3",ra:"2",n:"0}
```

pv - Protocol Version, 3 indicates TCP

ip - Please ignore this field as there is no guarantee that this field indicates the actual IP address of the client who did the reputation query

uu - File reputation client ID in WSA/ESA

SHA256 – SHA256 of the file

dn – The detection name

n - 1 if the file hash has never been seen before by AMP, 0 otherwise.

rd – Response Disposition. here 3 means DISP_MALICIOUS

1 DISP_UNKNOWN The file disposition is unknown.

2 DISP_CLEAN The file is believed to be benign.

3 DISP_MALICIOUS The file is believed to be malicious.

7 DISP_UNSEEN The file disposition is unknown and it is the first time we have seen the file.

13 DISP_BLOCK The file must not be executed.

14 DISP_IGNORE XXX

15 DISP_CLEAN_PARENT The file is believed to be benign, and any malicious files it creates must be treated as unknown.

16 DISP_CLEAN_NFM The file is believed to be benign, but the client must monitor its network traffic.

Testing the integration between Secure Email and AMP private cloud

There is no direct option to test the connectivity from the Secure Email gateway. You must inspect the logs or alerts to verify if there are any issues.

Configuration is done in the Secure Email incoming mail policy to enforce the AMP scanning.

Incoming Mail Policies

Find Policies									
		Email Address: <input type="text"/>		<input checked="" type="radio"/> Recipient <input type="radio"/> Sender		Find Policies			
Policies									
Add Policy...									
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	amp-testing-policy	Disabled	Disabled	File Reputation Malware File: Drop Pending Analysis: Deliver Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	(use default)	(use default)	(use default)	(use default)	

Mail Policies: Advanced Malware Protection

Advanced Malware Protection Settings	
Policy:	amp-testing-policy
Enable Advanced Malware Protection for This Policy:	<input checked="" type="radio"/> Enable File Reputation <input checked="" type="checkbox"/> Enable File Analysis <input type="radio"/> Use Default Settings (AMP and File Analysis Enabled) <input type="radio"/> No
Message Scanning	
	<input checked="" type="checkbox"/> (recommended) Include an X-header with the AMP results in messages
Unscannable Actions on Message Errors	
Action Applied to Message:	Deliver As Is <input type="button" value="v"/>
Advanced	Optional settings for custom header and message delivery.
Unscannable Actions on Rate Limit	
Action Applied to Message:	Deliver As Is <input type="button" value="v"/>
Advanced	Optional settings for custom header and message delivery.
Unscannable Actions on AMP Service Not Available	
Action Applied to Message:	Deliver As Is <input type="button" value="v"/>
Advanced	Optional settings for custom header and message delivery.
Messages with Malware Attachments:	
Action Applied to Message:	Drop Message <input type="button" value="v"/>
Archive Original Message:	<input type="radio"/> No <input checked="" 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
	<input type="text" value="[WARNING: MALWARE DETECTED]"/>
Advanced	Optional settings.
Messages with File Analysis Pending:	
Action Applied to Message:	Deliver As Is <input type="button" value="v"/>
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Message Attachments with File Analysis Verdict Pending : ?	<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
	<input type="text" value="[WARNING: ATTACHMENT(S) MAY CONTAIN]"/>
Advanced	Optional settings.

tested ESA with a non-malicious file. This is a CSV file.

