セキュアWebアプライアンスを以前のバージョンに戻す

内容

はじめに

前提条件

- 要 件
- 使用するコンポーネント

はじめる前に

SWAの準備とバックアップ

- ステップ 1：コンフィギュレーションファイルのエクスポート
- ステップ 2復号化証明書のエクスポート
- ステップ 3カスタム信頼ルート証明書のエクスポート
- ステップ 4GUI証明書のエクスポート
- ステップ 5ISE証明書のエクスポート
- ステップ 6ライセンス/機能
- ステップ 7認証リダイレクト証明書
- ステップ 8スタティックルートのエクスポート
- ステップ 9DNS設定

SWAを元に戻す

- ステップ 10SWAの復帰

設定が元に戻されたSWA

- ステップ 11SWAのライセンス
- ステップ 12システムセットアップウィザードを実行
- ステップ 13カスタムの信頼されたルート証明書のインポート
- 手順 14：設定ファイルのインポート
- 手順 15：ルートのインポート
- ステップ 16：DNS設定の構成
- ステップ 17：SWAのActive Directoryへの参加/再参加

関連情報

はじめに

このドキュメントでは、Secure Web Appliance(SWA)を以前のバージョンに戻す手順について説明します。

前提条件

要 件

次の項目に関する知識が推奨されます。

- SWAのグラフィックユーザインターフェイス(GUI)へのアクセス

- SWAへの管理アクセス
- Cisco Software Licensing PortalまたはSWAライセンスファイルへのアクセス
- SWAをドメインに参加させ、DNSレコードを作成するためのActive Directory特権ユーザアクセス

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

はじめる前に

アプライアンスの復帰は非常に破壊的です。
これは、プロセスで破棄され、バックアップする必要があるデータです。
– 現在のシステム構成ファイル。
– すべてのログファイル(詳細については、「セキュアWebアプライアンスログへのアクセス」を参照)
– すべてのレポートデータ（保存済みのスケジュール済みレポートおよびアーカイブレポートを含む）
– カスタムエンドユーザ通知ページ。

警告：以前のバージョンに戻す前に、その特定のバージョンに対応する暗号化された設定ファイルがあることを確認してください。現在のコンフィギュレーションファイルが古いソフトウェアバージョンと互換性がない可能性があります。

SWAの準備とバックアップ

復帰する前に、次の手順を使用してSWAから必要なファイルと設定を収集します。

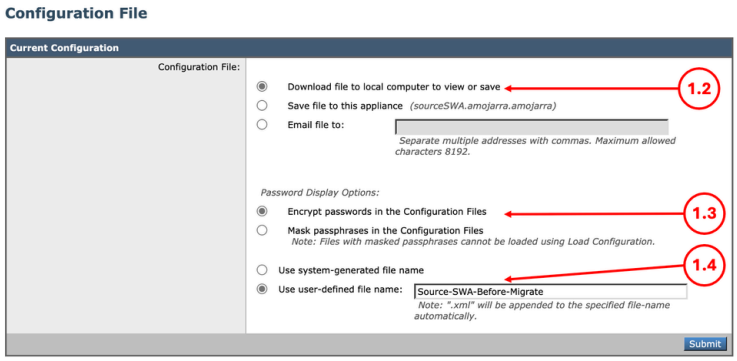
<table>
<tr>
<td>ステップ 1：コンフィギュレーションファイルのエクスポート</td>
<td>ステップ 1.1：GUIで、System Administrationに移動し、Configuration Fileを選択します。

