Migration der Konfiguration zwischen zwei SWAs

Inhalt

Einleitung

In diesem Dokument wird der Prozess zum Wiederherstellen der Konfiguration von einer sicheren Web-Appliance (SWA) auf eine andere beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA
- Administratorzugriff auf die SWA
- Administratorzugriff auf die Security Management Appliance (SMA)
- Zugriff auf das Cisco Software Licensing Portal oder die SWA-Lizenzdatei
- Zugriff durch privilegierten Active Directory-Benutzer, um der SWA-Domäne beizutreten und DNS-Einträge zu erstellen

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Vorbereitungen

In diesem Artikel beschreiben wir die Schritte zur Migration von der Quell-SWA zur Ziel-SWA. In dieser Tabelle sind die Spezifikationen für die einzelnen Systeme aufgeführt.

	Quell-SWA	Ziel-SWA
Modell	S396	S100V
Version	15.5.0-710	15.5.0-710
Lizenz	Smart-Lizenz	Smart-Lizenz
Active Directory	Verbunden	Verbunden
Integration mit Identity Services Engine (ISE)	Ja	Ja

Anzahl der Netzwerkkarten (NIC)	5	5
HTTPS-Entschlüsselung	Aktiviert mit selbstsigniertem Zertifikat	Aktiviert mit selbstsigniertem Zertifikat
Transparente Umleitung	WCCP	WCCP
Von SMA verwaltet	Ja	Ja
Externer Protokollserver	SCP-Push	SCP-Push
Hohe Verfügbarkeit	Aktiviert	Aktiviert

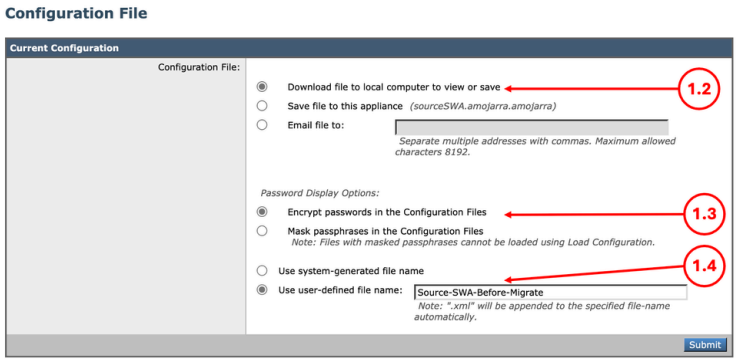
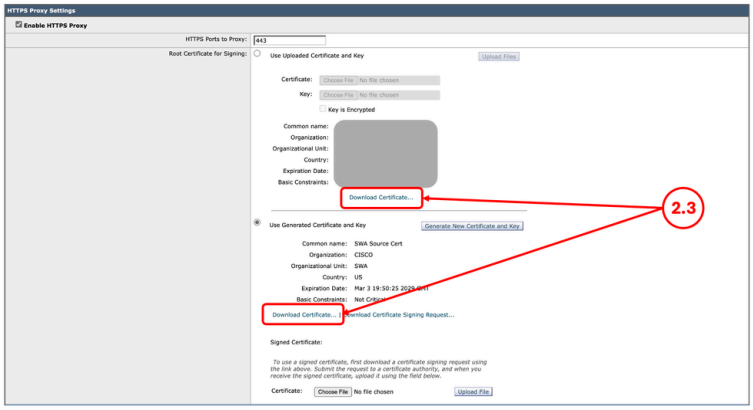
Anmerkung: Stellen Sie bei der Installation einer neuen virtuellen SWA sicher, dass alle von Cisco empfohlenen Netzwerkschnittstellen auf der virtuellen Maschine (VM) vorhanden und konfiguriert sind. Die Schnittstellen können getrennt bleiben, müssen jedoch innerhalb der VM verfügbar sein.

Bei der Migration der SWA von einem Gerät zu einem anderen gibt es zwei mögliche Szenarien:
[Szenario-1] Ersetzen des bestehenden SWA: Der ursprüngliche SWA wird außer Betrieb genommen, und die IP-Adresse des Ziel-SWA ist mit der Quell-SWA identisch.
[Szenario-2] Hinzufügen eines neuen SWA: Das ursprüngliche SWA bleibt in Betrieb, während das neue SWA konfiguriert wird.

