

# Intégrez le cloud privé Secure Endpoint avec le web et la messagerie sécurisés

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Vérifications avant de poursuivre l'intégration](#)

[Procédure](#)

[Configurer le cloud privé Secure Endpoint](#)

[Configuration de l'appliance Web sécurisée](#)

[Configuration de la messagerie sécurisée Cisco](#)

[Étapes de récupération des journaux AMP à partir de Secure Web and Email](#)

[Test de l'intégration entre le cloud privé Secure Web Appliance et Secure Endpoint.](#)

[Journaux d'accès SWA](#)

[Journaux SWA AMP](#)

---

## Introduction

Ce document décrit les étapes requises pour intégrer le cloud privé Secure Endpoint avec Secure Web Appliance (SWA) et Secure Email Gateway (ESA).

## Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cloud privé virtuel AMP pour terminaux sécurisés
- Appareil Web sécurisé (SWA)
- Passerelle de messagerie sécurisée

## Composants utilisés

SWA (Secure Web Appliance) 15.0.0-322

Cloud privé virtuel AMP 4.1.0\_202311092226

Passerelle de messagerie sécurisée 14.2.0-620



Remarque : la documentation est valide pour les variantes physiques et virtuelles de tous les produits concernés.

---

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Vérifications avant de poursuivre l'intégration

1. Vérifiez si Secure Endpoint Private Cloud/SWA/Secure Email Gateway dispose des licences requises. Vous pouvez vérifier la clé de fonction SWA/Secure Email ou vérifier que la licence Smart est activée.
2. Le proxy HTTPS doit être activé sur SWA si vous prévoyez d'inspecter le trafic HTTPS. Vous devez décrypter le trafic HTTPS afin d'effectuer des vérifications de réputation de fichiers.
3. L'appliance de cloud privé AMP/cloud privé virtuel et tous les certificats nécessaires doivent être configurés. Reportez-vous au guide de certificat VPC pour la vérification.

<https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/214326->

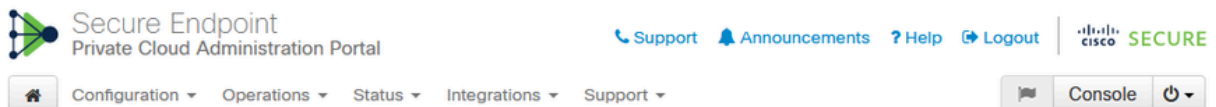
[how-to-generate-and-add-certificates-tha.html](https://www.cisco.com/.../how-to-generate-and-add-certificates-tha.html)

4. Tous les noms d'hôte des produits doivent pouvoir être résolus par DNS. Cela permet d'éviter tout problème de connectivité ou de sécurité lors de l'intégration. Sur le cloud privé Secure Endpoint, l'interface Eth0 est réservée à l'accès Admin et Eth1 doit pouvoir se connecter aux périphériques d'intégration.

## Procédure

### Configurer le cloud privé Secure Endpoint



1. Connectez-vous à la **Secure Endpoint VPC admin portal**.
2. Accédez à **“Configuration” > “Services” > “Disposition Server”** > Copiez le nom d'hôte du serveur de disposition (ce qui peut également être récupéré à la troisième étape).
3. Accédez à **“Integrations” > “Web Security Appliance”**.
4. Téléchargez la **“Disposition Server Public Key” & “Appliance Certificate Root”** .
5. Accédez à **“Integrations” > “Email Security Appliance”**.
6. Sélectionnez la version de votre ESA et téléchargez la « Clé publique du serveur de disposition » et la « Racine du certificat de l'appliance ».
7. Veuillez conserver le certificat et la clé en lieu sûr. Vous devez le télécharger ultérieurement dans l'e-mail SWA/Secure.



