Migration de la configuration entre deux SWA

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Avant de commencer
- Préparation et sauvegarde du SWA source
  - Étape 1. Exportation du fichier de configuration
  - Étape 2. Exportation du certificat de déchiffrement
  - Étape 3. Exportation des certificats racines de confiance personnalisés
  - Étape 4. Exportation du certificat de l'interface graphique
  - Étape 5. Exportation des certificats ISE
  - Étape 6. Licences / Fonctionnalités
  - Étape 7. Certificat de redirection d'authentification
  - Étape 8. Exportation des routes statiques
  - Étape 9. Paramètres DNS
- Préparation du SWA cible
  - Étape 10. Installation de Virtual SWA
  - Étape 11. Configuration initiale de SWA
  - Étape 12. Désactivation du fichier de configuration
- Importation du fichier de configuration dans le SWA cible
  - Étape 13. Importation de certificats racine de confiance personnalisés
  - Étape 14. Importation du fichier de configuration
  - Étape 15. Modification du mot de passe admin
  - Étape 16. Valider
  - Étape 17. Importation des routes
  - Étape 18. Configuration des paramètres DNS
  - Étape 19. Joindre/joindre de nouveau le SWA à Active Directory
  - Étape 20. Rejoindre SMA
- Correction des erreurs
  - Erreur d'analyse sur Element port_name
  - Erreur d'analyse sur l'élément ise_service
  - Le basculement ne fonctionne pas sur le nouveau SWA virtuel
- Autres informations utiles

Introduction

Ce document décrit le processus de restauration de la configuration d'un appareil Web sécurisé (SWA) vers un autre.

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 dispositif de gestion de la sécurité (SMA).
- Accès au portail de licences logicielles Cisco ou au fichier de licence SWA.
- Accès utilisateur privilégié Active Directory pour joindre le SWA au domaine et créer des enregistrements DNS.

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

Dans cet article, nous décrivons les étapes à suivre pour migrer du SWA source vers le SWA cible. Ce tableau répertorie les spécifications de chaque système.

	SWA source	SWA cible
Maquette	S396	S100v
Version	15.5.0-710	15.5.0-710

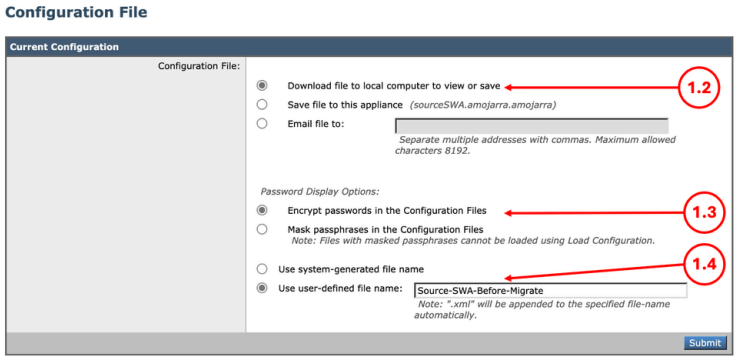
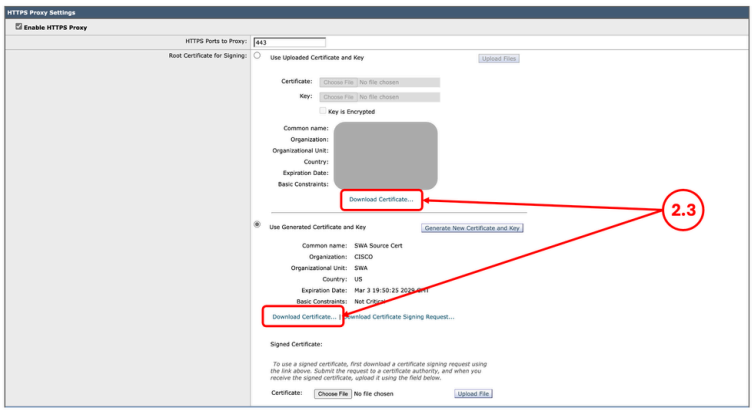
Licence	Licence Smart	Licence Smart
Active Directory	Joint	Joint
Intégré à Identity Services Engine (ISE)	Oui	Oui
Nombre de cartes réseau (NIC)	5	5
Décryptage HTTPS	Activé avec certificat auto-signé	Activé avec certificat auto-signé
Redirection transparente	Protocole WCCP (Web Cache Communication Protocol)	WCCP
Géré par SMA	Oui	Oui
Serveur de journal externe	Push SCP	Push SCP
Haute disponibilité	Activée	Activée

