Configuración y solución de problemas de actualización local de SWA, ESA y SMA

Contenido

Introducción

Este documento describe el escenario para actualizar y resolver problemas de la actualización local de Cisco Secure Web Appliance (SWA), Email Security Appliance (ESA).

Antecedentes

Debido a las restricciones de versión o a la política interna que conduce a un acceso limitado a Internet para el dispositivo de administración de correo electrónico y web (SMA) seguro, Cisco proporciona una solución alternativa para descargar la imagen de actualización y actualizar localmente el dispositivo.

Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso de administrador a SWA, ESA y SMA.
- Conocimiento básico de la configuración del servidor web.
- Servidor web accesible desde SWA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

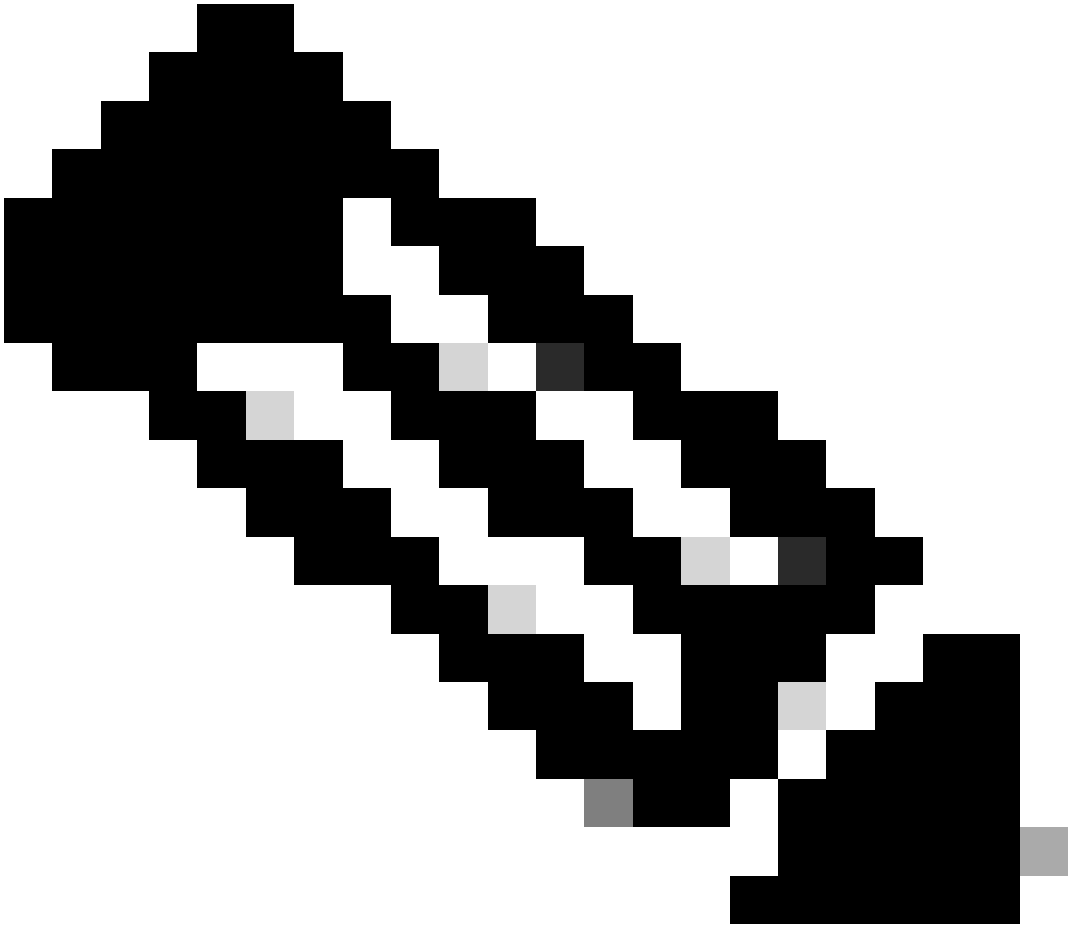
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Actualización local

Paso 1. Descargue el archivo del paquete de actualización de la versión que desee.

Paso 1.1. Vaya a Obtener una Imagen de Actualización Local

Paso 1.2. Introduzca los números de serie asociados para los dispositivos físicos o el número de licencia virtual (VLAN) y el modelo para los dispositivos virtuales.



Nota: Puede separar los números de serie con comas si hay más de uno.

Paso 1.3. En la etiqueta de versión base, introduzca la versión actual del campo del dispositivo

con el formato siguiente:

Para SWA: coeus-x-x-x-xxx (Ejemplo: coeus-15.0.0-355)
Para ESA: phoebe-x-x-x-xxx (ejemplo: phoebe-15-0-0-104)

Para SMA: zeus-x-x-x-xxx (Ejemplo: zeus-15-0-0-334)

