将SWA与SMA集成

目录

简介

先决条件

- 要求
- 使用的组件

开始使用前

将SWA集成到SMA的步骤

- 步骤1.从SWA导出配置文件
- 步骤2.创建配置管理器
- 步骤3.配置管理器设置
- 步骤4.添加Web设备
- 步骤5.验证集成

修复错误

- 集中服务已禁用
- IP身份验证失败
- SWA中禁用集中网络报告
- 此SWA上的URL类别列表早于SMA发布的列表
- 主机密钥似乎已更改

相关信息

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。

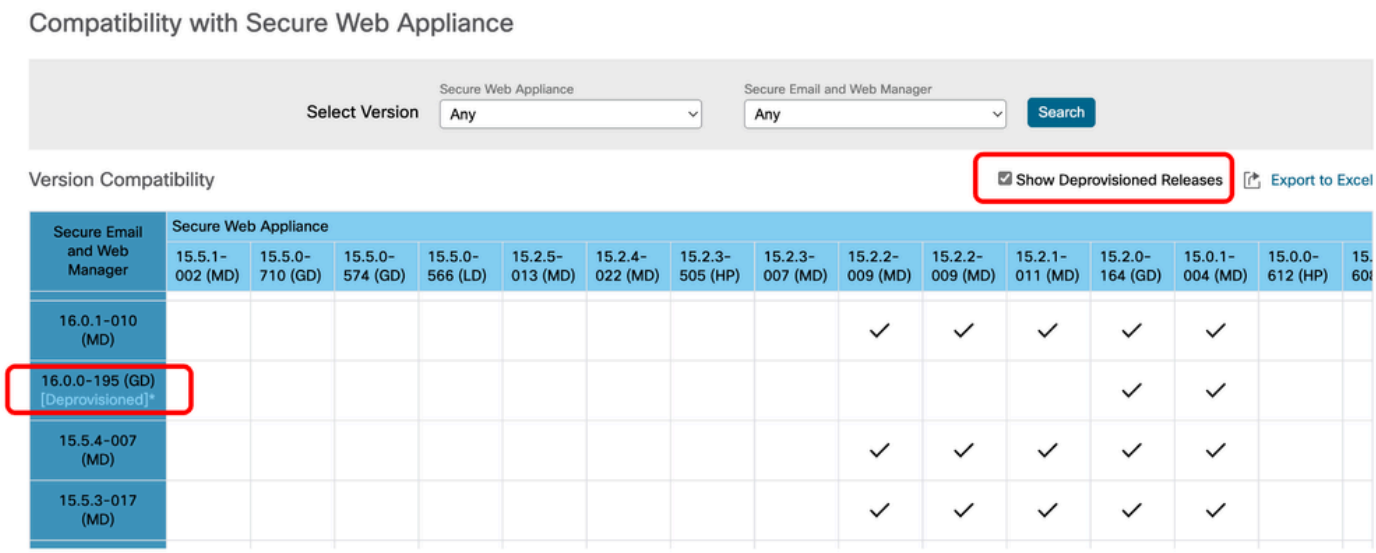
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

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。



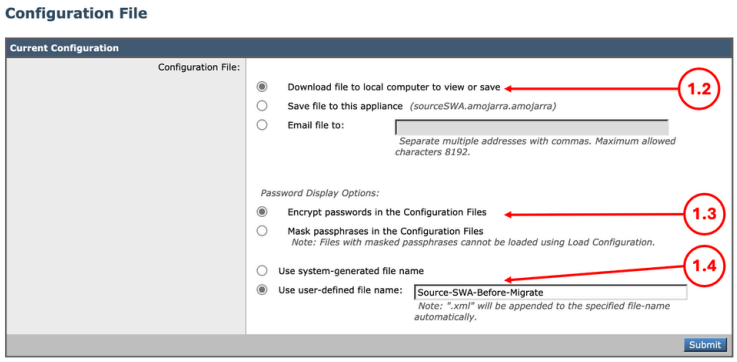
映像 — 取消调配的版本

将SWA集成到SMA的步骤

步骤1.从SWA导出配置文件	1.1.从GUI导航到系统管理，然后选择配置文件。 1.2.确保选中“将文件下载到本地计算机以查看或保存”。 1.3.在“配置文件”中选择“加密密码”。

