將SWA與SMA整合

目錄

簡介

本檔案介紹將安全網路裝置(SWA)整合到安全管理裝置(SMA)的過程。

必要條件

需求

思科建議瞭解以下主題：

- 訪問SWA的圖形使用者介面(GUI)。
- 對SWA的管理訪問。
- 對SMA的管理訪問。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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

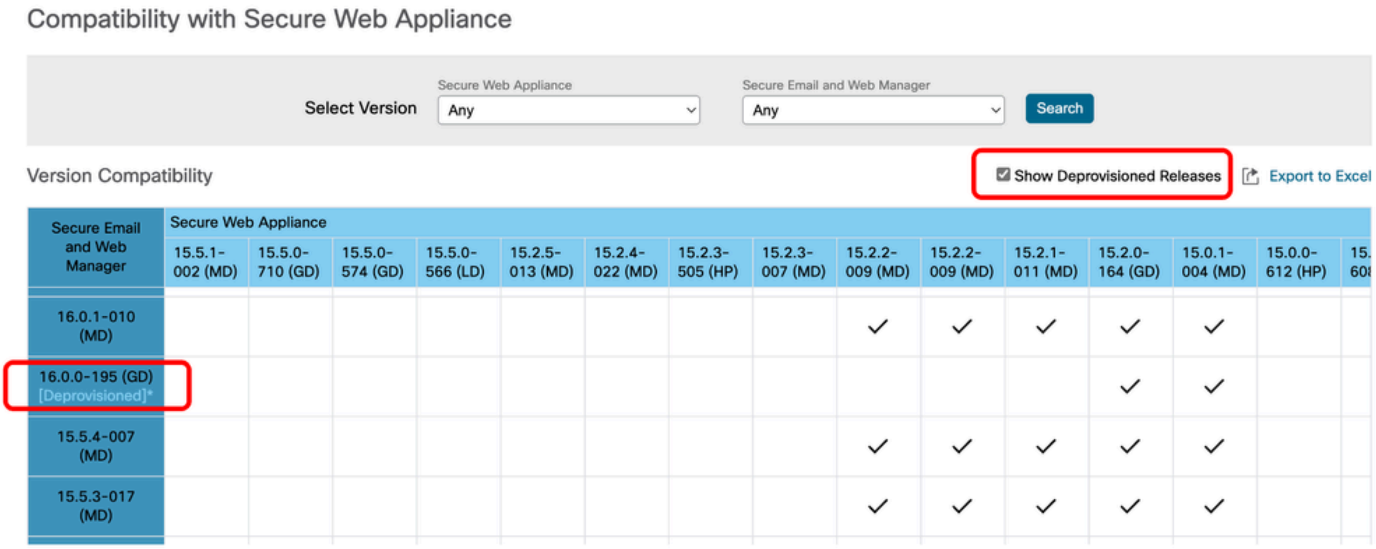
）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

開始之前

1.確保SMA和SWA都獲得許可。

2.檢查SWA和SMA的相容性矩陣，使用以下連結：SWA-SMA-ESA相容性矩陣。

附註：確保沒有取消設定您計畫整合的版本。



Compatibility with Secure Web Appliance

Select Version — Secure Web Appliance: Any — Secure Email and Web Manager: Any — Search

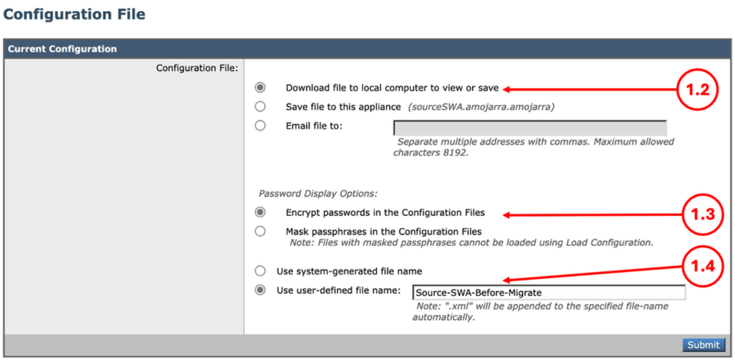
Version Compatibility — ☑ Show Deprovisioned Releases — Export to Excel

Secure Email and Web Manager	Secure Web Appliance														
	15.5.1-002 (MD)	15.5.0-710 (GD)	15.5.0-574 (GD)	15.5.0-566 (LD)	15.2.5-013 (MD)	15.2.4-022 (MD)	15.2.3-505 (HP)	15.2.3-007 (MD)	15.2.2-009 (MD)	15.2.2-009 (MD)	15.2.1-011 (MD)	15.2.0-164 (GD)	15.0.1-004 (MD)	15.0.0-612 (HP)	15. 60
16.0.1-010 (MD)									✓	✓	✓	✓	✓		
16.0.0-195 (GD) [Deprovisioned]*												✓	✓		
15.5.4-007 (MD)									✓	✓	✓	✓	✓		
15.5.3-017 (MD)									✓	✓	✓	✓	✓		

映像 — 已解除布建的版本

將SWA整合到SMA的步驟

步驟1.從SWA匯出配置檔案	步驟1.1.從GUI導航到System Administration並選擇Configuration File。 步驟1.2.確保選中「Download file to local computer to view or save（將檔案下載到本地電腦檢視或儲存）」。 步驟1.3.在Configuration Files中選擇Encrypt密碼。 步驟1.4.（可選）選擇配置檔案的名稱。 步驟1.5.按一下Submit。



Configuration File

Current Configuration

Configuration File:

● Download file to local computer to view or save

○ Save file to this appliance (sourceSWA.amojarra.amojarra)

○ Email file to:

Separate multiple addresses with commas. Maximum allowed characters 8192.