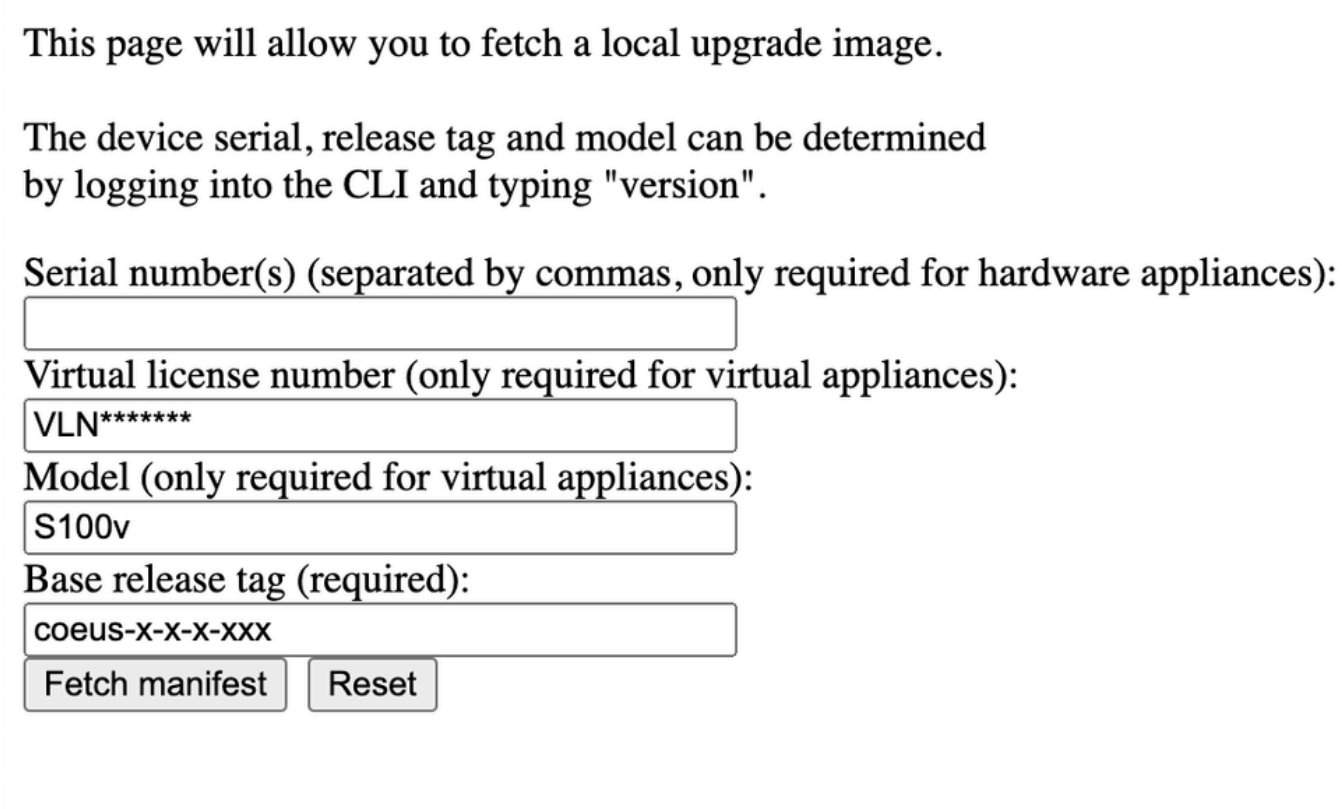
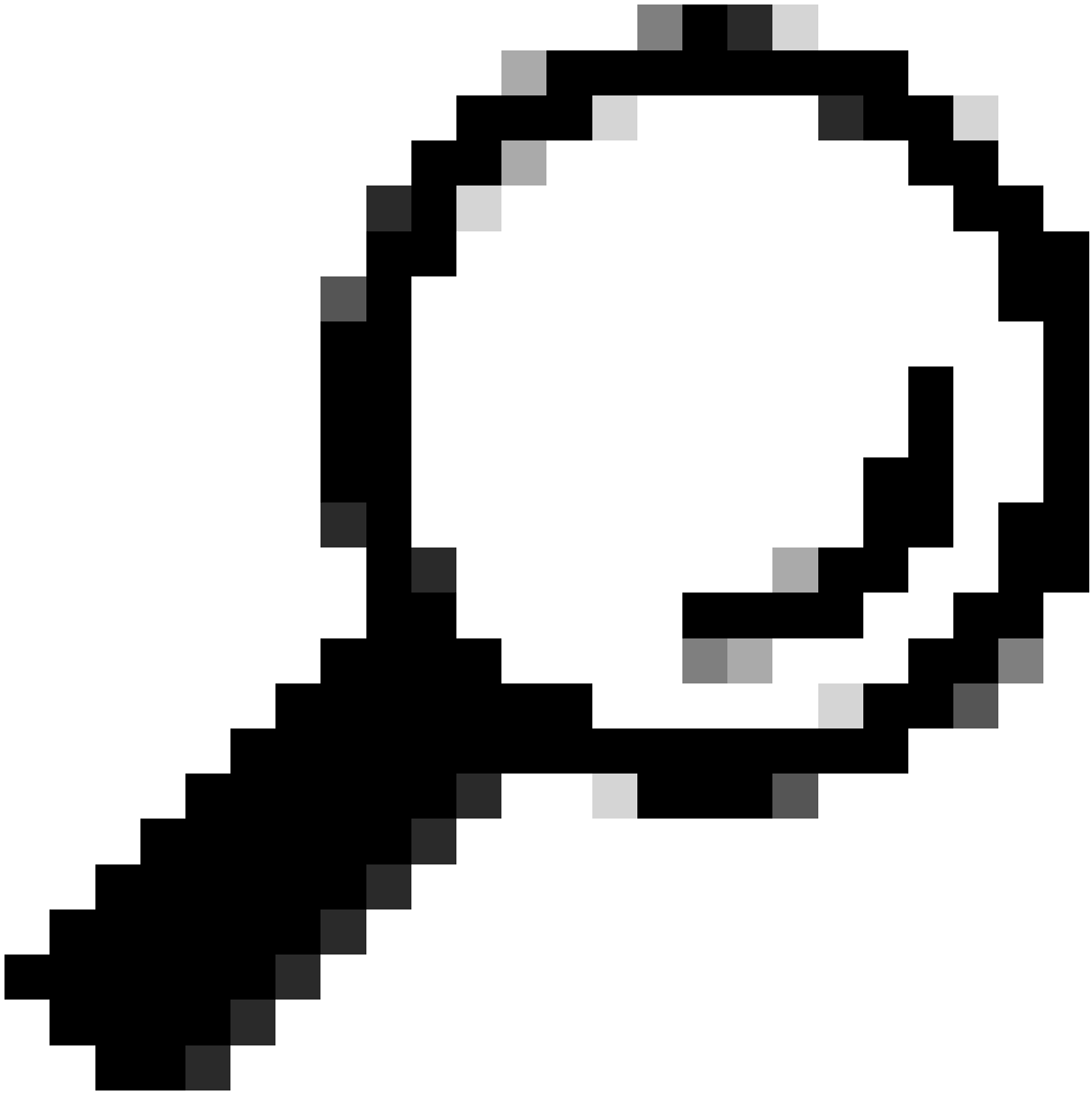


