Intégration de SWA à SMA

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Avant de commencer

Étapes d'intégration de SWA à SMA

- Étape 1 : exportation du fichier de configuration à partir de SWA
- Étape 2 : création de Configuration Manager
- Étape 3.Configuration des paramètres du gestionnaire
- Étape 4. Ajout d'un appareil Web
- Étape 5. Validation de l'intégration

Correction des erreurs

- Le service centralisé est désactivé
- Échec de l'authentification pour IP
- Le rapport Web centralisé est désactivé dans le SWA
- La liste des catégories d'URL de ce SWA était plus ancienne que la liste publiée par SMA
- La clé d'hôte semble avoir changé

Informations connexes

Introduction

Ce document décrit le processus d'intégration de l'appliance Web sécurisé (SWA) à l'appliance de gestion de la sécurité (SMA).

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Accès à l'interface graphique utilisateur (GUI) de SWA.
- Accès administratif au SWA.

- Accès administratif au SMA.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Avant de commencer

1. Assurez-vous que le SMA et le SWA sont tous deux sous licence.

2. Vérifiez la matrice de compatibilité du SWA et du SMA, utilisez ce lien : [Matrice de compatibilité SWA-SMA-ESA](#).

Remarque : assurez-vous que la version que vous prévoyez d'intégrer n'est pas désapprovisionnée.

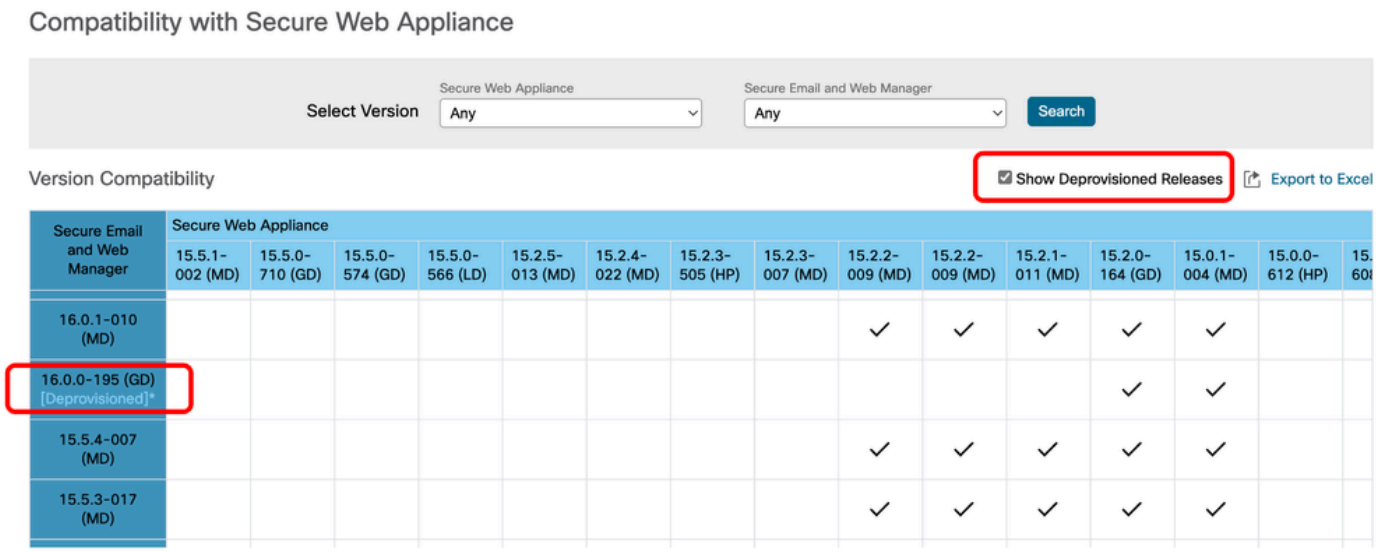
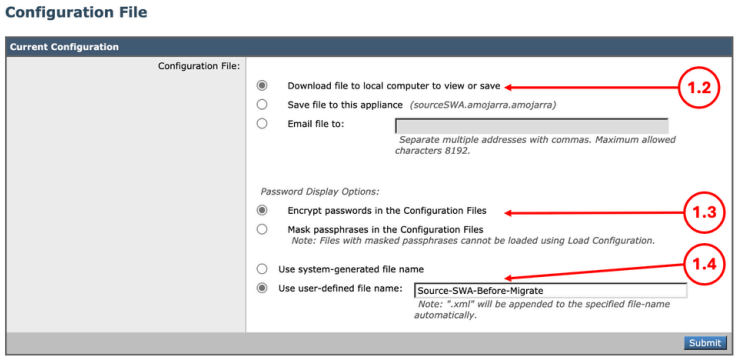
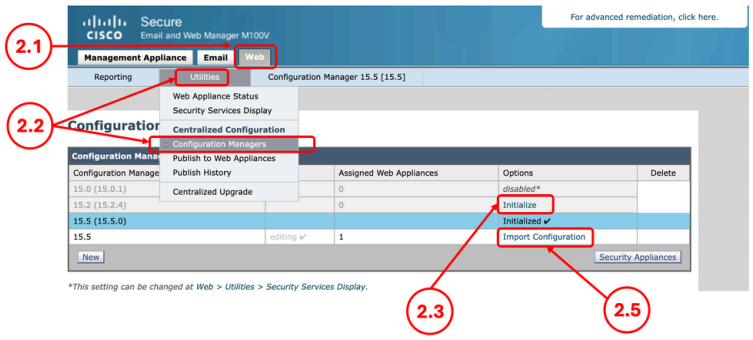


