

Geïntegreerd Secure Endpoint Private Cloud met beveiligd web en e-mail

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Gebruikte componenten](#)

[Verificatiecontroles alvorens over te gaan tot integratie](#)

[Procedure](#)

[De Secure Endpoint-privécloud configureren](#)

[De Secure Web-applicatie configureren](#)

[De Cisco Secure-e-mail configureren](#)

[De stappen om AMP-logboeken te halen van Secure Web en E-mail](#)

[De integratie tussen Secure Web Applicatie en Secure Endpoint private cloud testen.](#)

[SWA-toegangslogbestanden](#)

[SWA AMP-logbestanden](#)

Inleiding

In dit document worden de stappen beschreven die moeten worden uitgevoerd om Secure Endpoint private cloud met Secure Web Appliance (SWA) en Secure Email Gateway (ESA) te integreren.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure Endpoint AMP Virtual Private Cloud
- Secure Web applicatie (SWA)
- Secure e-mail gateway

Gebruikte componenten

SWA (Secure Web Applicatie) 15.0.0-322

AMP Virtual Private Cloud 4.1.0_202311092226

Secure Email Gateway 14.2.0-620



Opmerking: de documentatie is geldig voor zowel fysieke als virtuele variaties van alle betrokken producten.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Verificatiecontroles alvorens over te gaan tot integratie

1. Controleer of **Secure Endpoint Private Cloud/SWA/Secure Email Gateway** de klant over de vereiste licenties beschikt. U kunt de functiesleutel verifiëren **SWA/Secure Email** of controleren of de slimme licentie is ingeschakeld.
2. **HTTPS-proxy** moet worden ingeschakeld op **SWA** als u van plan bent het **HTTPS-verkeer** te inspecteren. U moet het **HTTPS-verkeer** ontsleutelen om de reputatie van het bestand te kunnen controleren.
3. Het **AMP Private Cloud/Virtual Private Cloud**-apparaat en alle benodigde certificaten moeten

worden geconfigureerd. Raadpleeg de VPC-certificeringsgids voor verificatie.

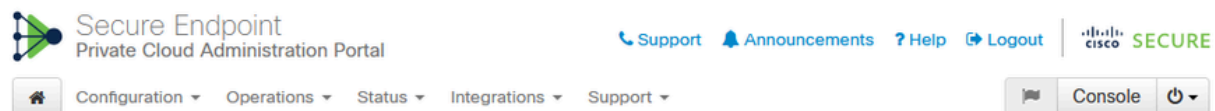
<https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/214326-how-to-generate-and-add-certificates-tha.html>

4. Alle hostnamen van de producten moeten DNS oplosbaar zijn. Dit is om problemen met de connectiviteit of bepaalde problemen tijdens de integratie te voorkomen. Op de Secure Endpoint private cloud is de Eth0-interface bedoeld voor Admin-toegang en Eth1 moet in staat zijn verbinding te maken met integrerende apparaten.

Procedure

De Secure Endpoint-privécloud configureren


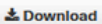
1. Log in op de Secure Endpoint VPC admin portaalpagina.
2. Ga naar "Configuration" > "Services" > "Disposition Server" > Kopieer de hostnaam van de verwerkingsserver (dit kan ook worden gehaald uit de derde stap).
3. Navigeer naar "Integrations" > "Web Security Appliance".
4. Download het "Disposition Server Public Key" & "Appliance Certificate Root" .
5. Navigeer naar "Integrations" > "Email Security Appliance".
6. Selecteer de versie van uw ESA en download de "Disposition Server Public Key" en "Applicatie Certificaat Root".
7. Houd zowel de cert als de sleutel veilig. Dit moet later geüpload worden naar SWA/Secure Email.



