

# Integre a nuvem privada de endpoint segura com Web e e-mail seguros

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Verificações antes de prosseguir com a integração](#)

[Procedimento](#)

[Configurar a nuvem privada do Secure Endpoint](#)

[Configurar o Secure Web Appliance](#)

[Configurar o Cisco Secure Email](#)

[As etapas para buscar registros da AMP no Secure Web e e-mail](#)

[Testando a integração entre o Secure Web Appliance e a nuvem privada do Secure Endpoint.](#)

[Logs de acesso SWA](#)

[Logs SWA AMP](#)

---

## Introdução

Este documento descreve as etapas necessárias para integrar a nuvem privada do Secure Endpoint ao Secure Web Appliance (SWA) e ao Secure Email Gateway (ESA).

## Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Endpoint seguro AMP Nuvem privada virtual
- Secure Web Appliance(SWA)
- Gateway de e-mail seguro

## Componentes Utilizados

SWA (Secure Web Appliance) 15.0.0-322

AMP virtual private cloud 4.1.0\_202311092226

Secure Email Gateway 14.2.0-620



Observação: a documentação é válida para variações físicas e virtuais de todos os produtos envolvidos.

---

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

### Verificações antes de prosseguir com a integração

1. Verifique se **Secure Endpoint Private Cloud/SWA/Secure Email Gateway** ele tem as licenças necessárias. Você pode verificar a chave de recurso **SWA/Secure Email** ou verificar se a licença inteligente está habilitada.
2. O proxy **HTTPS** deverá ser habilitado no **SWA** se você estiver planejando inspecionar o tráfego **HTTPS**. Você precisa descriptografar o tráfego **HTTPS** para fazer verificações de reputação de arquivo.
3. O dispositivo **AMP Private Cloud/Virtual Private Cloud** e todos os certificados necessários

devem ser configurados. Consulte o guia de certificado VPC para verificação.

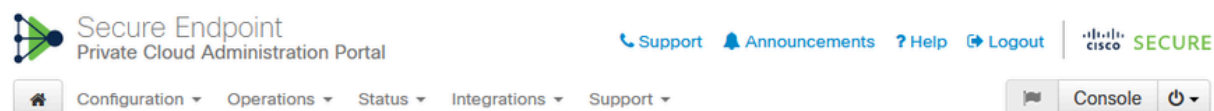
<https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/214326-how-to-generate-and-add-certificates-tha.html>

4. Todos os nomes de host dos produtos devem ser resolvíveis pelo DNS. Isso evita qualquer problema de conectividade ou de certificado durante a integração. Na nuvem privada do Secure Endpoint, a interface Eth0 é para acesso de Admin e Eth1 deve ser capaz de se conectar com dispositivos de integração.

## Procedimento

### Configurar a nuvem privada do Secure Endpoint


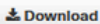
1. Faça login no Secure Endpoint VPC admin portal.
2. Vá para “Configuration” > “Services” > “Disposition Server” > Copie o nome de host do servidor de descarte (isso também pode ser buscado a partir da terceira etapa) .
3. Navegue até “Integrations” > “Web Security Appliance”.
4. Faça o download do “Disposition Server Public Key” & “Appliance Certificate Root” .
5. Navegue até “Integrations” > “Email Security Appliance”.
6. Selecione a versão do seu ESA e faça o download da "Disposition Server Public Key" e da "Appliance Certificate Root".
7. Mantenha o certificado e a chave em segurança. Ele deve ser carregado para SWA/Secure Email posteriormente.