Secure Email mail_logs

```
Tue Feb 20 11:55:58 2024 Info: New SMTP ICID 43855 interface Management (10.106.39.193) address 10.110.172.122 reverse dns host unknown verified no
Tue Feb 20 11:55:58 2024 Info: ICID 43855 ACCEPT 5G UNKNOWNLIST match sbrs[none] SBRS rfc1918 country not applicable
Tue Feb 20 11:55:58 2024 Info: Start MID 660 ICID 43855
Tue Feb 20 11:55:58 2024 Info: MID 660 ICID 43855 From: <ajayraj@gmail.com>
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: CSCD-W-PF253NK0, env-from: gmail.com, header-from: Not Present, reply-to: Not Present
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain: gmail.com
Tue Feb 20 11:55:58 2024 Info: MID 660 ICID 43855 RID 0 ID: <ajayraj@gmail.com>
Tue Feb 20 11:55:58 2024 Info: MID 660 Subject: testing amp private cloud
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: CSCD-W-PF253NK0, env-from: gmail.com, header-from: gmail.com, reply-to: Not Present
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain: gmail.com
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Tracker Header : 65d445f6_7d946k_7zoil66+HhA4cF3o0I9z)JQ5DhLDLExK9DPClxVhxF3o3lC136to+TzXKqIaVVFPh6XLcND+S1Q=
Tue Feb 20 11:55:58 2024 Info: MID 660 ready 5467 bytes from ajayraj@gmail.com
Tue Feb 20 11:55:58 2024 Info: MID 660 attachments: Training Details.csv
Tue Feb 20 11:55:58 2024 Info: MID 660 matched all recipients for per-recipient policy amp-testing-policy in the inbound table
Tue Feb 20 11:56:59 2024 Warning: graymail [RPC CLIENT] MID 660 Graymail scan timed out
Tue Feb 20 11:57:01 2024 Info: MID 660 AMP File reputation verdict: unknown (File analysis pending)
Tue Feb 20 11:57:01 2024 Info: MID 660 SHA 90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19dbe filename Training Details.csv queued for possible file analysis upload
Tue Feb 20 11:57:01 2024 Info: MID 660 Outbreak Filters: verdict negative
Tue Feb 20 11:57:01 2024 Info: MID 660 Message-ID: <99221a1kx@esai.nanganath.local>
Tue Feb 20 11:57:01 2024 Info: MID 660 queued for delivery
Tue Feb 20 11:57:01 2024 Info: New SMTP ICID 542 interface 20.106.39.193 address 173.37.147.230 port 25
Tue Feb 20 11:57:02 2024 Info: Delivery start DCID 542 MID 660 to RID [0]
Tue Feb 20 11:57:04 2024 Info: Message done DCID 542 MID 660 to RID [0]
Tue Feb 20 11:57:04 2024 Info: MID 660 RID [0] Response 'ok: Message 142767851 accepted'
Tue Feb 20 11:57:04 2024 Info: Message finished MID 660 done
Tue Feb 20 11:57:09 2024 Info: DCID 542 close
Tue Feb 20 11:57:23 2024 Info: ICID 43855 lost
Tue Feb 20 11:57:23 2024 Info: ICID 43855 close
```

Secure Email AMP Logs

Tue Feb 20 11:57:01 2024 Info: **Response received for file reputation query** from Cloud. **File Name = Training Details.csv**, MID = 660, **Disposition = FILE UNKNOWN**, Malware = None, Analysis Score = 0, sha256 = 90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19dbe, upload_action = Recommended to send the file for analysis, verdict_source = AMP, suspected_categories = None

Secure Endpoint Private Cloud event logs

{ "pv": 3, "ip": "10.106.72.238", "si": 0, "ti": 14, "tv": 6, "qt": 42, "pr": 1, "ets": 1708410419, "ts": 1708410366, "tsns": 29912939277-4008-a396-

6cd486ecc621", "ai": 1, "aptus": 295, "ptus": 2429102, "spero": { "h": "00", "fa": 0, "fs": 0, "ft": 0, "hd": 1 }, "sha256": { "h": "9

rd - 1 DISP_UNKNOWN. The file disposition is unknown.

Common issues observed that result in integration failure

1. Choosing the wrong “Routing Table” in SWA or Secure Email. The integrated device must be able to communicate with the AMP private cloud Eth1 interface.
2. The VPC hostname is not DNS resolvable in SWA or Secure Email which leads to failure in establishing the connection.
3. The CN (Common Name) in the VPC disposition certificate must match the VPC hostname as well as the one mentioned in SWA and Secure Email Gateway.
4. Using a private cloud and a cloud file analysis is not a supported design. If you are using an on-premise device, then File analysis and reputation must be an on-premise server.
5. Ensure there is no time sync issue between AMP private cloud and SWA, Secure Email.
6. SWA DVS Engine Object Scanning Limit is defaulted to 32 MB. Adjust this setting if you would like to scan bigger files. Please note that it is a global setting and affects all the scanning engines such as Webroot, Sophos, and so on.