Imagen: introduzca los detalles del dispositivo actual



Sugerencia: para buscar la VLAN de los appliances virtuales, puede utilizar el comando "showlicense" de la interfaz de línea de comandos (CLI).

Paso 1.4. Haga clic en Recuperar manifiesto para ver la lista de actualizaciones disponibles.

Paso 1.5. Descargue la versión deseada.

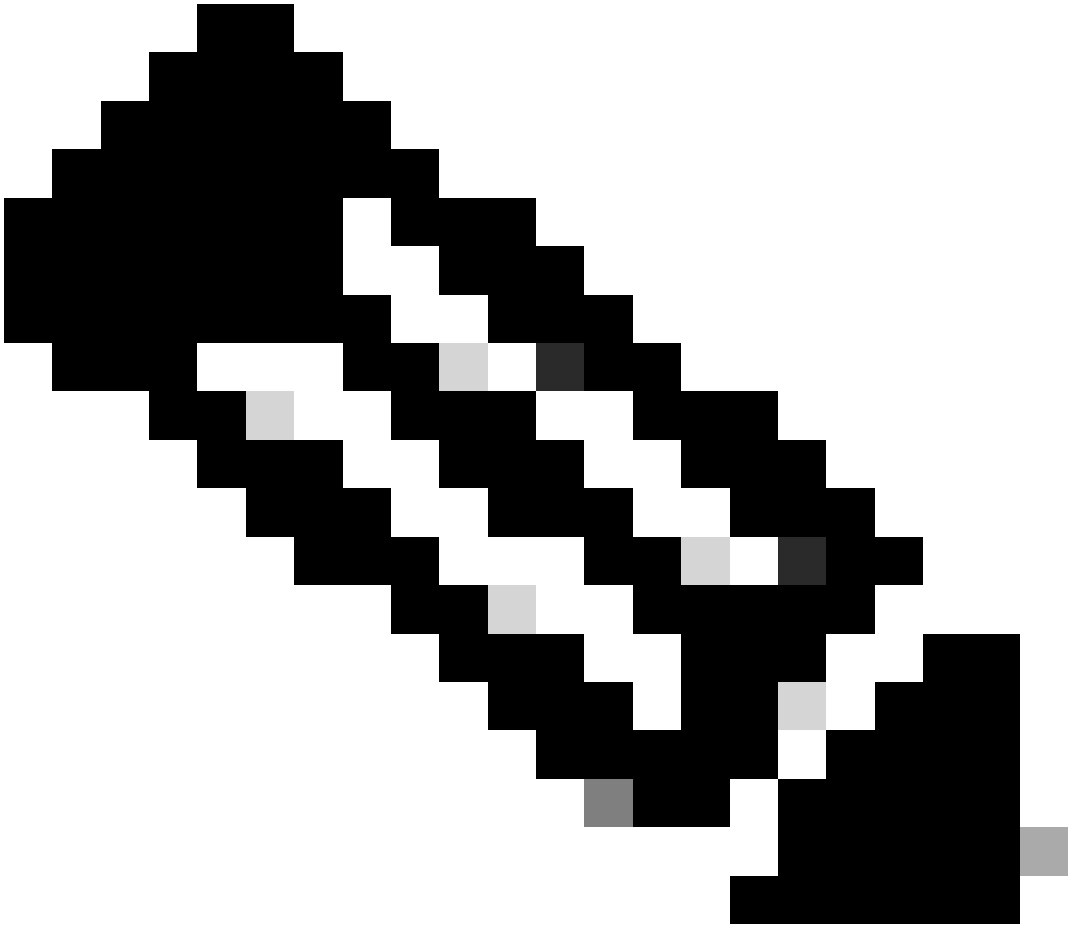
Paso 2. Extraiga el archivo descargado y cópielo en el servidor Web.
Paso 3. Verifique que el archivo coeus-x-x-x-xxx.xml y la estructura de directorios sean accesibles desde su dispositivo SWA

```
asyncos/coeus-x-x-x-xxx.xml/app/default/1
asyncos/coeus-x-x-x-xxx.xml/distroot/default/1
asyncos/coeus-x-x-x-xxx.xml/hints/default/1
asyncos/coeus-x-x-x-xxx.xml/scannerroot/default/1
asyncos/coeus-x-x-x-xxx.xml/upgrade.sh/default/1
```

Paso 4. Vaya a Administración del sistema >Configuración de actualización y actualización y elija Editar configuración de actualización.