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


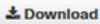
**Step 1: Web Security Appliance Setup**

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** 

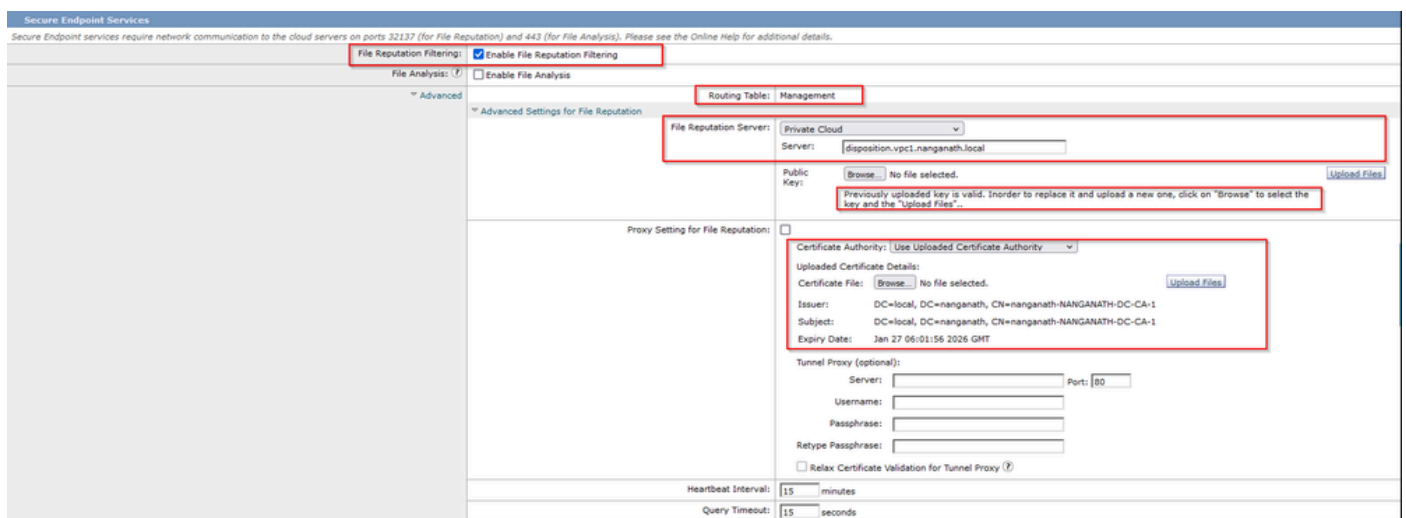
**Step 2: Proxy Setting**

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** 

## Configurar o Secure Web Appliance

1. Navegue até SWA GUI > “Security Services” > “Anti-Malware and Reputation” > **Edit Global Settings**
2. Na seção "Serviços de endpoint seguros", você pode ver a opção "Habilitar filtragem de reputação de arquivo" e "Marcar" esta opção mostra um novo campo "Avançado"
3. Selecione "Nuvem privada" no servidor de reputação de arquivos.
4. Forneça o nome de host do Servidor de descarte de nuvem privada como "Servidor".
5. Carregue a chave pública que você baixou anteriormente. Clique em "Carregar arquivos".
6. Há uma opção para carregar a Autoridade de Certificação. Selecione "Usar autoridade de certificação carregada" no menu suspenso e carregue o certificado de autoridade de certificação baixado anteriormente.
7. Enviar a alteração
8. Confirmar a alteração

