

Lokales SWA-, ESA- und SMA-Upgrade konfigurieren und Fehlerbehebung durchführen

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Voraussetzungen](#)

[Verwendete Komponenten](#)

[Lokales Upgrade](#)

[Fehlerbehebung](#)

[Manifest konnte nicht heruntergeladen werden](#)

[Fehler beim Herunterladen der Upgrade-Liste](#)

[Download-Fehler, Upgrade ohne Erfolg beendet](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird das Szenario für das Upgrade und die Fehlerbehebung bei lokalen Upgrades für Cisco Secure Web Appliance (SWA) und E-Mail Security Appliance (ESA) beschrieben.

Hintergrundinformationen

Aufgrund von Versionsbeschränkungen oder internen Richtlinien, die zu eingeschränktem Zugriff auf das Internet für sichere E-Mail- und Web-Verwaltungs-Appliances (SMA) führen, bietet Cisco eine alternative Lösung zum Herunterladen des Upgrade-Images und zum lokalen Upgrade der Appliance.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Administratorzugriff auf SWA, ESA, SMA.
- Grundkenntnisse der Webserverkonfiguration.
- Webserver, auf den von SWA zugegriffen werden kann

Verwendete Komponenten

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

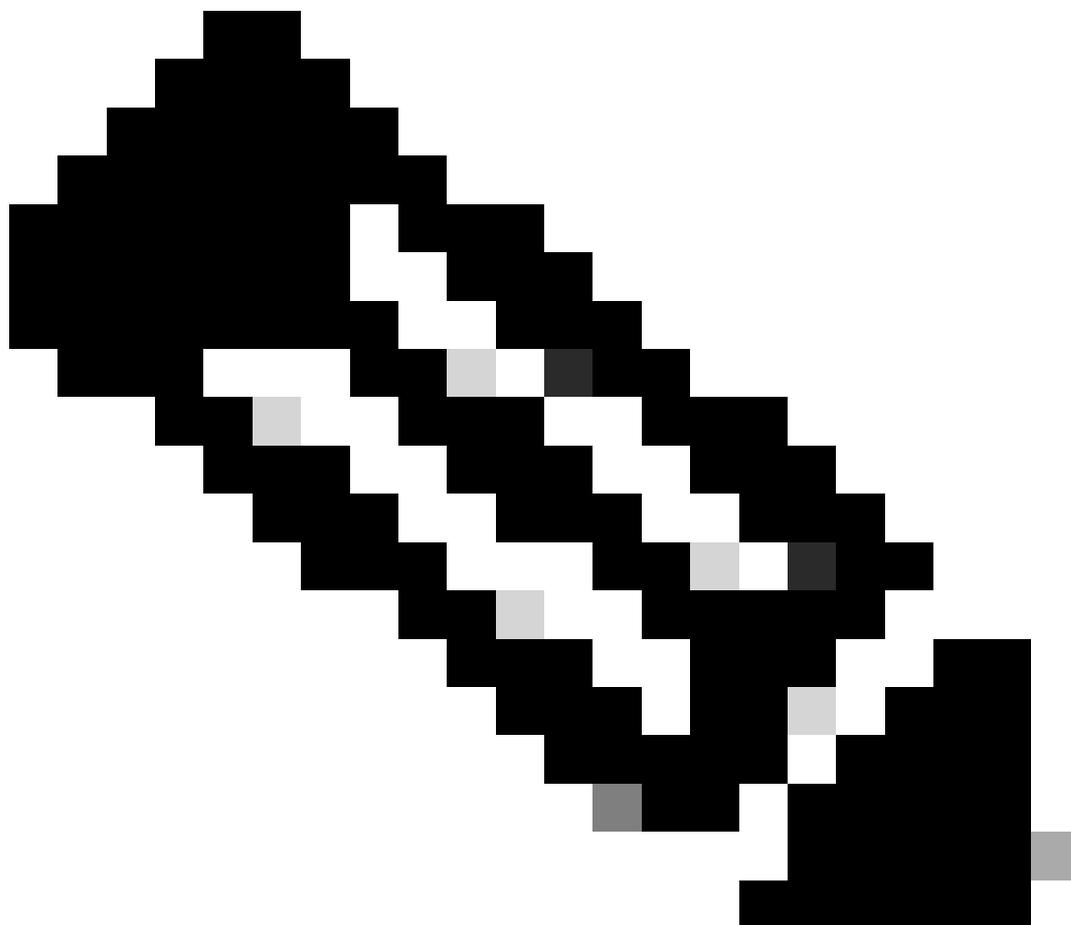
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Lokales Upgrade

