# Guía del usuario de BPA Actualización del SO v5.1

# Introducción

La aplicación de actualización de SO de Business Process Automation (BPA) proporciona una completa solución de automatización para realizar actualizaciones y conformidad de software de dispositivos de red en diferentes dominios. Admite varios controladores de dominio y proporciona una experiencia de usuario unificada. Admite actualizaciones básicas del sistema operativo (SO)

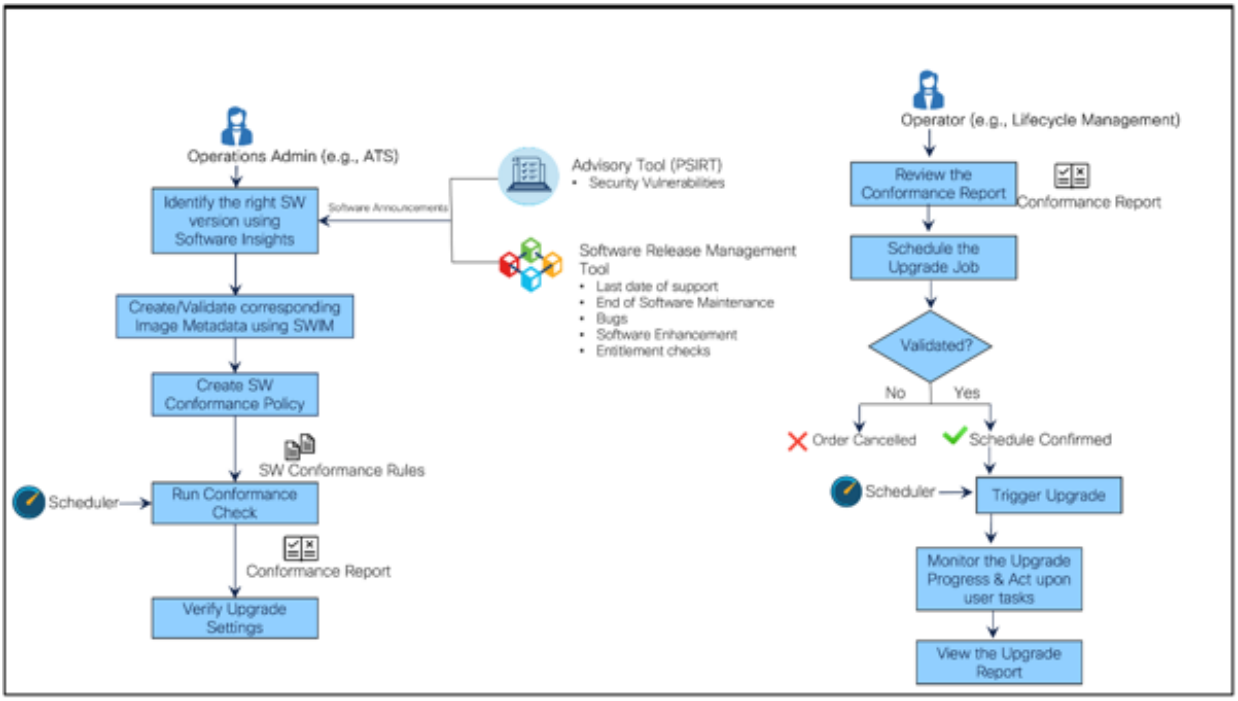
y actualizaciones de mantenimiento de software (SMU) o actualizaciones de parches del administrador de paquetes RPM (RPM).

## Capacidades clave

La aplicación Actualización del sistema operativo proporciona las siguientes capacidades de automatización clave:

- Gestión de imágenes de software: Una lista centralizada de imágenes de software y sus versiones (de todos los proveedores) para el proceso de actualización de software que se debe utilizar
- Información sobre software: Identifica los riesgos de software y las vulnerabilidades expuestas a los recursos de red y obtiene información sobre las versiones de software recomendadas por el proveedor.
- Conformidad de software: Identifica todos los recursos de la red cuyas imágenes de software se deben actualizar
- Definición del método de actualización del procedimiento (MOP): Predefine el proceso de actualización junto con comprobaciones previas y posteriores para cada familia o modelo de dispositivo del proveedor
- Trabajos de actualización: Programa actualizaciones para activos no conformes durante períodos de mantenimiento en regiones geográficas, supervisa el progreso de la actualización y obtiene informes detallados

## Flujo de extremo a extremo




Flujo de extremo a extremo

La figura anterior muestra los flujos de llamadas de la aplicación Actualización del SO para dos usuarios diferentes: Operations Administrator y Network Operator, que se suministran de forma inmediata (OOB). Consulte Control de Acceso para obtener más información sobre las funciones OOB y los permisos correspondientes.

| Persona | Descripción | Espacio de trabajo |
|---|---|---|
| Administrador de operaciones | Detecta vulnerabilidades de software (p. ej., recomendaciones, errores, boletines de fin de vida útil) que afectan a los recursos de red | BPA: Actualización del sistema operativo/Administración de imágenes de software/Asesores |
| Administrador de operaciones | Identifica la versión de software afectada y los recursos afectados, y determina la versión de destino correcta en función de las sugerencias proporcionadas por el proveedor | BPA: Actualización del sistema operativo/gestión de imágenes de software/perspectivas |
| Administrador de operaciones | Crea los metadatos de imagen de software necesarios | BPA: Actualización del sistema operativo/gestión de imágenes de software/imágenes de software |
| Administrador de operaciones | Crea la intent para los modelos de dispositivos afectados y ejecuta la política a demanda o en la ejecución programada de la política | BPA: Política de conformidad de software/actualización de SO |
| Administrador de operaciones | Identifica los activos no conformes o afectados | BPA: Actualización del SO/Conformidad de software/Ver resultados |
| Administrador de operaciones | Crea o modifica la directiva de actualización según el MOP de actualización; esto incluye la predefinición de las comprobaciones previas y posteriores, los flujos de trabajo para la distribución o activación, el desvío o la reversión del tráfico y la reversión para actualizaciones en uno o varios pasos | BPA: Política de actualización/actualización del SO |
| Operador de red | Programa un trabajo para actualizar todos los dispositivos no conformes | BPA: Trabajos de actualización/actualización del SO |
| Operador de red | Supervisa el progreso del trabajo de actualización | BPA: Actualización del SO/Trabajos de |

| Persona | Descripción | Espacio de trabajo |
|---|---|---|
| | | actualización/Detalles del trabajo |
| Operador de red | Actúa sobre las tareas del usuario, si las hay, para solucionar los problemas y permite que el proceso continúe con el siguiente paso | BPA: Actualización del SO/Trabajos de actualización/Detalles del trabajo |

## Propuesta de valor

La aplicación de actualización del sistema operativo proporciona los siguientes agregados de valor:

- Un enfoque de API inicial para facilitar el consumo de servicios desde los sistemas de soporte de operaciones (OSS) ascendentes y los sistemas de soporte de negocios (BSS)
- Validación rápida de la conformidad del software de los dispositivos de red en redes gestionadas por varios controladores de dominio
- Los operadores tienen más control sobre las tareas de actualización mediante mecanismos de procesamiento por lotes, colocación en cola y programación
- Los trabajos de actualización se pueden crear antes para las revisiones y ejecutarse después
- Un mecanismo de colocación en cola que permite un rendimiento más rápido y mejor con fallos mínimos o nulos
- Copias de seguridad de configuración automáticas previas a la actualización, lo que permite restauraciones sin problemas en caso de fallos
- Ejecuciones previas y posteriores a la comprobación, lo que garantiza el éxito de las actualizaciones sin interrupciones en el servicio.
- Un enfoque basado en políticas que proporciona la flexibilidad necesaria para predefinir el MOP de actualización con comprobaciones previas y posteriores a la validación, distribución o activación, desvío o reversión del tráfico y procesos de reversión, lo que permite personalizarlos según sea necesario

## Controladores y plataformas de dispositivos compatibles

Las siguientes plataformas se han validado en BPA y son compatibles con OOB. Sin embargo, el marco es genérico y puede ampliarse a nuevas plataformas. En las versiones futuras se proporcionará soporte OOB para plataformas adicionales en función de la prioridad.

| Controlador(es) de dominio | Plataformas de dispositivos |
|---|---|
| Cisco Catalyst Center v2.3.7.5-70434 | - Cisco IOS y Cisco IOS-XE<br>- Cisco IOS y Cisco IOS-XE |
| vManage v20.12.4 | Nota: Los dispositivos deben ser v17.9.x o superiores para que funcione la distribución de servidores remotos |
| Controlador de fabric de panel Nexus (NDFC) v12.1.2e y v12.2.2 | - Cisco NXOS (N9k) |
| Firewall Management Center (FMC) v7.4.1 | - Firepower 3140 |
| Network Services Orchestrator (NSO) v6.3 | - Cisco-IOSXR (NCS540, NCS560, ASR9K)<br>- Cisco NXOS (N9K)<br>Nota: Se requiere NX-OS NED v5.25.17 o superior |
| Controlador de red cruzada (CNC) v6.0 | - Cisco-IOSXR (NCS540, ASR9K) |
| ANSIBLE v2.9.18 (AWX - 17.1.0) | - Cisco-IOSXR (NCS540, ASR9K) |
| Directa al dispositivo (a través de Teletype Network (Telnet) y Secure Shell (SSH)) | - Cisco-IOSXR (NCS540, ASR9K) |

### Características nuevas

Para ver las funciones incrementales disponibles para el caso práctico de actualización del sistema operativo para esta versión, consulte las Notas de la versión de BPA.

## Prerequisites

Antes de utilizar la aplicación Actualización del SO, deben cumplirse las siguientes condiciones previas:

- Actualización del sistema operativo, copia de seguridad y restauración, servicios de Planificador y todos los servicios de plataforma o de agente de controlador necesarios están activos y en ejecución
- Se cargan los artefactos necesarios (por ejemplo, flujos de trabajo, plantillas de proceso, políticas de actualización predeterminadas, etc.)
- Se agregan los controladores necesarios y los dispositivos se sincronizan correctamente; consulte Controladores y plataformas de dispositivos compatibles para obtener más información

# Trabajo con la aplicación de actualización del sistema operativo

La aplicación Actualización del sistema operativo consta de los siguientes componentes:

- Gestión de imágenes de software (SWIM)
- Gestión del servidor de distribución de imágenes
- Perspectivas del software
- Conformidad de software
- Política de actualización
- Actualizar trabajos
- Configuración

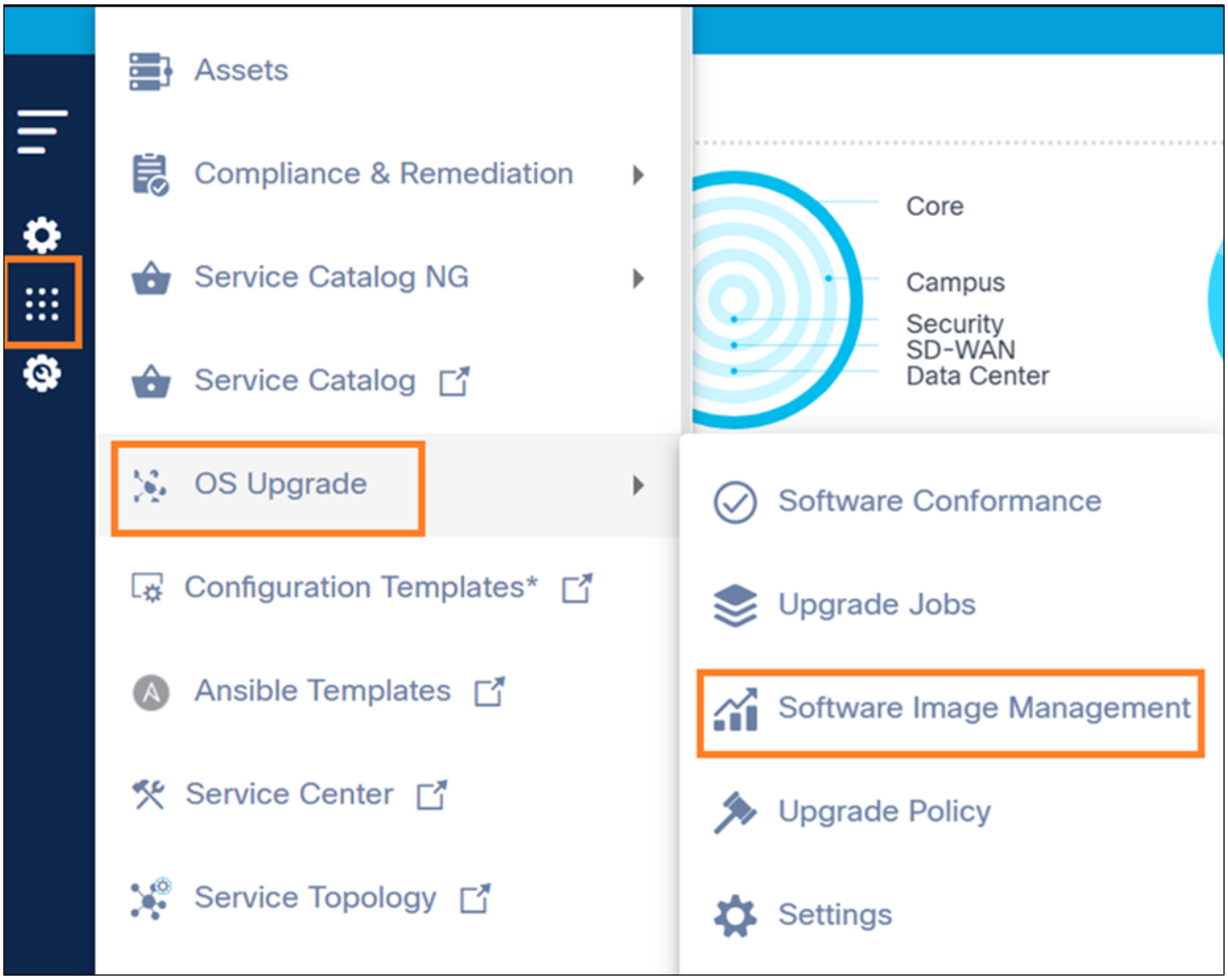
## Gestión de imágenes de software

El componente SWIM permite a los usuarios de Operations mantener los detalles de la imagen de software para controladores como NSO, ANSIBLE, CNC, FMC y Direct-to-Device que no tienen soporte de administración de imágenes OOB. También enumera los detalles de la imagen de software que mantienen los controladores como vManage, NDFC y Cisco Catalyst Center, y proporciona una lista centralizada de software que se mantiene en todos los controladores de dominio. Las imágenes de software y el servidor de distribución de imágenes son los dos subcomponentes principales dentro del módulo SWIM.

Imágenes de software

Para acceder a la página Imágenes de software:

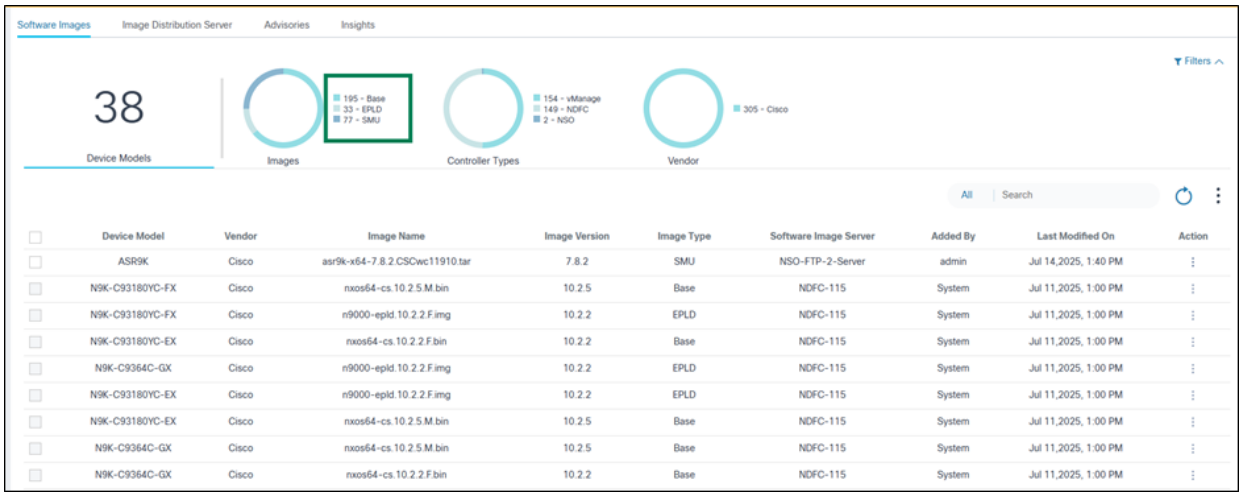
1. Inicie sesión en BPA con credenciales que tengan acceso a Software Image Management (Administración de imágenes de software).




Navegación de gestión de imágenes de software

2. Seleccione OS Upgrade > Software Image Management.

La página Administración de imágenes muestra las fichas siguientes: Software Images, Image Distribution Server, Advisories y Insights.




Ficha Imágenes de software

La pestaña Imágenes de software contiene lo siguiente:

- Una sección de análisis, que se muestra en la parte superior, que proporciona lo siguiente:
    - Número total de modelos de dispositivos e imágenes de software asociadas
    - Un filtro rápido Imágenes que permite filtrar imágenes basadas en el tipo (por ejemplo, base, SMU); el número indica el número total de imágenes asociadas a un tipo de imagen respectivo
    - Un filtro rápido Controller Types que permite filtrar imágenes según el tipo de controlador (por ejemplo, Cisco Catalyst Center, vManage, NSO o NDFC, Direct-to-Device, CNC, ANSIBLE, FMC) para el que se alojan las imágenes. el número indica el número total de imágenes asociadas a un tipo de controlador respectivo
    - Un filtro rápido del proveedor que permite filtrar imágenes según el proveedor que publicó el software
- El icono More Options proporciona las siguientes funcionalidades:
    - Agregar detalles de imagen: Agregar nuevos metadatos de imagen
    - Carga masiva: Carga masiva de metadatos de imagen en formato .csv
    - Sincronizar imágenes: Sincronizar metadatos de imagen de controladores (por ejemplo, Cisco Catalyst Center, vManage, NDFC y FMC)
    - Eliminar todos: Eliminación masiva de imágenes seleccionadas

---

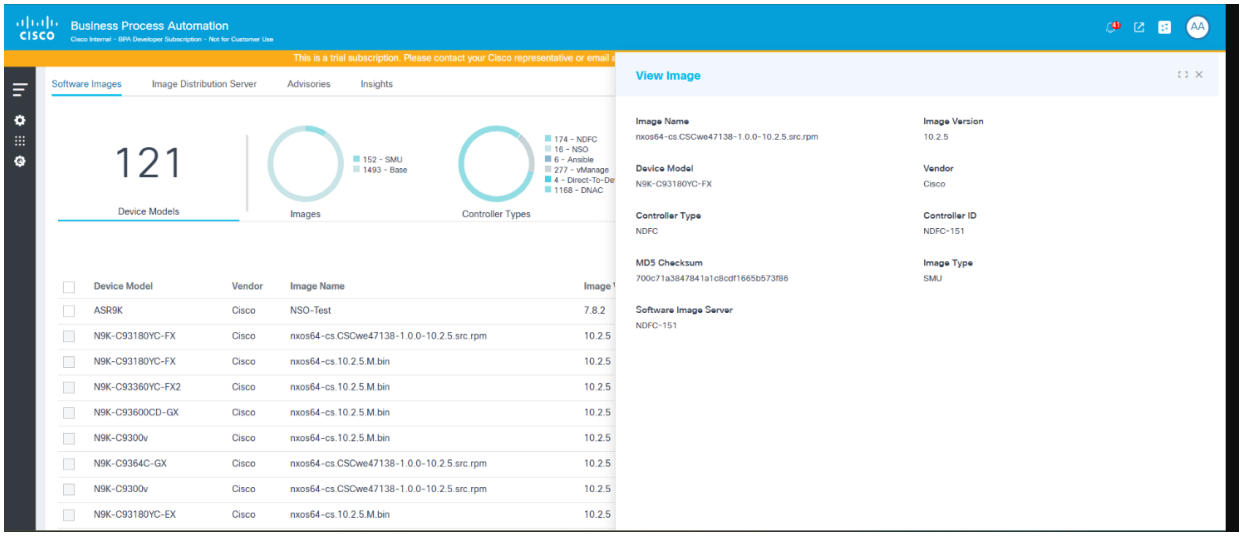
Nota: La adición, eliminación y carga masiva de detalles de imagen solo se permite para los controladores NSO, ANSIBLE, CNC y de conexión directa con el dispositivo.

---

- El filtro Search se puede utilizar para buscar imágenes e incluye los siguientes filtros de búsqueda exclusivos:
    - Todos: Buscar en todos los campos
    - Nombre de la imagen: Busque las imágenes con un nombre de imagen específico
    - Modelo de dispositivo: Buscar las imágenes con un modelo especificado
    - Versión de imagen: Buscar imágenes con una versión de software específica
    - Servidor de imágenes de software: Buscar las imágenes asociadas a un servidor de imágenes específico
- El icono Refresh actualiza la página y borra los filtros seleccionados.
- Las imágenes existentes se muestran en una tabla de cuadrícula con las siguientes columnas:
    - Modelo de dispositivo: Modelo de dispositivo al que se aplican los detalles de la imagen
    - Proveedor: Proveedor que publica las imágenes de software
    - Nombre de la imagen: Nombre de archivo de la imagen
    - Versión de imagen: Versión de software de la imagen
    - Tipo de imagen: Determina el tipo de imagen (por ejemplo, base, SMU, dispositivo lógico programable electrónico (EPLD))

- Servidor de imágenes de software: Servidor de imágenes donde existe la imagen actual
- Agregado por: Usuario que agregó los metadatos de la imagen
- Última modificación el: Marca de tiempo de la última actualización de detalles de la imagen
- Acción: Proporciona un icono Más opciones desde el que se pueden seleccionar acciones específicas de la fila (por ejemplo, editar, eliminar)

- Ordenar imágenes haciendo clic en el encabezado de una columna correspondiente




Ver imagen

- Al hacer clic en una fila, se abre la ventana Ver imagen

## Sincronización de metadatos de imágenes de software

Para realizar la sincronización a petición de imágenes de software:


Sincronizar imágenes

1. Seleccione el icono Más opciones > Sincronizar imágenes. Los detalles de metadatos de

imagen de vManage, Cisco Catalyst Center, NDFC y FMC se detectan y conservan en BPA.

---

Nota: En el caso de los controladores FMC, los datos existentes se conservan cada vez que se ejecuta una sincronización. Sólo se agregan imágenes nuevas.

---

2. Si el nombre de la imagen del controlador FMC incluye la palabra "FTD" o "Firepower Threat_Defense", el deviceModel de esa imagen se asigna como FTD.

O

Si el nombre de la imagen del controlador FMC incluye la palabra "FMC", "FW_Mgmt_Center" o "Firewall_Management_Center", el deviceModel para esa imagen se asigna como FMC.

---

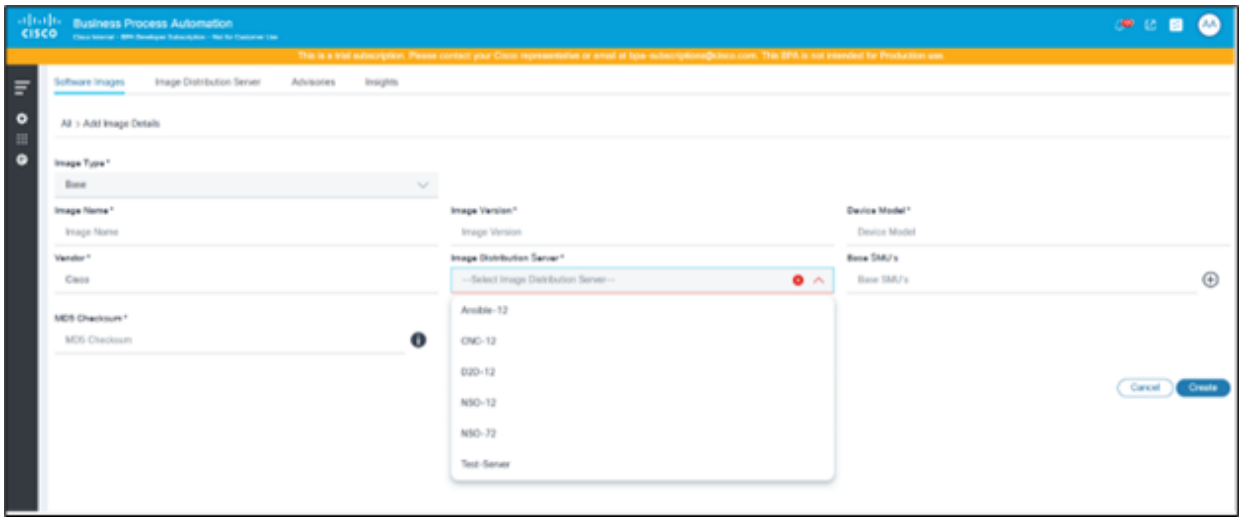
Nota: FMC no asocia la información del modelo a los metadatos de la imagen. Una vez finalizada la sincronización, edite los metadatos de la imagen correspondiente y actualice el modelo según sea necesario. El proceso de actualización de FMC no funciona como se esperaba sin la actualización del modelo.

---

3. Las imágenes de los servidores remotos de vManage tienen inicialmente el identificador único universal (UUID) asignado en la columna Version después de la operación de sincronización. Los operadores deben editar manualmente los metadatos de servidor remoto requeridos y actualizarlos con la versión de imagen adecuada. Si no se realiza esta asignación, otros componentes de actualización del sistema operativo (por ejemplo, conformidad del software, políticas de actualización, trabajos de actualización, etc.) no funcionan según lo esperado.
4. Para programar la sincronización automática de metadatos SWIM a intervalos regulares, consulte Configuración de implementación.

Adición de metadatos de imagen de software

1. Seleccione el icono Más opciones > Agregar detalles de imagen. Se muestra la página Add Image Details.




Agregar detalles de imagen

2. Introduzca información en los campos siguientes:

- Tipo de imagen: El tipo de imagen (por ejemplo, base, SMU, EPLD)
- Nombre de la imagen: Nombre del archivo de imagen; los usuarios pueden introducir una ruta de acceso relativa o absoluta de la imagen en el campo Nombre. Si los usuarios proporcionan una ruta de acceso absoluta, la imagen se obtiene directamente de esa ruta de acceso; si los usuarios proporcionan una ruta relativa, el sistema resuelve la ruta completa agregando la ruta base definida en el servidor del repositorio durante la distribución
- Versión de imagen: Versión de software de la imagen
- Modelo de dispositivo: Modelo de dispositivo para el que se está etiquetando la imagen

---

Nota: El modelo de dispositivo debe coincidir con la información del modelo proporcionada por el controlador CNC, NSO, Direct-To-Device o ANSIBLE para los dispositivos aplicables.

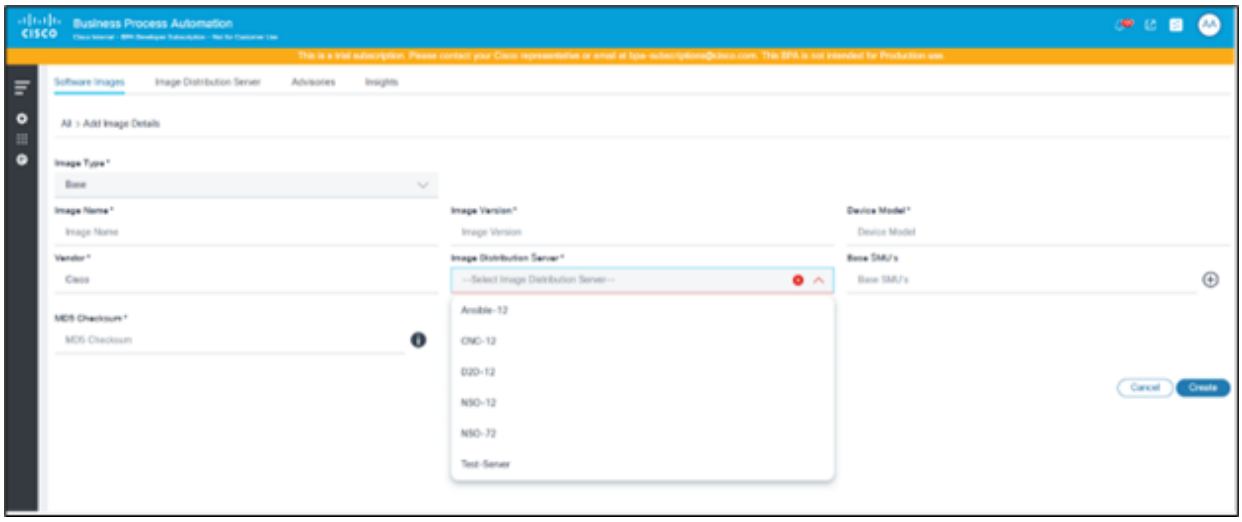
---

- Proveedor: El proveedor o proveedor que publicó la imagen; el valor predeterminado es Cisco, pero se puede cambiar según sea necesario
- Servidor de distribución de imágenes: Seleccione el servidor de distribución de imágenes que aloja el archivo de software indicado en el campo Nombre de imagen. Al seleccionar un servidor de distribución de imágenes, se generan imágenes para todos los ID de controlador asociados con el tipo de controlador especificado definido dentro del servidor de distribución de imágenes. Si un usuario agrega o quita instancias de controlador bajo el servidor de distribución de imágenes, las imágenes de software correspondientes se agregan o eliminan para esas instancias de controlador.
- SMU de base: SMU presentes en la imagen dorada de base; esta opción sólo es aplicable si el tipo de imagen es Base
- Suma de comprobación MD5: Suma de comprobación MD5 de imagen para verificación

3. Haga clic en Crear. Se muestra la notificación Progress seguida de un mensaje de

confirmación.

Nota: Los metadatos de imagen para las SMU de puente deben agregarse antes de utilizarlos en una política de actualización. Para agregar SMU de puente, seleccione SMU en la lista desplegable Tipo de imagen.