ステップ 1.2：Download file to local computer to view or saveが選択されていることを確認します。

ステップ 1.3：Encrypt passwords in the Configuration Filesを選択します

ステップ1.4:（オプション）コンフィギュレーションファイルの名前を選択します。

ステップ 1.5：[Submit] をクリックします。

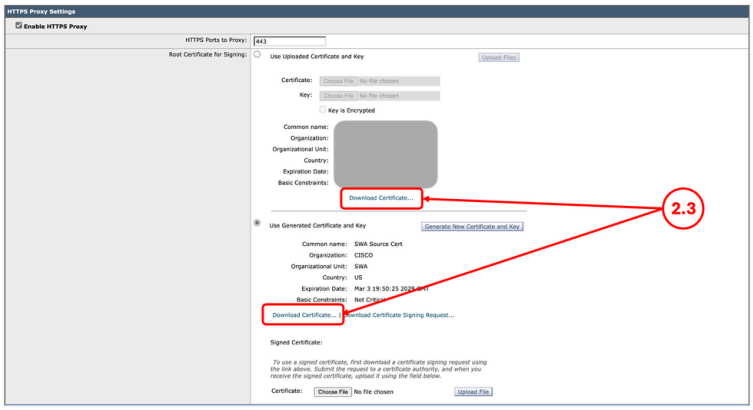
 

イメージ：コンフィギュレーションファイルのエクスポート</td>
</tr>
<tr>
<td>ステップ 2復号化証明書のエクスポート

注:HTTPS復号化が無効になっている場合は、ステップ3に進んでください。</td>
<td>ステップ 2.1：GUIで、Security Servicesに移動し、HTTPS Proxyをクリックします。

ステップ 2.2：[Edit Settings] をクリックします。

ステップ 2.3：Download Certificate...リンクをクリックして、HTTPS Decryption Certificateをダウンロードします。</td>
</tr>
</table>



イメージ：HTTPS暗号解除証明書

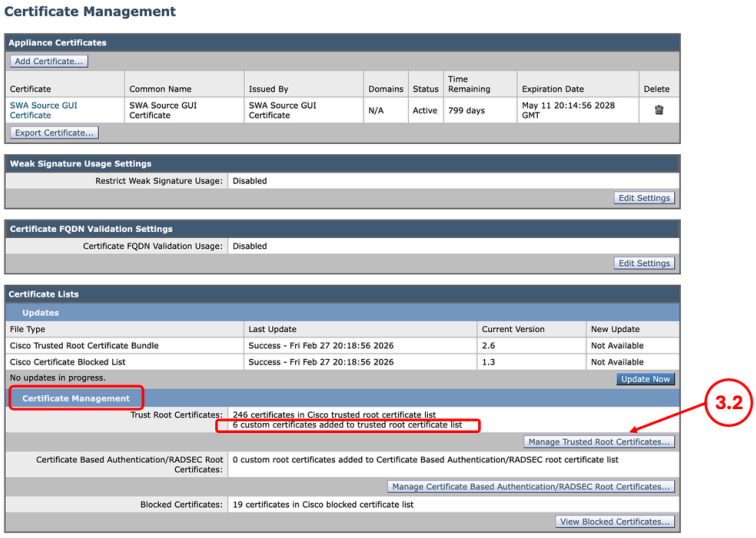
注：この例では、両方のタイプのHTTPS復号化証明書を示していますが、ネットワークには1つのタイプしか導入できません。

ステップ 3カスタム信頼ルート証明書のエクスポート

注:SWAに追加されたカスタムの信頼されたルート証明書がない場合は、ステップ4に進んでください。

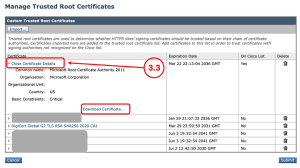
ステップ 3.1： GUIで、Networkに移動し、Certificate Managementをクリックします。