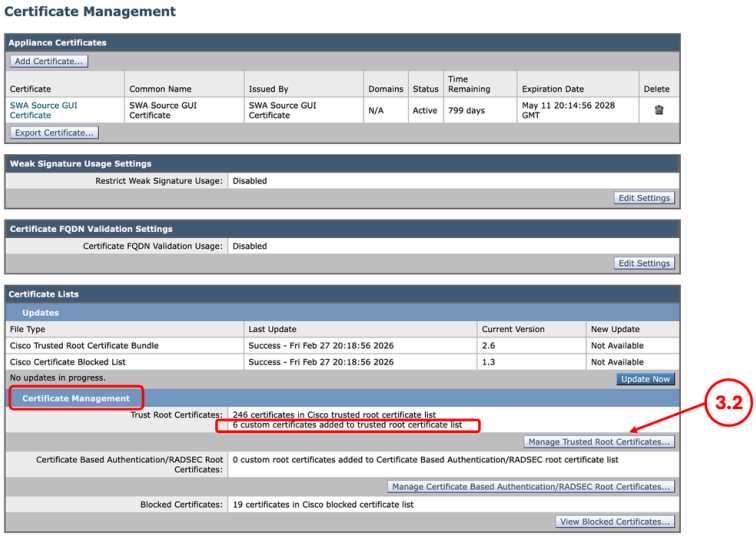
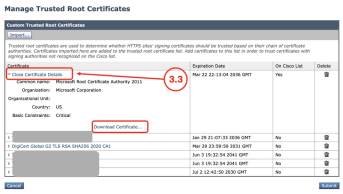
Remarque : Assurez-vous toujours que, lors de l'installation d'un nouveau SWA virtuel, toutes les interfaces réseau recommandées par Cisco sont présentes et configurées sur la machine virtuelle (VM). Les interfaces peuvent rester déconnectées, mais elles doivent être disponibles au sein de la VM.

Il existe deux scénarios possibles lors de la migration du SWA d'un périphérique à un autre :
[Scénario-1] Remplacement de l'approche SWA existante : Le SWA d'origine est mis hors service et l'adresse IP du SWA cible est la même que celle du SWA source.
[Scénario-2] Ajout d'un nouvel énoncé des besoins : Le SWA d'origine reste en service tant que le nouveau SWA est configuré.

Préparation et sauvegarde du SWA source

Suivez ces étapes pour collecter les fichiers et la configuration nécessaires à partir du SWA source :

Étape 1. Exportation du fichier de configuration	Étape 1.1. Dans l'interface utilisateur graphique, accédez à Administration système et sélectionnez Fichier de configuration. Étape 1.2. Assurez-vous que l'option Download file to local computer to view or save est sélectionnée. Étape 1.3. Sélectionnez Chiffrer les mots de passe dans les fichiers de configuration. Étape 1.4. (Facultatif) Choisissez un nom pour le fichier de configuration. Étape 1.5. Cliquez sur Submit.  Image - Exportation du fichier de configuration
Étape 2. Exportation du certificat de déchiffrement Remarque : Si le décodage HTTPS est désactivé, passez à l'étape 3.	Étape 2.1. Dans l'interface utilisateur graphique, accédez à Security Services et cliquez sur HTTPS Proxy. Étape 2.2. Cliquez sur Edit Settings. Étape 2.3. Téléchargez le certificat de déchiffrement HTTPS en cliquant sur Télécharger le certificat... lien.  Image - Certificat de décodage HTTPS

