2つのSWA間での設定の移行

内容

はじめに

このドキュメントでは、Secure Web Appliance(SWA)から別のアプライアンスに設定を復元するプロセス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
- セキュリティ管理アプライアンス(SMA)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

この記事では、移行元SWAから移行先SWAに移行する手順の概要を説明します。この表は、各システムの仕様を示しています。

	ソースSWA	ターゲットSWA
モデル	S396	S100v
バージョン	15.5.0-710	15.5.0-710
ライセンス	スマートライセンス	スマートライセンス
Active Directory	結合	結合
Identity Services Engine(ISE)との統合	Yes	Yes

ネットワークインターフェイスカード(NIC)の数	5	5
HTTPS復号化	自己署名証明書で有効化	自己署名証明書で有効化
透過的なリダイレクト	WCCP	WCCP
SMAによる管理	Yes	Yes
外部ログサーバ	SCPプッシュ	SCPプッシュ
ハイ アベイラビリティ	Enabled	Enabled

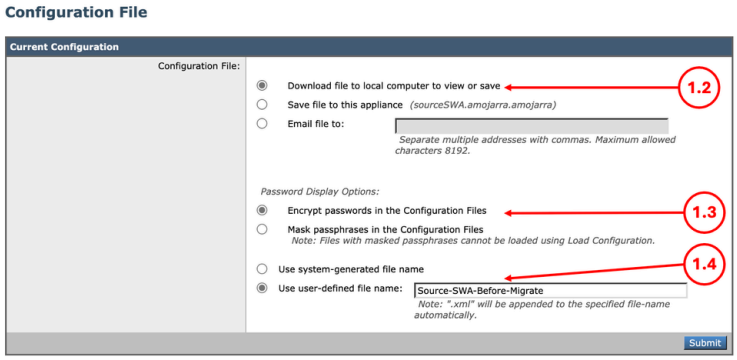
注：新しい仮想SWAをインストールするときは、必ずシスコが推奨するすべてのネットワークインターフェイスが仮想マシン(VM)上に存在し、設定されていることを確認してください。 インターフェイスは切断されたままでも構いませんが、VM内で使用可能である必要があります。

SWAをあるデバイスから別のデバイスに移行する場合には、次の2つのシナリオが考えられます。
[シナリオ–1]既存のSWAの置き換え：元のSWAは廃止され、ターゲットSWAのIPアドレスは送信元SWAと同じになります。
[シナリオ–2]新しいSWAの追加：新しいSWAが設定されている間、元のSWAはサービス状態のままです。

ソースSWAの準備とバックアップ

ソースSWAから必要なファイルと設定を収集するには、次の手順を使用します。

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 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。