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** 

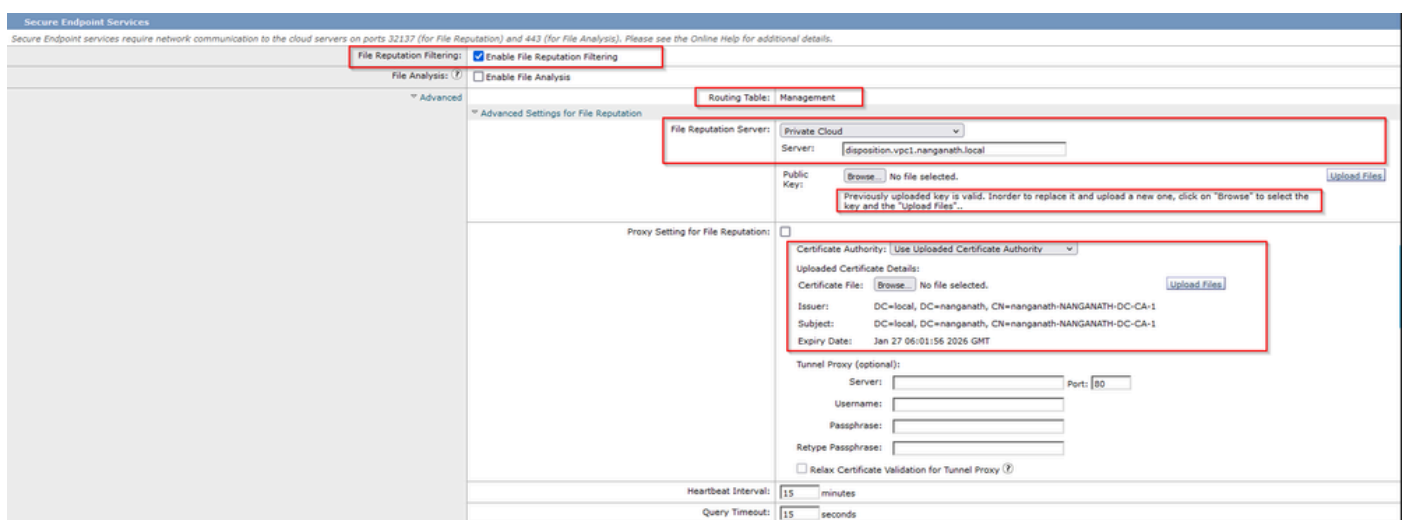
Step 2: Proxy Setting

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** 

De Secure Web-applicatie configureren

1. Naar navigeren SWA GUI > "Security Services" > "Anti-Malware and Reputation" > Edit Global Settings
2. Onder de sectie "Secure Endpoint Services" ziet u de optie "Filtering bestandsnaam inschakelen" en "Controleren" toont deze optie een nieuw veld "Geavanceerd"
3. Selecteer "Private Cloud" in de File Reputation Server.
4. Geef de private cloud Disposition Server hostnaam als "Server".
5. Upload de openbare sleutel die u eerder hebt gedownload. Klik op "Bestanden uploaden".
6. Er is een optie om de certificaatautoriteit te uploaden. Kies "Gebruik geüploade certificaatinstantie" in de vervolgkeuzelijst en upload het CA-certificaat dat u eerder hebt gedownload.
7. Verzend de wijziging
8. De wijziging doorvoeren