#### Connect Cisco Web Security Appliance to Secure Endpoint Appliance


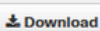
**Step 1: Web Security Appliance Setup**

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** 

### Configuration de l'appliance Web sécurisée

1. Naviguez jusqu'à SWA GUI > «Security Services» > «Anti-Malware and Reputation» > Edit Global Settings
2. Dans la section « Secure Endpoint Services », vous pouvez voir l'option « Enable File Reputation Filtering », et « Check » cette option affiche un nouveau champ « Advanced »
3. Sélectionnez « Private Cloud » dans le serveur de File Reputation.
4. Indiquez le nom d'hôte du serveur de disposition du cloud privé « Serveur ».
5. Téléchargez la clé publique que vous avez téléchargée précédemment. Cliquez sur « Télécharger les fichiers ».
6. Une option permet de télécharger l'autorité de certification. Sélectionnez « Use Uploaded Certificate Authority » (Utiliser l'autorité de certification téléchargée) dans la liste déroulante et téléchargez le certificat CA que vous avez téléchargé précédemment.
7. Envoyer la modification
8. Valider la modification

Secure Endpoint Services

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

File Reputation Filtering:  Enable File Reputation Filtering

File Analysis:  Enable File Analysis

Routing Table: Management

Advanced Settings for File Reputation

File Reputation Server: Private Cloud

Server: disposition.vpc1.nanganath.local

Public Key:  No file selected.

Previously uploaded key is valid. In order to replace it and upload a new one, click on "Browse" to select the key and the "Upload Files"...

Proxy Setting for File Reputation:

Certificate Authority: Use Uploaded Certificate Authority

Uploaded Certificate Details:

Certificate File:  No file selected.

Issuer: DC=local, DC=nanganath, CN=nanganath-NANGANATH-DC-CA-1

Subject: DC=local, DC=nanganath, CN=nanganath-NANGANATH-DC-CA-1

Expiry Date: Jan 27 06:01:56 2026 GMT

Tunnel Proxy (optional):

Server:  Port: 80

Username:

Passphrase:

Retype Passphrase:

Relax Certificate Validation for Tunnel Proxy (?)