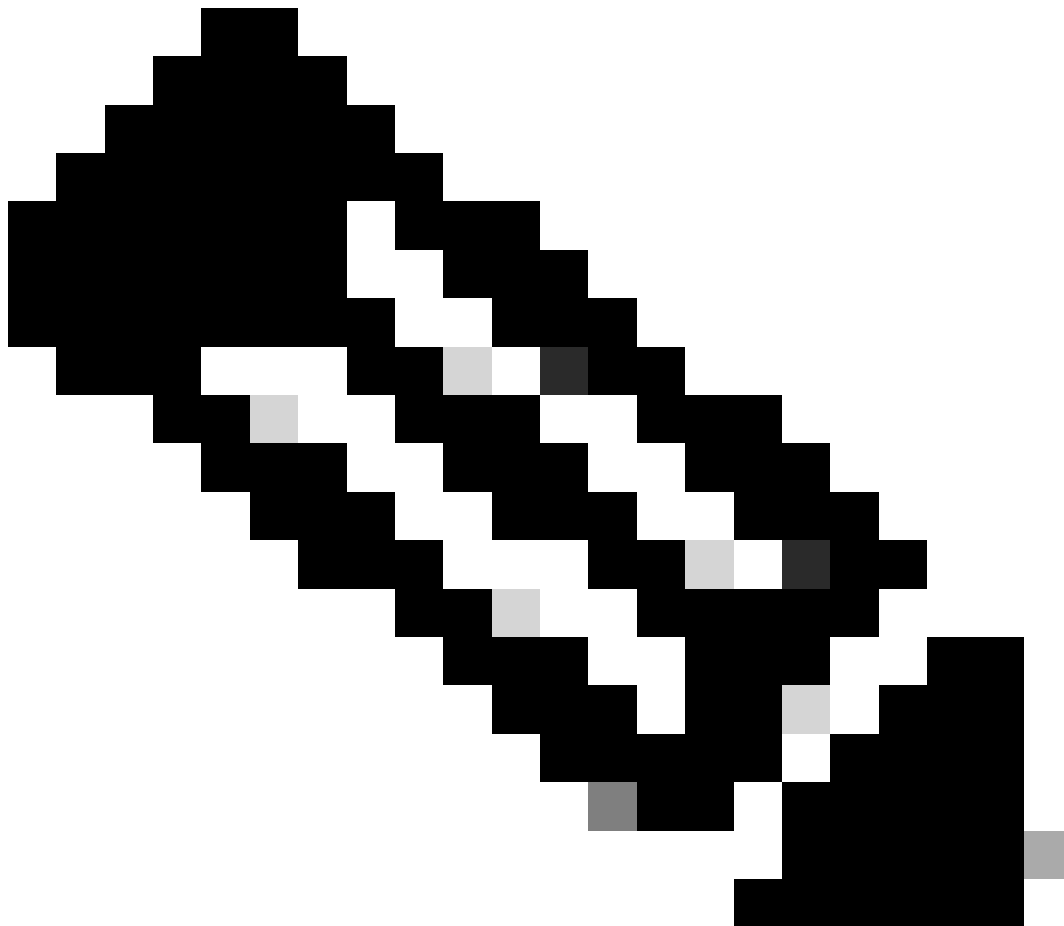


## Configurar o Cisco Secure Email

1. Navegue até Secure Email GUI > Security Services” > “File Reputation and Analysis” > **Edit Global Settings** > “Enable” or “Edit Global Settings”
2. Selecione "Nuvem privada" no servidor de reputação de arquivos
3. Forneça o nome de host do Servidor de descarte da nuvem privada como "Servidor".
4. Carregue a chave pública que baixamos anteriormente. Clique em "Carregar arquivos".
5. Faça upload da Autoridade de Certificação. Selecione "Usar autoridade de certificação carregada" no menu suspenso e carregue o certificado de autoridade de certificação baixado anteriormente.
6. Submeta a alteração
7. Confirme a alteração

## 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



Observação: o Cisco Secure Web Appliance e o Cisco Secure Email Gateway são baseados no AsyncOS e compartilham quase os mesmos registros quando a reputação do arquivo é inicializada. O registro da AMP pode ser observado nos registros da AMP do Secure Web Appliance ou do Secure Email Gateway (registros semelhantes em ambos os dispositivos). Isso indica apenas que o serviço foi inicializado no SWA e no Secure Email Gateway. Não indicou que a conectividade foi totalmente bem-sucedida. Se houver qualquer problema de conectividade ou certificado, você poderá ver erros após a mensagem "Reputação de arquivo inicializada". Na maioria das vezes, indica um erro "Erro inalcançável" ou "certificado inválido".

