Rétablir la version précédente de l'appliance Web sécurisée

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Avant de commencer
- Préparation et sauvegarde du SWA
  - 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
- Rétablir le SWA
  - Étape 10. Rétablissement du SWA
- SWA de configuration inversée
  - Étape 11. Licence du SWA
  - Étape 12. Exécutez l'Assistant de configuration du système
  - Étape 13. Importation de certificats racine de confiance personnalisés
  - Étape 14. Importation du fichier de configuration
  - Étape 15. Importation des routes
  - Étape 16. Configuration des paramètres DNS
  - Étape 17. Joindre/joindre de nouveau le SWA à Active Directory
- Informations connexes

Introduction

Ce document décrit les étapes à suivre pour rétablir la version précédente de l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

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

- Accès administratif au SWA
- Accès au portail Cisco Software Licensing Portal 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.

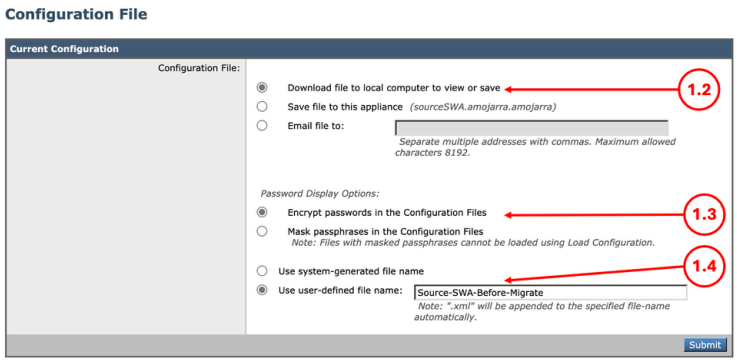
Avant de commencer

La restauration de l'appliance est extrêmement destructrice.
Il s'agit des données qui sont détruites au cours du processus et qui doivent être sauvegardées :
- Fichier de configuration système actuel.
- Tous les fichiers journaux (Pour plus d'informations, consultez : Accéder aux journaux de l'appliance Web sécurisée)
- Toutes les données de rapport (y compris les rapports programmés et archivés enregistrés)
- Toutes les pages de notification utilisateur final personnalisées.

Avertissement : Avant de revenir à une version antérieure, vérifiez que vous disposez du fichier de configuration chiffré correspondant à cette version spécifique. Il est possible que le fichier de configuration actuel ne soit pas compatible avec les versions logicielles plus anciennes.

Préparation et sauvegarde du SWA

Procédez comme suit pour collecter les fichiers et la configuration nécessaires à partir du SWA avant de revenir à la version précédente :

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. Choisissez Encrypt passwords 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.

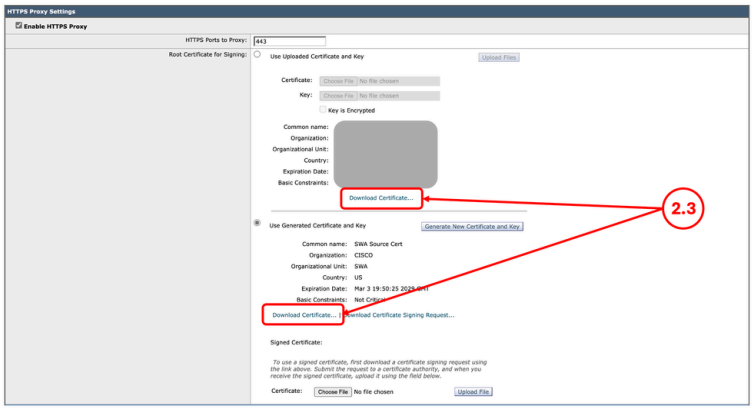


Image - Certificat de décodage HTTPS

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.