Paso 5. Seleccione Servidores de actualización local e ingrese la URL completa para el archivo de manifiesto http://YourWebserverAddress/asyncos/coeus-14-5-1-008.xml

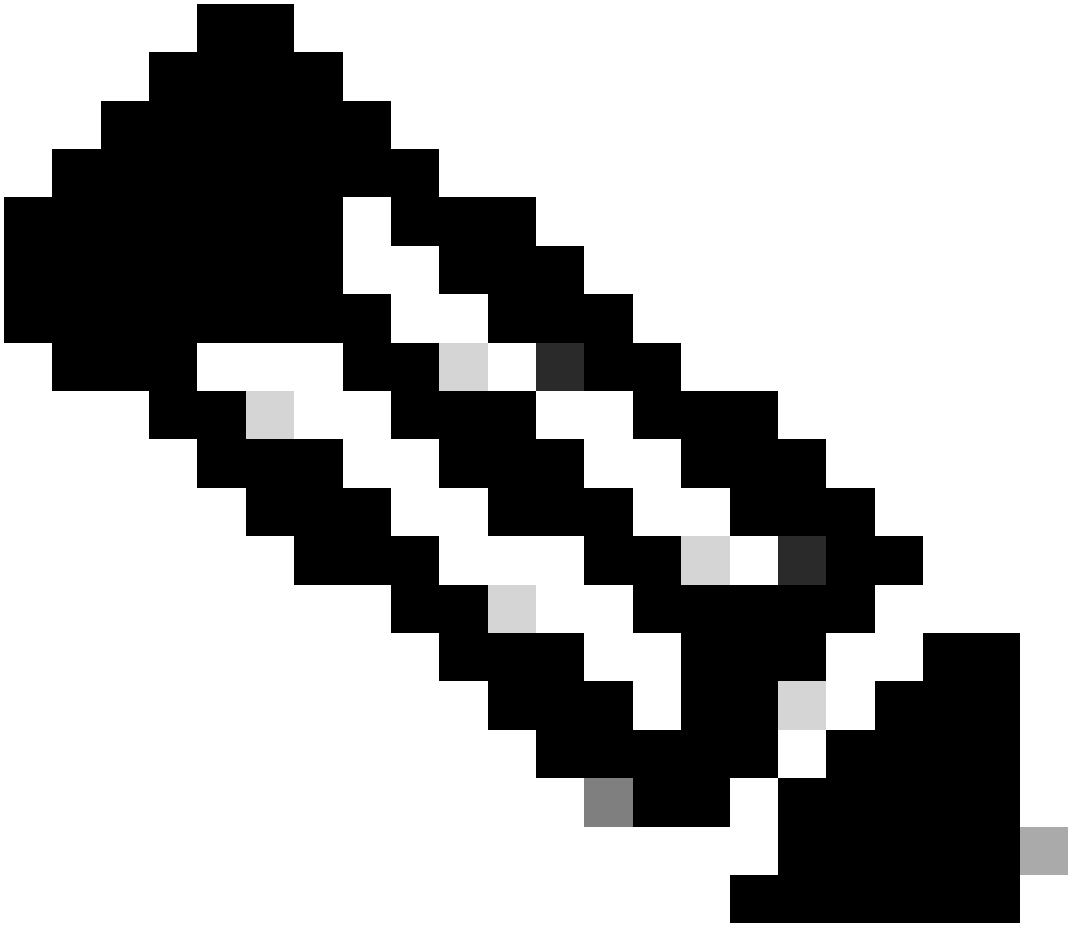
---



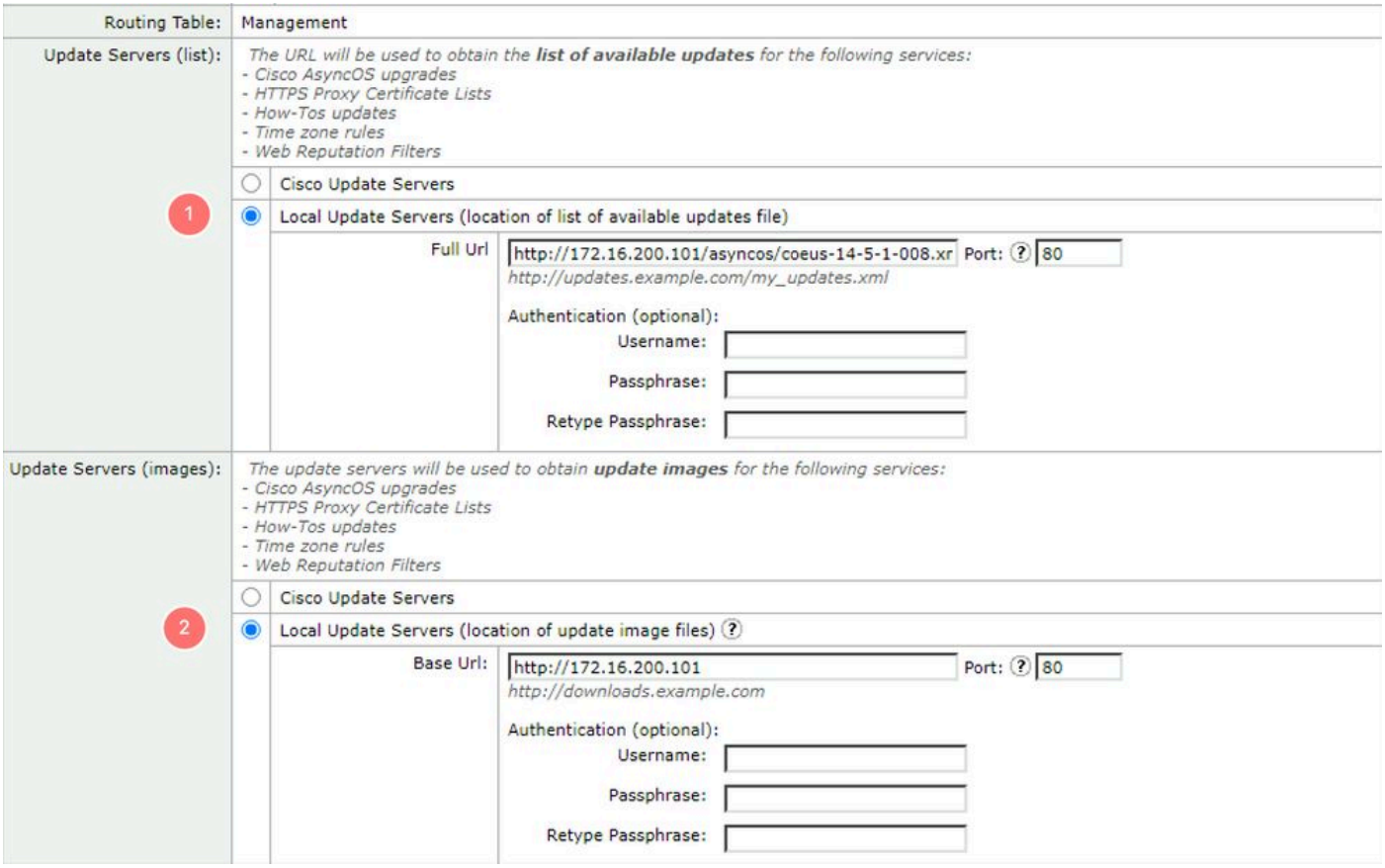
Nota: el archivo de manifiesto es el archivo .xml ubicado en la carpeta asyncos

---

