

# Processo de atualização local WSA/ESA

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Atualizações para dispositivos que executam AsyncOS versões 10.0 e posteriores](#)

[Faça o download da atualização do AsyncOS](#)

[Atualizar a ferramenta](#)

## Introduction

Este documento descreve o processo usado para atualizar o Cisco Web Security Appliance (WSA) e o Cisco Email Security Appliance (ESA) localmente.

O processo de atualização local só é executado **AsyncOS** atualizações. ele faz **NÃO** aplicar a *atualizações do mecanismo de serviço*.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento dos procedimentos de atualização do padrão Cisco WSA e ESA (on-line).

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

AsyncOS versões 10.0 e posteriores.

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.

## Informações de Apoio

Às vezes, quando a rede está congestionada, as tentativas de atualizar o WSA ou o ESA via Internet podem falhar. Por exemplo, se houver uma atualização disponível para um dispositivo, o AsyncOS faz o download dele e o instala simultaneamente. No entanto, se a rede estiver congestionada, o download poderá travar e a atualização falhará. Em cenários como esses, uma opção disponível é atualizar o WSA ou o ESA localmente.

# Atualizações para dispositivos que executam AsyncOS versões 10.0 e posteriores

Para atualizar os dispositivos que executam as versões 10.0 e posteriores do AsyncOS, você deve baixar a atualização do AsyncOS e aplicá-la ao dispositivo usando um servidor local IIS ou Apache.

## Faça o download da atualização do AsyncOS

Conclua estes passos para fazer o download da atualização do AsyncOS:

1. Navegue até a página [Buscar uma imagem de atualização local](#).
2. Insira os números de série apropriados para dispositivos físicos ou VLN e Modelo para dispositivos virtuais. Separe os números de série com vírgulas se houver mais de um.

Deve ser uma ID de série ou VLN válida

- a) A máquina para a qual o download foi feito deve ser a mesma para a qual foi feito.
- b) O arquivo manifest terá um hash para a VLN ou serial como parte do processo de autenticação usado offline

**Nota:** A série do dispositivo, a etiqueta de liberação e o modelo podem ser determinados fazendo login na CLI e digitando "version". Para detalhes de VLN do dispositivo virtual, use o comando CLI "showlicense".

3. No campo Etiqueta de versão básica, insira a versão atual do dispositivo com este formato:

- Para o WSA: **coeus-x-x-x-xxx** (coeus-10-5-1-296, por exemplo)
- Para o SEC: **phoebe-x-x-x-xxx** (phoebe-10-0-0-203, por exemplo)
- Para o SMA: **zeus-x-x-x-xxx** (zeus-10-1-0-037, por exemplo)

Clique em **Buscar Manifesto** para exibir uma lista de possíveis atualizações para o(s) número(s) de série especificado(s) ou VLN.

4. Para fazer o download da atualização, clique no pacote de versão da versão para a qual você deseja atualizar o aplicativo.

**Note:** Este pacote contém o arquivo XML necessário dentro do arquivo zip que está preparado para os números de série que você inseriu.

5. Extraia o pacote baixado no servidor HTTP.

6. Verifique se a estrutura do diretório está acessível e se tem aparência semelhante a esta:

**Para o 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
```

## Para o 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:** Neste exemplo, **10.5.1-296** para WSA e **10.0.0-203** para ESA são as versões de destino. Você não precisa navegar no diretório do servidor HTTP.

## Atualizar a ferramenta

Conclua estes passos para configurar o ESA para usar o servidor de atualização local:

1. Navegue para **Serviços de segurança > Atualizações de serviço** e clique em **Editar configurações de atualização**.
2. Ao lado da configuração **Atualizar servidores (imagens)**, clique no botão de opção **Local Update Server**. Altere a configuração **Base URL (atualizações do IronPort AsyncOS)** para o servidor de atualização local e a porta apropriada (**local.upgrade.server:80**, por exemplo).

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:   
Passphrase:   
Retype Passphrase:

3. Escolha a opção **Local Update Server** ao lado da configuração **Update Servers (list)** e insira o URL completo do arquivo de manifesto (<http://local.upgrade.server/asyncos/phoebe-10-0-3-003.xml>, por exemplo).

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>																	
	<p><input type="radio"/> Cisco IronPort Update Servers</p> <p><input checked="" type="radio"/> Local Update Servers (location of list of available updates file)</p> <table border="1"><tr><td>Full Uri</td><td><input type="text" value="http://local.upgrade.server/asyncos/phoet"/></td><td>Port: <input type="text" value="80"/></td></tr><tr><td colspan="3">Ex. http://updates.example.com/my_updates.xml</td></tr><tr><td colspan="3">Authentication (optional):</td></tr><tr><td></td><td>Username: <input type="text"/></td><td></td></tr><tr><td></td><td>Passphrase: <input type="text"/></td><td></td></tr><tr><td></td><td>Retype Passphrase: <input type="text"/></td><td></td></tr></table>	Full Uri	<input type="text" value="http://local.upgrade.server/asyncos/phoet"/>	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"/>
Full Uri	<input type="text" value="http://local.upgrade.server/asyncos/phoet"/>	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. Quando terminar, envie e confirme as alterações.

5. Siga o processo normal de atualização para baixar e instalar a imagem do servidor local.