Password Display Options:

● Encrypt passwords in the Configuration Files

○ Mask passphrases in the Configuration Files

Note: Files with masked passphrases cannot be loaded using Load Configuration.

○ Use system-generated file name

● Use user-defined file name: Source-SWA-Before-Migrate

Note: ".xml" will be appended to the specified file-name automatically.

映像 — 匯出配置檔案

步驟2.建立配置管理器

附註：如果SMA中已配置了Configuration Manager，請跳至步驟4。

步驟2.1.在SMA GUI中按一下Web選項卡。

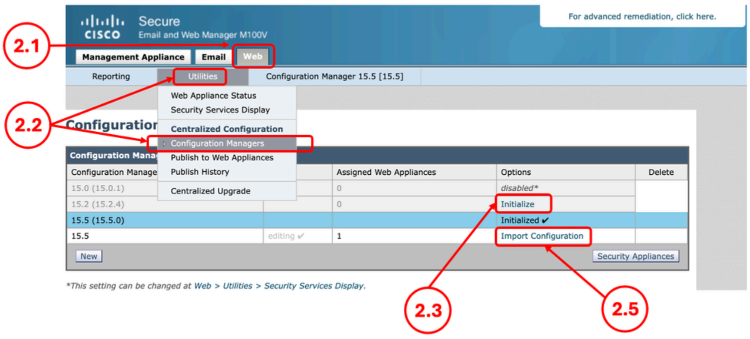
步驟2.2.從Utilities中選擇Configuration Manager。

步驟2.3.如果配置管理器尚未初始化，請按一下所需Configuration Manager的Initialize連結，否則跳至步驟2.5。

提示：Configuration Manager版本必須與SWA版本的前兩個分段保持一致。例如，如果您的SWA版本是15.5.0-710，則必須使用Configuration Manager 15.5。

步驟2.4.選擇使用預設設定，然後單擊Initialize。

步驟2.5.單擊Import Configuration以匯入所需的Configuration Manager。



Secure
CISCO Email and Web Manager M100V
For advanced remediation, click here.
Management Appliance
Email
Web
Reporting
Utilities
Configuration Manager 15.5 [15.5]
Web Appliance Status
Security Services Display
Centralized Configuration
Configuration Managers
Publish to Web Appliances
Publish History
Centralized Upgrade
Configuration
New
Security Appliances
2.1
2.2
2.3
2.5

Configuration Mana

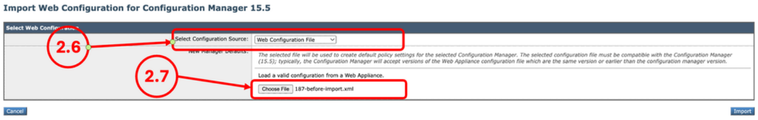
Configuration Manage		Assigned Web Appliances	Options	Delete
15.0 (15.0.1)		0	disabled*	
15.2 (15.2.4)		0	Initialize	
15.5 (15.5.0)			Initialized ✓	
15.5	editing ✓	1	Import Configuration	

*This setting can be changed at Web > Utilities > Security Services Display.

映像 — Configuration Manager

步驟2.6.從Select Configuration Source中選擇Web Configuration File。

步驟2.7.選擇在步驟1中匯出的配置檔案。

<table>
<tr>
<td></td>
<td>


Import Web Configuration for Configuration Manager 15.5

Select Web Confi...

Select Configuration Source: Web Configuration File

New Manager Defaults: The selected file will be used to create default policy settings for the selected Configuration Manager. The selected configuration file must be compatible with the Configuration Manager (15.5); typically, the Configuration Manager will accept versions of the Web Appliance configuration file which are the same version or earlier than the configuration manager version.

Load a valid configuration from a Web Appliance.

Choose File 187-before-import.xml

映像 — 匯入配置

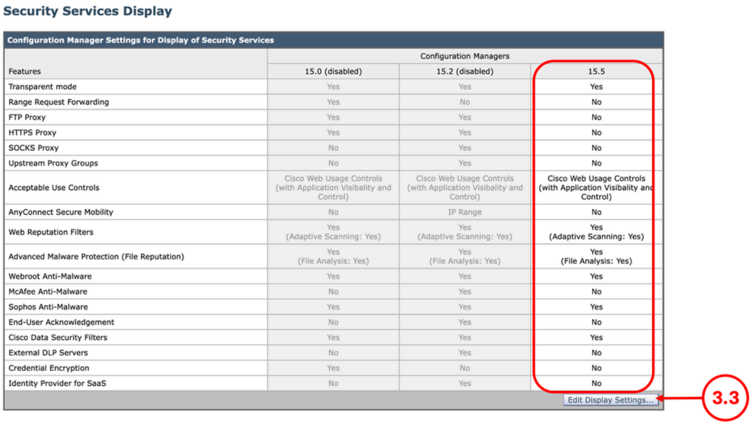
步驟2.8.單擊Import。

步驟2.9. 提交更改。
</td>
</tr>
<tr>
<td>步驟3. Configuration Manager設定</td>
<td>
步驟3.1.在SMA GUI中按一下Web選項卡。