Paso 6. En Update Servers (images) configuration, elija Local Update Servers. Cambie la configuración de la URL base (actualizaciones de IronPort AsyncOS) a su servidor de actualizaciones local y al número de puerto apropiado.

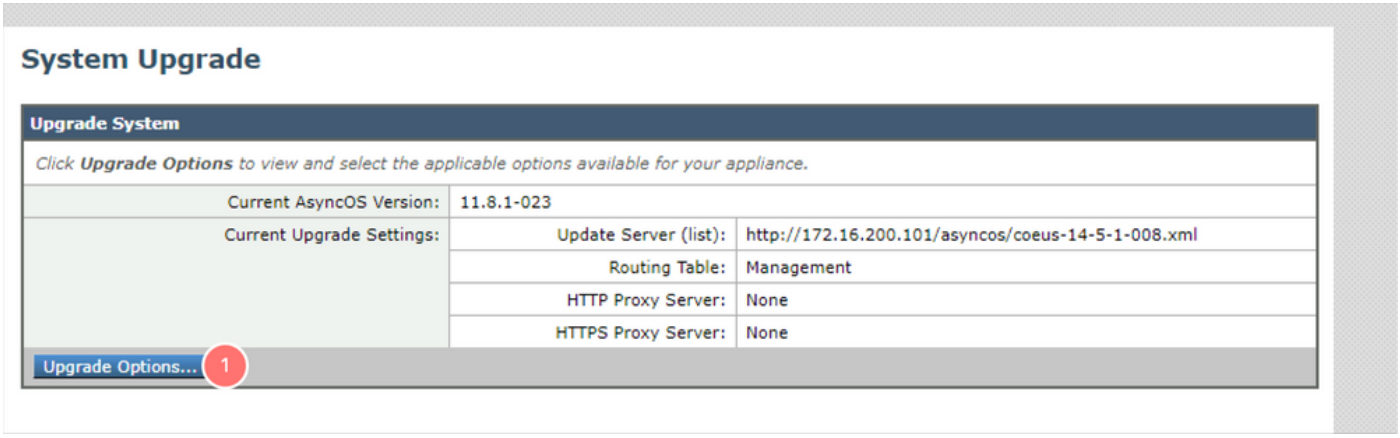


Nota: Si el servidor Web está configurado para la autenticación, puede establecer las credenciales en la sección Autenticación.

