# 將安全終端私有雲與安全Web和電子郵件整合

## 目錄

## 簡介

本文檔介紹將安全終端私有雲與安全Web裝置(SWA)和安全郵件網關(ESA)整合所需的步驟。

## 必要條件

思科建議您瞭解以下主題：

- 安全終端AMP虛擬私有雲
- 安全網路裝置(SWA)
- 安全電子郵件閘道

### 採用元件

SWA（安全網路裝置） 15.0.0-322

AMP虛擬私有雲4.1.0_202311092226

安全電子郵件網關14.2.0-620

注意：此文檔對所有相關產品的物理和虛擬變體均有效。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 進行整合前先進行驗證檢查

1. 驗證是否Secure Endpoint Private Cloud/SWA/Secure Email Gateway具有所需的許可證。您可以SWA/Secure Email在驗證功能金鑰或檢查智慧許可證是否已啟用。
2. 如果您計畫檢查HTTPS流量，則必須在SWA上啟用HTTPS代理。您需要解密HTTPS流量才能執行任何檔案信譽檢查。
3. 必須配置AMP私有雲/虛擬私有雲裝置和所有必需的證書。請參閱VPC證書指南進行驗證。

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

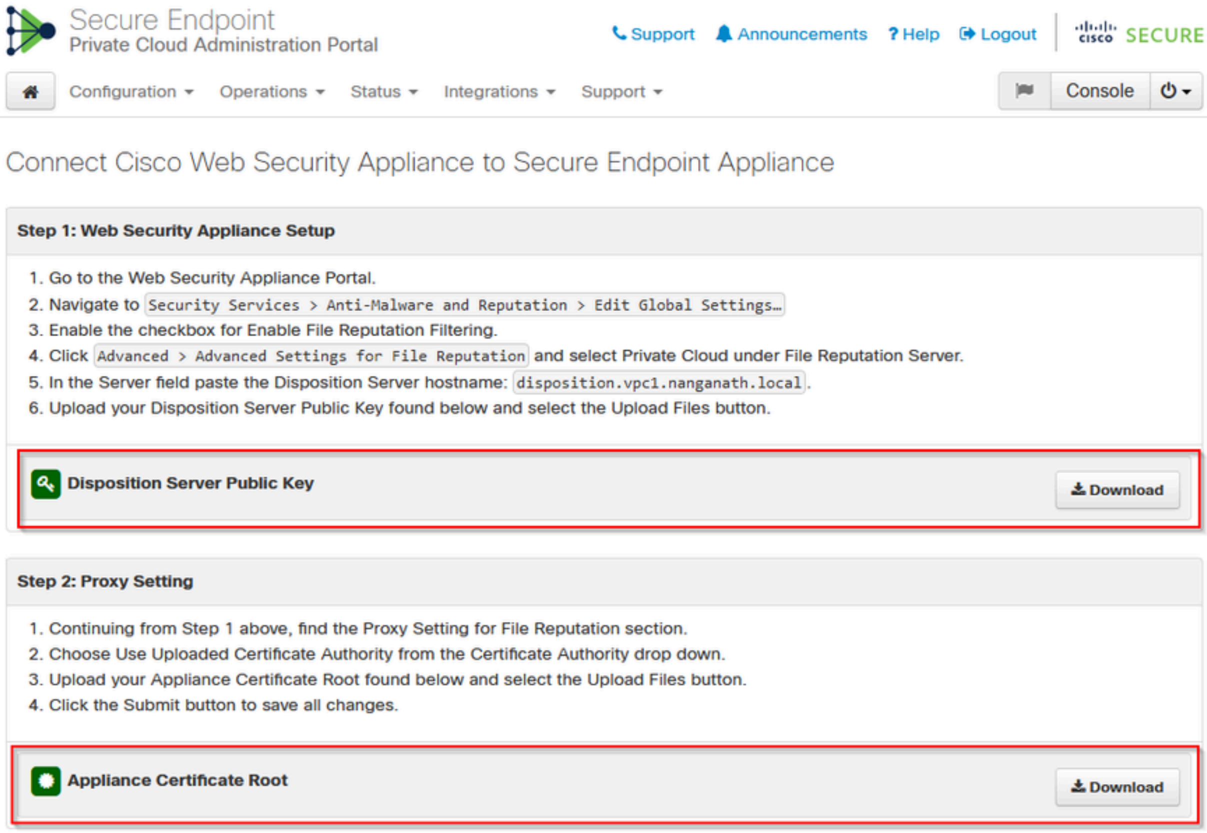
4. 產品的所有主機名必須是DNS可解析的。這是為了避免在整合期間出現任何連線問題或證書問題

