

# Upgrade SWA, ESA, SMA Locally

## Contents

---

[Introduction](#)

[Prerequisites](#)

[Components Used](#)

[Background Information](#)

[Upgrades for Appliances that Run AsyncOS Versions 10.0 and Later](#)

[Download the AsyncOS Upgrade](#)

[Upgrade the Appliance](#)

---

## Introduction

This document describes the process to upgrade Cisco Secure Web Appliance (SWA) and Cisco Email Security Appliance (ESA) locally.

## Prerequisites

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of SWA, ESA, SMA administration.
- Basic knowledge of web server configuration.

To perform the local upgrade you need:

- A Web Server accessible from SWA.
- Admin access to SWA, ESA or SMA.



**Note:** The local upgrade process only performs Async OS upgrades. it does NOT apply to service engine updates.

---

## Components Used

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.

## Background Information

At times, when the network is congested, attempts to upgrade the SWA or the ESA, SMA, via Internet can fail. For example, if there is an available upgrade for an appliance, the AsyncOS downloads it and installs it simultaneously. However, if the network is congested, the download can hang and the upgrade fails. In scenarios such as these, one available option is to upgrade the SWA or the ESA locally.

## Upgrades for Appliances that Run AsyncOS Versions 10.0 and

# Later

In order to upgrade appliances that run AsyncOS Versions 10.0 and later, you must download the AsyncOS upgrade and then apply it to the appliance from a local web server, such as Microsoft Internet Information System (IIS) or Apache server.

## Download the AsyncOS Upgrade

Complete these steps in order to download the AsyncOS upgrade:

**Step 1.** Navigate to the [Fetch a Local Upgrade Image](#) page.


**Step 2.** Enter the appropriate serial number(s) for physical devices or **VLN** and model for virtual devices. Separate the serial numbers with commas if there are more than one.

It must be a valid serial or **VLN**.

a) The machine it is downloaded for, must be the same as the one it is given to.

b) The manifest file holds a hash for the **VLN** or the serial number as part of the authentication process used offline

---

 **Note:** The device serial, release tag and model can be determined by logging into the CLI and typing "version". For virtual device **VLN** details use CLI command "**showlicense**".

---


**Step 3.** In the Base Release Tag field, enter the current version of the appliance with this format:

- For the SWA: **coeus-x-x-x-xxx** (coeus-10-5-1-296, for example)
- For the ESA: **phoebe-x-x-x-xxx** (phoebe-10-0-0-203, for example)
- For the SMA: **zeus-x-x-x-xxx** (zeus-10-1-0-037, for example)

Click **Fetch Manifest** to view the list of the possible upgrades for the specified serial number(s) or **VLN**.

**Step 4.** In order to download the upgrade, click the release package of the version to which you want to upgrade your appliance.

---

 **Note:** This package contains the necessary XML file inside of the zip file that is prepared for the serial number(s) that you entered.

---

**Step 5.** Extract the downloaded package on your Web server.

**Step 6.** Verify that the directory structure is accessible and looks similar to this:

### For the SWA

```
asyncos/coeus-10-5-1-296/app/default/1
asyncos/coeus-10-5-1-296/distroot/default/1
asyncos/coeus-10-5-1-296/hints/default/1
```

asyncos/coeus-10-5-1-296/scannerroot/default/1  
asyncos/coeus-10-5-1-296/upgrade.sh/default/1

## For the ESA

asyncos/phoebe-10-0-0-203/app/default/1  
asyncos/phoebe-10-0-0-203/distroot/default/1  
asyncos/phoebe-10-0-0-203/hints/default/1  
asyncos/phoebe-10-0-0-203/scannerroot/default/1  
asyncos/phoebe-10-0-0-203/upgrade.sh/default/1

