将SWA与SMA集成

目录

简介

本文档介绍将安全网络设备(SWA)集成到安全管理设备(SMA)的过程。

先决条件

要求

建议掌握下列主题的相关知识：

- 访问SWA的图形用户界面(GUI)。
- 对SWA的管理访问。
- 对SMA的管理访问。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

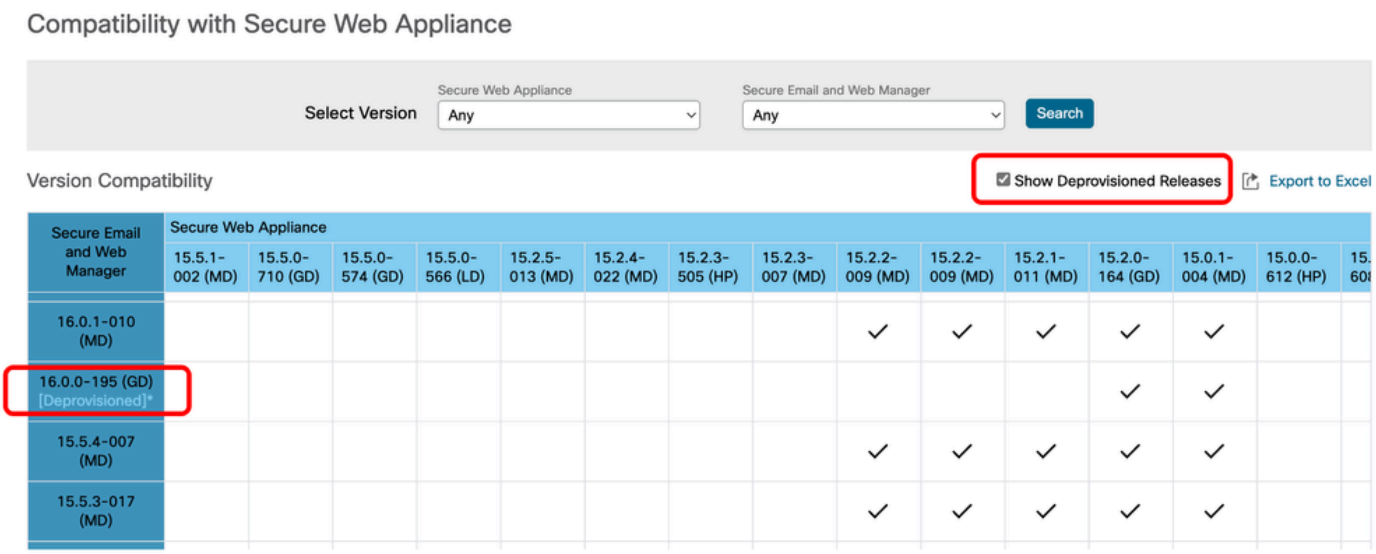
始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

开始使用前

1.确保SMA和SWA均已获得许可。

2.检查SWA和SMA的兼容性矩阵，请使用此链接：[SWA-SMA-ESA兼容性矩阵]。

注意：确保没有取消调配您计划集成的版本。



Compatibility with Secure Web Appliance

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

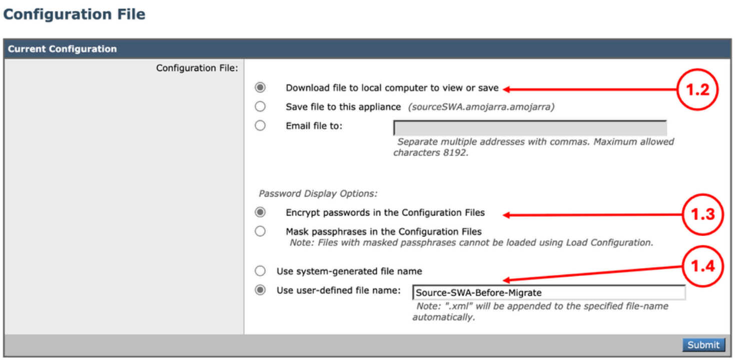
Version Compatibility — ☑ Show Deprovisioned Releases — Export to Excel