Schritt 1: Laden Sie die gewünschte Paketdatei für das Versionsupgrade herunter.

Schritt 1.1: Navigieren Sie zum [Abrufen eines lokalen Upgrade-Images](#).

Schritt 1.2: Geben Sie die entsprechende(n) Seriennummer(n) für physische Geräte oder die virtuelle Lizenznummer (VLN) und das Modell für virtuelle Appliances ein.



Hinweis: Sie können die Seriennummern durch Kommas trennen, wenn mehrere Nummern vorhanden sind.

Schritt 1.3: Geben Sie unter Basisfreigabetag die aktuelle Version des Appliance-Felds in folgendem Format ein:

Für SWA: coeus-x-x-xxx-Beispiel: coeus-15.0.0-355

Für ESA: phoebe-x-x-x-xxx (Beispiel: phoebe-15-0-0-104)

Für SMA: zeus-x-x-x-xxx (Beispiel: zeus-15-0-0-334)

This page will allow you to fetch a local upgrade image.

The device serial, release tag and model can be determined by logging into the CLI and typing "version".

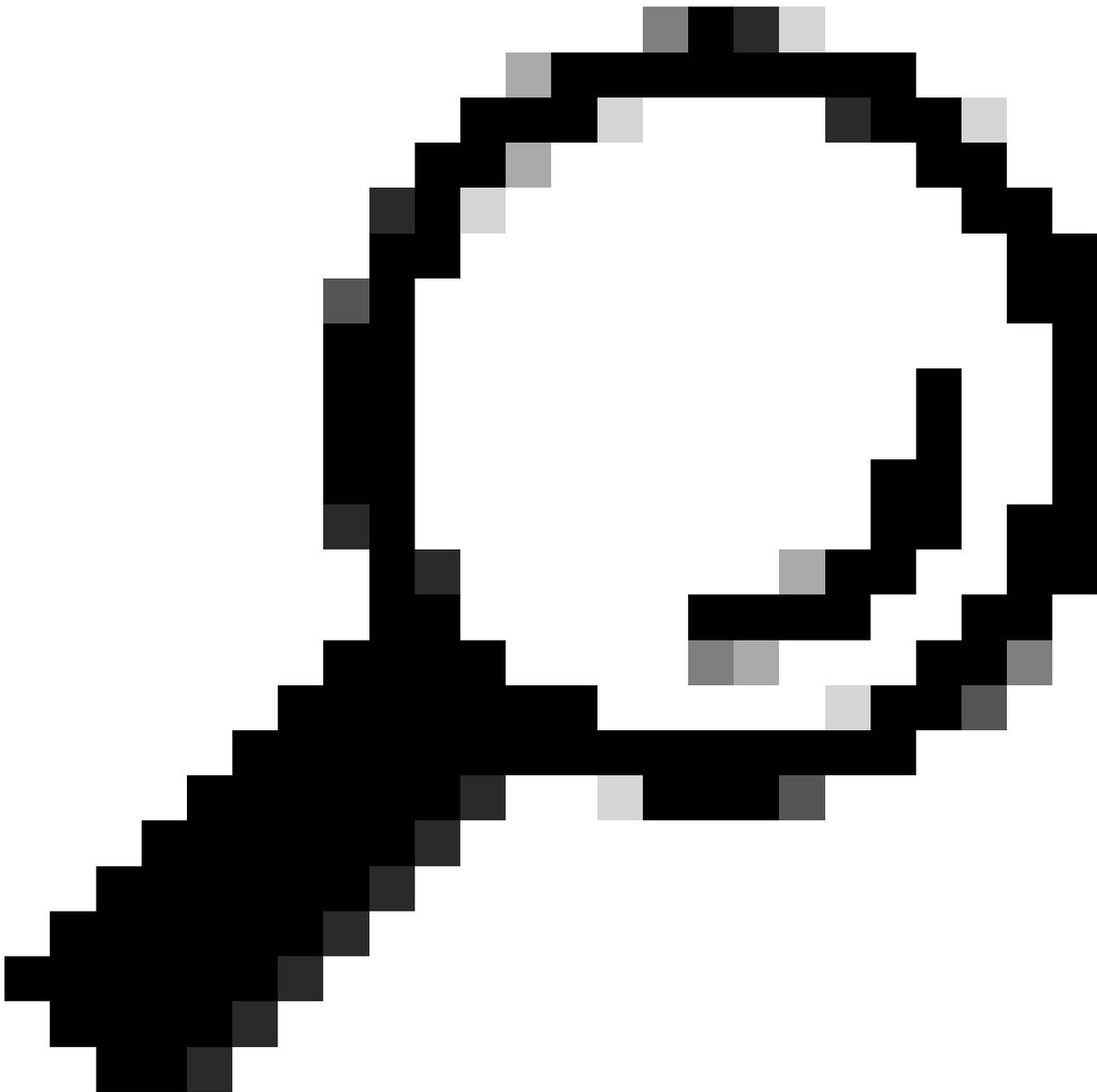
Serial number(s) (separated by commas, only required for hardware appliances):