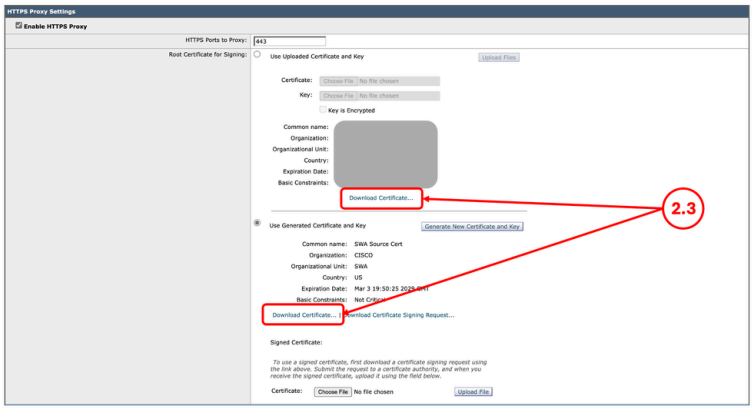
<table>
<tr>
<td></td>
<td> 

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。

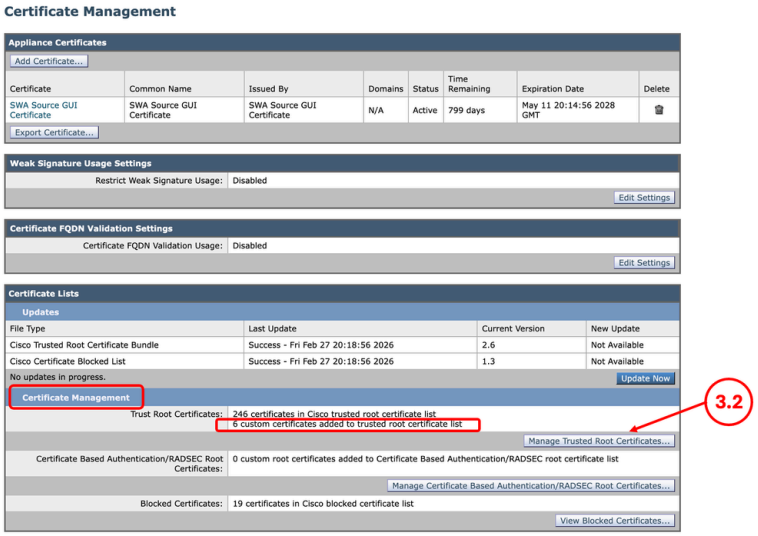
 

イメージ：HTTPS暗号解除証明書

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。</td>
</tr>
<tr>
<td>ステップ 3カスタム信頼ルート証明書のエクスポート

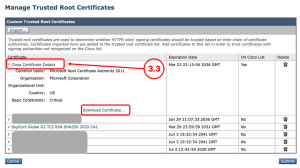
注:SWAに追加されたカスタムの信頼されたルート証明書がない場合は、ステップ4に進んでください。</td>
<td>ステップ 3.1： GUIで、Networkに移動し、Certificate Managementをクリックします。

