

# Integrazione di Secure Endpoint Private Cloud con Secure Web e Email

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Verifiche prima di procedere all'integrazione](#)

[Procedura](#)

[Configurare il cloud privato Secure Endpoint](#)

[Configurazione di Secure Web Appliance](#)

[Configurazione di Cisco Secure Email](#)

[Procedura per recuperare i registri AMP da Secure Web e posta elettronica](#)

[Test dell'integrazione tra Secure Web Appliance e il cloud privato Secure Endpoint.](#)

[Log degli accessi SWA](#)

[Registri SWA AMP](#)

---

## Introduzione

In questo documento vengono descritti i passaggi necessari per integrare il cloud privato Secure Endpoint con Secure Web Appliance (SWA) e Secure Email Gateway (ESA).

## Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

## Componenti usati

SWA (Secure Web Appliance) 15.0.0-322

AMP virtual private cloud 4.1.0\_202311092226

Secure Email Gateway 14.2.0-620



Nota: la documentazione è valida per le variazioni fisiche e virtuali di tutti i prodotti interessati.

---

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### Verifiche prima di procedere all'integrazione

1. Verificare che **Secure Endpoint Private Cloud/SWA/Secure Email Gateway** disponga delle licenze necessarie. È possibile verificare la chiave di funzionalità **SWA/Secure Email** o controllare che la licenza smart sia abilitata.
2. Se si prevede di ispezionare il traffico HTTPS, è necessario abilitare il proxy HTTPS su SWA. È necessario decrittografare il traffico HTTPS per eseguire i controlli della reputazione dei file.
3. È necessario configurare l'appliance **AMP Private Cloud/Virtual Private Cloud** e tutti i

certificati necessari. Consultare la guida al certificato VPC per la verifica.

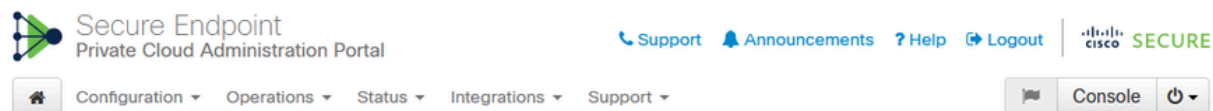
<https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/214326-how-to-generate-and-add-certificates-tha.html>

4. Tutti i nomi host dei prodotti devono essere DNS risolvibili. In questo modo si evitano problemi di connettività o problemi di certificato durante l'integrazione. Sul cloud privato Secure Endpoint, l'interfaccia Eth0 è per l'accesso Admin e Eth1 deve essere in grado di connettersi con i dispositivi di integrazione.

## Procedura

### Configurare il cloud privato Secure Endpoint


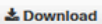
1. Accedere a Secure Endpoint VPC admin portal.
2. Andare a "Configuration" > "Services" > "Disposition Server" > Copia il nome host del server di disposizione (questo può essere recuperato anche dal terzo passo).
3. Passare a "Integrations" > "Web Security Appliance".
4. Scaricare il file "Disposition Server Public Key" & "Appliance Certificate Root" .
5. Passare a "Integrations" > "Email Security Appliance".
6. Selezionare la versione dell'ESA e scaricare "Disposition Server Public Key" e "Appliance Certificate Root".
7. Conservare il certificato e la chiave in un luogo sicuro. Deve essere caricato in SWA/Secure Email in un secondo momento.