。在安全終端私有雲上，Eth0介面用於管理員訪問，Eth1必須能夠與整合裝置連線。

# 程式

## 配置安全終端私有雲

1. 登入到**Secure Endpoint VPC admin portal**。
2. 轉至**“Configuration” > “Services” > “Disposition Server”**>複製處置伺服器主機名（這也可以從第三步獲取）。
3. 導航到**“Integrations” > “Web Security Appliance”**。
4. 下載**“Disposition Server Public Key” & “Appliance Certificate Root”**。
5. 導航到**“Integrations” > “Email Security Appliance”**。
6. 選擇ESA的版本並下載「Disposition Server Public Key」和「Appliance Certificate Root」。
7. 請保證證書和金鑰均安全。這必須稍後上傳到SWA/Secure Email。



Connect Cisco Web Security Appliance to Secure Endpoint Appliance

**Step 1: Web Security Appliance Setup**

1. Go to the Web Security Appliance Portal.
2. Navigate to `Security Services > Anti-Malware and Reputation > Edit Global Settings…`
3. Enable the checkbox for Enable File Reputation Filtering.
4. Click `Advanced > Advanced Settings for File Reputation` and select Private Cloud under File Reputation Server.
5. In the Server field paste the Disposition Server hostname: `disposition.vpc1.nanganath.local`.
6. Upload your Disposition Server Public Key found below and select the Upload Files button.

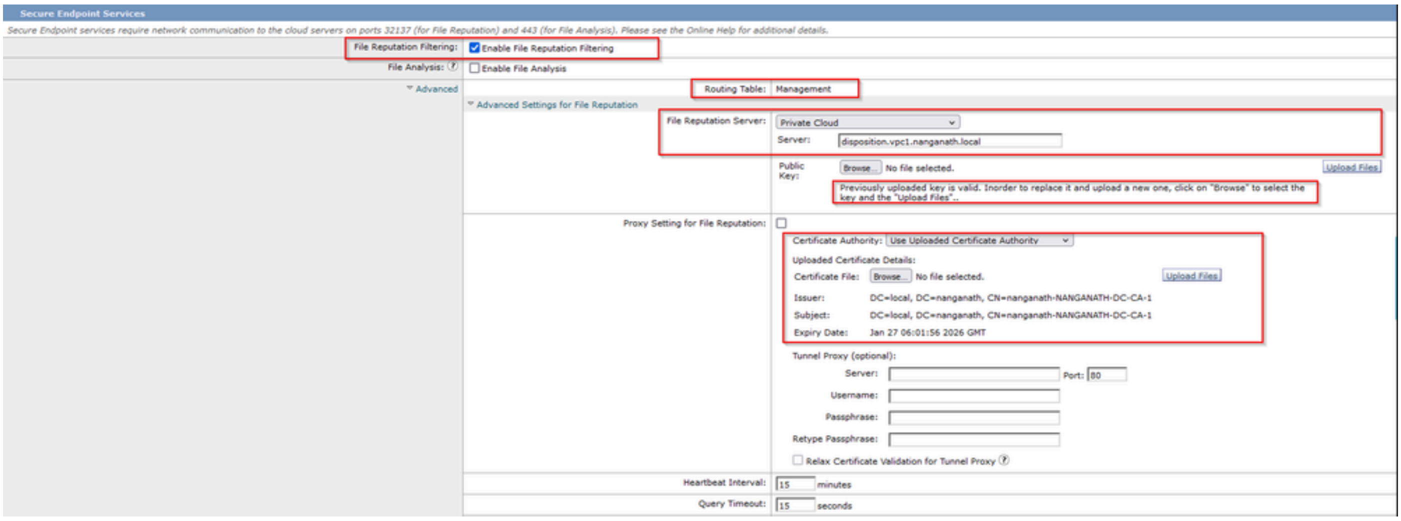
**Step 2: Proxy Setting**

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.

## 配置安全網路裝置

1. 導覽至 **SWA GUI > “Security Services” > “Anti-Malware and Reputation” > Edit Global Settings**
2. 在「Secure Endpoint Services」部分，您可以看到「Enable File Reputation Filtering」選項，並且「Check」此選項顯示一個新欄位「Advanced」
3. 在檔案信譽伺服器中選擇「私有雲」。
4. 提供私有雲處置伺服器主機名作為「伺服器」。
5. 上傳您之前下載的公鑰。按一下「上傳檔案」。

6. 可以選擇上傳證書頒發機構。從下拉選單中選擇「Use Uploaded Certificate Authority」（使用上傳的證書頒發機構）並上傳您之前下載的CA證書。
7. 提交變更
8. 提交更改