Agregar metadatos de imagen SMU de puente

Carga masiva de metadatos de imagen de software

| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | Device Model | Vendor | Image Name | Version | Image Type | Image Distribution Server | MD5 Checksum |
| 2 | NCS-540 | Cisco | test22 | 1.1.1 | Base | Ansible server | 680fcd5f9f3558d6fd581edc0835ce2a |
| 3 | NCS-540 | Cisco | test23 | 2.2.2 | Base | Ansible server | b4eceaf95e419c63d8da124d214deaaf |
| 4 | NCS-540 | Cisco | test33 | 2.2.2 | Base | Ansible server | b4eceaf95e419c63d8da124d214deaaf |
| 5 | NCS-540 | Cisco | test421 | 2.2.2 | Base | Ansible server1 | b4eceaf95e419c63d8da124d214deaaf |

Archivo CSV de ejemplo con información de imagen

1. Prepare un archivo .csv con los detalles de imagen necesarios y los siguientes nombres de columna:

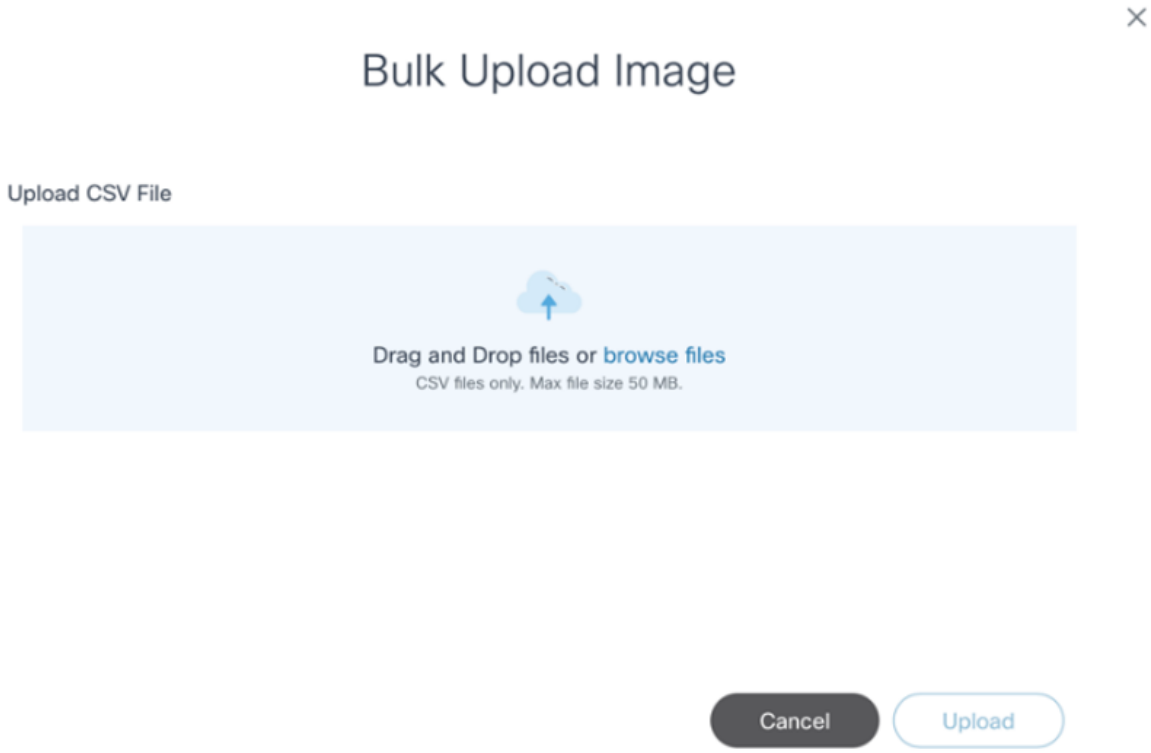
- Nombre de la imagen
- Versión
- Modelo de dispositivo
- Proveedor
- Tipo de imagen

Nota: Sólo se admiten valores Base, SMU y EPLD.

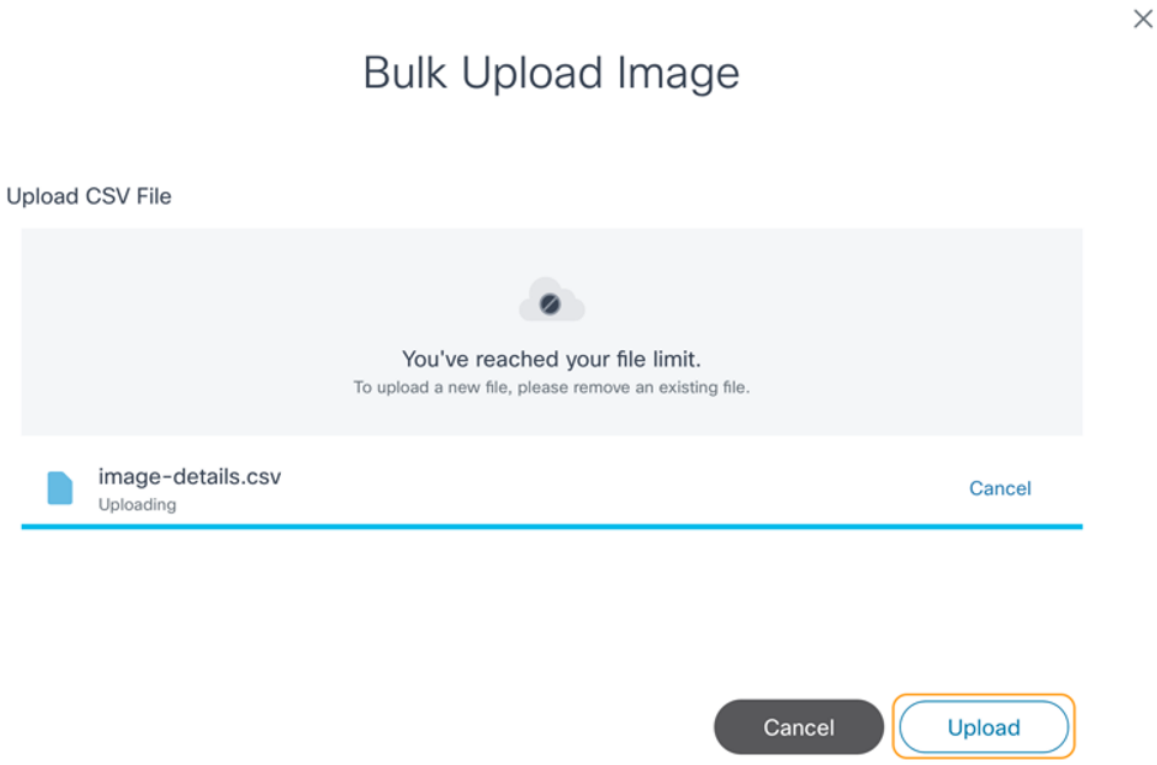
- Servidor de distribución de imágenes

- Suma de comprobación MD5

2. Seleccione el icono Más opciones > Carga masiva. Se abre la ventana Carga masiva de imágenes.

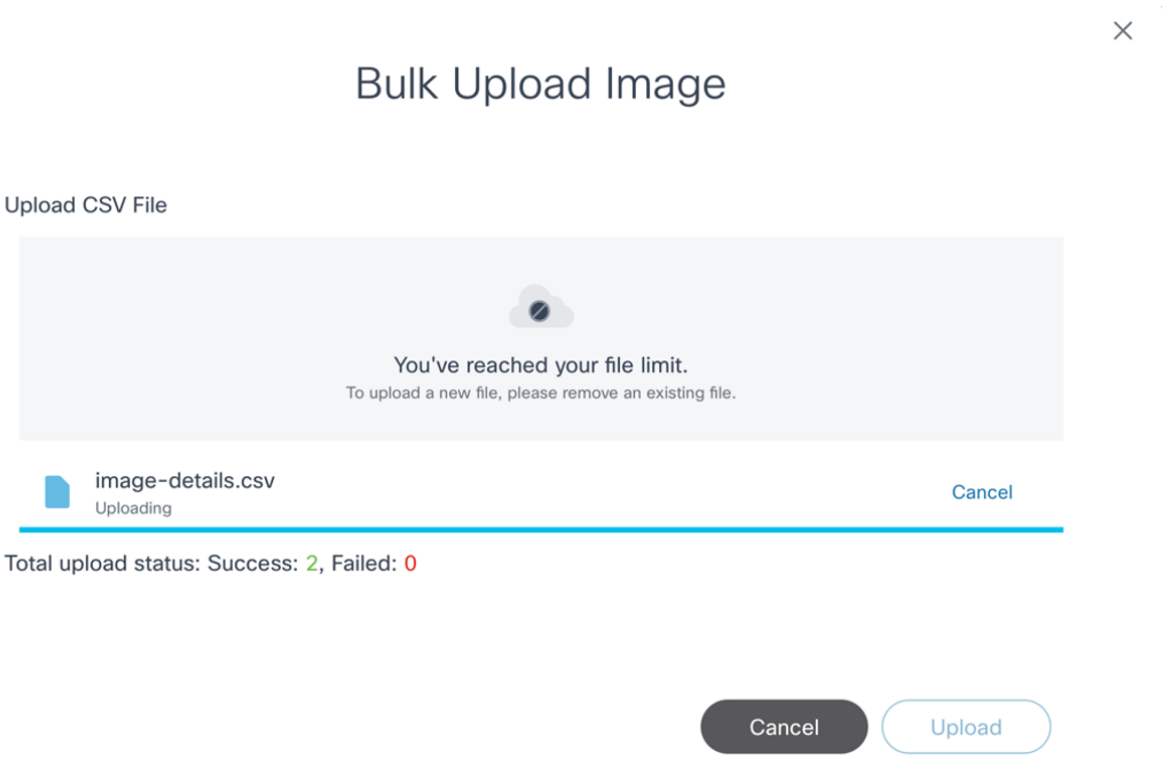



Carga masiva de imágenes




Carga masiva de imágenes: carga de CSV

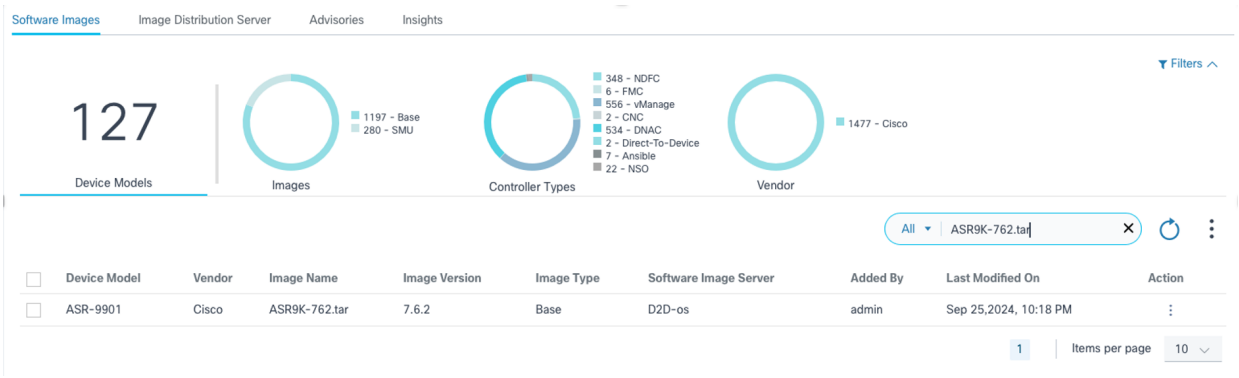
3. Seleccione un archivo .csv preparado y haga clic en Cargar. Los detalles de la imagen del archivo .csv se validan y se procesan. Una vez cargado el archivo, se muestra el estado final de la carga masiva.




Estado de carga de imagen masiva correcto

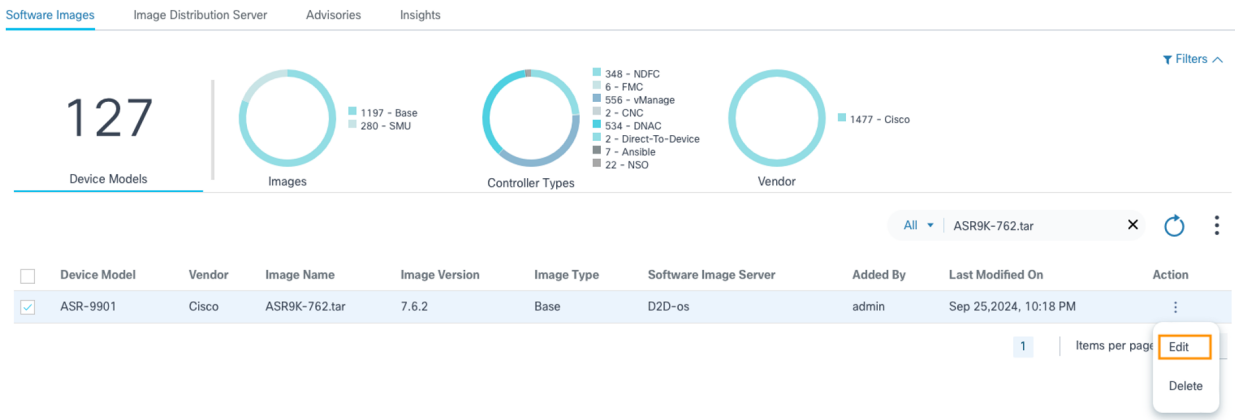
Nota: En caso de errores de validación de datos (por ejemplo, registros duplicados o parámetros no válidos), los mensajes de error se muestran como una cuadrícula en la ventana Carga masiva de imágenes. Los usuarios pueden corregir los valores del archivo .csv y volver a cargarlo.

## Edición de metadatos de imágenes de software existentes



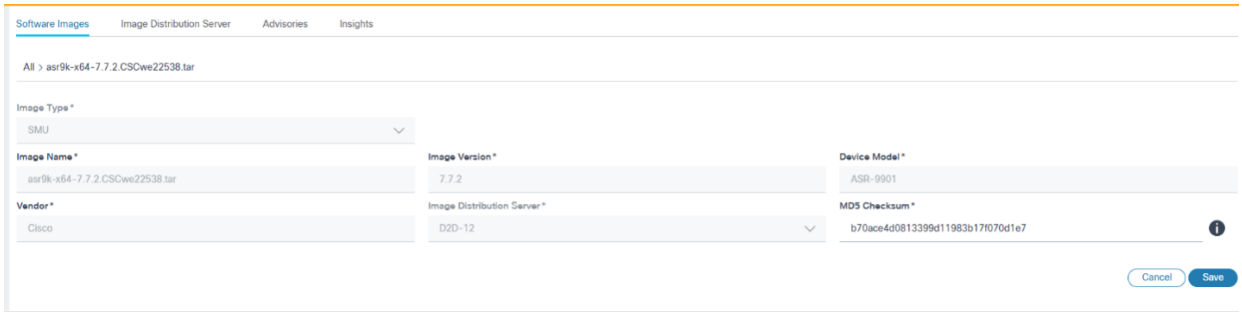

Buscar en metadatos de imágenes de software

1. Busque la imagen que debe actualizarse mediante el filtro Buscar.




Editar

2. En la columna Acción de la imagen deseada, seleccione el icono Más opciones > Editar.




Editar imágenes de software

3. Actualice los parámetros necesarios y haga clic en Guardar para guardar los cambios o haga clic en Cancelar para descartarlos. Aparecerá una notificación de progreso seguida de un mensaje de confirmación para la actualización de la imagen.

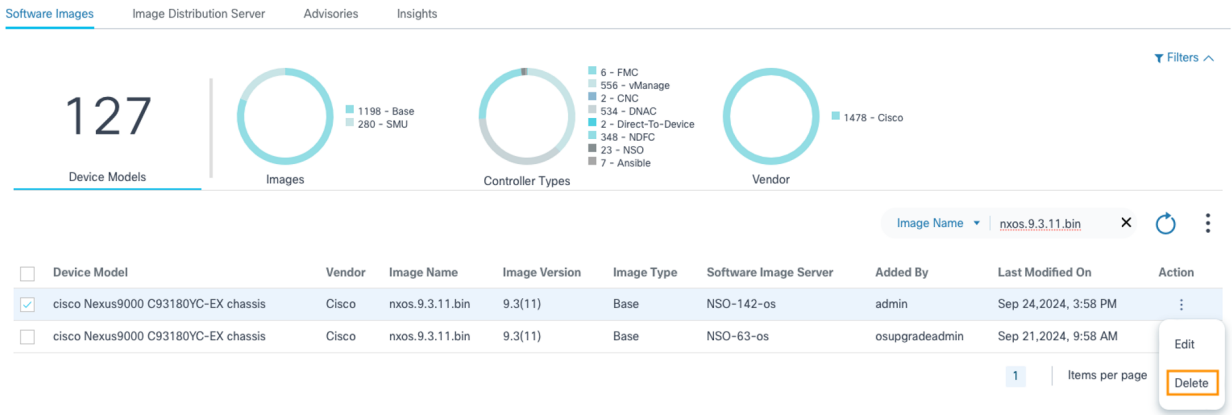
Nota: Debe tenerse en cuenta la siguiente lista.

- La edición está disponible para los controladores CNC, NSO, D2D, ANSIBLE, FMC y vManage (solo se aplica a los metadatos de imagen del servidor remoto)
- La actualización del modelo de dispositivo solo es compatible con las imágenes de servidor remoto de vManage
- Sólo el campo Versión de software se puede actualizar para los metadatos de imagen del servidor remoto de vManage
- En el caso de las imágenes de vManage, los usuarios pueden ver el servidor de imágenes de software en lugar de las instancias del controlador

Eliminación de metadatos de imagen de software

Buscar en metadatos de imágenes de software

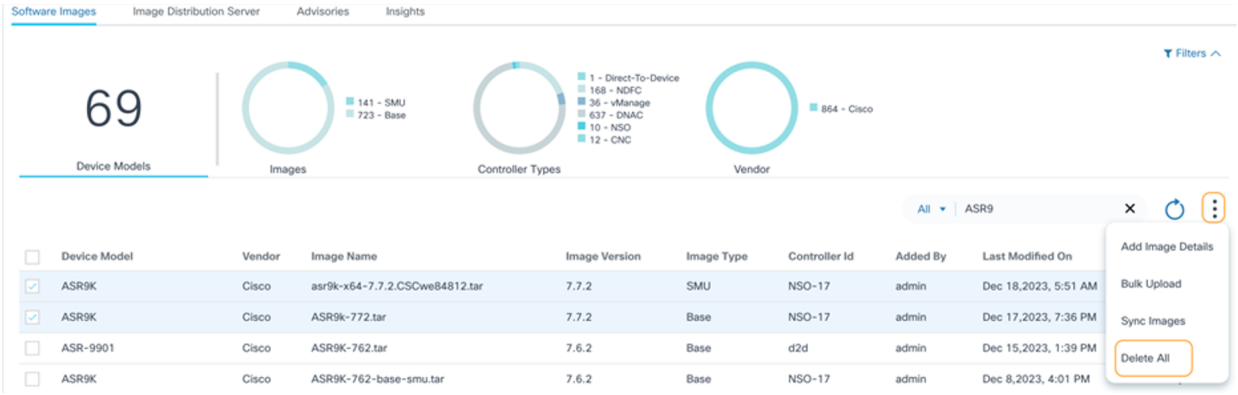
1. Utilice el campo Buscar para localizar la imagen deseada.




Eliminar

2. En la columna Acción de la imagen deseada, seleccione el icono Más opciones > Eliminar para eliminar una imagen.

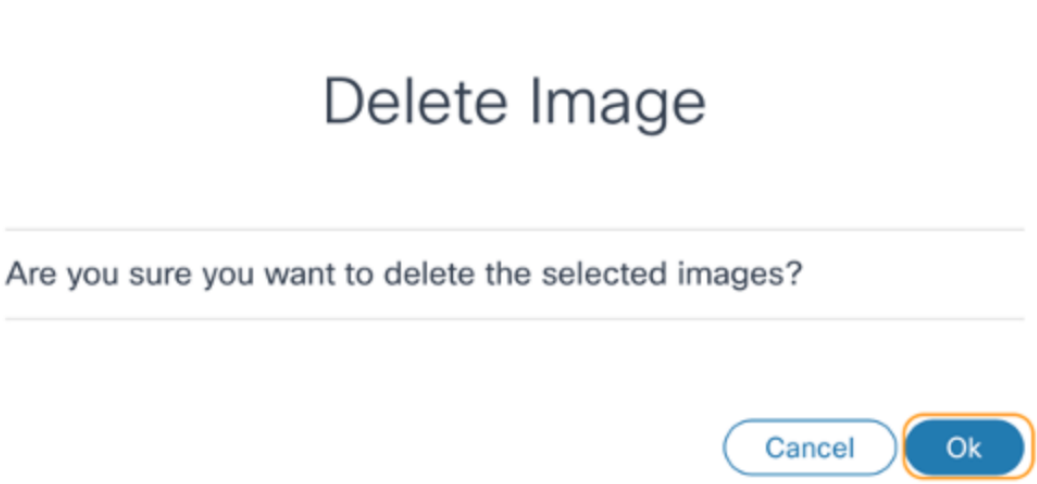
O




Eliminar todo

Seleccione las imágenes que desee y seleccione el icono Más opciones > Eliminar todo para eliminar varias imágenes.

Aparecerá una confirmación.




Confirmación

3. Click OK. Aparecerá una notificación de progreso seguida de un mensaje de confirmación.

Nota: Debe tenerse en cuenta la siguiente lista.

- Los metadatos de imagen solo se pueden agregar para controladores NSO, ANSIBLE, de conexión directa con el dispositivo y CNC. Para el resto de los controladores empresariales, se aprovecha la capacidad SWIM integrada y se descubren imágenes de los controladores respectivos
- La capacidad de detección de imágenes no es compatible con los servidores de imágenes de controladores CNC, NSO, ANSIBLE, de conexión directa con el dispositivo.
- De forma predeterminada, los metadatos de la imagen del servidor remoto de vManage contienen UUID para el parámetro de versión posterior a la sincronización. Los usuarios deben editar los metadatos y actualizar el UUID con la versión correspondiente. La versión de la imagen correspondiente se puede identificar desde el controlador vManage o iniciando sesión en el dispositivo donde se encuentra la imagen.

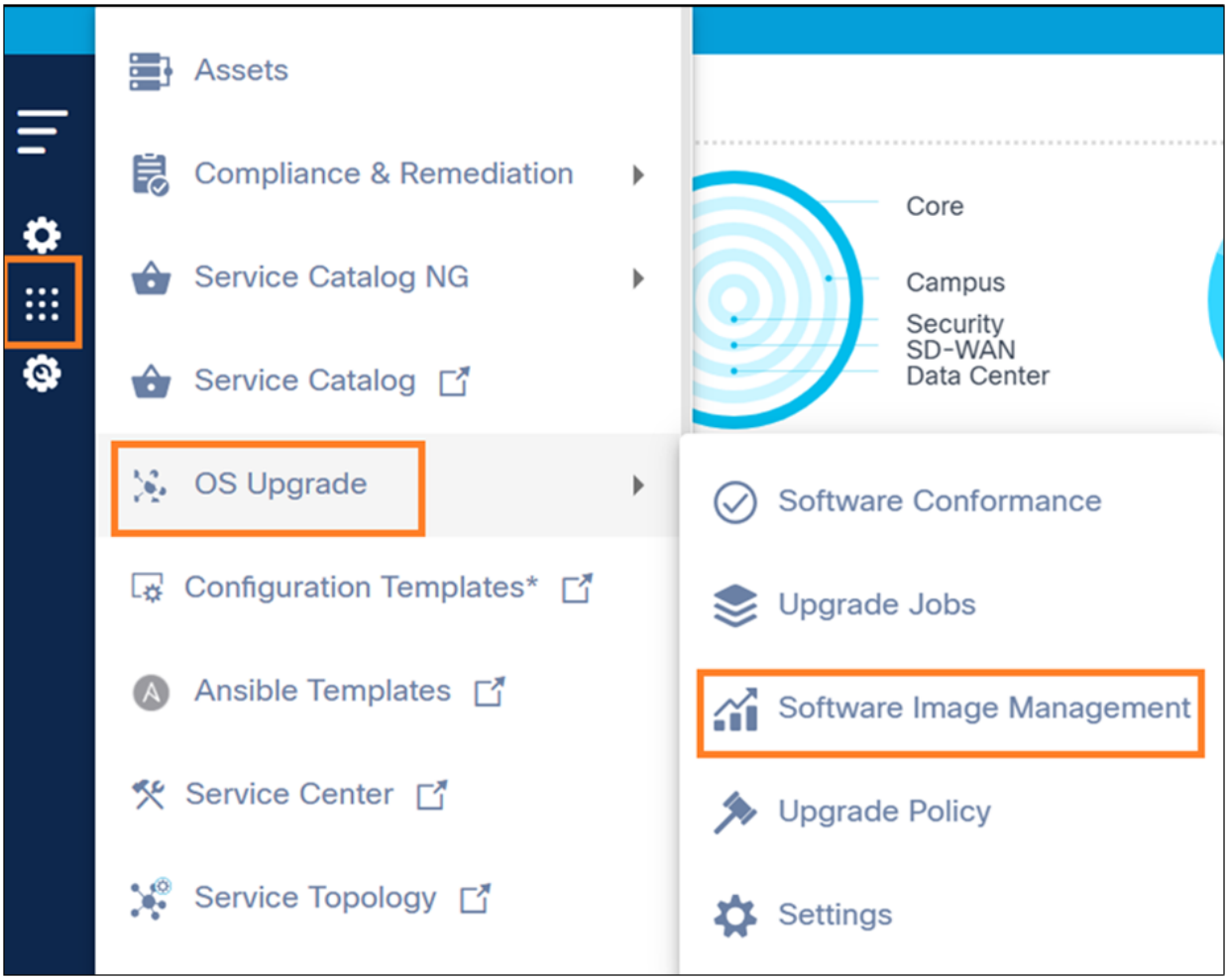
## Gestión del servidor de distribución de imágenes

### Servidor de distribución de imágenes

El componente permite a los usuarios de Operations mantener los detalles del servidor del repositorio de imágenes para los controladores CNC, NSO, ANSIBLE, FMC y Direct-To-Device que no tienen soporte de administración del repositorio de imágenes OOB.

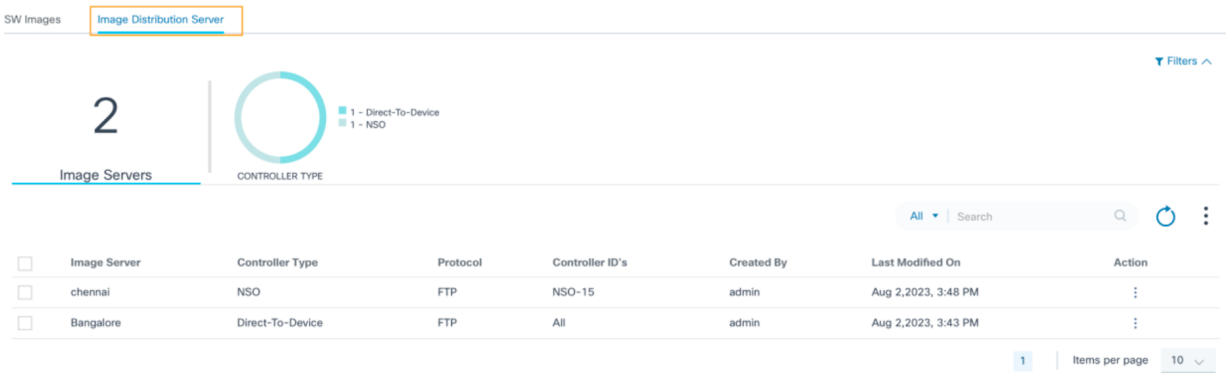
Para acceder a la página Servidor de distribución de imágenes:

1. Inicie sesión en BPA con credenciales que tengan acceso de administración al servidor de distribución de imágenes.




Gestión de imágenes de software

2. Seleccione OS Upgrade > Software Image Management.




Ficha Servidor de distribución de imágenes

3. Haga clic en la pestaña Servidor de distribución de imágenes.

La pestaña Servidor de distribución de imágenes contiene lo siguiente:

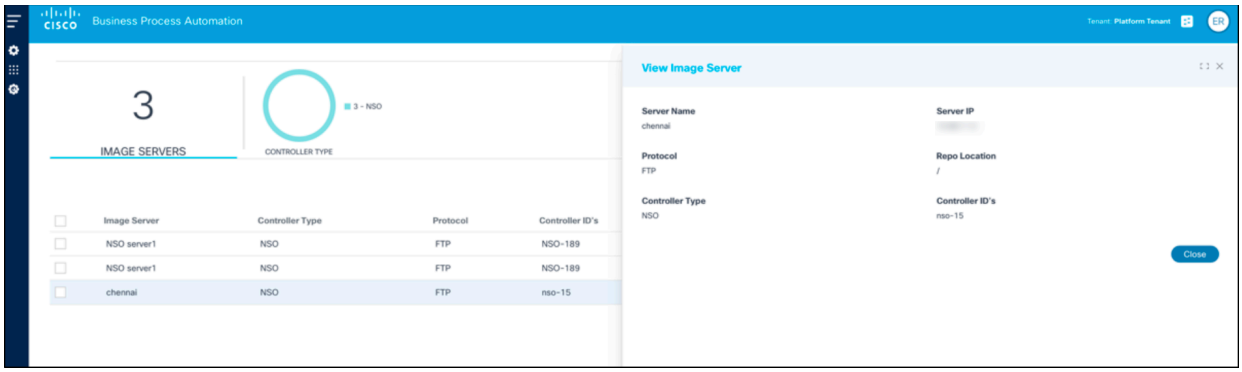
- Una sección de análisis, que se muestra en la parte superior, que proporciona lo siguiente:
    - El número total de servidores de imágenes incorporados en esta instancia de BPA
    - Un filtro rápido Tipo de controlador que permite filtrar servidores de imágenes en función del tipo de controlador (por ejemplo, NSO, Direct-to-Device, CNC, ANSIBLE, FMC); el número indica el número total de servidores de distribución de imágenes asociados a ese tipo de controlador
- Un icono Más opciones que proporciona las siguientes funcionalidades:
    - Agregar servidor de imágenes: Agregar nuevo servidor de distribución de imágenes
    - Eliminar todos: Eliminación masiva de servidores de distribución seleccionados
- Un filtro Search que se puede utilizar para buscar en los servidores de distribución e incluye los siguientes filtros de búsqueda exclusivos:
    - Todos: Busca en todos los campos
    - Servidor de imágenes: Busca servidores con un nombre de servidor específico
    - ID del controlador: Busca servidores asociados a un identificador de controlador específico
- Un icono Refresh que se puede utilizar para actualizar la página y borrar los filtros seleccionados
- Los servidores de distribución existentes se muestran en una tabla de cuadrícula con las siguientes columnas:
- Servidor de imágenes: Nombre único del servidor del repositorio
    - Tipo de controlador: Tipo de controlador al que se aplica este servidor de imágenes
    - Protocolo: Protocolo de copia compatible con el servidor del repositorio

---

Nota: Sólo se admiten FTP, SCP y el protocolo seguro de transferencia de archivos (SFTP)

---

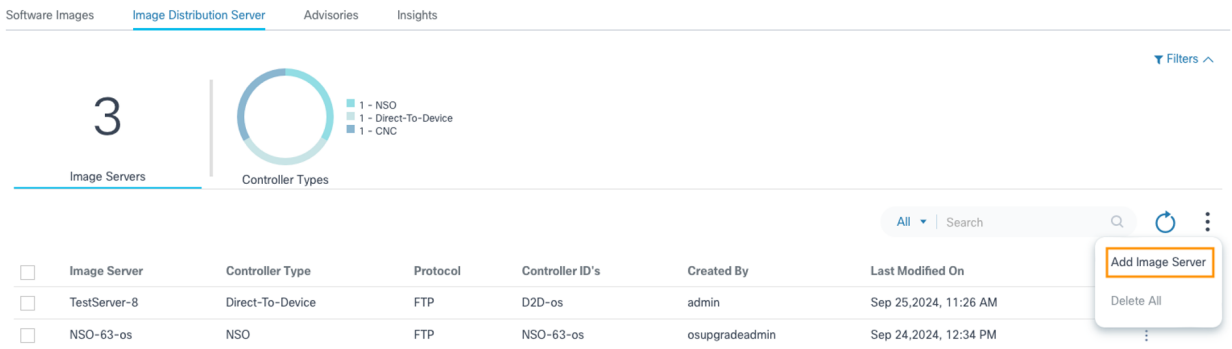
- ID de controlador: Instancias de controlador para las que el servidor de repositorio actual es utilizable o aplicable; instancia del controlador hace referencia a los dispositivos administrados a través de ese controlador
- Creado por: El usuario que incorporó el servidor del repositorio
- Última modificación el: Marca de tiempo de la última actualización de los detalles del servidor
- Acción: Proporciona acciones específicas de la fila como Editar y Eliminar




Panel Ver servidor de imágenes

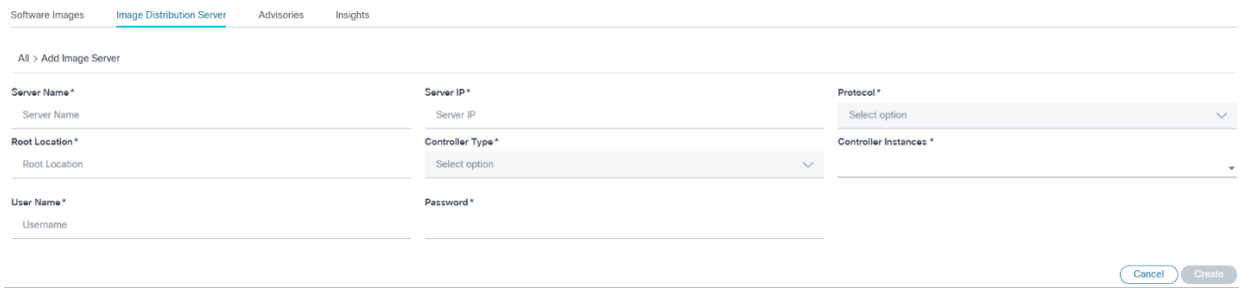
- Al hacer clic en una fila, se abre la ventana Ver servidor de imágenes

Adición de detalles del servidor de imágenes

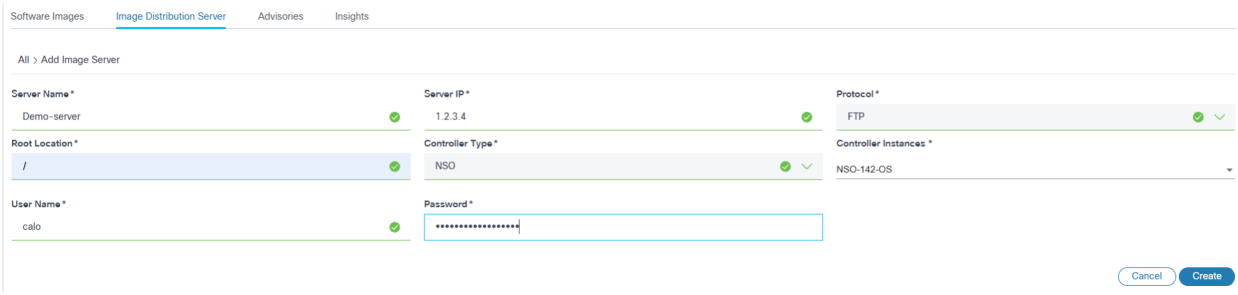



Agregar servidor de imágenes

4. Seleccione el icono Más opciones > Agregar servidor de imágenes. Se muestra la página Add Image Server.




Agregar detalles del servidor de imágenes




Agregar servidor de imágenes con detalles de ejemplo

5. Introduzca información en los campos siguientes:

- Nombre del servidor: Nombre único para el servidor del repositorio de imágenes
- IP del servidor: Dirección IPv4 del servidor del repositorio

---

Nota: Asegúrese de que esta IP es accesible desde los dispositivos de red antes de agregarla.