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。</td>
</tr>
</table>



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。



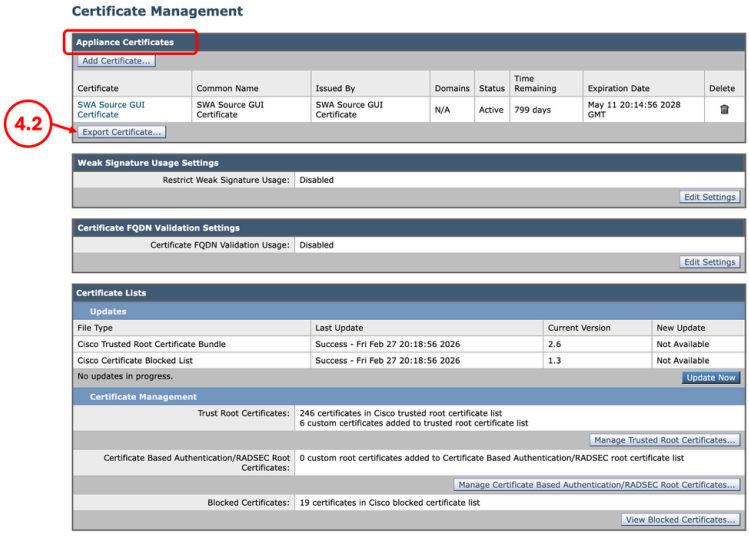
イメージ：信頼できるルート証明書のダウンロード

ステップ 4GUI証明書のエクスポート

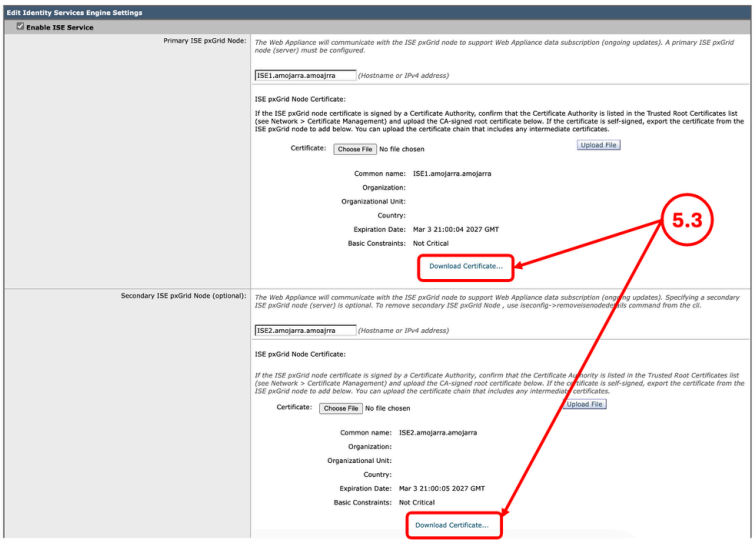
注：組み込みのGUI証明書を使用している場合は、ステップ5に進んでください。

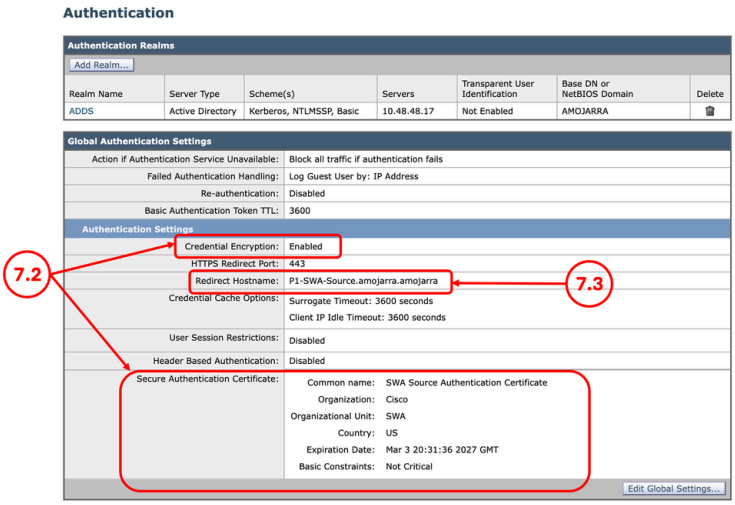
ステップ 4.1： GUIで、Networkに移動し、Certificate Managementをクリックします。

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。

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

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。</td>
</tr>
<tr>
<td>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。</td>
<td>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。

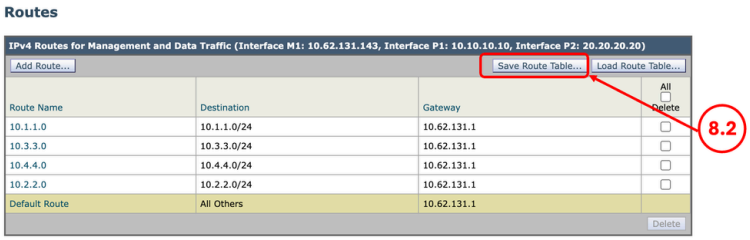
 

図 – ルーティングテーブルのエクスポート</td>
</tr>
<tr>
<td>ステップ 9DNS設定

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。</td>
<td>ステップ 9.1： GUIで、Networkに移動し、DNSをクリックします。

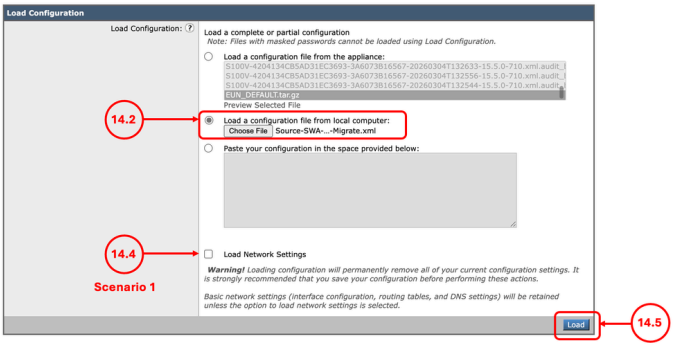
ステップ 9.2：DNS設定のスクリーンショットを取得します。</td>
</tr>
</table>