	Remarque : Dans cet exemple, les deux types de certificats de décodage HTTPS sont illustrés ; cependant, dans votre réseau, un seul type peut être déployé.
Étape 3. Exportation des certificats racines de confiance personnalisés Remarque : Si aucun certificat racine approuvé personnalisé n'est ajouté sur le SWA, passez à l'étape 4.	Étape 3.1. À partir de l'interface utilisateur graphique, accédez à Réseau et cliquez sur Gestion des certificats. Étape 3.2. Dans la section Certificate Management, cliquez sur Manage Trusted Root Certificates.  Image - Gérer les certificats racine approuvés Étape 3.3. Développez chaque certificat racine de confiance personnalisé en cliquant sur son nom, puis sur Télécharger le certificat...  Image - Télécharger les certificats racines de confiance
Étape 4. Exportation du certificat de l'interface graphique Remarque : Si vous utilisez un certificat de GUI intégré, passez à l'étape 5.	Étape 4.1. Dans l'interface graphique utilisateur, accédez à Network et cliquez sur Certificate Management. Étape 4.2. Dans la section Appliance Certificates, cliquez sur Export Certificate.

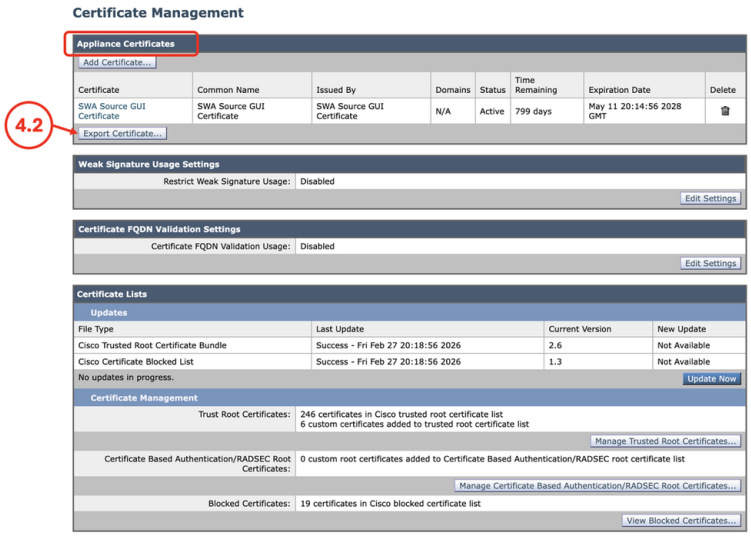
<table>
<tr>
<td></td>
<td>

Image - Exporter le certificat GUI</td>
</tr>
<tr>
<td>Étape 5. Exportation des certificats ISE

Remarque : S'il n'y a pas d'intégration SWA, ISE, passez à l'étape 6.</td>
<td>Étape 5.1. Dans l'interface utilisateur graphique, accédez à Réseau et cliquez sur Identity Services Engine.

Étape 5.2. Cliquez sur Edit Settings.

Étape 5.3. Téléchargez tous les certificats disponibles.