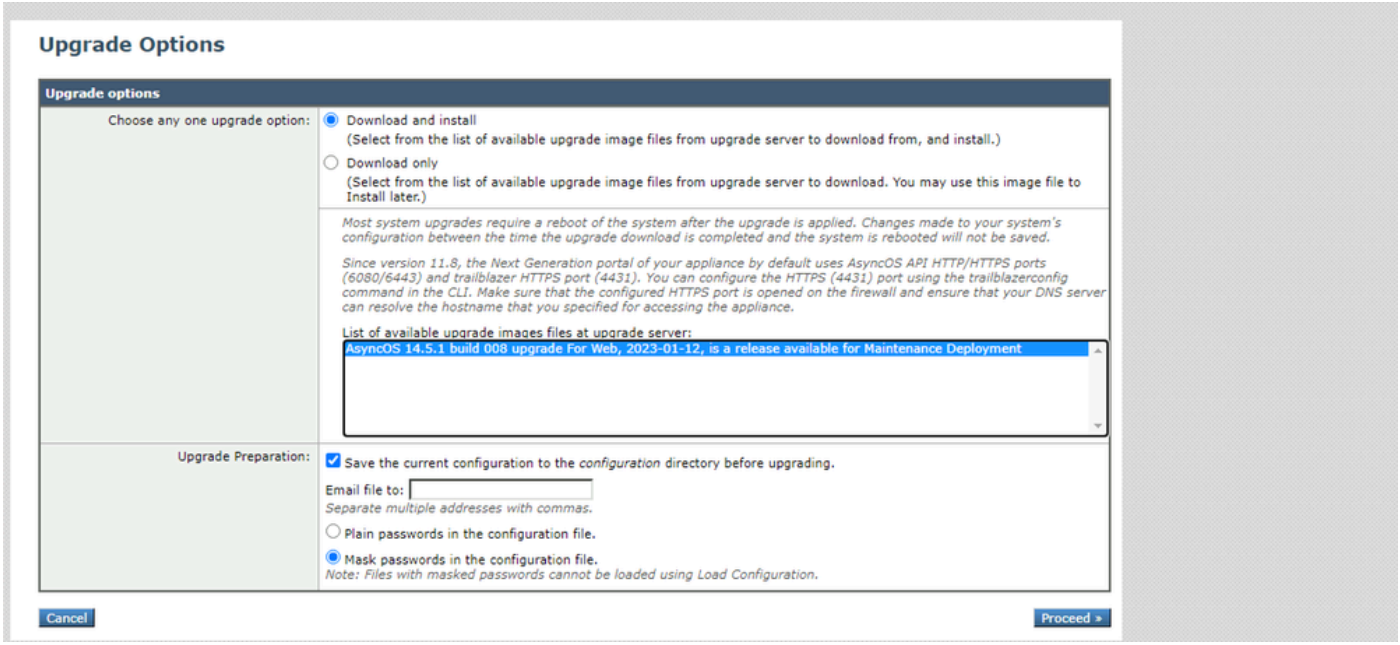


Paso 7. Enviar y confirmar cambios.

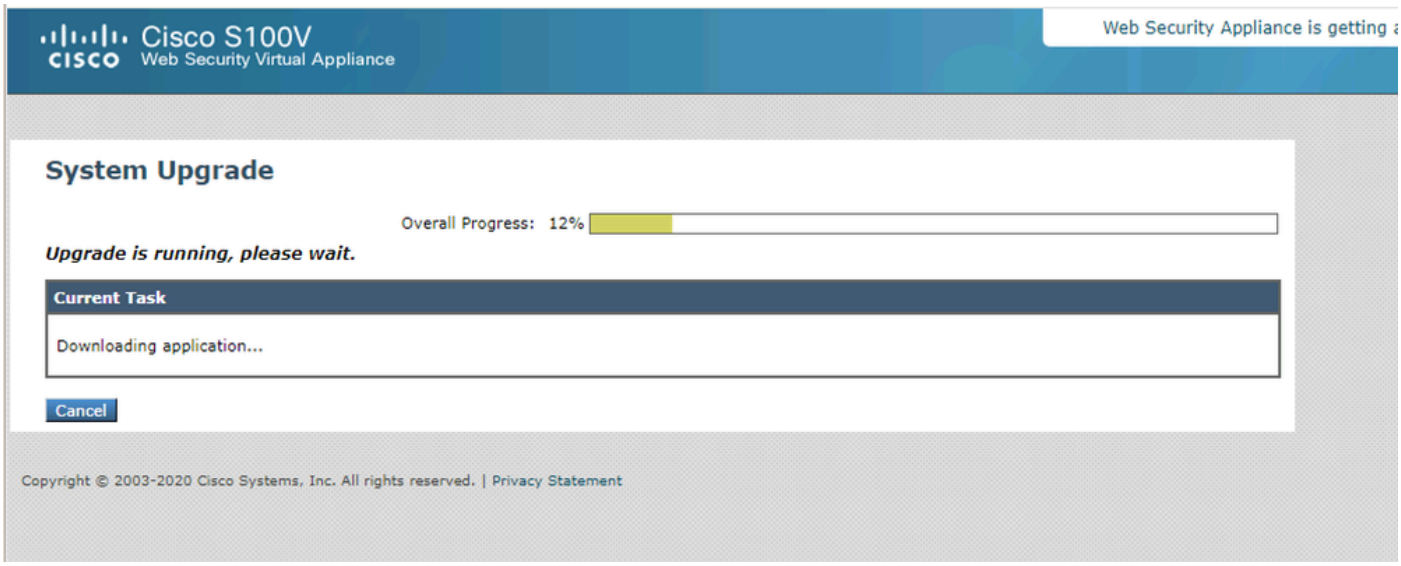
Paso 8. Haga clic en Opciones de actualización para ver la lista de versiones disponibles.



Paso 9. Elija la versión deseada y haga clic en "Proceed":



Paso 10. Consulte las instrucciones de la página Actualización del sistema.