## As etapas para buscar registros da AMP no Secure Web e e-mail

1. Faça login na CLI do SWA/Secure Email Gateway e digite o comando "grep"
2. Selecione "amp" or "amp\_logs"
3. Deixe todos os outros campos como estão e digite "Y" para acompanhar os logs. Registre os logs para mostrar os eventos ao vivo. Se você estiver procurando por eventos antigos, digite a data em "expressão 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.
```

## Testando a integração entre o Secure Web Appliance e a nuvem privada do Secure Endpoint.

Não há opção direta para testar a conectividade do SWA. Você deve inspecionar os logs ou alertas para verificar se há algum problema.

Para simplificar, estamos testando uma URL HTTP em vez de HTTPS. Observe que você precisa descriptografar o tráfego HTTPS para qualquer verificação de reputação de arquivo.

A configuração é feita na política de acesso do SWA e a verificação da AMP é aplicada.

Observação: revise o [guia do usuário do SWA](#) para entender como configurar as políticas no Cisco Secure Web Appliance.

### Access Policies

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"/>

Tentou-se fazer o download de um arquivo malicioso "Bombermania.exe.zip" da Internet através do Cisco secure web appliance. O registro mostra que o arquivo malicioso está BLOQUEADO.

### Logs de acesso SWA

Os logs de acesso podem ser buscados por estas etapas.

1. Faça login no SWA e digite o comando "grep"
2. Selecione "accesslogs"
3. Se você quiser adicionar qualquer "expressão regular", como o IP do cliente, por favor, mencione-o.
4. Digite "Y" para terminar o 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-NONE-DefaultGroup-NONE <"IW_comp",3.7,1,"-,-,-,-,1,"-,-,-,
,-,-,-,1,-,-,"-,-,-,"IW_comp",-,"AMP de alto risco","Computadores e Internet",-
,"Desconhecido","Desconhecido",-,"-",-,"333.79,0,-,-,-"
",-,"Win.Ransomware.Protected::Trojan.Agent.talos",0,0,"Bombermania.exe.zip","46ee42fb7
9a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8",3,-,-,-> -
```

TCP\_DENIED/403 → SWA negou esta solicitação HTTP GET.

BLOCK\_AMP\_RESP → A solicitação HTTP GET foi bloqueada devido à resposta da AMP.

Win.Ransomware.Protected::Trojan.Agent.talos → Nome da Ameaça

Bombermania.exe.zip → Nome do arquivo que tentamos baixar

46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8 → Valor SHA do arquivo

## Logs SWA AMP

Os registros da AMP podem ser obtidos usando essas etapas.

1. Faça login no SWA e digite o comando "grep"
2. Selecione "amp\_logs"
3. Deixe todos os outros campos como estão e digite "Y" para acompanhar os logs. Registre os logs para mostrar os eventos ao vivo. Se você estiver procurando por eventos antigos, digite a data em "expressão regular"

'verdict\_from': 'Cloud' Parece ser o mesmo para nuvem privada e pública. Não confunda isso com um veredito da nuvem pública.

```
Seg 19 de fevereiro 10:53:56 2024 Depuração: Veredito ajustado - {'category': 'amp', 'spyname': 'Win.Ransomware.Protected::Trojan.Agent.talos', 'original_verdict': 'MALICIOUS', 'analysis_status': 18, 'verdict_num': 3, 'analysis_score': 0, 'uploaded': False, 'file_name': 'Bombermania.exe zip', 'verdict_source': None, 'extract_file_verdict_list': '', 'verdict_from': 'Cloud', 'analysis_action': 2, 'file_type': 'application/zip', 'score': 0, 'upload_reason': 'Tipo de arquivo não configurado para sandbox', 'sha256': '46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8', 'verdict_str': 'MALICIOUS', 'malicioso_child': Nenhum}
```

## Logs de eventos de nuvem privada de endpoint seguro

Os registros de eventos estão disponíveis em /data/cloud/log

Você pode procurar o evento com o SHA256 ou usando o "ID do cliente de reputação de arquivo" do SWA. A "ID do cliente do File Reputation" está presente na página de configuração da AMP do SWA.

```
[root@fireamp log]# pwd
/data/cloud/log
[root@fireamp log]# less eventlog | grep -E "46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8"
[cpu:3] ip: "10.106.39.144" si:0, ti:3, tv:6, qt:42, pr:i, ets:1708320235, ts:1708320232, tsn4:707403179, 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:{"id":47, dn:win.Ransomware.Protected::Trojan.Agent.talos, url:"http://static1.1.sqspcdn.com/static/1/7830757/21908425/1350888016307/Bombermania.exe.zip?token=g3FX10FLU0mnyJAm%2Bpg31jK9wQ%3D", rd:3, ra:2, n:0}
```