Vorbereiten und Sichern des Quell-SWA

Führen Sie die folgenden Schritte aus, um die erforderlichen Dateien und Konfigurationen vom Quell-SWA zu erfassen:

Schritt 1: Exportieren der Konfigurationsdatei	Schritt 1.1. Navigieren Sie in der GUI zu Systemverwaltung, und wählen Sie Konfigurationsdatei. Schritt 1.2. Stellen Sie sicher, dass Datei auf lokalen Computer herunterladen zum Anzeigen oder Speichern ausgewählt ist. Schritt 1.3. Wählen Sie in den Konfigurationsdateien "Kennwörter verschlüsseln" aus.

	Schritt 1.4. (Optional) Wählen Sie einen Namen für die Konfigurationsdatei aus. Schritt 1.5: Klicken Sie auf Senden.  Bild - Exportieren der Konfigurationsdatei
Schritt 2: Entschlüsselungszertifikat exportieren Anmerkung: Wenn die HTTPS-Entschlüsselung deaktiviert ist, fahren Sie mit Schritt 3 fort.	Schritt 2.1. Navigieren Sie in der GUI zu Sicherheitsdienste, und klicken Sie auf HTTPS-Proxy. Schritt 2.2. Klicken Sie auf Einstellungen bearbeiten. Schritt 2.3. Laden Sie das HTTPS-Entschlüsselungszertifikat herunter, indem Sie auf Zertifikat herunterladen... klicken. Link.  Bild - HTTPS-Entschlüsselungszertifikat Anmerkung: In diesem Beispiel werden beide Typen von HTTPS-Entschlüsselungszertifikaten veranschaulicht. In Ihrem Netzwerk kann jedoch nur ein Typ bereitgestellt werden.
Schritt 3: Exportieren der Stammzertifikate der	Schritt 3.1. Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf Zertifikatsverwaltung.

benutzerdefinierten Vertrauensstellung

Anmerkung: Wenn dem SWA kein benutzerdefiniertes vertrauenswürdiges Stammzertifikat hinzugefügt wurde, fahren Sie mit Schritt 4 fort.

Schritt 3.2. Klicken Sie im Abschnitt Zertifikatsverwaltung auf Vertrauenswürdige Stammzertifikate verwalten.

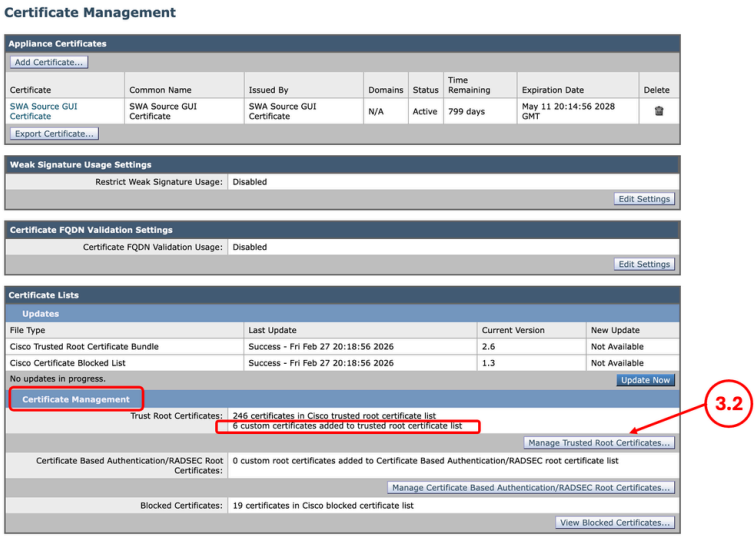


Bild - Vertrauenswürdige Stammzertifikate verwalten

Schritt 3.3. Erweitern Sie jedes benutzerdefinierte vertrauenswürdige Stammzertifikat, indem Sie auf den Namen des Zertifikats klicken und auf Zertifikat herunterladen... klicken.

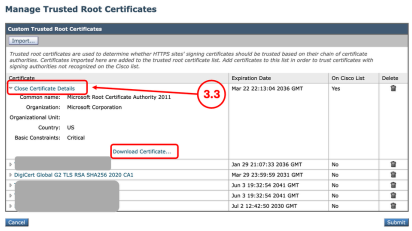


Bild - Vertrauenswürdige Stammzertifikate herunterladen

Schritt 4: Exportieren des GUI-Zertifikats

Anmerkung: Wenn Sie ein integriertes GUI-Zertifikat verwenden, fahren Sie mit Schritt 5 fort.