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 — 取消调配的版本

将SWA集成到SMA的步骤

步骤1.从SWA导出配置文件	第1.1步：从GUI中，导航到System Administration并选择Configuration File。 第1.2步：确保已选择将文件下载到本地计算机以查看或保存。 第1.3步：在配置文件中选择加密密码。 第1.4步(可选)选择配置文件的名称。 第1.5步。单击提交。



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 — 导出配置文件

步骤2.创建配置管理器

注意：如果Configuration Manager已在SMA中配置，请跳至步骤4。

步骤2.1.从SMA GUI中单击Web选项卡卡。

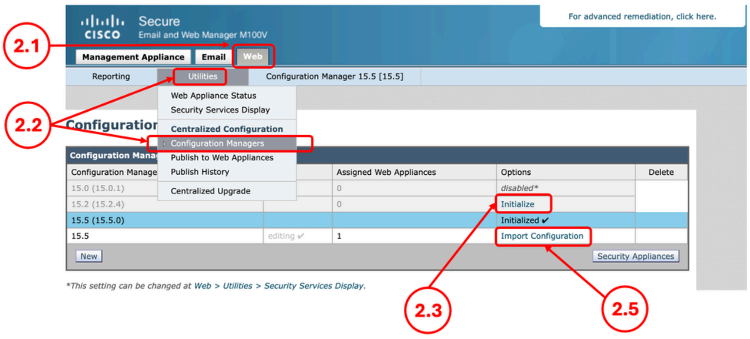
第2.2步：从实用程序选择Configuration Manager。

第2.3步：如果配置管理器尚未初始化，请点击所需配置管理器的Initialize链接，否则跳至第2.5步。

提示：Configuration Manager版本必须与SWA版本的前两个网段保持一致。例如，如果您的SWA版本是15.5.0-710，则必须使用Configuration Manager 15.5。

第2.4步：选择使用默认设置，然后点击Initialize。

第2.5步：点击所需的Configuration Manager的Import Configuration。



Configuration Manager 15.5 [15.5]

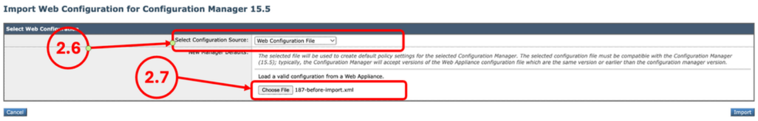
Configuration Manage		Assigned Web Appliances	Options	Delete
15.0 (15.0.1)		0	disabled*	
15.2 (15.2.4)		0	Initialize	
15.5 (15.5.0)			Initialized ✔	
15.5	editing ✔	1	Import Configuration	

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

映像 — 配置管理器

第2.6步：从Select Configuration Source中选择Web Configuration File。

第2.7步。选择您在第1步中导出的配置文件。

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


Import Web Configuration for Configuration Manager 15.5

Select Web Configuration

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 — 导入配置

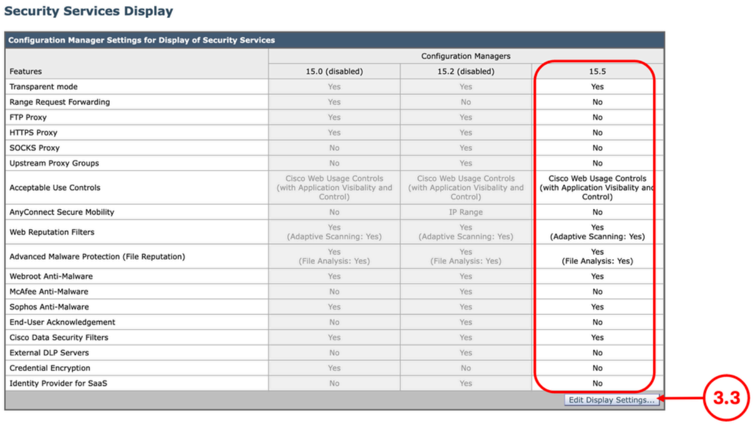
第2.8步。单击导入。

步骤2.9.提交更改。
</td>
</tr>
<tr>
<td>步骤3. Configuration Manager设置</td>
<td>
步骤3.1.从SMA GUI单击Web选项卡卡。