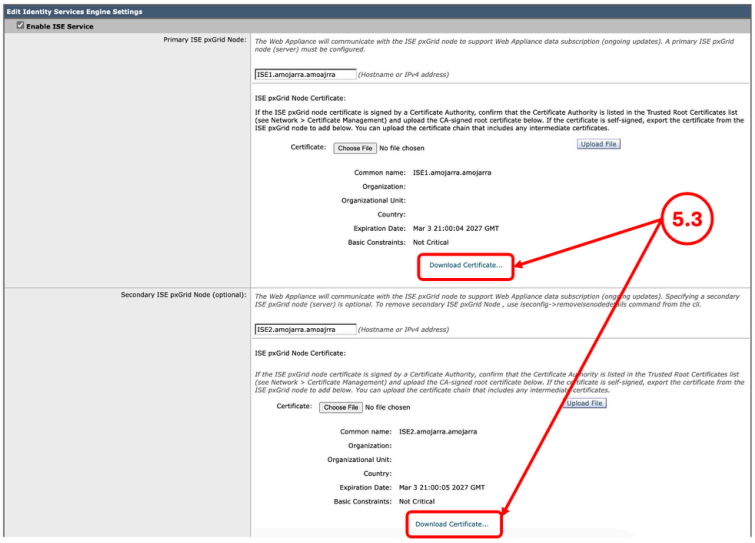
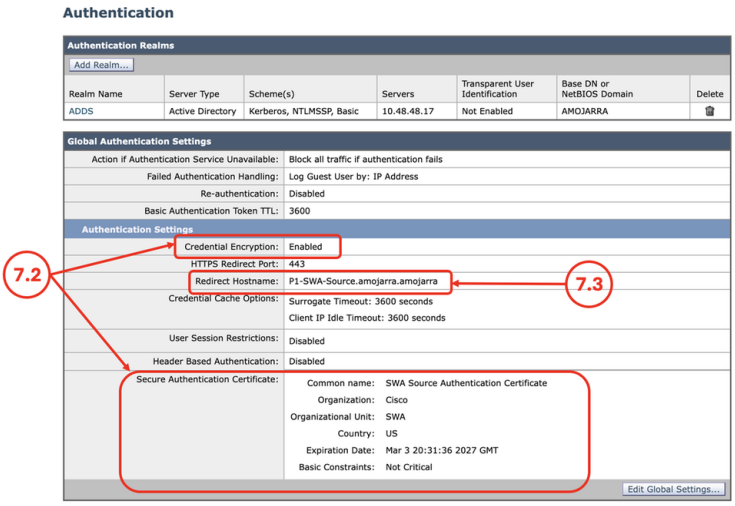
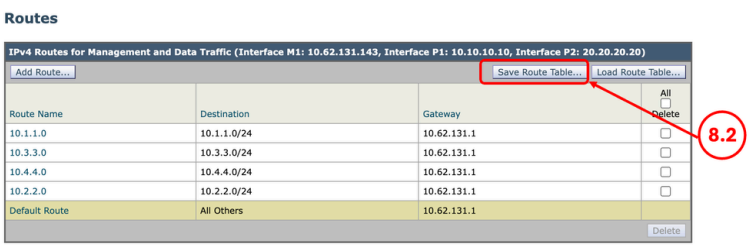


Image - Télécharger les certificats ISE</td>
</tr>
<tr>
<td>Étape 6. Licences / Fonctionnalités</td>
<td>Étape 6.1. Dans l'interface utilisateur graphique, accédez à Administration système et cliquez sur Licences ou Fonctionnalités, selon le type de licence que vous utilisez.

Étape 6.2. Faites une capture d'écran de vos</td>
</tr>
</table>

	licences/fonctionnalités.
Étape 7. Certificat de redirection d'authentification	Étape 7.1. À partir de l'interface utilisateur graphique, accédez à Network et cliquez sur Authentication. Étape 7.2. Si le chiffrement des informations d'identification est activé, assurez-vous que vous disposez du certificat et de la clé. Étape 7.3. Effectuez une capture d'écran de la configuration actuelle.  Image - Certificat d'authentification Remarque : Vous ne pouvez pas télécharger le certificat d'authentification depuis l'interface utilisateur graphique.
Étape 8. Exportation des routes statiques Remarque : Si vous prévoyez d'utiliser la même configuration réseau et la même adresse IP pour le SWA cible, passez à l'étape 10.	Étape 8.1. Dans l'interface utilisateur graphique, accédez à Network et cliquez sur Routes. Étape 8.2. Pour chaque table de routage, cliquez sur Save Route Table.  Image - Exportation de la table de routage

Étape 9. Paramètres DNS Remarque : Si vous prévoyez d'utiliser la même configuration réseau et la même adresse IP pour le SWA cible, passez à l'étape 10.	Étape 9.1. À partir de l'interface utilisateur graphique, accédez à Network et cliquez sur DNS. Étape 9.2. Capture d'écran de la configuration DNS