Schritt 4.1: Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf Zertifikatsverwaltung.

Schritt 4.2. Klicken Sie im Abschnitt Appliance-Zertifikate auf Zertifikat exportieren.

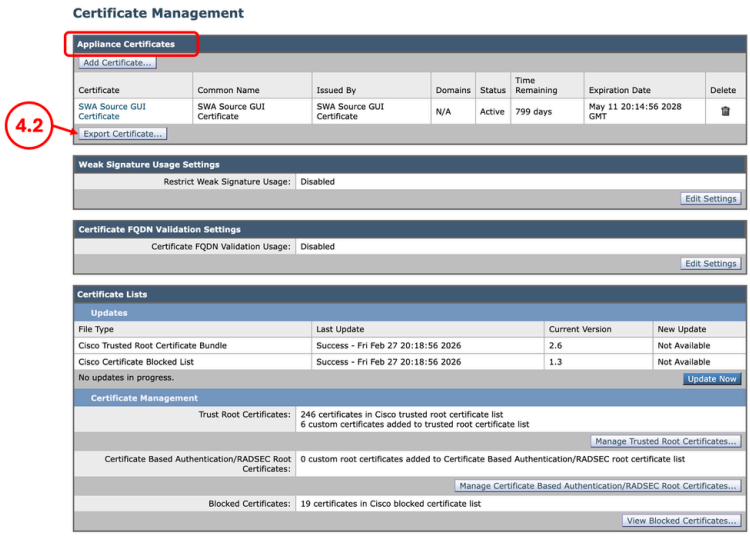


Bild - GUI-Zertifikat exportieren

Schritt 5: Exportieren der ISE-Zertifikate

Anmerkung: Wenn keine SWA oder ISE integriert sind, fahren Sie mit Schritt 6 fort.

Schritt 5.1: Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf Identity Services Engine.

Schritt 5.2. Klicken Sie auf Einstellungen bearbeiten.

Schritt 5.3. Laden Sie alle verfügbaren Zertifikate herunter.

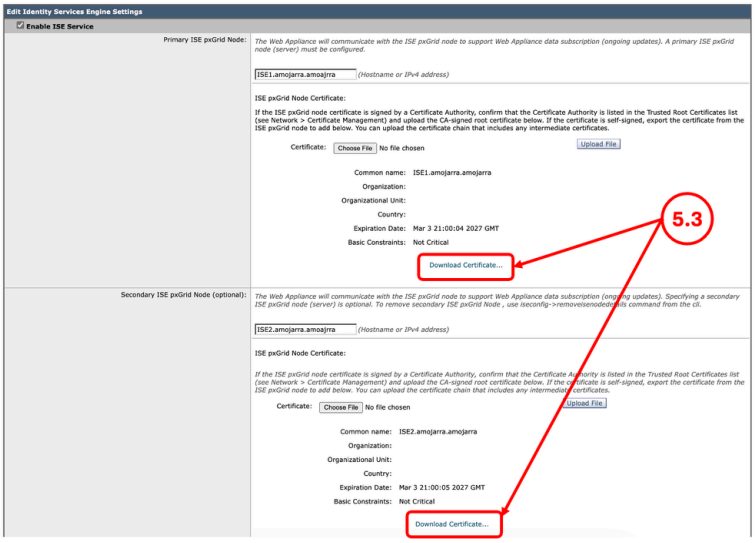
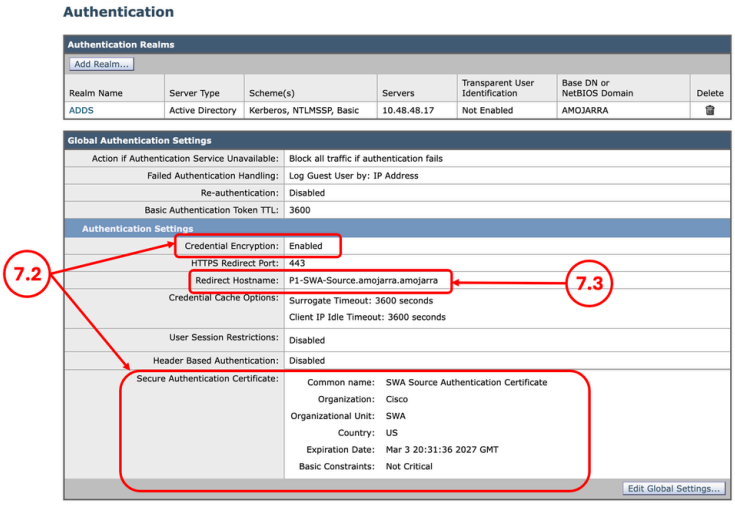
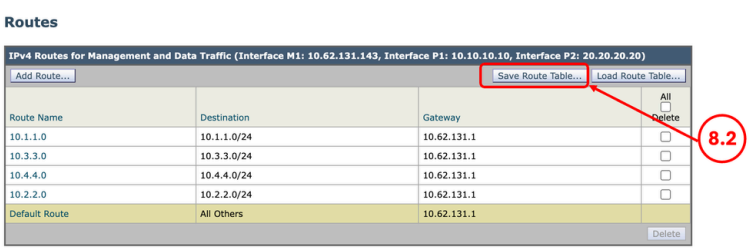


