Sichere Web-Appliance auf vorherige Version zurücksetzen

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Zurücksetzen der Secure Web Appliance (SWA) auf die vorherige Version beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA

- Administratorzugriff auf die SWA
- 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

Das Zurücksetzen des Geräts ist äußerst zerstörerisch.
Diese Daten werden dabei vernichtet und müssen gesichert werden:
- Aktuelle Systemkonfigurationsdatei
- Alle Protokolldateien (Weitere Informationen finden Sie unter: Zugriff auf sichere Web-Appliance-Protokolle)
- Alle Berichtsdaten (einschließlich der gespeicherten geplanten und archivierten Berichte)
- Alle benutzerdefinierten Endbenutzer-Benachrichtigungsseiten.

Warnung: Stellen Sie vor dem Zurücksetzen auf eine frühere Version sicher, dass die verschlüsselte Konfigurationsdatei mit der entsprechenden Version vorliegt. Es ist möglich, dass die aktuelle Konfigurationsdatei nicht mit älteren Softwareversionen kompatibel ist.

Vorbereitung und Sicherung der SWA

Gehen Sie folgendermaßen vor, um die erforderlichen Dateien und Konfigurationen aus dem SWA zu sammeln, bevor Sie die Wiederherstellung durchführen:

<table>
<tr>
<td>Schritt 1: Exportieren der Konfigurationsdatei</td>
<td>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.

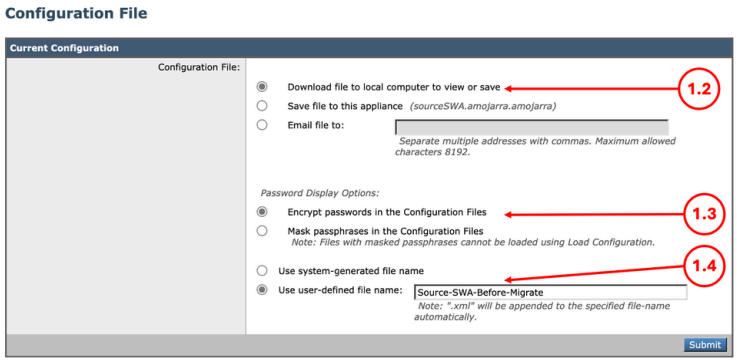
 

Bild - Exportieren der Konfigurationsdatei</td>
</tr>
<tr>
<td>Schritt 2: Entschlüsselungszertifikat exportieren

Anmerkung: Wenn die HTTPS-Entschlüsselung deaktiviert ist, fahren Sie mit Schritt 3 fort.</td>
<td>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.</td>
</tr>
</table>

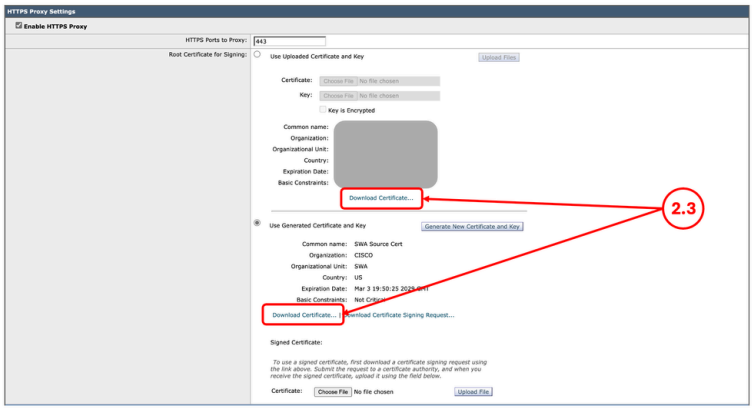


Bild - HTTPS-Entschlüsselungszertifikat

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 benutzerdefinierten Vertrauensstellung

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

Schritt 3.1. Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf Zertifikatsverwaltung.