步驟3.2.從Utilities中選擇Security Services Display。

步驟3.3.確保正確配置了所需的功能，您可以從Edit Display Settings啟用或禁用這些功能。

步驟3.4.如果有任何變更，請提交並提交。



Security Services Display

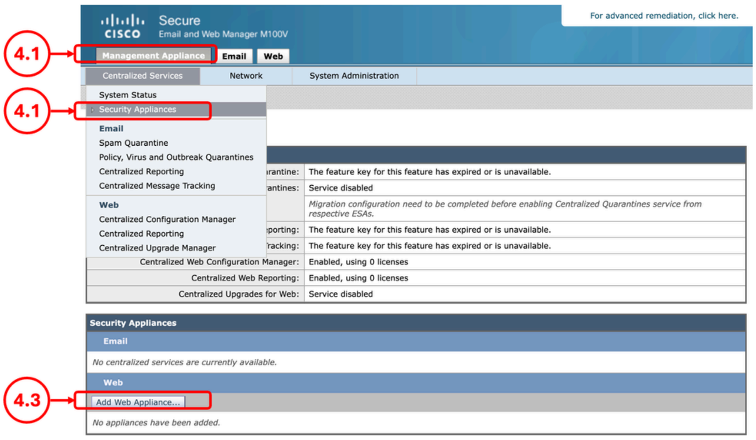
Configuration Manager Settings for Display of Security Services

<table>
<tr><th></th><th colspan="3">Configuration Managers</th></tr>
<tr><th>Features</th><th>15.0 (disabled)</th><th>15.2 (disabled)</th><th>15.5</th></tr>
<tr><td>Transparent mode</td><td>Yes</td><td>Yes</td><td>Yes</td></tr>
<tr><td>Range Request Forwarding</td><td>Yes</td><td>No</td><td>No</td></tr>
<tr><td>FTP Proxy</td><td>Yes</td><td>Yes</td><td>No</td></tr>
<tr><td>HTTPS Proxy</td><td>Yes</td><td>Yes</td><td>No</td></tr>
<tr><td>SOCKS Proxy</td><td>No</td><td>Yes</td><td>No</td></tr>
<tr><td>Upstream Proxy Groups</td><td>No</td><td>Yes</td><td>No</td></tr>
<tr><td>Acceptable Use Controls</td><td>Cisco Web Usage Controls (with Application Visibility and Control)</td><td>Cisco Web Usage Controls (with Application Visibility and Control)</td><td>Cisco Web Usage Controls (with Application Visibility and Control)</td></tr>
<tr><td>AnyConnect Secure Mobility</td><td>No</td><td>IP Range</td><td>No</td></tr>
<tr><td>Web Reputation Filters</td><td>Yes (Adaptive Scanning: Yes)</td><td>Yes (Adaptive Scanning: Yes)</td><td>Yes (Adaptive Scanning: Yes)</td></tr>
<tr><td>Advanced Malware Protection (File Reputation)</td><td>Yes (File Analysis: Yes)</td><td>Yes (File Analysis: Yes)</td><td>Yes (File Analysis: Yes)</td></tr>
<tr><td>Webroot Anti-Malware</td><td>Yes</td><td>Yes</td><td>Yes</td></tr>
<tr><td>McAfee Anti-Malware</td><td>No</td><td>Yes</td><td>No</td></tr>
<tr><td>Sophos Anti-Malware</td><td>Yes</td><td>Yes</td><td>Yes</td></tr>
<tr><td>End-User Acknowledgement</td><td>No</td><td>Yes</td><td>No</td></tr>
<tr><td>Cisco Data Security Filters</td><td>Yes</td><td>Yes</td><td>Yes</td></tr>
<tr><td>External DLP Servers</td><td>No</td><td>Yes</td><td>No</td></tr>
<tr><td>Credential Encryption</td><td>Yes</td><td>No</td><td>No</td></tr>
<tr><td>Identity Provider for SaaS</td><td>No</td><td>Yes</td><td>No</td></tr>
</table>

影象 — 安全服務顯示
</td>
</tr>
<tr>
<td>步驟4.新增Web裝置</td>
<td>
步驟4.1.從SMA GUI中按一下Management Appliance選項卡。

步驟4.2.從Centralized Services選擇Security Appliances。

步驟4.3.按一下「Add Web Appliance」
</td>
</tr>
</table>



rantine:	The feature key for this feature has expired or is unavailable.
antines:	Service disabled *Migration configuration need to be completed before enabling Centralized Quarantines service from respective ESAs.*
porting:	The feature key for this feature has expired or is unavailable.
racking:	The feature key for this feature has expired or is unavailable.
Centralized Web Configuration Manager:	Enabled, using 0 licenses
Centralized Web Reporting:	Enabled, using 0 licenses
Centralized Upgrades for Web:	Service disabled

Security Appliances

Email

No centralized services are currently available.

Web

No appliances have been added.