Heartbeat Interval: 15 minutes

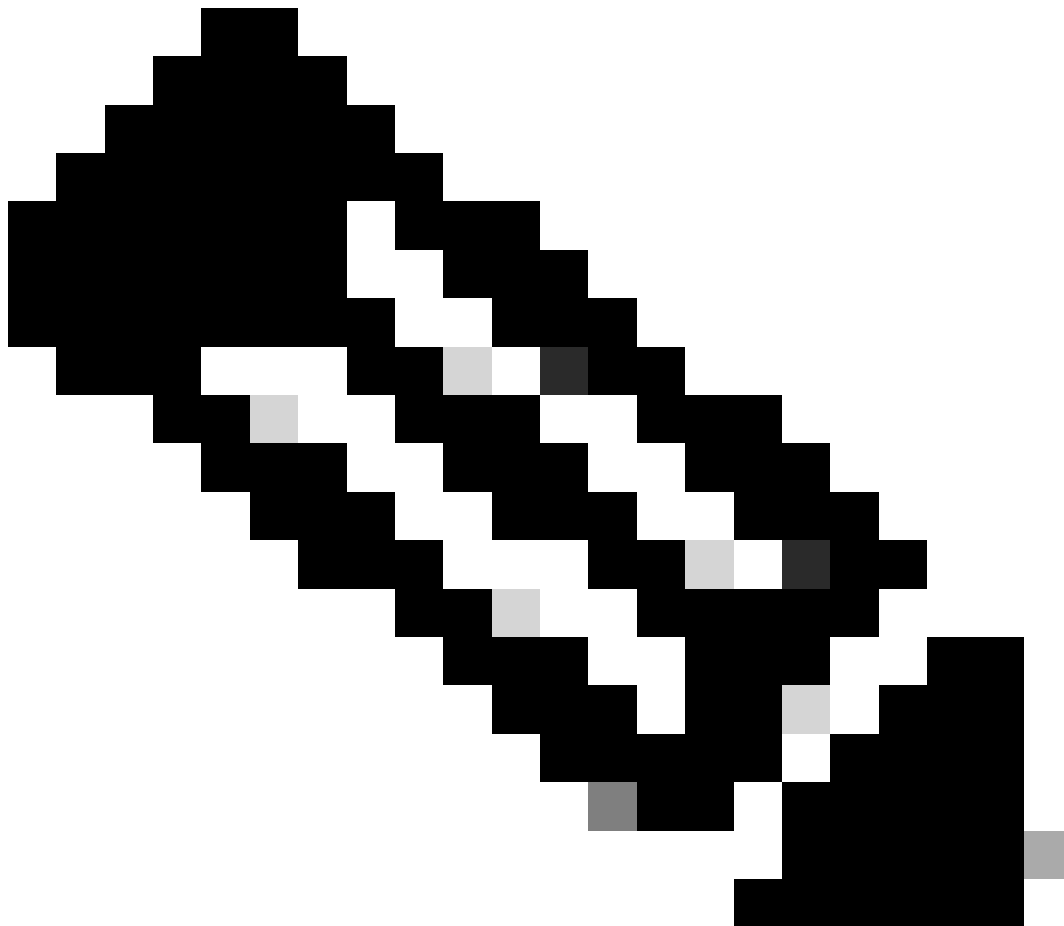
Query Timeout: 15 seconds

## Configuration de la messagerie sécurisée Cisco

1. Accédez à Secure Email GUI > Security Services» > «File Reputation and Analysis» > Edit Global Settings > «Enable» or «Edit Global Settings»
2. Sélectionnez « Private Cloud » dans le serveur de File Reputation
3. Attribuez le nom d'hôte « Serveur » au serveur de disposition du cloud privé.
4. Téléchargez la clé publique que nous avons téléchargée précédemment. Cliquez sur « Télécharger les fichiers ».
5. Téléchargez l'autorité de certification. Sélectionnez « Use Uploaded Certificate Authority » (Utiliser l'autorité de certification téléchargée) dans la liste déroulante et téléchargez le certificat CA que vous avez téléchargé précédemment.
6. Soumettre la modification
7. Validez la modification

## 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 (?)
<a href="#">Cache Settings</a>	Advanced settings for Cache
<a href="#">Threshold Settings</a>	Advanced Settings for File Analysis Threshold Score



Remarque : l'appliance Web sécurisé Cisco et la passerelle de messagerie sécurisée Cisco sont basés sur AsyncOS et partagent presque les mêmes journaux lorsque la réputation des fichiers est initialisée. Le journal AMP peut être observé dans les journaux AMP de l'appliance Web sécurisé ou de la passerelle de messagerie sécurisée (journaux similaires dans les deux périphériques). Cela indique uniquement que le service est initialisé sur SWA et Secure Email Gateway. Elle n'indique pas que la connectivité a réussi. En cas de problèmes de connectivité ou de certificat, des erreurs s'affichent après le message « File Reputation initialized ». Il indique principalement une erreur « Inaccessible » ou « Certificat non valide ».

## Étapes de récupération des journaux AMP à partir de Secure Web and Email

1. Connectez-vous à l'interface de ligne de commande de la passerelle SWA/Secure Email Gateway et entrez la commande "grep"
2. Sélectionnez "amp" or "amp\_logs"
3. Laissez tous les autres champs tels quels et tapez « Y » pour suivre les journaux. Suivez les journaux pour afficher les événements en direct. Si vous recherchez d'anciens événements, vous pouvez taper la date dans "expression régulière"

```
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.
```

## Test de l'intégration entre le cloud privé Secure Web Appliance et Secure Endpoint.

Il n'existe aucune option directe pour tester la connectivité à partir de SWA. Vous devez inspecter les journaux ou les alertes pour vérifier s'il y a des problèmes.

Pour simplifier, nous testons une URL HTTP au lieu de HTTPS. Veuillez noter que vous devez déchiffrer le trafic HTTPS pour toute vérification de la réputation des fichiers.

La configuration est effectuée dans la stratégie d'accès SWA et appliquée à l'analyse AMP.

Remarque : consultez le [guide de l'utilisateur](#) SWA pour comprendre comment configurer les stratégies sur l'appliance Web sécurisé Cisco.

### 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"/>

Une tentative de téléchargement d'un fichier malveillant « Bombermania.exe.zip » à partir d'Internet via l'appliance Web sécurisée Cisco a été effectuée. Le journal indique que le fichier malveillant est BLOQUÉ.

