

Configure and Troubleshoot SWA, ESA and SMA Local Upgrade

Contents

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[Components Used](#)

[Local Upgrade](#)

[Troubleshoot](#)

[Could not download manifest](#)

[Failure downloading upgrade list](#)

[Download error.Upgrade exited without success](#)

[Related Information](#)

Introduction

This document describes the scenario to Upgrade and troubleshoot Cisco Secure Web Appliance (SWA), Email Security Appliance (ESA) local upgrade.

Background Information

Due to version restrictions or internal policy which leads to limited access to Internet for secure Email and Web Management Appliance (SMA), Cisco provides alternate solution to download the upgrade image and locally upgrade the appliance.

Prerequisites

Cisco recommends that you have knowledge of these topics:

- Admin access to SWA, ESA, SMA.
- Basic knowledge of web server configuration.
- Web Server accessible from SWA.

Components Used

This document is not restricted to specific software and hardware versions.

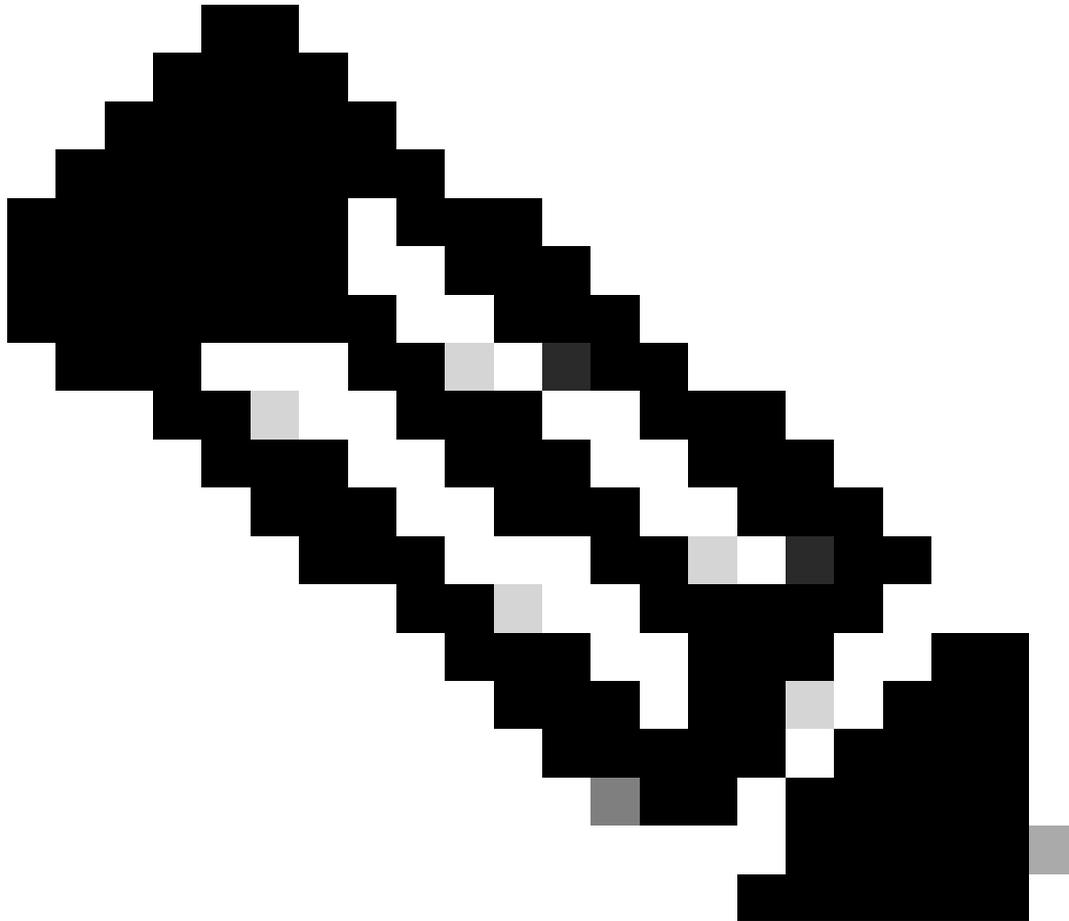
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Local Upgrade

Step 1. Download the desired version upgrade package file.