Virtual license number (only required for virtual appliances):

Model (only required for virtual appliances):

Base release tag (required):

Image: Geben Sie die aktuellen Appliance-Details ein.



Tipp: Um die VLN virtueller Appliances zu finden, können Sie den Befehl "showlicense" über die Befehlszeilenschnittstelle (CLI) verwenden.

Schritt 1.4: Klicken Sie auf Manifest abrufen, um die Liste der verfügbaren Upgrades anzuzeigen.

Schritt 1.5: Laden Sie die gewünschte Version herunter.

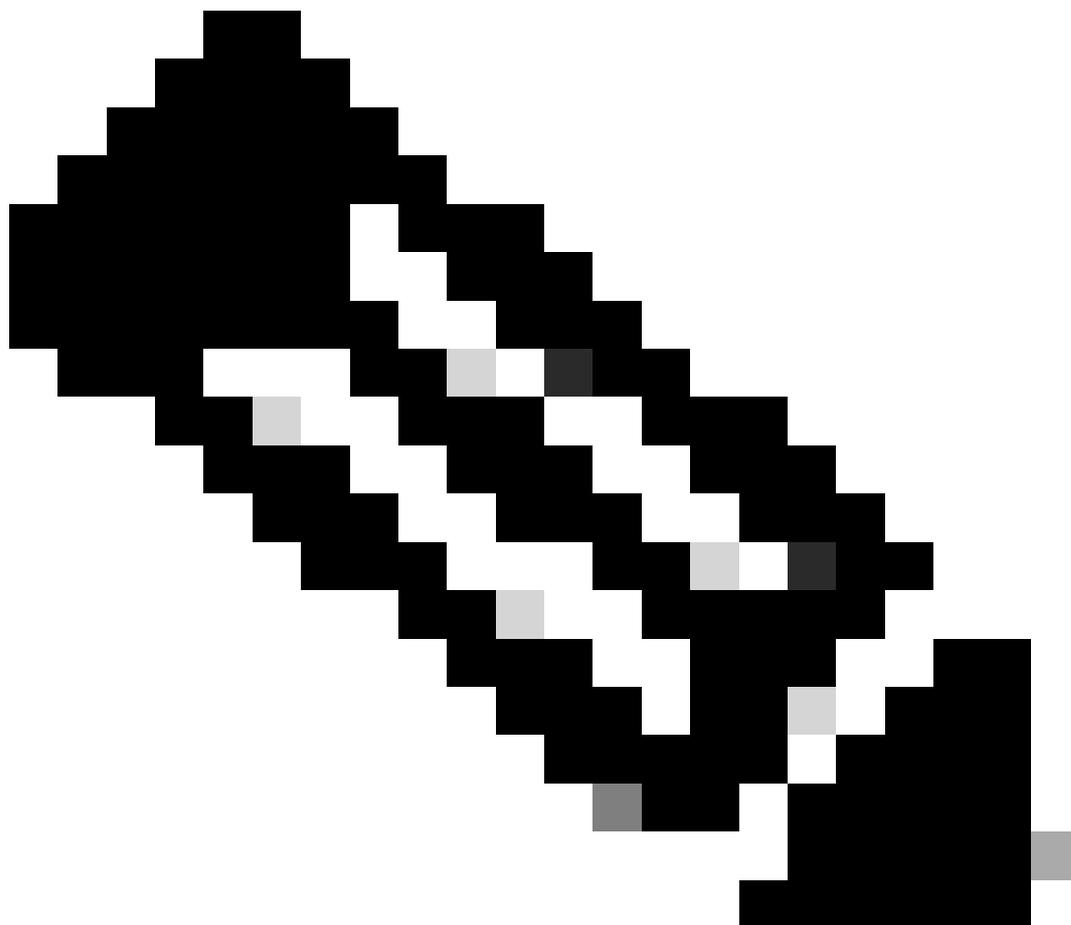
Schritt 2. Extrahieren Sie die heruntergeladene Datei und kopieren Sie sie auf Ihren Webserver.