#### 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** 

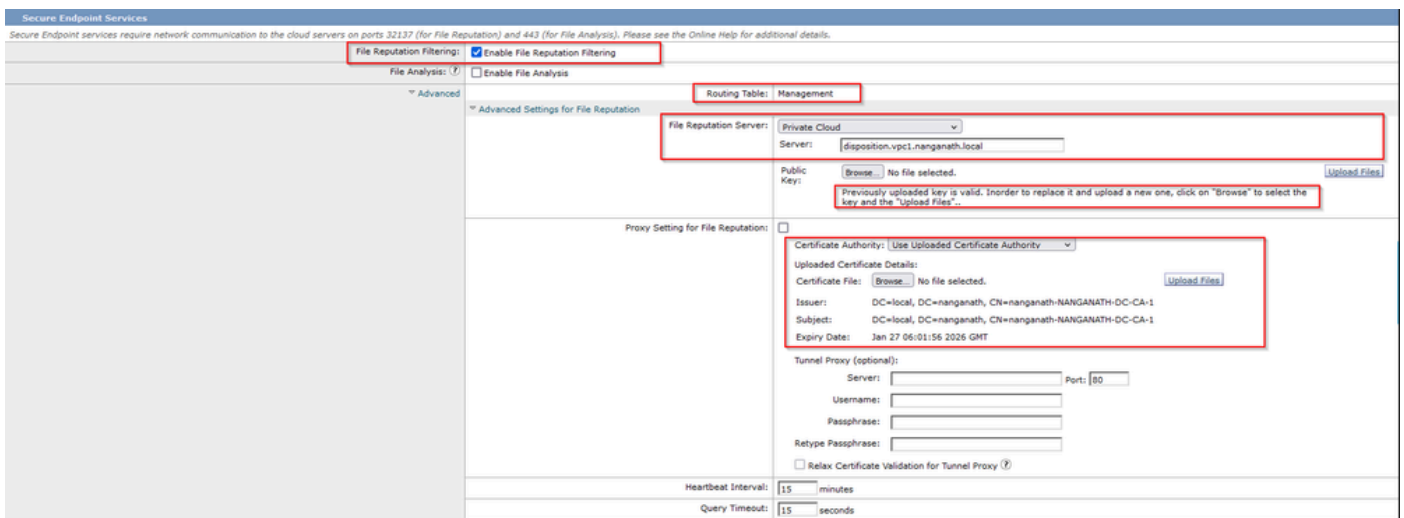
**Step 2: Proxy Setting**

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** 

## Configurazione di Secure Web Appliance

1. Passa a SWA GUI > "Security Services" > "Anti-Malware and Reputation" > Edit Global Settings
2. Nella sezione "Secure Endpoint Services" è possibile vedere l'opzione "Enable File Reputation Filtering", e "Check" questa opzione mostra un nuovo campo "Avanzate"
3. Selezionare "Private Cloud" nel file Reputation Server.
4. Specificare il nome host del server di disposizione del cloud privato come "Server".
5. Caricare la chiave pubblica scaricata in precedenza. Fare clic su "Upload Files".
6. È disponibile un'opzione per caricare l'Autorità di certificazione. Scegliere "Usa Autorità di certificazione caricata" dall'elenco a discesa e caricare il certificato CA scaricato in precedenza.
7. Invia la modifica
8. Conferma la modifica