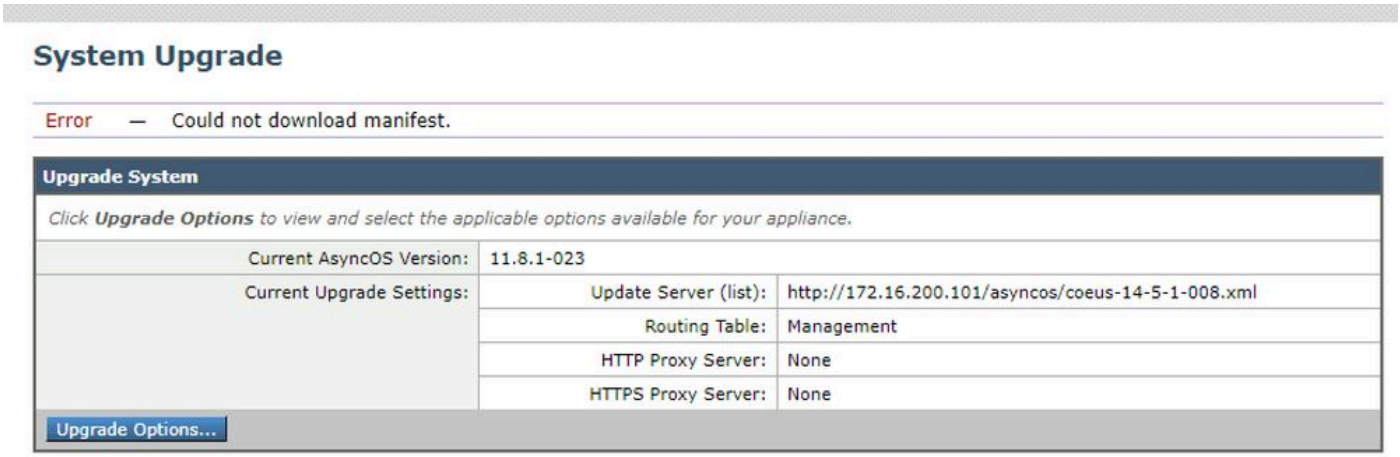
Troubleshoot

puede ver los registros de actualización desde CLI > grep > elija el número asociado con los registros de actualización

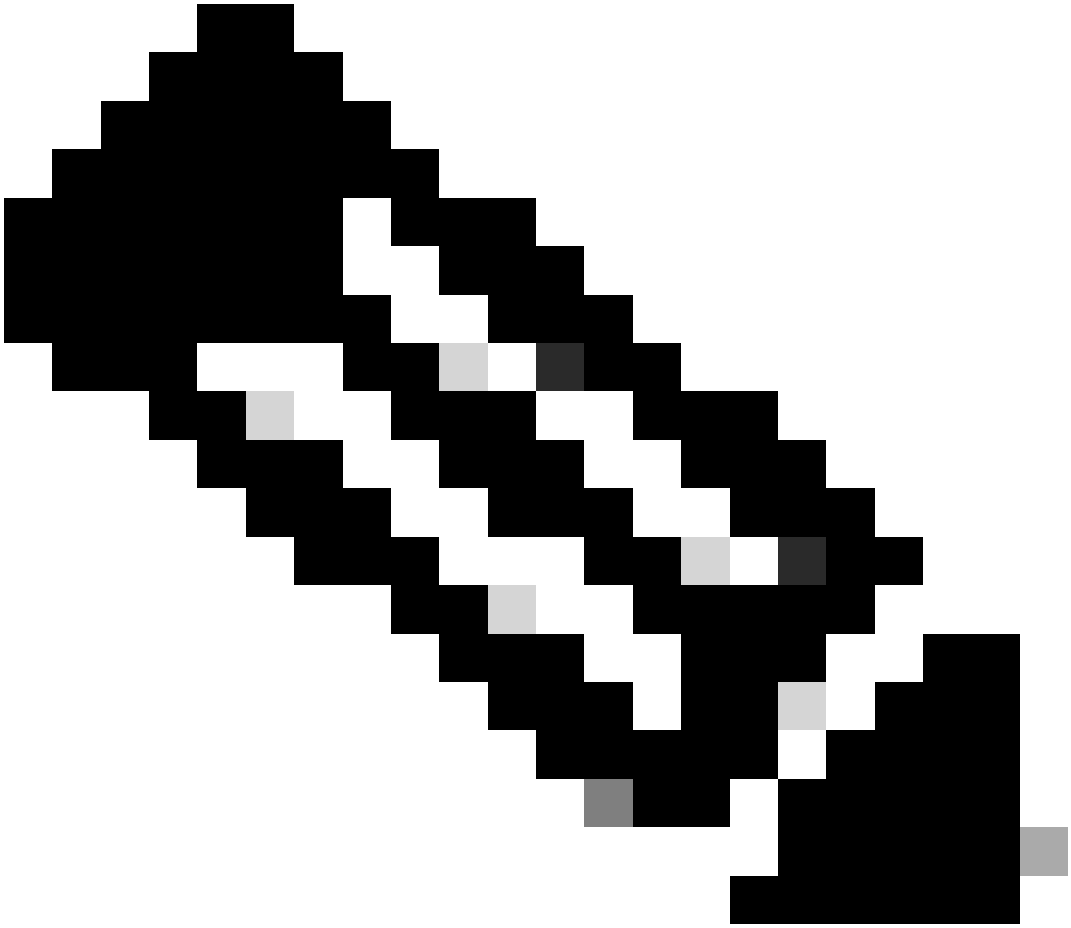
A continuación se muestran algunos registros de actualización exitosa:

```
Wed Feb  18 04:08:12 2024 Info: Begin Logfile
Wed Feb  18 04:08:12 2024 Info: Version: 11.8.1-023 SN: 420D8120350A5CB03F1E-EEE6300DA0C4
Wed Feb  18 04:08:12 2024 Info: Time offset from UTC: 3600 seconds
Wed Feb  18 05:18:10 2024 Info: The SHA of the file hints is 5a9987847797c9193f8d0ba1c7ad6270587bcf82f1
Wed Feb  18 05:18:10 2024 Info: Download and installation of AsyncOS 14.5.1 build 008 upgrade For Web,
Wed Feb  18 05:18:10 2024 Info: The SHA of the file upgrade.sh is 41da10da137bb9a7633a5cede9636de239907
```

