

Processus de mise à niveau local WSA/ESA

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Mises à niveau pour les appliances qui exécutent AsyncOS versions 10.0 et ultérieures](#)

[Télécharger la mise à niveau AsyncOS](#)

[Mettre à niveau l'appareil](#)

Introduction

Ce document décrit le processus utilisé pour mettre à niveau localement l'appareil de sécurité Web (WSA) de Cisco et l'appareil de sécurité de la messagerie électronique (ESA) de Cisco.

Le processus de mise à niveau local ne fonctionne que **AsyncOS** mises à niveau. il le fait **NON** s'appliquer à *mises à jour du moteur de service*.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître les procédures de mise à niveau standard (en ligne) de Cisco WSA et ESA.

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

AsyncOS versions 10.0 et ultérieures.

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, make sure that you understand the potential impact of any command.

Informations générales

Parfois, lorsque le réseau est encombré, les tentatives de mise à niveau du WSA ou du ESA via Internet peuvent échouer. Par exemple, s'il existe une mise à niveau disponible pour une appliance, AsyncOS la télécharge et l'installe simultanément. Cependant, si le réseau est encombré, le téléchargement peut être interrompu et la mise à niveau échoue. Dans de tels scénarios, une option disponible est de mettre à niveau localement le WSA ou le ESA.

Mises à niveau pour les appliances qui exécutent AsyncOS versions 10.0 et ultérieures

Afin de mettre à niveau les appliances qui exécutent AsyncOS versions 10.0 et ultérieures, vous devez télécharger la mise à niveau AsyncOS, puis l'appliquer à l'appliance à l'aide d'un serveur IIS ou Apache local.

Télécharger la mise à niveau AsyncOS

Complétez ces étapes afin de télécharger la mise à niveau AsyncOS :

1. Accédez à la page [Récupérer une image de mise à niveau locale](#).
2. Saisissez le ou les numéros de série appropriés pour les périphériques physiques ou le VLAN et le modèle pour les périphériques virtuels. Séparez les numéros de série par des virgules s'il y en a plusieurs.

Il doit s'agir d'un ID de série ou de VLAN valide

a) La machine pour laquelle il est téléchargé doit être la même que celle à laquelle il est donné.

b) Le fichier manifest aura un hachage pour le VLAN ou la série dans le cadre du processus d'authentification utilisé hors connexion

Remarque : Vous pouvez déterminer la série, l'étiquette de version et le modèle du périphérique en vous connectant à l'interface de ligne de commande et en tapant « version ». Pour les détails VLN de périphérique virtuel, utilisez la commande CLI « showlicense ».

3. Dans le champ Base Release Tag, saisissez la version actuelle de l'appliance au format suivant :

- Pour le WSA : **coeus-x-x-x-xxx** (coeus-10-5-1-296, par exemple)
- Pour le SEEE : **phoebe-x-x-x-xxx** (phoebe-10-0-0-203, par exemple)
- Pour SMA : **zeus-x-x-x-xxx** (zeus-10-1-0-037, par exemple)

Cliquez sur **Récupérer le manifeste** afin d'afficher une liste des mises à niveau possibles pour le ou les numéros de série ou le VLAN spécifiés.

4. Afin de télécharger la mise à niveau, cliquez sur le package de version de la version vers laquelle vous voulez mettre à niveau votre appliance.

Note: Ce package contient le fichier XML nécessaire à l'intérieur du fichier zip préparé pour le ou les numéros de série que vous avez entrés.

5. Extrayez le package téléchargé sur votre serveur HTTP.

6. Vérifiez que la structure de répertoire est accessible et ressemble à ceci :

Pour 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
```

Pour l'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: Dans cet exemple, **10.5.1-296** pour WSA et **10.0.0-203** pour ESA sont les versions cibles. Vous n'avez pas besoin de parcourir le répertoire de votre serveur HTTP.

Mettre à niveau l'appareil

Complétez ces étapes afin de configurer l'ESA pour utiliser le serveur de mise à niveau local :

1. Accédez à **Services de sécurité > Mises à jour de service** et cliquez sur **Modifier les paramètres de mise à jour**.
2. En regard de la configuration des serveurs de mise à jour (images), cliquez sur la case d'option **Serveurs de mise à jour locaux**. Modifiez le paramètre **URL de base (mises à niveau IronPort AsyncOS)** sur votre serveur de mise à niveau local et le port approprié (**local.upgrade.server:80**, par exemple).

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. Choisissez l'option Serveurs de **mise à jour locale** en regard de la configuration **Serveurs de mise à jour (liste)** et entrez l'URL complète du fichier manifeste (<http://local.upgrade.server/asyncos/phoebe-10-0-3-003.xml>, par exemple).

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">- 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- External Threat Feeds updates- How-Tos updates- Notification Component updates- Smart License Agent updates- Mailbox Remediation updates- Talos updates
<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. http://updates.example.com/my_updates.xml	
Authentication (optional):	
Username: <input type="text"/>	
Passphrase: <input type="text"/>	
Retype Passphrase: <input type="text"/>	

4. Une fois que vous avez terminé, envoyez et validez les modifications.

5. Suivez le processus de mise à niveau normal pour télécharger et installer l'image à partir du serveur local.