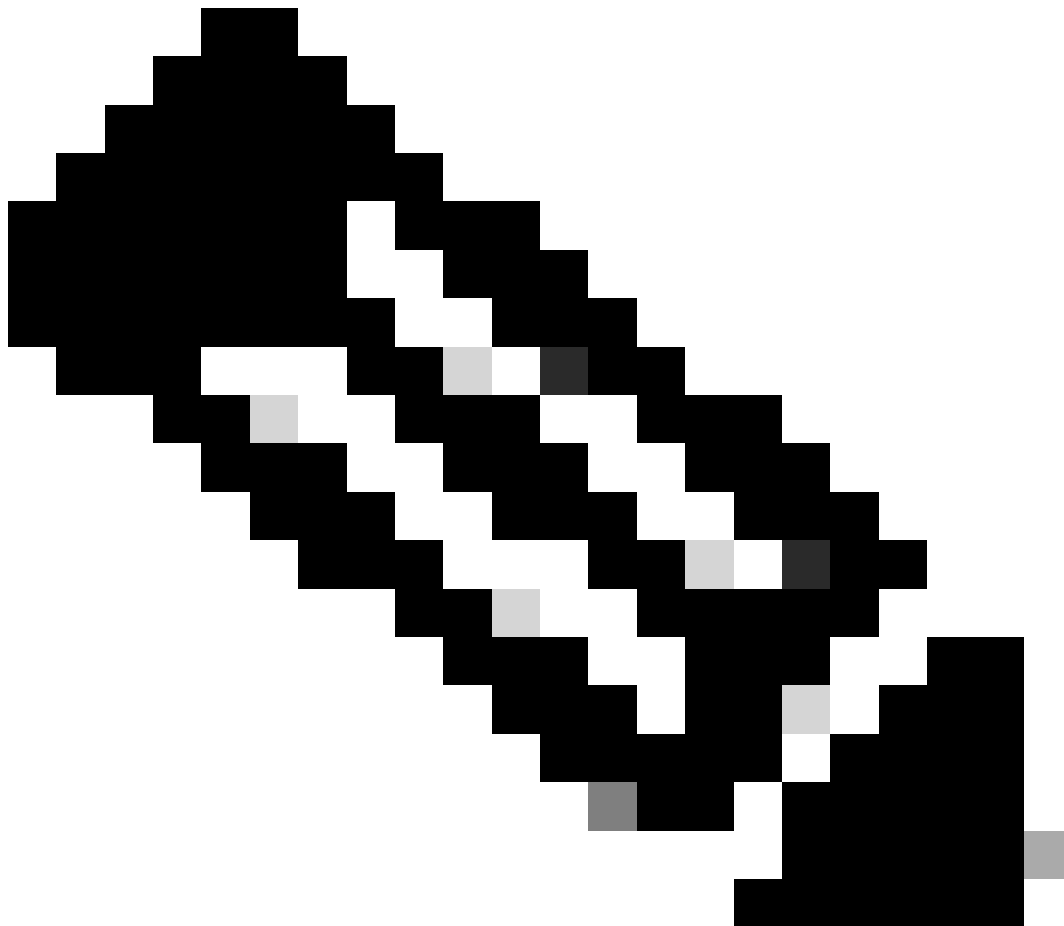


## Configurazione di Cisco Secure Email

1. Passare a Secure Email GUI > Security Services" > "File Reputation and Analysis" > Edit Global Settings > "Enable" or "Edit Global Settings"
2. Selezionare "Private Cloud" nel file Reputation Server
3. Specificare il nome host del server di disposizione del cloud privato come "Server".
4. Caricare la chiave pubblica che è stata scaricata in precedenza. Fare clic su "Upload Files".
5. Caricare l'autorità di certificazione. Scegliere "Usa Autorità di certificazione caricata" dall'elenco a discesa e caricare il certificato CA scaricato in precedenza.
6. Sottomettere la modifica
7. Confermare la modifica

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



Nota: Cisco Secure Web Appliance e Cisco Secure Email Gateway sono basati su AsyncOS e condividono quasi gli stessi log quando viene inizializzata la reputazione del file. Il registro AMP può essere osservato in Secure Web Appliance o nei registri AMP di Secure Email Gateway (registri simili in entrambi i dispositivi). Ciò indica solo che il servizio è inizializzato sul gateway SWA e Secure Email. Non è stato indicato che la connettività è stata eseguita correttamente. In caso di problemi di connettività o di certificato, è possibile visualizzare gli errori dopo il messaggio "Reputazione file inizializzata". Per lo più indica un errore "Errore irraggiungibile" o "Certificato non valido".

## Procedura per recuperare i registri AMP da Secure Web e posta elettronica

1. Accedere alla CLI di SWA/Secure Email Gateway e digitare il comando "grep"
2. Selezionare "amp" or "amp\_logs"
3. Lasciare invariati tutti gli altri campi e digitare "Y" per eseguire la coda dei log. Archiviare i log per visualizzare gli eventi live. Se si stanno cercando vecchi eventi, è possibile digitare la data in "espressione regolare"

```
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 dell'integrazione tra Secure Web Appliance e il cloud privato Secure Endpoint.

Non esiste un'opzione diretta per verificare la connettività da SWA. È necessario ispezionare i registri o gli avvisi per verificare l'eventuale presenza di problemi.

Per semplicità, stiamo testando un URL HTTP invece di HTTPS. È necessario decrittografare il traffico HTTPS per i controlli della reputazione dei file.

La configurazione viene eseguita in base alle regole di accesso SWA e viene applicata la scansione AMP.

Nota: consultare la [guida dell'utente](#) SWA per informazioni su come configurare i criteri in Cisco Secure Web Appliance.

### Access Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	<b>AP.Users</b> 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"/>

È stato effettuato un tentativo di scaricare un file dannoso "Bombermania.exe.zip" da Internet tramite Cisco Secure Web Appliance. Il registro indica che il file dannoso è BLOCCATO.

Log degli accessi SWA

I log degli accessi possono essere recuperati eseguendo la procedura seguente.

1. Accedere all'SWA e digitare il comando "grep"
2. Selezionare "accesslogs"
3. Se si desidera aggiungere una "espressione regolare" come IP client, specificarla.
4. Digitare "Y" per terminare il 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=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,"-","-",-1,"-","-","-","-","1,-
","-","-","IW_comp",-,"AMP High Risk","Computers and Internet","-","Unknown","Unknown","-","-
",333.79,0,-,"-","-
",37,"Win.Ransomware.Protected::Trojan.Agent.talos",0,"Bombermania.exe.zip","46ee42fb79a161bf3763
","-","-,-> -
```