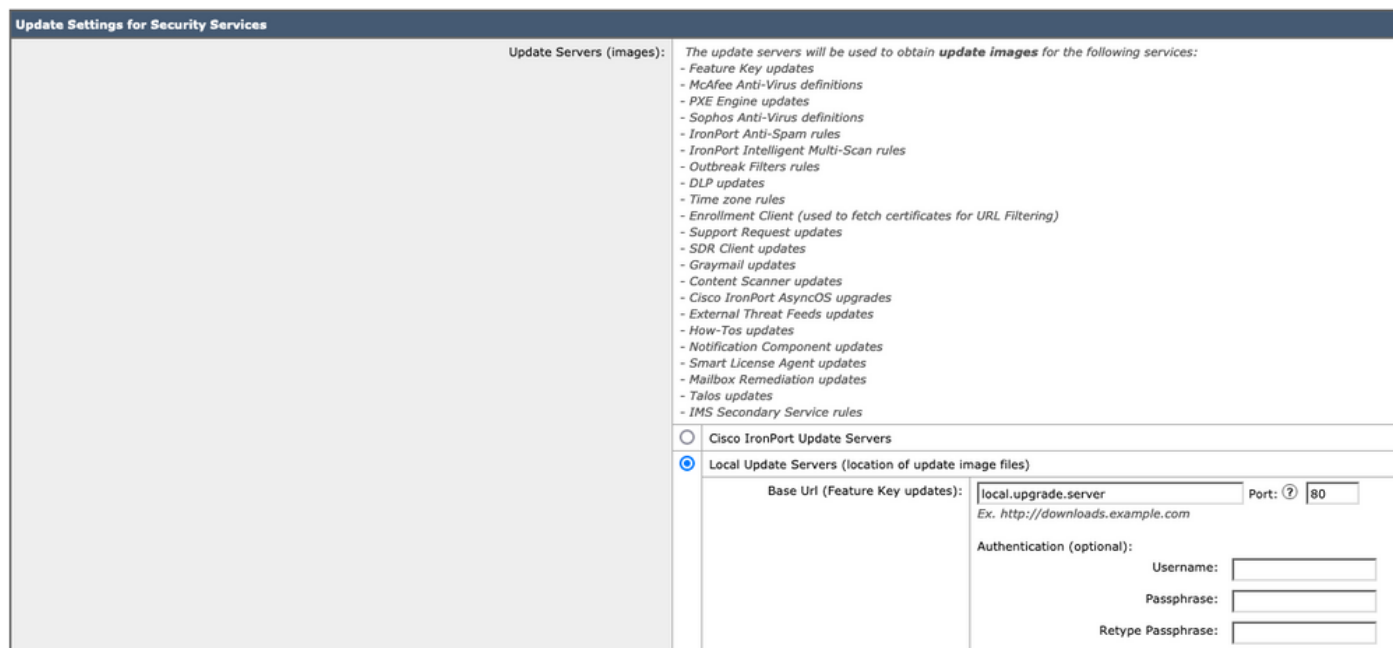
 **Note:** In this example, **10.5.1-296** for SWA and **10.0.0-203** for ESA are the target versions. You are not required to browse the directory at your HTTP server.

## Upgrade the Appliance

Complete these steps in order to configure the SWA, ESA to use the local upgrade server:

**Step 1.** Navigate to **Security Services > Service Updates** and click **Edit Update Settings**.

**Step 2.** Beside the **Update Servers (images)** configuration, click the **Local Update Servers** radio button. Change the **Base URL (IronPort AsyncOS upgrades)** setting to your local upgrade server and appropriate port (**local.upgrade.server:80**, for example).



**Update Settings for Security Services**

**Update Servers (images):** The update servers will be used to obtain **update images** for the following services:

- Feature Key updates
- McAfee Anti-Virus definitions
- PXE Engine updates
- Sophos Anti-Virus definitions
- IronPort Anti-Spam rules
- IronPort Intelligent Multi-Scan rules
- Outbreak Filters rules
- DLP updates
- Time zone rules
- Enrollment Client (used to fetch certificates for URL Filtering)
- Support Request updates
- SDR Client updates
- Graymail updates
- Content Scanner updates
- Cisco IronPort AsyncOS upgrades
- External Threat Feeds updates
- How-Tos updates
- Notification Component updates
- Smart License Agent updates
- Mailbox Remediation updates
- Talos updates
- IMS Secondary Service rules