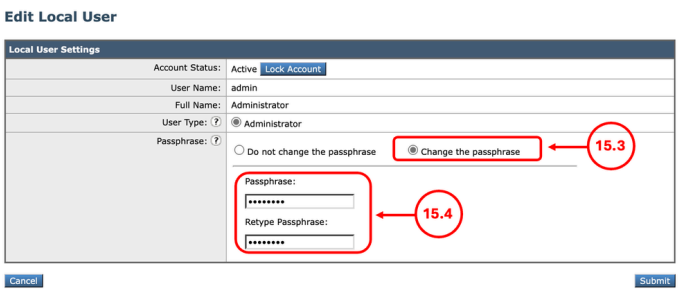
ターゲットSWAの準備

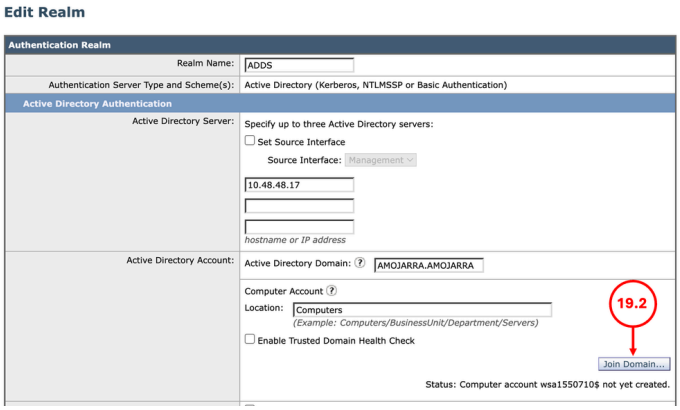
ステップ 10仮想SWAのインストール 注：ターゲットSWAが物理的なものである場合は、ステップ11に進んでください。	ステップ 10.1：仮想SWAをインストールするには、次のガイドを使用します。 • Vmware ESXiへのセキュアWebアプライアンスのインストール • Microsoft Hyper-Vへのセキュアwebアプライアンスのインストール ステップ 10.2：新しいSWAに推奨されるネットワークアクセスがあることを確認します。 • セキュアWebアプライアンス用のファイアウォールの設定
ステップ 11SWAの初期設定	ステップ 11.1：IP アドレスを設定します。 ステップ 11.2：Default Gateway を設定します。 ステップ 11.3： DNSサーバを設定します。 ステップ11.4:アプライアンスにライセンスを付与します。 ステップ 11.5：機能を有効にします。 ステップ 11.6：システムセットアップウィザードを実行。 詳細な手順については、「Secure Web Appliance Initial Setup」を参照してください。
ステップ 12構成ファイルのサニタイズ 注:ISEをSWAと統合しない場合は、ステップ13に進んでください。	ステップ 12.1：XMLバックアップファイルからISE証明書設定を削除するには、この記事の「エラーの修正」セクションを参照してください。

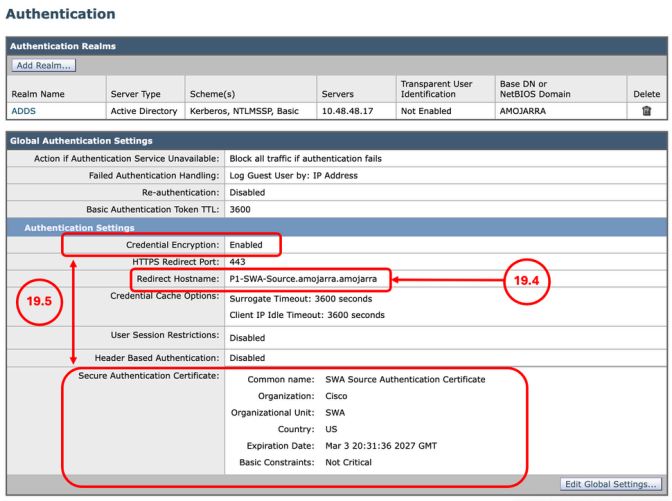
ターゲットSWAへのコンフィギュレーションファイルのインポート

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	ステップ 13.1： GUIで、Networkに移動し、Certificate Managementをクリックします。

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 13.2：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	ステップ 14.1：GUIで、System Administrationに移動し、Configuration Fileを選択します。 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、XML設定ファイルを選択します。 ステップ 14.4：移行がシナリオ1に一致し、以前のIPアドレスを新しいSWAで使用する必要がある場合は、チェックボックスLoad Network Settingsを選択します。それ以外の場合は、このオプションを選択しません。 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：設定のインポート
手順 15：管理者パスワードの変更 注：ソースSWA管理者パスワードがある場合は、ステップ16に進んでください。	15.1. GUIから、System Administrationに移動し、Usersを選択します。 15.2.管理者ユーザ名をクリックします。 15.3. Change the passphraseを選択します。 15.4.パスワードを入力します。 15.5. Submitをクリックします。  イメージ – 管理者パスワードの変更
ステップ 16：Commit	ステップ 16.1： これで、変更をコミットできます。
ステップ 17：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19に進んでください。	ステップ 17.1： GUIで、Networkに移動し、Routesをクリックします。 ステップ 17.2：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 17.3：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 17.4：[Submit] をクリックします。 ステップ 17.5：変更を保存します。
ステップ 18：DNS設定の構成 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19に進んでください。	ステップ 18.1： GUIで、Networkに移動し、DNSをクリックします。 ステップ 18.2：[Edit Settings] をクリックします。 ステップ 18.3：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 18.4：[Submit] をクリックします。 ステップ 18.5：変更を保存します。
ステップ 19：SWAのActive Directoryへの参加/再参加	ステップ 19.1： GUIで、Networkに移動し、Authenticationをクリックします。 ステップ19.2: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 19.2：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ドメインへの参加 ステップ 19.3：[Submit] をクリックします。 ステップ 19.4：リダイレクトホスト名が正しいことを確認します。 ステップ 19.5：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が正しいことを確認します。