Image - Versions désapprovisionnées

Étapes d'intégration de SWA à SMA

Étape 1 : exportation du fichier de configuration à partir de SWA	1.1. Dans l'interface utilisateur graphique, accédez à Administration système et sélectionnez Fichier de configuration. 1.2. Assurez-vous que l'option Download file to local computer to view or save est sélectionnée. 1.3. Sélectionnez Chiffrer les mots de passe dans les fichiers de configuration. 1.4. (Facultatif) Choisissez un nom pour le fichier de configuration. 1.5. Cliquez sur Envoyer.  Image - Exportation du fichier de configuration
Étape 2 : création de Configuration Manager Remarque : Si Configuration Manager est déjà configuré dans le SMA, passez à l'étape 4.	2.1.Dans l'interface utilisateur graphique de SMA, cliquez sur l'onglet Web. 2.2. Dans Utilitaires, sélectionnez Gestionnaire de configuration. 2.3. Si le gestionnaire de configuration n'est pas encore initialisé, cliquez sur le lien Initialize pour le gestionnaire de configuration souhaité, sinon passez à l'étape 2.5. Conseil : La version de Configuration Manager doit correspondre aux deux premiers segments de votre version SWA. Par exemple, si votre version SWA est 15.5.0-710, vous devez utiliser Configuration Manager 15.5. 2.4. Sélectionnez Utiliser les paramètres par défaut et sélectionnez Initialiser.

	2.5. Sélectionnez Importer la configuration pour le gestionnaire de configuration souhaité.  Image - Gestionnaire de configuration 2.6. Dans Sélectionner la source de configuration, sélectionnez Fichier de configuration Web. 2.7. Sélectionnez le fichier de configuration que vous avez exporté à l'étape 1.  Image - Importer la configuration 2.8. Sélectionnez Importer. 2.9. Valider les modifications.
Étape 3 : configuration des paramètres du gestionnaire	3.1. Dans l'interface utilisateur graphique de SMA, cliquez sur l'onglet Web. 3.2. Dans Utilities, sélectionnez Security Services Display. 3.3. Assurez-vous que les fonctionnalités souhaitées sont configurées correctement, vous pouvez les activer ou les désactiver à partir de Modifier les paramètres d'affichage. 3.4. Si vous avez apporté des modifications, cliquez sur Envoyer et confirmer.

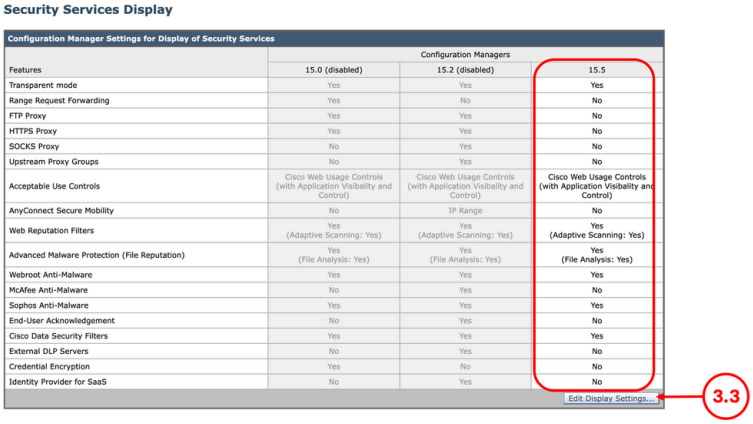
<table>
<tr>
<td></td>
<td>


Image - Affichage des services de sécurité</td>
</tr>
<tr>
<td>Étape 4. Ajout d'un appareil Web</td>
<td>4.1.Dans l'interface utilisateur graphique SMA, cliquez sur l'onglet Management Appliance (Appareil de gestion).