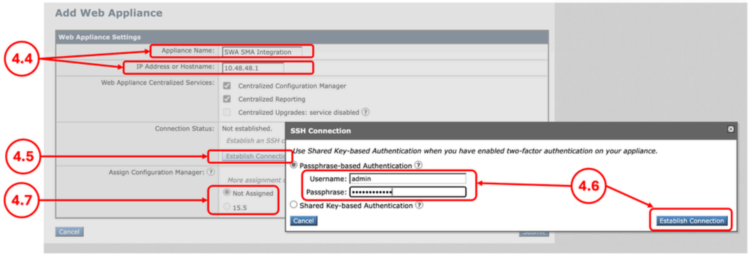
影象 — 新增Web裝置

步驟4.4.輸入裝置名稱和IP地址或主機名。

步驟4.5.單擊建立連線。

步驟4.6.輸入Username和Passphrase，然後點選Establish Connection。

步驟4.7.分配Configuration Manager。



Appliance Name: SWA SMA Integration

IP Address or Hostname: 10.48.48.1

Web Appliance Centralized Services: ☑ Centralized Configuration Manager ☑ Centralized Reporting □ Centralized Upgrades: service disabled

Connection Status: Not established.

Establish an SSH c

Assign Configuration Manager: ● Not Assigned ○ 15.5

More assignment

Use Shared Key-based Authentication when you have enabled two-factor authentication on your appliance.

● Passphrase-based Authentication

Username: admin

Passphrase: ••••••••••••

○ Shared Key-based Authentication

影象 — 新增SWA

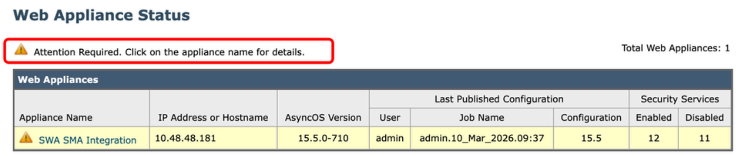
步驟4.8. Submit和Commit變更。

步驟5.驗證整合

步驟5.1.在SMA GUI中，按一下Web選項卡。

步驟5.2.從Utilities中選擇Web Appliance Status。

步驟5.3.如果您看到警告消息「Attention Required」。按一下裝置名稱瞭解詳細資訊，按一下SWA名稱並檢視詳細資訊。



Web Appliance Status

⚠ Attention Required. Click on the appliance name for details.

Total Web Appliances: 1

Web Appliances

			Last Published Configuration			Security Services	
Appliance Name	IP Address or Hostname	AsyncOS Version	User	Job Name	Configuration	Enabled	Disabled
⚠ SWA SMA Integration	10.48.48.181	15.5.0-710	admin	admin.10_Mar_2026.09:37	15.5	12	11

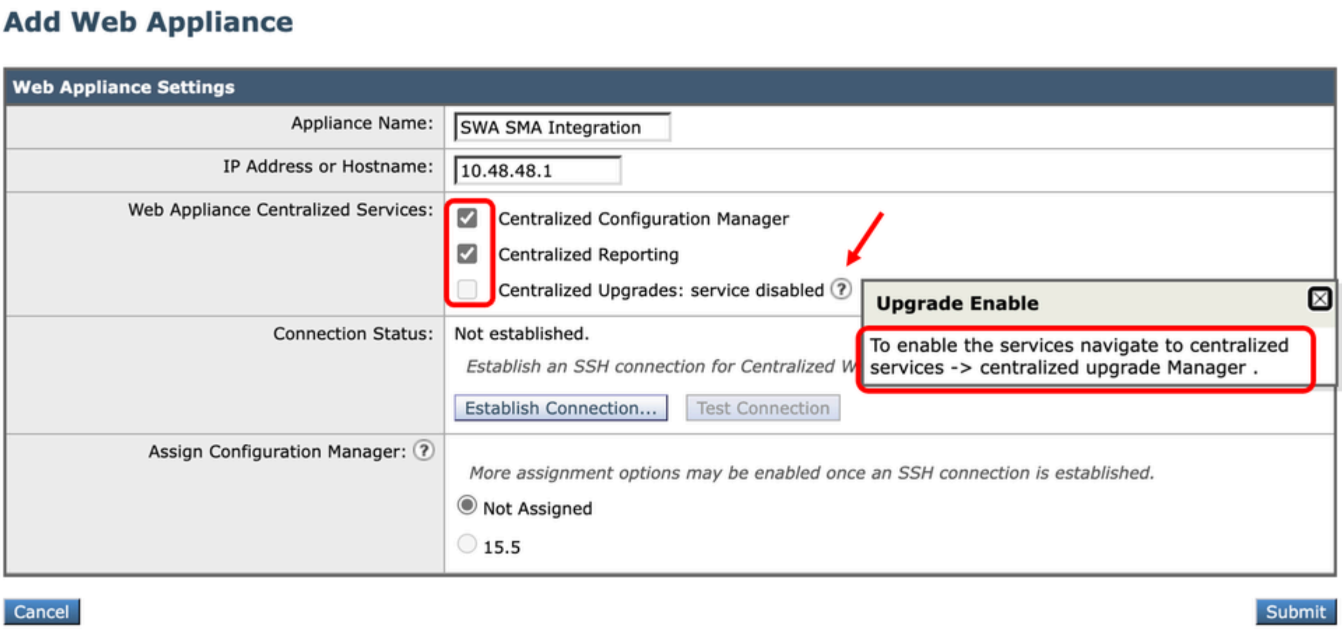
影象 — Web裝置狀態

提示：有關故障排除資訊，請參閱本文的修復錯誤部分。

修復錯誤

"集中服務已禁用"