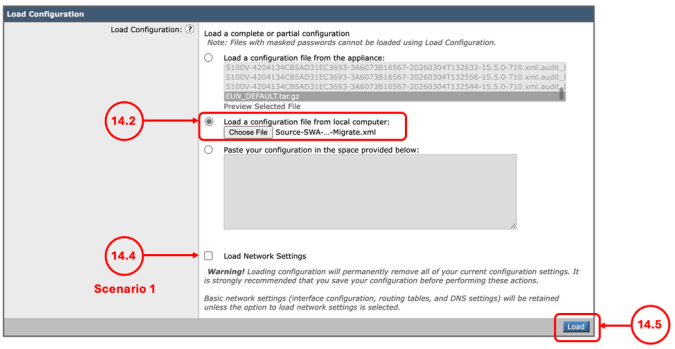
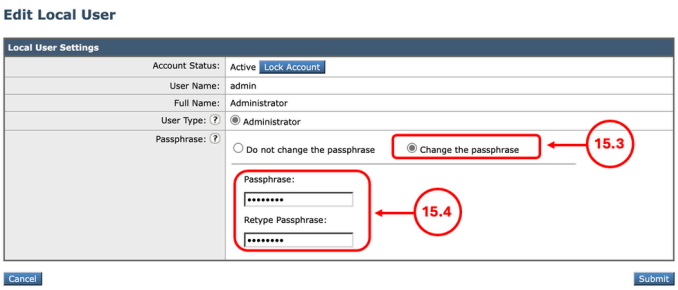
Préparation du SWA cible

Étape 10. Installation de Virtual SWA Remarque : Si le SWA cible est un appareil physique, passez à l'étape 11.	Étape 10.1. Pour plus d'informations sur l'installation du SWA virtuel : • Installer l'appliance Web sécurisée sur VMware ESXi • Installer l'appliance Web sécurisée sur Microsoft Hyper-V Étape 10.2. Assurez-vous que le nouveau SWA dispose de l'accès réseau recommandé : • Configurer le pare-feu pour l'appliance Web sécurisée
Étape 11. Configuration initiale de SWA	Étape 11.1 : configuration de l'adresse IP Étape 11.2 : configuration de la passerelle par défaut Étape 11.3 : configuration du serveur DNS Étape 11.4. Licence de l'appliance Étape 11.5. Activez les fonctionnalités. Étape 11.6. Exécutez l'assistant de configuration du système. Vous trouverez les étapes détaillées dans cet article : Secure Web Appliance Initial Setup
Étape 12. Désactivation du fichier de configuration Remarque : Si vous n'intégrez pas	Étape 12.1. Consultez la section Correction des erreurs dans cet article pour supprimer la configuration du certificat ISE du fichier de sauvegarde XML.

ISE avec le SWA, vous pouvez passer à l'étape 13.	

Importation du fichier de configuration dans le SWA cible

Étape 13. Importation de certificats racine de confiance personnalisés Remarque : Si vous n'utilisez pas de certificat racine de confiance personnalisé, passez à l'étape 14.	Étape 13.1. Dans l'interface graphique utilisateur, accédez à Network et cliquez sur Certificate Management. Étape 13.2. Dans la section Certificate Management, cliquez sur Manage Trusted Root Certificates. Étape 13.3. Cliquez sur Import. Étape 13.4. Téléchargez les certificats précédemment téléchargés à l'étape 3. Mise en garde : Lorsque les certificats racine et intermédiaire sont disponibles, commencez par télécharger le certificat d'autorité de certification racine. Après avoir envoyé et validé les modifications, continuez à importer le certificat intermédiaire.
Étape 14. Importation du fichier de configuration	Étape 14.1. Dans l'interface utilisateur graphique, accédez à Administration système et sélectionnez Fichier de configuration. Étape 14.2. Dans la section Load Configuration, sélectionnez Load a configuration file from local computer. Étape 14.3. Cliquez sur Choose File et sélectionnez le fichier de configuration XML. Étape 14.4. Si la migration correspond au scénario 1 et que l'adresse IP précédente doit être utilisée dans le nouveau SWA, cochez la case Load Network Settings, sinon ne sélectionnez pas cette option. Étape 14.5. Cliquez sur Load.

	Étape 14.6. Cliquez sur Continue dans la fenêtre contextuelle Confirm Load Configuration.  Image - Importation de la configuration
Étape 15. Modification du mot de passe admin Remarque : si vous disposez du mot de passe source SWA admin, passez à l'étape 16.	15.1. Dans l'interface utilisateur graphique, accédez à Administration système et sélectionnez Utilisateurs. 15.2. cliquez sur le nom d'utilisateur admin. 15.3. Sélectionnez Modifier la phrase de passe. 15.4. Entrez le mot de passe. 15.5. cliquez sur Envoyer.  Image - Modification du mot de passe administrateur
Étape 16. Valider	Étape 16.1. Vous pouvez maintenant valider les modifications.
Étape 17. Importation des routes Remarque : si vous chargez les paramètres réseau lors de l'importation de la configuration, passez à l'étape 19.	Étape 17.1. Dans l'interface graphique utilisateur, accédez à Network et cliquez sur Routes. Étape 17.2. Pour chaque table de routage, cliquez sur Load Route Table.