No se pudo descargar el manifiesto



Debe asegurarse de que SWA pueda acceder a los archivos en el servidor web, para verificar la conectividad, puede utilizar el comando curl desde CLI.



Nota: Al elegir Directa, SWA prueba la conectividad desde el sistema operativo y no desde el servicio proxy.

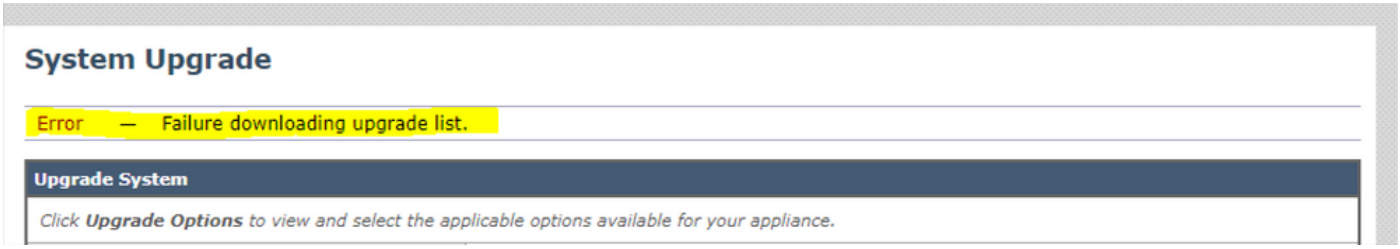
```
SWA_CLI> curl


Choose the operation you want to perform:
- DIRECT - URL access going direct
- APPLIANCE - URL access through the Appliance
[]> direct

Do you wish to choose particular interface of appliance?
[N]>

Enter URL to make request to
[]> http://172.16.200.101/asyncos/coeus-14-5-1-008.xml
```

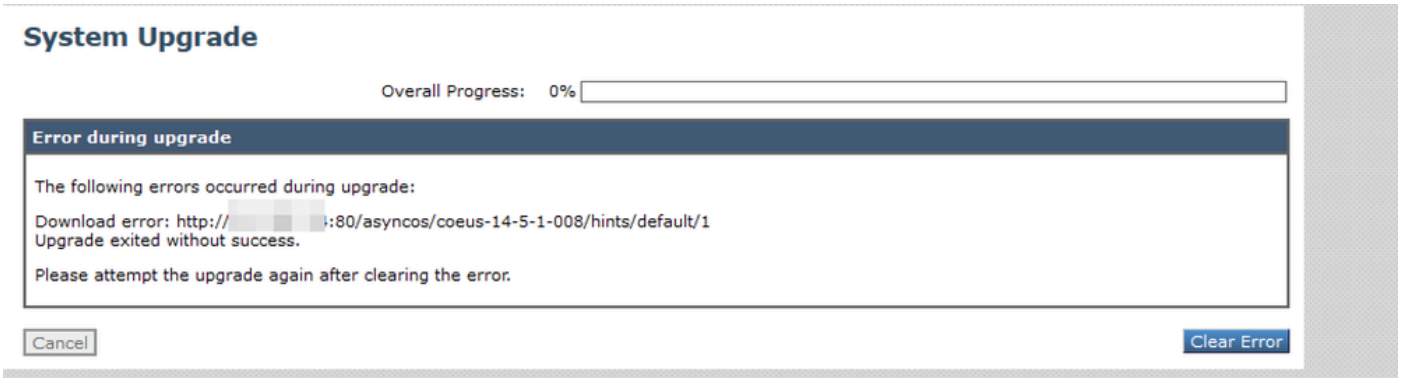
Fallo al descargar la lista de actualizaciones



Primero, verifique la conectividad entre SWA y el servidor de actualización; puede utilizar el comando curl como se mencionó.

Si la conectividad era correcta, verifique el VLAN o el número de serie del archivo de manifiesto para asegurarse de que son iguales que el dispositivo. Puede abrir el archivo .xml y buscar la etiqueta <keys>.

Error de descarga, la actualización se cerró sin éxito



Asegúrese de que ha configurado correctamente el permiso en el servidor Web.

Información Relacionada

Al intentar actualizar, ¿por qué aparece el error Falla al descargar la lista de actualizaciones? "Error al realizar la actualización: error de E/S"? -Cisco

Proceso de actualización para Secure Web Appliance - Cisco

Actualización del dispositivo de seguridad Email Security Appliance (ESA) con GUI o CLI - Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).