---

- Protocolo: Compatible con el servidor del repositorio de imágenes para la copia de la imagen

---

Nota: Solo se admiten los protocolos FTP, SCP y SFTP.

---

- Ubicación del Repo: Ruta base de los archivos de imagen en el servidor del repositorio

---

Nota: Si los archivos de imagen están presentes en la raíz de la carpeta de repositorio del servidor de imágenes, entonces "/" funciona como un valor.

---

- Tipo de controlador: Tipo de controlador para el que es aplicable el servidor de imágenes actual

---

Nota: Solo se admiten NSO, Direct-To-Device, CNC y ANSIBLE.

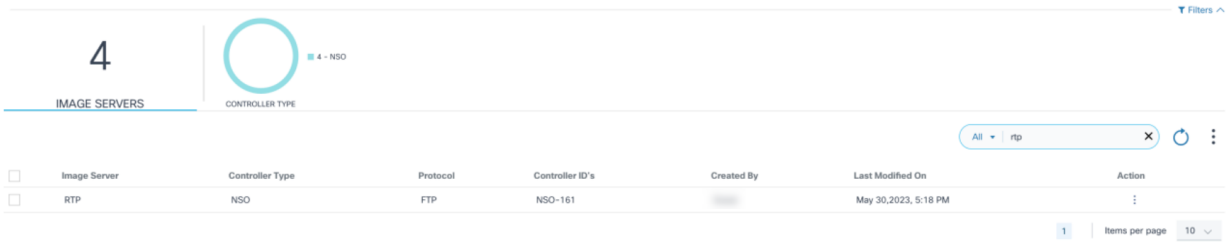
---

- Instancias de controlador: Una o más instancias de controlador aplicables basadas en los dispositivos que administran para los cuales el servidor de repositorio de imágenes dado debería ser utilizado para copiar la imagen
- Usuario: Credenciales personalizadas para acceder a los archivos de imagen desde el repositorio

6. Haga clic en Crear. Aparecerá la notificación de progreso seguida de un mensaje de

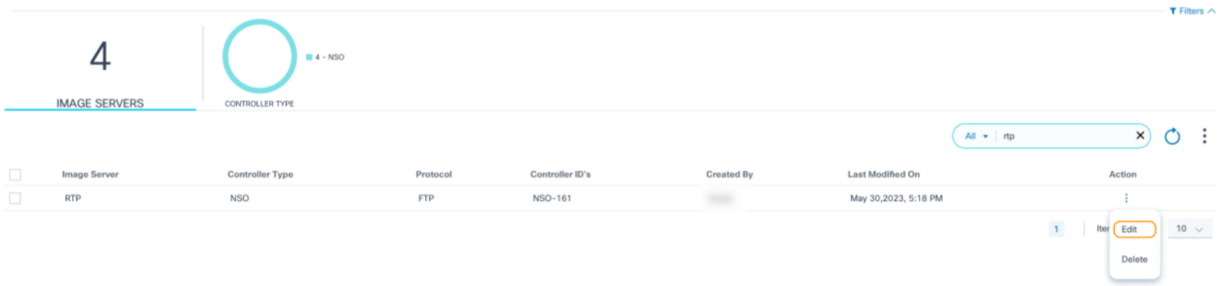
confirmación.

## Edición de detalles del servidor de imágenes




Búsqueda del servidor de imágenes

7. Mediante el campo Buscar, localice el servidor de distribución que debe actualizarse.

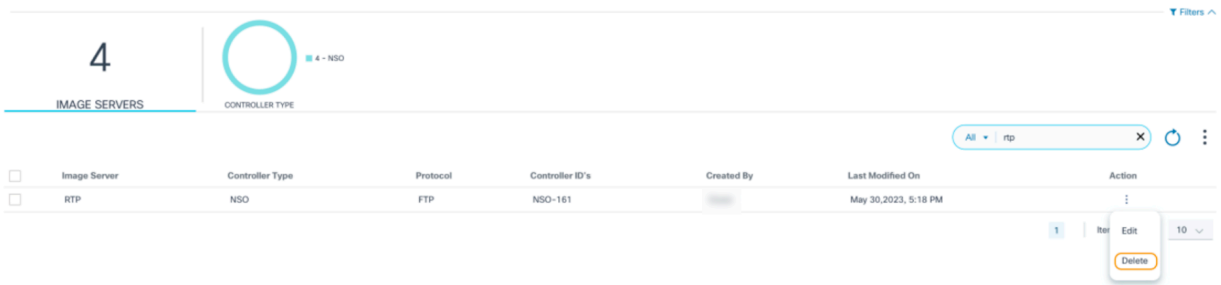



Editar servidor de imágenes

8. En la columna Acción, seleccione el icono Más opciones > Editar.
9. Actualice los parámetros necesarios.
10. Click Save. Aparecerá una notificación de progreso seguida de un mensaje de confirmación.

## Eliminación de detalles del servidor de imágenes

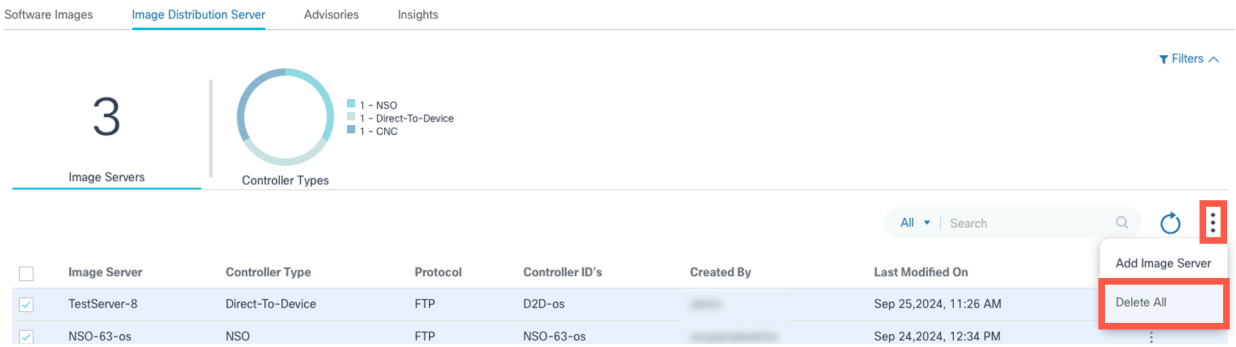
1. Con el filtro Buscar, localice los servidores deseados.




Eliminar servidor de imágenes

2. En la columna Acción, seleccione el icono Más opciones > Eliminar para eliminar un único servidor de distribución.

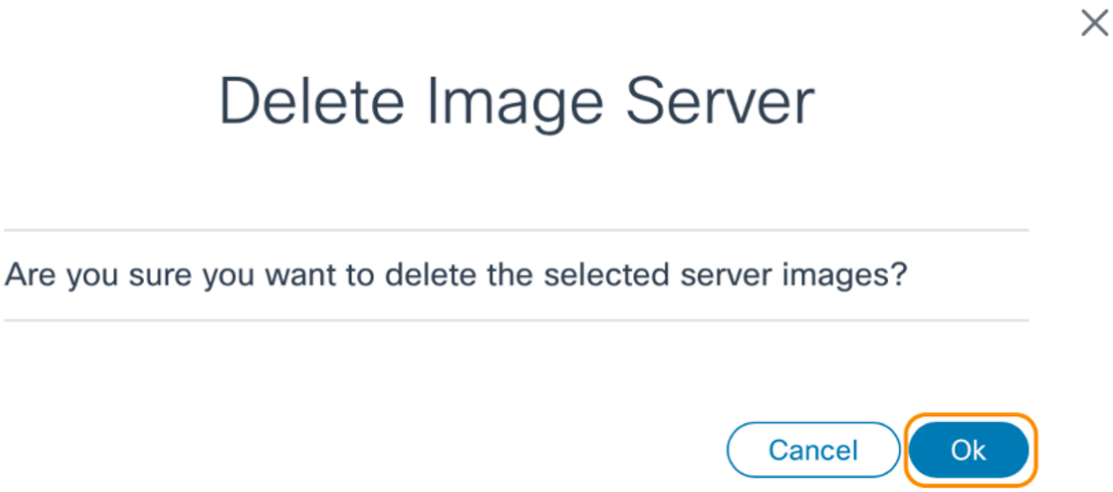
O




Eliminar varios servidores de imágenes

Seleccione los servidores deseados y seleccione el icono Más opciones > Eliminar todo para eliminar varios servidores de distribución.

Aparecerá una confirmación.




Confirmación de eliminación

3. Click OK. Las notificaciones de progreso se muestran seguidas de un mensaje de confirmación.

## Perspectivas del software

Software Insights detecta todas las vulnerabilidades de seguridad, como los avisos de seguridad, los errores y el fin de vida útil del software expuestos por los recursos de red. También

proporciona sugerencias de software para los modelos de dispositivos administrados por Cisco Catalyst Center y los controladores NDFC. Permite a los usuarios administradores seleccionar la versión de software sugerida para los recursos de red y crea una política de conformidad para los modelos de dispositivos si la sugerencia está disponible.

Prerequisites

- Habilite el adaptador para obtener información. El adaptador para el servidor de información de Cisco, denominado "Cisco-Insights-Adapter", está disponible en línea. Para integrarse con algunos servidores de terceros de Insights, es necesario crear los adaptadores correspondientes. Consulte Configuración de Insights Adapter en la Guía del Desarrollador de BPA para obtener más información.
- Se requiere conectividad a Internet para que el sistema BPA se conecte a la nube de Cisco.
- Verifique que client_id y client_secret estén en la configuración del adaptador antes de continuar con la operación de sincronización.
- Si es necesario, el proxy para Internet se puede configurar siguiendo estos pasos.
- Para el tipo de SO IOS-XR, la asignación personalizada de series a modelos de dispositivos se puede realizar en Reference Data Management (RefD) según sea necesario. Para obtener más información sobre la asignación personalizada de series a modelos, consulte la Guía del desarrollador de BPA.
- Los dispositivos BPA Kubernetes requieren acceso a Internet para recopilar los avisos, los errores y los detalles del fin de vida útil de Cisco. Si la red BPA no tiene acceso directo a Internet, pero está disponible a través de proxy, siga los pasos a continuación para hacer que los dispositivos Kubernetes utilicen el proxy para Internet.

1. Actualice el script con la dirección de proxy real en lugar de **<<**http://proxy-domain.com:port**>>**.
2. Configure los parámetros de entorno con cada grupo de dispositivos en los gráficos de implementación YAML o helm.
3. Ejecute el siguiente script en el nodo Kubernetes agregando todos los nombres de implementación en la configuración NO_PROXY o no_proxy.

```
#!/bin/bash
# Define the environment variables
HTTP_PROXY="<



     >"
HTTPS_PROXY="<< http://proxy-domain.com:port>>"
http_proxy="<



      >"
https_proxy="<
```

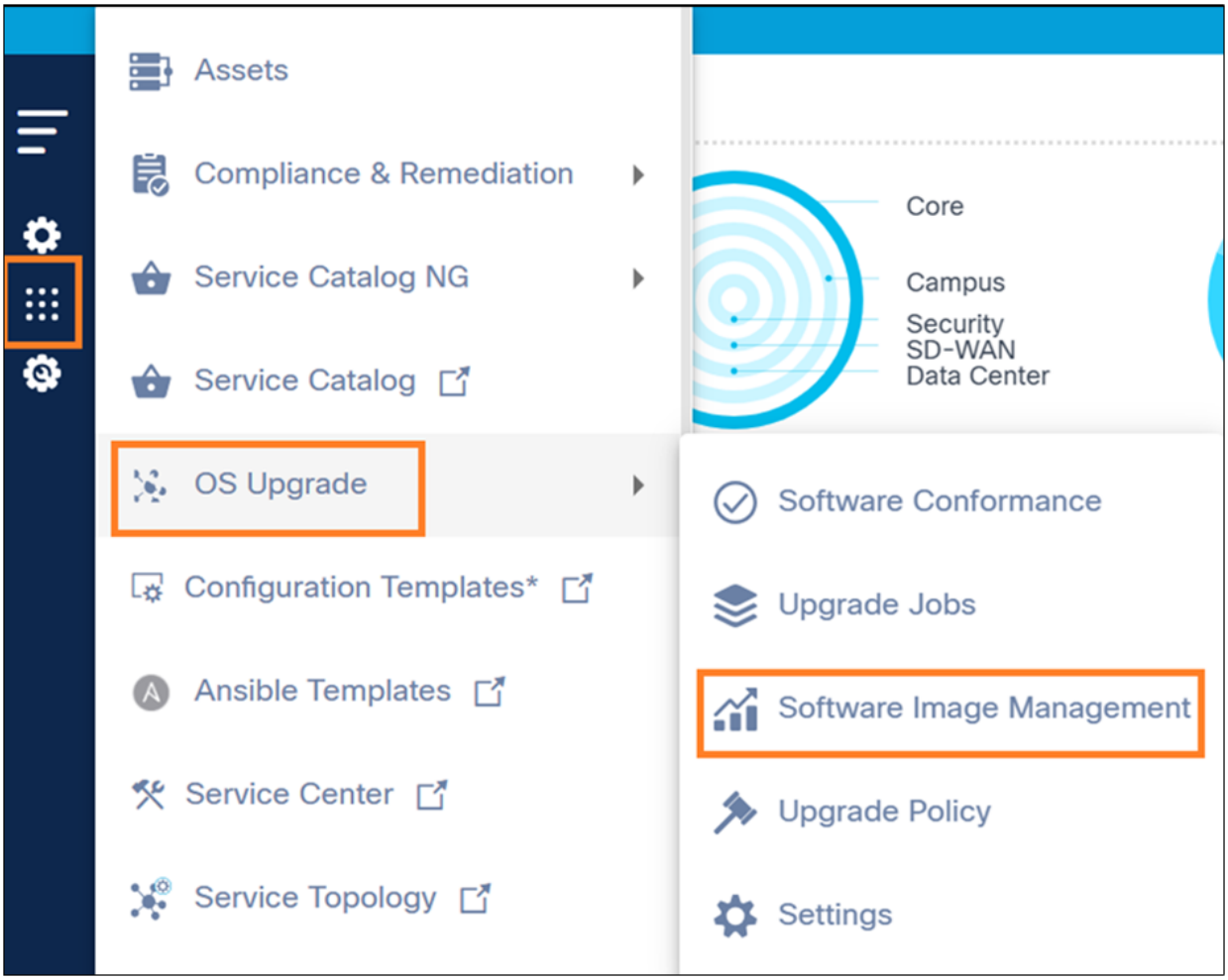
```
       >”

NO_PROXY="*.svc,localhost,127.0.0.1,192.168.0.0/16,10.0.0.0/8,172.16 .0.0/12,adaptor-builder,agent-mana

no_proxy="*.svc,localhost,127.0.0.1,192.168.0.0/16,10.0.0.0/8,172.16 .0.0/12,adaptor-builder,agent-mana
# Get the list of deployments
deployments=$(kubectl get deployments -n bpa-ns | grep -v NAME | awk '{print $1}')

# Loop through each deployment and set the environment variables
for dp in $deployments;do
         kubectl set env deployment/$dp\
                     HTTP_PROXY=$HTTP_PROXY \
                     HTTPS_PROXY=$HTTPS_PROXY \
                    http_proxy=$http_proxy \
                     https_proxy=$https_proxy \
                     NO_PROXY=$NO_PROXY \
                     no_proxy=$no_proxy \
                    -n bpa-ns
done
```

Nota: Al configurar el proxy como se ha descrito anteriormente, el adaptador de información puede acceder a la red de Cisco y descargar los datos de información de software necesarios en BPA. Para conectarse a cualquier otro servidor Insights externo directamente sin un proxy, asegúrese de agregarlos a la variable no_proxy.

Obtención de datos de perspectivas de software en BPA

Para sincronizar los datos de perspectivas de software en BPA:

1. Inicie sesión en BPA con credenciales que tengan acceso a los datos de sync software insights.




Navegación de gestión de imágenes de software

2. Seleccione OS Upgrade > Software Image Management en el panel lateral.


Ficha Avisos

3. Haga clic en la pestaña Asesores.

Sincronización para obtener información sobre el software en BPA


Sincronización para obtener información sobre el software en BPA

4. Haga clic en Sync.

Esto detecta todos los avisos de seguridad, errores de prioridad, boletines de fin de vida útil y

sugerencias de software relacionados con los activos presentes en el inventario. Los avisos de seguridad y las fechas de fin de vida del software se determinan en función del tipo de SO y la versión de software. Los bugs de prioridad y las sugerencias de software se determinan en función de la ID del producto y la versión del software.

Última actualización muestra la fecha y la hora en que se sincronizaron por última vez los datos de información y el campo Estado de sincronización muestra el último estado de sincronización.

---

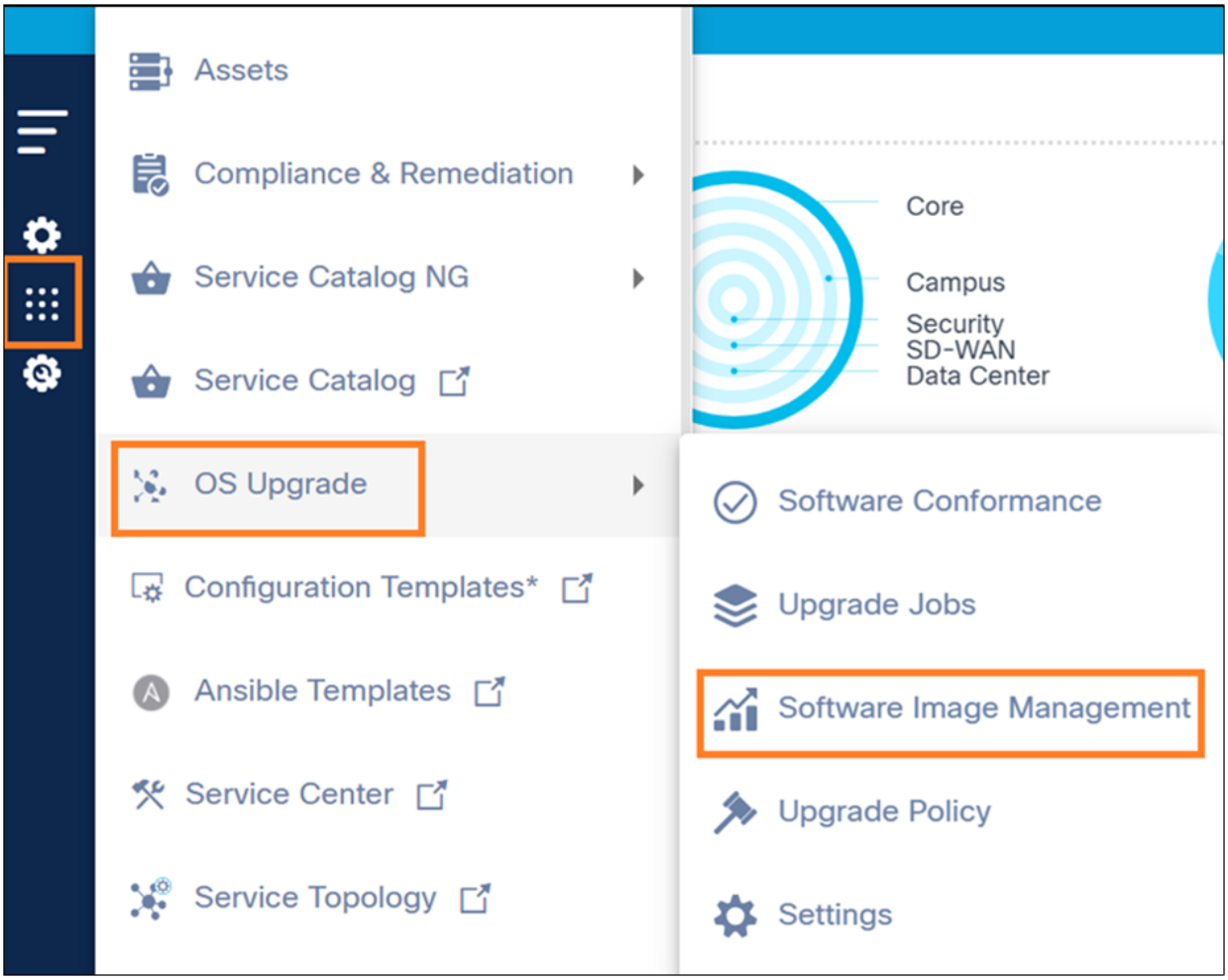
Nota: Todas las recomendaciones, errores, notas de la versión y sugerencias aplicables se obtienen de la nube de Cisco a través del archivo "Cisco-Insights-Adapter".

---

Visualización y gestión de avisos de seguridad

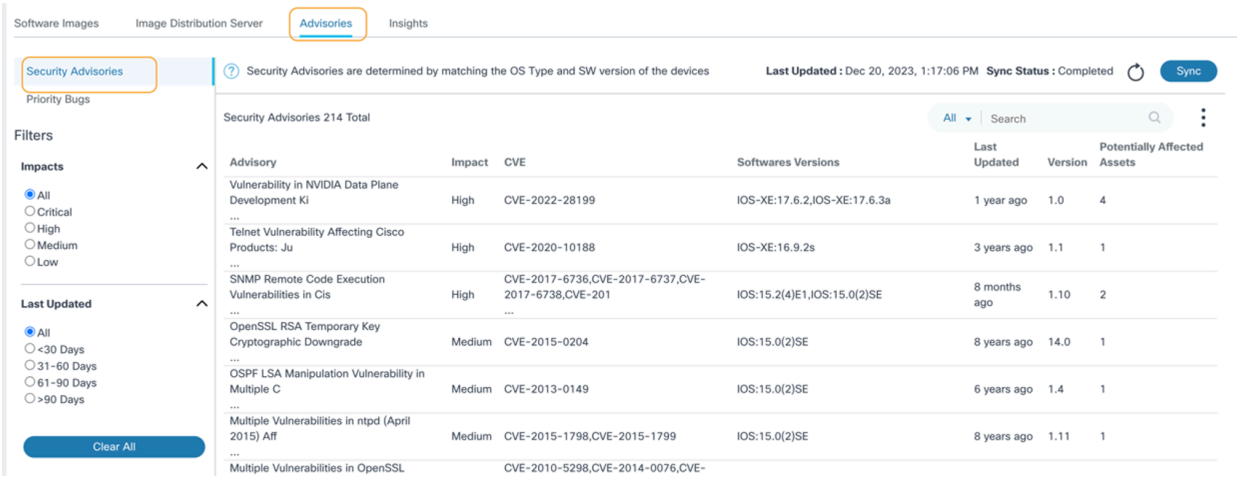
Para acceder a la página Asesores:

1. Inicie sesión en BPA con credenciales que tengan acceso de gestión a los asesores.




Navegación de gestión de imágenes de software

2. Seleccione OS Upgrade > Software Image Management.



Avisos de seguridad

3. Haga clic en la pestaña Asesores. De forma predeterminada, se abre la página Asesores de seguridad.

Se muestran las siguientes opciones para filtrar los datos de los asesores:

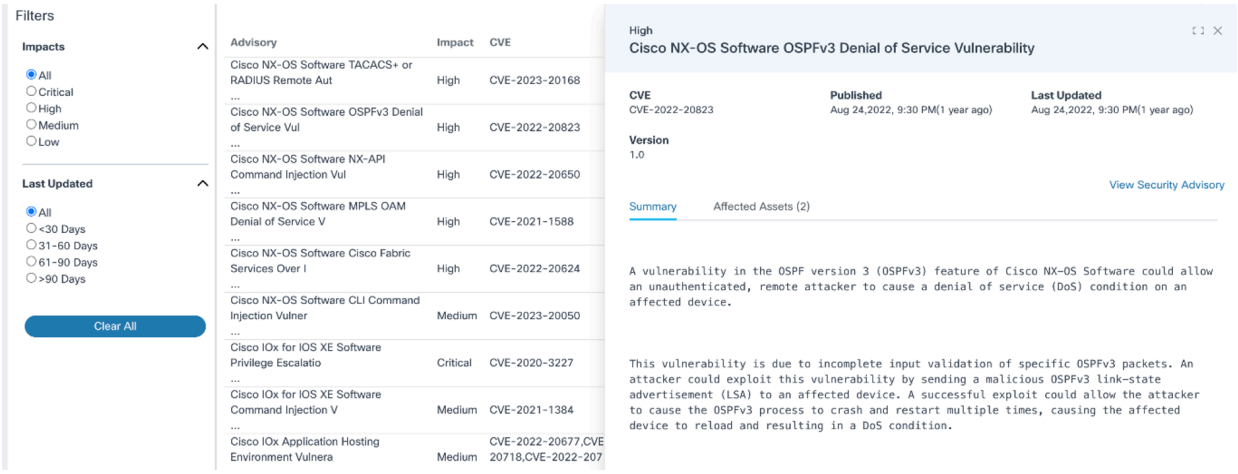
- Impactos permite filtrar en función de la gravedad del aviso; Todo está seleccionado de forma predeterminada
- Última actualización permite el filtrado según la fecha de la última actualización del aviso; Todo está seleccionado de forma predeterminada
- Borrar todo restablece los filtros seleccionados
- El filtro Search se utiliza para buscar los asesores e incluye los siguientes filtros de búsqueda exclusivos:
- Todos: Realiza búsquedas en columnas como Advisory, CVE y Software.
- Asesoramiento: Busca asesores con los términos especificados en la búsqueda
- CVE: Busca recomendaciones con exposiciones y vulnerabilidades comunes (CVE) específicas.
- Versiones de software: Busca recomendaciones asociadas con tipos de SO o versiones de software específicos
- El icono Refresh se utiliza para actualizar la página y borrar los filtros seleccionados
- Los asesores existentes se muestran con las columnas siguientes:
    - Asesoramiento: Resumen de las recomendaciones
    - Impacto: Gravedad de aviso
    - CVE: CVE asignados
    - Versiones de software: Tipo de SO y versiones de software afectadas
    - Última actualización: Fecha y hora en que se actualizó el aviso por última vez
    - Versión: Versión de asesoramiento
    - Recursos potencialmente afectados: Número de activos que podrían verse afectados por el aviso

- Al hacer clic en el campo de encabezado se ordenan los asesores

---

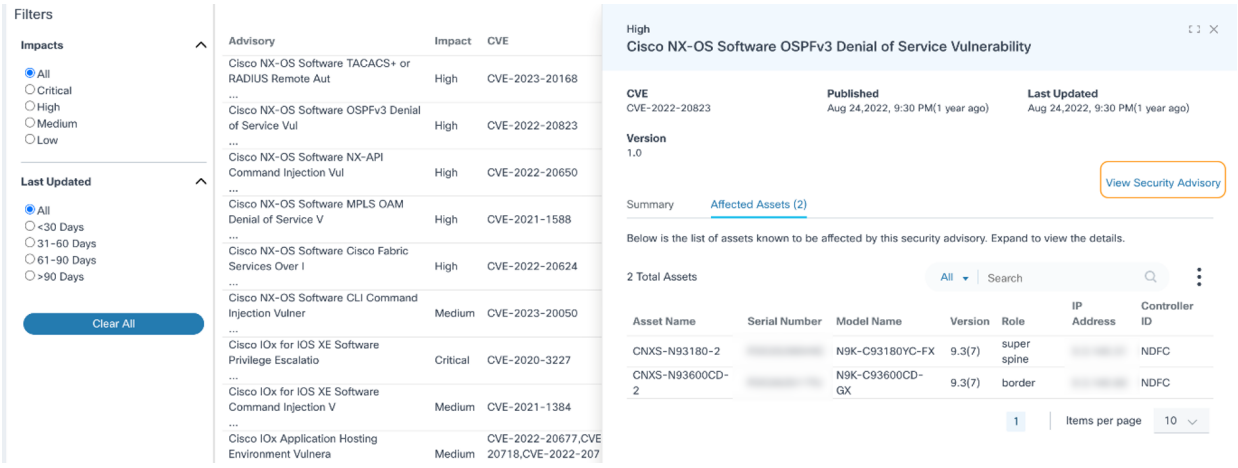
Nota: La clasificación no es una opción para los activos potencialmente afectados.