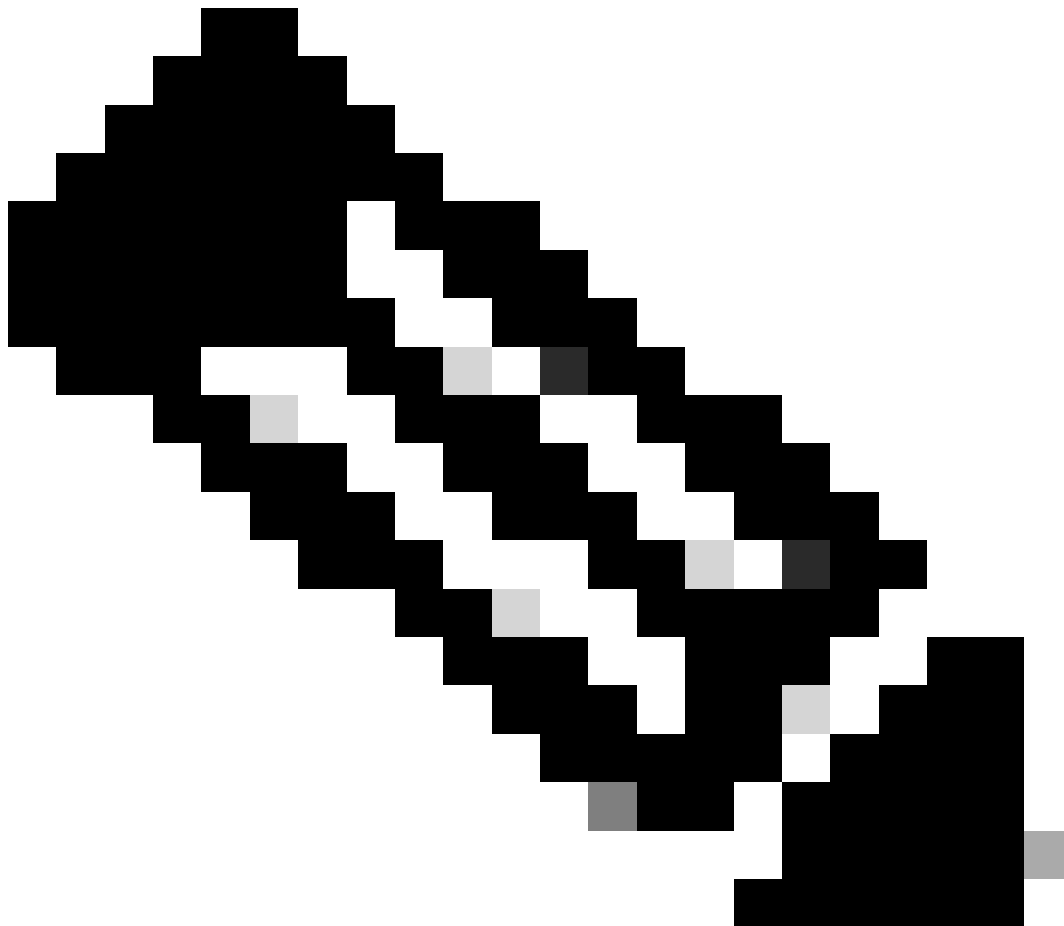


De Cisco Secure-e-mail configureren

1. Navigeer naar Secure Email GUI > Security Services" > "File Reputation and Analysis" > Edit Global Settings > "Enable" or "Edit Global Settings"
2. Selecteer "Private Cloud" in de File Reputation Server
3. Geef de hostnaam van de private cloud Disposition Server als "Server".
4. Upload de openbare sleutel die we eerder hebben gedownload. Klik op "Bestanden uploaden".
5. Upload de certificeringsinstantie. Kies "Gebruik geüploade certificaatinstantie" in de vervolgkeuzelijst en upload het CA-certificaat dat u eerder hebt gedownload.
6. Verzend de wijziging
7. De wijziging doorvoeren

Edit File Reputation and Analysis Settings

Advanced Malware Protection	
<i>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.</i>	
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"/>
<i>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".</i>	
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	<i>Advanced settings for Cache</i>
Threshold Settings	<i>Advanced Settings for File Analysis Threshold Score</i>



Opmerking: Cisco Secure Web Applicatie en Cisco Secure Email Gateway zijn gebaseerd op AsyncOS en delen vrijwel dezelfde logbestanden wanneer de bestandsreputatie wordt geïnitieerd. Het AMP log kan worden waargenomen in Secure Web Applicatie of Secure Email Gateway AMP logs (soortgelijke logbestanden in beide apparaten). Dit geeft alleen aan dat de service is geïnitieerd op de SWA en Secure Email Gateway. Het gaf niet aan dat de verbinding volledig succesvol was. Als er problemen zijn met de connectiviteit of het certificaat, kunt u fouten zien na het bericht "Bestandsreputatie geïnitieerd". Meestal duidt het op een "Onbereikbare fout" of "certificaat ongeldig" fout.