1.4.（可选）选择配置文件的名称。

1.5.单击Submit。



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。

2.1.在SMA GUI中，单击Web选项卡。

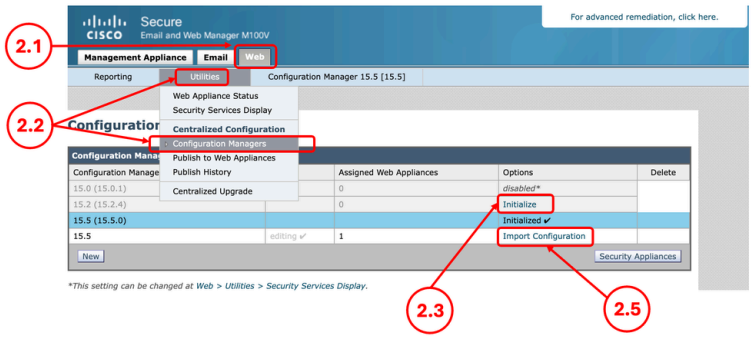
2.2.从Utilities中选择Configuration Manager。

2.3.如果配置管理器尚未初始化，请单击所需配置管理器的初始化链接，否则跳到步骤2.5。

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。

2.4.选择使用默认设置，然后选择初始化。

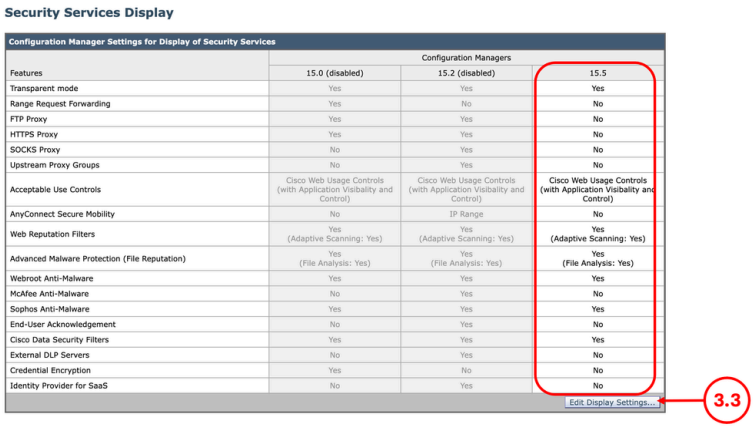
2.5.为所需的Configuration Manager选择Import Configuration。

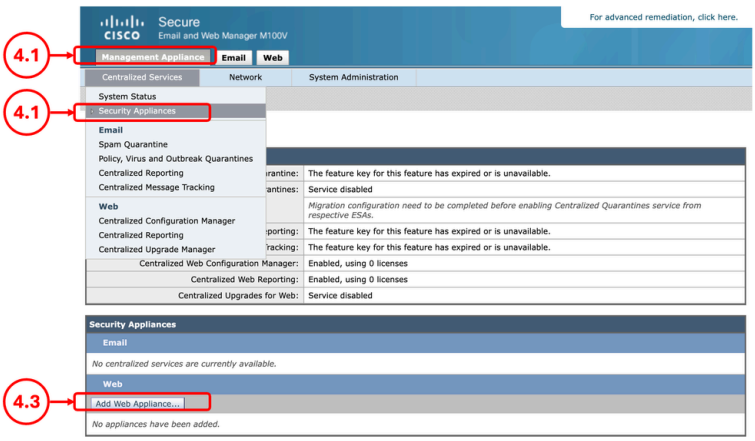


映像 — 配置管理器

2.6.从选择配置源中选择Web配置文件。

2.7.选择您在第1步中导出的配置文件。

	 映像 — 导入配置 2.8.选择导入。 2.9.确定更改。
步骤3.配置管理器设置	3.1.在SMA GUI中，单击Web选项卡。 3.2.从实用程序中选择安全服务显示。 3.3.确保所需功能配置正确，您可以在编辑显示设置中启用或禁用这些功能。 3.4.如果您进行了任何更改，请提交并提交。  图像 — 安全服务显示
步骤4.添加Web设备	4.1.在SMA GUI中，单击Management Appliance选项卡。 4.2.从Centralized Services中选择Security Appliances。 4.3.选择添加Web设备。