Bild - ISE-Zertifikate herunterladen

Schritt 6: Lizenzen/Funktionen

Schritt 6.1. Navigieren Sie in der GUI zu Systemverwaltung, und klicken Sie auf Lizenzen oder Funktionen, je nach Lizenztyp, den Sie verwenden.

Schritt 6.2. Erstellen Sie einen Screenshot Ihrer Lizenzen/Funktionen.

Schritt 7: Zertifikat für die Authentifizierungsumleitung	Schritt 7.1: Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf Authentifizierung. Schritt 7.2. Wenn die Verschlüsselung der Anmeldeinformationen aktiviert ist, stellen Sie sicher, dass das Zertifikat und der Schlüssel vorhanden sind. Schritt 7.3: Erstellen Sie einen Screenshot der aktuellen Konfiguration.  Bild - Authentifizierungszertifikat Anmerkung: Das Authentifizierungszertifikat kann nicht von der GUI heruntergeladen werden.
Schritt 8: Exportieren statischer Routen Anmerkung: Wenn Sie die Verwendung derselben Netzwerkkonfiguration und IP-Adresse für das Ziel-SWA planen, fahren Sie mit Schritt 10 fort.	Schritt 8.1: Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf Routes (Routen). Schritt 8.2: Klicken Sie für jede Routing-Tabelle auf Route Table speichern.  Bild - Exportieren der Routing-Tabelle
Schritt 9: DNS-Einstellungen	Schritt 9.1: Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf DNS.

Anmerkung: Wenn Sie die Verwendung derselben Netzwerkkonfiguration und IP-Adresse für das Ziel-SWA planen, fahren Sie mit Schritt 10 fort.	Schritt 9.2. Erstellen Sie einen Screenshot der DNS-Konfiguration.

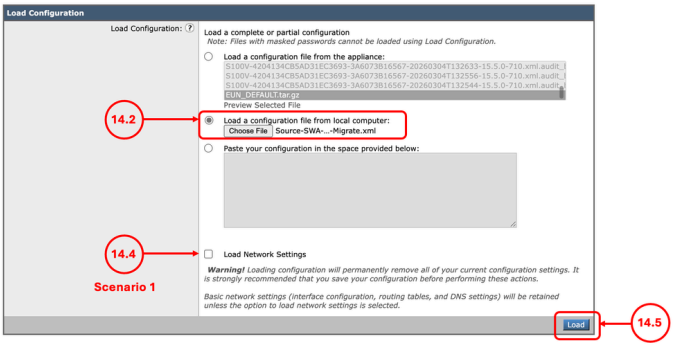
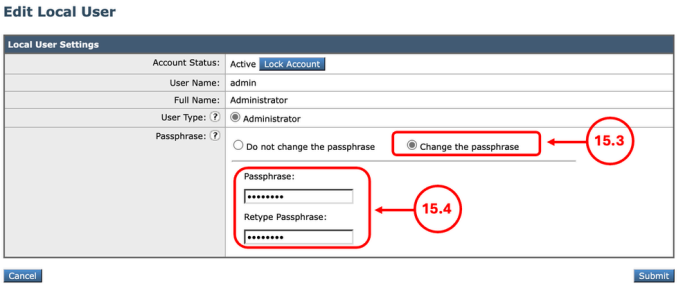
Vorbereiten der Ziel-SWA

