

# Processo di aggiornamento locale WSA/ESA

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Aggiornamenti per appliance con AsyncOS versione 10.0 e successive](#)

[Scarica l'aggiornamento di AsyncOS](#)

[Aggiornamento dell'accessorio](#)

## Introduzione

In questo documento viene descritto il processo utilizzato per aggiornare localmente Cisco Web Security Appliance (WSA) e Cisco Email Security Appliance (ESA).

Il processo di aggiornamento locale esegue solo **AsyncOS** aggiornamenti. lo fa *NON* applica a *aggiornamenti del service engine*.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza delle procedure di aggiornamento (online) degli standard Cisco WSA ed ESA.

### Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

AsyncOS versione 10.0 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

A volte, quando la rete è congestionata, i tentativi di aggiornare il WSA o l'ESA via Internet potrebbero non riuscire. Se ad esempio è disponibile un aggiornamento per un accessorio, AsyncOS lo scarica e lo installa contemporaneamente. Tuttavia, se la rete è congestionata, il download potrebbe interrompersi e l'aggiornamento non riesce. In scenari come questi, una delle opzioni disponibili è aggiornare il WSA o l'ESA localmente.

# Aggiornamenti per appliance con AsyncOS versione 10.0 e successive

Per aggiornare accessori che eseguono AsyncOS versione 10.0 e successive, è necessario scaricare l'aggiornamento AsyncOS e quindi applicarlo all'accessorio utilizzando un server IIS o Apache locale.

## Scarica l'aggiornamento di AsyncOS

Completare questa procedura per scaricare l'aggiornamento di AsyncOS:

1. Passare alla pagina [Recupera immagine di aggiornamento locale](#).
2. Immettere i numeri di serie appropriati per i dispositivi fisici o la VLAN e il modello per i dispositivi virtuali. Se i numeri di serie sono più di uno, separarli con una virgola.

Deve essere un ID seriale o VLAN valido

- a) La macchina per la quale viene scaricata deve essere la stessa a cui viene fornita.
- b) Il file manifest avrà un hash per la VLAN o il seriale come parte del processo di autenticazione utilizzato offline

**Nota:** il numero di serie, il tag di rilascio e il modello del dispositivo possono essere determinati accedendo alla CLI e digitando "version" (versione). Per i dettagli sulla VLAN del dispositivo virtuale, usare il comando CLI "show license".

3. Nel campo Codice di matricola versione di base, inserire la versione corrente dell'accessorio nel seguente formato:

- Per il WSA: **coeus-x-x-x-xxx** (ad esempio coeus-10-5-1-296)
- Per l'ESA: **phoebe-x-x-x-xxx** (ad esempio, phoebe-10-0-203)
- Per SMA: **zeus-x-x-x-xxx** (ad esempio, zeus-10-1-0-037)

Fare clic su **Fetch Manifest** per visualizzare un elenco dei possibili aggiornamenti per i numeri di serie o le VLAN specificati.

4. Per scaricare l'aggiornamento, fare clic sul pacchetto della versione a cui si desidera aggiornare l'accessorio.

**Nota:** Questo pacchetto contiene il file XML necessario all'interno del file zip preparato per i numeri di serie immessi.

5. Estrarre il pacchetto scaricato sul server HTTP.

6. Verificare che la struttura della directory sia accessibile e che abbia un aspetto simile al seguente:

## Per il WSA

```
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
```

## Per il SEC

```
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
```

**Nota:** Nell'esempio, le versioni target sono **10.5.1-296** per WSA e **10.0.0-203** per ESA. Non è necessario sfogliare la directory sul server HTTP.

## Aggiornamento dell'accessorio

Per configurare l'ESA in modo che utilizzi il server di aggiornamento locale, attenersi alla seguente procedura:

1. Selezionare **Security Services > Service Updates** e fare clic su **Edit Update Settings**.
2. Accanto alla configurazione **Server di aggiornamento (immagini)**, fare clic sul pulsante di opzione **Server di aggiornamento locale**. Modificare l'impostazione dell'**URL di base (aggiornamenti IronPort AsyncOS)** sul server di aggiornamento locale e sulla porta appropriata (ad esempio **local.upgrade.server:80**).

**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:

3. Scegliere l'opzione Server di **aggiornamento locale** accanto alla configurazione **Server di aggiornamento (elenco)** e immettere l'URL completo per il file manifesto (ad esempio, <http://local.upgrade.server/asyncos/phoebe-10-0-3-003.xml>).

Update Servers (list):	<p>The URL will be used to obtain the <i>list of available updates</i> for the following services:</p> <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)	
Full Uri <input type="text" value="http://local.upgrade.server/asyncos/phoebe-10-0-3-003.xml"/> Port: <input type="text" value="80"/>	
Ex. <a href="http://updates.example.com/my_updates.xml">http://updates.example.com/my_updates.xml</a>	
Authentication (optional):	
Username: <input type="text"/>	
Passphrase: <input type="text"/>	
Retype Passphrase: <input type="text"/>	

4. Al termine, sottomettere ed eseguire il commit delle modifiche.

5. Seguire il normale processo di aggiornamento per scaricare e installare l'immagine dal server locale.