第3.2步：从Utilities中选择Security Services Display。

第3.3步：确保所需的功能配置正确，您可以启用或禁用编辑显示设置的功能。

第3.4步：如果进行了任何更改，请提交并提交。



Security Services Display

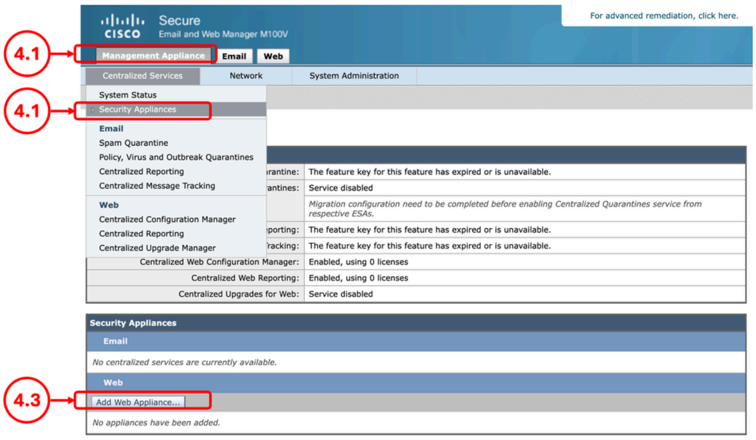
Configuration Manager Settings for Display of Security Services

<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 Visibality and Control)</td><td>Cisco Web Usage Controls (with Application Visibality and Control)</td><td>Cisco Web Usage Controls (with Application Visibality 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>

图像 — 安全服务显示
</td>
</tr>
<tr>
<td>步骤4.添加Web设备</td>
<td>
第4.1步：从SMA GUI中点击管理设备选项卡。

第4.2步：从集中服务选择安全设备。

第4.3步：点击添加Web设备
</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.

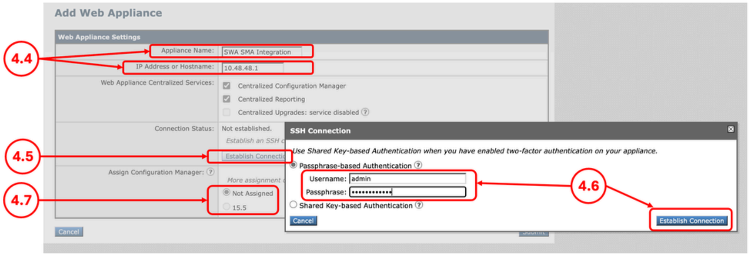
图像 — 添加Web设备

步骤4.4.输入设备名称和IP地址或主机名。

第4.5步。单击建立连接。

第4.6步：输入Username和Passphrase，然后单击Establish Connection。

步骤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

Establish Connecti

Assign Configuration Manager:

More assignment o

● Not Assigned ○ 15.5

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

图像 — 添加SWA

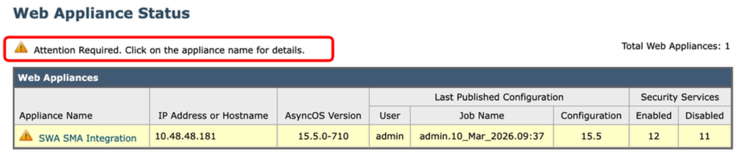
步骤4.8.提交并提交更改。

步骤5.验证集成

步骤5.1.在SMA GUI中，点击Web选项卡卡。

第5.2步：从Utilities中，选择Web Appliance Status。

第5.3步：如果您看到警告消息“Attention Required”。点击设备名称了解详细信息，点击SWA的名称，然后查看详细信息。



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

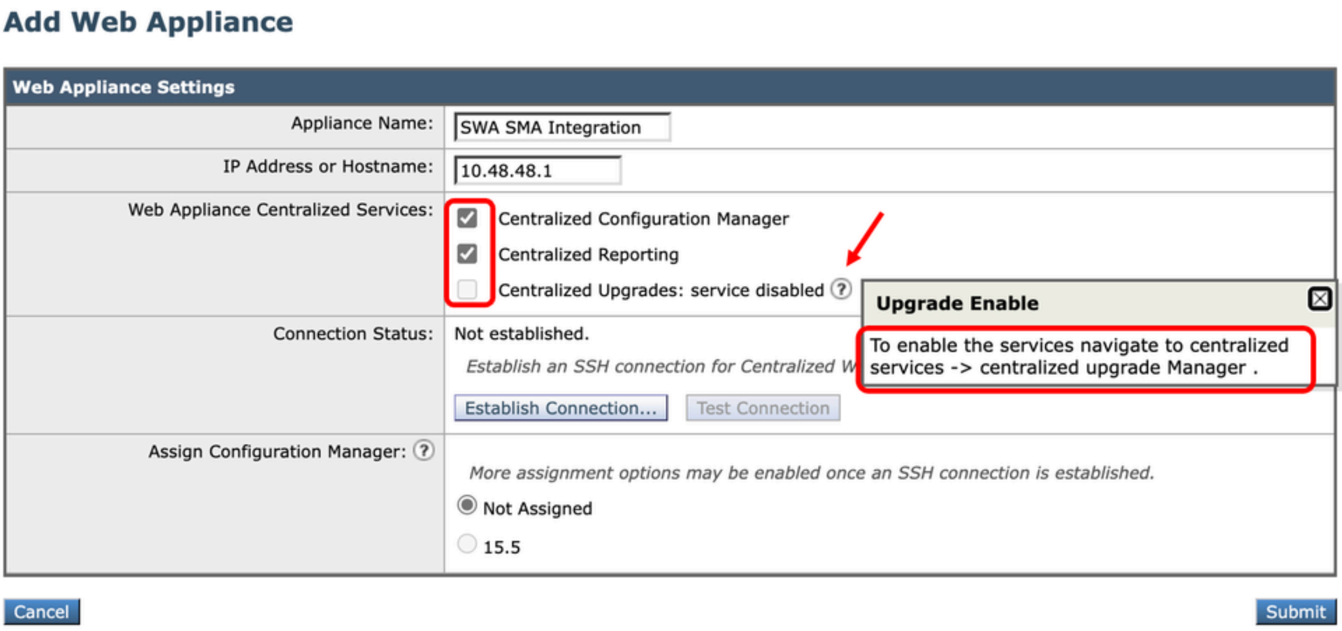
图像 — Web设备状态

	提示：对于故障排除，请查看本文的修复错误部分。

修复错误

"集中服务已禁用"

当您尝试选择集中服务时，如果复选框处于非活动状态，请点击问号(?)，指南将引导您通过路径来启用该服务。



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*
Assign Configuration Manager: ?	*More assignment options may be enabled once an SSH connection is established.* ● Not Assigned ○ 15.5