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

Advanced

Routing Table: Management

Advanced Settings for File Reputation

File Reputation Server: Private Cloud
Server: disposition.vpc1.nanganath.local

Public Key: Browse... No file selected. Upload Files
Previously uploaded key is valid. Inorder 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: Browse... No file selected. Upload Files
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

## 配置Cisco Secure Email

1. 瀏覽至 **Secure Email GUI > Security Services" > "File Reputation and Analysis" > Edit Global Settings > "Enable" or "Edit Global Settings"**

2. 在檔案信譽伺服器中選擇「私有雲」

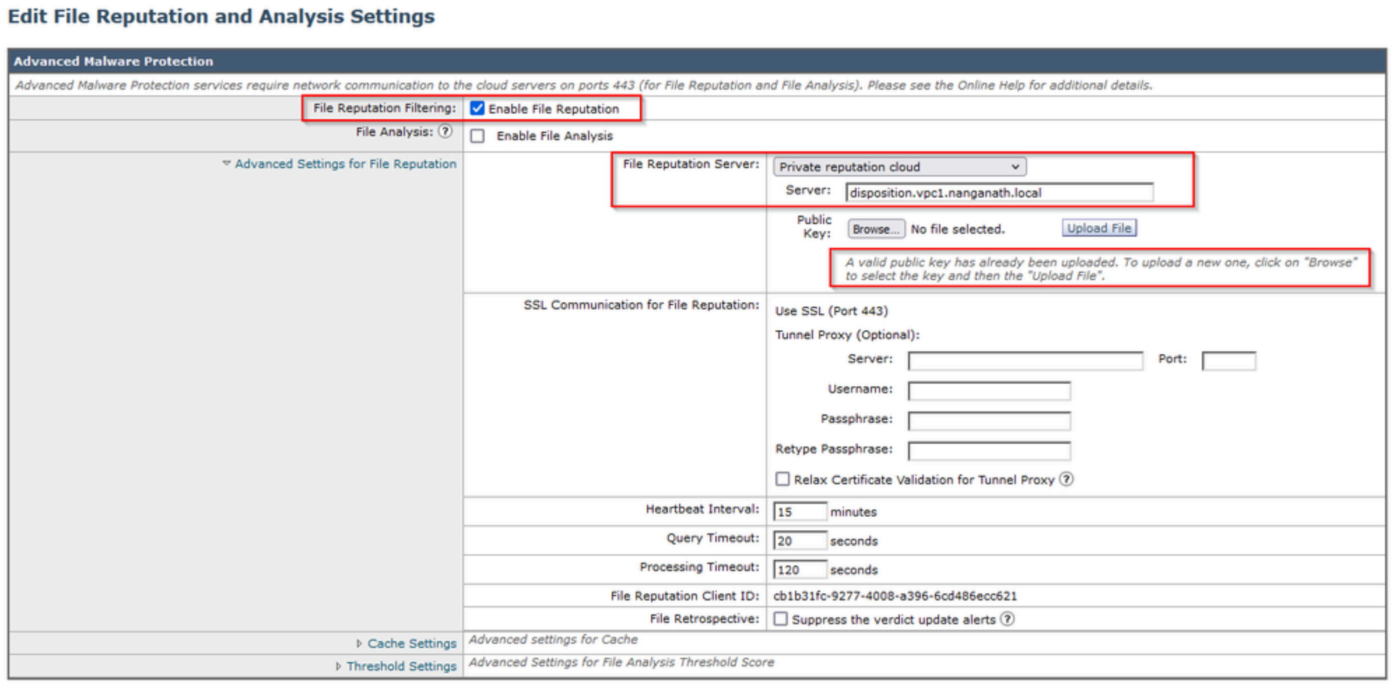
3. 將私有雲處置伺服器主機名提供為「伺服器」。

4. 上傳我們之前下載的公鑰。按一下「上傳檔案」。

5. 上傳證書頒發機構。從下拉選單中選擇「Use Uploaded Certificate Authority」（使用上傳的證書頒發機構）並上傳您之前下載的CA證書。

6. 提交變更

7. 提交更改



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: | ☑ Enable File Reputation |
| File Analysis: ? | □ Enable File Analysis |
| ▿ Advanced Settings for File Reputation | File Reputation Server: Private reputation cloud<br>Server: disposition.vpc1.nanganath.local<br>Public Key: Browse... No file selected. Upload File<br>*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".*<br>SSL Communication for File Reputation: Use SSL (Port 443)<br>Tunnel Proxy (Optional):<br>Server: Port:<br>Username:<br>Passphrase:<br>Retype Passphrase:<br>□ Relax Certificate Validation for Tunnel Proxy ?<br>Heartbeat Interval: 15 minutes<br>Query Timeout: 20 seconds<br>Processing Timeout: 120 seconds<br>File Reputation Client ID: cb1b31fc-9277-4008-a396-6cd486ecc621<br>File Retrospective: □ Suppress the verdict update alerts ? |
| ▹ Cache Settings | *Advanced settings for Cache* |
| ▹ Threshold Settings | *Advanced Settings for File Analysis Threshold Score* |