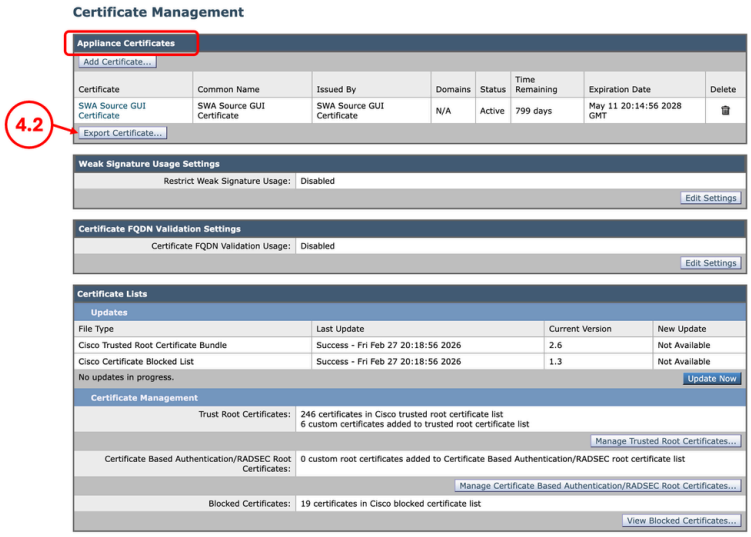
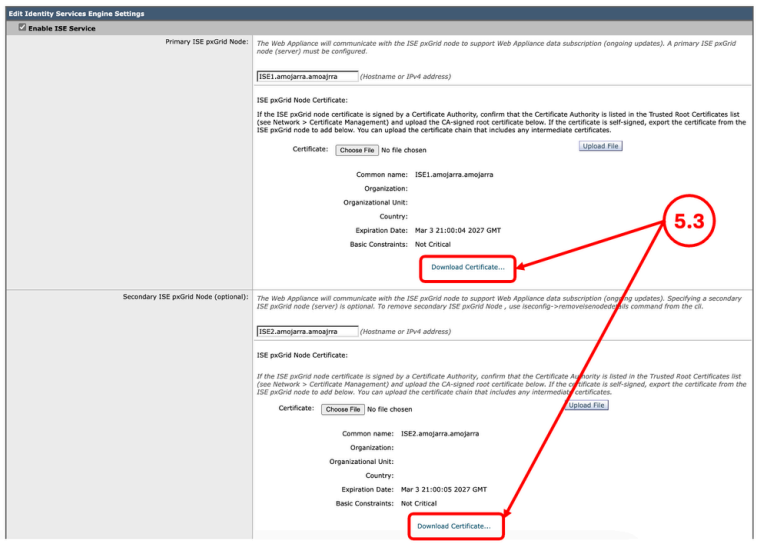
ステップ 3.2：Certificate Managementセクションで、Manage Trusted Root Certificatesをクリックします。

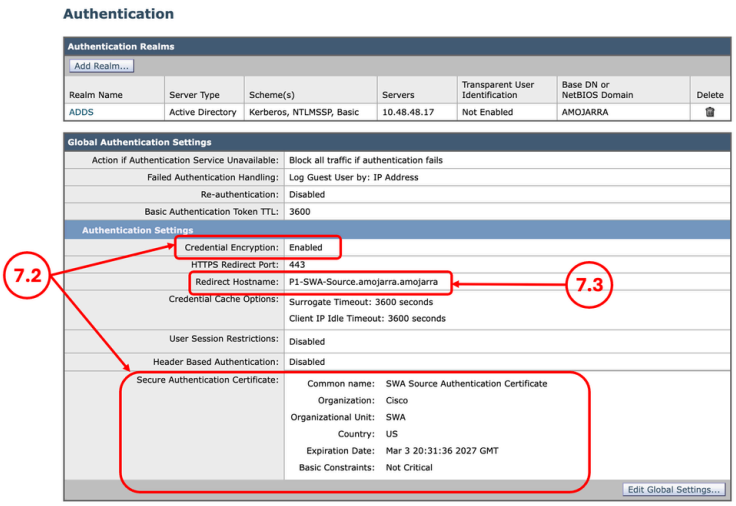


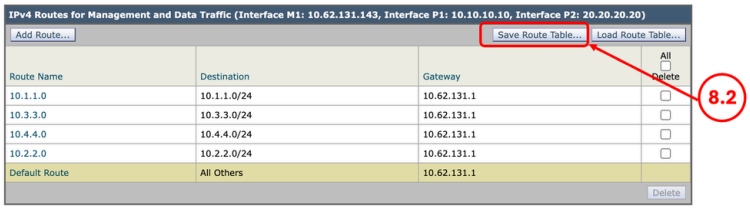
イメージ – 信頼されたルート証明書の管理

ステップ 3.3：名前をクリックして、各カスタム信頼できるルート証明書を展開し、Download Certificate...をクリックします。



	イメージ：信頼できるルート証明書のダウンロード
ステップ 4GUI証明書のエクスポート 注：組み込みのGUI証明書を使用している場合は、ステップ5に進んでください。	ステップ 4.1： GUIで、Networkに移動し、Certificate Managementをクリックします。 ステップ 4.2：Appliance Certificatesセクションで、Export Certificateをクリックします。  イメージ：GUI証明書のエクスポート
ステップ 5ISE証明書のエクスポート 注:SWA、ISE統合がない場合は、ステップ6に進んでください。	ステップ 5.1： GUIで、Networkに移動し、Identity Services Engineをクリックします。 ステップ 5.2：[Edit Settings] をクリックします。 ステップ 5.3：使用可能な証明書をすべてダウンロードします。  イメージ：ISE証明書のダウンロード