Schritt 3: Stellen Sie sicher, dass die Datei- und Verzeichnisstruktur coeus-x-x-x-xxx.xml von Ihrer SWA-Appliance aus zugänglich ist.

```
asyncos/coeus-x-x-x-xxx.xml/app/default/1
asyncos/coeus-x-x-x-xxx.xml/distroot/default/1
asyncos/coeus-x-x-x-xxx.xml/hints/default/1
asyncos/coeus-x-x-x-xxx.xml/scannerroot/default/1
asyncos/coeus-x-x-x-xxx.xml/upgrade.sh/default/1
```

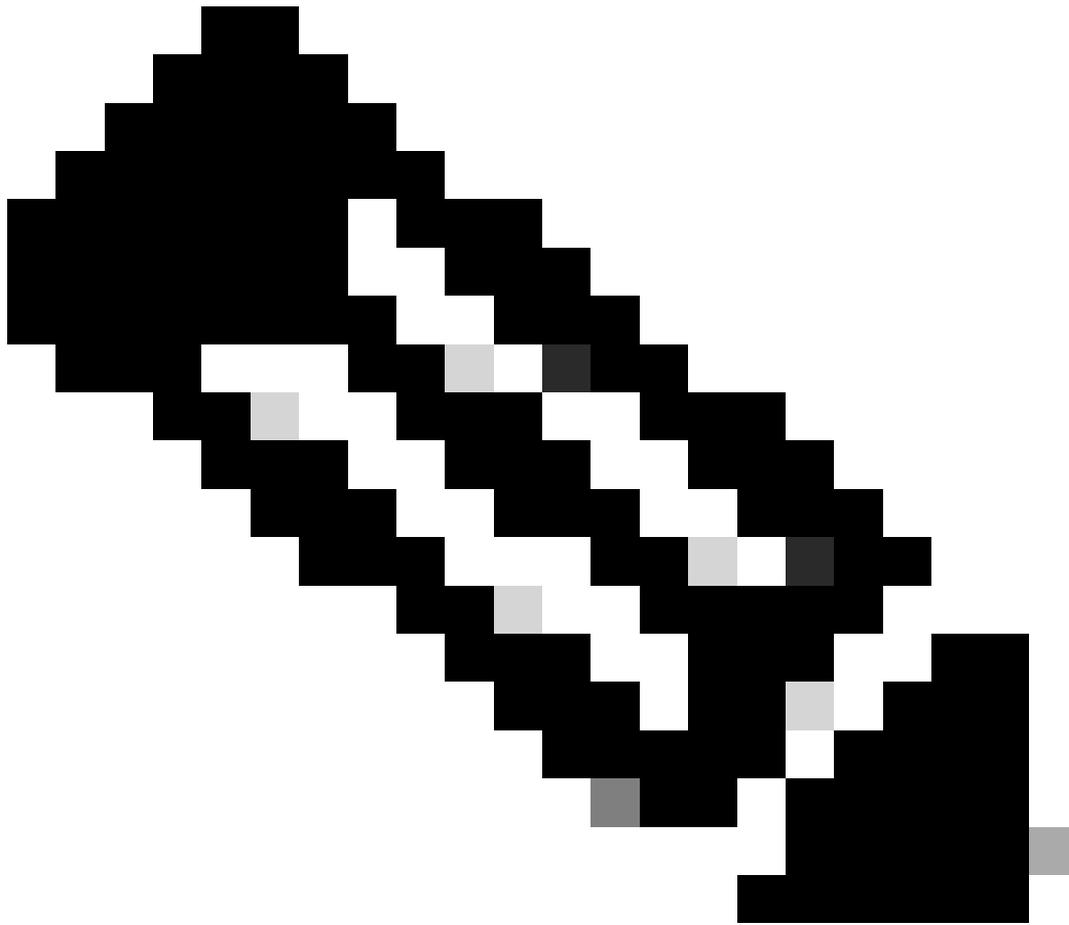
Schritt 4: Navigieren Sie zu Systemverwaltung >Einstellungen für Aktualisierung und Aktualisierung, und wählen Sie Aktualisierungseinstellungen bearbeiten aus.

Schritt 5: Wählen Sie Lokale Aktualisierungsserver aus, und geben Sie den vollständigen URL für die Manifestdatei ein: <http://YourWebserverAddress/asyncos/coeus-14-5-1-008.xml>



Hinweis: Die Manifestdatei ist eine .xml-Datei im asyncos-Ordner.

Schritt 6: Wählen Sie in Update Servers (images) configuration die Option Local Update Servers (Lokale Aktualisierungsserver). Ändern Sie die Base URL-Einstellungen (IronPort AsyncOS-Upgrades) auf Ihren lokalen Upgrade-Server und die entsprechende Portnummer.



Hinweis: Wenn Ihr Webserver für die Authentifizierung konfiguriert ist, können Sie die Anmeldeinformationen im Abschnitt Authentifizierung festlegen.

Routing Table:	Management