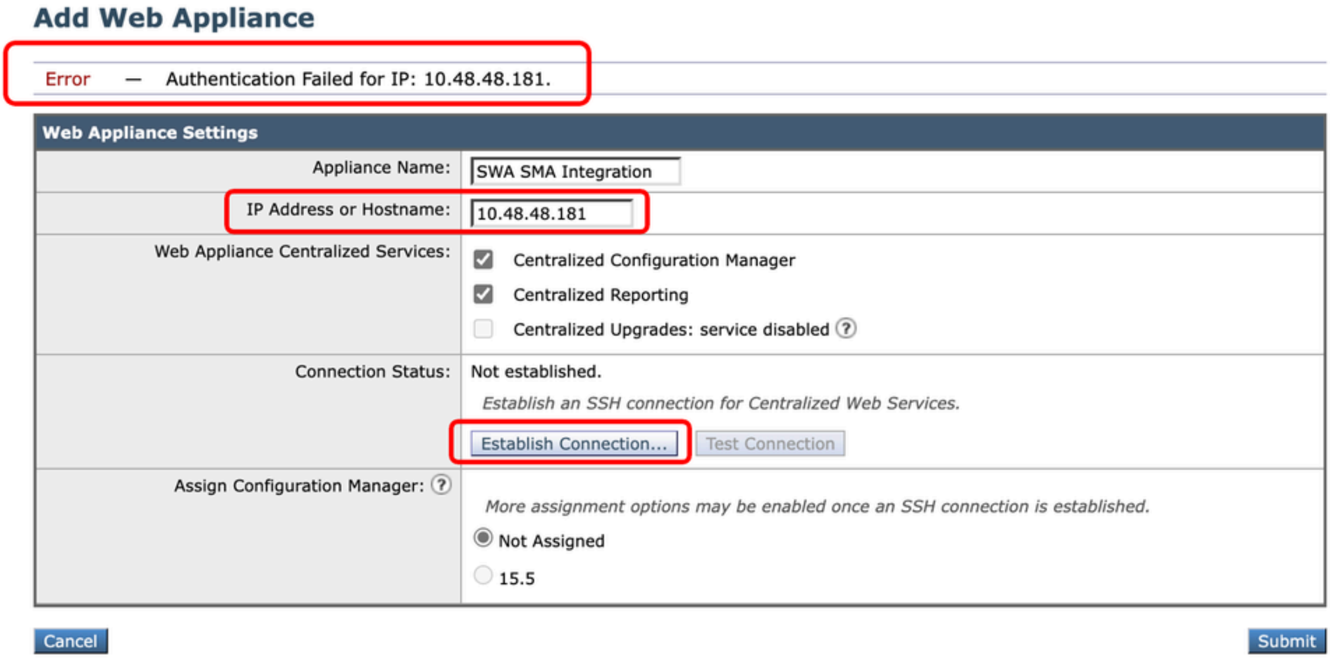
Upgrade Enable

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

映像 — 集中服务已禁用

"IP身份验证失败"

如果您收到此错误，请将SWA集成到SMA时，请确保IP地址或主机名以及凭证正确。



Add Web Appliance

Error — Authentication Failed for IP: 10.48.48.181.