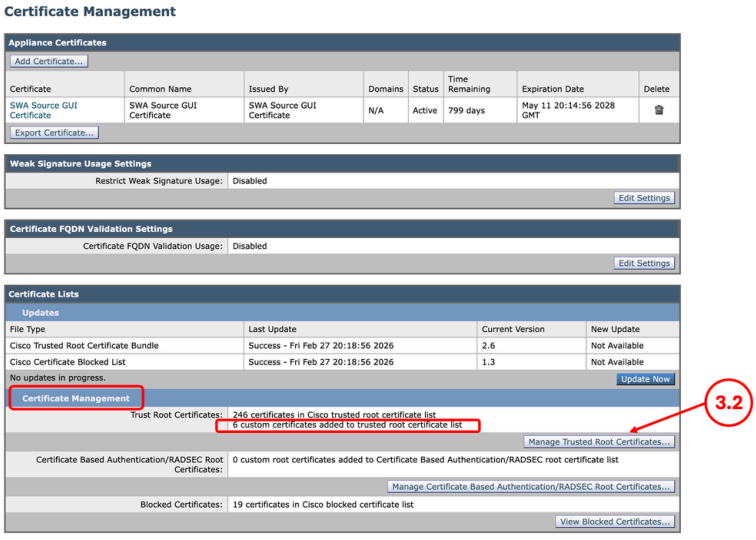


Image - Gérer les certificats racine approuvés

Étape 3.3. Développez chaque certificat racine de confiance personnalisé en cliquant sur son nom, puis sur Télécharger le certificat...

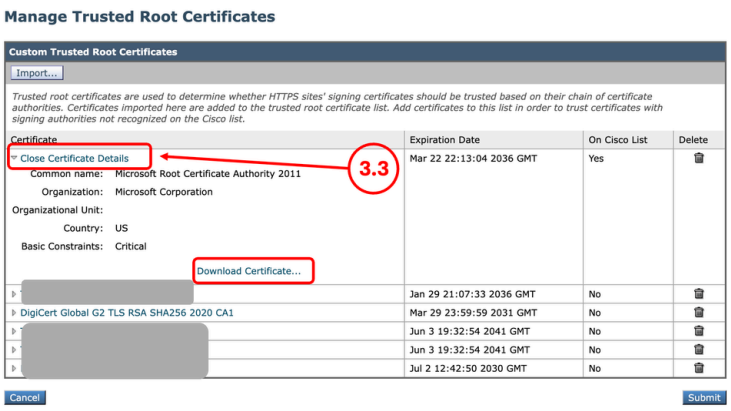


Image - Télécharger les certificats racines de confiance

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.

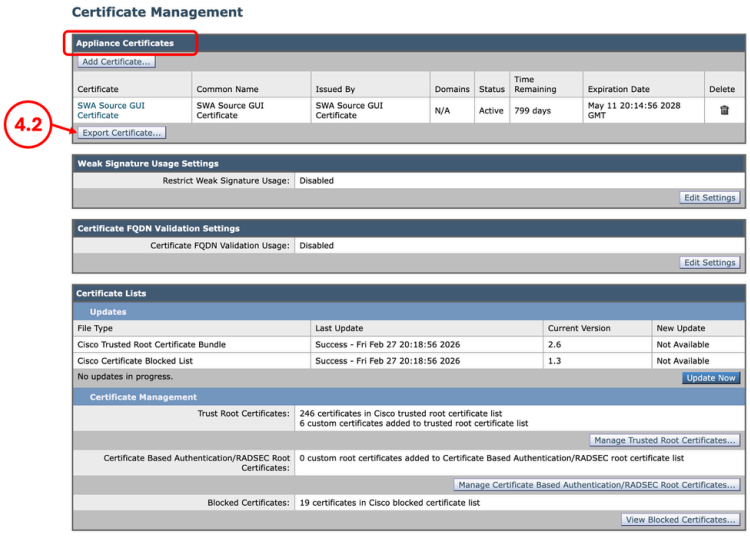


Image - Exporter le certificat GUI

Étape 5. Exportation des certificats ISE

Remarque : S'il n'y a pas d'intégration SWA, ISE, passez à l'étape 6.

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.