イメージ – 認証設定

ステップ 19.6：変更を保存します。

ステップ 20：SMAへの再参加

注:SWAがSMAによって管理されない場合は、このステップをスキップします。

注：既存のSWA（シナリオ2）を置き換えておらず、移行されたSWAに新しいIPアドレスがある場合、SWAを新しいデバイスとしてSMAに追加し、ステップ20をスキップします。

ステップ 20.1：SMAのCLIに接続します。

ステップ20.2:logconfigを実行します。

ステップ 20.3：「HOSTKEYCONFIG」と入力します。

ステップ 20.4：DELETEと入力してEnterキーを押します。

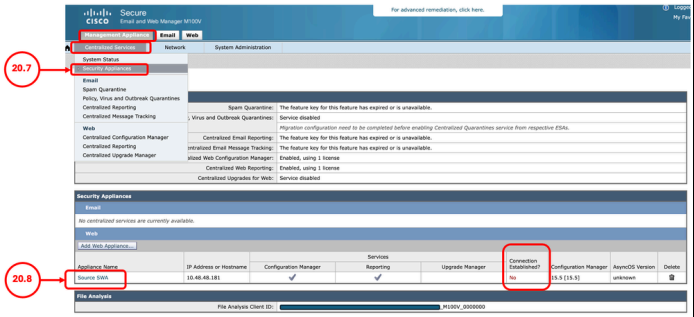
ステップ 20.5：最近移行したSWAに関連付けられている番号を入力し、ウィザードが終了するまでEnterキーを押します。

ステップ 20.6：commitと入力してEnterキーを押し、変更を保存します。

ステップ 20.7：SMAのGUIで、管理アプライアンスに移動します。 Centralized Servicesを選択し、Security Appliancesをクリックします。

ステップ20.8:移行したSWAの名前をクリックします。

ヒント:「Connection Established」列が「No」に設定されていることがわかります。



イメージ：SMAセキュリティアプライアンスのステータス

ステップ20.9:Establish Connectionをクリックします。

ステップ 20.10：ユーザ名とパスフレーズを入力して、Establish Connectionをクリックします。

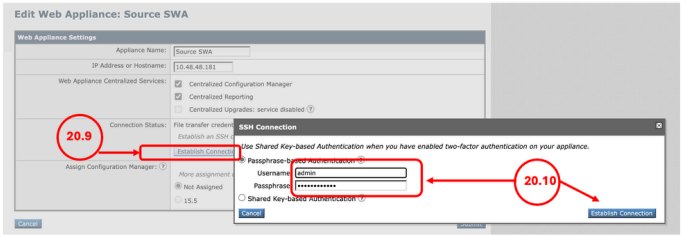
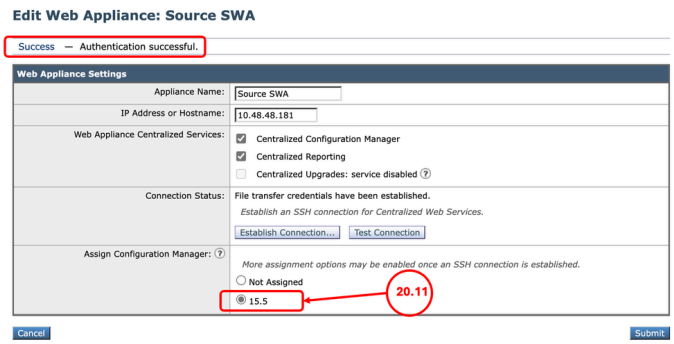