當您嘗試選擇集中服務時，如果覈取方塊處於非活動狀態，則按一下問號(?)，嚮導將引導您通過路徑來啟用該服務。



Add Web Appliance

Web Appliance Settings

Appliance Name:	SWA SMA Integration
IP Address or Hostname:	10.48.48.1
Web Appliance Centralized Services:	☑ Centralized Configuration Manager ☑ Centralized Reporting □ Centralized Upgrades: service disabled ?
Connection Status:	Not established. *Establish an SSH connection for Centralized W* Establish Connection... Test Connection
Assign Configuration Manager: ?	*More assignment options may be enabled once an SSH connection is established.* ● Not Assigned ○ 15.5

Upgrade Enable ☒

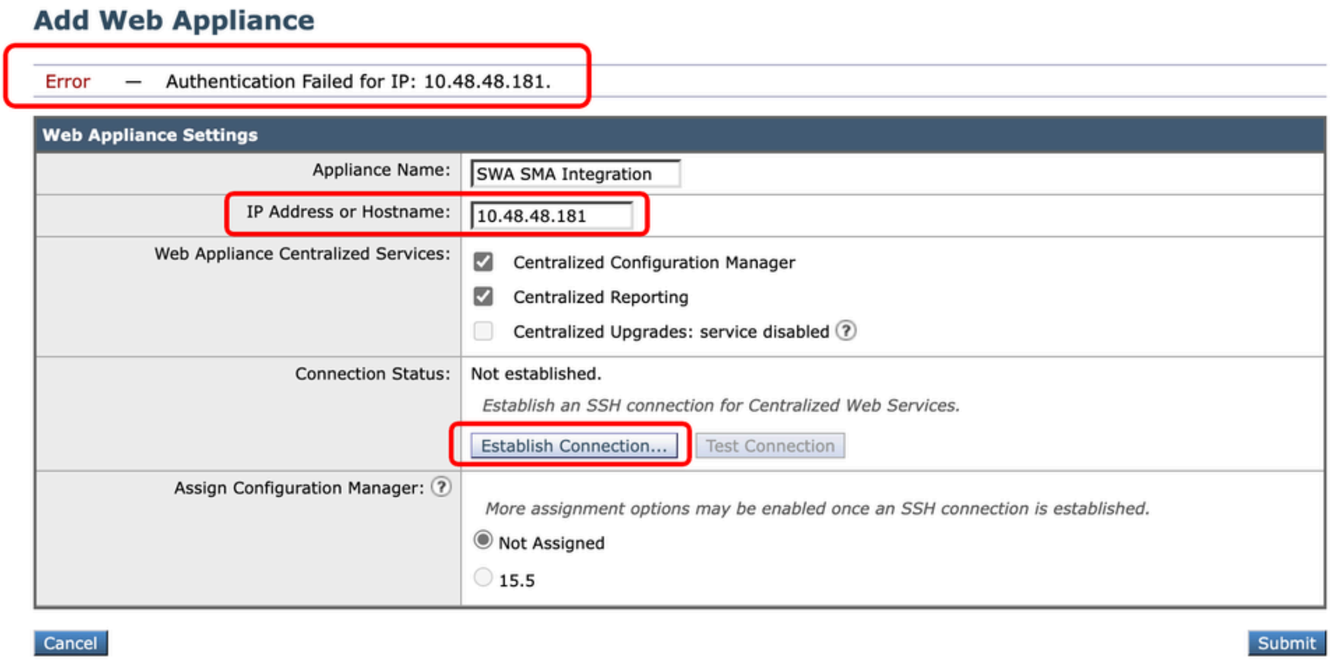
To enable the services navigate to centralized services -> centralized upgrade Manager .

Cancel Submit

影象 — 集中服務已禁用

"IP身份驗證失敗"

如果您收到此錯誤，將SWA整合到SMA時，請確保IP地址或主機名以及憑據正確。



Add Web Appliance

Error — Authentication Failed for IP: 10.48.48.181.