Update Servers (list):	<p>The URL will be used to obtain the list of available updates for the following services:</p> <ul style="list-style-type: none"> - Cisco AsyncOS upgrades - HTTPS Proxy Certificate Lists - How-Tos updates - Time zone rules - Web Reputation Filters
1	<input type="radio"/> Cisco Update Servers <input checked="" type="radio"/> Local Update Servers (location of list of available updates file)
	<p>Full Url: <input type="text" value="http://172.16.200.101/asyncos/coeus-14-5-1-008.xr"/> Port: <input type="text" value="80"/></p> <p><i>http://updates.example.com/my_updates.xml</i></p> <p>Authentication (optional):</p> <p>Username: <input type="text"/></p> <p>Passphrase: <input type="text"/></p> <p>Retype Passphrase: <input type="text"/></p>
Update Servers (images):	<p>The update servers will be used to obtain update images for the following services:</p> <ul style="list-style-type: none"> - Cisco AsyncOS upgrades - HTTPS Proxy Certificate Lists - How-Tos updates - Time zone rules - Web Reputation Filters
2	<input type="radio"/> Cisco Update Servers <input checked="" type="radio"/> Local Update Servers (location of update image files) ?
	<p>Base Url: <input type="text" value="http://172.16.200.101"/> Port: <input type="text" value="80"/></p> <p><i>http://downloads.example.com</i></p> <p>Authentication (optional):</p> <p>Username: <input type="text"/></p> <p>Passphrase: <input type="text"/></p> <p>Retype Passphrase: <input type="text"/></p>

Schritt 7. Änderungen senden und bestätigen.

