

# WSA/ESA のローカル アップグレード プロセス

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[AsyncOS バージョン 10.0 以降を実行するアプライアンスのアップグレード](#)

[AsyncOS アップグレードのダウンロード](#)

[機器のアップグレード](#)

## 概要

このマニュアルについて説明します。Cisco Webセキュリティ アプライアンス ( WSA ) および Cisco 電子メール セキュリティ アプライアンス ( ESA ) をローカルにアップグレードする場合に使用されます。

ローカルアップグレードプロセスは次の処理のみを実行します **AsyncOS** アップグレード.これは **NOT** 適用する **サービスエンジンのアップデート**

## 前提条件

### 要件

Cisco WSA と ESA の標準 ( オンライン ) アップグレード手順に関する知識があることが推奨されます。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

AsyncOSバージョン10.0以降。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 背景説明

ネットワークで輻輳が発生していると、インターネットで WSA または ESA をアップグレードしようとしても失敗する可能性があります。たとえば、アプライアンスのアップグレードが使用可能になると、AsyncOS はそのアップグレードのダウンロードとインストールを同時に行います。ただし、ネットワークで輻輳が発生している場合、ダウンロードが停止してアップグレードが失

敗する可能性があります。このようなシナリオで使用できる 1 つのオプションは、WSA または ESA をローカルでアップグレードすることです。

## AsyncOS バージョン 10.0 以降を実行するアプライアンスのアップグレード

AsyncOSバージョン10.0以降を実行するアプライアンスをアップグレードするには、AsyncOSアップグレードをダウンロードし、ローカルIISまたはApacheサーバを使用してアプライアンスに適用する必要があります。

### AsyncOS アップグレードのダウンロード

AsyncOS アップグレードをダウンロードするには、次の手順を実行します。

1. [Fetch a Local Upgrade Image] [ページに移動します。](#)

2. 物理デバイスの適切なシリアル番号を入力するか、仮想デバイスのVLANとモデルを入力します。複数のシリアル番号が複数ある場合は、カンマで区切ります。

有効なシリアルIDまたはVLAN IDである必要があります

a)ダウンロード対象のマシンは、指定したものと同じでなければなりません。

b)manifestファイルには、オフラインで使用される認証プロセスの一部として、VLANまたはシリアルのハッシュが含まれます

注:デバイスのシリアル、リリースタグ、およびモデルは、CLIにログインし、「version」と入力することで確認できます。仮想デバイスのVLANの詳細については、CLIコマンド「showlicense」を使用します。

3. [Base Release Tag]フィールドに、アプライアンスの現在のバージョンを次の形式で入力します。

- WSA の場合 : **coeus-x-x-x-xxx** ( 例 : **oeus-10-5-1-296** )
- ESA の場合 : **phoebe-x-x-x-xxx** ( 例 : **phoebe-10-0-0-203** )
- SMA の場合 : **zeus-x-x-x-xxx** ( 例 : **zeus-10-1-0-037** )

[Fetch Manifest] をクリックすると、指定したシリアル番号またはVLANのアップグレードが可能なリストが表示されます。

4.アップグレードをダウンロードするには、アプライアンスをアップグレードするバージョンのリリースパッケージをクリックします。

注 : このパッケージには、入力したシリアル番号に対して用意されている ZIP ファイルの中に、必要な XML ファイルが含まれています。

5.ダウンロードしたパッケージをHTTPサーバから抽出します。

6.ディレクトリ構造がアクセス可能で、次のように表示されることを確認します。

## WSA の場合

```
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
```

## ESA の場合

```
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
```

注：この例では、WSAの10.5.1-296、ESAの10.0.0-203がターゲットバージョンです。  
HTTP サーバでは、ディレクトリを参照する必要はありません。

## 機器のアップグレード

ローカルアップグレードサーバを使用するESAを設定するには、次の手順を実行します。

1. [セキュリティサービス]>[サービスアップデート]に移動し、[更新設定の編集]をクリックします。
2. [Update Servers (images)]設定の横にある[Local Update Servers]ラジオボタンをクリックします。Base URL (IronPort AsyncOSのアップグレード)の設定をローカルアップグレードサーバと適切なポート(local.upgrade.server:80など)に変更します。

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): local.upgrade.server Port: 80  
Ex. http://downloads.example.com

Authentication (optional):

Username:

Password:

Retype Password:

3. [Update Servers (list)]構成の横にある[Local Update Server]オプションを選択し、マニフェストファイルの完全なURLを入力します(例えば<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 Url <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.完了したら、変更を送信して確定します。

5.通常のアップグレードプロセスに従って、ローカルサーバからイメージをダウンロードしてインストールします。