

# Integre la nube privada de terminales seguros con una Web y un correo electrónico seguros

## Contenido

---

### [Introducción](#)

### [Prerequisites](#)

[Componentes Utilizados](#)

[Comprobaciones de verificación antes de proceder a la integración](#)

### [Procedimiento](#)

[Configuración de la nube privada de terminal seguro](#)

[Configuración del dispositivo web seguro](#)

[Configuración de Cisco Secure Email](#)

[Los pasos para obtener registros de AMP desde la Web segura y el correo electrónico](#)

[Prueba de la integración entre el dispositivo web seguro y la nube privada de terminal seguro.](#)

[Registros de acceso SWA](#)

[Registros de AMP SWA](#)

---

## Introducción

En este documento se describen los pasos necesarios para integrar la nube privada de terminal seguro con el dispositivo web seguro (SWA) y el gateway de correo electrónico seguro (ESA).

## Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- AMP para terminales seguros para nube privada virtual
- Dispositivo web seguro (SWA)
- Gateway de correo electrónico seguro

## Componentes Utilizados

SWA (Secure Web Appliance) 15.0.0-322

AMP para nube privada virtual 4.1.0\_202311092226

Secure Email Gateway 14.2.0-620

---



Nota: La documentación es válida para variaciones físicas y virtuales de todos los productos involucrados.

---

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

### Comprobaciones de verificación antes de proceder a la integración

1. Compruebe si **Secure Endpoint Private Cloud/SWA/Secure Email Gateway** dispone de las licencias necesarias. Puede comprobar la clave de característica **SWA/Secure Email** o comprobar que la licencia inteligente está habilitada.
2. El proxy **HTTPS** debe estar activado en **SWA** si tiene previsto inspeccionar el tráfico **HTTPS**. Debe descifrar el tráfico **HTTPS** para poder realizar cualquier comprobación de reputación de archivos.
3. Se deben configurar el appliance **AMP** para nube privada/nube privada virtual y todos los

certificados necesarios. Consulte la guía de certificados VPC para obtener información sobre la verificación.

<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. Todos los nombres de host de los productos deben poder resolverse mediante DNS. Esto es para evitar cualquier problema de conectividad o problemas de certificados mientras se integra. En la nube privada de Secure Endpoint, la interfaz Eth0 es para el acceso de administrador y Eth1 debe poder conectarse con los dispositivos de integración.

## Procedimiento

### Configuración de la nube privada de terminal seguro

1. Inicie sesión en el Secure Endpoint VPC admin portal.
2. Vaya a “Configuration” > “Services” > “Disposition Server” > Copiar el nombre de host del servidor de disposición (también se puede obtener desde el tercer paso) .
3. Vaya a .“Integrations” > “Web Security Appliance”
4. Descargue el “Disposition Server Public Key” & “Appliance Certificate Root” .
5. Vaya a .“Integrations” > “Email Security Appliance”
6. Seleccione la versión de su ESA y descargue las opciones "Disposition Server Public Key" (Clave pública del servidor de disposición) y "Appliance Certificate Root" (Raíz del certificado del dispositivo).
7. Por favor, guarde el certificado y la clave a salvo. Debe cargarse en SWA/Secure Email más tarde.