TCP\_DENIED/403 → SWA ha negato questa richiesta HTTP GET.

BLOCK\_AMP\_RESP → La richiesta HTTP GET è stata bloccata a causa della risposta AMP.

Win.Ransomware.Protected::Trojan.Agent.talos → Nome minaccia

Bombermania.exe.zip → Nome del file che si è tentato di scaricare

46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8 → Valore SHA del

file

## Registri SWA AMP

I registri AMP possono essere recuperati eseguendo la procedura seguente.

1. Accedere all'SWA e digitare il comando "grep"
2. Selezionare "amp\_logs"
3. Lasciare invariati tutti gli altri campi e digitare "Y" per eseguire la coda dei log. Archiviare i log per visualizzare gli eventi live. Se si stanno cercando vecchi eventi, è possibile digitare la data in "espressione regolare"

'verdict\_from': 'Cloud' Sembra essere lo stesso per il cloud privato e il cloud pubblico. Non confondetelo come un verdetto della cloud pubblica.

```
lun feb 19 10:53:56 2024 Debug: Verdetto adattato - {'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': Nessuno, 'extract_file_verdict_list': '', 'verdict_from': 'Cloud', 'analysis_action': 2, 'file_type': 'application/zip', 'score': 0, 'upload_reason': 'Il tipo di file non è configurato per la sandboxing', 'sha256': '46ee42fb79a161bf3763e8e34a047018bd16d872f8d31c2cdecae3d2e7a57a8', 'verdict_str': 'MALICIOUS', 'malicious_child': None}
```

## Registri eventi cloud privati endpoint sicuro

I registri eventi sono disponibili in /data/cloud/log

È possibile cercare l'evento con SHA256 o utilizzando l'ID client di reputazione file dell'SWA. "File Reputation Client ID" è presente nella pagina di configurazione AMP dell'SWA.

```
[root@fireamp log]# pwd
/data/cloud/log
[root@fireamp log]# less eventlog | grep -iE "46ee42fb79a161bf3763e8e34a047018bd16d872f8d31c2cdecae3d2e7a57a8"
"op":3,"ip":"10.106.39.144","si":0,"ti":3,"tv":6,"qt":42,"pr":1,"ets":1708320235,"ts":1708320232,"tsns":707403179,"uu":"9a7a27a1-40aa-452f-a070-ed78e215b717","al":1,"aptus":1344,"ptus":975590,"spero":{"h":"00","fa":0,"fs":0,"ft":0,"hd":1},"sha256":{"h":"46EE42FB79A161BF3763E8E34A047018BD16D872F8D31C2CDECAE3D2E7A57A8","fa":0,"fs":0,"ft":0,"hd":3},"hord":{"s":4},"on":"win.Ransomware.Protected::Trojan.Agent.talos","url":"http://static1.1.sqspcdn.com/static/7/630757/219084257138068801630778b0mgerman.va.exe.zip?token=g3rA10rL00mMy2Aw1c28pg31jKw2s30","rd":3,"ra":2,"n":0}
```

pv - Versione protocollo, 3 indica TCP

ip - Ignorare questo campo perché non vi è alcuna garanzia che questo campo indichi l'indirizzo IP effettivo del client che ha eseguito la query sulla reputazione

uu - ID client reputazione file in WSA/ESA

SHA256 - SHA256 del file

dn - Nome del rilevamento

n - 1 se l'hash del file non è mai stato rilevato da AMP, 0 in caso contrario.