---




Vista de detalles de asesoría

- Al seleccionar una fila de asesoramiento, se abre una vista detallada del asesor que incluye las siguientes fichas:
    - Resumen Muestra un resumen del asesor seleccionado; se muestra de forma predeterminada
    - Recursos afectados: Muestra los detalles de activos potencialmente afectados, como el nombre del activo, el número de serie, el nombre del modelo, la versión del software, la dirección IP y el ID del controlador; en esta ficha se pueden ordenar y buscar los activos



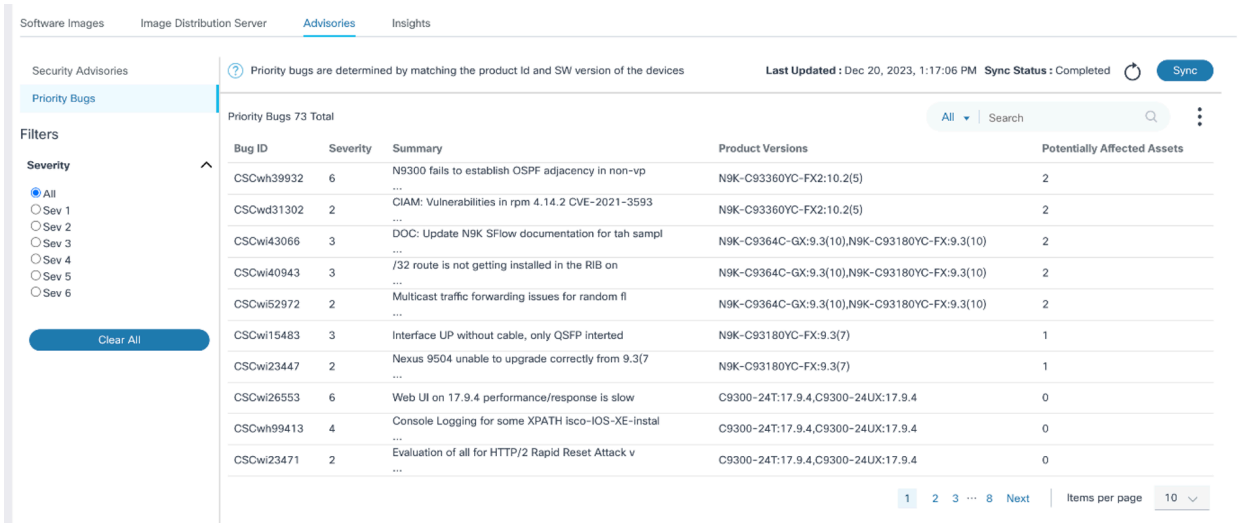

Ver aviso de seguridad

- Ver el enlace Asesor de seguridad: Se desplaza a la página de asesoramiento oficial

Visualización y administración de errores de prioridad


Seleccionar errores de prioridad

Después de abrir la página Asesores como se describe en la sección anterior, haga clic en la pestaña Errores de Prioridad. Se muestra la página Priority Bugs.



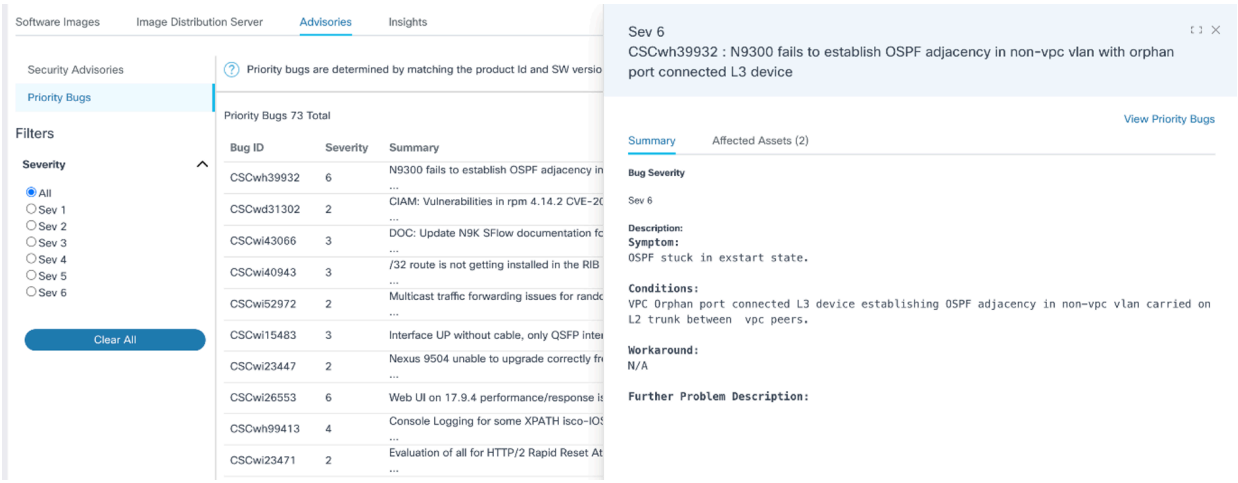

Errores de prioridad

Las siguientes opciones están disponibles en la página Priority Bugs:

- Un filtro Severity que permite el filtrado basado en la severidad del bug; Todo está seleccionado de forma predeterminada
- El filtro Search se puede utilizar para buscar errores e incluye los siguientes filtros de búsqueda exclusivos:
    - Todos: Busca en todos los campos
    - ID de la falla: Busca errores con un Id. de error especificado
    - Resumen Busca errores con palabras clave específicas presentes en el resumen
    - Versiones de productos: Busca errores asociados a una versión de software o una ID de producto específica.
- El icono Refresh se puede utilizar para actualizar la página y borrar los filtros seleccionados
- Los errores de prioridad se muestran en la tabla con las siguientes columnas:
    - ID de la falla
    - Gravedad: Gravedad del error
    - Resumen Detalles del resumen del error

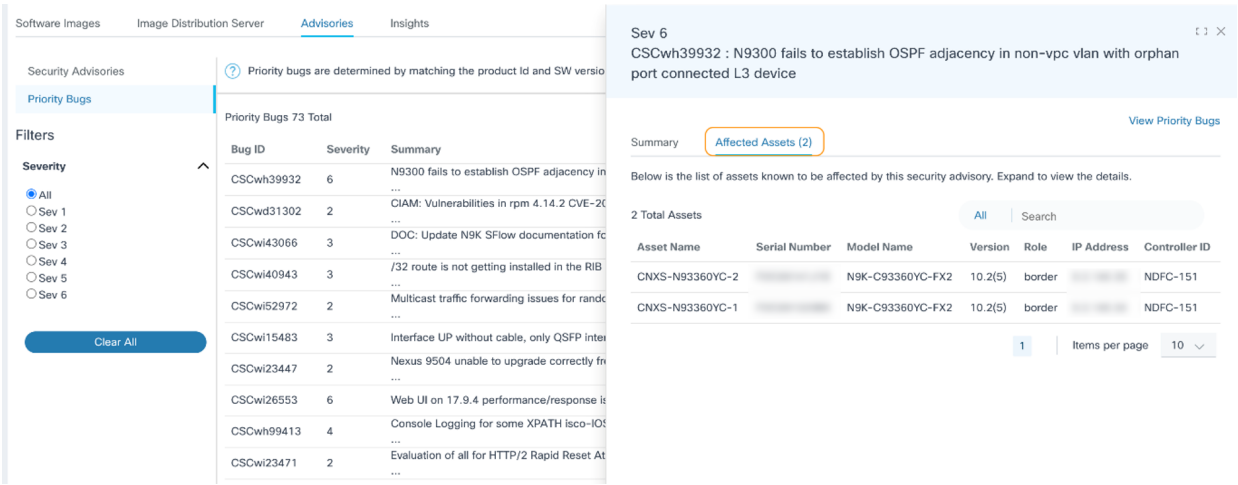
- Versiones de productos: ID del producto y versiones de software afectadas
- Recursos potencialmente afectados: Número de activos que podrían verse afectados por el error

- La ordenación se puede realizar haciendo clic en cualquier encabezado de columna, excepto en los activos potencialmente afectados



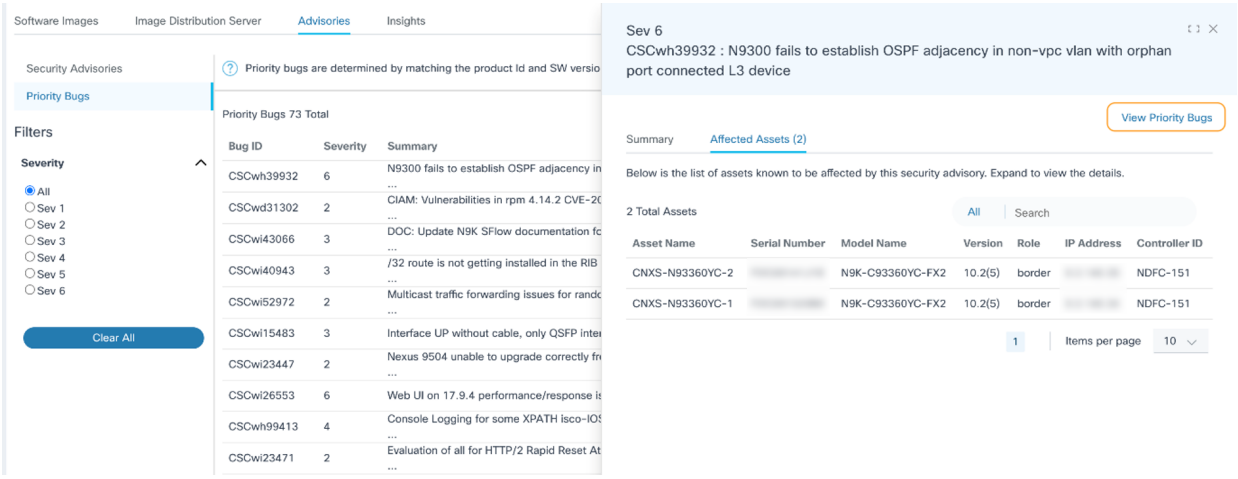

Vista de detalles del error

- Al hacer clic en un error, se abre la vista detallada del error, que incluye lo siguiente:
  - Pestaña Resumen: Muestra los detalles de gravedad del error, descripción y solución alternativa



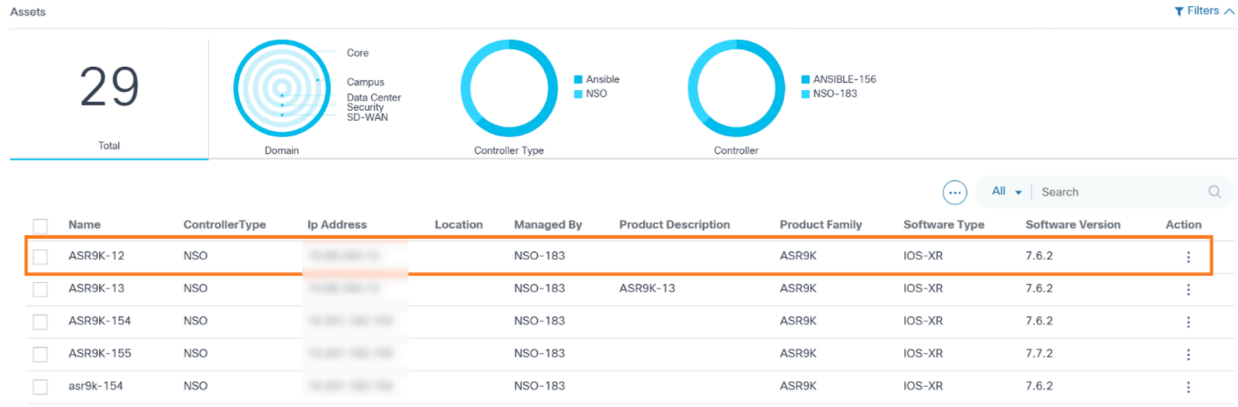

Ficha Activos afectados

- Pestaña Activos afectados: Muestra todos los detalles de los activos potencialmente afectados, como el nombre del activo, el número de serie, el nombre del modelo, la versión del software, la dirección IP y el ID del controlador. en esta ficha se pueden ordenar y buscar los activos



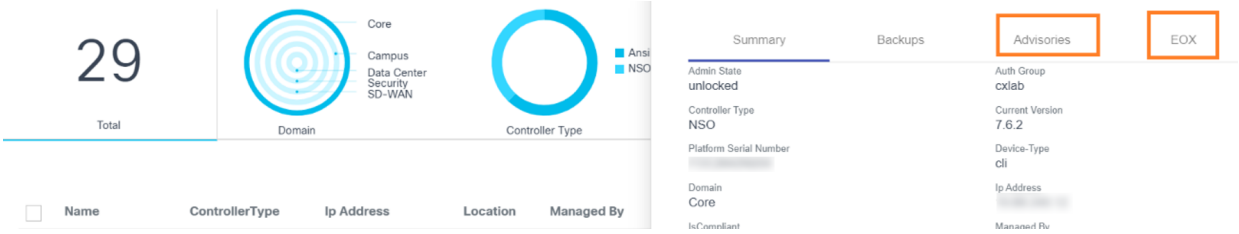

Ver errores de prioridad

- Enlace Ver errores prioritarios: Se desplaza a la herramienta oficial de búsqueda de errores




Recursos

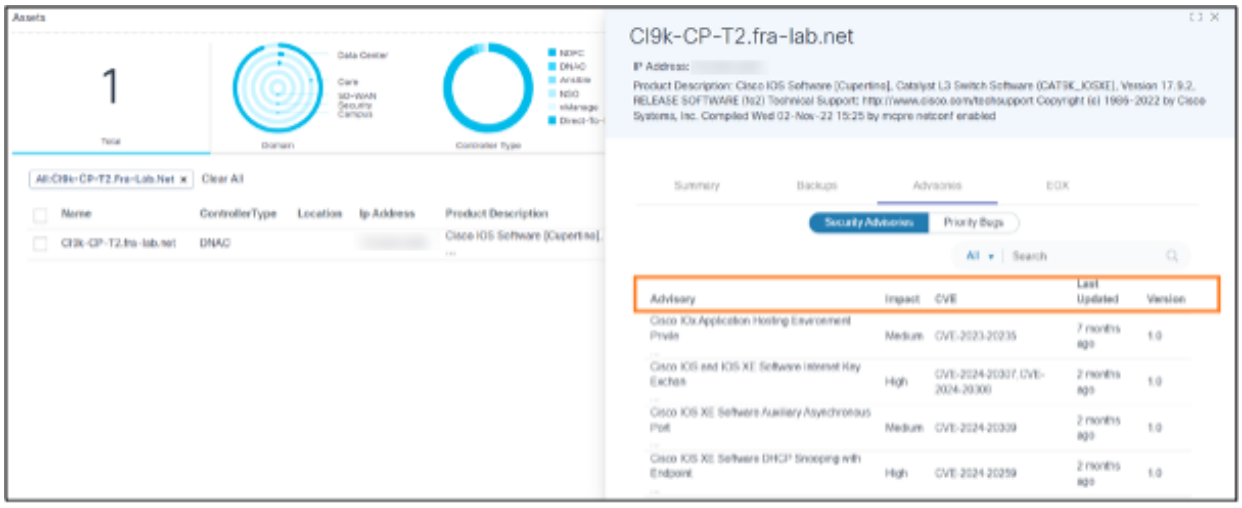
En Asset Manager, los usuarios pueden ver una lista de todos los activos. Al seleccionar un activo, un panel muestra información del nivel del activo, que incluye detalles de vulnerabilidades del software del activo organizados en dos pestañas: Asesores y EOX.




Asesores y EOX

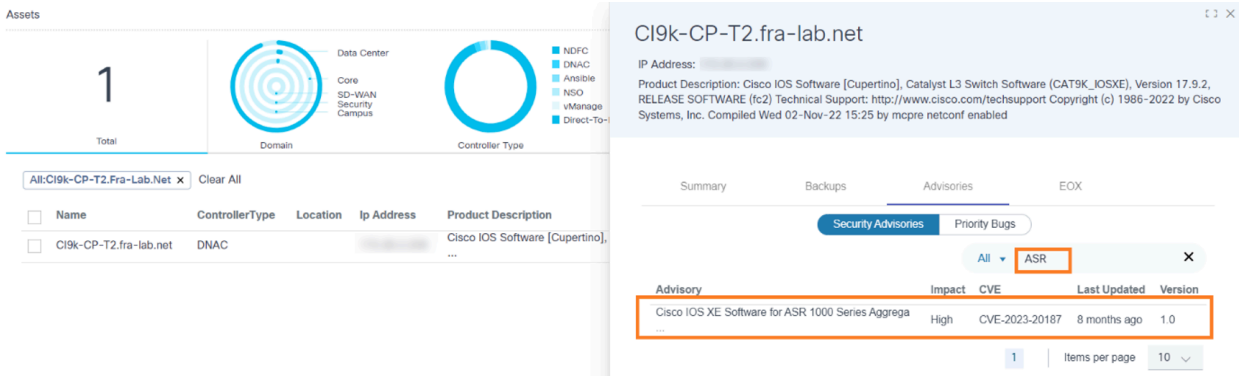
La pestaña Asesores contiene dos subpestañas, Asesores de Seguridad y Errores de Prioridad. En las secciones siguientes se proporciona más información acerca de estas fichas.

Avisos de seguridad

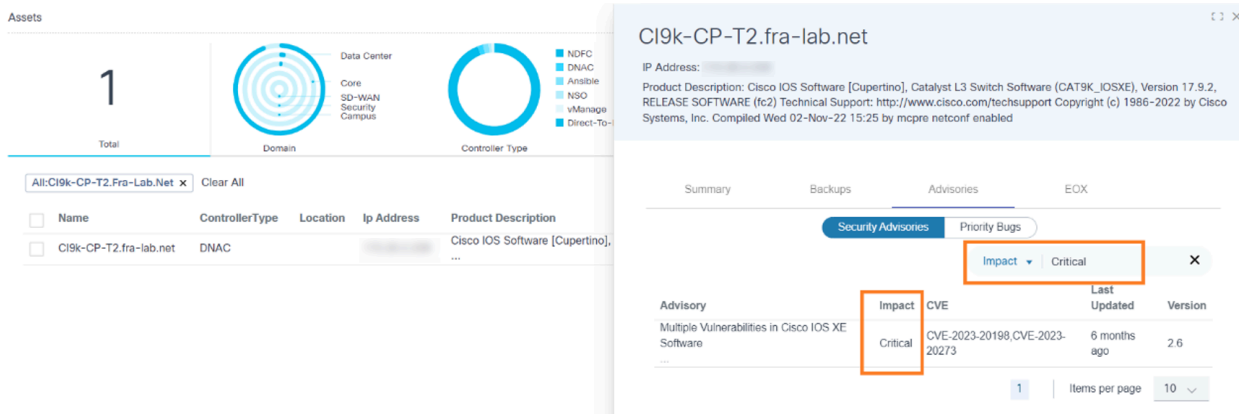



Avisos de seguridad del activo seleccionado

En la subpestaña Asesores de seguridad, los usuarios pueden ver todos los avisos de seguridad que afectan a un activo seleccionado. Las columnas de la tabla de avisos de seguridad incluyen Asesores, Impacto, CVE, Última actualización y Versión.



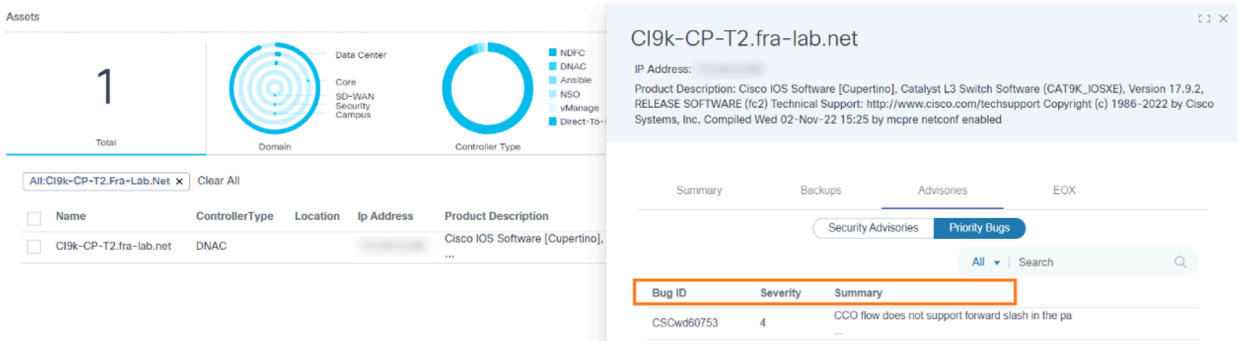

Búsqueda de avisos de seguridad




Búsqueda de avisos de seguridad: opción de impacto

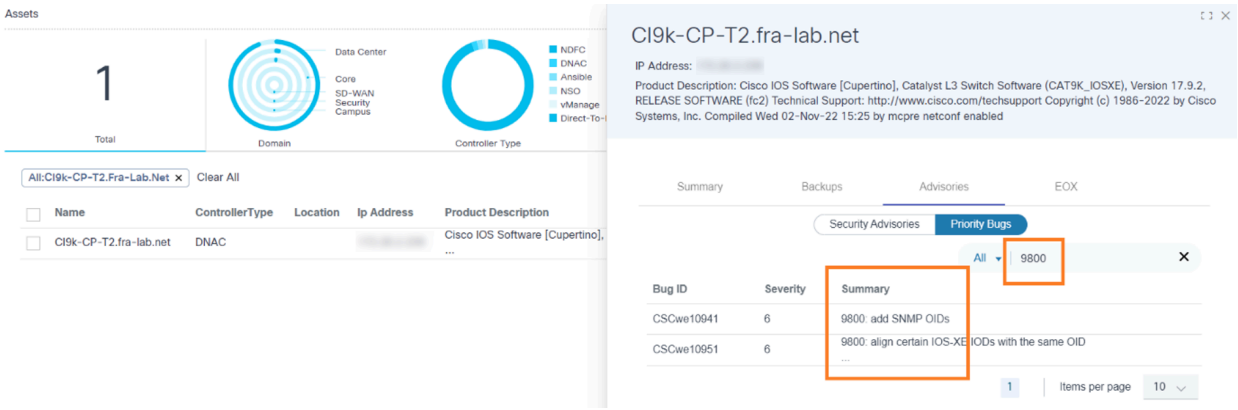
Los usuarios pueden buscar asesores en función de los valores de las columnas Asesores, Impacto, CVE, Última actualización y Versión. La paginación permite a los usuarios navegar entre páginas.

Errores de prioridad

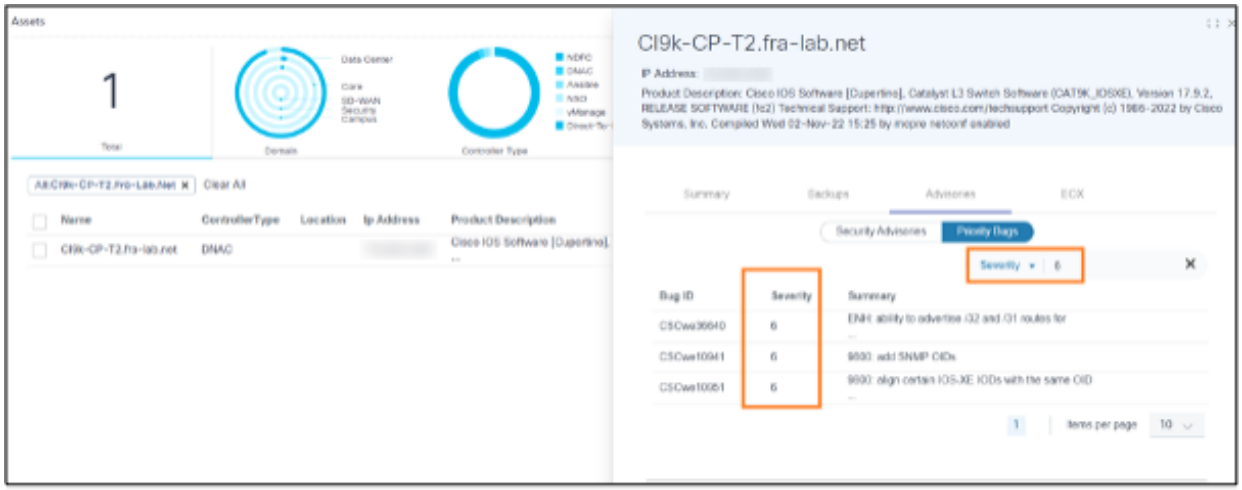



Errores de prioridad que afectan a un activo seleccionado

En la subpestaña Errores de prioridad, los usuarios pueden acceder a todos los errores de prioridad que afectan a un recurso determinado. Las columnas de esta pestaña incluyen Bug ID, Severity y Summary.




Búsqueda de errores de prioridad por resumen




Búsqueda de errores de prioridad por gravedad

Los usuarios pueden buscar errores de prioridad según los valores de las columnas Bug ID, Severity y Summary. La paginación facilita la navegación entre páginas.

EOX


Ficha EOX

La pestaña EOX muestra los datos de fin de vida útil del software específicos de un recurso, incluidas tres fechas importantes:

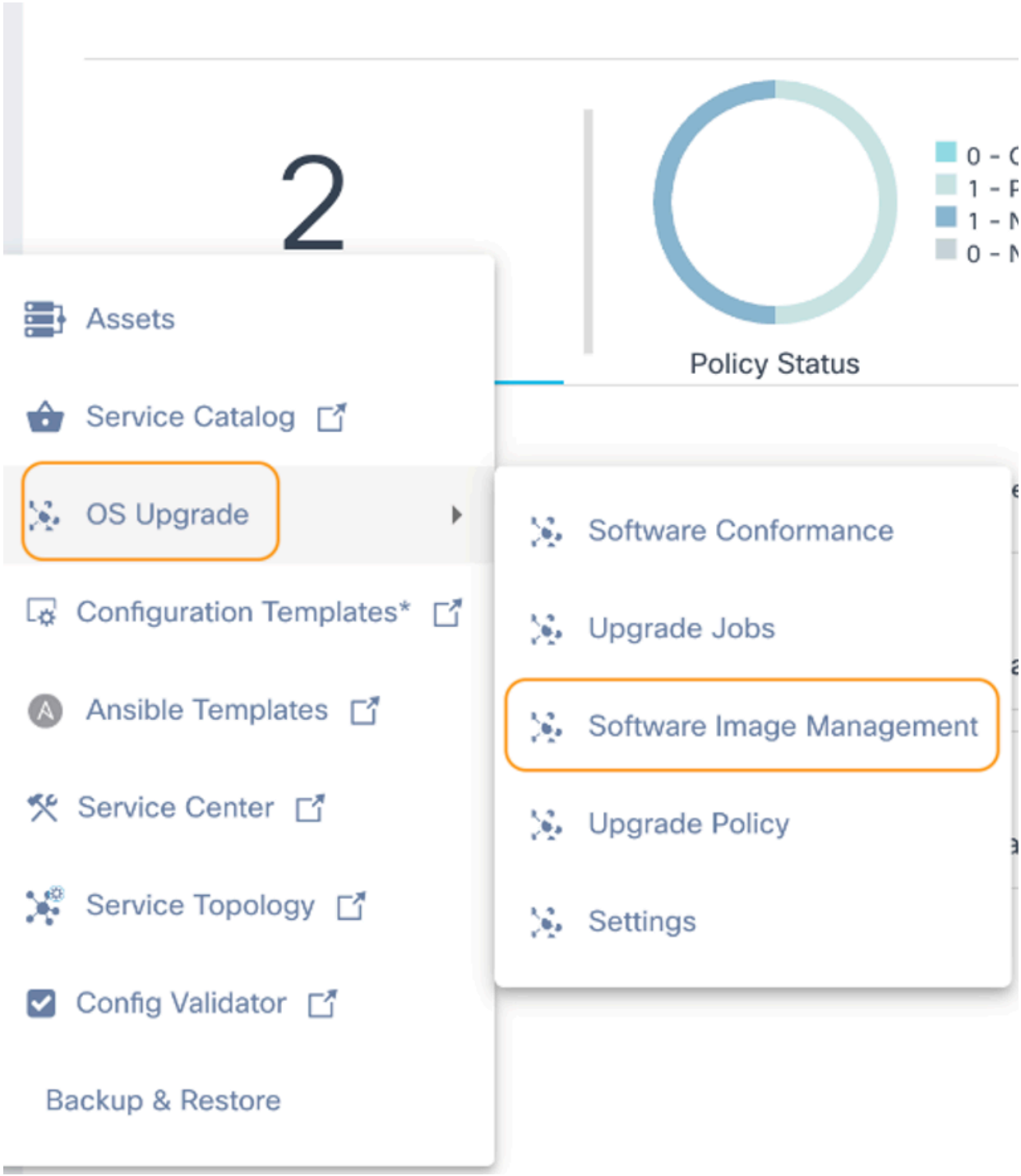
- Fin del mantenimiento del software
- Fin del soporte de seguridad
- Última fecha del soporte

Visualización de Software Insights

Software Insights proporciona sugerencias de software para los modelos de dispositivos administrados por Cisco Catalyst Center y los controladores NDFC, lo que permite a los usuarios administradores crear una política de conformidad para los modelos de dispositivos si la sugerencia está disponible.