4.2. Dans Services centralisés, sélectionnez Appareils de sécurité.

4.3. Sélectionnez Add Web Appliance.

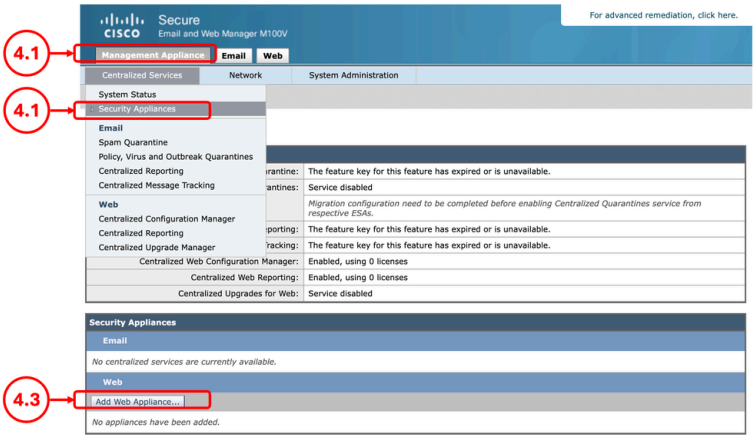


Image - Ajouter un appareil Web

4.4. Saisissez le nom du matériel et l'adresse IP ou le nom d'hôte.

4.5. Sélectionnez Établir la connexion.

4.6. Saisissez le nom d'utilisateur et la phrase de passe, puis sélectionnez Établir la connexion.

4.7. Attribution du gestionnaire de configuration.</td>
</tr>
</table>

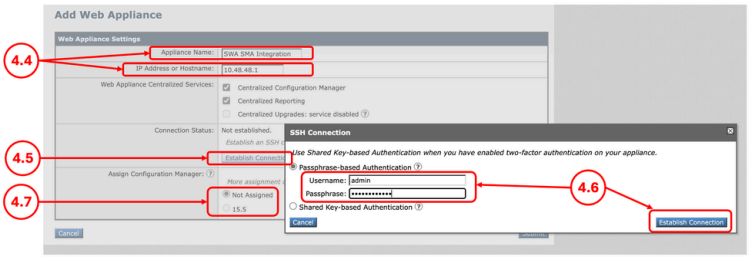
<table>
<tr>
<td></td>
<td>

Image - Ajout du SWA

4.8. Soumettre et valider les modifications</td>
</tr>
<tr>
<td>Étape 5. Validation de l'intégration</td>
<td>5.1.Dans l'interface utilisateur graphique de SMA, cliquez sur l'onglet Web.

5.2. Dans Utilities, sélectionnez Web Appliance Status.

5.3. Si un message d'avertissement s'affiche Attention requise, cliquez sur le nom de l'appliance pour plus d'informations. Cliquez sur le nom du SWA et affichez les détails.

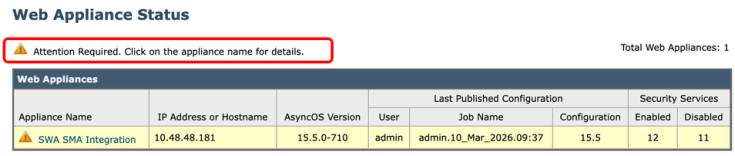


Image - État de l'appliance Web

Conseil : Pour obtenir une vue de dépannage, consultez la section Correction des erreurs de cet article.</td>
</tr>
</table>

Correction des erreurs

Le service centralisé est désactivé

Lorsque vous essayez de sélectionner un service centralisé, si la case est inactive, cliquez sur le point d'interrogation (?) et le guide vous guide dans le chemin pour activer ce service.