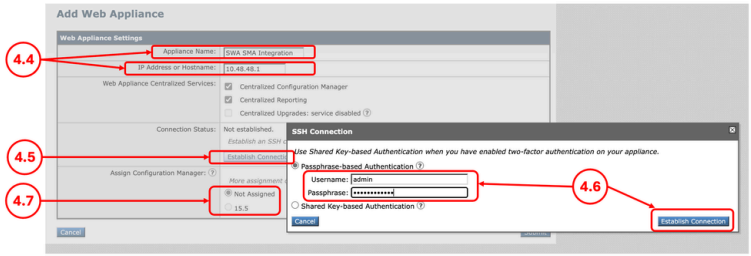
图像 — 添加Web设备

4.4.输入设备名称和IP地址或主机名。

4.5.选择建立连接。

4.6.输入用户名和密码，然后选择建立连接。

4.7.分配Configuration Manager。



图像 — 添加SWA

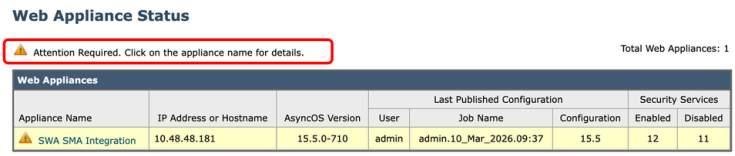
4.8.提交并提交更改。

步骤5.验证集成

5.1.从SMA GUI中，单击Web选项卡。

5.2.从实用程序中选择Web设备状态。

5.3.如果您看到警告消息Attention Required，请点击设备名称了解详细信息。单击SWA的名称，然后查看详细信息。



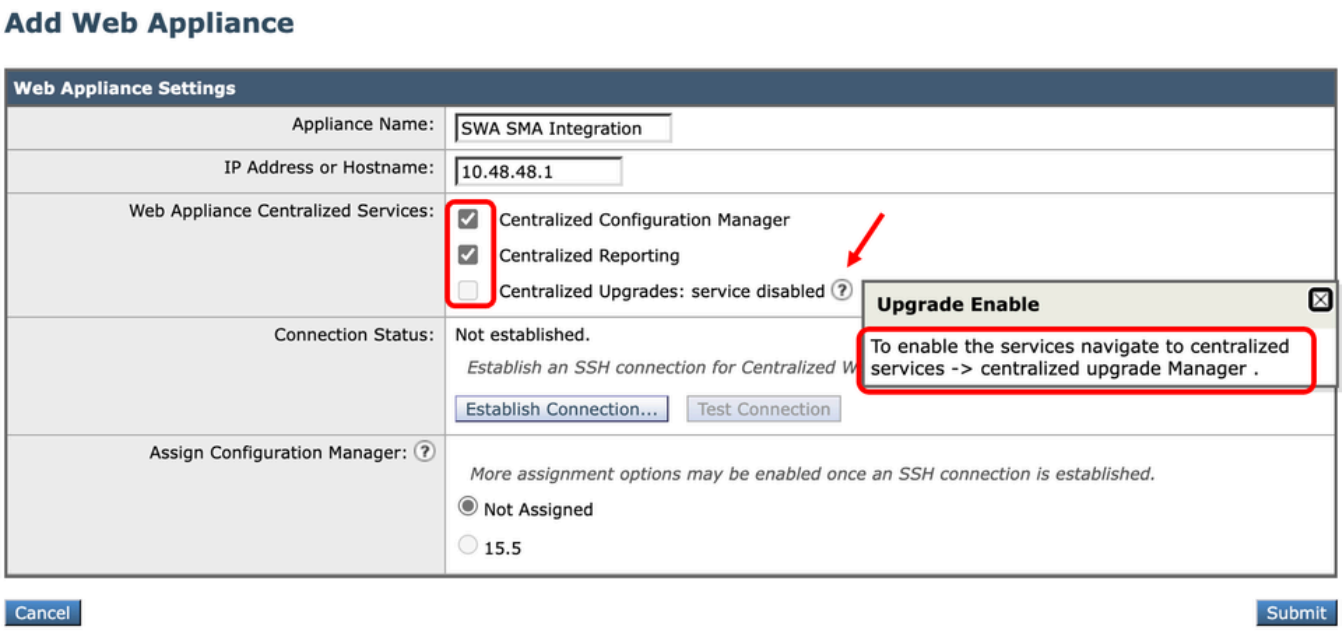
图像 — Web设备状态

提示：有关疑难解答视图，请参见本文中的“修复错误”一节。

修复错误

集中服务已禁用

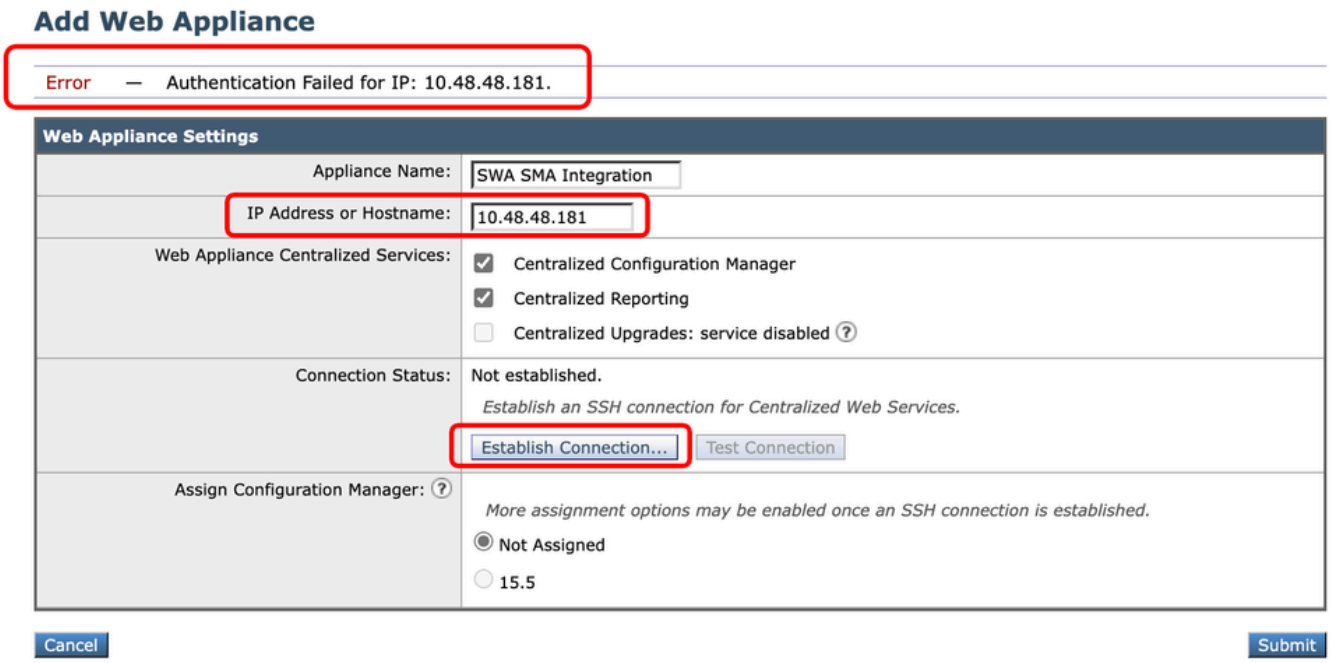
当您尝试选择集中服务时，如果复选框处于非活动状态，请点击问号(?)，指南将引导您通过路径来启用该服务。