Step 1.1. Navigate to [Fetch a Local Upgrade Image](#)

Step 1.2. Enter the associated serial number(s) for physical devices or Virtual License Number (VLN) and Model for virtual appliances.



Note: You can separate the serial numbers with commas if there is more than one.

Step 1.3. In the Base Release Tag, enter the current version of the appliance field in this format:

For SWA: coeus-x-x-x-xxx (Example: coeus-15.0.0-355)

For ESA: phoebe-x-x-x-xxx (Example: phoebe-15-0-0-104)

For SMA: zeus-x-x-x-xxx (Example: 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".

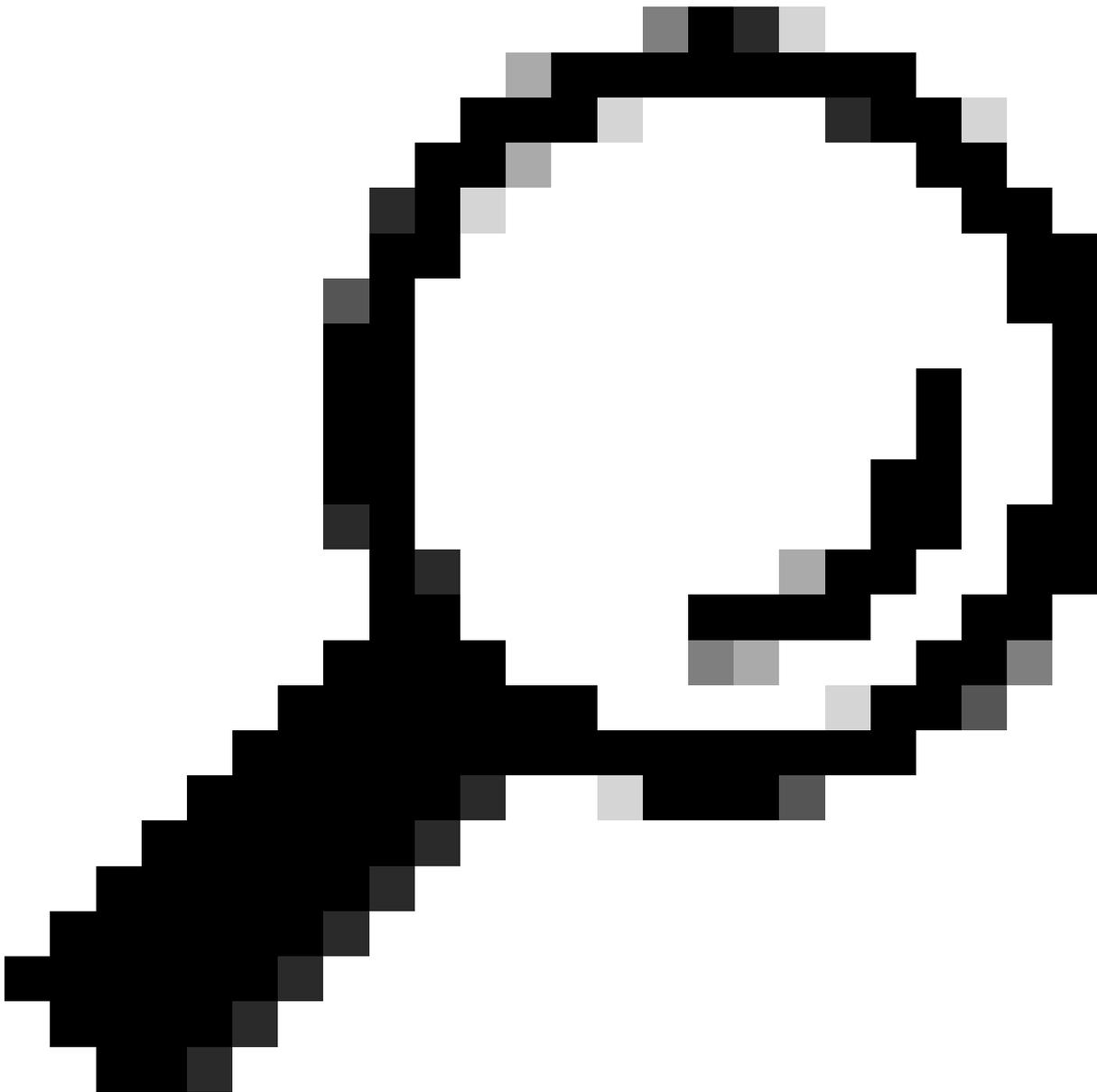
Serial number(s) (separated by commas, only required for hardware appliances):