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

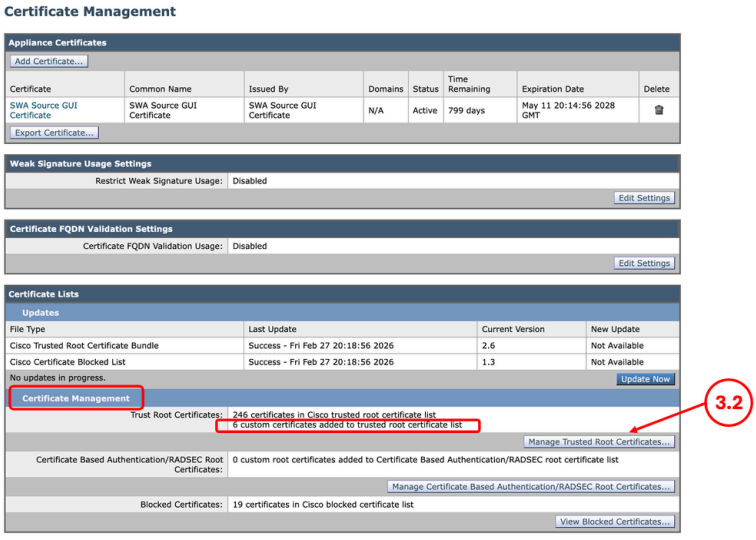


Bild - Vertrauenswürdige Stammzertifikate verwalten

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

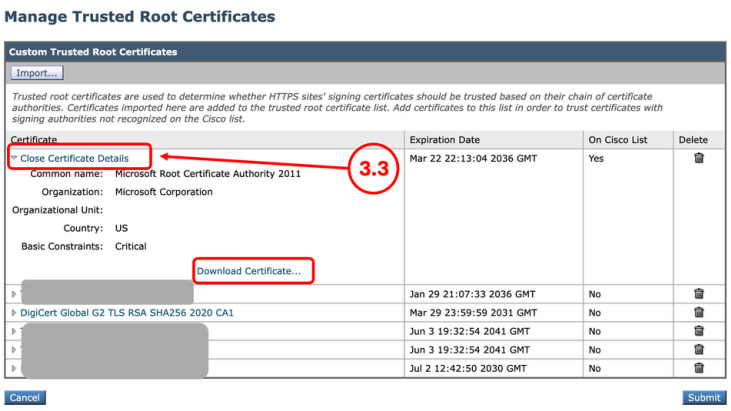
<table>
<tr>
<td></td>
<td> 

Bild - Vertrauenswürdige Stammzertifikate herunterladen</td>
</tr>
<tr>
<td>Schritt 4: Exportieren des GUI-Zertifikats

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

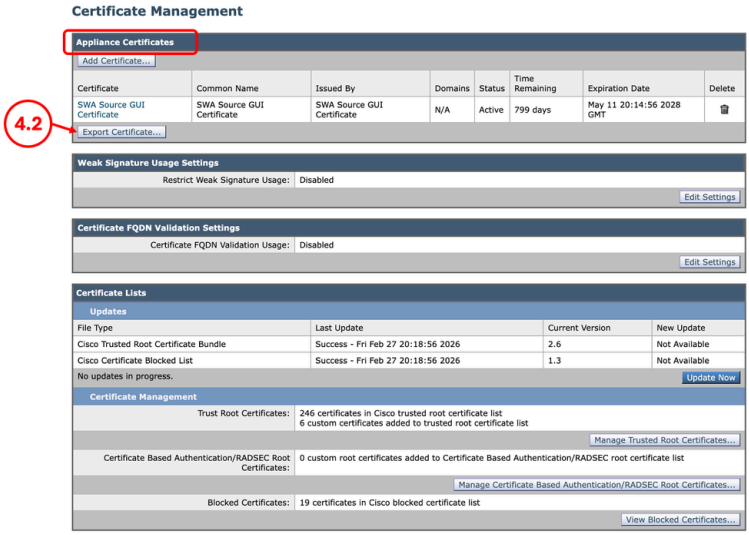
 

Bild - GUI-Zertifikat exportieren</td>
</tr>
<tr>
<td>Schritt 5: Exportieren der ISE-Zertifikate

Anmerkung: Wenn keine SWA oder ISE integriert sind, fahren Sie mit Schritt 6 fort.</td>
<td>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.</td>
</tr>
</table>