rd - Response Disposition. dove 3 indica DISP\_MALICIOUS



- 1 DISP\_UNKNOWN La disposizione del file è sconosciuta.
- 2 DISP\_CLEAN Il file è considerato innocuo.
- 3 DISP\_MALICIOUS Si ritiene che il file sia dannoso.
- 7 DISP\_UNSAW La disposizione del file è sconosciuta ed è la prima volta che lo vediamo.
- 13 DISP\_BLOCK Non eseguire il file.
- 14 DISP\_IGNORE XXX
- 15 DISP\_CLEAN\_PARENT Si ritiene che il file sia innocuo e che tutti i file dannosi creati debbano essere considerati sconosciuti.
- 16 DISP\_CLEAN\_NFM Il file è ritenuto innocuo, ma il client deve monitorare il traffico di rete.

## Test dell'integrazione tra Secure Email e AMP private cloud

Non è disponibile un'opzione diretta per verificare la connettività dal gateway di posta elettronica sicura. È necessario ispezionare i registri o gli avvisi per verificare l'eventuale presenza di problemi.

La configurazione viene eseguita nel criterio Posta in arrivo posta elettronica protetta per applicare la scansione AMP.

### 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	
<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.

l'ESA è stata sottoposta a prova con un file non dannoso. Questo è un file CSV.

Registri\_posta posta elettronica protetta

```

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-PF253NKG, 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-PF253NKG, 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+HhA4cFJo0192j3QSDhLDnEkX9DPClxVhx3o3lC136to+7zXqIaVVPPh6X+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-90381C261f0e3e9330710ab96647358c461f6834c0ca001408e40decdf19dbe 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 : <99221a1xwesi1.nanganath.local>
Tue Feb 20 11:57:01 2024 Info: MID 660 queued for delivery
Tue Feb 20 11:57:02 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
  
```

Registri AMP Secure Email

Mar Feb 20 11:57:01 2024 Informazioni: risposta ricevuta per la query sulla reputazione del file da Cloud. Nome file = Dettagli formazione.csv, MID = 660, Disposizione = FILE SCONOSCIUTO, Malware = Nessuno, Punteggio analisi = 0, sha256 = 90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19d, upload\_action = Consigliato per inviare il file per l'analisi, verdict\_source = AMP, suspense\_categories = None

Registri eventi cloud privati endpoint sicuri

```
{"pv":3,"ip":"10.106.72.238","si":0,"ti":14,"tv":6,"qt":42,"pr":1,"ets":1708410419,"ts":1708410366,"tsns":291,"u":"cb1b31fc-9277-4008-a396-6cd486ecc621","ai":1,"aptus":295,"ptus":2429102,"spero":{"h":"00","fa":0,"fs":0,"ft":0,"hd":1},"sha256":{"h":"90381C261F8BE3E933071DAB9647358C461F6834C8CA0014D8E40DEC4F19DBE","fa":0,"fs":0,"ft":0,"ra":1,"n":0}}
```

rd - 1 DISP\_UNKNOWN. La disposizione del file è sconosciuta.

## Problemi comuni osservati che determinano un errore di integrazione

1. Scelta della "tabella di routing" errata in SWA o Secure Email. Il dispositivo integrato deve essere in grado di comunicare con l'interfaccia Eth1 del cloud privato AMP.
2. Il nome host VPC non è risolvibile DNS in SWA o Secure Email, il che porta a errori nel stabilire la connessione.
3. Il CN (nome comune) nel certificato di smaltimento VPC deve corrispondere al nome host VPC e a quello indicato in SWA e Secure Email Gateway.
4. L'utilizzo di un cloud privato e di un'analisi di file cloud non è una progettazione supportata. Se si utilizza un dispositivo locale, l'analisi e la reputazione del file devono essere un server locale.
5. Verificare che non vi siano problemi di sincronizzazione dell'ora tra AMP private cloud e SWA, Secure Email.
6. L'impostazione predefinita di SWA DVS Engine Object Scanning Limit è 32 MB. Modificare questa impostazione se si desidera eseguire la scansione di file di dimensioni maggiori. Si noti che si tratta di un'impostazione globale e influisce su tutti i motori di scansione, quali Webroot, Sophos e così via.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).