## 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.

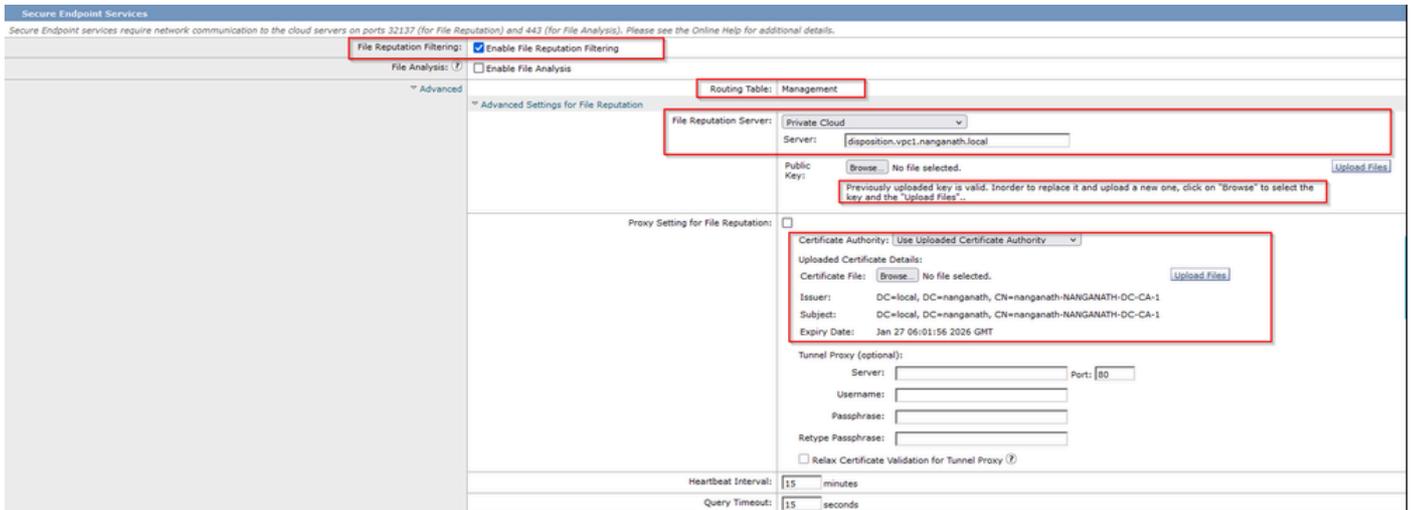


Appliance Certificate Root

Download

## Configuración del dispositivo web seguro

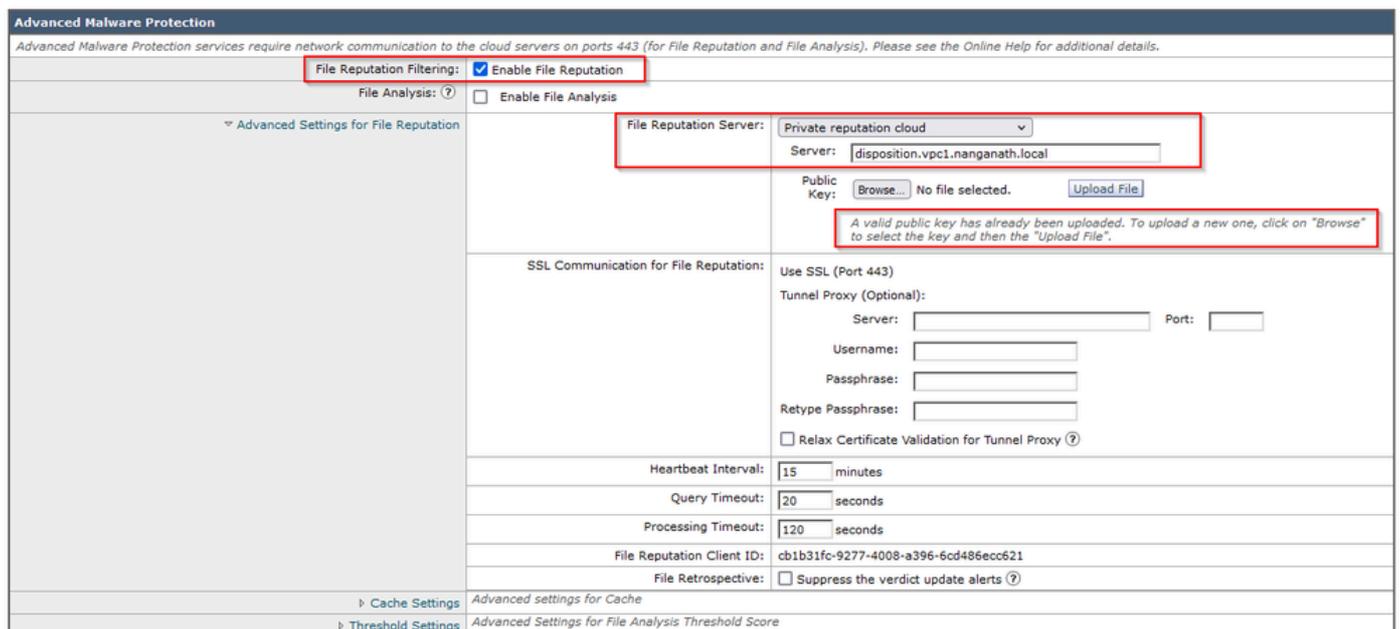
1. Vaya a SWA GUI > "Security Services" > "Anti-Malware and Reputation" > Edit Global Settings
2. En la sección "Secure Endpoint Services" puede ver la opción "Enable File Reputation Filtering" (Activar filtrado de reputación de archivos) y "Check" (Comprobar). Esta opción muestra un nuevo campo "Advanced" (Avanzado).
3. Seleccione "Nube privada" en File Reputation Server.
4. Proporcione el nombre de host del servidor de disposición de la nube privada como "Servidor".
5. Cargue la clave pública que descargó anteriormente. Haga clic en Cargar archivos.
6. Existe la opción de cargar la autoridad de certificación. Elija "Usar autoridad de certificación cargada" en el menú desplegable y cargue el certificado de CA que descargó anteriormente.
7. Envíe el cambio
8. Confirme el cambio