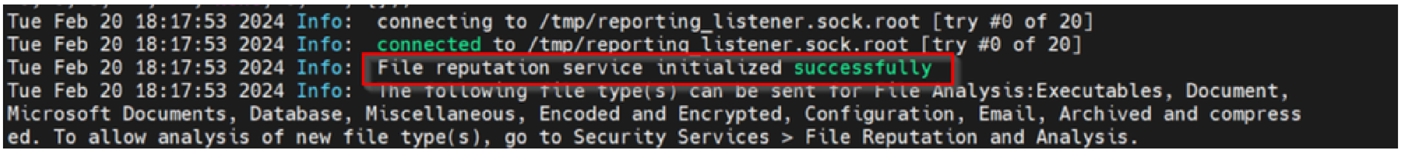
注意：Cisco Secure Web Appliance和Cisco Secure Email Gateway基於AsyncOS，初始化檔案信譽時共用幾乎相同的日誌。AMP日誌可在安全Web裝置或安全郵件網關AMP日誌（兩台裝置中的類似日誌）中檢視。這僅表示服務已在SWA和安全郵件網關上初始化。它並不表示連線完全成功。如果存在任何連線或證書問題，則在「File Reputation initialized」（檔案信譽已初始化）消息後會顯示錯誤。它主要表示「無法連線錯誤」或「憑證無效」錯誤。

## 從安全Web和電子郵件獲取AMP日誌的步驟

1. 登入到SWA/Secure Email Gateway CLI並鍵入命令 **"grep"**

2. 選取 **"amp" or "amp_logs"**

3. 保留所有其他欄位，並輸入「Y」以追蹤記錄檔。跟蹤日誌以顯示即時事件。如果您正在尋找舊事件，則可以在「正規表示式」中鍵入日期



```
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.
```