図 – SWAへの接続の確立

ステップ 20.11：Configuration Managerを割り当てます。



イメージ – Configuration Managerの割り当て

ステップ 20.12：変更を [Submit] して [Commit] します。

ステップ20.13:（オプション）設定をSWAに発

	行することでテストできます。 ヒント:SMAは以前のSWAからのすべてのレポートおよびトラッキングデータを保持します。

エラーの修正

要素port_nameの解析エラー

ネットワークポート名は['Management', 'P1', 'P2', 'T1', 'T2']のいずれかである必要があります：

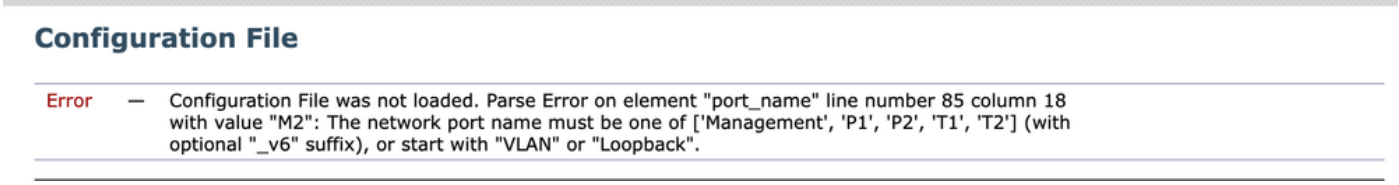


図 – ネットワークインターフェイスの名前付けエラー

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

このエラーは、物理SWAから仮想SWAに移行するときに発生します。仮想SWAには5つのNICしかなく、M2インターフェイスは無効です。このエラーを修正するには、テキストエディタでXML設定ファイルを編集し、次の行を削除します。

```
        M2
```

```
        M2
```

M2

autoselect

aa:bb:cc:00:00:00

要素ise_serviceの解析エラー

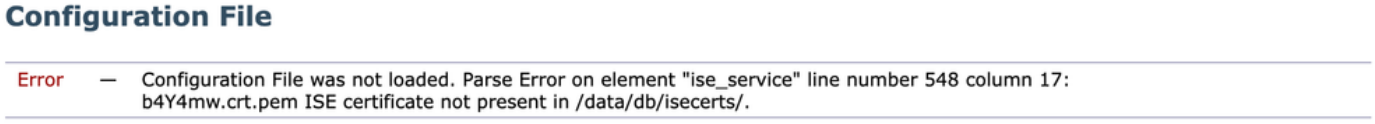


図 – ISE証明書エラー

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

ISE証明書はSWA設定のエクスポートに含まれておらず、デバイスに直接アップロードされているため、XMLファイルから証明書設定を削除し、インポートが成功したらISEを手動で設定する必要があります。この問題を解決するには、テキスト工ディタでXML設定ファイルを編集し、エラーで証明書名を検索(この例ではAA11AA)して、設定ファイルから削除します。

Before:

```
        AA11AA

        BB22BB
```

After:

証明書名以外に、Webアプライアンスクライアント証明書名も削除する必要があります。

次の例では、Webアプライアンスクライアント証明書は自己署名証明書です。

Before:

```
       1

       xAcK6T
```

After:

0

新しい仮想SWAでフェールオーバーが機能していない

ターゲットの仮想SWAでハイアベイラビリティ（フェールオーバー）が機能していない場合は、ハイパーバイザが正しく設定されていることを確認します。詳細については、次のサイトを参照してください。VMware環境で仮想WSA HAグループが適切に機能することを確認する

関連情報

- AsyncOS 15.2 for Cisco Secure Web Applianceユーザガイド
- Vmware ESXiへのセキュアWebアプライアンスのインストール
- Microsoft Hyper-Vへのセキュアwebアプライアンスのインストール
- セキュアなWebアプライアンスの初期設定
- Cisco Secure Email & Web仮想アプライアンスインストールガイド
- Secure Web Applianceでのカスタムurlカテゴリの設定：シスコ
- 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Webアプライアンス用のファイアウォールの設定
- Secure Web Applianceでの復号化証明書の設定
- Secure Web Appliance DNSサービスのトラブルシューティング
- Vmware 環境で適切な仮想 WSA HA グループ機能を確認する

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。