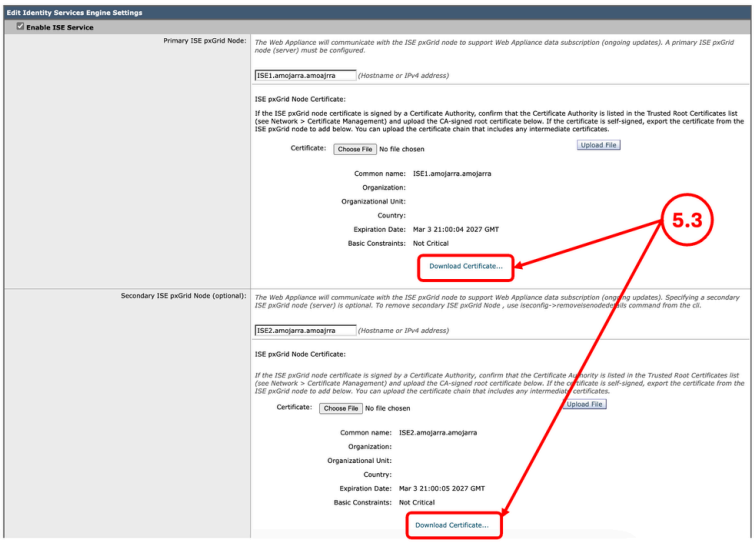
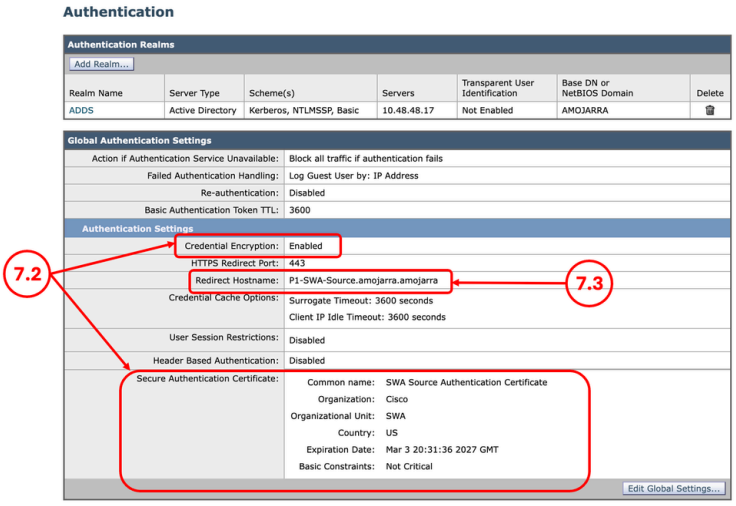
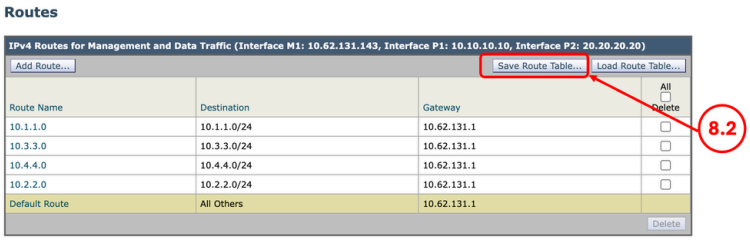
	 Image - Télécharger les certificats ISE
Étape 6. Licences / Fonctionnalités	Étape 6.1. Dans l'interface graphique utilisateur, accédez à Administration système et cliquez sur Licences ou Fonctionnalités selon le type de licence que vous utilisez. Étape 6.2. Faites une capture d'écran de vos licences/fonctionnalités.
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

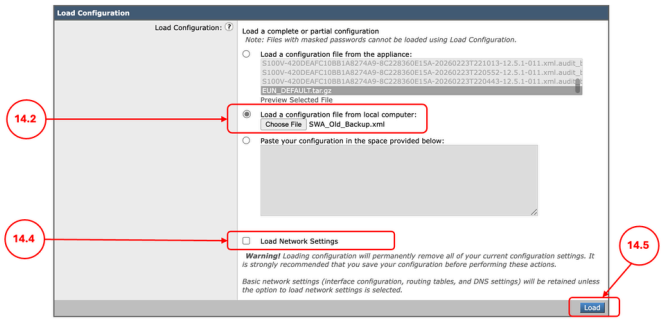
Rétablir le SWA

Étape 10. Rétablissement du SWA	Étape 10.1. Connexion à l'interface de ligne de commande Étape 10.2. Tapez revert et appuyez sur Entrée. Étape 10.3. Tapez Y et appuyez sur Entrée pour « Voulez-vous continuer ? [N]> " Étape 10.4. Tapez Y et appuyez sur Entrée pour « Voulez-vous vraiment continuer ? [N]>" Étape 10.5. Choisissez le numéro associé à la version que vous souhaitez rétablir dans la liste et appuyez sur Entrée.

	SWA_CLI> revert This command will revert the appliance to a previous version of AsyncOS. Warning: Reverting the appliance is extremely destructive. The following data will be destroyed in the process and should be backed up: - current system configuration file - all log files - all reporting data (including saved scheduled and archived reports) - any custom end user notification pages This command will try to preserve the current network settings. Reverting the device will cause a reboot to take place. After rebooting, the appliance reinitializes itself and reboots again to the desired version, with the earlier system configuration. Do you want to continue? [N]> Y Are you sure you want to continue? [N]> Y Available versions ========== 1. 12.5.1-011 Please select an AsyncOS version: 1 You have selected "12.5.1-011". The system will now reboot to perform the revert operation.