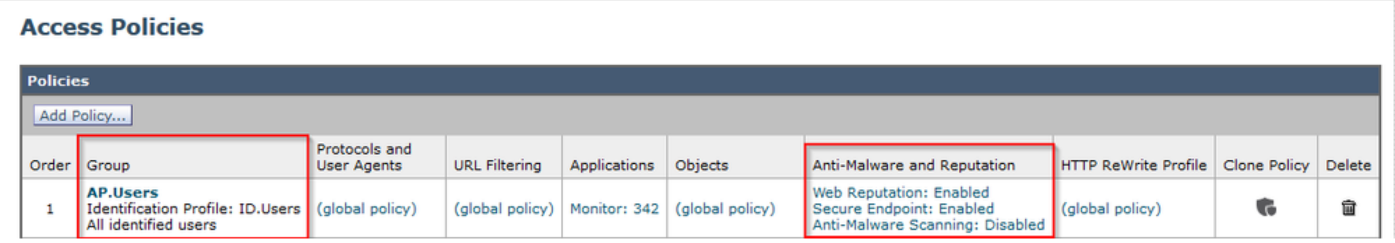
## 測試安全Web裝置和安全終端私有雲之間的整合。

沒有直接選項可用於測試SWA的連線。您必須檢查日誌或警報，以驗證是否存在任何問題。

為簡單起見，我們測試的是HTTP URL而不是HTTPS。請注意，您需要解密HTTPS流量以進行任何檔案信譽檢查。

配置在SWA訪問策略中完成，並強制執行AMP掃描。

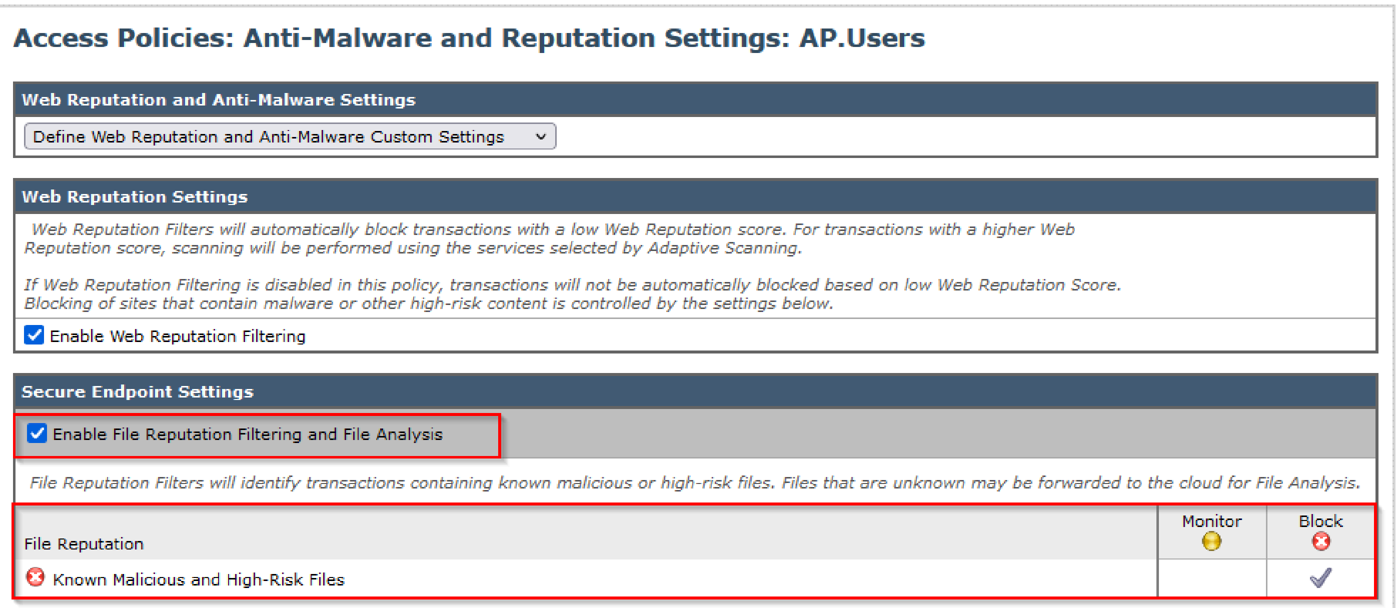
注意：請檢視SWA使用手冊，瞭解如何在Cisco Secure Web裝置上配置策略。



Access Policies

Policies

| Order | Group | Protocols and User Agents | URL Filtering | Applications | Objects | Anti-Malware and Reputation | HTTP ReWrite Profile | Clone Policy | Delete |
|---|---|---|---|---|---|---|---|---|---|
| 1 | AP.Users<br>Identification Profile: ID.Users<br>All identified users | (global policy) | (global policy) | Monitor: 342 | (global policy) | Web Reputation: Enabled<br>Secure Endpoint: Enabled<br>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 ☒ |
|---|---|---|
| ☒ Known Malicious and High-Risk Files |  | ✓ |

試圖透過思科安全網路裝置從網際網路下載惡意檔案「Bombermania.exe.zip」。日誌顯示惡意檔案已阻止。

SWA訪問日誌

這些步驟可擷取存取記錄。

1. 登入SWA並鍵入命令 "grep"

2. 選取 "accesslogs"

3. 如果您想增加任何「正規表示式」（如客戶端IP），請加以說明。

4. 鍵入「Y」以跟蹤日誌

```
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 , "- , - , - , - , -
 , - , 1 , "- , - , - , "- , - , - , - , - , - , - , - , "- , "- , - , - , "- , - , - , - , - , - - 「-」、-、-、 「
IW_comp」、-、「AMP高風險」、「電腦和網際網路」、「-」、「未知」、「未知」、「未知」
、「-」、333.79、0、-、「-」、「-」、「-」、37、「
Win.Ransomware.Protected：：Trojan.Agent.talos」、0、0、「Bombermania.exe.zip」、「
46ee42fb79a16 3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8" , 3 , - , "-" , - , -> -
```

TCP_DENIED/403 —> SWA拒絕此HTTP GET請求。

BLOCK_AMP_RESP —> HTTP GET請求由於AMP響應而被阻止。

Win.Ransomware.Protected：：Trojan.Agent.talos —>威脅名稱

Bombermania.exe.zip —>我們嘗試下載的檔名

46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8 —>檔案的SHA值

SWA AMP日誌

使用這些步驟可獲取AMP日誌。

1. 登入SWA並鍵入命令 **"grep"**

2. 選取 **"amp_logs"**

3. 保留所有其他欄位，並輸入「Y」以追蹤記錄檔。跟蹤日誌以顯示即時事件。如果您正在尋找舊事件，則可以在「正規表示式」中鍵入日期

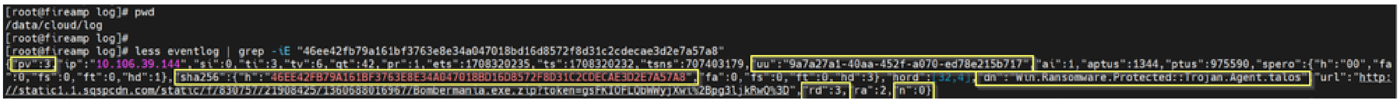
「verdict_from」：「雲」對於私有雲和公共雲而言，這似乎是一樣的。不要將其混淆為公共雲的裁決。

