

WSA/ESA lokaal upgrade-proces

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Uploads voor applicaties die AsyncOS-versies 10.0 en hoger uitvoeren](#)

[Download de AsyncOS-upgrade
upgrade van de applicatie](#)

Inleiding

Dit document beschrijft het proces dat wordt gebruikt om de Cisco web security applicatie (WSA) en de Cisco e-mail security applicatie (ESA) lokaal te verbeteren.

Het lokale upgradeproces wordt alleen uitgevoerd **AsyncOS** upgrades. het doet *NIET* aanvragen om *updates van de servicemodule*.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de Cisco WSA en ESA standaard (online) upgradeprocedures.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

AsyncOS-versies 10.0 en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Op bepaalde momenten, wanneer het netwerk verstopt is, kunnen pogingen om de WSA of de ESA via het internet te verbeteren mislukken. Als er bijvoorbeeld een beschikbare upgrade voor een apparaat beschikbaar is, wordt AsyncOS gedownload en tegelijkertijd geïnstalleerd. Als het netwerk echter verstopt is, kan de download ophangen en mislukt de upgrade. In dergelijke scenario's is één beschikbare optie de WSA of de ESA ter plaatse te verbeteren.

Uploads voor applicaties die AsyncOS-versies 10.0 en hoger uitvoeren

Om apparaten te upgraden die AsyncOS versies 10.0 en hoger uitvoeren, moet u de AsyncOS-upgrade downloaden en dan op het apparaat toepassen met een lokale IS- of Apache-server.

Download de AsyncOS-upgrade

Voltooi deze stappen om de AsyncOS-upgrade te downloaden:

1. Navigeer naar de [Facebook](#)-pagina [van de Afbeelding van lokale upgrade](#).
2. Voer het(de) juiste serienummer(s) in voor fysieke apparaten of VLN en model voor virtuele apparaten. Koppel de serienummers los met komma's als er meer dan één is.

Dit moet een geldig serienummer of een VLN-id zijn

a) De gedownload machine moet dezelfde zijn als de gedownload machine.

b) Het manifest-bestand heeft een hash voor de VLN of de serie als onderdeel van het offline gebruikte verificatieproces

Opmerking: Het seriële apparaat, de releasetag en het model kunnen worden bepaald door in de CLI te loggen en "versie" te typen. Gebruik voor VLN-details van virtueel apparaat de CLI-opdracht "showlicentie".

3. Voer in het veld Base release Tag de huidige versie van het apparaat in met deze indeling:

- Voor de WSA: **coeus-x-x-x-xxx** (coeus-10-5-1-296, bijvoorbeeld)
- Voor het ESR: **phoebe-x-x-x-xxx** (bijvoorbeeld phoebe-10-0-203)
- Voor de SMA: **zeus-x-x-x-xxx** (zeus-10-1-0-037, bijvoorbeeld)

Klik op **Facebook manipuleren** om een lijst met mogelijke upgrades te bekijken voor het opgegeven serienummer(s) of VLN.

4. Klik om de upgrade te downloaden op het vrijgavenpakket van de versie waaraan u uw apparaat wilt upgraden.

Opmerking: Dit pakket bevat het benodigde XML-bestand binnen het zip-bestand dat is bereid voor het (de) opgegeven serienummer(s).

5. Pak het gedownload pakket op uw HTTP server uit.

6. Controleer dat de telefoongidsstructuur toegankelijk is en er op lijkt:

Voor de 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
```

Voor het 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
```

Opmerking: In dit voorbeeld zijn **10.5.1-296** voor WSA en **10.0.0-203** voor ESA de doelversies. U hoeft niet in de map op uw HTTP-server te bladeren.

upgrade van de applicatie

Voltooi deze stappen om de ESA te configureren en de lokale upgradeserver te gebruiken:

1. Navigeer naar **Beveiligingsservices > Updates van de service** en klik op **Instellingen voor bijwerken**.
2. Klik naast **de configuratie van de servers (beelden)** op de radioknop **Local Update Servers**. Wijzig **de instelling van de basisURL (IronPort AsyncOS-upgrades)** aan uw lokale upgradeserver en juiste poort (**local.upgrade.server:80**, bijvoorbeeld).

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. Kies **de optie Local Update Servers** Option naast **de configuratie van de update servers (lijst)** en voer de volledige URL voor het manifest bestand (<http://local.upgrade.server/asyncos/phoebe-10-0-3-003.xml>, bijvoorbeeld) in.

Update Servers (list):	The URL will be used to obtain the list of available updates for the following services: <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/phoet"/> Port: <input type="text" value="80"/> <small>Ex. http://updates.example.com/my_updates.xml</small> Authentication (optional): Username: <input type="text"/> Passphrase: <input type="text"/> Retype Passphrase: <input type="text"/>

4. Nadat u klaar is, kunt u de wijzigingen indienen en doorgeven.

5. Volg het normale upgradeproces om de afbeelding te downloaden en te installeren vanaf de lokale server.