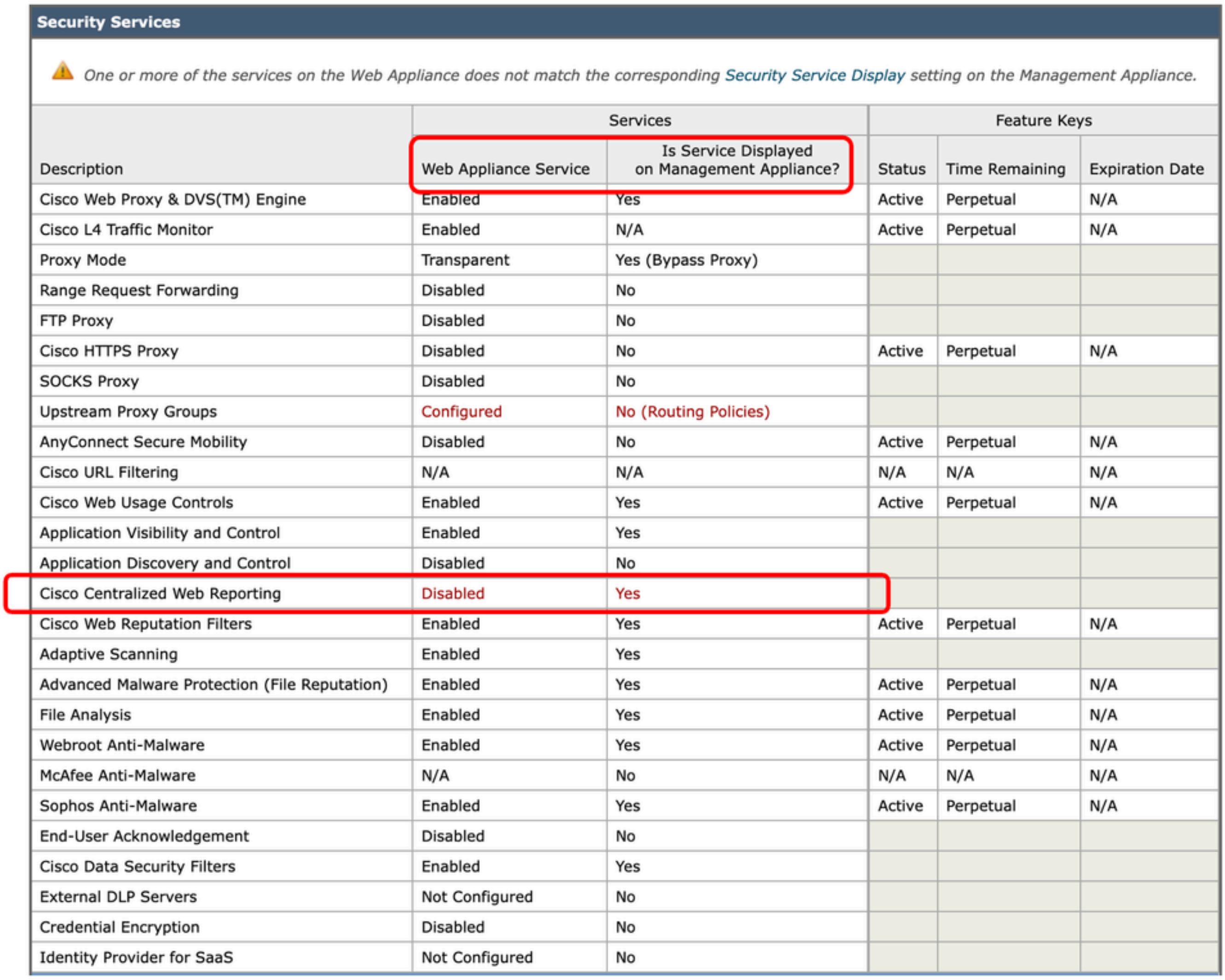
Web Appliance Settings

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

映像 — 身份验证失败

“思科集中网络报告在SWA中已禁用”

如果SMA配置了集中网络报告，并且您在“第4步”中将SWA集成到SMA时将该功能分配给SWA，则需要启用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			