2024年2月19日星期一10:53:56除錯：調整後的裁決- {'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， 'Exit_file_verdict_verdict'、'verdict_from'： 'Cloud'， 'analysis_action'： 2， 'file_type'： 'application/zip'， 'score'： 0， 'upload_reason'： 'File type is not configured for sandboxing'， 'sha256'： '46ee42fb79a1 61bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8'， 'verdict_str'： 'MALICIOUS'， 'malicious_child'： None}

安全端點私有雲事件日誌

事件日誌位於 **/data/cloud/log**

您可以使用SHA256或使用SWA的「檔案信譽客戶端ID」搜尋事件。SWA的AMP配置頁面中顯示「檔案信譽客戶端ID」。



```
[root@fireamp log]# pwd
/data/cloud/log
[root@fireamp log]#
[root@fireamp log]# less eventlog | grep -iE "46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8"
{"pv":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","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},"hord":[32,4],"dn":"Win.Ransomware.Protected::Trojan.Agent.talos","url":"http:
//static1.1.sqspcdn.com/static/f/830757/21908425/1360688016967/Bombermania.exe.zip?token=gsFK1OFLQbWWyjXwl%2Bpg3ljkRwQ%3D","rd":3,"ra":2,"n":0}
```

pv -協定版本，3表示TCP

ip -請忽略此欄位，因為無法保證此欄位指示執行信譽查詢的客戶端的實際IP地址

uu - WSA/ESA中的檔案信譽客戶端ID

檔案的SHA256 - SHA256

dn -檢測名稱

n - 1（如果AMP以前從未見過檔案雜湊），否則為0。

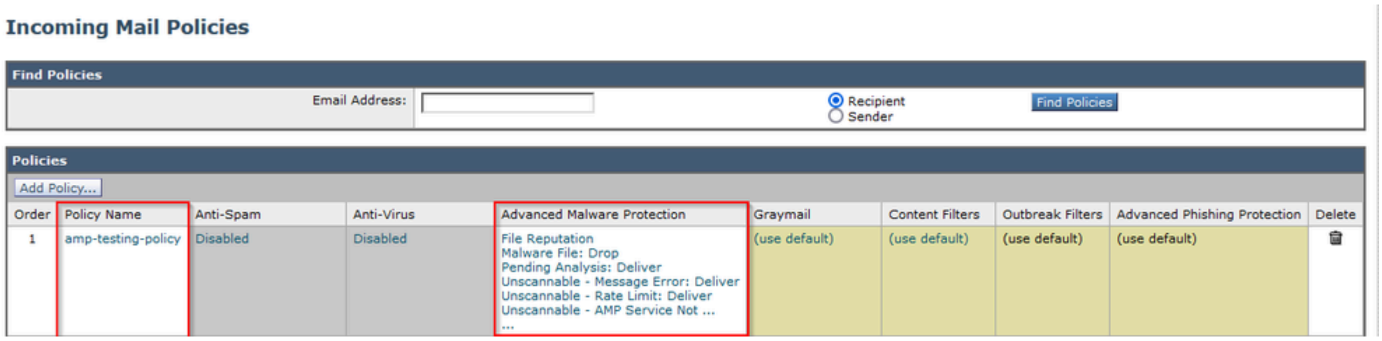
rd -回應處置。此處3表示DISP_MALICIOUS

1 DISP_UNKNOWN檔案性質未知。
2 DISP_CLEAN此檔案被認為是良性的。
3 DISP_MALICIOUS認為該檔案是惡意的。
7 DISP_UNSEEN檔案性質未知，這是我們第一次看到該檔案。
13 DISP_BLOCK不能執行檔案。
14 DISP_IGNORE XXX
15 DISP_CLEAN_PARENT認為該檔案是良性的，它建立的任何惡意檔案都必須視為未知。
16 DISP_CLEAN_NFM認為該檔案是良性的，但客戶端必須監控其網路流量。