	Étape 17.3. Choisissez le fichier que vous avez exporté à l'étape 8. Étape 17.4. Cliquez sur Submit. Étape 17.5. Validez les modifications.
Étape 18. Configuration des paramètres DNS Remarque : Si vous Load Network Settings lors de l'importation de la configuration, passez à l'étape 19.	Étape 18.1. Dans l'interface graphique utilisateur, accédez à Network et cliquez sur DNS. Étape 18.2. Cliquez sur Edit Settings. Étape 18.3. Utiliser la capture d'écran de l'étape 9 Étape 18.4. Cliquez sur Submit. Étape 18.5. Validez les modifications.
Étape 19. Joindre/joindre de nouveau le SWA à Active Directory	Étape 19.1. Dans l'interface graphique, accédez à Network et cliquez sur Authentication. Étape 19.2. cliquez sur le nom du domaine d'authentification. Conseil : Si une nouvelle adresse IP et un nouveau nom d'hôte sont affectés au SWA, assurez-vous que les enregistrements DNS nécessaires sont créés dans le service DNS Active Directory. Étape 19.3. Cliquez sur Join Domain et entrez les informations d'identification :

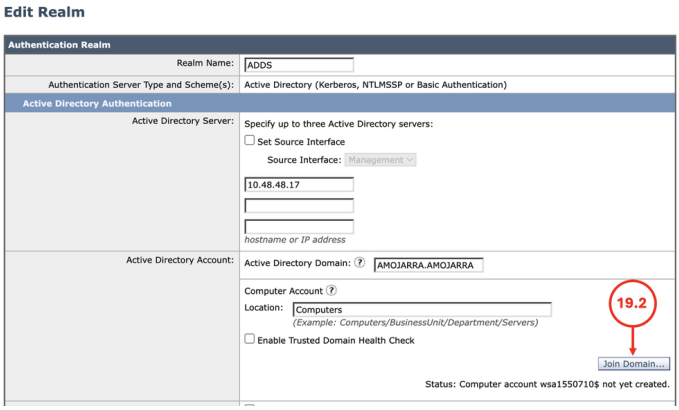


Image - Joindre au domaine Active Directory

Étape 19.4. Cliquez sur Submit.

Étape 19.5. Assurez-vous que le nom d'hôte de redirection est correct.

Étape 19.6. Si le chiffrement des informations d'identification est activé, vérifiez que le certificat d'authentification sécurisée est correct.

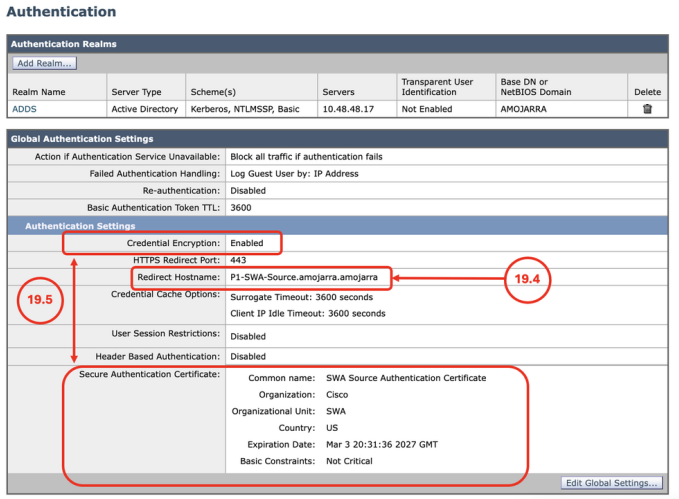


Image - Paramètres d'authentification

Étape 19.7. Validez les modifications.

Étape 20. Rejoindre SMA

Remarque : Si le SWA n'est pas géré par SMA, ignorez cette étape.