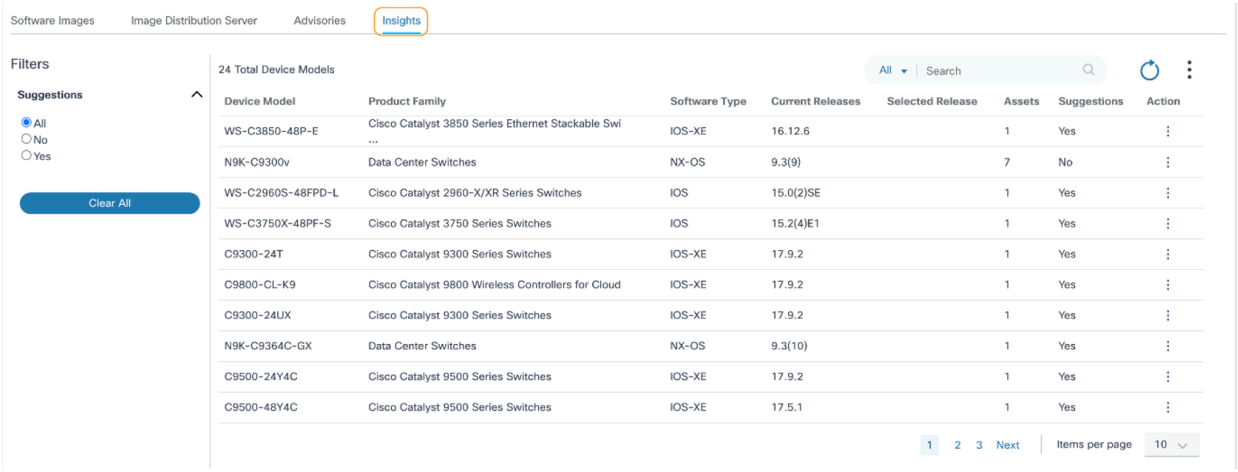
Para acceder a Software Insights:

1. Inicie sesión en BPA con credenciales que tengan acceso de administrador a Insights.




Gestión de imágenes de software

2. Seleccione OS Upgrade > Software Image Management en el panel lateral.

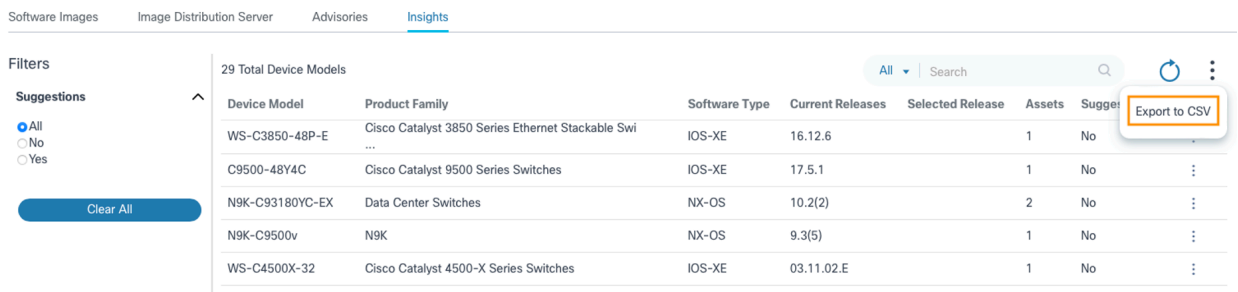



Ficha Perspectivas

3. Haga clic en la pestaña Insights.

La pestaña Insights contiene lo siguiente:

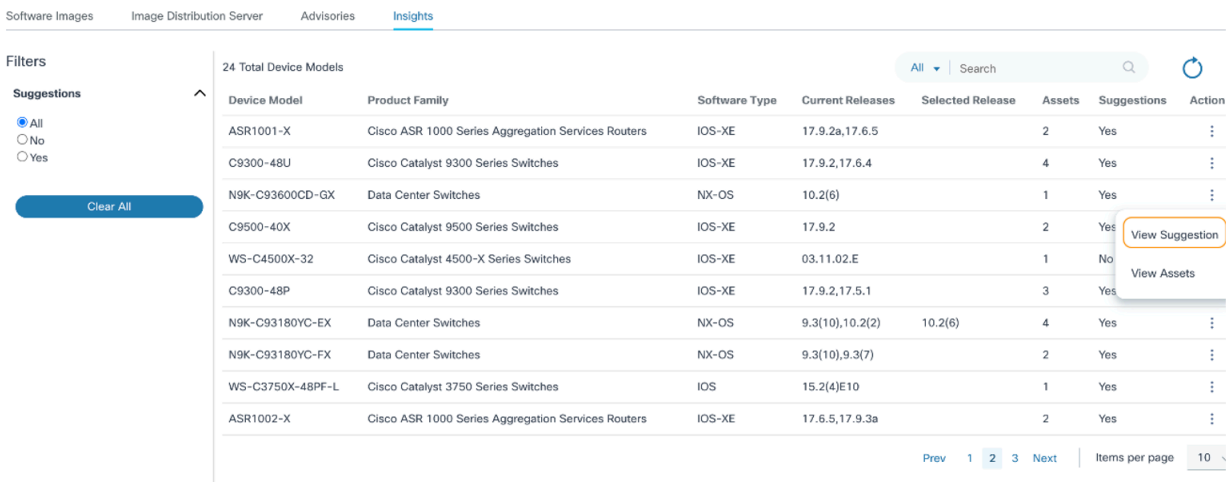
- Filtro que permite a los usuarios filtrar datos según las sugerencias. Todo está seleccionado de forma predeterminada.
    - Sí filtra los datos para los modelos de dispositivos con sugerencias
    - No filtra los datos para los modelos de dispositivos sin sugerencias




Exportar a CSV

- El icono Más opciones proporciona una opción Exportar a CSV para exportar los datos mostrados en la página
    - El icono Refresh actualiza la página y borra los filtros seleccionados
    - El filtro Search se utiliza para buscar los datos e incluye los siguientes filtros de búsqueda exclusivos:
- Todos: Realiza búsquedas en todas las columnas (por ejemplo, Modelo de dispositivo, Familia de productos y Tipo de software).
- Modelo de dispositivo: Busca datos con un nombre de modelo de dispositivo específico
- Familia de productos Busca datos con el nombre específico de la familia de productos
- Tipo de software: Busca datos con un nombre de tipo de software específico

- Los modelos de dispositivos existentes se muestran con las siguientes columnas:
- Modelo de dispositivo: Nombre del modelo de dispositivo
- Familia de productos: Nombre de la familia de productos a la que pertenece el modelo de dispositivo
- Tipo de software: Nombre del tipo de software al que pertenece el modelo de dispositivo
- Versiones actuales: Lista de las versiones de software únicas que están presentes actualmente en el inventario para el modelo de dispositivo
- Versión seleccionada: Versión sugerida que se ha seleccionado como una versión opcional de las sugerencias proporcionadas por Cisco
- Recursos: Número de activos presentes en el administrador de activos para el modelo de dispositivo
- Sugerencias: Muestra Yes o No para las sugerencias disponibles para el modelo de dispositivo



Ver navegación de sugerencias

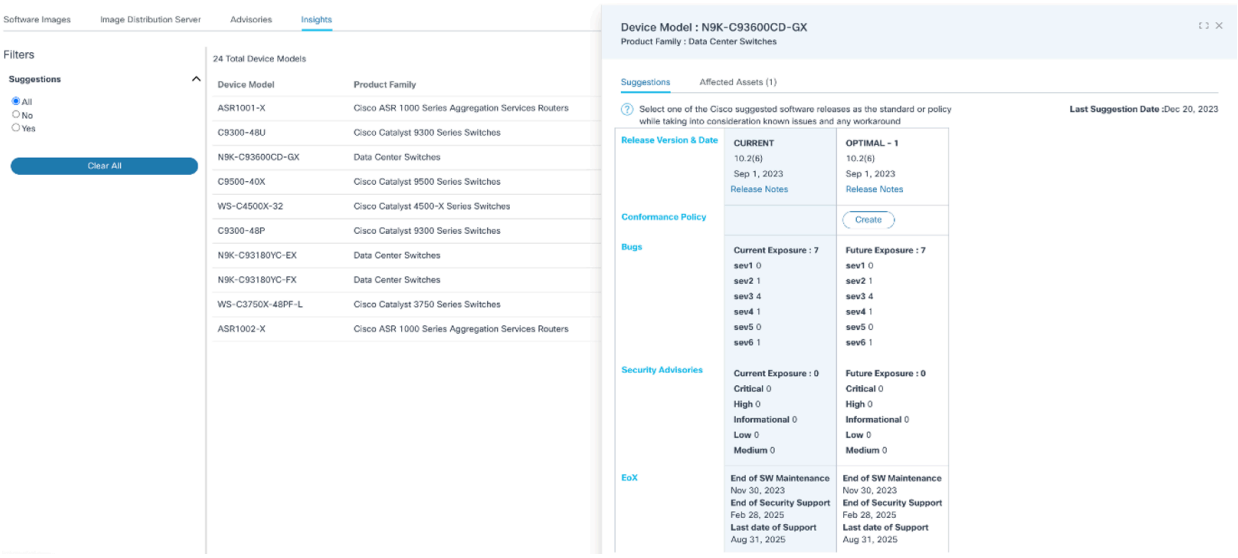
- Acción: Proporciona acciones específicas de la fila mediante el icono Más opciones (por ejemplo, Ver sugerencias y Ver recursos)

---

Nota: Ver sugerencias está deshabilitado si el modelo de dispositivo no tiene sugerencias.

---

Visualización y selección de versiones de software sugeridas por el proveedor




Ficha Sugerencias

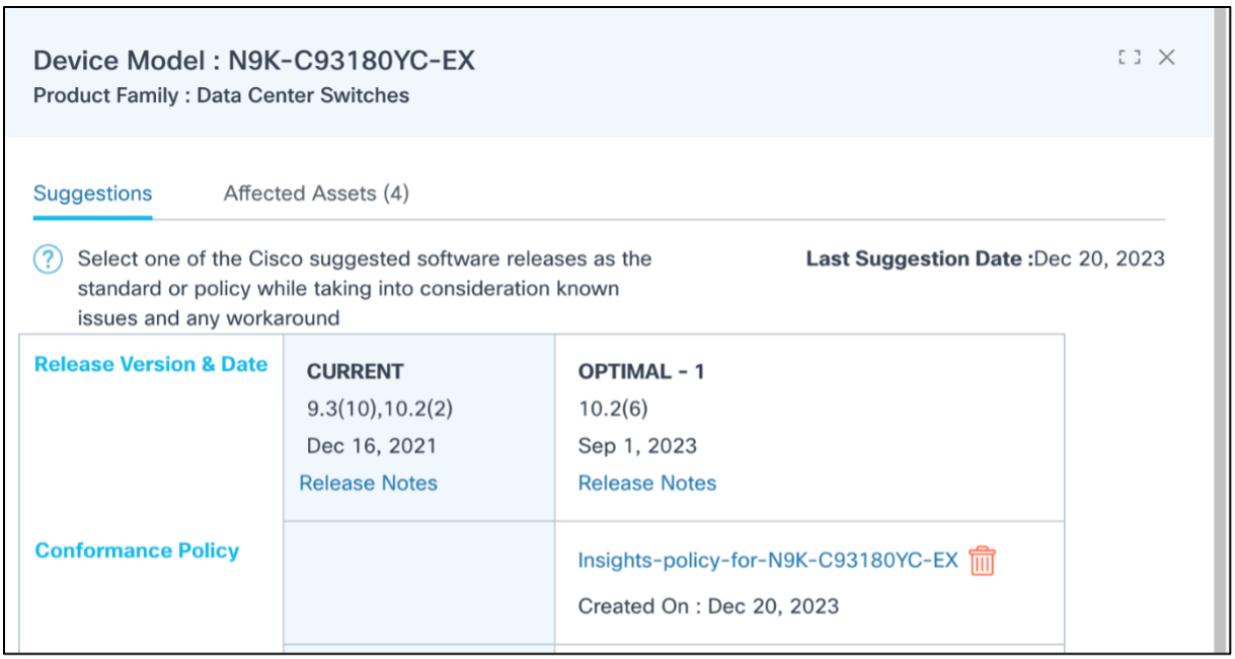
Al seleccionar el icono Más opciones > Ver sugerencias de la columna Acción, se abre un panel lateral con todos los detalles de la información. La pestaña Sugerencias tiene los detalles de la versión actual y sugerida para el modelo de dispositivo seleccionado; es posible que un modelo de dispositivo tenga más de una sugerencia. Están disponibles los siguientes datos:

- Versión y fecha de lanzamiento: La versión de la versión, la fecha y los detalles de las notas se muestran para las versiones actuales y sugeridas, si están disponibles en la nube de Cisco; si los activos del inventario pertenecen a más de una versión, todas las versiones aplicables se muestran como valores separados por comas en la columna Actual
- Crear directiva de conformidad: Permite a los administradores crear una directiva de conformidad para una versión específica con el rol de dispositivo Any.

---

Nota: La creación de políticas de conformidad solo se admite para los modelos de dispositivos de controlador NDFC

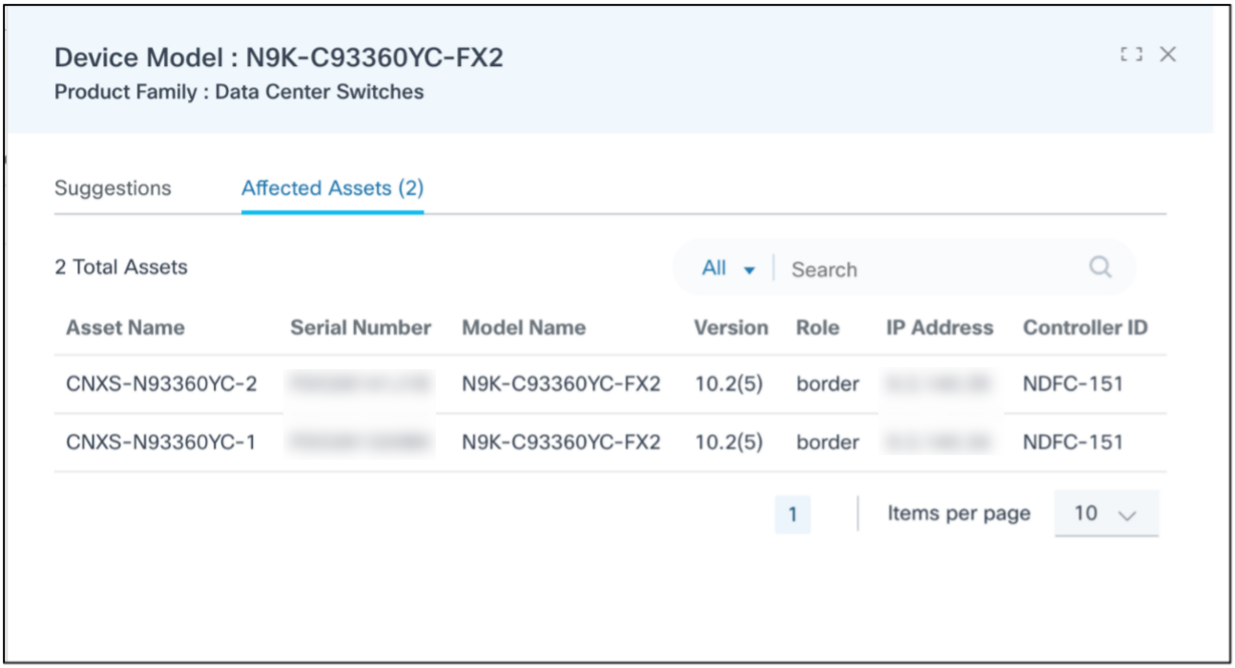
---




Eliminar opción de directiva

Nota: Si ya existe alguna política para el modelo de dispositivo, se muestra un error. Si no existe ninguna directiva, se crea una directiva con el estado Activado. Si se crea una directiva a partir de Insights, los usuarios tienen la opción de eliminarla.

- Errores: Muestra un recuento de errores consolidado para cada versión
- Avisos de seguridad: Muestra un recuento de asesores consolidados para cada versión
- EoX: Muestra las fechas de fin de mantenimiento del software, fin de soporte de seguridad y fecha final de soporte técnico para cada versión




Ficha Activos afectados

Al seleccionar el icono Más opciones > Ver activos de la columna Acción, se abre un panel lateral en el que se muestra de forma predeterminada la pestaña Activos afectados. La pestaña Activos afectados muestra los detalles de los activos potencialmente afectados en columnas como Nombre del activo, Número de serie, Nombre del modelo, Versión del software, Dirección IP e ID del controlador. En esta ficha se pueden ordenar y buscar los activos.

Identificación de dispositivos que necesitan actualización de software

Consulte Conformidad de Software para obtener más información.

## Conformidad de software

La conformidad del software ayuda a identificar los recursos de una red que no son compatibles con la versión de software de destino deseada. La validación se basa en políticas y reglas a través de las cuales se definen los intentos de conformidad de software. Estas políticas se pueden ejecutar de forma programada o a demanda. Una vez ejecutada correctamente la directiva de conformidad, se obtiene el resultado de conformidad que proporciona el estado de los activos aplicables. El alcance de conformidad depende de varios criterios, como la función del dispositivo, la administración de la instancia del controlador, etc.

Prerequisites

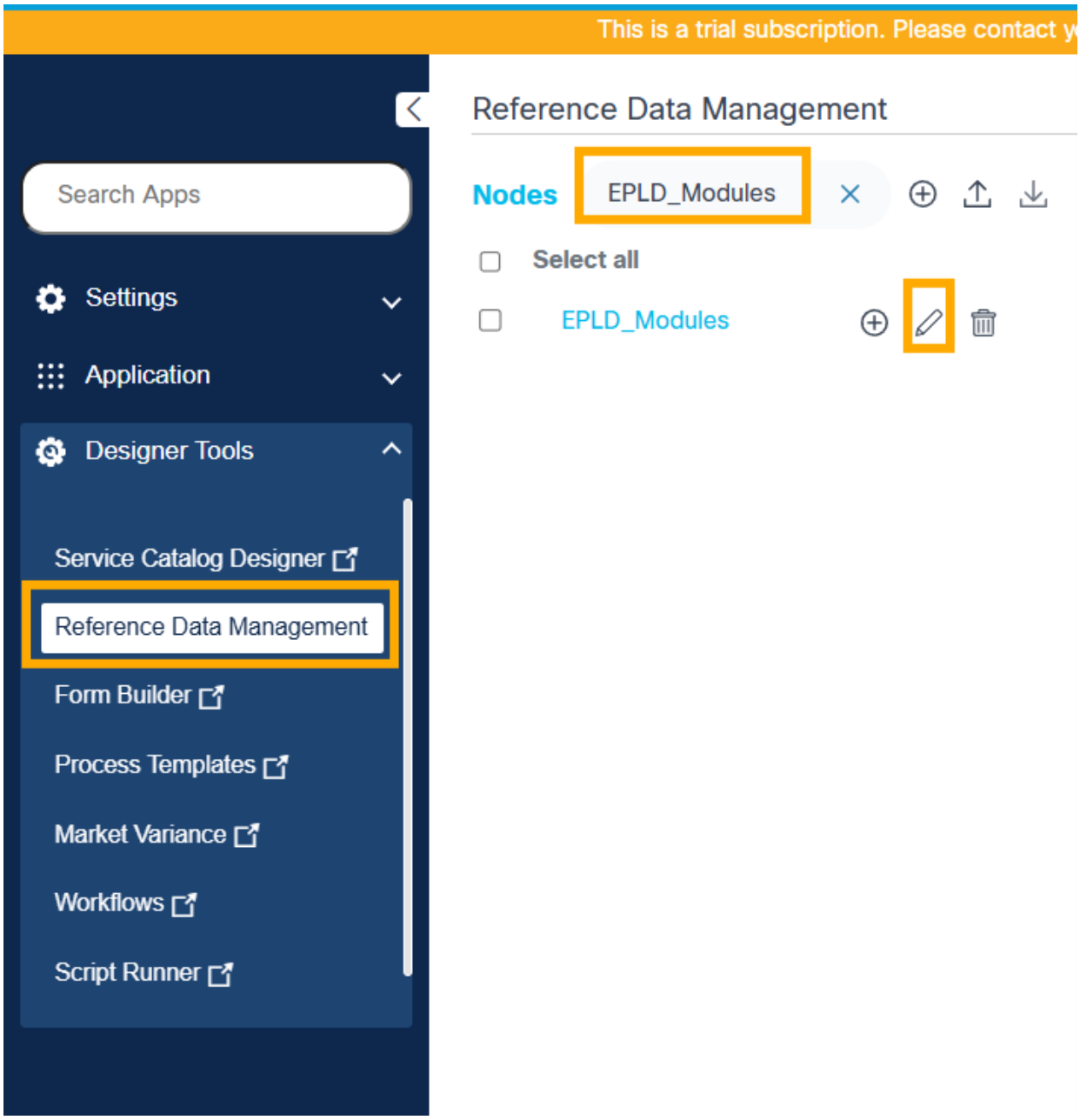
- Las imágenes de software de controladores como Cisco Catalyst Center, vManage, NDFC y FMC deben estar sincronizadas. Consulte Sincronización de Metadatos de Imágenes de Software para obtener más información.
- Se deben agregar los metadatos de imagen de software necesarios para controladores como NSO, CNC, Direct-to-Device y ANSIBLE. Consulte Adición de Metadatos de Imagen de Software para obtener más información.
- Los usuarios deben tener acceso a la aplicación RefD para administrar los datos del módulo EPLD.
- La información del módulo EPLD para las versiones requeridas se debe rellenar previamente en la aplicación RefD
- Los usuarios deben agregar manualmente la información del módulo EPLD en la aplicación RefD si no está disponible OOB

Creación de Datos del Módulo EPLD en la Aplicación de Gestión de Datos de Referencia

Antes de crear una directiva de conformidad, cree datos de referencia del módulo EPLD en la aplicación RefD. La aplicación RefD incluye información del módulo EPLD para las versiones de software de Nexus v10.2(8) y v10.4(5), respectivamente. Para otras versiones del dispositivo, la

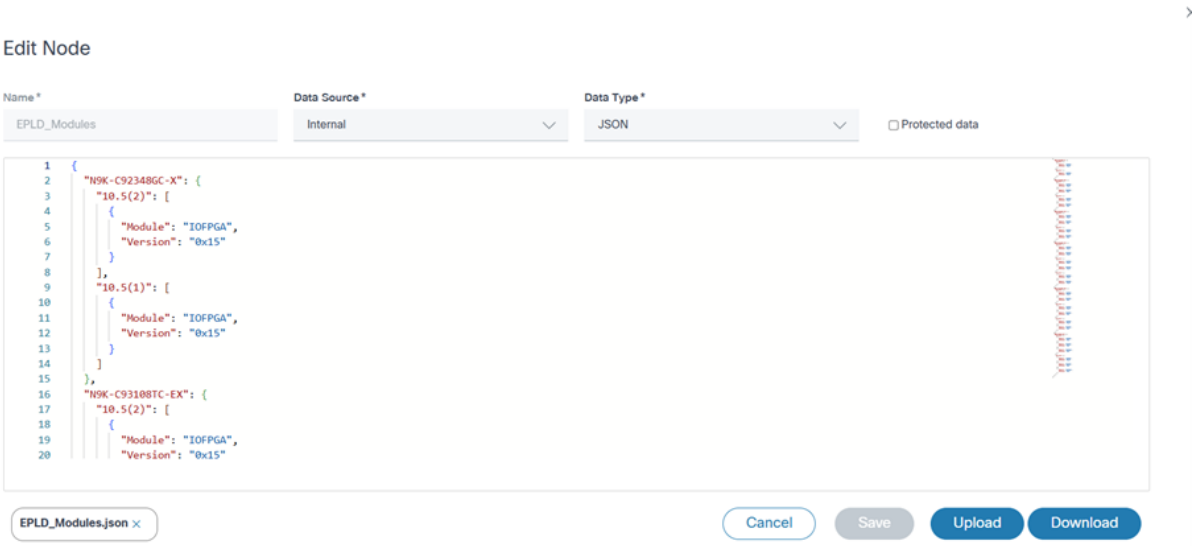
información del modelo EPLD se debe añadir manualmente en la aplicación RefD.

Realice los siguientes pasos para agregar otras versiones a los metadatos del módulo EPLD:




Gestión de datos de referencia

1. Vaya a la aplicación Gestión de Datos de Referencia y busque "EPLD_Modules".
2. Seleccione el archivo "EPLD_Modules" y el icono Edit.




Editar nodo

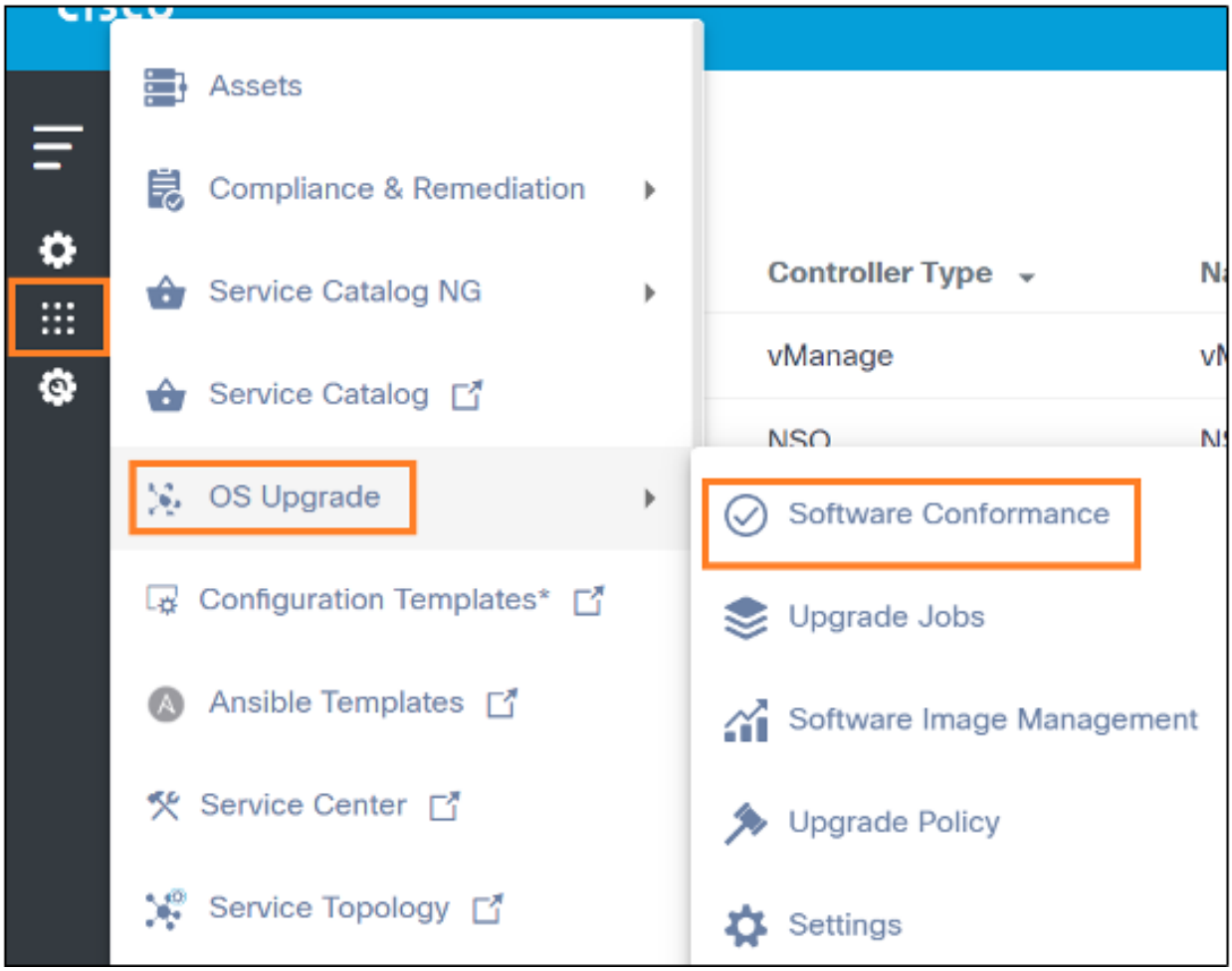
3. Agregue los metadatos del módulo EPLD de la nueva versión añadiendo una nueva entrada con la siguiente estructura:

```
structure:
  "N9K-C92348GC-X": {
    "10.5(2)": [
      {
        "Module": "IOFPGA",
        "Version": "0x15"
      }
    ]
  }
```

4. Haga clic en Guardar y valide los nuevos metadatos del módulo EPLD disponibles para su selección en la directiva de conformidad. Se rellenan previamente los datos EPLD de las versiones compatibles.