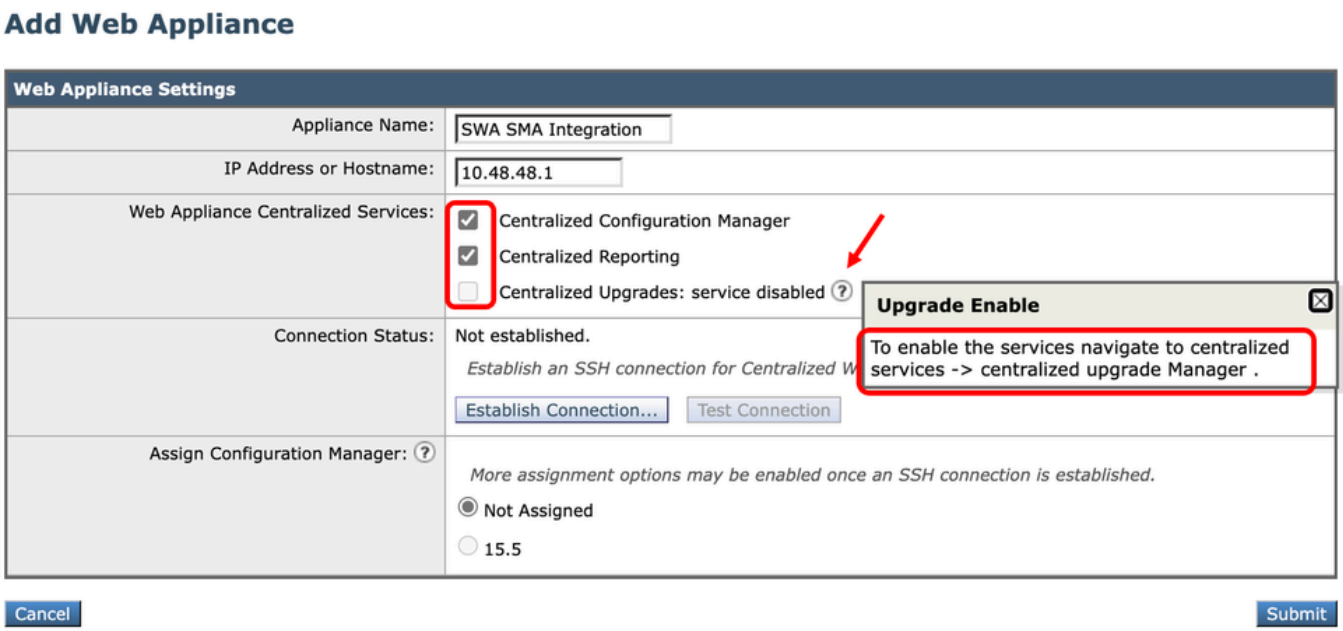


Image - Les services centralisés sont désactivés

Échec de l'authentification pour IP

Lorsque vous intégrez le SWA à SMA, si vous recevez cette erreur, vérifiez que l'adresse IP ou le nom d'hôte et les informations d'identification sont corrects.