Schritt 10: Installieren der virtuellen SWA Anmerkung: Wenn die Ziel-SWA physisch ist, können Sie mit Schritt 11 fortfahren.	Schritt 10.1. Installieren Sie die virtuelle SWA mithilfe der folgenden Anleitungen: • Installieren der sicheren Web-Appliance auf VMware ESXi • Installieren der sicheren Web-Appliance auf Microsoft Hyper-V Schritt 10.2. Vergewissern Sie sich, dass der neue SWA über den empfohlenen Netzwerkzugriff verfügt: • Firewall für sichere Web-Appliance konfigurieren
Schritt 11: Erste SWA-Einrichtung	Schritt 11.1: Konfigurieren der IP-Adresse Schritt 11.2: Konfigurieren des Standardgateways Schritt 11.3: Konfigurieren des DNS-Servers Schritt 11.4: Lizenzierung der Appliance. Schritt 11.5: Aktivieren Sie die Funktionen. Schritt 11.6: Führen Sie den Systemeinrichtungsassistenten aus. In diesem Artikel finden Sie die einzelnen Schritte: Ersteinrichtung der sicheren Webappliance
Schritt 12: Bereinigen der Konfigurationsdatei Anmerkung: Wenn Sie die ISE nicht in die SWA integrieren, können Sie	Schritt 12.1. Lesen Sie den Abschnitt Behebungsfehler in diesem Artikel, um die ISE-Zertifikatkonfiguration aus der XML-Sicherungsdatei zu entfernen.

mit Schritt 13 fortfahren.	

Importieren der Konfigurationsdatei in das Ziel-SWA

Schritt 13: Benutzerdefinierte vertrauenswürdige Stammzertifikate importieren Anmerkung: Wenn Sie kein benutzerdefiniertes vertrauenswürdiges Stammzertifikat verwenden, fahren Sie mit Schritt 14 fort.	Schritt 13.1. Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf Zertifikatsverwaltung. Schritt 13.2. Klicken Sie im Abschnitt Zertifikatsverwaltung auf Vertrauenswürdige Stammzertifikate verwalten. Schritt 13.3: Klicken Sie auf Importieren. Schritt 13.4: Laden Sie die zuvor in Schritt 3 heruntergeladenen Zertifikate hoch. Vorsicht: Wenn sowohl das Root- als auch das Zwischenzertifikat verfügbar sind, laden Sie zuerst das Root-Zertifizierungsstellenzertifikat hoch. Nachdem Sie die Änderungen übermittelt und bestätigt haben, fahren Sie mit dem Importieren des Zwischenzertifikats fort.
Schritt 14: Importieren der Konfigurationsdatei	Schritt 14.1. Navigieren Sie in der GUI zu Systemverwaltung, und wählen Sie Konfigurationsdatei. Schritt 14.2. Wählen Sie im Abschnitt Konfiguration laden die Option Konfigurationsdatei vom lokalen Computer laden aus. Schritt 14.3: Klicken Sie auf Choose File (Datei auswählen), und wählen Sie die XML-Konfigurationsdatei aus. Schritt 14.4. Wenn die Migration mit Szenario 1 übereinstimmt und die vorherige IP-Adresse im neuen SWA verwendet werden muss, aktivieren Sie das Kontrollkästchen Netzwerkeinstellungen laden, andernfalls wählen Sie diese Option nicht.

	Schritt 14.5. Klicken Sie auf Laden. Schritt 14.6: Klicken Sie im Popup-Fenster Konfiguration bestätigen auf Weiter.  Image - Importieren der Konfiguration
Schritt 15: Ändern des Admin-Kennworts Hinweis: Wenn Sie das Quell-SWA-Admin-Kennwort haben, fahren Sie mit Schritt 16 fort.	15.1. Navigieren Sie in der GUI zu Systemverwaltung, und wählen Sie Benutzer aus. 15.2. Klicken Sie auf den Benutzernamen admin. 15.3. Wählen Sie Passphrase ändern aus. 15.4. Geben Sie das Kennwort ein. 15.5. Klicken Sie auf Senden.  Image - Ändern des Administratorkennworts
Schritt 16: Verpflichten	Schritt 16.1. Jetzt können Sie die Änderungen bestätigen.
Schritt 17: Importieren der Routen Hinweis: Wenn Sie beim Importieren der	Schritt 17.1: Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf Routes (Routen). Schritt 17.2. Klicken Sie für jede Routing-Tabelle