Virtual license number (only required for virtual appliances):

Model (only required for virtual appliances):

Base release tag (required):

Image- Enter the Current Appliance Details



Tip: To find the VLN of virtual appliances, you can use "**showlicense**" command from Command Line Interface (CLI).

Step 1.4. Click Fetch manifest to view the list of available upgrades.

Step 1.5. Download the desire version.

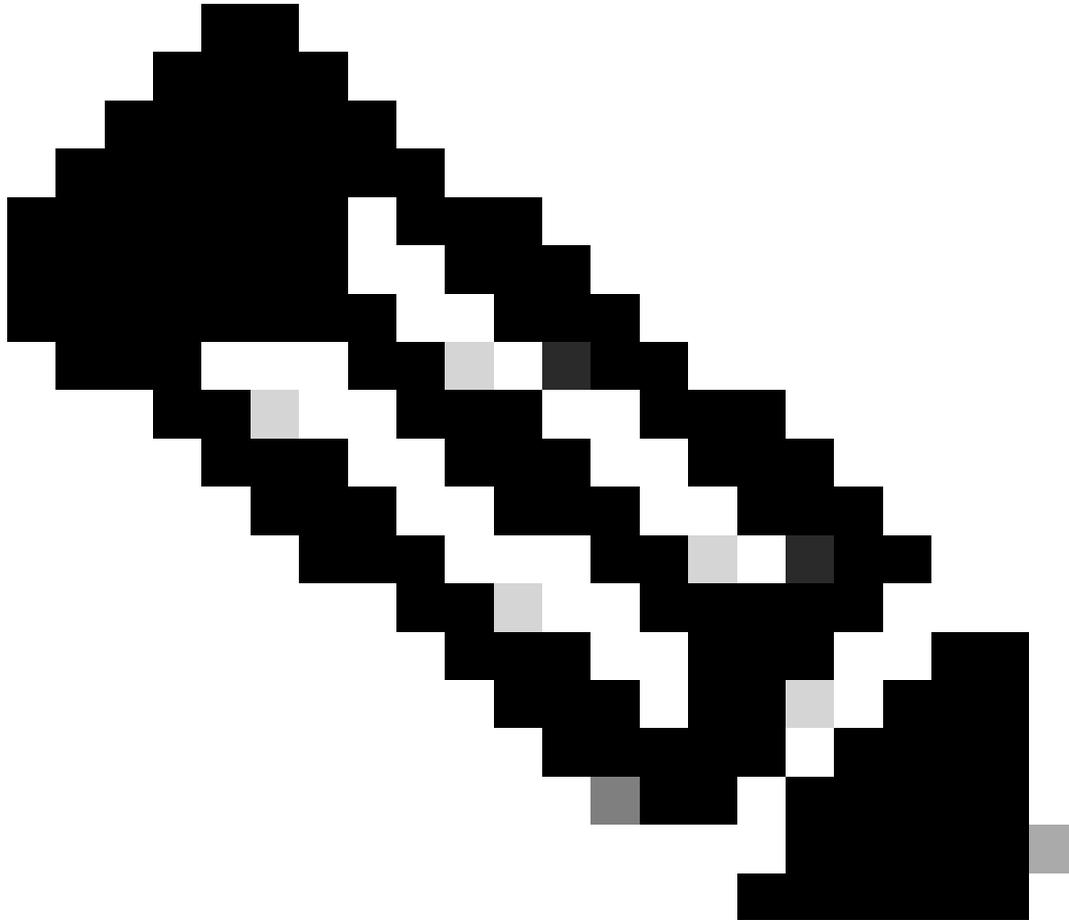
Step 2. Extract the downloaded file and copy to your Web server.