pv - Versão do Protocolo, 3 indica TCP

ip - Ignore esse campo, pois não há garantia de que ele indique o endereço IP real do cliente que fez a consulta de reputação

uu - ID do cliente de reputação de arquivo no WSA/ESA

SHA256 - SHA256 do arquivo

dn - O nome da detecção

n - 1 se o hash do arquivo nunca tiver sido visto antes pelo AMP, 0 caso contrário.



o - Disposição da resposta. aqui 3 significa DISP\_MALICIOUS

1 DISP\_UNKNOWN A disposição do arquivo é desconhecida.

2 DISP\_CLEAN O arquivo é considerado benigno.

3 DISP\_MALICIOUS O arquivo é considerado mal-intencionado.

7 DISP\_UNSEEN A disposição do arquivo é desconhecida e é a primeira vez que o vemos.

13 DISP\_BLOCK O arquivo não deve ser executado.

14 DISP\_IGNORE XXX

15 DISP\_CLEAN\_PARENT Acredita-se que o arquivo seja benigno e que quaisquer arquivos mal-intencionados que ele crie devam ser tratados como desconhecidos.

16 DISP\_CLEAN\_NFM Acredita-se que o arquivo seja benigno, mas o cliente deve monitorar o tráfego de rede.

## Testando a integração entre e-mail seguro e a nuvem privada da AMP

Não há opção direta para testar a conectividade do gateway do Secure Email. Você deve inspecionar os logs ou alertas para verificar se há algum problema.

A configuração é feita na política de recebimento de e-mail seguro para aplicar a varredura da 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.

testou o ESA com um arquivo não mal-intencionado. Este é um arquivo CSV.

Email mail\_logs seguro

```

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+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-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
  
```

Logs AMP de e-mail seguros

Ter 20 de fevereiro 11:57:01 2024 Informações: Resposta recebida para consulta de reputação de arquivo da nuvem. Nome do arquivo = Detalhes do treinamento.csv, MID = 660, Disposição = ARQUIVO DESCONHECIDO, Malware = Nenhum, Pontuação da análise = 0, sha256 = 90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19dbe, upload\_action = Recomendado para enviar o arquivo para análise, dict\_source = AMP, suspect\_categories = None

Logs de eventos de nuvem privada de endpoints seguros

```
{"pv":3,"ip":"10.106.72.238","si":0,"ti":14,"tv":6,"qt":42,"pr":1,"ets":1708410419,"ts":1708410366,"tsns":2999277-4008-a396-6cd86ecc621","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. A disposição do arquivo é desconhecida.

## Problemas comuns observados que resultam em falha de integração

1. Escolher a "tabela de roteamento" incorreta no SWA ou no Secure Email. O dispositivo integrado deve ser capaz de se comunicar com a interface Eth1 da nuvem privada do AMP.
2. O nome de host VPC não pode ser resolvido por DNS em SWA ou Secure Email, o que leva a uma falha no estabelecimento da conexão.
3. O CN (Nome comum) no certificado de descarte do VPC deve corresponder ao nome de host do VPC, bem como ao mencionado no SWA e no Secure Email Gateway.
4. O uso de uma nuvem privada e uma análise de arquivo de nuvem não é um projeto suportado. Se você estiver usando um dispositivo local, a análise e a reputação do arquivo devem ser um servidor local.
5. Certifique-se de que não haja nenhum problema de sincronização de tempo entre a nuvem privada da AMP e o SWA, e-mail seguro.
6. O padrão do limite de verificação de objetos do mecanismo SWA DVS é 32 MB. Ajuste essa configuração se quiser fazer a varredura de arquivos maiores. Observe que essa é uma configuração global e afeta todos os mecanismos de verificação, como Webroot, Sophos e assim por diante.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.