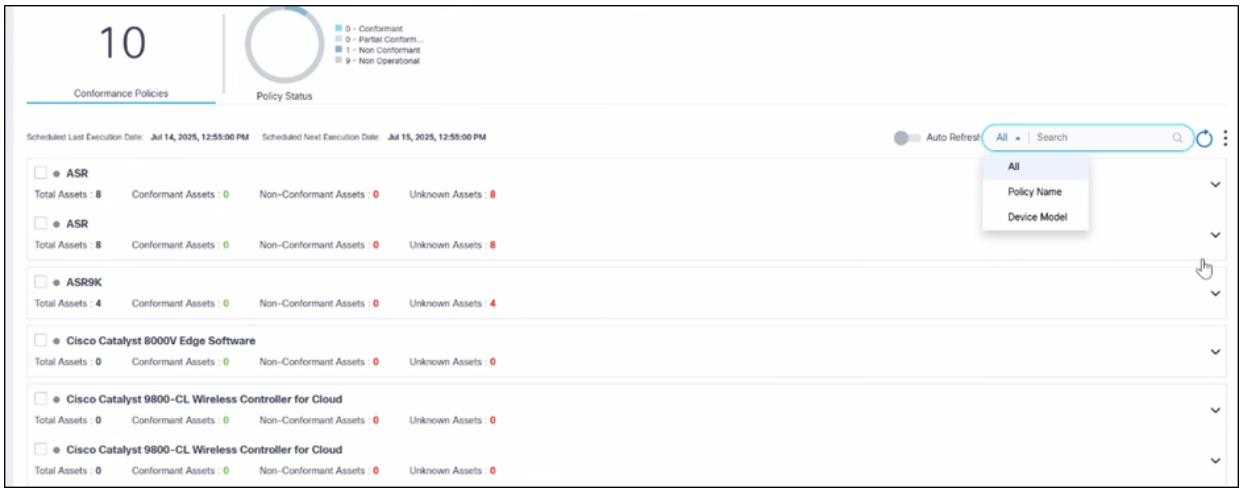
## Visualización y gestión de la conformidad del software

1. Inicie sesión en BPA con credenciales que tengan acceso a Software Conformance.




Navegación de conformidad del software

2. Seleccione OS Upgrade > Software Conformance. Se muestra la página Software Conformance.




Conformidad de software

La página Software Conformance contiene lo siguiente:

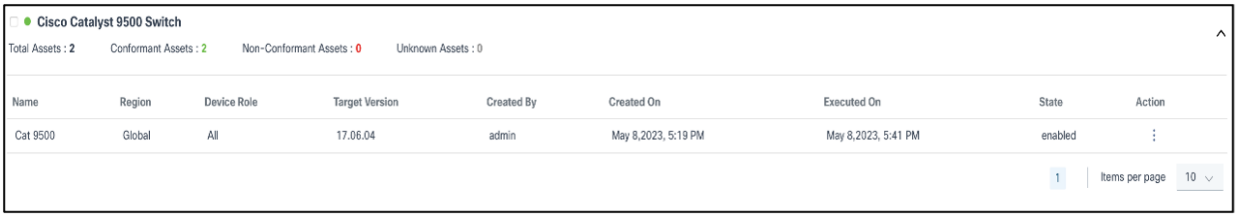
- Una sección de análisis, que se muestra en la parte superior, que proporciona lo siguiente:

- Número total de directivas de conformidad existentes en el sistema
- Un filtro rápido Estado de política para filtrar basado en los siguientes criterios:
    - Conforme: Todos los dispositivos gestionados por BPA con un modelo especificado se encuentran en la versión de software definida
    - Conformidad parcial: Algunos dispositivos administrados por BPA con un modelo especificado se encuentran en la versión de software definida; los dispositivos restantes están en versiones de software diferentes
    - No conforme: Todos los dispositivos gestionados BPA con un modelo especificado se encuentran en versiones de software diferentes en comparación con una versión de software determinada
    - No operativo: No se encuentra ningún dispositivo aplicable según el modelo de dispositivo especificado en la política
- Fecha de última ejecución programada y Fecha de próxima ejecución programada, que indican la fecha y la hora de las comprobaciones de conformidad programadas ejecutadas anteriormente y cuándo se realizará la siguiente comprobación de conformidad programada para todas las directivas
- Un campo Search que se utiliza para filtrar políticas basadas en el modelo del dispositivo, el nombre de la política o todo; los usuarios pueden seleccionar All para buscar en todos los parámetros
- La opción Actualización automática permite la actualización automática de la directiva de conformidad en curso a intervalos definidos por el usuario cuando está activada. Para activar la alternancia:
    - Vaya a OS Upgrade > Settings para cambiar el intervalo de actualización
    - Modifique el intervalo de actualización automática con el valor deseado
    - Haga clic en Save (Guardar).
- El panel de directivas de conformidad de software se actualiza en el nuevo intervalo cuando se habilita la opción Actualización automática
- Un icono Refresh para actualizar la página y borrar los filtros seleccionados
- Un icono Más opciones que proporciona las siguientes opciones:
    - Crear una directiva
    - Ejecutar todas las políticas
    - Eliminar varias políticas seleccionadas

Las políticas se agrupan en función de los modelos de dispositivos y se muestran como paneles expandibles para proporcionar una única vista de todos los modelos de dispositivos administrados por diferentes controladores.


Vista contraída de la política de conformidad

En la vista contraída, el panel muestra el modelo de dispositivo y estadísticas rápidas como Total Assets, Conformant Assets, Non-Conformant Assets y Unknown Assets.

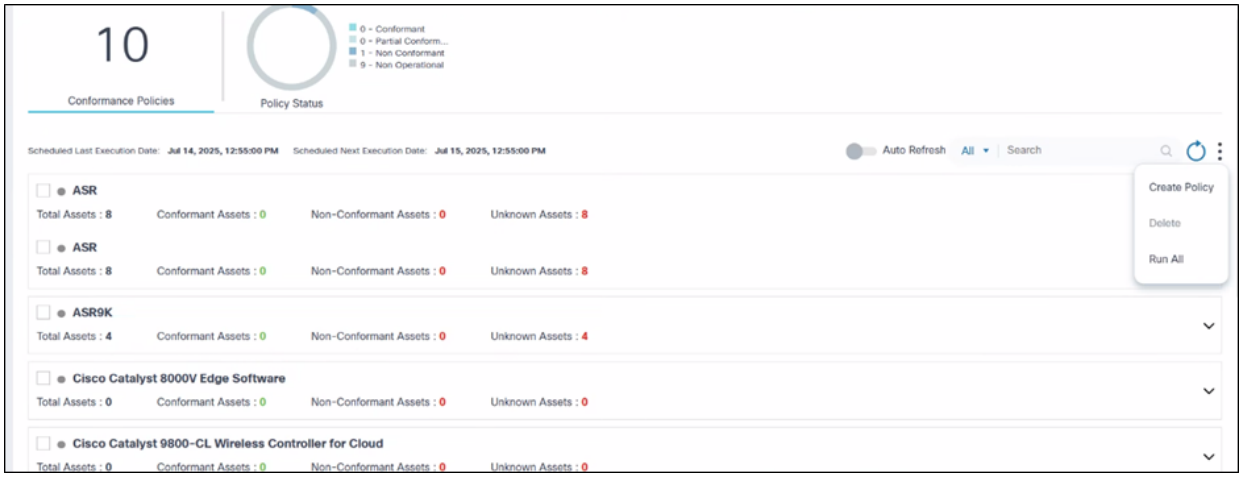



Vista ampliada de la política de conformidad

En la vista expandida, se muestran todas las directivas relacionadas con el modelo de dispositivo. Para cada directiva, se pueden realizar acciones adicionales, como ejecutar, editar directiva, ver resultados, etc., seleccionando el icono Más opciones de la columna Acción.

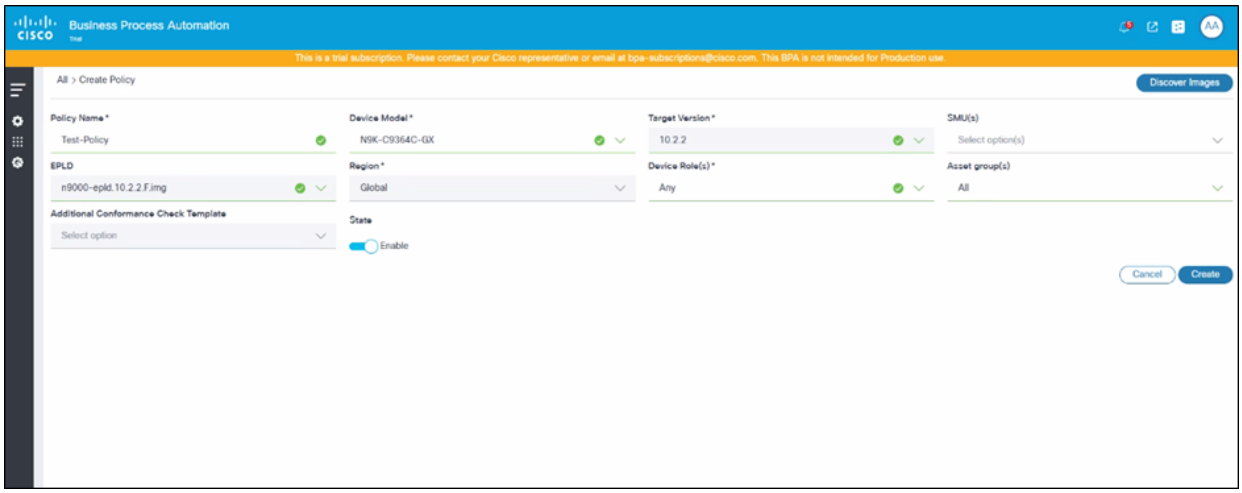
Creación de políticas de conformidad de software

1. Inicie sesión en el BPA con credenciales que tengan acceso de gestión a la conformidad de software.
2. Seleccione OS Upgrade > Software Conformance. Se muestra la página Software Conformance.




Crear política

3. Seleccione el icono Más opciones > Crear directiva.




Crear formulario de directiva

4. Introduzca la información en los campos Nombre de la política, Modelo(s) del dispositivo, Versión de destino, SMU, EPLD, Función del dispositivo, Grupos de activos y Plantilla de comprobación de conformidad adicional. SMU(s), grupo(s) de activos y plantilla de comprobación de conformidad adicional son campos opcionales.

---

Nota: Ahora los usuarios pueden seleccionar más de un modelo de dispositivo en el formulario Crear directiva de conformidad.

---

---

Nota: El marco de conformidad de software puede ejecutar comprobaciones de conformidad en la versión de SO base y parches SMU en los dispositivos de un modelo, rol o instancia de controlador específico que administre el dispositivo. Si se requiere alguna comprobación personalizada adicional, se puede crear una plantilla de proceso con los comandos y reglas de validación necesarios que se pueden asignar al campo Plantilla de comprobación de conformidad adicional.

---

5. Haga clic en Crear. Aparecerá una confirmación.

---

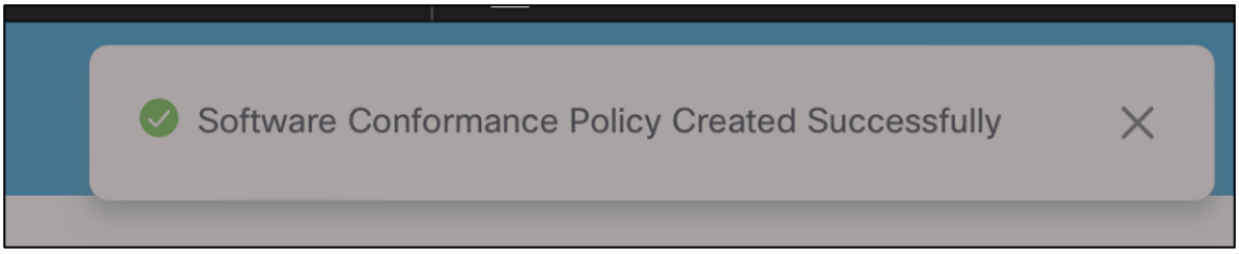
Nota: Debe tenerse en cuenta la siguiente lista.

---

- Los administradores de casos prácticos tienen la flexibilidad de crear varias políticas con diferentes funciones de dispositivo para un modelo de dispositivo seleccionado. Se puede seleccionar más de un rol en una sola política.
- Si se selecciona Any en la lista desplegable Device Role(s), se desactivarán todas las demás funciones de dispositivo (por ejemplo, Access, Core, etc.). Si se selecciona cualquier otro rol de dispositivo, se deshabilita Any.
- Para los dispositivos administrados por controladores como CNC, NSO, ANSIBLE y Direct-to-Device, se puede utilizar la función Any (seleccionada en la lista desplegable Device Role(s)) para realizar la comprobación de conformidad porque los dispositivos no tienen

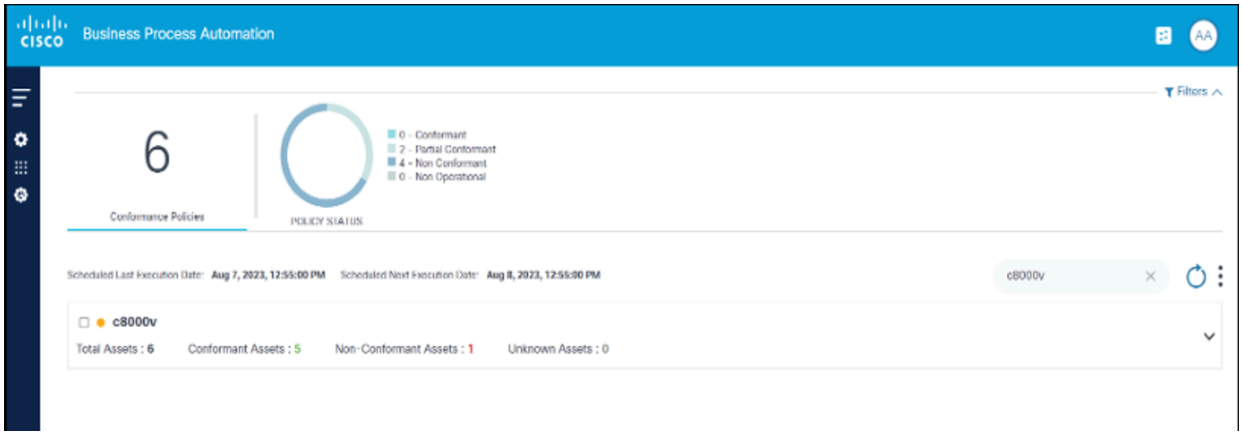
información de funciones.

- Si se selecciona Any en la lista desplegable Device Role(s) para FMC, la conformidad del software se ejecuta en todos los dispositivos, incluidos los dispositivos independientes, de control y de datos.
- La conformidad y las actualizaciones de SMU solo son compatibles con los controladores CNC, NSO, ANSIBLE, FMC, Direct-to-Device y NDFC.
- En esta versión sólo se admite Global de la lista desplegable Region
- Los usuarios pueden seleccionar grupos de activos en la lista desplegable. Todo está seleccionado de forma predeterminada. Los usuarios tienen la opción de seleccionar uno o más grupos de activos. Si se selecciona un grupo de activos específico, la política solo se ejecuta en los dispositivos del grupo de activos seleccionado.
- Si no se muestran los valores esperados para los campos Modelo de dispositivo, Versión de destino y SMU(s), haga clic en Detectar imágenes e inténtelo de nuevo.
- Los campos Modelo de dispositivo, Grupo(s)de activos y Rol forman una política única; no se permiten políticas duplicadas.
- El campo EPLD rellena los valores solo cuando los metadatos de imagen EPLD están disponibles para los modelos de dispositivo seleccionados y la versión de destino.
- El nombre de política es único y no se permiten nombres de política duplicados.



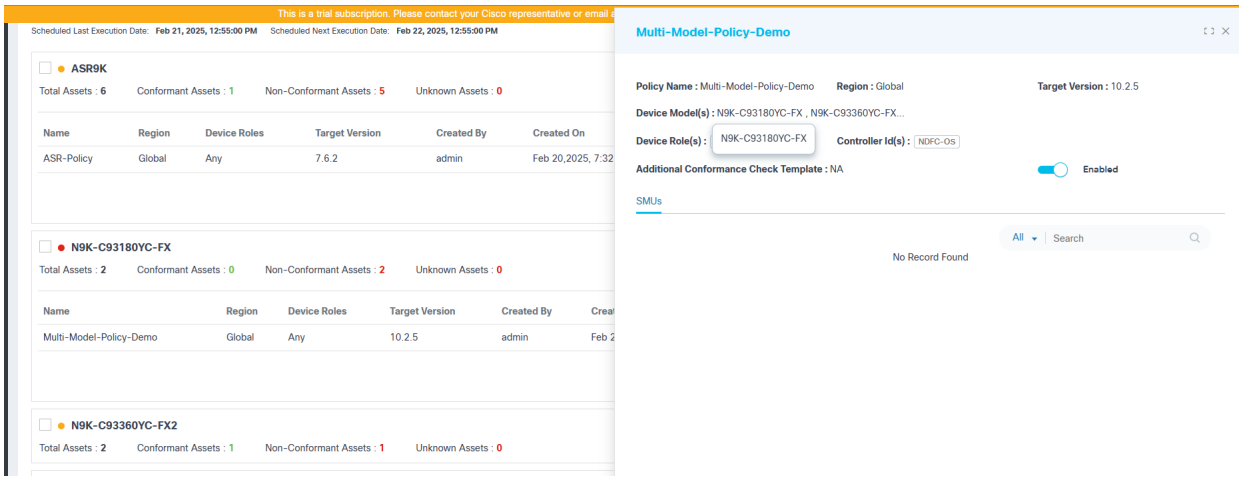

Confirmación de creación de directiva de conformidad

- Las plantillas de proceso que están etiquetadas como Actualización del sistema operativo de última generación (Next-Gen) se muestran en el campo Plantilla de comprobación de conformidad adicional.




Buscar resultado de directiva de conformidad

6. Localice la política creada introduciendo el modelo de dispositivo en el campo Buscar.

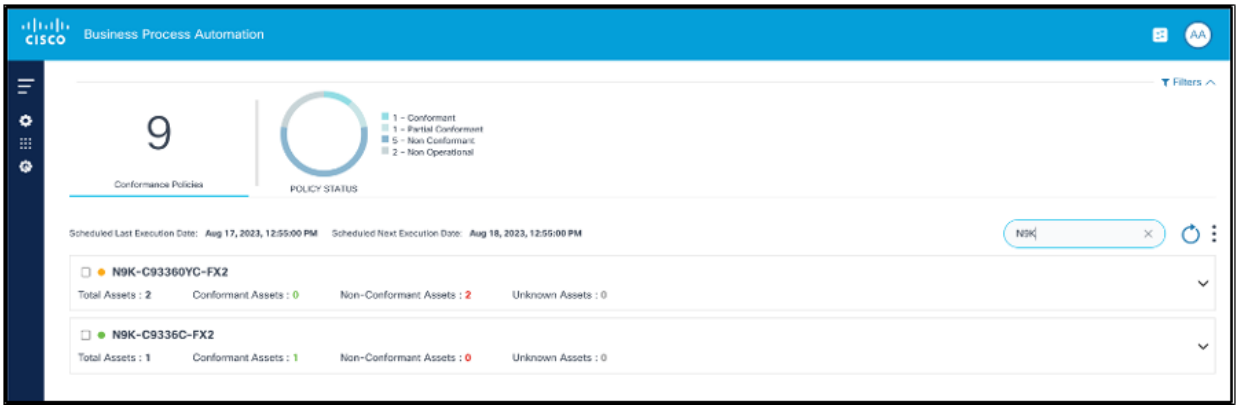



Ver directiva de conformidad

7. Haga clic en Policy para ver la vista detallada de la política.

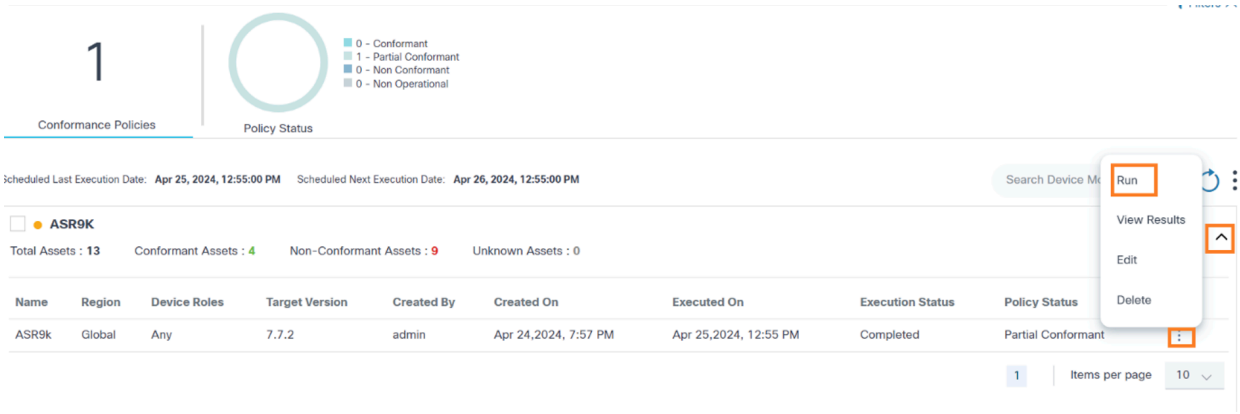
## Ejecución de comprobaciones de conformidad de software a demanda

1. Inicie sesión en BPA con credenciales que tengan acceso de ejecución.
2. Seleccione OS Upgrade > Software Conformance. Se muestra la página Software Conformance.



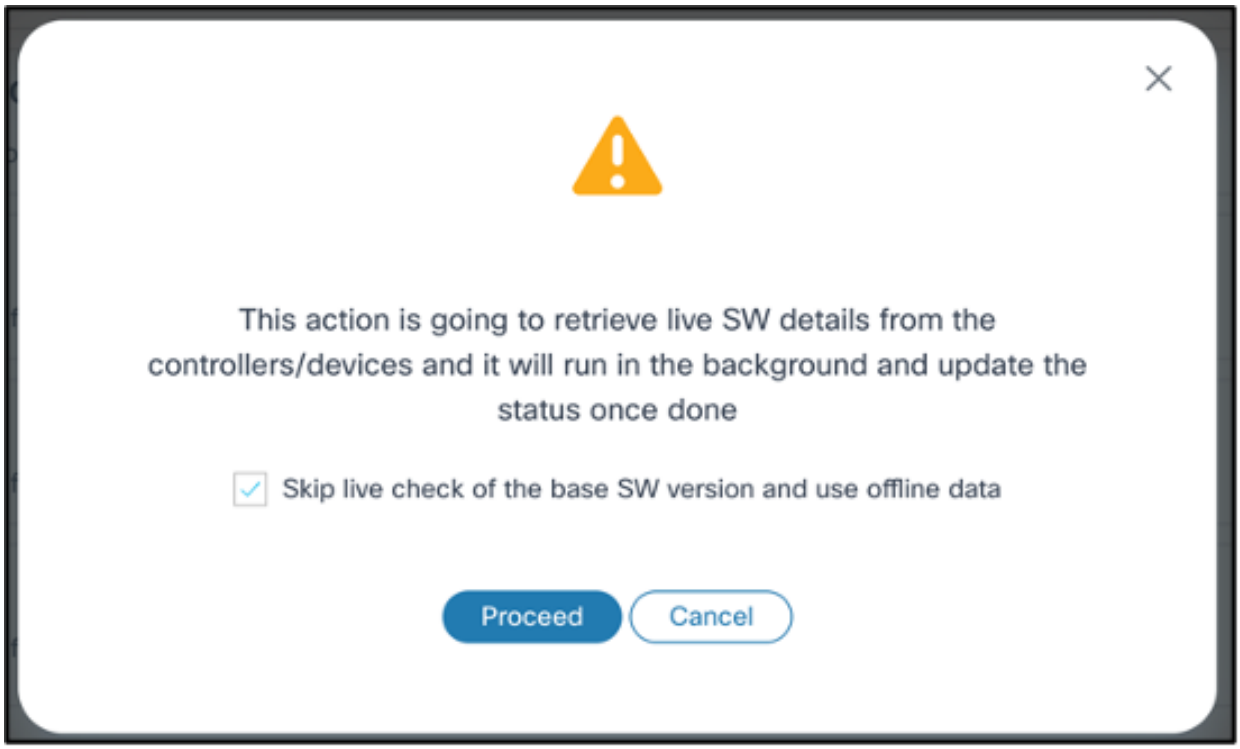

Búsqueda de políticas

3. Localice la política que se ejecutará a petición mediante el campo Buscar.



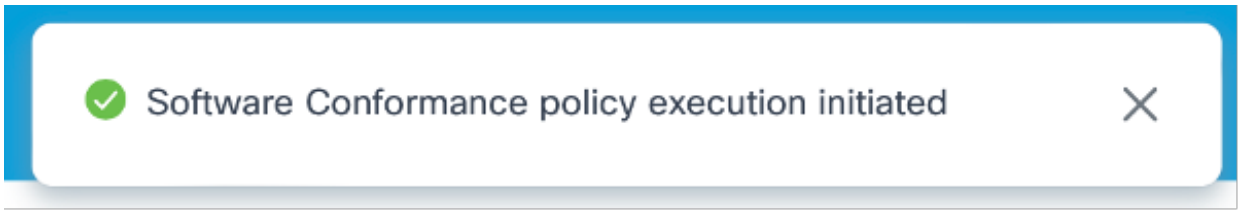

Ejecute

4. En la columna Action de la política, seleccione More Options > Run. Se muestra una confirmación para validar si se debe realizar una comprobación del inventario en tiempo real de los dispositivos.




Confirmación para ejecutar la política de conformidad

5. Si se requiere una sincronización del inventario en tiempo real antes de ejecutar las comprobaciones de conformidad, desactive la casilla de verificación Omitir comprobación en tiempo real de la versión de software básica y usar datos sin conexión y haga clic en Continuar. En este caso, la comprobación de conformidad sólo se ejecuta después de la sincronización. Se muestra una notificación en la esquina superior derecha.




Notificación de ejecución de directiva de conformidad

Nota: Debe tenerse en cuenta la siguiente lista.

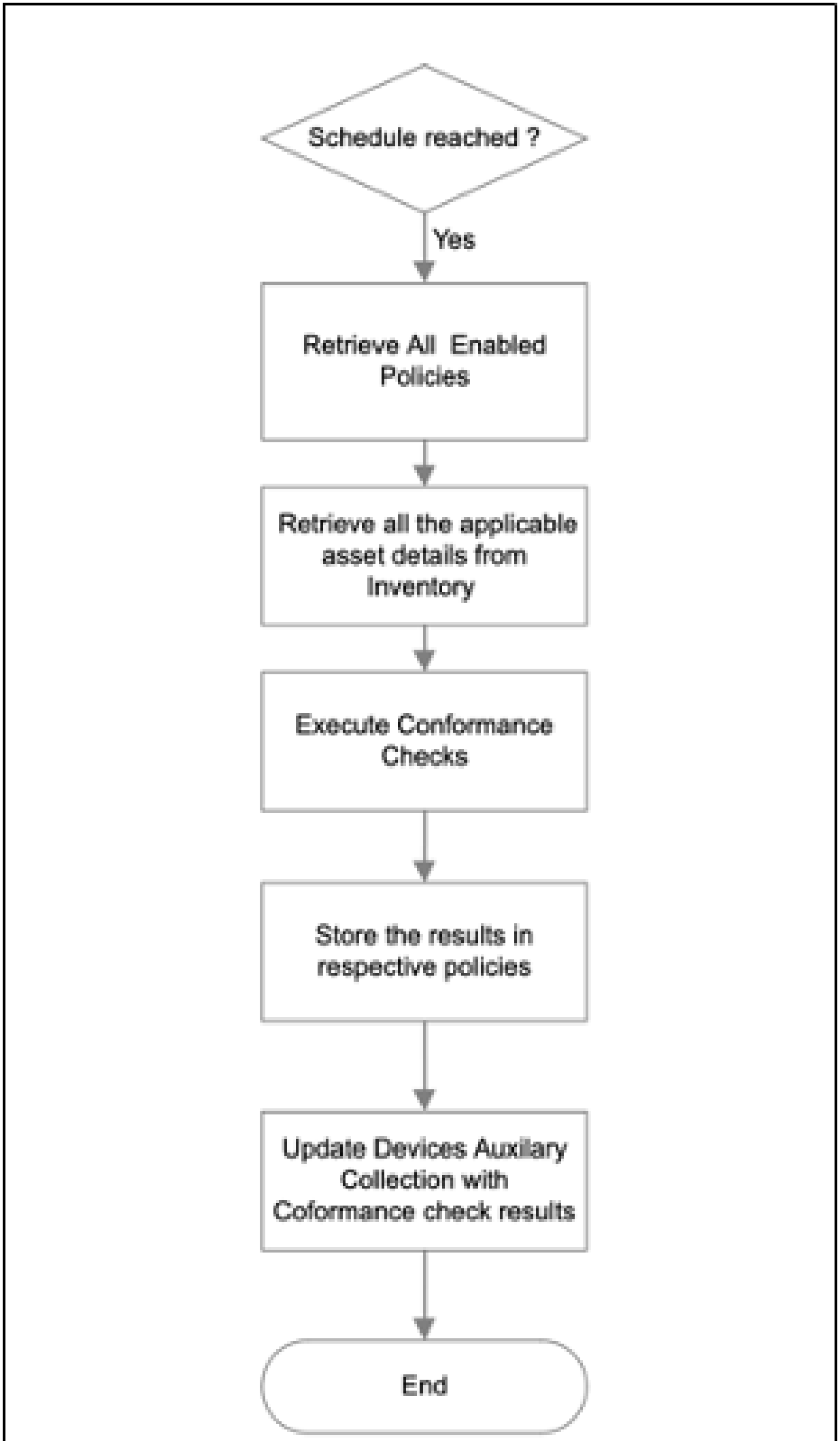
- De forma predeterminada, se realiza una comprobación de conformidad mediante los datos de inventario de activos.
- Durante este proceso, si falla la sincronización del inventario o del dispositivo, el dispositivo de política respectivo se marca como Desconocido y se omite la verificación de SMU.
- Para SMU, los datos en tiempo real se recuperan del dispositivo antes de realizar comprobaciones de conformidad si la casilla de verificación Omitir comprobación en directo de la versión de software base y utilizar datos sin conexión está activada o no.
- Cuando una directiva incluye varios modelos de dispositivos, la ejecución de esa directiva para un modelo de dispositivos inicia la ejecución de todas las directivas asociadas.

Programación de la ejecución de comprobaciones de conformidad del software

Las comprobaciones de conformidad del software se pueden realizar automáticamente a intervalos regulares mediante el servicio del planificador. Las comprobaciones de conformidad programadas se pueden configurar para ejecutarse:

- Diario
- Dos veces al día
- Semanalmente
- Una

Una vez alcanzada la programación, todas las directivas con el estado Activado se ejecutan automáticamente y los resultados de conformidad se almacenan en las directivas respectivas.

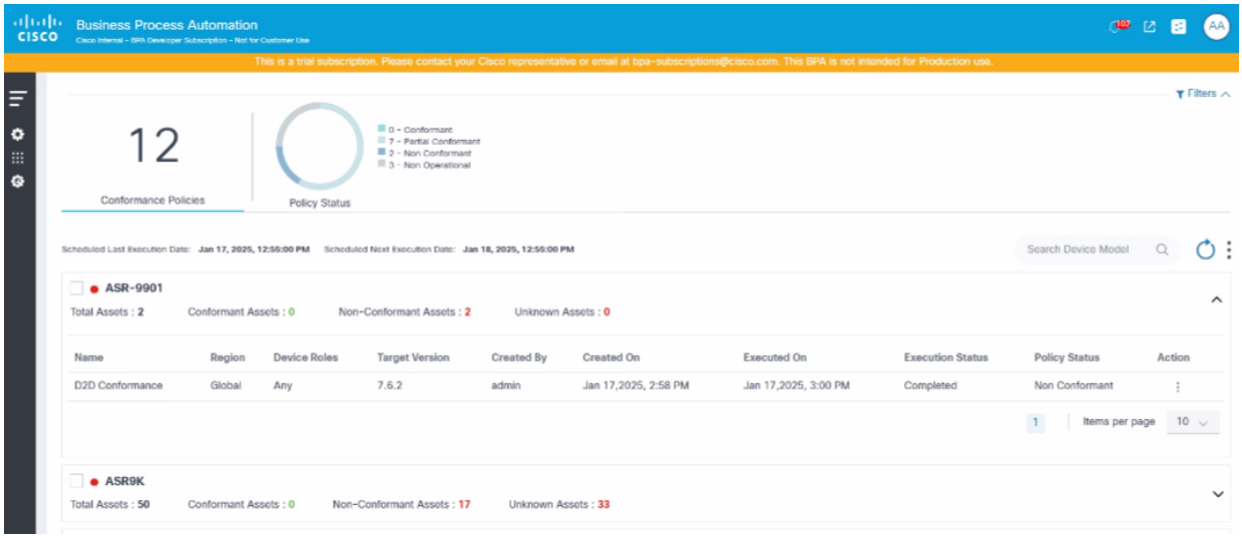

Schedule reached ?
Yes
Retrieve All Enabled Policies
Retrieve all the applicable asset details from Inventory
Execute Conformance Checks
Store the results in respective policies
Update Devices Auxilary Collection with Coformance check results
End

Ejecución Programada de Verificaciones de Conformidad de Software Flujo de Llamadas

Consulte Conformidad de Software para obtener más información.