图像 — 在SWA中禁用集中网络报告

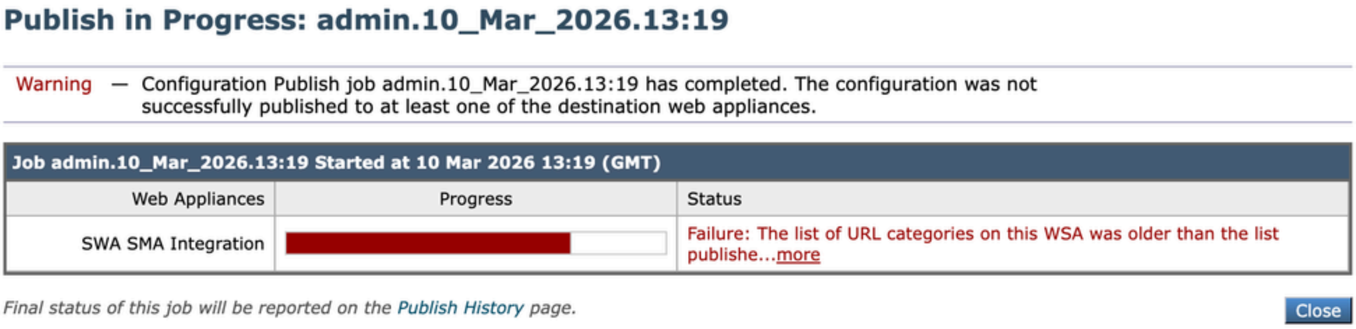
要解决此问题，请从CLI连接到SWA并键入reportingconfig并选择CENTRALIZED，按照向导操作以启用集中报告并提交更改。

```
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类别列表早于从SMA发布的列表"

如果您将配置发布到SWA并收到Error（错误）指示SWA和SMA中的URL类别列表不同，请确保两个设备均可连接到Cisco Update Server，并且“updater_logs”中没有错误：



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.

图像 — URL类别列表不匹配

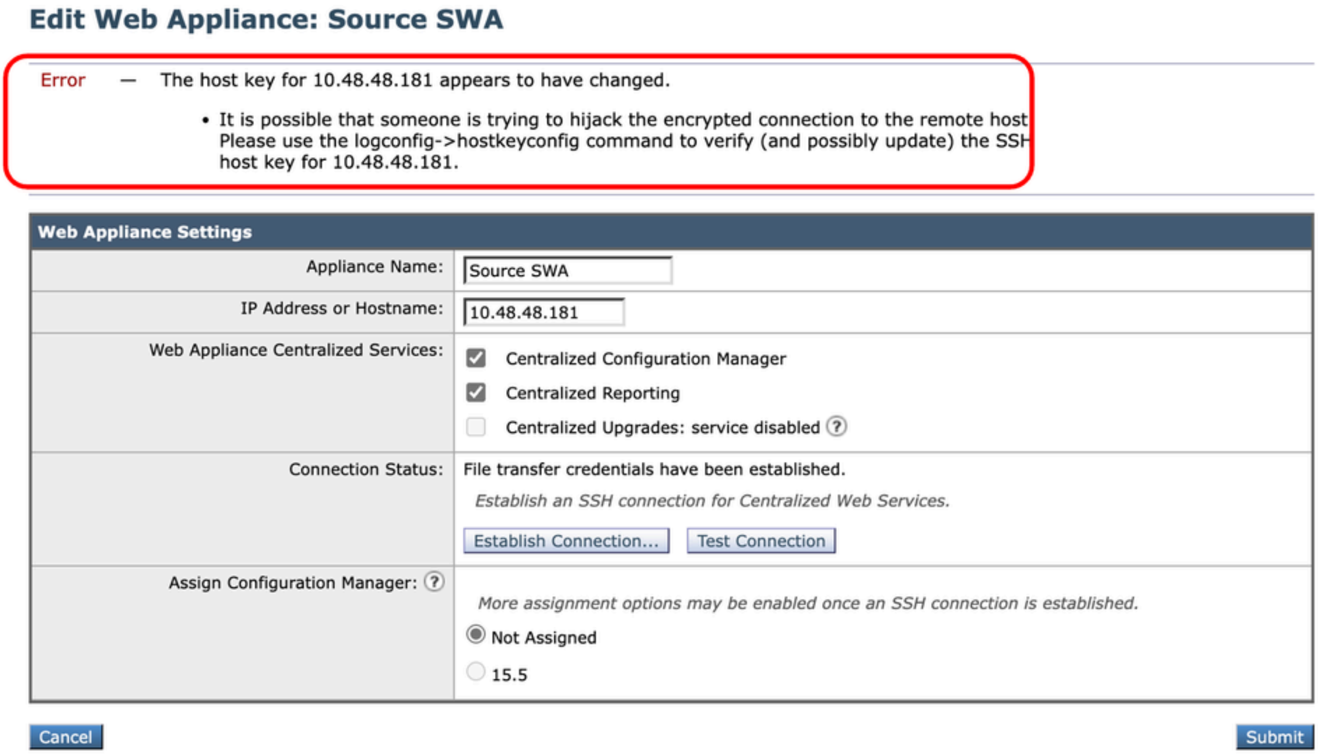
要强制SWA或SMA下载更新，请从CLI键入updatenow。

要查看与更新相关的SMA或SMA日志，请从CLI键入grep并选择与updater_logs关联的编号，然后按照向导操作

提示：要查看实时日志，请在答案Do you want to tail the logs？（是否要跟踪日志？）中键入“Y”。[N]>。

"主机密钥似乎已更改"

如果您将SWA集成到SMA并收到“Error that the host key has been changed”（主机密钥已更改），这是因为SMA在其密钥存储中存储了同一IP地址的不同主机密钥。



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

图像 — 主机密钥似乎已更改

要解决此错误，请登录SMA的CLI，运行logconfig并输入HOSTKEYCONFIG。键入DELETE，然后按Enter。然后，选择与SWA关联的编号，然后按Enter直到完成向导。

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
```

相关信息

- 思科安全Web设备AsyncOS 15.2用户指南
- 在Vmware ESXi上安装安全Web设备
- 在Microsoft Hyper-V上安装安全Web设备

- 安全Web设备初始设置

- 思科安全邮件和Web虚拟设备安装指南
- 在安全Web设备中配置自定义URL类别 — 思科

- 使用安全Web设备最佳实践

- 为安全Web设备配置防火墙

- 在安全Web设备中配置解密证书

- 安全网络设备DNS服务故障排除

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。