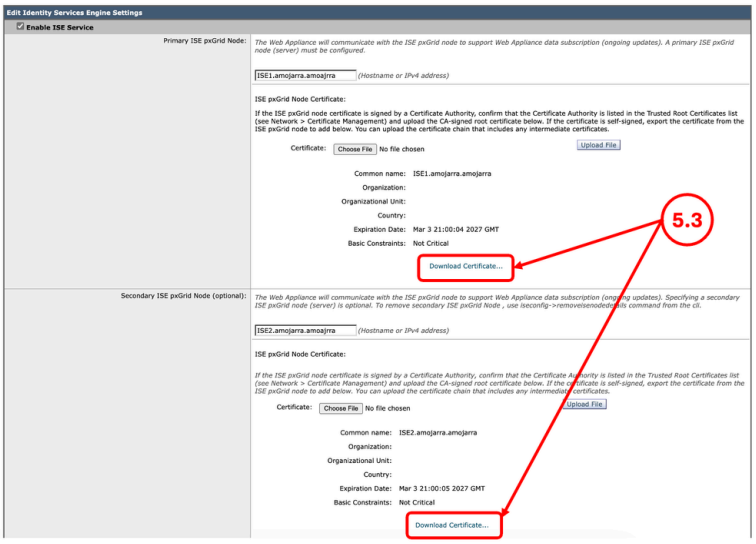
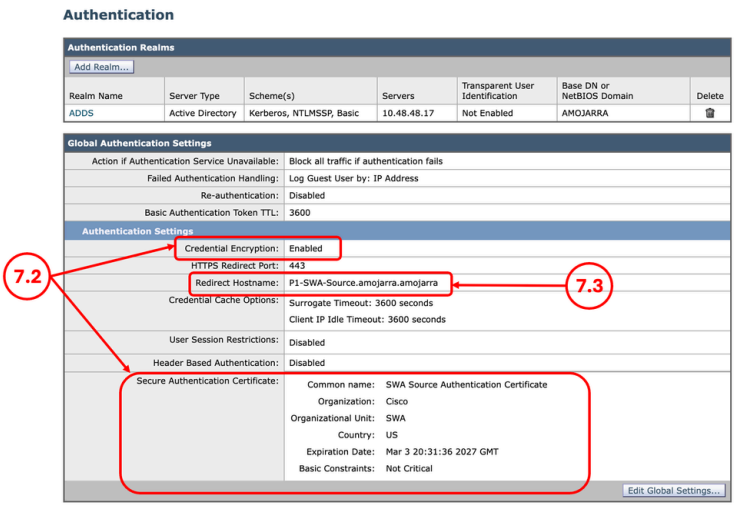
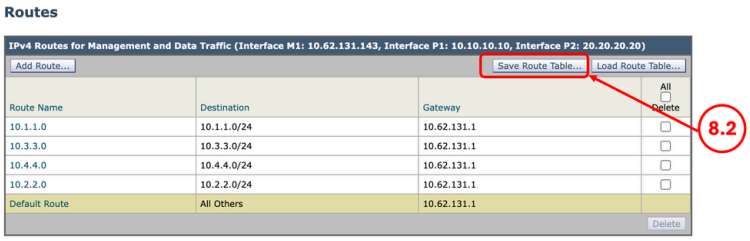
	 Bild - ISE-Zertifikate herunterladen
Schritt 6: Lizenzen/Funktionen	Schritt 6.1. Navigieren Sie in der GUI zu Systemverwaltung, und klicken Sie auf Lizenzen oder Funktionen, je nach Lizenztyp, den Sie verwenden. Schritt 6.2. Erstellen Sie einen Screenshot Ihrer Lizenzen/Funktionen.
Schritt 7: Zertifikat 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: Statische Routen exportieren 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 Anmerkung: Wenn Sie die Verwendung derselben Netzwerkkonfiguration und IP-Adresse für das Ziel-SWA planen, fahren Sie mit Schritt 10 fort.	Schritt 9.1: Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf DNS. Schritt 9.2. Erstellen Sie einen Screenshot der DNS-Konfiguration.

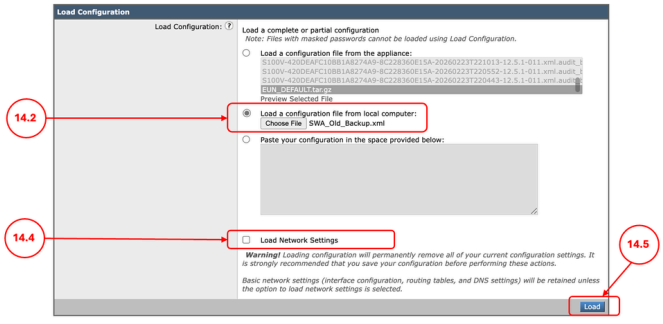
Zurücksetzen des SWA

Schritt 10: Zurücksetzen des SWA	Schritt 10.1: Herstellen einer Verbindung mit der CLI Schritt 10.2. Geben Sie revert ein, und drücken Sie die Eingabetaste. Schritt 10.3. Geben Sie Y ein, und drücken Sie die Eingabetaste für "Möchten Sie fortfahren? [N]> " Schritt 10.4. Geben Sie Y ein, und drücken Sie die Eingabetaste für "Möchten Sie wirklich fortfahren? [N]>" Schritt 10.5. Wählen Sie die Nummer aus, die der Version zugeordnet ist, die Sie zurücksetzen möchten, und drücken Sie die Eingabetaste.

	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.