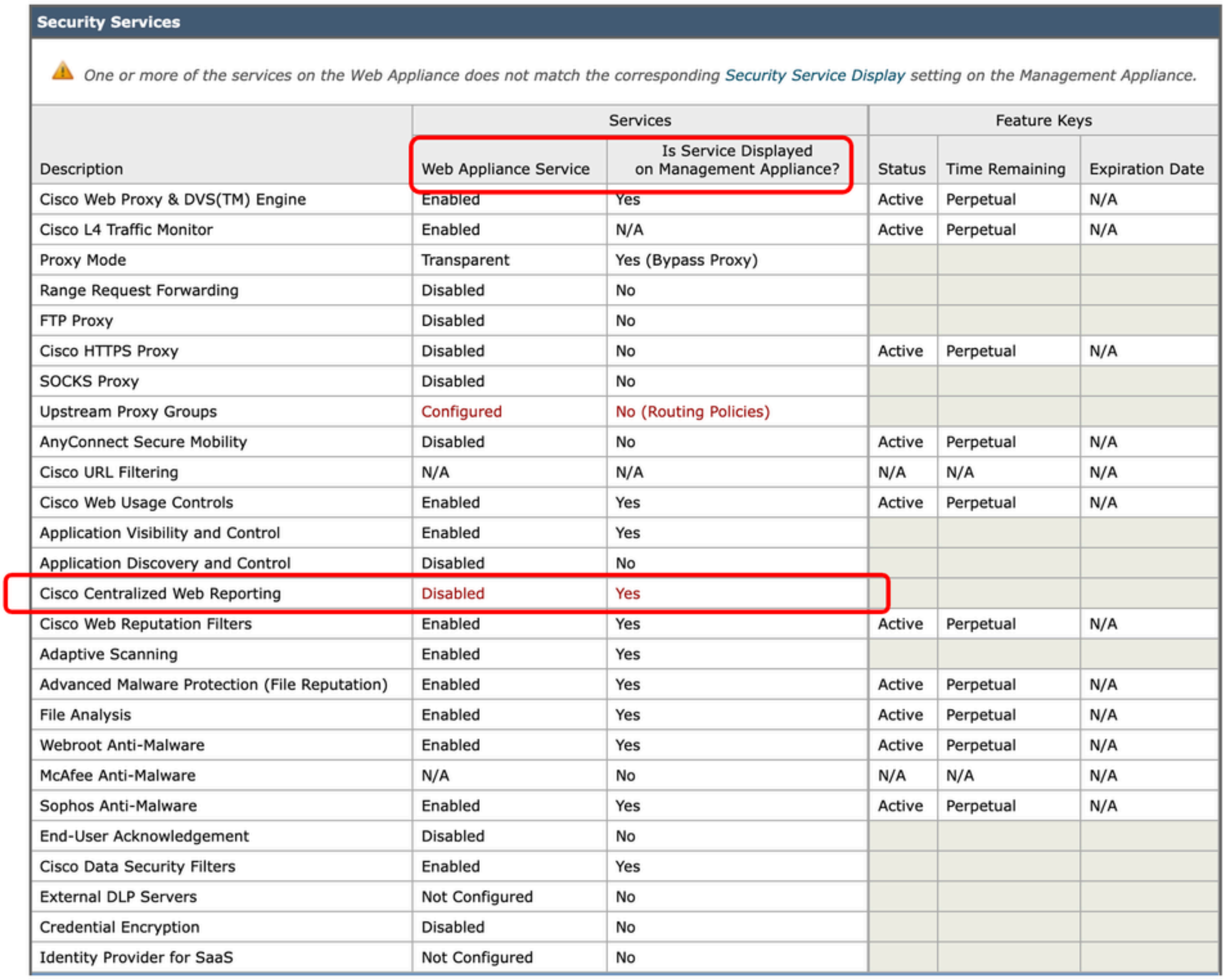
Web Appliance Settings

Appliance Name:	SWA SMA Integration
IP Address or Hostname:	10.48.48.181
Web Appliance Centralized Services:	☑ Centralized Configuration Manager ☑ Centralized Reporting □ Centralized Upgrades: service disabled
Connection Status:	Not established. *Establish an SSH connection for Centralized Web Services.* Establish Connection... Test Connection
Assign Configuration Manager:	*More assignment options may be enabled once an SSH connection is established.* ● Not Assigned ○ 15.5

影象 — 身份驗證失敗

「Cisco Centralized Web Reporting is disabled in the SWA（SWA中禁用思科集中網路報告）」

如果SMA配置了集中網路報告，並且您在「第4步」中將SWA整合到SMA時將該功能分配給SWA，則需要啟用Cisco Centralized Web Reporting:



Security Services

⚠ *One or more of the services on the Web Appliance does not match the corresponding Security Service Display setting on the Management Appliance.*

	Services		Feature Keys		
Description	Web Appliance Service	Is Service Displayed on Management Appliance?	Status	Time Remaining	Expiration Date
Cisco Web Proxy & DVS(TM) Engine	Enabled	Yes	Active	Perpetual	N/A
Cisco L4 Traffic Monitor	Enabled	N/A	Active	Perpetual	N/A
Proxy Mode	Transparent	Yes (Bypass Proxy)			
Range Request Forwarding	Disabled	No			
FTP Proxy	Disabled	No			
Cisco HTTPS Proxy	Disabled	No	Active	Perpetual	N/A
SOCKS Proxy	Disabled	No			
Upstream Proxy Groups	Configured	No (Routing Policies)			
AnyConnect Secure Mobility	Disabled	No	Active	Perpetual	N/A
Cisco URL Filtering	N/A	N/A	N/A	N/A	N/A
Cisco Web Usage Controls	Enabled	Yes	Active	Perpetual	N/A
Application Visibility and Control	Enabled	Yes			
Application Discovery and Control	Disabled	No			
Cisco Centralized Web Reporting	Disabled	Yes			
Cisco Web Reputation Filters	Enabled	Yes	Active	Perpetual	N/A
Adaptive Scanning	Enabled	Yes			
Advanced Malware Protection (File Reputation)	Enabled	Yes	Active	Perpetual	N/A
File Analysis	Enabled	Yes	Active	Perpetual	N/A
Webroot Anti-Malware	Enabled	Yes	Active	Perpetual	N/A
McAfee Anti-Malware	N/A	No	N/A	N/A	N/A
Sophos Anti-Malware	Enabled	Yes	Active	Perpetual	N/A
End-User Acknowledgement	Disabled	No			
Cisco Data Security Filters	Enabled	Yes			
External DLP Servers	Not Configured	No			
Credential Encryption	Disabled	No			
Identity Provider for SaaS	Not Configured	No			