De stappen om AMP-logboeken te halen van Secure Web en E-mail

1. Log in op de CLI van de SWA/Secure Email Gateway en typ de opdracht "grep"
2. Selecteer "amp" or "amp_logs"
3. Laat alle andere velden ongewijzigd en typ "Y" om de logbestanden bij te houden. Ga naar de logboeken om de live-evenementen te tonen. Als u op zoek bent naar oude gebeurtenissen, dan kunt u de datum in "reguliere expressie" typen

```
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.
```

De integratie tussen Secure Web Applicatie en Secure Endpoint private cloud testen.

Er is geen directe optie om de connectiviteit van SWA te testen. U moet de logbestanden of waarschuwingen bekijken om te controleren of er problemen zijn.

Voor de eenvoud testen we een HTTP URL in plaats van HTTPS. Houd er rekening mee dat u het HTTPS-verkeer moet decoderen voor alle reputatieschakelingen van bestanden.

De configuratie vindt plaats in het SWA-toegangsbeleid en het scannen van AMP wordt afgedwongen.

Opmerking: raadpleeg de SWA-[gebruikershandleiding](#) om te begrijpen hoe u het beleid op Cisco Secure Web Applicatie kunt configureren.

Access Policies

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"/>

Er is geprobeerd een kwaadaardig bestand "Bombermania.exe.zip" via de beveiligde internetapplicatie van Cisco van het internet te downloaden. Het logbestand toont aan dat het kwaadaardige bestand is geblokkeerd.

SWA-toegangslogbestanden

De toegangslogboeken kunnen door deze stappen worden gehaald.

1. Log in op de SWA en typ de opdracht "grep"
2. Selecteer "accesslogs"
3. Als u een "reguliere expressie" zoals client-IP wilt toevoegen, vermeld dit dan.
4. Type "Y" om het logbestand te schaduwen

```
1708320236.640 61255 10.106.37.2005 TCP_DENIED/403 2555785 GET
http://static1.1.sqspcdn.com/static/f/830757/21908425/1360688016967/Bombermania.exe.zip?token=gsF
- DEFAULT_PARENT/bg11-lab-wsa-2.cisco.com application/zip BLOCK_AMP_RESP_12-
AP.users-ID.users-NONE-NONE-DefaultGroup-NONE <"IW_comp",3.7,1,"-","-","-","-","-","-","-","-","-","-","-
,W_comp",-,"AMP High Risk","Computers en internet",-,"Onbekend", "Onbekend",-,"-
",333.79,0,-,"-","-",37,"Win.Ransomware.Protected::Trojan.Agent.talos",0,0,"exe
Bombermania.zip","46ee42fb79a161bf3766
e34a047018bd16d857f8d31c2cdecae3d2e7a57a8",3,-,"-","-","-,-> -
```

TCP_DENIED/403 → SWA ontkende dit HTTP GET verzoek.

BLOCK_AMP_RESP → Het HTTP GET-verzoek is geblokkeerd vanwege AMP-respons.

Win.Ransomware.Protected::Trojan.Agent.talos → Threat Name

Bombermania.exe.zip → Bestandsnaam die we probeerden te downloaden

46ee42fb79a161bf376e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8 → SHA-waarde van het bestand

SWA AMP-logbestanden

De AMP-logbestanden kunnen met deze stappen worden opgehaald.