Konfiguration Netzwerkeinstellungen laden, fahren Sie mit Schritt 19 fort.	auf Routing-Tabelle laden. Schritt 17.3. Wählen Sie die Datei aus, die Sie in Schritt 8 exportiert haben. Schritt 17.4: Klicken Sie auf Senden. Schritt 17.5. Bestätigen Sie die Änderungen.
Schritt 18: Konfigurieren der DNS-Einstellungen Anmerkung: Wenn Sie beim Importieren der Konfiguration die Netzwerkeinstellungen laden, fahren Sie mit Schritt 19 fort.	Schritt 18.1. Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf DNS. Schritt 18.2. Klicken Sie auf Einstellungen bearbeiten. Schritt 18.3. Verwenden Sie den Screenshot aus Schritt 9 Schritt 18.4. Klicken Sie auf Senden. Schritt 18.5. Übernehmen Sie die Änderungen.
Schritt 19: Treten Sie dem SWA beim Active Directory bei bzw. treten Sie erneut bei.	Schritt 19.1. Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf Authentifizierung. Schritt 19.2: Klicken Sie auf den Namen des Authentifizierungsbereichs. Tipp: Wenn dem SWA eine neue IP-Adresse und ein neuer Hostname zugewiesen wird, stellen Sie sicher, dass die erforderlichen DNS-Einträge im Active Directory-DNS-Dienst erstellt werden. Schritt 19.2. Klicken Sie auf Join Domain (Domäne beitreten), und geben Sie die Anmeldeinformationen ein:

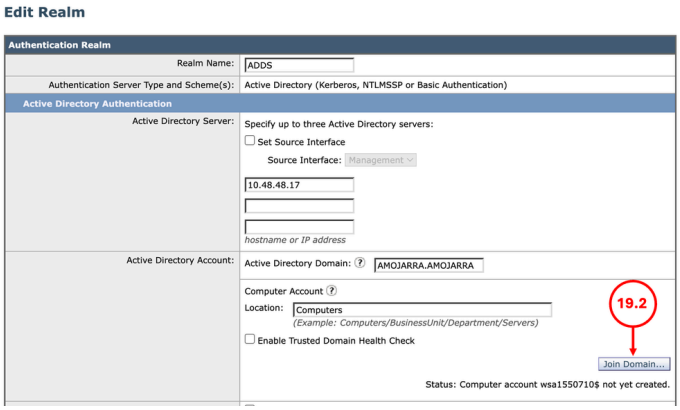


Bild - Beitreten zur Active Directory-Domäne

Schritt 19.3: Klicken Sie auf Senden.

Schritt 19.4. Stellen Sie sicher, dass der Umleitungshostname korrekt ist.

Schritt 19.5. Wenn die Verschlüsselung der Anmeldeinformationen aktiviert ist, stellen Sie sicher, dass das Zertifikat für die sichere Authentifizierung korrekt ist.

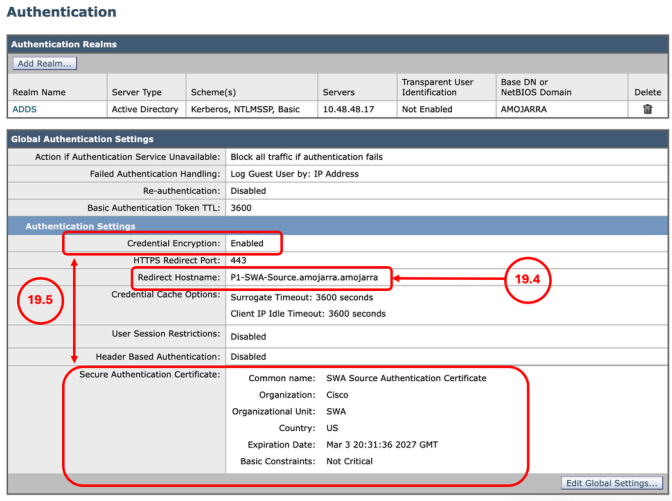


Bild - Authentifizierungseinstellungen

Schritt 19.6. Bestätigen Sie die Änderungen.

Schritt 20: Erneutes Beitreten zu SMA

Anmerkung: Wenn die SWA nicht von SMA verwaltet wird, überspringen Sie diesen Schritt.

Anmerkung: Wenn Sie den vorhandenen SWA nicht ersetzt haben (Szenario 2) und der migrierte SWA über eine neue IP-Adresse verfügt, fügen Sie den SWA als neues Gerät zu SMA hinzu, und überspringen Sie Schritt 20.