## Configuración de Cisco Secure Email

1. Acceda a Secure Email GUI > Security Services” > “File Reputation and Analysis” > Edit Global Settings > “Enable” or “Edit Global Settings”
2. Seleccione "Nube privada" en File Reputation Server
3. Proporcione el nombre de host del servidor de disposición de la nube privada como "Servidor".
4. Cargue la clave pública que hemos descargado anteriormente. Haga clic en Cargar archivos.
5. Cargue la autoridad certificadora. Elija "Usar autoridad de certificación cargada" en el menú desplegable y cargue el certificado de CA que descargó anteriormente.
6. Ejecute el cambio
7. Confirme el cambio

### Edit File Reputation and Analysis Settings





Nota: Cisco Secure Web Appliance y Cisco Secure Email Gateway se basan en AsyncOS y comparten casi los mismos registros cuando se inicializa la reputación del archivo. El registro de AMP se puede observar en los registros de AMP de Secure Web Appliance o Secure Email Gateway (registros similares en ambos dispositivos). Esto solo indica que el servicio se ha inicializado en el SWA y el gateway de correo electrónico seguro. No indicó que la conectividad fuera completamente exitosa. Si hay algún problema de conectividad o de certificado, puede ver errores después del mensaje "Reputación de archivos inicializada". Principalmente, indica un error de "error inalcanzable" o "certificado no válido".

---

## Los pasos para obtener registros de AMP desde la Web segura y el correo electrónico

1. Inicie sesión en la CLI de SWA/Secure Email Gateway y escriba el comando `"grep"`
2. Seleccione `"amp"` or `"amp_logs"`

3. Deje todos los demás campos tal como están y escriba "Y" para finalizar los registros. Siga los registros para mostrar los eventos en directo. Si está buscando eventos antiguos, puede escribir la fecha en "expresión regular"

```
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.
```

Prueba de la integración entre el dispositivo web seguro y la nube privada de terminal seguro.

No existe ninguna opción directa para probar la conectividad desde SWA. Debe inspeccionar los registros o alertas para comprobar si hay algún problema.

Para simplificar el proceso, estamos probando una URL HTTP en lugar de HTTPS. Tenga en cuenta que debe descifrar el tráfico HTTPS para realizar cualquier comprobación de reputación de archivos.

La configuración se realiza en la política de acceso de SWA y se aplica el análisis de AMP.

Nota: Revise la [guía del usuario de SWA](#) para saber cómo configurar las políticas en 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	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.

	Monitor	Block
File Reputation		
Known Malicious and High-Risk Files		

Se intentó descargar un archivo malicioso "Bombermania.exe.zip" de Internet a través del dispositivo web seguro de Cisco. El registro muestra que el archivo malicioso está BLOQUEADO.



```
18, 'verdict_num': 3, 'analysis_score': 0, 'upload': False, 'file_name': 'Bombermania.exe.zip',
'verdict_source': Ninguno, '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', 'malicioso_child': None}
```

Registros de eventos de nube privada de terminal seguro

Los registros de eventos están disponibles en `/data/cloud/log`

Puede buscar el evento con el SHA256 o mediante la "ID de cliente de reputación de archivo" del SWA. "ID de cliente de Reputación de archivos" está presente en la página de configuración de AMP del SWA.

```
[root@fireamp log]# pwd
/data/cloud/log
[root@fireamp log]#
[root@fireamp log]# less eventlog | grep -iE "46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8"
[cpu:3] ip:"10.106.39.144" si:"0" ti:"3" tv:"6" qt:"d2" pr:"i" ets:"1708320235" ts:"1708320232" tsn:"1707403179" uu:"9a7a27a1-46aa-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:"52.4.4" dn:"w.urn.Kansomware.Protected:trojan.Agent.talos" url:"http:
//static1.1.sqspcdn.com/static/7/830757/z1908425/z1300888016907/Bombermania.exe.zip/token=gsRk10FL00mnyJAM1%2Bpg31jKRWQ%3D" rd:"3" ra:"2" n:"0"
```

pv - Versión de protocolo, 3 indica TCP

ip: ignore este campo porque no hay garantía de que este campo indique la dirección IP real del cliente que realizó la consulta de reputación

uu: ID de cliente de reputación de archivos en WSA/ESA

SHA256 - SHA256 del archivo

dn: el nombre de la detección

n - 1 si AMP nunca ha visto el hash de archivos, 0 en caso contrario.

rd - Disposición de respuesta. aquí 3 significa DISP\_MALICIOUS

- 1 DISP\_UNKNOWN Se desconoce la disposición del archivo.
- 2 DISP\_CLEAN Se cree que el archivo es benigno.
- 3 DISP\_MALICIOUS Se cree que el archivo es malicioso.
- 7 DISP\_UNSEEN La disposición del archivo es desconocida y es la primera vez que vemos el archivo.
- 13 DISP\_BLOCK No se debe ejecutar el archivo.
- 14 DISP\_IGNORE XXX
- 15 DISP\_CLEAN\_PARENT Se cree que el archivo es benigno, por lo que cualquier archivo malicioso que cree debe tratarse como desconocido.
- 16 DISP\_CLEAN\_NFM Se cree que el archivo es benigno, pero el cliente debe supervisar el tráfico de red.