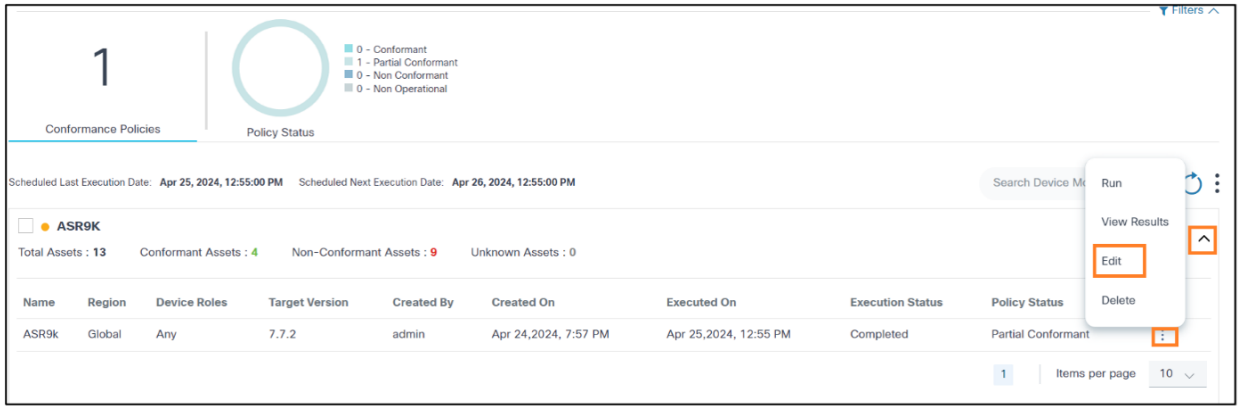
Actualización de políticas de conformidad de software

1. Inicie sesión en el BPA con credenciales que tengan acceso de administración para la conformidad del software
2. Seleccione OS Upgrade > Software Conformance. Se muestra la página Software Conformance.



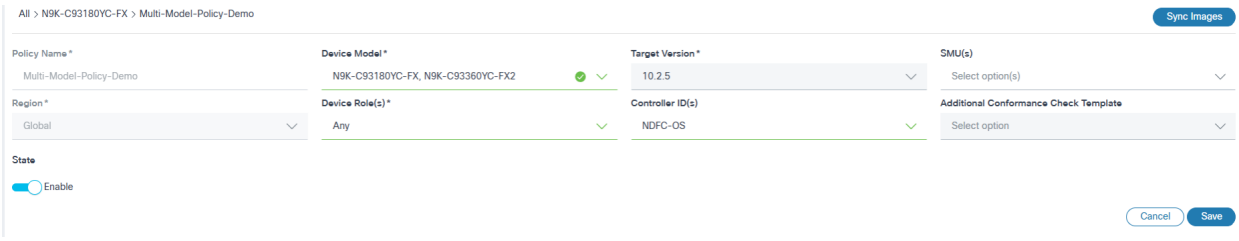

Conformidad de software

3. Utilice el campo Search para localizar la política deseada.



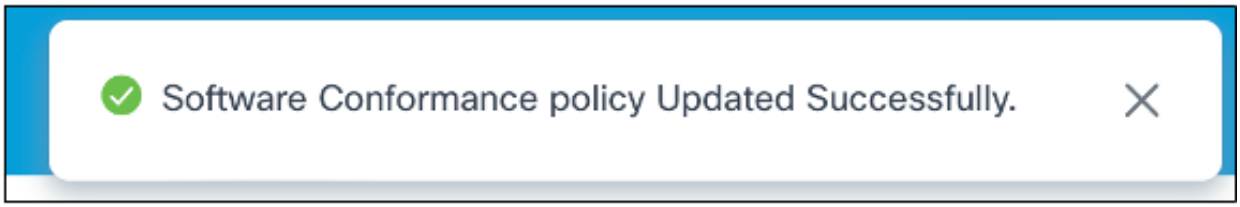

Editar

4. En la columna Acción de la política, seleccione el icono Más opciones > Editar.




Editar política de conformidad con los detalles rellenos

5. Edite los campos Versión de destino, SMUs, Funciones de dispositivo, ID de controlador, Estado de directiva y Plantilla de comprobación de conformidad adicional, según sea necesario.
6. Click Save. Aparecerá una confirmación.

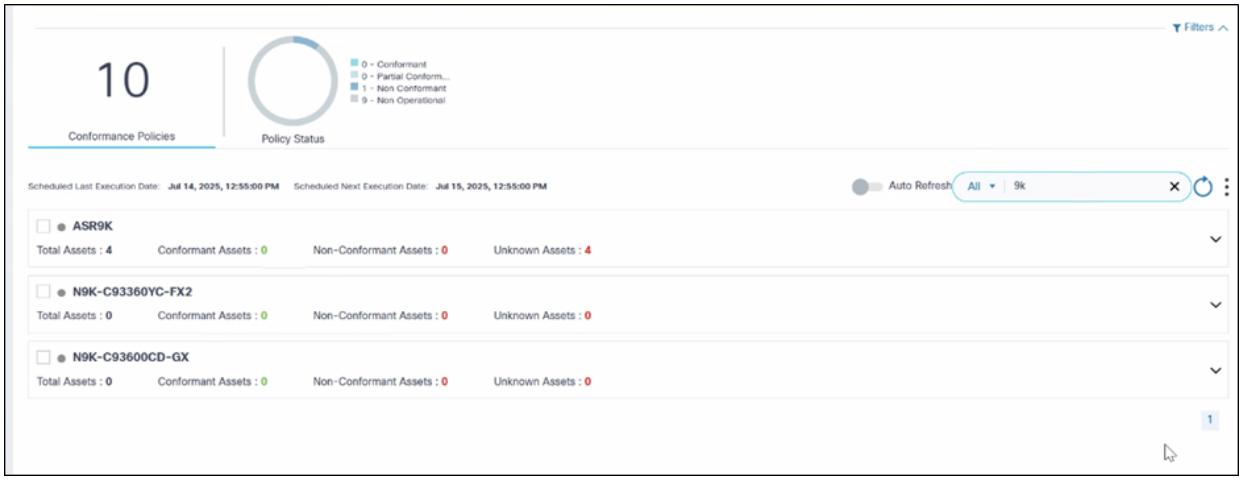



Confirmación de actualización correcta

Nota: Cuando se utiliza la directiva de conformidad de software para un trabajo de actualización en curso, la directiva no se puede editar.

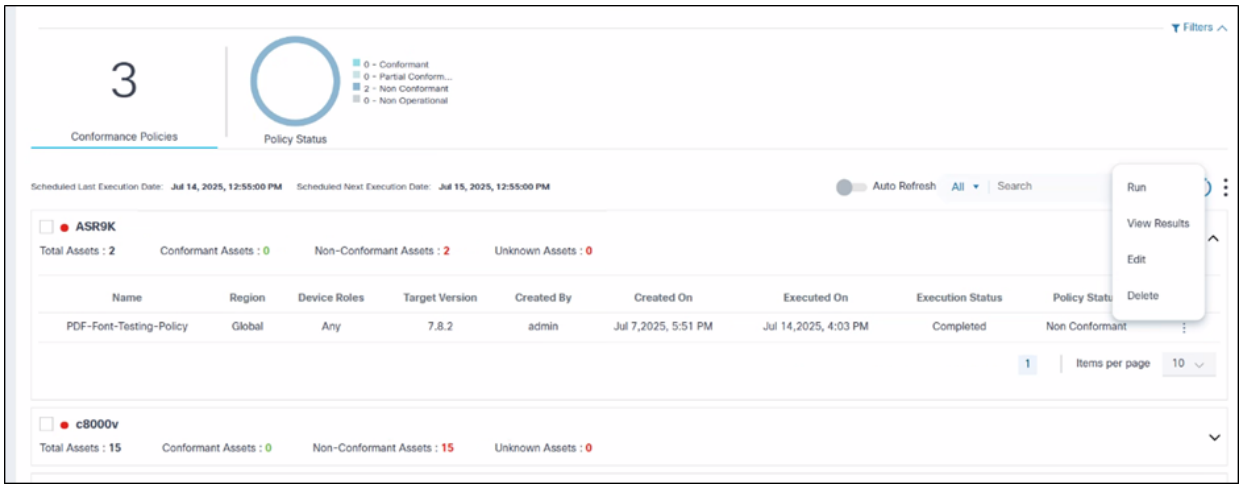
Eliminación de políticas de conformidad de software

1. Inicie sesión en BPA con credenciales que tengan acceso de administrador.
2. Seleccione OS Upgrade > Software Conformance. Se muestra la página Software Conformance.



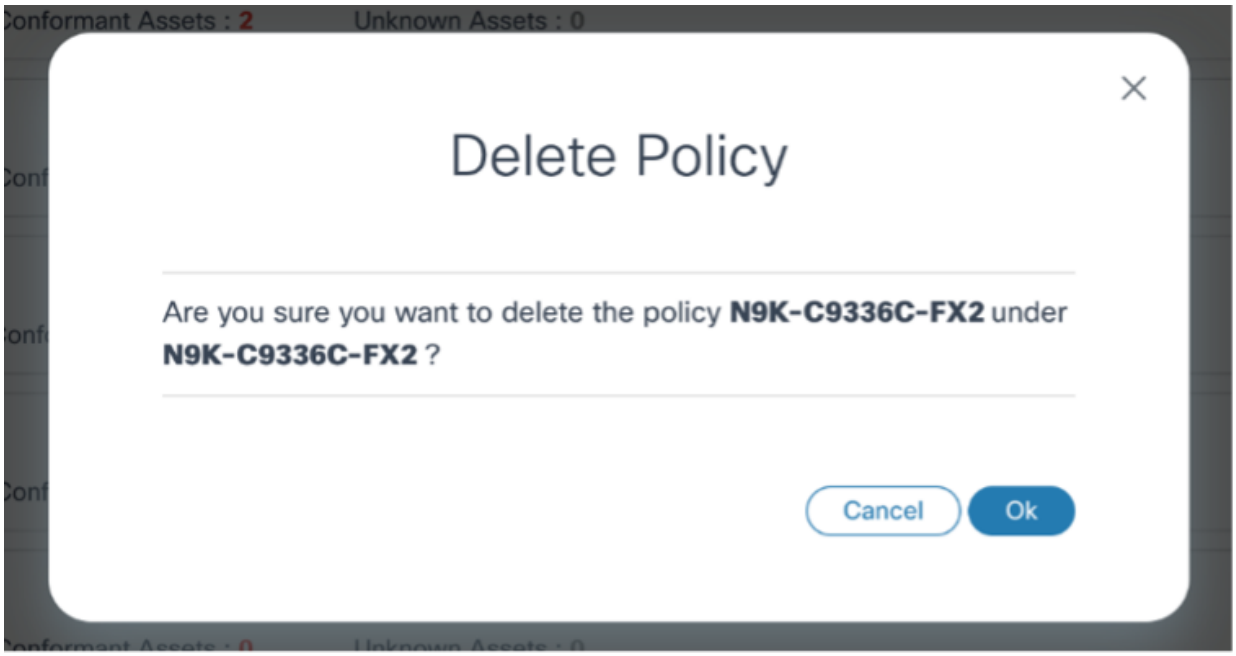

Buscar resultado de directiva de conformidad

3. Utilice el campo Search para localizar la política deseada.

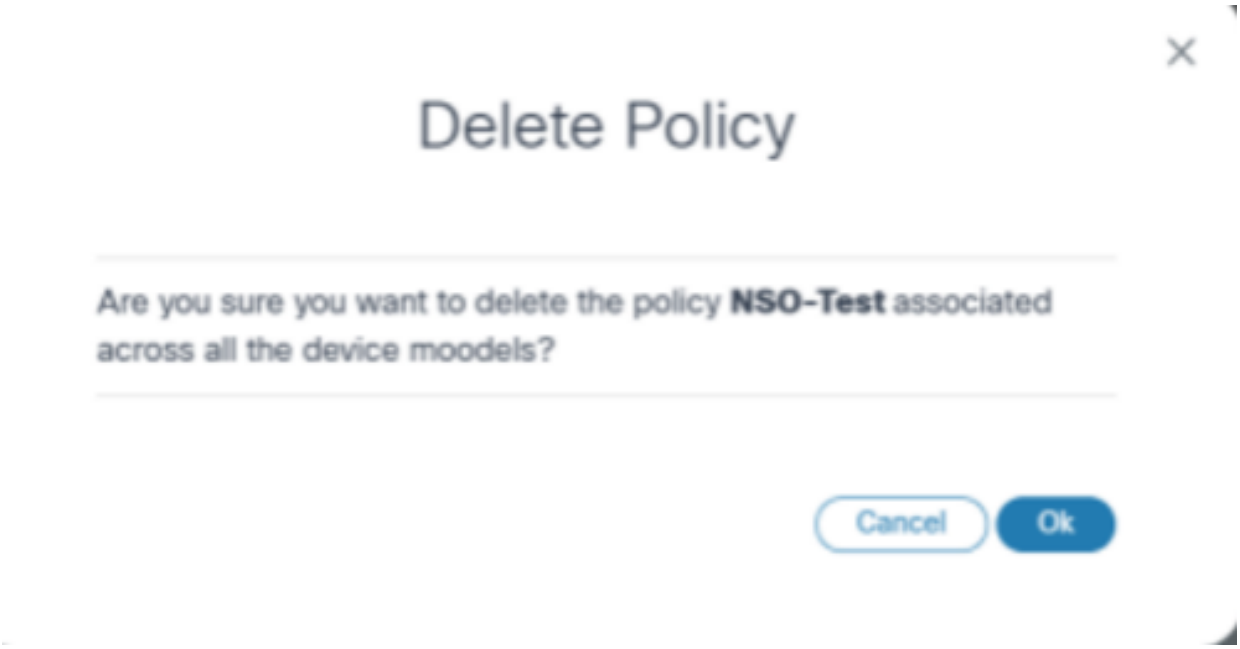



Eliminar

4. En la columna Acción de la política, seleccione el icono Más opciones > Eliminar. Se abrirá una ventana de confirmación.




Confirmación de eliminación de política




Confirmación de eliminación de directiva (si la directiva está asociada a varios modelos)

5. Click OK. Se elimina la política.

---

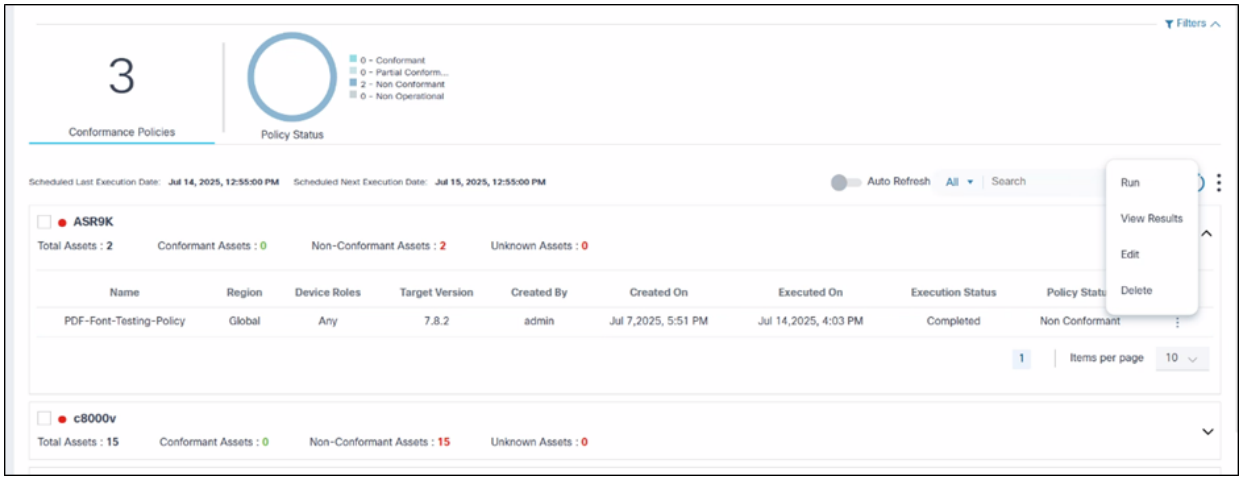
Nota: Debe tenerse en cuenta la siguiente lista.

---

- Si una directiva está asociada a más de un modelo de dispositivo, al eliminar una directiva se quitan todas las directivas relacionadas de cada modelo asociado.
- Cuando se utiliza la directiva de conformidad de software para un trabajo de actualización en curso, la directiva no se puede eliminar.

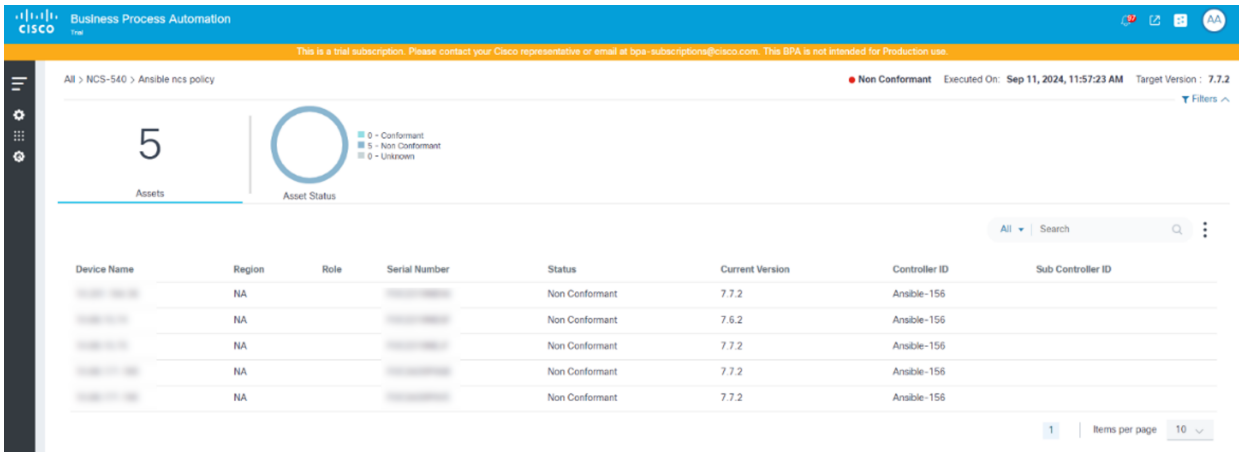
Visualización y descarga de resultados de conformidad

Una vez que se ejecuta una política:

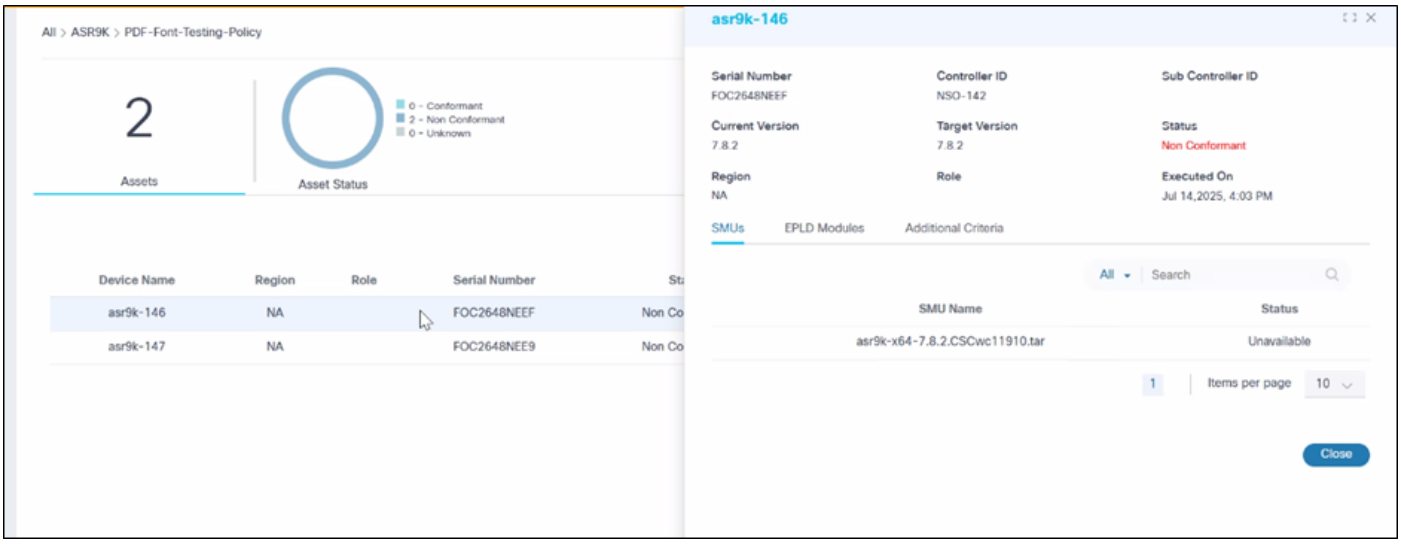


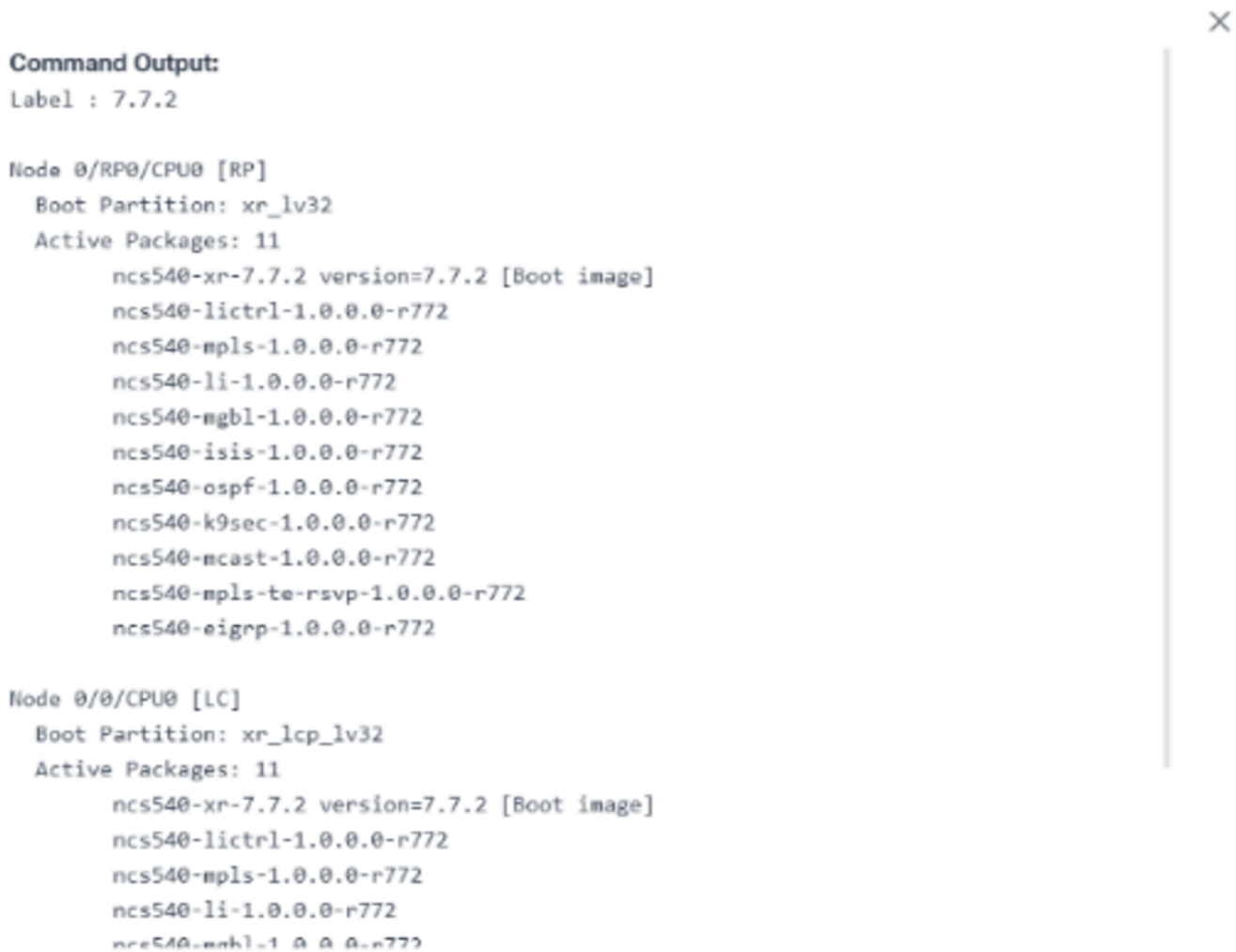
Opción Ver resultados

1. En la página Software Conformance, seleccione el icono More Options > View Results. La página Resultados muestra dónde los usuarios pueden ver el estado de conformidad de los dispositivos.




Ver resultados



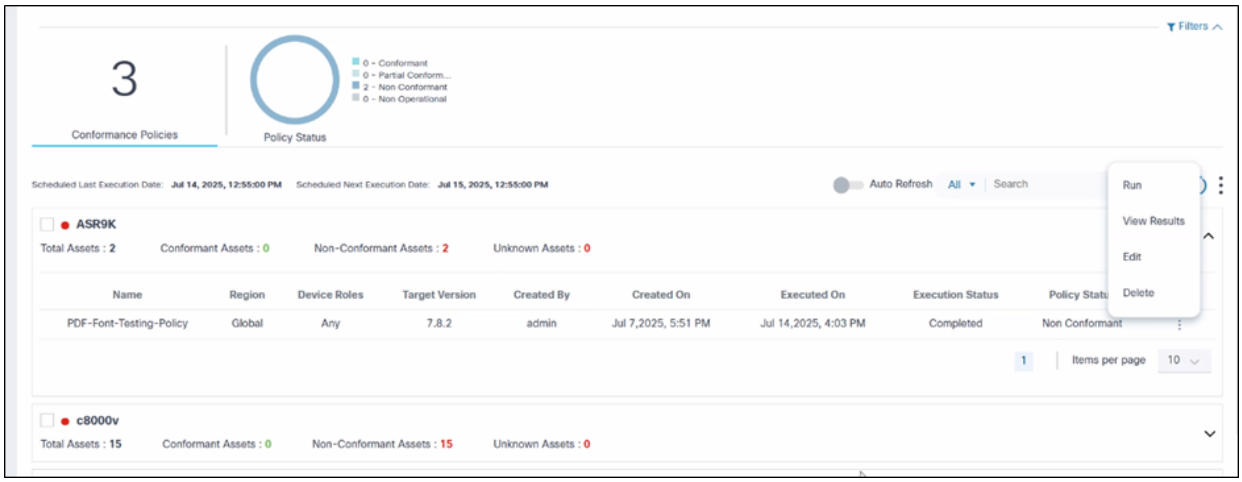



2. Seleccione una fila para mostrar detalles de activos específicos junto con el estado de SMU y criterios adicionales.

---

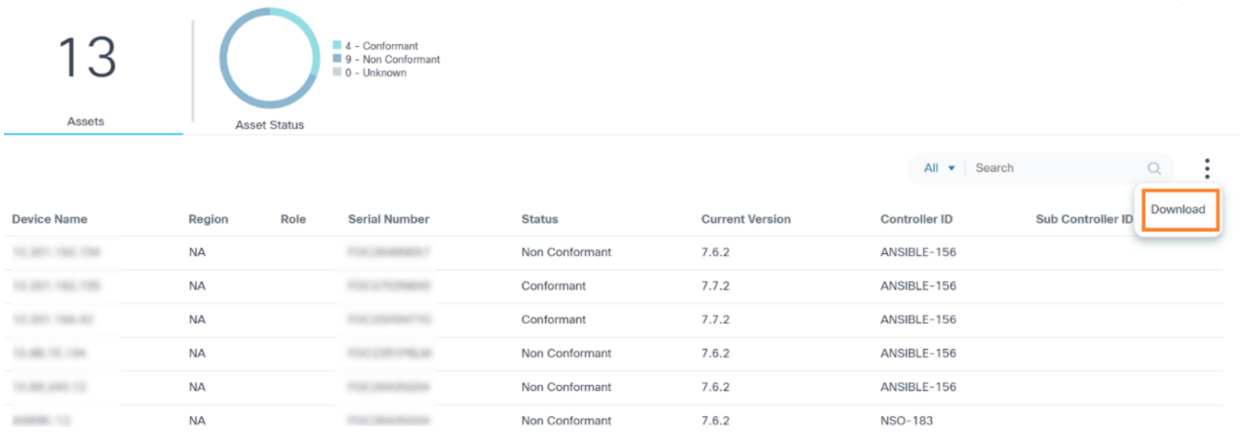
Nota: Los detalles de SMU solo se muestran para los recursos de controlador NSO, CNC, ANSIBLE, de conexión directa con el dispositivo y NDFC. Los módulos EPLD solo se muestran para los controladores NDFC.

---




Ver resultados

3. En la columna Action de un dispositivo, seleccione el icono More Options > View Results.




Descargar

4. Seleccione el icono Más opciones > Descargar para descargar los resultados en formato .csv con el estado de disponibilidad de SMU.


Vista de hoja de Excel

Nota: Ver resultados sólo muestra los resultados de la comprobación de conformidad ejecutada más recientemente. Los usuarios solo pueden ver los recursos a los que tienen acceso. En el caso de las políticas no operativas, la opción Ver resultados está desactivada.

Posibles estados de dispositivo:

- Conforme: Indica que el dispositivo se ajusta a la política definida
- No conforme: Indica que el dispositivo no es conforme cuando cumple las siguientes condiciones:

| Versión de destino | SMU | Comprobación de conformidad | Estado |
|---|---|---|---|
| No conforme | NA | NA | No conforme |
| Conforme | No disponible | Error de reglas | No conforme |
| Conforme | Disponible | Error de reglas | No conforme |
| Conforme | No disponible | Reglas correctas | No conforme |

- Desconocido: Indica que no se pudo realizar la comprobación de conformidad del software del dispositivo porque el dispositivo no tiene información de versión de software actual.