Schritt 20.1: Herstellen einer Verbindung mit der CLI der SMA

Schritt 20.2. Führen Sie logconfig aus.

Schritt 20.3. Geben Sie HOSTKEYCONFIG ein.

Schritt 20.4. Geben Sie LÖSCHEN ein, und drücken Sie die Eingabetaste.

Schritt 20.5. Geben Sie die Nummer ein, die mit dem kürzlich migrierten SWA verknüpft ist, und drücken Sie die Eingabetaste, bis der Assistent beendet ist.

Schritt 20.6. Geben Sie commit ein, und drücken Sie die Eingabetaste, um die Änderungen zu speichern.

Schritt 20.7. Navigieren Sie in der SMA-GUI zu Verwaltungs-Appliance. Wählen Sie Zentrale Dienste aus, und klicken Sie auf Sicherheits-Appliances.

Schritt 20.8: Klicken Sie auf den Namen der SWA, die vor kurzem migriert wurden.

Tipp: Sie können sehen, dass die Spalte Verbindung hergestellt auf Nein gesetzt ist.

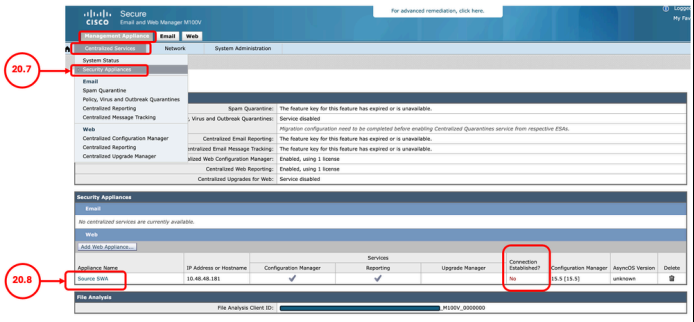


Bild - Status der SMA Security Appliance

Schritt 20.9: Klicken Sie auf Verbindung herstellen.

Schritt 20.10. Geben Sie den Benutzernamen und die Passphrase ein, und klicken Sie auf Verbindung herstellen.

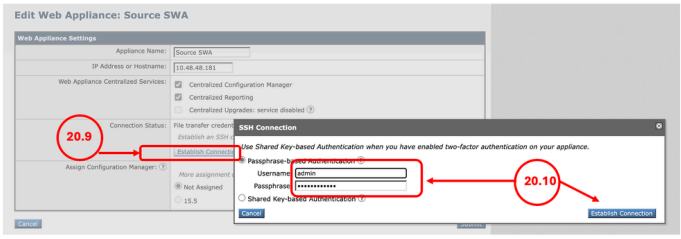
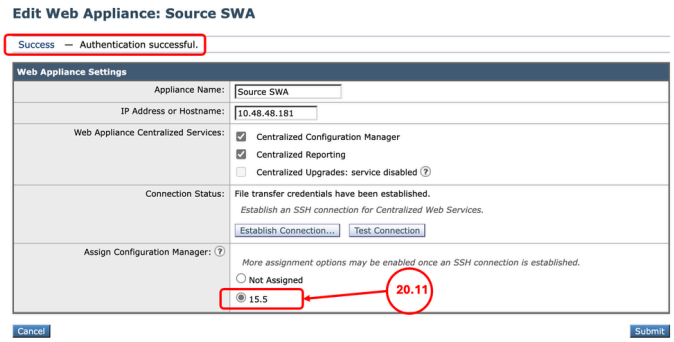


Bild - Verbindung mit dem SWA herstellen

Schritt 20.11: Zuweisen des Konfigurations-Managers



Abbild - Konfigurationsmanager zuweisen

Schritt 20.12: Senden und bestätigen Sie die Änderungen.

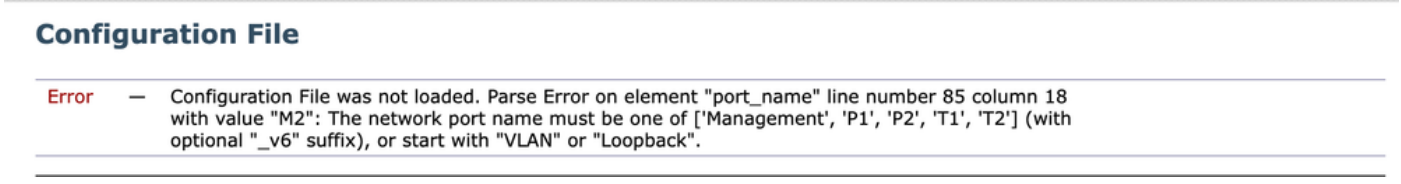
Schritt 20.13. (Optional) Sie können testen, indem Sie die Konfiguration in der SWA veröffentlichen.