## 測試安全電郵與AMP私有雲之間的整合

從安全郵件網關測試連線沒有直接選項。您必須檢查日誌或警報，以驗證是否存在任何問題。

在Secure Email incoming mail策略中完成配置以實施AMP掃描。



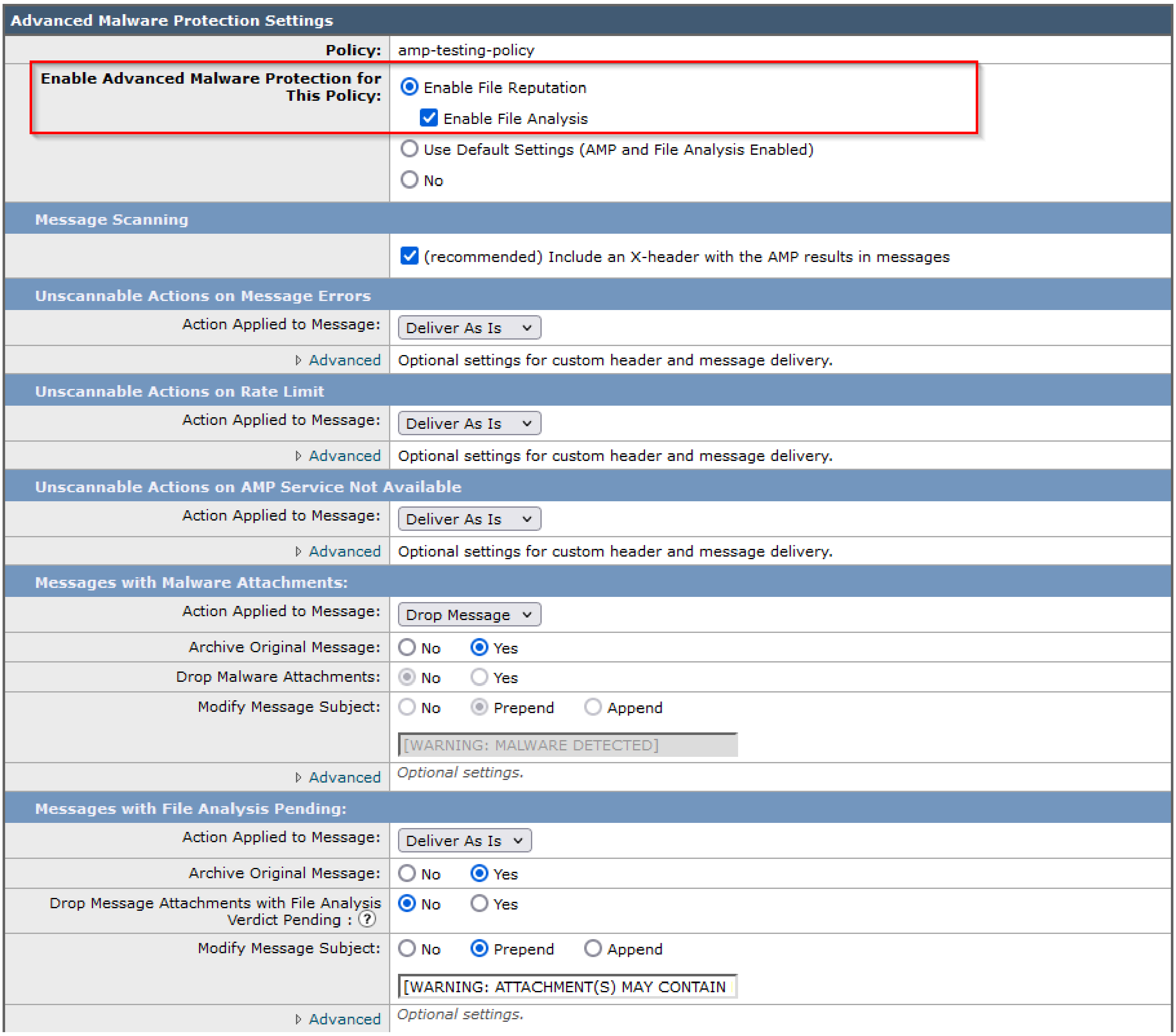
Incoming Mail Policies

Find Policies

Email Address: ● Recipient ○ Sender

Policies

| 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<br>Malware File: Drop<br>Pending Analysis: Deliver<br>Unscannable - Message Error: Deliver<br>Unscannable - Rate Limit: Deliver<br>Unscannable - AMP Service Not ...<br>... | (use default) | (use default) | (use default) | (use default) | 🗑 |