Schritt 8: Klicken Sie auf Upgrade Options (Upgrade-Optionen), um die Liste der verfügbaren Versionen anzuzeigen.

System Upgrade

Upgrade System

*Click **Upgrade Options** to view and select the applicable options available for your appliance.*

Current AsyncOS Version:	11.8.1-023	
Current Upgrade Settings:	Update Server (list):	http://172.16.200.101/asyncos/coeus-14-5-1-008.xml
	Routing Table:	Management
	HTTP Proxy Server:	None
	HTTPS Proxy Server:	None

Upgrade Options... 1

Schritt 9. Wählen Sie die gewünschte Version aus und klicken Sie auf "Proceed" (Weiter):

Upgrade Options

Upgrade options

Choose any one upgrade option:

- Download and install
(Select from the list of available upgrade image files from upgrade server to download from, and install.)
- Download only
(Select from the list of available upgrade image files from upgrade server to download. You may use this image file to Install later.)

Most system upgrades require a reboot of the system after the upgrade is applied. Changes made to your system's configuration between the time the upgrade download is completed and the system is rebooted will not be saved.

Since version 11.8, the Next Generation portal of your appliance by default uses AsyncOS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can configure the HTTPS (4431) port using the trailblazerconfig command in the CLI. Make sure that the configured HTTPS port is opened on the firewall and ensure that your DNS server can resolve the hostname that you specified for accessing the appliance.

List of available upgrade images files at upgrade server:

- AsyncOS 14.5.1 build 008 upgrade For Web, 2023-01-12, is a release available for Maintenance Deployment

Upgrade Preparation:

- Save the current configuration to the configuration directory before upgrading.

Email file to:

Separate multiple addresses with commas.

- Plain passwords in the configuration file.
- Mask passwords in the configuration file.

Note: Files with masked passwords cannot be loaded using Load Configuration.

Schritt 10. Suchen Sie nach den Anweisungen auf der Seite System Upgrade (Systemaktualisierung).

Cisco S100V
Web Security Virtual Appliance

Web Security Appliance is getting a

System Upgrade

Overall Progress: 12%

Upgrade is running, please wait.

Current Task

Downloading application...

Copyright © 2003-2020 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

Fehlerbehebung

Sie können die Upgrade-Protokolle in der CLI anzeigen > grep > wählen Sie die Nummer, die den Upgrade-Protokollen zugeordnet ist.

Hier einige Beispiele für erfolgreiche Upgrades:

```
Wed Feb 18 04:08:12 2024 Info: Begin Logfile
Wed Feb 18 04:08:12 2024 Info: Version: 11.8.1-023 SN: 420D8120350A5CB03F1E-EEE6300DA0C4
Wed Feb 18 04:08:12 2024 Info: Time offset from UTC: 3600 seconds
Wed Feb 18 05:18:10 2024 Info: The SHA of the file hints is 5a9987847797c9193f8d0ba1c7ad6270587bcf82f1
Wed Feb 18 05:18:10 2024 Info: Download and installation of AsyncOS 14.5.1 build 008 upgrade For Web,
Wed Feb 18 05:18:10 2024 Info: The SHA of the file upgrade.sh is 41da10da137bb9a7633a5ced9636de239907
```