Umgekehrte SWA-Konfiguration

Schritt 11: Lizenzierung der SWA	Schritt 11.1. Weitere Informationen finden Sie unter Konfigurieren der sicheren Web-Appliance bei der Ersteinrichtung.
Schritt 12: Führen Sie den Systemeinrichtungs-Assistenten aus.	Schritt 12.1. Weitere Informationen finden Sie unter Konfigurieren der sicheren Web-Appliance beim erstmaligen Setup.
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 ⚠ Vorsicht: Stellen Sie sicher, dass Sie die Konfigurationsdatei für die aktuelle Version importieren, und nicht die Konfigurationsdatei, die Sie in Schritt 1 exportiert haben.	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 für die aktuelle Version aus. Schritt 14.4. (Optional) Wenn bei der Zurücksetzung die IP-Adresse und die Netzwerkkonfiguration entfernt wurden, aktivieren Sie das Kontrollkästchen Netzwerkeinstellungen laden, andernfalls wählen Sie diese Option nicht aus. Schritt 14.5. Klicken Sie auf Laden. Schritt 14.6: Klicken Sie im Popup-Fenster Konfiguration bestätigen auf Weiter.  Image: Alte Konfigurationsdatei laden

	Schritt 14.7: Bestätigen Sie die Änderungen.
Schritt 15: Importieren der Routen Hinweis: Wenn Sie beim Importieren der Konfiguration Netzwerkeinstellungen laden, fahren Sie mit Schritt 17 fort.	Schritt 15.1: Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf Routes (Routen). Schritt 15.2. Klicken Sie für jede Routing-Tabelle auf Routing-Tabelle laden. Schritt 15.3. Wählen Sie die Datei aus, die Sie in Schritt 8 exportiert haben. Schritt 15.4: Klicken Sie auf Senden. Schritt 15.5. Bestätigen Sie die Änderungen.
Schritt 16: Konfigurieren der DNS-Einstellungen Anmerkung: Wenn Sie beim Importieren der Konfiguration die Netzwerkeinstellungen laden, fahren Sie mit Schritt 17 fort.	Schritt 16.1. Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf DNS. Schritt 16.2. Klicken Sie auf Einstellungen bearbeiten. Schritt 16.3. Verwenden Sie den Screenshot aus Schritt 9 Schritt 16.4. Klicken Sie auf Senden. Schritt 16.5. Bestätigen Sie die Änderungen.
Schritt 17: Treten Sie dem SWA beim Active Directory bei bzw. treten Sie erneut bei.	Schritt 17.1. Navigieren Sie in der GUI zu Netzwerk, und klicken Sie auf Authentifizierung. Schritt 17.2: 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 17.3. Klicken Sie auf Join Domain (Domäne beitreten), und geben Sie die Anmeldeinformationen ein:

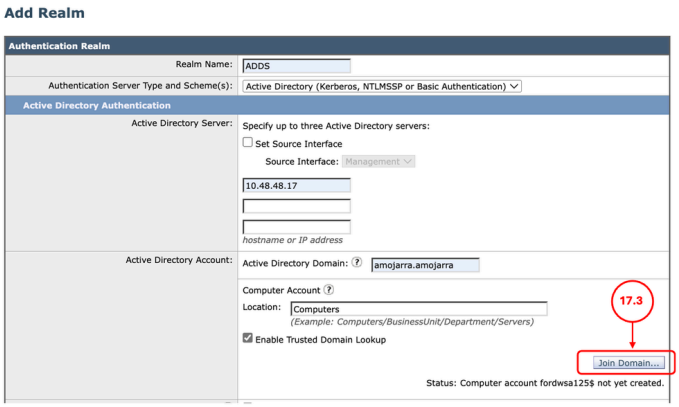


Bild - Join to Active Directory

Schritt 17.4: Klicken Sie auf Senden.

Schritt 17.5: Wenn die Verschlüsselung der Anmeldeinformationen aktiviert ist, importieren Sie das Zertifikat für die sichere Authentifizierung.

Schritt 17.6. Stellen Sie sicher, dass der Umleitungshostname korrekt ist.

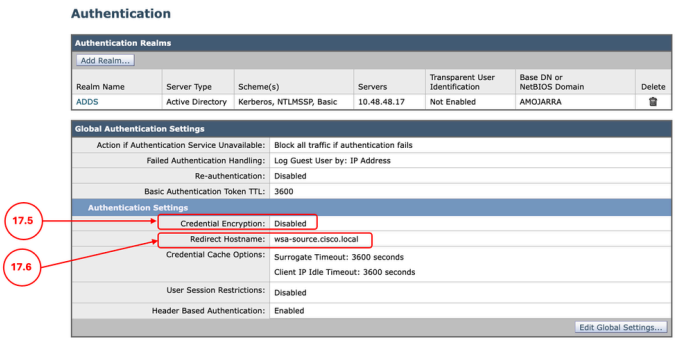


Bild - Authentifizierungseinstellungen

Schritt 17.7. Bestätigen Sie die Änderungen.

Zugehörige Informationen

- Bedienungsanleitung für AsyncOS 15.2 für Cisco Secure Web Appliance
- Ersteinrichtung der sicheren Web-Appliance
- Best Practices für sichere Web-Appliances
- Zugreifen auf Protokolle der sicheren Web-Appliance

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.