1. Log in op de SWA en typ de opdracht "grep"
2. Selecteer "amp_logs"
3. Laat alle andere velden ongewijzigd en typ "Y" om de logbestanden bij te houden. Ga naar de logboeken om de live-evenementen te tonen. Als u op zoek bent naar oude gebeurtenissen, dan kunt u de datum in "reguliere expressie" typen

'verdict_from': 'Cloud' Dit lijkt hetzelfde te zijn voor private cloud en public cloud. Verwar het niet als een vonnis uit de publieke cloud.

```
Mon Feb 19 10:53:56 2024 Debug: Aangepast vonnis - {'category': 'amp', 'spyname': 'Win.Ransomware.Protected::Trojan.Agent.talos', 'original_verdict': 'MALICIOUS', 'analysis_status': 18, 'verdict_num': 3, 'analysis_score': 0, 'geupload': False, 'file_name': 'Bombermania.zip', 'exe_t_source': Geen, 'extract_file_verdict_list': '', 'verdict_from': 'Cloud', 'analysis_action': 2, 'file_type': 'application/zip', 'score': 0, 'upload_sense': 'File type is niet geconfigureerd voor sandboxing', 'sha256': '46ee42fb79a161bf376e8e34a047018bd857 f8d31c2cdecae3d2e7a57a8', 'verdict_str': 'MALICIOUS', 'malicious_child': geen}
```

Secure Endpoint - logbestanden van privé-clouds

De logboeken van de gebeurtenissen zijn beschikbaar onder /data/cloud/log

U kunt zoeken naar de gebeurtenis met de SHA256 of met behulp van de "File Reputation Client ID" van de SWA. De "File Reputation Client ID" is aanwezig op de AMP-configuratiepagina van de SWA.

```
[root@fireamp log]# pwd
/data/cloud/log
[root@fireamp log]#
[root@fireamp log]# less eventlog | grep -iE "46ee42fb79a161bf376e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8"
[py:33] ip:"10.106.39.144", "si":0, "ti":3, "tv":6, "qt":42, "pr":1, "ets":1708320235, "ts":1708320232, "tsn":707403179, [uu]:"9a7a27a1-40aa-452f-a070-ed78e215b717", "ai":1, "aptus":1344, "ptus":975590, "spero":{"h":00, "fa":0, "fs":0, "ft":0, "hd":1}, [sha256":{"h":"46EE42FB79A161BF376E8E34A047018BD16D8572F8D31C2CDECAE3D2E7A57A8", "fa":0, "fs":0, "ft":0, "hd":3}, "nord":{"id":3247, "dn":"win.Ransomware.Protected::Trojan.Agent.talos", "url":"http://static1.1.sqspcdn.com/static/1/7830757/z1908425/1350888016397/Bombermania.exe.zip/token=g3FN10FLU0mnyJAm%2Bpg31jRwQ%3D", "rd":3, "ra":2, "n":0}
```

pv - Protocol versie, 3 geeft TCP aan

ip - Negeer dit veld omdat er geen garantie is dat dit veld het werkelijke IP-adres aangeeft van de klant die de reputatie heeft opgevraagd

u - File reputation client ID in WSA/ESA

SHA256 - SHA256 van het dossier

DN - De detectienaam

n - 1 als de file hash nog nooit eerder geïdentificeerd is door AMP, 0 anders.

rd - Response Disposition. hier 3 betekent DISP_MALICIOUS

1 DISP_UNNOWNKDe bestandsdispositie is onbekend.

2 DISP_CLEAN Het bestand wordt geacht goedaardig te zijn.

3 DISP_MALICIOUS Men gelooft dat het bestand kwaadaardig is.

7 DISP_UNSEE De bestandsdispositie is onbekend en het is de eerste keer dat we het bestand hebben gezien.

13 DISP_BLOCKS K Het bestand mag niet worden uitgevoerd.

14 DISP_IGNORE XXX

15 DISP_CLEAN_PARENT Het bestand wordt verondersteld goedaardig te zijn, en alle kwaadaardige bestanden die het maakt moeten worden behandeld als onbekend.

16 DISP_CLEAN_NFM Het bestand wordt geacht goedaardig te zijn, maar de client moet zijn netwerkverkeer controleren.

De integratie tussen Secure Email en AMP private cloud testen

Er is geen directe optie om de connectiviteit van de Secure Email gateway te testen. U moet de logbestanden of waarschuwingen bekijken om te controleren of er problemen zijn.

De configuratie wordt uitgevoerd in het beleid voor beveiligde e-mail met inkomende e-mail om het scannen van AMP's af te dwingen.