Tipp: Die SMA speichert alle Reporting- und Tracking-Daten der vorherigen SWA.

Beheben von Fehlern

Fehler beim Einlesen des Elementports_name

Beim Namen des Netzwerkports muss es sich um ['Management', 'P1', 'P2', 'T1', 'T2'] handeln:



Abbild - Netzwerkschnittstellen-Benennungsfehler

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

Dieser Fehler tritt auf, wenn Sie von einem physischen SWA zu einem virtuellen System migrieren. Der virtuelle SWA verfügt nur über 5 NICs, und die M2-Schnittstelle ist ungültig. Um den Fehler zu beheben, bearbeiten Sie die XML-Konfigurationsdatei in einem Texteditor, und entfernen Sie die folgenden Zeilen:

```
        M2

         M2

        M2

        autoselect
```

```
        aa:bb:cc:00:00:00
```

Fehler beim Einlesen des Elements ise_service

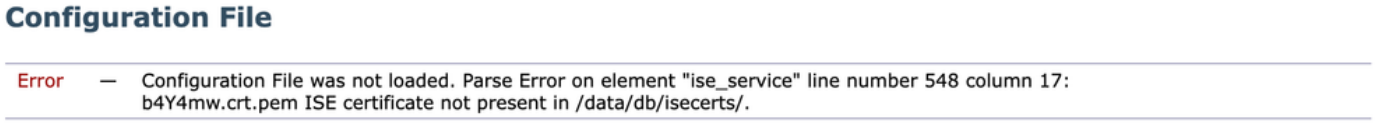


Bild - ISE-Zertifikatfehler

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

Da die ISE-Zertifikate nicht im SWA-Konfigurationsexport enthalten und direkt auf das Gerät hochgeladen werden, müssen Sie die Zertifikatkonfiguration aus der XML-Datei entfernen und nach erfolgreichem Import die ISE manuell konfigurieren. Um dieses Problem zu beheben, bearbeiten Sie die XML-Konfigurationsdatei im Text-Editor, suchen Sie im Fehler nach dem Namen des Zertifikats (in diesem Beispiel suchen Sie nach AA11AA) und löschen Sie es aus der Konfigurationsdatei:

```
Before:
```

```
        AA11AA
```

```
        BB22BB
```

```
After:
```

Abgesehen vom Zertifikatsnamen müssen Sie auch den Namen des Webappliance-Clientzertifikats entfernen.

In diesem Beispiel ist das Webappliance-Clientzertifikat ein selbstsigniertes Zertifikat:

```
Before:

        1

        xAcK6T

After:

        0
```

Failover funktioniert nicht mit neuem virtuellen SWA

Wenn die Hochverfügbarkeit (Failover) für die virtuelle SWA des Ziels nicht funktioniert, stellen Sie sicher, dass der Hypervisor richtig konfiguriert ist. Weitere Informationen finden Sie unter: Gewährleistung der ordnungsgemäßen Funktionalität der virtuellen WSA HA-Gruppe in einer VMware-Umgebung

Zugehörige Informationen

- Bedienungsanleitung für AsyncOS 15.2 für Cisco Secure Web Appliance
- Installieren der sicheren Web-Appliance auf VMware ESXi
- Installieren der sicheren Web-Appliance auf Microsoft Hyper-V

- Ersteinrichtung der sicheren Web-Appliance

- Installationsleitfaden für die Cisco Secure Email und Web Virtual Appliance
- Benutzerdefinierte URL-Kategorien in einer sicheren Web-Appliance konfigurieren - Cisco

- Best Practices für sichere Web-Appliances

- Firewall für sichere Web-Appliance konfigurieren

- Entschlüsselungszertifikat in sicherer Web-Appliance konfigurieren

- Fehlerbehebung beim DNS-Dienst der sicheren Webappliance
- Gewährleistung der korrekten Funktionalität der virtuellen WSA HA-Gruppe in einer VMware-Umgebung

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.