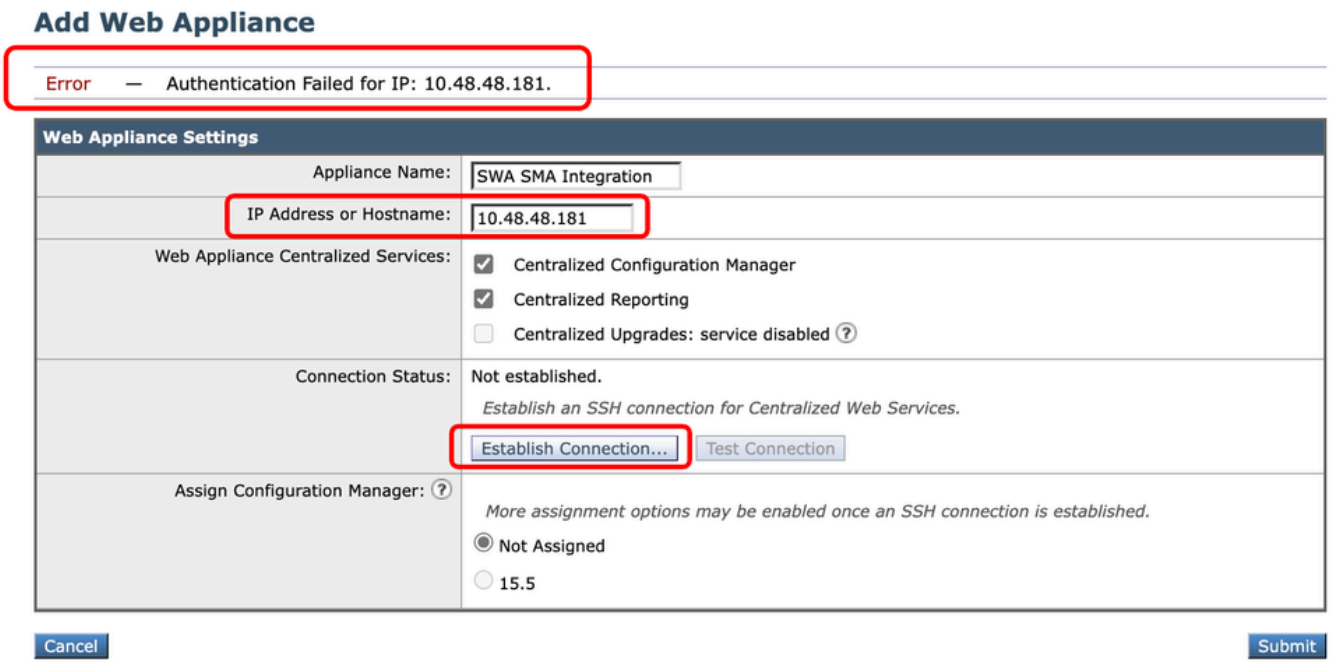


Image - Échec de l'authentification

Le rapport Web centralisé est désactivé dans le SWA

Si le SMA est configuré avec la fonction de rapport Web centralisé et que vous attribuez cette fonctionnalité au SWA tout en intégrant le SWA au SMA à l'étape 4, vous devez activer 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			

Image - La fonction de rapport Web centralisé est désactivée dans le SWA

Pour résoudre le problème, connectez-vous au SWA à partir de l'interface de ligne de commande et tapez reportingconfig et sélectionnez CENTRALIZED, terminez l'assistant pour activer le rapport centralisé et validez les modifications.

```
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
```

La liste des catégories d'URL de ce SWA était plus ancienne que la liste publiée par SMA

Si, pendant que vous publiez la configuration sur SWA et recevez l'erreur indiquant que la liste des catégories d'URL dans SWA et SMA ne sont pas identiques, assurez-vous que les deux périphériques sont capables de se connecter à Cisco Update Server et qu'il n'y a pas d'erreurs dans le fichier updater_logs :

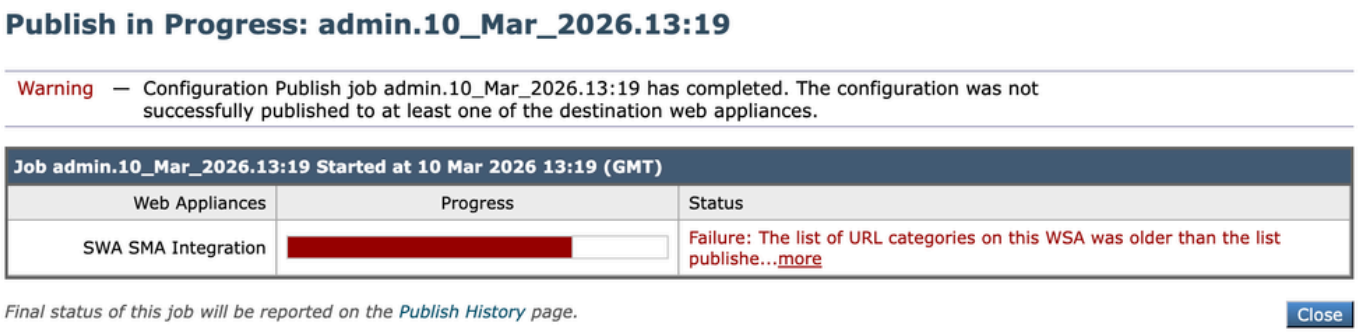


Image - La liste des catégories d'URL ne correspond pas

Pour forcer le SWA ou le SMA à télécharger la mise à jour, à partir de l'interface de ligne de commande, tapez updatenow.

Pour afficher le SMA ou le SMA, Journaux associés à la mise à jour, à partir de l'interface de ligne de commande, tapez grep et choisissez le numéro associé à updater_logs et terminez l'assistant.

Conseil : pour afficher les journaux en direct, tapez Y dans la réponse à Voulez-vous suivre

les journaux ? [N]>.

La clé d'hôte semble avoir changé

Si vous intégrez le SWA au SMA et recevez l'erreur indiquant que la clé d'hôte a été modifiée, cela est dû au fait que SMA a stocké une autre clé d'hôte pour la même adresse IP dans son magasin de clés.