### Journaux d'accès SWA

Les journaux d'accès peuvent être lus par ces étapes.

1. Connectez-vous au SWA et entrez la commande "grep"
2. Sélectionnez "accesslogs"
3. Si vous souhaitez ajouter une "expression régulière" telle que l'adresse IP du client, veuillez la mentionner.
4. Tapez « Y » pour suivre le journal

```
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=gsF
- DEFAULT_PARENT/bgl11-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,"-,-,-,-","-
,"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","46ee42fb79a161bf37
63e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8",3,-,"-","-,-> -
```

TCP\_DENIED/403 → SWA a refusé cette requête HTTP GET.

BLOCK\_AMP\_RESP → La requête HTTP GET a été bloquée en raison d'une réponse AMP.

Win.Ransomware.Protected::Trojan.Agent.talos → Nom de la menace

Bombermania.exe.zip → Nom du fichier que nous avons essayé de télécharger

46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8 → Valeur SHA du fichier

## Journaux SWA AMP

Les journaux AMP peuvent être lus à l'aide de ces étapes.

1. Connectez-vous au SWA et entrez la commande "grep"
2. Sélectionnez "amp\_logs"
3. Laissez tous les autres champs tels quels et tapez « Y » pour suivre les journaux. Suivez les journaux pour afficher les événements en direct. Si vous recherchez d'anciens événements, vous pouvez taper la date dans "expression régulière"

'verdict\_from' : 'Cloud' Cela semble être le même pour le cloud privé et le cloud public. Ne le confondez pas avec un verdict du cloud public.

```
Lun Fév 19 10:53:56 2024 Débogage : Verdict ajusté - {'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' : Aucun, 'extraction_file_verdict_list' : "", 'verdict_from' : 'Cloud', 'analysis_action' : 2, 'file_type' : 'application/zip', 'score' : 0, 'upload_reason' : 'le type de fichier n'est pas configuré pour le sandboxing', 'sha256' : '46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8', 'verdict_str' : 'MALICIEUX', 'malicious_child' : Aucun}
```

## Journaux des événements du cloud privé Secure Endpoint

Les journaux des événements sont disponibles sous /data/cloud/log

Vous pouvez rechercher l'événement avec le SHA256 ou en utilisant l'« ID client de réputation de fichiers » du SWA. L'ID du client File Reputation est présent dans la page de configuration AMP du SWA.

```
[root@fireamp log]# pwd
/data/cloud/log
[root@fireamp log]# less eventlog | grep -E "46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8"
[09:23] ip:"10.106.39.144" si:"0" ti:"3" tv:"6" qt:"d2" pr:"i" ets:"1708320235" ts:"1708320232" tsn:"707403179" uu:"9a7427a1-40aa-452f-a070-ed78e215b717" ai:"1" aptus:"1344" ptus:"975590" spero":{"h":"00" fa:"0" fs:"0" ft:"0" hd:"1"} sha256":{"h":"46EE42FB79A161BF3763E8E34A047018BD16D8572F8D31C2CDECAE3D2E7A57A8" fa:"0" fs:"0" ft:"0" hd:"3" nord:"32.4" dn:"win.Ransomware.Protected::Trojan.Agent.talos" url:"http://static1.1.sqspcdn.com/static/1/7830757/z1908425/1350888016307/Bombermania.exe.zip?token=g3FN10FLU0mnyJAm%2Bpg31jK9wQ%3D" rd:"3" ra:"2" n:"0" }
```

pv - Protocol Version, 3 indique TCP

ip - Veuillez ignorer ce champ car il n'est pas garanti qu'il indique l'adresse IP réelle du client qui a effectué la requête de réputation

uu - ID client de réputation de fichiers dans WSA/ESA

SHA256 - SHA256 du fichier

dn : nom de détection

n - 1 si le hachage du fichier n'a jamais été vu auparavant par AMP, 0 sinon.



rd - Response Disposition. here 3 signifie DISP\_MALICIOUS

1 DISP\_UNKNOWN La disposition du fichier est inconnue.

2 DISP\_CLEAN Le fichier est considéré comme inoffensif.

3 DISP\_MALICIOUS Le fichier est considéré comme malveillant.

7 DISP\_UNSEEN La disposition du fichier est inconnue et c'est la première fois que nous voyons le fichier.

13 DISP\_BLOCK Le fichier ne doit pas être exécuté.

14 DISP\_IGNORE XXX

15 DISP\_CLEAN\_PARENT Le fichier est considéré comme inoffensif et tout fichier malveillant qu'il crée doit être considéré comme inconnu.