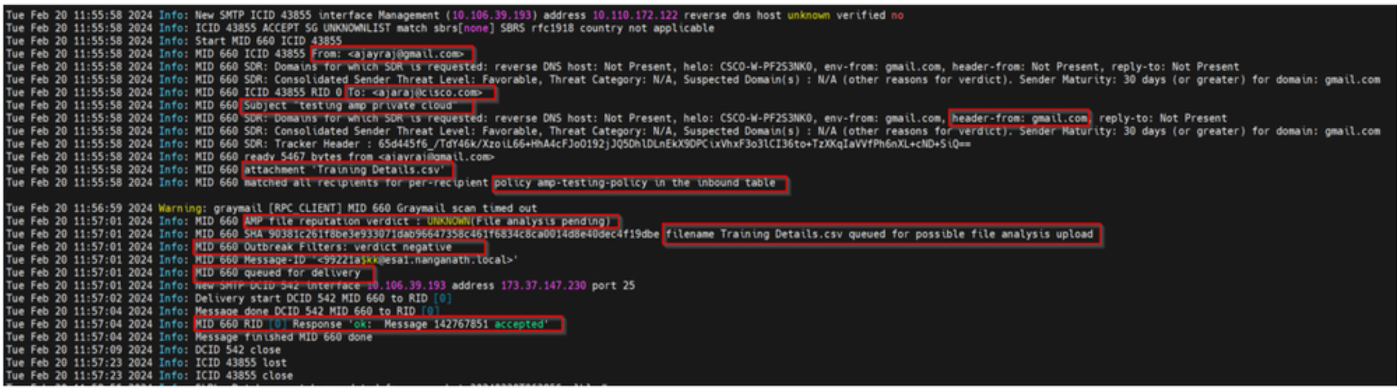


## Mail Policies: Advanced Malware Protection

| | |
|---|---|
| **Advanced Malware Protection Settings** | |
| **Policy:** | amp-testing-policy |
| **Enable Advanced Malware Protection for This Policy:** | ● Enable File Reputation<br>☑ Enable File Analysis<br>○ Use Default Settings (AMP and File Analysis Enabled)<br>○ No |
| **Message Scanning** | |
| | ☑ (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: | ○ No ● Yes |
| Drop Malware Attachments: | ● No ○ Yes |
| Modify Message Subject: | ○ No ● Prepend ○ Append<br>[WARNING: MALWARE DETECTED] |
| ▷ Advanced | *Optional settings.* |
| **Messages with File Analysis Pending:** | |
| Action Applied to Message: | Deliver As Is |
| Archive Original Message: | ○ No ● Yes |
| Drop Message Attachments with File Analysis Verdict Pending : ? | ● No ○ Yes |
| Modify Message Subject: | ○ No ● Prepend ○ Append<br>[WARNING: ATTACHMENT(S) MAY CONTAIN |
| ▷ Advanced | *Optional settings.* |

已使用非惡意檔案對ESA進行了測試。這是CSV檔案。

Secure Email 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: CSCO-W-PF2S3NK0, 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: <ajaraj@cisco.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: CSCO-W-PF2S3NK0, 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+HhA4cFJoO192jJQ5DhlDLnEkX9DPCixVhxF3o3lCI36to+TzXKqIaVVfPh6nXL+cND+SiQ==
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 '<99221a$kk@esa1.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 DCID 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
```

安全電子郵件AMP日誌

```
2024年2月20日星期二11:57:01 2024資訊：從Cloud收到檔案信譽查詢的響應。檔名= Training
Details.csv，MID = 660，性質= FILE UNKNOWN，惡意軟體=無，分析得分= 0，sha256 =
90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19dbe，upload_action =建
議傳送檔案進行分析， verdict_source = AMP，可疑類別= None
```

安全端點私有雲事件日誌

```
{"pv"：3，"ip"："10.106.72.238"，"si"：0，"ti"：14，"tv"：6，"qt"：42，"pr"：1，"ets"：1708410419，"t
9277-4008-a396-6cd486ecc621"，"ai"：1，"aptus"
295，"ptus"：2429102，"spero"：{"h"："00"，"fa"：0，"fs"：0，"ft"：0，"hd"：1}，"sha256"：{"h"："90
"，" fa"：0，"fs"：0，"ft"：0，"hd"：1}，"hord"：[32,4]，"rd"：1，"ra"：1，"n"：0}
```

rd - 1個DISP_UNKNOWN。檔案性質未知。

## 發現導致整合失敗的常見問題

1. 在SWA或安全郵件中選擇錯誤的「路由表」。整合裝置必須能夠與AMP私有雲Eth1介面通訊。
2. VPC主機名在SWA或安全郵件中不可進行DNS解析，從而導致建立連線失敗。
3. VPC處置證書中的CN（通用名稱）必須與VPC主機名以及SWA和安全郵件網關中提到的主機名匹配。
4. 不支援使用私有雲和雲檔案分析。如果使用本地裝置，則檔案分析和信譽必須是本地伺服器。
5. 確保AMP私有雲與SWA、安全電子郵件之間不存在時間同步問題。
6. SWA DVS引擎對象掃描限制預設為32 MB。如果要掃描較大的檔案，請調整此設定。請注意，這是一個全局設定，會影響所有掃描引擎，如Webroot、Sophos等。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。