Incoming Mail Policies

Find Policies									
Email Address:				<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
Advanced	Optional settings for custom header and message delivery.
Unscannable Actions on Rate Limit	
Action Applied to Message:	Deliver As Is
Advanced	Optional settings for custom header and message delivery.
Unscannable Actions on AMP Service Not Available	
Action Applied to Message:	Deliver As Is
Advanced	Optional settings for custom header and message delivery.
Messages with Malware Attachments:	
Action Applied to Message:	Drop Message
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
	[WARNING: MALWARE DETECTED]
Advanced	Optional settings.
Messages with File Analysis Pending:	
Action Applied to Message:	Deliver As Is
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
	[WARNING: ATTACHMENT(S) MAY CONTAIN
Advanced	Optional settings.

getest ESA met een niet-kwaadaardig bestand. Dit is een CSV-bestand.

Beveiligde e-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: <ajayra@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: CSC0-M-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 To: <ajayra@cisisco.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: CSC0-M-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_TdY46k/XzoIL66+HhA4cFJo0192j3QSDhLDnEkX9DPCkVhXf3o3lC136to+TzXqIaVfPh6X+cND+S1Q=
Tue Feb 20 11:55:58 2024 Info: MID 660 ready 5467 bytes from <ajayra@gmail.com>
Tue Feb 20 11:55:58 2024 Info: MID 660 attachment: Training Details.csv
Tue Feb 20 11:55:58 2024 Info: MID 660 matches 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-90381C261f0be3e9330710ab96647358c461f6834c0ca001408e40decdf19dbe 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 : <99221a1xwesi.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 10.106.39.193 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
```

Beveiligde e-mail AMP logbestanden

Tue Feb 20 11:57:01 2024 Info: Antwoord ontvangen voor bestandsreputatie query van Cloud.
Bestandsnaam = Training Details.csv, MID = 660, Afwijzing = FILE UNKNOWN, Malware = Geen,
Analysescore = 0, sha256 =
90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19dbe, upload_action =
Aanbevolen om het bestand ter analyse te verzenden, verdict_source = AMP, Geen

Secure Endpoint voor privé-clouds

```
{"pv":3,"ip":"10.106.72.238","si":0,"ti":14,"tv":6,"qt":42,"pr":1,"ets":1708410419,"ts":1708410366,"tsns":299  
9277-4008-a396-6cd486ecb6  
1","ai":1,"aptus":295,"ptus":2429102,"spero":{"h":"00","fa":0,"fs":0,"ft":0,"hd":1},"sha256":{"h":"90381C261F  
9DBE","fa":0,"fs":0,"ft":0,"hd":1},"hord":[32,4],"rd":1,"ra":1,"n":0}
```

rd - 1 DISP_UNKNOWN. De bestandsdispositie is onbekend.

Vaak voorkomende problemen die leiden tot mislukte integratie

1. Kies de verkeerde "Routing Table" in SWA of Secure Email. Het geïntegreerde apparaat moet kunnen communiceren met de AMP private cloud Eth1 interface.
2. De VPC hostname is niet DNS oplosbaar in SWA of Secure Email wat leidt tot een storing in het opzetten van de verbinding.
3. De CN (Common Name) in het VPC dispositiecertificaat moet overeenkomen met de VPC hostnaam en de naam die in SWA en Secure Email Gateway wordt vermeld.
4. Het gebruik van een privécloud en een cloudbestandsanalyse is geen ondersteund ontwerp. Als u een on-premise apparaat gebruikt, dan moet de bestandsanalyse en reputatie een on-premise server zijn.
5. Zorg ervoor dat er geen tijd synchronisatie probleem is tussen AMP private cloud en SWA, Secure Email.
6. SWA DVS Engine Object Scanning Limit is standaard ingesteld op 32 MB. Pas deze instelling aan als u grotere bestanden wilt scannen. Houd er rekening mee dat dit een algemene instelling is die van invloed is op alle scanmachines, zoals Webroot, Sophos, enzovoort.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.