ステップ 6ライセンス/機能	ステップ 6.1： GUIから、System Administrationに移動し、使用しているライセンスのタイプに応じてLicensesまたはFeaturesをクリックします。 ステップ 6.2：ライセンス/機能のスクリーンショットを撮ります。
ステップ 7認証リダイレクト証明書	ステップ 7.1： GUIで、Networkに移動し、Authenticationをクリックします。 ステップ 7.2：Credential Encryptionが有効な場合、証明書とキーがあることを確認します。 ステップ 7.3：現在の設定のスクリーンショットを取得します。  イメージ – 認証証明書 注：認証証明書はGUIからはダウンロードできません。
ステップ 8スタティックルートのエクスポート 注：ターゲットSWAに同じネットワーク設定とIPアドレスを使用する場合は、ステップ10に進んでください。	ステップ 8.1： GUIで、Networkに移動し、Routesをクリックします。 ステップ 8.2：各ルーティングテーブルで、Save Route Tableをクリックします。

	Routes  図 – ルーティングテーブルのエクスポート
ステップ 9DNS設定 注：ターゲットSWAに同じネットワーク設定とIPアドレスを使用する場合は、ステップ10に進んでください。	ステップ 9.1： GUIで、Networkに移動し、DNSをクリックします。 ステップ 9.2：DNS設定のスクリーンショットを取得します。

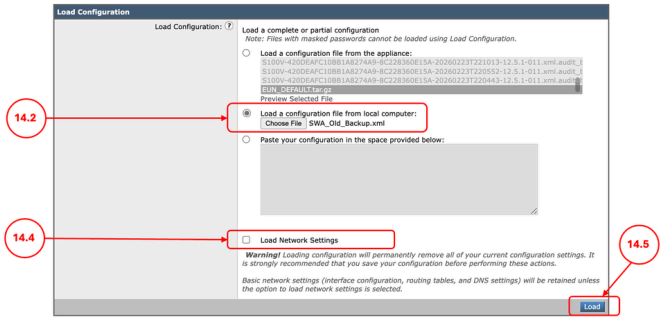
SWAを元に戻す

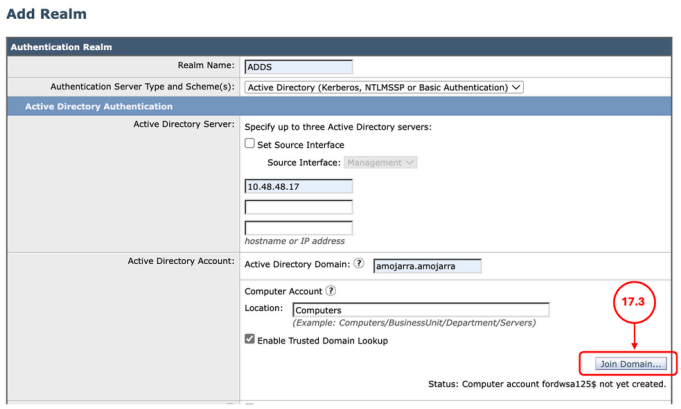
ステップ 10SWAの復帰	ステップ 10.1：CLIに接続します。 ステップ 10.2： revertと入力してEnterキーを押す。 ステップ 10.3： Yと入力してEnterキーを押し、「Do you want to continue?[N]>" ステップ 10.4： Yと入力してEnterキーを押し、「Are you sure you want to continue?[N]>" ステップ 10.5： リストから戻すバージョンに関連付けられている番号を選択し、Enterキーを押します。 SWA_CLI> revert This command will revert the appliance 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.

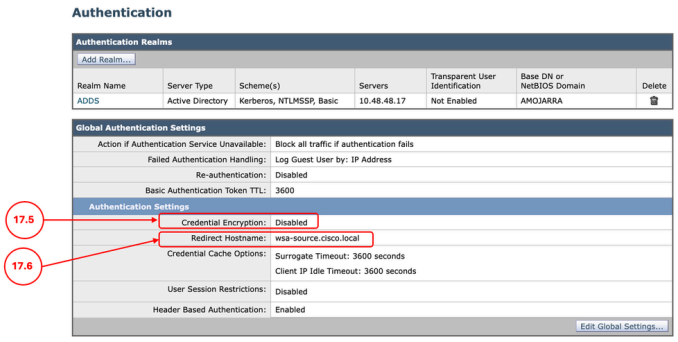
	Do you want to continue? [N]> Y Are you sure you want to continue? [N]> Y Available versions ========== 1. 12.5.1-011 Please select an AsyncOS version: 1 You have selected "12.5.1-011". The system will now reboot to perform the revert operation.