Step 3. Verify that the coeus-x-x-x-xxx.xml file and directory structure is accessible from your SWA appliance

```
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
```

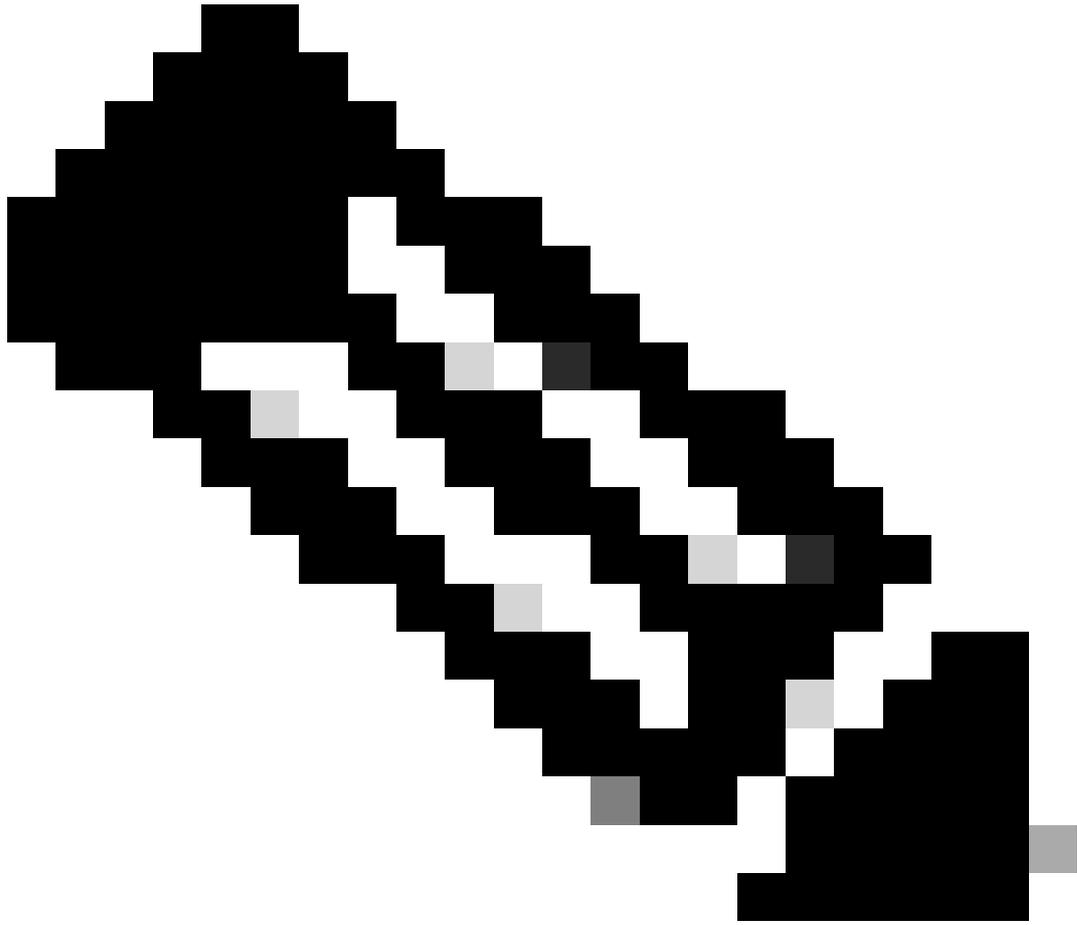
Step 4. Navigate to **System Administration >Upgrade and Update Settings** and choose **Edit Update Settings**.

Step 5. Select **Local Update Servers**, and enter the full URL for the manifest file <http://YourWebserverAddress/asyncos/coeus-14-5-1-008.xml>



Note: Manifest file is **.xml** file located in **asyncos** folder

Step 6. In **Update Servers (images)** configuration, choose **Local Update Servers**. Change the **Base URL (IronPort AsyncOS upgrades)** settings to your local upgrade server and appropriate port number.



Note: If your web server is configured for authentication, you can set the credentials in **Authentication** section.

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>

Step 7. Submit and commit changes.

Step 8. Click Upgrade Options to view the list of available versions.

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

Step 9. Choose the desired version and click "Proceed":

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.

Step 10. Check for the instructions on the **System Upgrade** page.