映像 — 集中服务已禁用

IP身份验证失败

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



映像 — 身份验证失败

SWA中禁用集中网络报告

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时将该功能分配到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.

Description	Services		Feature Keys		
	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，完成向导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
```

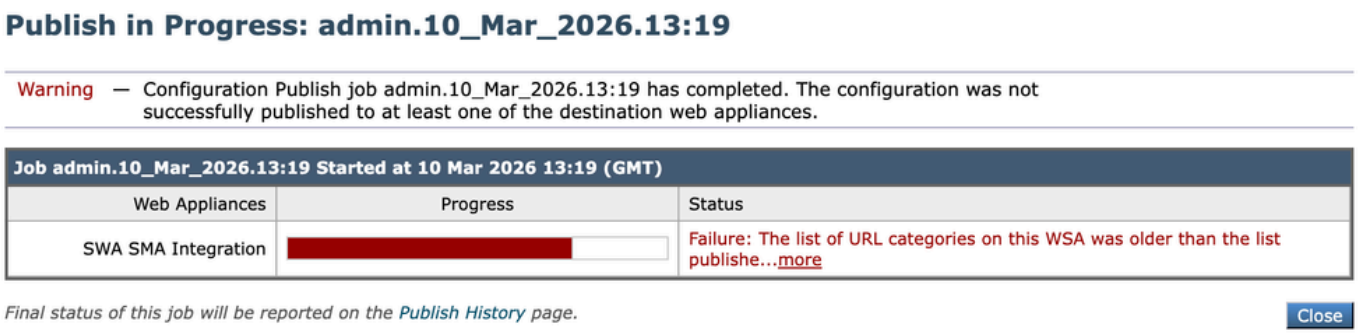
```
Reporting service status: Centralized Reporting enabled.  (Show usernames in reports.)