影象 — 在SWA中禁用集中式Web報告

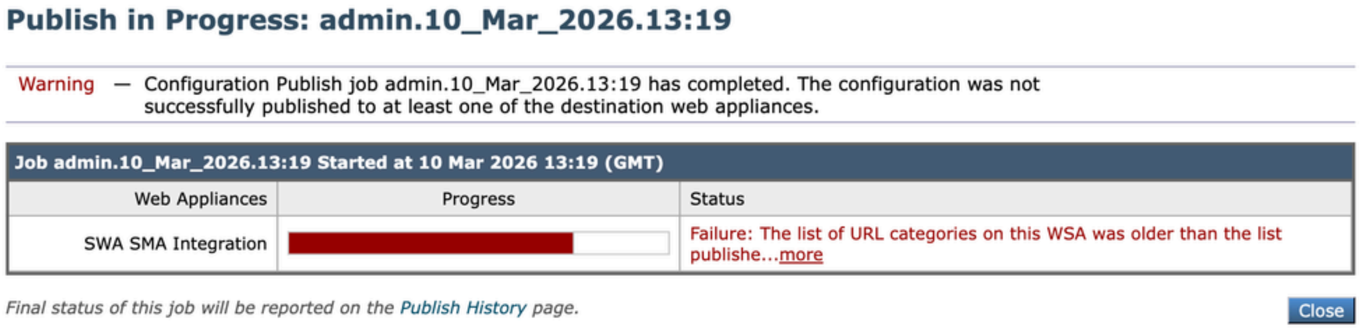
要解決此問題，請從CLI連線到SWA，然後鍵入reportingconfig並選擇CENTRALIZED，按照嚮導的說明啟用集中報告並提交更改。

```
SWA_CLI> reportingconfig

Choose the operation you want to perform:
- COUNTERS - Limit counters recorded by the reporting system.
- WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
- AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
- WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
- CTROBSERVABLE - Enable or Disable CTR observable based indexing.
- CENTRALIZED - Enable/Disable Centralized Reporting for this Secure Web Appliance.
[]> CENTRALIZED

Reporting service status: Local Reporting enabled.  (Show usernames in reports.)

Do you want to enable Centralized Reporting for this appliance? [N]> Y

Do you want to anonymize usernames in reports? [N]> N

Reporting service status: Centralized Reporting enabled.  (Show usernames in reports.)
```

```
Choose the operation you want to perform:
- COUNTERS - Limit counters recorded by the reporting system.
- WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
- AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
- WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
- CTROBSERVABLE - Enable or Disable CTR observable based indexing.
- CENTRALIZED - Enable/Disable Centralized Reporting for this Secure Web Appliance.
[]>

SWA_CLI> commit
```

"此WSA上的URL類別清單早於從SMA發佈的清單"

如果您將配置發佈到SWA並收到Error指示SWA和SMA中的URL類別清單不同，請確保兩台裝置都能連線到Cisco Update Server，並且「updater_logs」中沒有Errors:



Publish in Progress: admin.10_Mar_2026.13:19

Warning — Configuration Publish job admin.10_Mar_2026.13:19 has completed. The configuration was not successfully published to at least one of the destination web appliances.

Job admin.10_Mar_2026.13:19 Started at 10 Mar 2026 13:19 (GMT)

Web Appliances	Progress	Status
SWA SMA Integration		Failure: The list of URL categories on this WSA was older than the list publishe...more

Final status of this job will be reported on the Publish History page.