16 DISP\_CLEAN\_NFM Le fichier est considéré comme inoffensif, mais le client doit surveiller son trafic réseau.

## Test de l'intégration entre Secure Email et le cloud privé AMP

Il n'existe pas d'option directe pour tester la connectivité à partir de la passerelle de messagerie sécurisée. Vous devez inspecter les journaux ou les alertes pour vérifier s'il y a des problèmes.

La configuration s'effectue dans la stratégie de courrier entrant de la messagerie sécurisée pour appliquer l'analyse AMP.

### Incoming Mail Policies

Find Policies									
Email Address:				<input checked="" type="radio"/> Recipient <input type="radio"/> Sender		<a href="#">Find Policies</a>			
Policies									
<a href="#">Add Policy...</a>									
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	
<b>Policy:</b>	amp-testing-policy
<b>Enable Advanced Malware Protection for This Policy:</b>	<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.

a testé ESA avec un fichier non malveillant. Ceci est un fichier CSV.

## Journaux de messagerie électronique sécurisés

```
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-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 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-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_TdY46k/XzoIL66+HhA4cFJo0192j3QSDhLDnEkX9DPClxVhx3f3o3lC136to+7zXqIaVVP6hX+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-90381C261f0e3e9330710ab96647358c461f6834c0ca001408e40decdf19d8e 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 : <99221a1x0es81.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
```

## Journaux AMP sécurisés de la messagerie

Mar Feb 20 11:57:01 2024 Info : réponse reçue pour la requête de réputation de fichier du cloud.  
Nom du fichier = Training Details.csv, MID = 660, Disposition = FILE UNKNOWN, Malware =  
None, Analysis Score = 0, sha256 =  
90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19dbe, upload\_action =  
Recommandé pour envoyer le fichier pour analyse, verdict\_source = AMP suspicions\_catégories =  
Aucune

Journaux des événements du cloud privé Secure Endpoint

```
{"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-a396-6cd486ecc66  
1","ai":1,"aptus":295,"ptus":2429102,"spero":{"h":"00","fa":0,"fs":0,"ft":0,"hd":1},"sha256":{"h":"90381C261F  
19DBE","fa":0,"fs":0,"ft":0,"hd":1},"hord":[32,4],"rd":1,"ra":1,"n":0}
```

rd - 1 DISP\_UNKNOWN. La disposition du fichier est inconnue.

## Problèmes fréquents entraînant un échec de l'intégration

1. Choix de la mauvaise « table de routage » dans SWA ou Secure Email. Le périphérique intégré doit pouvoir communiquer avec l'interface Eth1 du cloud privé AMP.
2. Le nom d'hôte VPC ne peut pas être résolu par DNS dans SWA ou Secure Email, ce qui entraîne l'échec de l'établissement de la connexion.
3. Le CN (Common Name) dans le certificat de disposition VPC doit correspondre au nom d'hôte VPC ainsi qu'à celui mentionné dans SWA et Secure Email Gateway.
4. L'utilisation d'un cloud privé et d'une analyse de fichiers cloud n'est pas prise en charge. Si vous utilisez un périphérique sur site, alors l'analyse des fichiers et la réputation doivent être un serveur sur site.
5. Assurez-vous qu'il n'y a aucun problème de synchronisation temporelle entre le cloud privé AMP et SWA, Secure Email.
6. La limite d'analyse des objets du moteur SWA DVS est par défaut de 32 Mo. Réglez ce paramètre si vous souhaitez analyser des fichiers plus volumineux. Notez qu'il s'agit d'un paramètre global qui affecte tous les moteurs d'analyse tels que Webroot, Sophos, etc.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.