## Prueba de la integración entre Secure Email y la nube privada de AMP

No existe ninguna opción directa para probar la conectividad desde el gateway de correo electrónico seguro. Debe inspeccionar los registros o alertas para comprobar si hay algún

problema.

La configuración se realiza en la directiva de correo entrante de correo electrónico seguro para aplicar el análisis de 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
<b>Message Scanning</b>	
	<input checked="" type="checkbox"/> (recommended) Include an X-header with the AMP results in messages
<b>Unscannable Actions on Message Errors</b>	
Action Applied to Message:	Deliver As Is
Advanced	Optional settings for custom header and message delivery.
<b>Unscannable Actions on Rate Limit</b>	
Action Applied to Message:	Deliver As Is
Advanced	Optional settings for custom header and message delivery.
<b>Unscannable Actions on AMP Service Not Available</b>	
Action Applied to Message:	Deliver As Is
Advanced	Optional settings for custom header and message delivery.
<b>Messages with Malware Attachments:</b>	
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
Advanced	[WARNING: MALWARE DETECTED] Optional settings.
<b>Messages with File Analysis Pending:</b>	
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
Advanced	[WARNING: ATTACHMENT(S) MAY CONTAIN Optional settings.

ESA probado con un archivo no malintencionado. Este es un archivo CSV.

## Correo electrónico seguro 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 SG 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: 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: <ajayraj@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_/T0Y46k/XzoIL66+HNA4cF3o0192j305Dh1DLnEx90PClxVhx3o3lC136to+72XQiaVVP6hXLcND+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 attachment "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: <9222a3kqesai.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
```

## Registros de AMP de correo electrónico seguro

Mar Feb 20 11:57:01 2024 Info: Respuesta recibida para la consulta de reputación de archivos desde la nube. Nombre de archivo = Detalles de formación.csv, MID = 660, Disposición = ARCHIVO DESCONOCIDO, Malware = Ninguno, Puntuación del análisis = 0, sha256 = 90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19dbe, upload\_action = Se recomienda enviar el archivo para su análisis, veredicto t\_source = AMP, categorías\_sospechosas = Ninguna

## Registros de eventos de Secure Endpoint Private Cloud

```
{"pv":3,"ip":"10.106.72.238","si":0,"ti":14,"tv":6,"qt":42,"pr":1,"ets":1708410419,"ts":1708410366,"tsns":2999277-4008-a396-6cd4
```

```
86ecc621","ai":1,"aptus":295,"ptus":2429102,"spero":{"h":"00","fa":0,"fs":0,"ft":0,"hd":1},"sha256":{"h":"90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19dbe","fa":0,"fs":0,"ft":0,"hd":1},"hord":[32,4],"rd":1,"ra":1,"n":0}
```

rd - 1 DISP\_UNKNOWN. Se desconoce la disposición del archivo.

## Problemas habituales observados que provocan errores de integración

1. Elegir la "tabla de routing" incorrecta en SWA o correo electrónico seguro. El dispositivo integrado debe poder comunicarse con la interfaz Eth1 de la nube privada de AMP.
2. El nombre de host de VPC no se puede resolver mediante DNS en SWA o Secure Email, lo que provoca un fallo al establecer la conexión.
3. El CN (nombre común) del certificado de disposición de VPC debe coincidir con el nombre de host de VPC, así como con el mencionado en SWA y Secure Email Gateway.
4. El uso de una nube privada y un análisis de archivos en la nube no es un diseño compatible. Si utiliza un dispositivo en las instalaciones, el análisis de archivos y la reputación deben ser un servidor en las instalaciones.
5. Asegúrese de que no haya ningún problema de sincronización horaria entre la nube privada de AMP y SWA, Secure Email.
6. El valor predeterminado del límite de escaneo de objetos del motor DVS de SWA es 32 MB.

Ajuste esta configuración si desea analizar archivos más grandes. Tenga en cuenta que se trata de una configuración global que afecta a todos los motores de análisis, como Webroot, Sophos, etc.

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).