Remarque : Si vous n'avez pas remplacé le SWA existant (scénario 2) et que le SWA migré possède une nouvelle adresse IP, ajoutez le SWA en tant que nouveau périphérique au SMA et ignorez l'étape 20.

Étape 20.1. Connexion à l'interface de ligne de commande du SMA

Étape 20.2. exécutez logconfig.

Étape 20.3. Entrez HOSTKEYCONFIG.

Étape 20.4. Tapez DELETE et appuyez sur Entrée.

Étape 20.5. Tapez le numéro associé au SWA qui a été récemment migré et appuyez sur Entrée jusqu'à ce que l'assistant soit terminé.

Étape 20.6. Tapez commit et appuyez sur Entrée pour enregistrer les modifications.

Étape 20.7. À partir de l'interface utilisateur graphique de SMA, accédez à Appliance de gestion. Sélectionnez Centralized Services et cliquez sur Security Appliances.

Étape 20.8. cliquez sur le nom du SWA qui a été migré récemment.

Conseil : Vous pouvez voir que la colonne Connexion établie est définie sur Non.

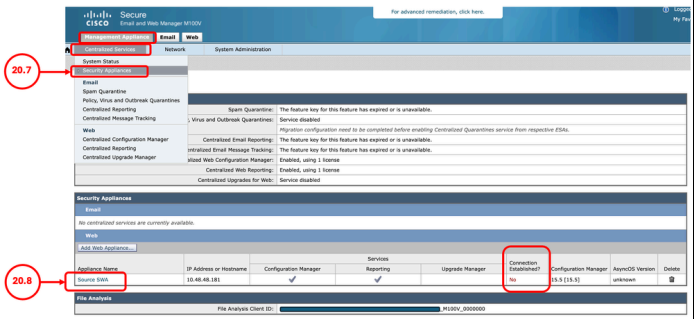


Image - État du dispositif de sécurité SMA

Étape 20.9. cliquez sur Établir la connexion.

Étape 20.10. Entrez le nom d'utilisateur et la phrase de passe, puis cliquez sur Établir la connexion.

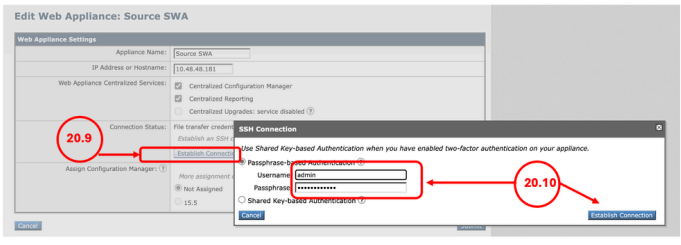


Image - Établir la connexion au SWA

Étape 20.11. Attribuez le gestionnaire de configuration.

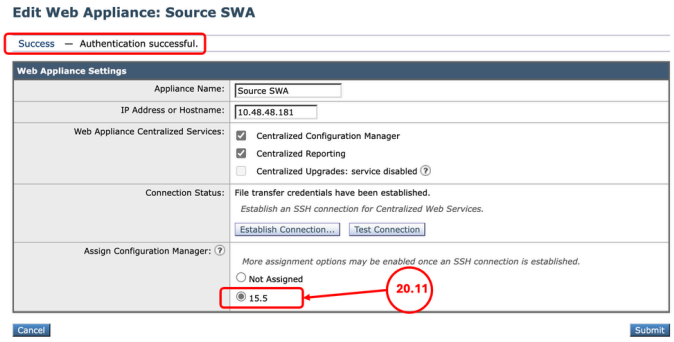


Image - Attribuer le gestionnaire de configuration

Étape 20.12. Soumettre et valider les modifications

Étape 20.13. (Facultatif) vous pouvez tester en publiant la configuration sur le SWA.

Conseil : Le SMA conserve toutes les données de reporting et de suivi de l'ancien SWA.