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](#)

Troubleshoot

you can view the upgrade logs from **CLI > grep >** choose the number associated with **Upgrade Logs**

Here is a sample logs of successful upgrade:

```

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

```

Could not download manifest

System Upgrade

Error — Could not download manifest.

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...](#)

You need to make sure SWA can access the files in web server, to check the connectivity, you can use **curl** command from **CLI**.

Note: When you choose Direct, SWA tests the connectivity from Operating system and not the proxy service.

```
SWA_CLI> curl
```

Choose the operation you want to perform:

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

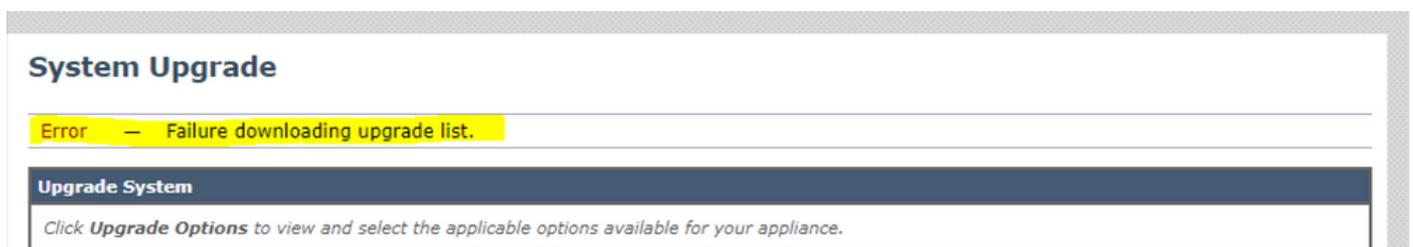
Do you wish to choose particular interface of appliance?

```
[N]>
```

Enter URL to make request to

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

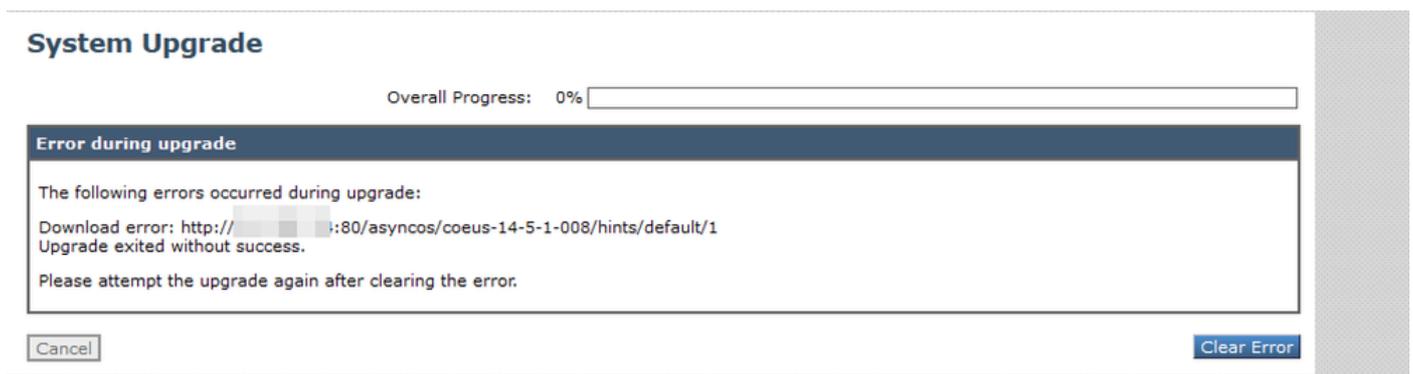
## Failure downloading upgrade list



First, verify the connectivity between SWA and upgrade server you can use the **curl** command as mentioned.

If the connectivity was fine, check the **VLN** or Serial number of the manifest file to make sure they are same as the device. you can open the **.xml** file and look for **<keys>** tag.

## Download error, Upgrade exited without success



Make sure you configured permission in your web server correctly.

## Related Information

[When attempting to upgrade, why do I get the error Failure downloading upgrade list. "Error performing upgrade: I/O error"? - Cisco](#)

[Upgrade Process for Secure Web Appliance - Cisco](#)

[Upgrade Email Security Appliance \(ESA\) with GUI or CLI - Cisco](#)