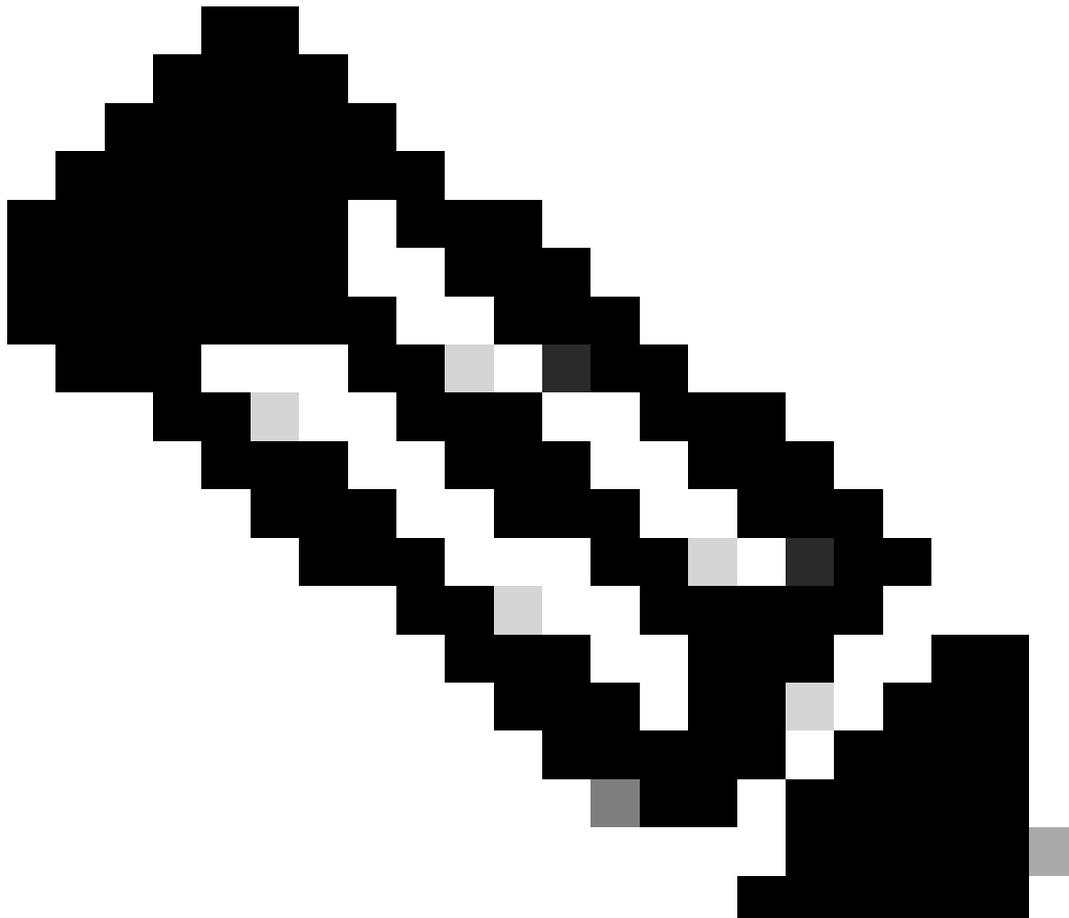
Manifest konnte nicht heruntergeladen werden

System Upgrade

Error — Could not download manifest.

Upgrade System		
<i>Click Upgrade Options to view and select the applicable options available for your appliance.</i>		
Current AsyncOS Version:	11.8.1-023	
Current Upgrade Settings:	Update Server (list):	http://172.16.200.101/asyncos/coeus-14-5-1-008.xml
	Routing Table:	Management
	HTTP Proxy Server:	None
	HTTPS Proxy Server:	None
Upgrade Options...		

Sie müssen sicherstellen, dass SWA auf die Dateien im Webserver zugreifen kann. Um die Verbindung zu überprüfen, können Sie den curl-Befehl aus der CLI verwenden.



Hinweis: Wenn Sie Direkt wählen, testet SWA die Verbindung vom Betriebssystem und nicht vom Proxydienst.