Cisco IronPort Update Servers

Local Update Servers (location of update image files)

Base URL (Feature Key updates):  Port:

Ex. <http://downloads.example.com>

Authentication (optional):

Username:

Passphrase:

Retype Passphrase:

**Step 3.** Choose the **Local Update Servers** option beside the **Update Servers (list)** configuration and enter the full URL for the manifest file (<http://upgradeServer.local/asyncos/phoebe-10-0-3-003.xml>, for example).

Update Servers (list):	The URL will be used to obtain the <b>list of available updates</b> for the following services:																								
	<ul style="list-style-type: none"> <li>- McAfee Anti-Virus definitions</li> <li>- PXE Engine updates</li> <li>- Sophos Anti-Virus definitions</li> <li>- IronPort Anti-Spam rules</li> <li>- IronPort Intelligent Multi-Scan rules</li> <li>- Outbreak Filters rules</li> <li>- DLP updates</li> <li>- Time zone rules</li> <li>- Enrollment Client (used to fetch certificates for URL Filtering)</li> <li>- Support Request updates</li> <li>- SDR Client updates</li> <li>- Graymail updates</li> <li>- Content Scanner updates</li> <li>- External Threat Feeds updates</li> <li>- How-Tos updates</li> <li>- Notification Component updates</li> <li>- Smart License Agent updates</li> <li>- Mailbox Remediation updates</li> <li>- Talos updates</li> </ul>																								
	<input type="radio"/> Cisco IronPort Update Servers <input checked="" type="radio"/> Local Update Servers (location of list of available updates file)																								
	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%; border-bottom: 1px solid #ccc;">Full Uri</td> <td style="border-bottom: 1px solid #ccc;"><a href="http://local.upgrade.server/asyncos/phoet">http://local.upgrade.server/asyncos/phoet</a></td> <td style="width: 10%; border-bottom: 1px solid #ccc;">Port: ?</td> <td style="width: 20%; border-bottom: 1px solid #ccc; text-align: center;">80</td> </tr> <tr> <td colspan="4" style="font-size: x-small;">Ex. <a href="http://updates.example.com/my_updates.xml">http://updates.example.com/my_updates.xml</a></td> </tr> <tr> <td colspan="4">Authentication (optional):</td> </tr> <tr> <td></td> <td style="text-align: right;">Username:</td> <td colspan="2"><input style="width: 80%;" type="text"/></td> </tr> <tr> <td></td> <td style="text-align: right;">Passphrase:</td> <td colspan="2"><input style="width: 80%;" type="text"/></td> </tr> <tr> <td></td> <td style="text-align: right;">Retype Passphrase:</td> <td colspan="2"><input style="width: 80%;" type="text"/></td> </tr> </table>	Full Uri	<a href="http://local.upgrade.server/asyncos/phoet">http://local.upgrade.server/asyncos/phoet</a>	Port: ?	80	Ex. <a href="http://updates.example.com/my_updates.xml">http://updates.example.com/my_updates.xml</a>				Authentication (optional):					Username:	<input style="width: 80%;" type="text"/>			Passphrase:	<input style="width: 80%;" type="text"/>			Retype Passphrase:	<input style="width: 80%;" type="text"/>	
Full Uri	<a href="http://local.upgrade.server/asyncos/phoet">http://local.upgrade.server/asyncos/phoet</a>	Port: ?	80																						
Ex. <a href="http://updates.example.com/my_updates.xml">http://updates.example.com/my_updates.xml</a>																									
Authentication (optional):																									
	Username:	<input style="width: 80%;" type="text"/>																							
	Passphrase:	<input style="width: 80%;" type="text"/>																							
	Retype Passphrase:	<input style="width: 80%;" type="text"/>																							

**Step 4.** Once you are finished, submit and commit the changes.

**Step 5.** Use the normal upgrade process to download and install the image from the local server.