SWA de configuration inversée

Étape 11. Licence du SWA	Étape 11.1. Pour plus d'informations, consultez la page : Configuration initiale de Secure Web Appliance.
Étape 12. Exécutez l'Assistant de configuration du système	Étape 12.1. Pour plus d'informations, consultez la page : Configuration initiale de Secure Web Appliance.
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 ⚠ Mise en garde : Assurez-vous que vous importez le fichier de configuration correspondant à votre version actuelle et non le fichier de configuration que vous avez exporté à l'étape 1.	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 associé à la version actuelle. Étape 14.4. (Facultatif) Si le rétablissement a supprimé l'adresse IP et la configuration réseau , cochez la case Charger les paramètres réseau, 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 - Chargement de l'ancien fichier de configuration Étape 14.7. Validez les modifications.
Étape 15. Importation des routes	Étape 15.1. À partir de l'interface utilisateur graphique, accédez à Network et cliquez sur Routes.

Remarque : si vous chargez les paramètres réseau lors de l'importation de la configuration, passez à l'étape 17.	Étape 15.2. Pour chaque table de routage, cliquez sur Load Route Table. Étape 15.3. Choisissez le fichier que vous avez exporté à l'étape 8. Étape 15.4. Cliquez sur Submit. Étape 15.5. Validez les modifications.
Étape 16. Configuration des paramètres DNS Remarque : Si vous Load Network Settings lors de l'importation de la configuration, passez à l'étape 17.	Étape 16.1. Dans l'interface graphique utilisateur, accédez à Network et cliquez sur DNS. Étape 16.2. Cliquez sur Edit Settings. Étape 16.3. Utiliser la capture d'écran de l'étape 9 Étape 16.4. Cliquez sur Submit. Étape 16.5. Validez les modifications.
Étape 17. Joindre/joindre de nouveau le SWA à Active Directory	Étape 17.1. À partir de l'interface utilisateur graphique, accédez à Network et cliquez sur Authentication. Étape 17.2. 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 17.3. Cliquez sur Join Domain et entrez les informations d'identification :

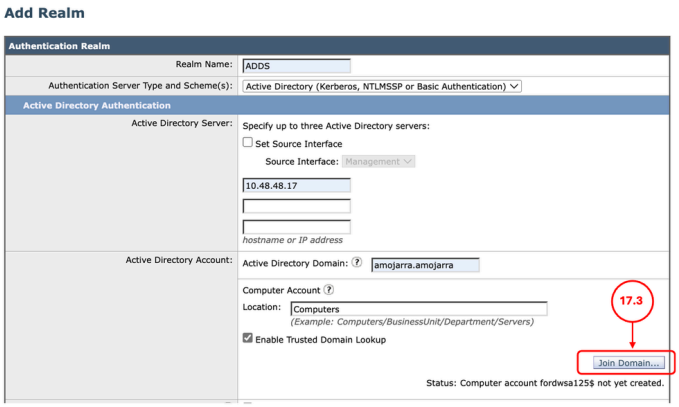


Image - Joindre à Active Directory

Étape 17.4. Cliquez sur Submit.

Étape 17.5. Si le chiffrement des informations d'identification est activé, importez le certificat d'authentification sécurisé.

Étape 17.6. Assurez-vous que le nom d'hôte de redirection est correct.

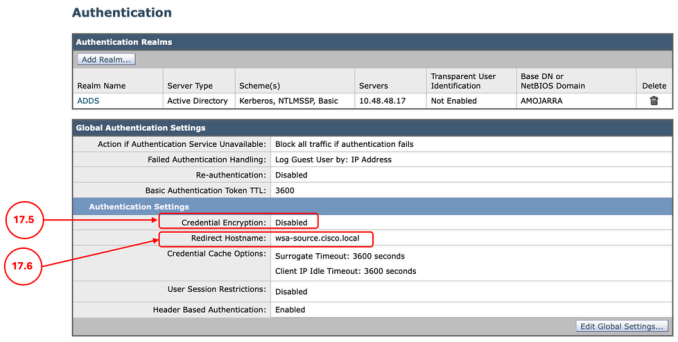


Image - Paramètres d'authentification

Étape 17.7. Validez les modifications.

Informations connexes

- Guide de l'utilisateur d'AsyncOS 15.2 pour Cisco Secure Web Appliance
- Configuration initiale de Secure Web Appliance
- Utilisation des meilleures pratiques de sécurisation des appliances Web
- Accéder aux journaux 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.