設定が元に戻されたSWA

ステップ 11SWAのライセンス	ステップ 11.1： 詳細については、「セキュアWebアプライアンスの初期設定の設定」を参照してください。
ステップ 12システムセットアップウィザードを実行	ステップ 12.1： 詳細については、「セキュアWebアプライアンスの初期設定の設定」を参照してください。
ステップ 13カスタムの信頼されたルート証明書のインポート 注：カスタムの信頼できるルート証明書を使用していない場合は、ステップ14に進んでください。	ステップ 13.1： GUIで、Networkに移動し、Certificate Managementをクリックします。 ステップ 13.2：Certificate Managementセクションで、Manage Trusted Root Certificatesをクリックします。 ステップ 13.3：[Import] をクリックします。 ステップ 13.4：ステップ3でダウンロードした証明書をアップロードします。 注意：ルート証明書と中間証明書の両方が使用可能な場合は、ルートCA証明書のアップロードから始めます。変更を送信してコミットした後、中間証明書のインポートに進みます。
手順 14：設定ファイルのインポート 注意：インポートするコンフィギュレーシ	ステップ 14.1：GUIで、System Administrationに移動し、Configuration Fileを選択します。

⚠ ョンファイルが、ステップ1でエクスポートしたコンフィギュレーションファイルではなく、現在のバージョンに対応していることを確認してください。	ステップ 14.2：Load Configurationセクションで、Load a configuration file from local computerを選択します。 ステップ 14.3：Choose Fileをクリックし、現在のバージョンに関連するXMLコンフィギュレーションファイルを選択します。 ステップ14.4.（オプション）復元によってIPアドレスとネットワーク設定が削除された場合は、「ネットワーク設定のロード」チェックボックスをオンにします。削除されなかった場合は、このオプションは選択しません。 ステップ 14.5：Loadをクリックします。 ステップ 14.6：Confirm Load Configurationポップアップでcontinueをクリックします。  イメージ：古いコンフィギュレーションファイルのロード ステップ 14.7： 変更を保存します。
手順 15：ルートのインポート 注：設定のインポート中にネットワーク設定のロードを行う場合は、ステップ17に進んでください。	ステップ 15.1： GUIで、Networkに移動し、Routesをクリックします。 ステップ 15.2：各ルーティングテーブルで、Load Route Tableをクリックします。 ステップ 15.3：ステップ8でエクスポートしたファイルを選択します。 ステップ 15.4：[Submit] をクリックします。 ステップ 15.5：変更を保存します。
ステップ 16：DNS設定の構成	ステップ 16.1： GUIで、Networkに移動し、DNSをクリックします。

注：設定のインポート中にネットワーク設定のロードを行う場合は、ステップ17に進んでください。	ステップ 16.2：[Edit Settings] をクリックします。 ステップ 16.3：ステップ9のスクリーンショットを使用してください。 ステップ 16.4：[Submit] をクリックします。 ステップ 16.5：変更を保存します。
ステップ 17：SWAのActive Directoryへの参加/再参加	ステップ 17.1： GUIで、Networkに移動し、Authenticationをクリックします。 ステップ 17.2： 認証レルム名の名前をクリックします。 ヒント: SWAに新しいIPアドレスとホスト名を割り当てる場合は、必要なDNSレコードがActive Directory DNSサービスで作成されていることを確認します。 ステップ 17.3：Join Domainをクリックして、クレデンシャルを入力します。  イメージ – Active Directoryへの参加 ステップ 17.4：[Submit] をクリックします。 ステップ 17.5：クレデンシャルの暗号化が有効になっている場合は、セキュア認証証明書をインポートします。 ステップ 17.6：リダイレクトホスト名が正しいことを確認します。



イメージ – 認証設定

ステップ 17.7：変更を保存します。

関連情報

- AsyncOS 15.2 for Cisco Secure Web Applianceユーザガイド
- セキュアなWebアプライアンスの初期設定
- セキュアなWebアプライアンスのベストプラクティスの使用
- セキュアなWebアプライアンスのログへのアクセス

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。