Correction des erreurs

Erreur d'analyse sur Element port_name

Le nom du port réseau doit être ['Management', 'P1', 'P2', 'T1', 'T2'] :

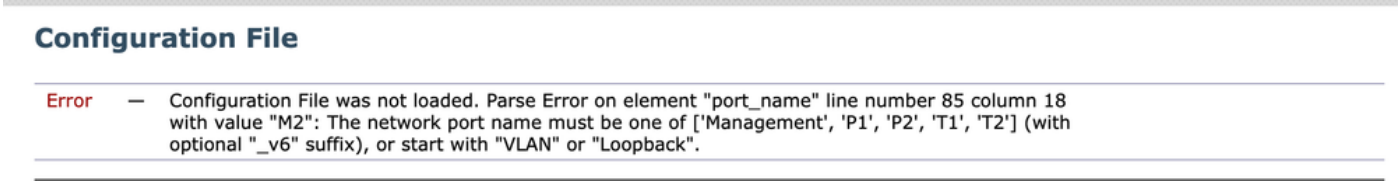


Image - Erreur de nom d'interface réseau

```
Error    —    Configuration File was not loaded. Parse Error on element "port_name" line number 85 colu
```

Cette erreur se produit lorsque vous migrez d'un SWA physique vers un Virtual. le Virtual SWA ne comporte que 5 cartes réseau et l'interface M2 n'est pas valide. Pour corriger l'erreur, modifiez le fichier de configuration XML dans un éditeur de texte et supprimez les lignes suivantes :

```
<port_interface>
      <port_name>M2</port_name>
      <direct>
        <jack>M2</jack>
      </direct>
</port_interface>
```

```
<ethernet>
      <ethernet_interface>M2</ethernet_interface>
      <media>autoselect</media>
      <media_opt></media_opt>
      <macaddr>aa:bb:cc:00:00:00</macaddr>
</ethernet>
```

Erreur d'analyse sur l'élément ise_service

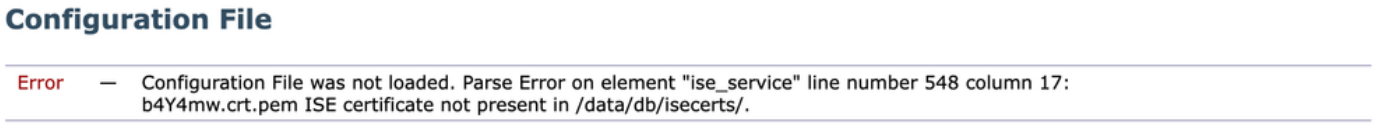


Image - Erreur de certificat ISE

```
Error - Configuration File was not loaded. Parse Error on element "ise_service" line number 548 column
```

Étant donné que les certificats ISE ne sont pas inclus dans l'exportation de la configuration SWA et qu'ils sont téléchargés directement sur le périphérique, vous devez supprimer la configuration des certificats du fichier XML et, après une importation réussie, configurer ISE manuellement. pour résoudre ce problème, modifiez le fichier de configuration XML dans l'éditeur de texte et recherchez le nom du certificat dans l'erreur (dans cet exemple, recherchez AA11AA) et supprimez-le du fichier de configuration :

```
Before:
      <ise_service_pxgrid_certs>
         <pxgrid_cert>AA11AA</pxgrid_cert>
         <pxgrid_cert>BB22BB</pxgrid_cert>
      </ise_service_pxgrid_certs>
```

```
After:
      <ise_service_pxgrid_certs></ise_service_pxgrid_certs>
```

Outre le nom du certificat, vous devez également supprimer le nom du certificat client de l'appliance Web.

Dans cet exemple, le certificat client de l'appliance Web est un certificat auto-signé :

```
Before:
<ise_service_cert_generated>1</ise_service_cert_generated>
<ise_service_generated_name>xAcK6T</ise_service_generated_name>

After:
<ise_service_cert_generated>0</ise_service_cert_generated>
<ise_service_generated_name></ise_service_generated_name>
```

Le basculement ne fonctionne pas sur le nouveau SWA virtuel

Si la haute disponibilité (basculement) ne fonctionne pas sur le SWA virtuel cible, assurez-vous que l'hyperviseur est correctement configuré. Pour plus d'informations, consultez : Assurez-vous que le groupe WSA HA virtuel fonctionne correctement dans un environnement VMware

Autres informations utiles

- 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
- Garantir le bon fonctionnement du groupe WSA HA virtuel dans un environnement VMware

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.