SWA_CLI> curl

Choose the operation you want to perform:

- DIRECT - URL access going direct
 - APPLIANCE - URL access through the Appliance
- [>] direct

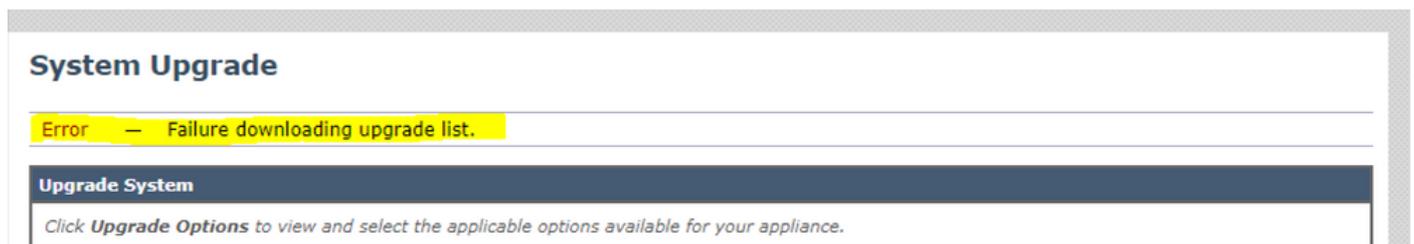
Do you wish to choose particular interface of appliance?

[N]>

Enter URL to make request to

[>] http://172.16.200.101/asyncos/coeus-14-5-1-008.xml

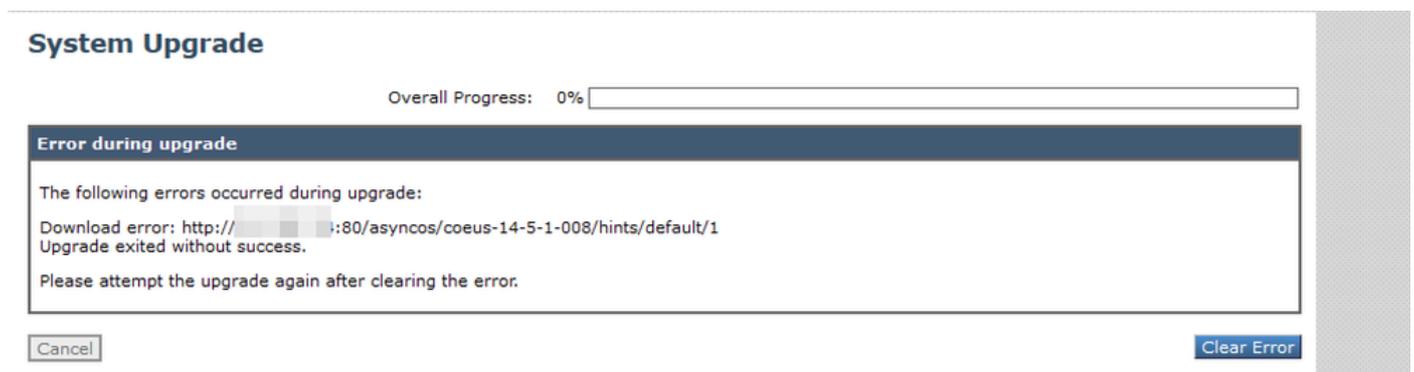
Fehler beim Herunterladen der Upgrade-Liste



Überprüfen Sie zunächst die Verbindung zwischen SWA und dem Upgrade-Server. Sie können den Befehl curl wie erwähnt verwenden.

Wenn die Verbindung einwandfrei war, überprüfen Sie die VLN- oder Seriennummer der Manifestdatei, um sicherzustellen, dass sie mit dem Gerät übereinstimmen. Sie können die .xml-Datei öffnen und nach dem <keys>Tag suchen.

Download-Fehler, Upgrade ohne Erfolg beendet



Stellen Sie sicher, dass Sie die Berechtigung auf Ihrem Webserver richtig konfiguriert haben.

Zugehörige Informationen

[Warum erhalte ich beim Upgrade die Fehlermeldung Fehler beim Herunterladen der Upgrade-Liste? "Fehler beim Durchführen des Upgrades: E/A-Fehler"? - Cisco](#)

[Upgrade-Prozess für sichere Web-Appliance - Cisco](#)

[Upgrade der E-Mail Security Appliance \(ESA\) mit Benutzeroberfläche oder Kommandozeile - Cisco](#)

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.