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SWA上的URL类别列表早于SMA发布的列表

如果您将配置发布到SWA并收到指示SWA和SMA中的URL类别列表不相同的错误，请确保两台设备都可以连接到Cisco更新服务器，并且updater_logs中没有错误：



图像 — URL类别列表不匹配

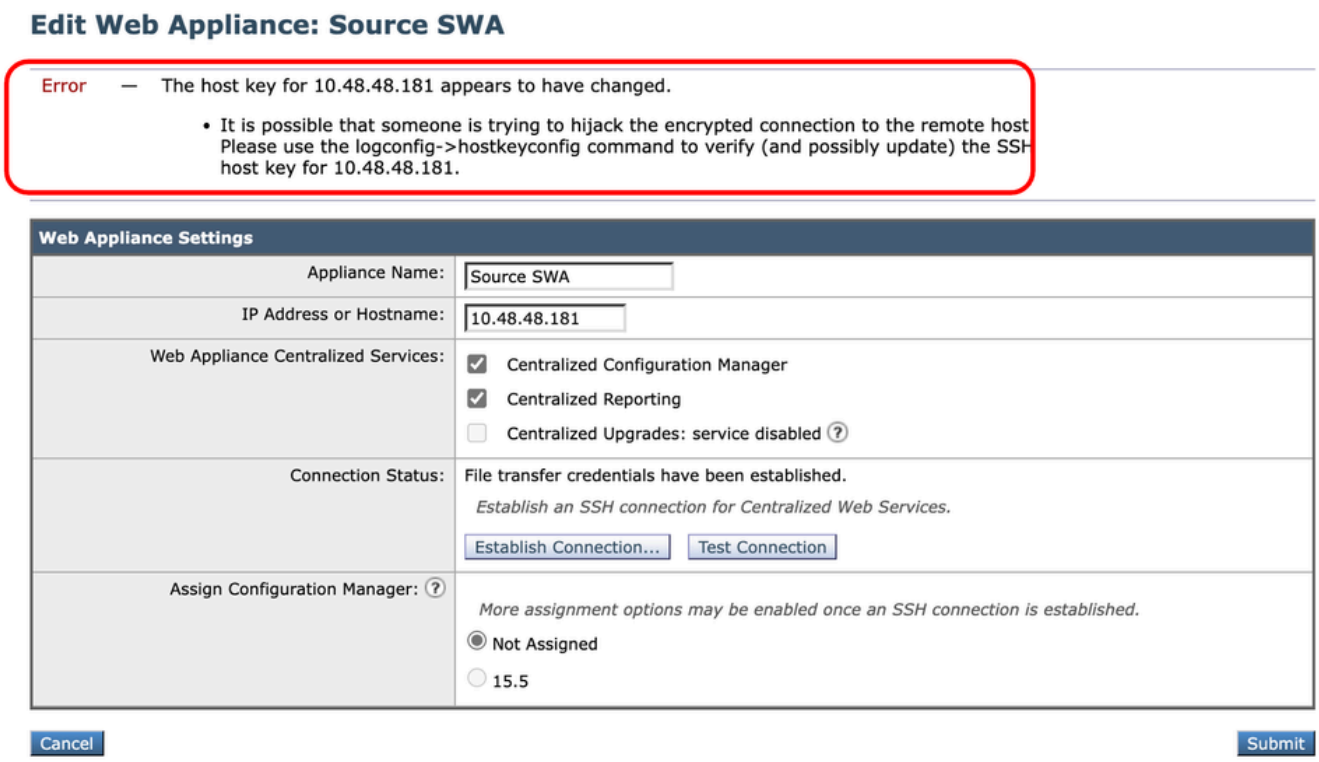
要强制SWA或SMA下载更新，请从CLI键入updatenow。

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，并完成向导。

提示：要查看实时日志，请在答案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。



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关联的号码，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 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...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 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...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）。