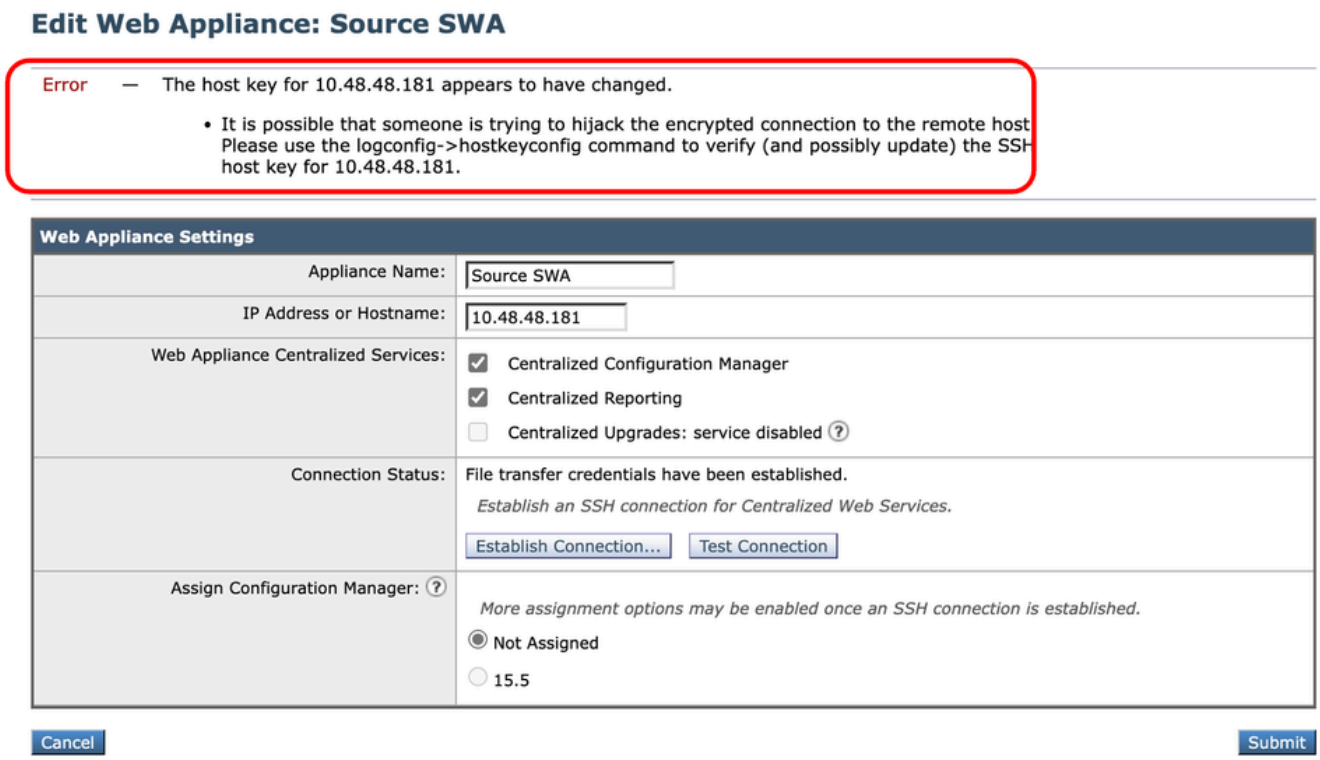


Image : la clé d'hôte semble avoir été modifiée

Pour corriger cette erreur, connectez-vous à l'interface CLI de SMA, exécutez logconfig et entrez HOSTKEYCONFIG. Tapez DELETE et appuyez sur Entrée. Ensuite, sélectionnez le numéro associé à l'Assistant et appuyez sur Entrée jusqu'à ce que l'Assistant ait terminé.

Validez les modifications :

```
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 BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBb...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
```

Informations connexes

- Guide de l'utilisateur d'AsyncOS 15.2 pour Cisco Secure Web Appliance
- Installer l'appliance Web sécurisée sur VMware ESXi
- Installer l'appliance Web sécurisée sur Microsoft Hyper-V
- Configuration initiale de Secure Web Appliance
- Guide d'installation de l'appliance virtuelle Cisco Secure Email and Web
- Configurer des catégories d'URL personnalisées dans Secure Web Appliance - Cisco
- Utilisation des meilleures pratiques de sécurisation des appliances Web
- Configurer le pare-feu pour l'appliance Web sécurisée
- Configurer le certificat de déchiffrement dans l'appareil Web sécurisé
- Dépannage du service DNS de l'appliance Web sécurisée

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.