影象 — URL類別清單不匹配

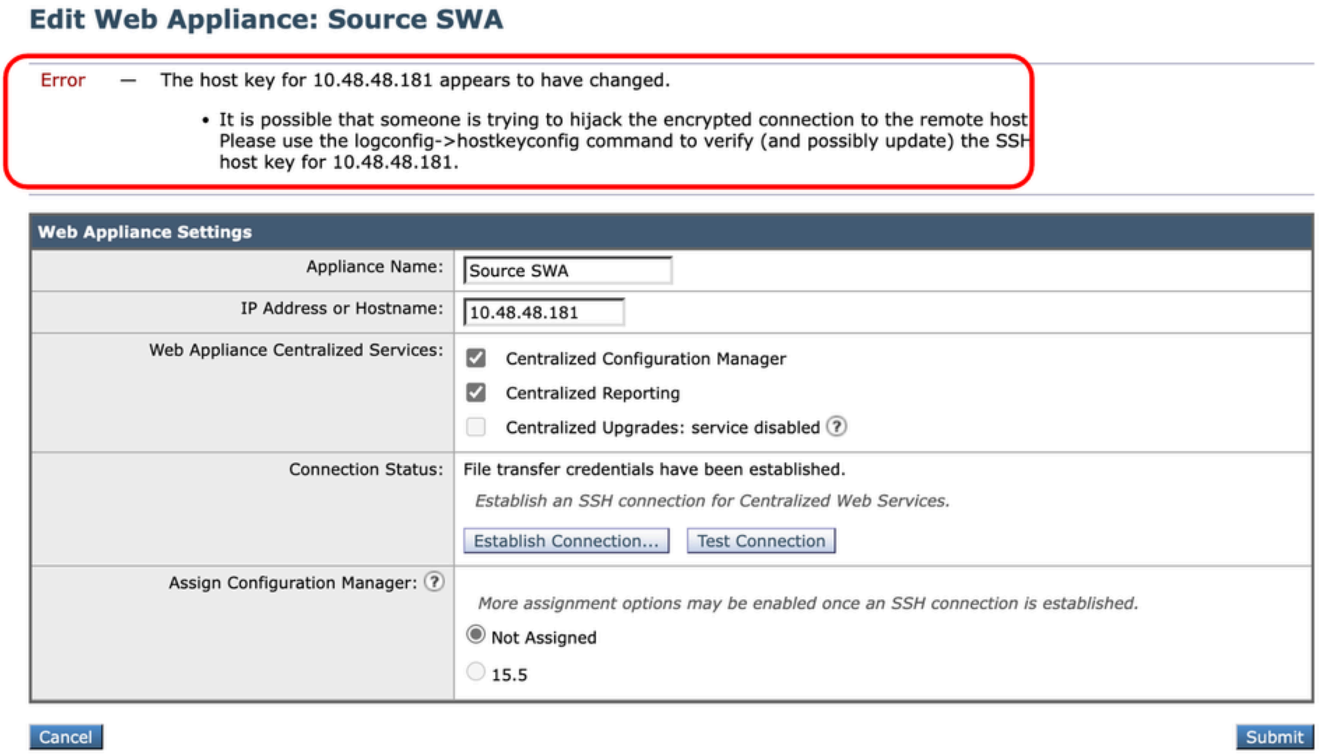
要強制SWA或SMA下載更新，請從CLI鍵入updatenow。

要檢視與更新相關的SMA或SMA日誌，請從CLI鍵入grep並選擇與updater_logs關聯的編號，然後按照嚮導操作

提示：要檢視即時日誌，請在回答Do you want to trail the logs？中鍵入「Y」。[N]>。

"主機金鑰似乎已更改"

如果您正在將SWA整合到SMA並收到主機金鑰已更改的錯誤，則這是因為SMA在其金鑰儲存中儲存了同一IP地址的不同主機金鑰。



Edit Web Appliance: Source SWA

Error — The host key for 10.48.48.181 appears to have changed.

- It is possible that someone is trying to hijack the encrypted connection to the remote host Please use the logconfig->hostkeyconfig command to verify (and possibly update) the SSH host key for 10.48.48.181.

Web Appliance Settings	
Appliance Name:	Source SWA
IP Address or Hostname:	10.48.48.181
Web Appliance Centralized Services:	☑ Centralized Configuration Manager ☑ Centralized Reporting □ Centralized Upgrades: service disabled ?
Connection Status:	File transfer credentials have been established. *Establish an SSH connection for Centralized Web Services.* Establish Connection... Test Connection
Assign Configuration Manager: ?	*More assignment options may be enabled once an SSH connection is established.* ● Not Assigned ○ 15.5

影象 — 主機金鑰似乎已更改

要解決此錯誤，請登入到SMA的CLI，運行logconfig並輸入HOSTKEYCONFIG。鍵入DELETE 並按Enter。然後，選擇與SWA關聯的編號，然後按Enter鍵，直到完成嚮導。

提交更改：

```
SMA_CLI> logconfig

Currently configured logs:
    Log Name             Log Type                      Retrieval           Interval
 --------------------------------------------------------------------------------
 1. aggregatord_logs     Aggregatord Logs              Manual Download     None
 2. authentication       Authentication Logs           Manual Download     None
...

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- DELETELOGFILE - Delete log files
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> HOSTKEYCONFIG

Currently installed host keys:
1. 10.48.48.182 ssh-rsa AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...ZhW4gEXWE=
2. 10.48.48.181 ssh-rsa BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBb...4p74b9Q9k=

Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
- REGENERATESCPKEYS - Regenerate SSH Keys for SCP Log Subscription Retrieval.
[]> DELETE

Enter the number of the key you wish to delete.
[]> 2

Currently installed host keys:
1. 10.62.131.143 ssh-rsa AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...ZhW4gEXWE=

...
SMA_CLI> commit
```

相關資訊

- Cisco Secure Web Appliance AsyncOS 15.2使用手冊
- 在Vmware ESXi上安裝安全Web裝置
- 在Microsoft Hyper-V上安裝安全網路裝置
- 安全Web裝置初始設定
- 思科安全電子郵件和網路虛擬裝置安裝指南
- 在Secure Web Appliance中配置自定義URL類別 — Cisco
- 使用安全Web裝置最佳做法
- 為安全Web裝置配置防火牆
- 在安全Web裝置中配置解密證書
- 對安全Web裝置DNS服務進行故障排除

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）。