Los criterios para el estado Desconocido incluyen:

| Versión de destino | SMU | EPLD | Comprobación de conformidad | Estado |
|---|---|---|---|---|
| No conforme | NA | NA | NA | No conforme |
| Conforme | No disponible | No conforme | Error de reglas | No conforme |
| Conforme | No disponible | Conforme | Error de reglas | No conforme |
| Conforme | Disponible | Conforme | Error de reglas | No conforme |
| Conforme | Disponible | No conforme | Error de reglas | No conforme |
| Conforme | No disponible | Conforme | Reglas correctas | No conforme |
| Conforme | No disponible | Conforme | Reglas correctas | No conforme |

Posibles estados de SMU:

- Disponible: Indica que SMU está presente en el dispositivo y en estado Activo
- No disponible: Indica que SMU puede no existir o que sí existe pero está en estado Inactivo

Posibles estados del módulo EPLD:

- Conforme: Indica que el módulo EPLD está presente en el dispositivo con la versión de destino esperada
- No conforme: Indica que el módulo EPLD está presente en el dispositivo con una versión de destino esperada no coincidente
- Falta módulo: Indica que los módulos EPLD no están configurados o suscritos en el dispositivo

Posibles estados de plantilla de comprobación de cumplimiento:

- Éxito: Indica que el dispositivo ejecutó correctamente la plantilla de proceso con comandos y reglas válidos
- Error: Indica que el dispositivo no pudo ejecutar la plantilla de proceso (por ejemplo, cuando los comandos son incorrectos)
- NA: Indica que el dispositivo no es apto para ejecutar la plantilla de proceso (por ejemplo, cuando el dispositivo no es conforme con la versión de destino definida)

---

 Nota: Debe tenerse en cuenta la siguiente lista.

---

- Las comprobaciones de conformidad del software solo funcionan con dispositivos que pertenecen al arrendatario predeterminado
- Las comprobaciones de conformidad del software se basan en el inventario de activos como fuente de información para las versiones de software actuales de los dispositivos. Si los datos del inventario de activos están obsoletos, los resultados de las comprobaciones de conformidad del software están obsoletos. Para evitar el problema de los datos obsoletos, utilice la función de comprobación de inventario en tiempo real al iniciar la ejecución de la política de conformidad
- La programación predeterminada se puede cambiar en OS Upgrade > Settings > Software Conformance
- Después de actualizar a BPA 5.1, todas las políticas existentes se mueven a un estado inhabilitado; los usuarios deben editar cada directiva, seleccionar los valores adecuados, habilitarla y, a continuación, guardar los cambios para su uso posterior

## Política de actualización

El componente de directiva de actualización admite dos tipos de directivas:

- Política de un solo paso:
  - Any-Any
  - <specific source version (7.7.1)> - <specific target version (7.7.2)>
- Política de varios pasos:
  - v7.7.1 - 7.7.2
  - v7.7.2 - 7.7.8

- La actualización en varios pasos puede incluir SMU de puente, como se muestra en el siguiente ejemplo:
    - v7.7.1 - v7.7.1[SMU de puente]
    - V7.7.1[SMU de puente] - 7.7.8

El componente de política de actualización proporciona la flexibilidad necesaria para predefinir los siguientes artefactos específicos de la plataforma:

- Rutas de actualización
- Plantillas o flujos de trabajo previos y posteriores a la validación
- Flujo de distribución
- Flujo de activación
- Flujo de trabajo de backup
- Valores de límite de tiempo
- Flujo de trabajo de reversión
- Diferencias anteriores y posteriores válidas
- Flujo de trabajo de desvío de tráfico o flujo de trabajo de inversión de tráfico

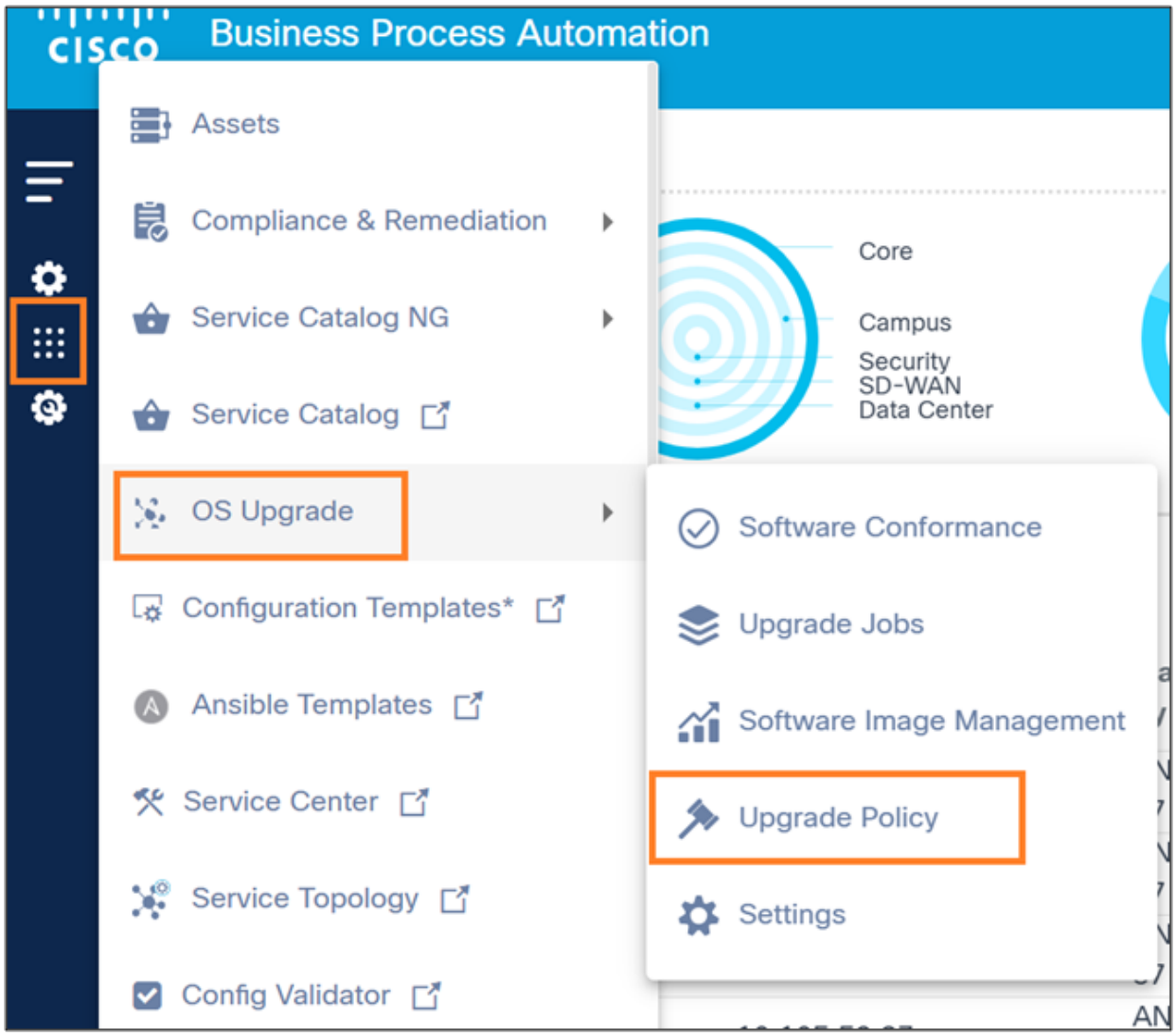
Prerequisites

- Plantillas o flujos de trabajo de procesos de validación previos y posteriores requeridos
- Flujos de trabajo de copia de seguridad, distribución, activación y reversión necesarios
- Metadatos de imagen requeridos

Visualización y administración de políticas de actualización

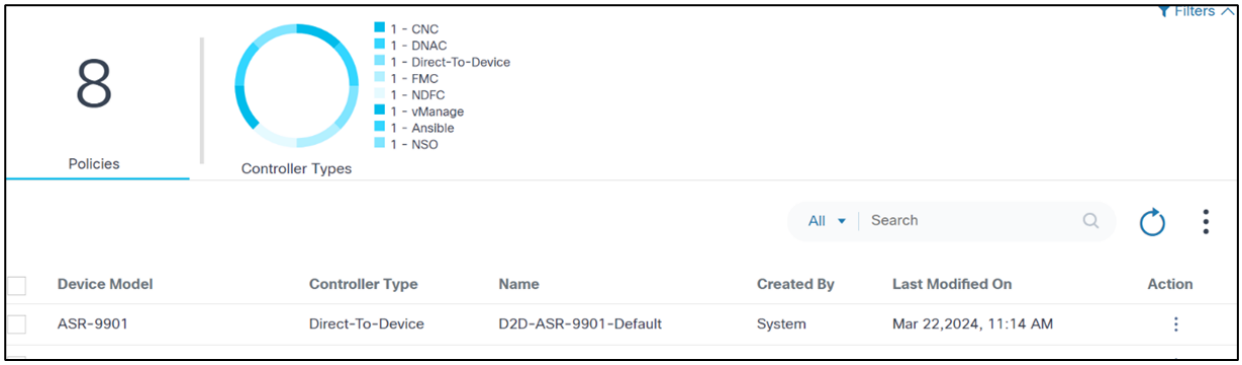
Para acceder a la página Política de Actualización:

1. Inicie sesión en BPA con credenciales que tengan acceso suficiente a la política de actualización.




Navegación de directivas de actualización

2. Seleccione OS Upgrade > Upgrade Policy. Se muestra la página Política de actualización.

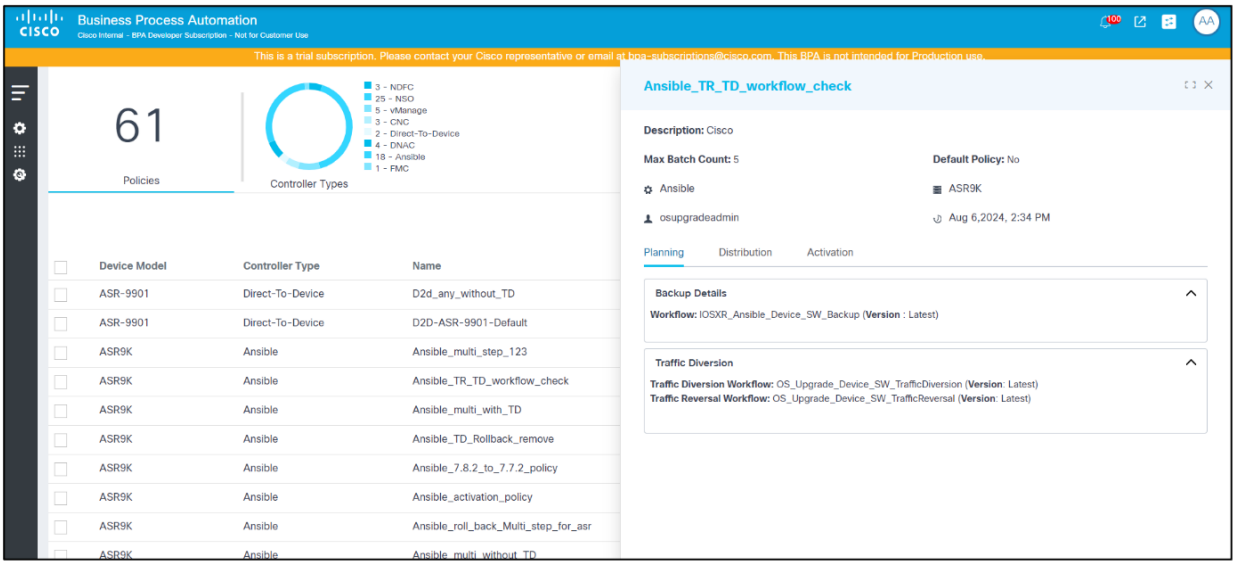



Política de actualización

La página Política de Upgrade contiene lo siguiente:

- Una sección de análisis, que se muestra en la parte superior, que proporciona lo siguiente:

    - El número total de directivas de actualización del sistema
    - Un filtro rápido Tipos de controlador que proporciona la capacidad de filtrar por tipo de controlador
- Un icono Más opciones que proporciona la opción de Crear política y acciones de procesamiento masivo como Eliminar todas las políticas seleccionadas
- Un filtro Search para buscar políticas que se pueden filtrar de la siguiente manera:
    - Todos: Buscar en todos los campos
    - Modelo de dispositivo: Buscar políticas con un modelo especificado
    - Nombre: Buscar directivas con un nombre de directiva especificado
    - Creado por: Buscar directivas con un usuario especificado
- Ordenar directivas haciendo clic en los nombres de columna o campos de tabla correspondientes




Vista de detalles de política

- Hacer clic en una política concreta o en una fila de la vista de detalles de una política

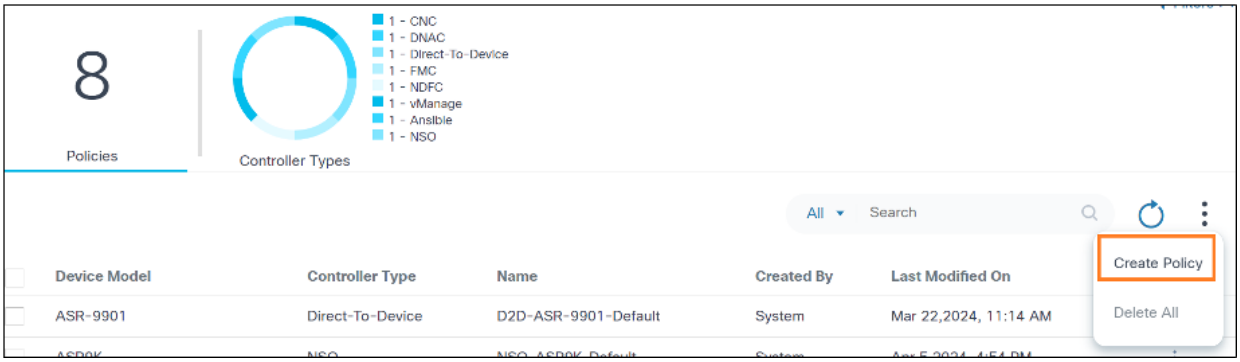
---

Nota: El mismo modelo de dispositivo y el mismo tipo de controlador pueden tener cualquier número de políticas si los nombres de las políticas son únicos.

---

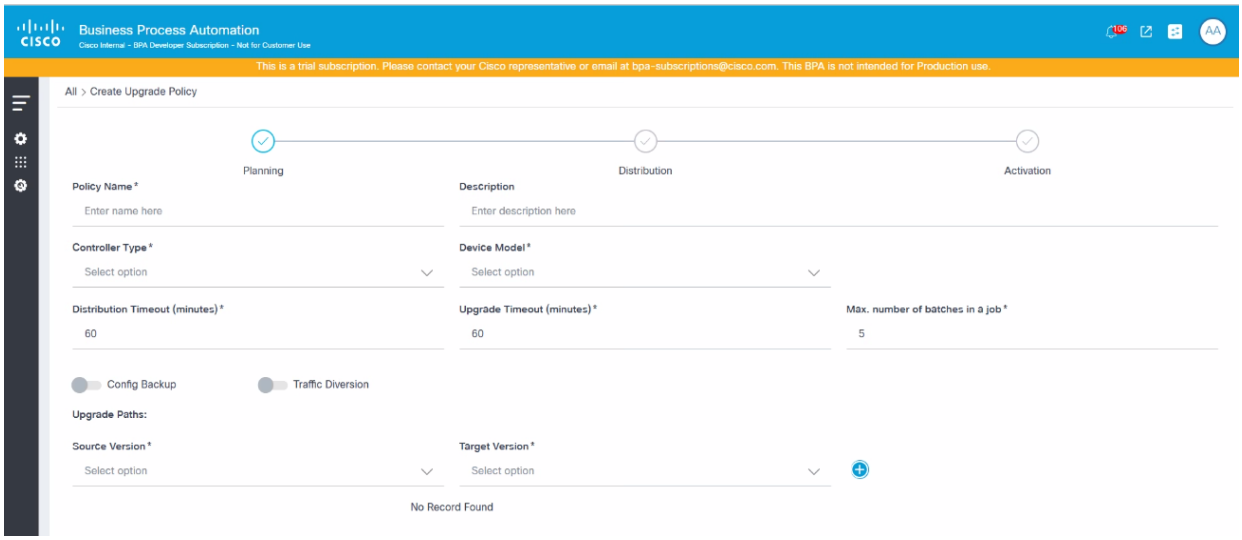
Creación de políticas de actualización

1. Inicie sesión en BPA con credenciales que tengan acceso de gestión para las políticas de actualización.
2. Seleccione OS Upgrade > Upgrade Policy. Se muestra la página Política de actualización.




Crear política

3. Seleccione Más opciones > Crear directiva. Se muestra la página Create Upgrade Policy.




Crear política de actualización

Planificación

1. Configure los parámetros relacionados con la política general. En la tabla siguiente se proporciona una breve descripción de cada campo.

| Campo | Descripción |
|---|---|
| Nombre de política | Nombre de la política |
| Descripción | Breve descripción de la política |
| Tipo de controlador | Controlador apropiado que se utiliza para realizar la actualización del sistema operativo |
| Modelo de dispositivo | Modelo de dispositivo que se utiliza para realizar la actualización del SO |
| Límite de tiempo de distribución (minutos) | Tiempo de espera máximo en minutos para la actividad de distribución de imágenes |

| Campo | Descripción |
| --- | --- |
| Límite de tiempo de actualización (minutos) | Tiempo de espera máximo en minutos para la actividad de activación de la imagen |
| Número máximo de lotes en un trabajo | Número de lotes que se pueden agregar en un trabajo; el número máximo de lotes permitidos es 20 |
| Configurar alternancia de copia de seguridad | Active esta opción si la copia de seguridad es necesaria y rellene los siguientes campos en la ventana para los controladores de vManage y de conexión directa con el dispositivo:<br><br>- Nombre del flujo de trabajo: El flujo de trabajo de backup aplicable<br><br>Nota: Si no se encuentran los flujos de trabajo, asegúrese de que estén etiquetados correctamente con la etiqueta NextGen de actualización del sistema operativo<br><br>- Utilizar el flujo de trabajo más reciente: Si se selecciona, se utiliza la última versión del flujo de trabajo seleccionado<br><br>- Versión del flujo de trabajo: La versión personalizada del flujo de trabajo; solo se puede seleccionar si no se ha seleccionado Usar último flujo de trabajo.<br><br>Para los controladores NDFC, NSO, CNC y Cisco Catalyst Center, la copia de seguridad se realiza a través del servicio de copia de seguridad y restauración. Por lo tanto, se debe seleccionar una política de copia de seguridad y restauración en la ventana Detalles de la copia de seguridad.<br><br>Nota: Los usuarios deben seleccionar la política apropiada para el tipo de controlador. Consulte la sección Copia de Seguridad y Restauración para obtener más información sobre las políticas de copia de seguridad y restauración.<br><br>Para activar la copia de seguridad de los dispositivos Nexus, la configuración de la función scp-server debe estar presente en los dispositivos de destino. |

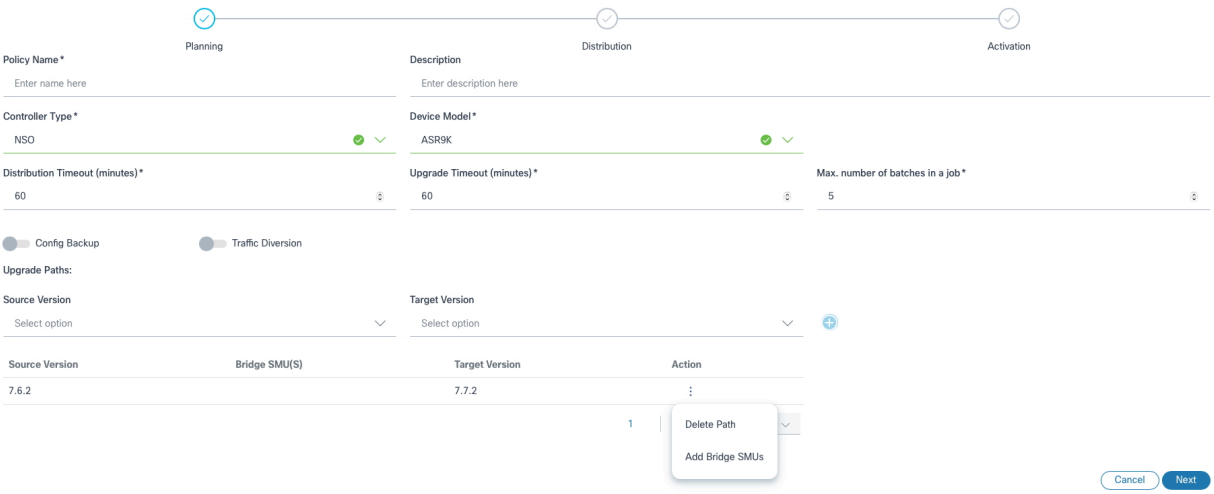
| Campo | Descripción |
| --- | --- |
| Alternancia de desvío de tráfico | Active esta opción si el desvío del tráfico es necesario y rellene los campos siguientes de la ventana Traffic Diversion:<br><br>- Flujo de trabajo de desvío de tráfico: El flujo de trabajo de desvío de tráfico aplicable.<br><br>Nota: Si no se encuentran los flujos de trabajo, asegúrese de que estén etiquetados correctamente con la etiqueta NextGen de actualización del sistema operativo<br><br>- Flujo de trabajo de reversión de tráfico: El flujo de trabajo de reversión de tráfico aplicable.<br><br>Nota: Si no se encuentran los flujos de trabajo, asegúrese de que estén etiquetados correctamente con la etiqueta NextGen de actualización del sistema operativo<br><br>- Utilizar el flujo de trabajo más reciente: La última versión del flujo de trabajo seleccionado anteriormente<br><br>- Versión del flujo de trabajo: La versión personalizada del flujo de trabajo; solo se puede seleccionar si no se ha seleccionado Usar flujo de trabajo más reciente. |
| Rutas de actualización | Las rutas de actualización definen las rutas de actualización escalonadas aplicables; se pueden agregar varias versiones de origen y destino en los campos siguientes para satisfacer las distintas demandas<br><br>- Versión de origen: La versión inicial de la ruta de actualización<br><br>- Versión de destino: La versión final de la ruta de actualización<br><br>- Versión de origen (Cualquiera) a Versión de destino (Cualquiera): Esto está disponible al seleccionar Any para los campos Source Version y Target Version, que es el valor predeterminado para todos los modelos de dispositivos; en este escenario, las páginas Distribución y Activación proporcionan un proceso unificado para la actualización |

| Campo | Descripción |
| --- | --- |
| | - Versión de Origen (Versión Específica) a Versión de Destino (Versión Específica): Esto está disponible al seleccionar las versiones de imagen específicas disponibles para el modelo de dispositivo; se pueden agregar varias versiones de origen y destino; el número de entradas del proceso de actualización de distribución y activación coincide con el número de versiones de origen y destino agregadas, y cada una se presenta como una sección contraíble etiquetada con las versiones de origen y destino correspondientes. Una ruta de actualización requiere que se apliquen las SMU obligatorias en la versión de origen antes de actualizar a la versión de destino agregándolas como SMU de puente a la ruta de actualización correspondiente. Para obtener más información sobre las SMU de puente, consulte la siguiente sección. |

SMU de puente

Las SMU de puente, también denominadas SMU de actualización o degradación obligatorias, son un requisito previo y deben instalarse antes de actualizar o reducir a otra versión de software de la misma plataforma o modelo.

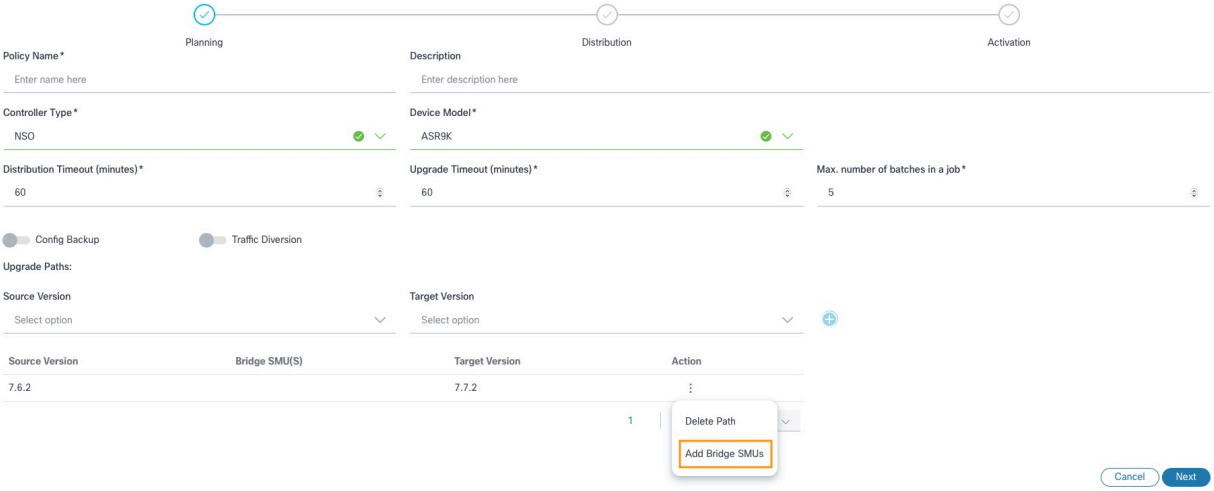
Adición de SMU de puente en una ruta de actualización




Opciones de ruta de actualización

1. Después de agregar una ruta de actualización, seleccione el icono Más opciones. Se

muestran las opciones Delete Path y Add Bridge SMUs.

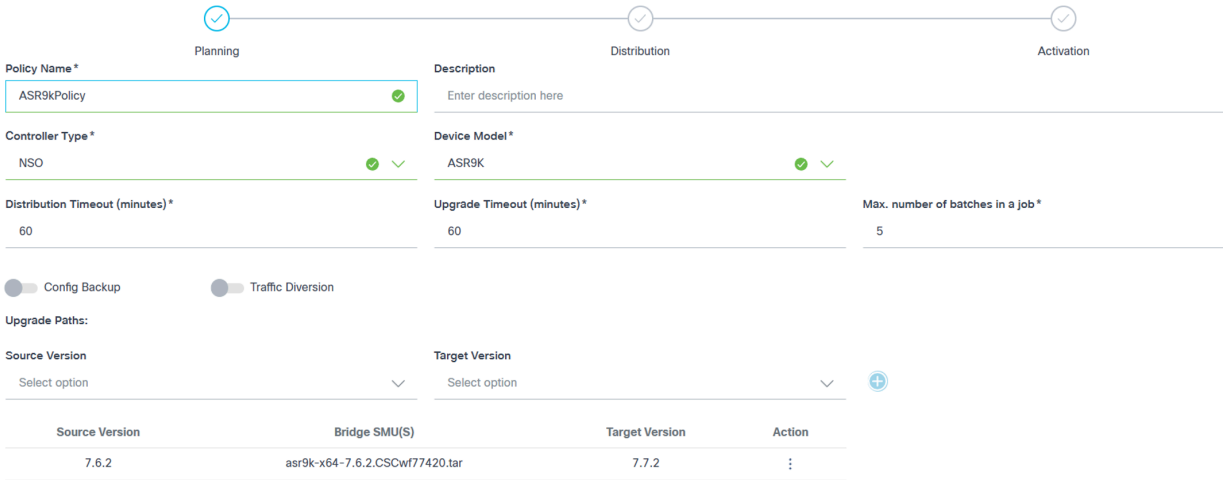



Agregar SMU de puente

2. Seleccione Add Bridge SMUs. Se abre la ventana Add Bridge SMUs. Se muestran todas las SMU de puente disponibles para la ruta de actualización especificada.


Agregar SMU de puente

3. En la ventana Add Bridge SMUs, seleccione las casillas de verificación apropiadas para agregar Bridge SMUs o desactive las casillas para quitarlas. Después de agregar las SMU del puente, la ruta de actualización se actualiza con los detalles de la SMU del puente seleccionada.




Ruta de actualización con SMU de puente

---

Nota: Cada ruta de actualización que incluye SMU(s) de puente se considera una actualización de dos pasos en el proceso de actualización. Para la ruta de actualización que se muestra en la figura anterior, la ruta de actualización final es:

---

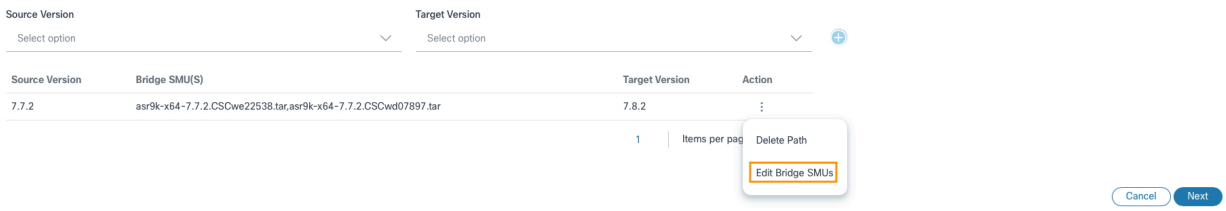
- 7.6.2 - 7.6.2 [SMU de puente]

Esta ruta representa la actualización del dispositivo que se ejecuta en la versión 7.6.2 con las SMU del puente.

- 7.6.2 [SMU de puente] - 7.7.2

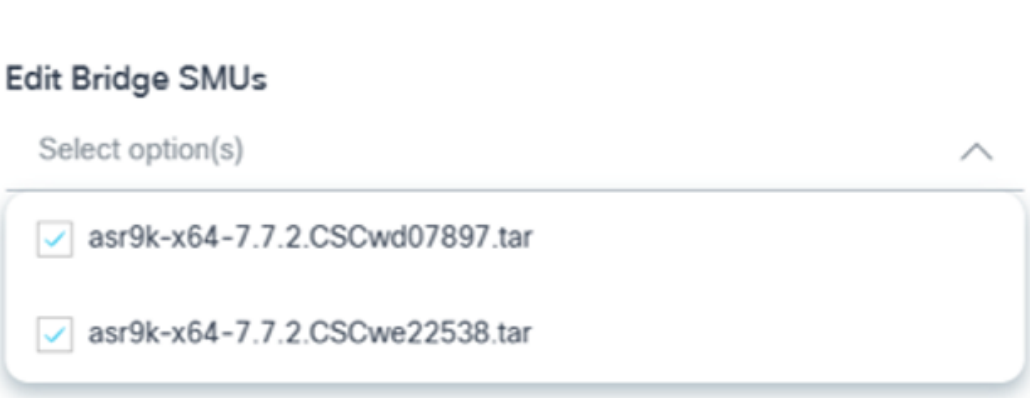
Esta ruta representa la actualización del dispositivo de v7.6.2 a v7.7.2. En este caso, la versión de origen del dispositivo es 7.6.2, incluidas las SMU de puente aplicadas.

Edición de SMU de Bridge



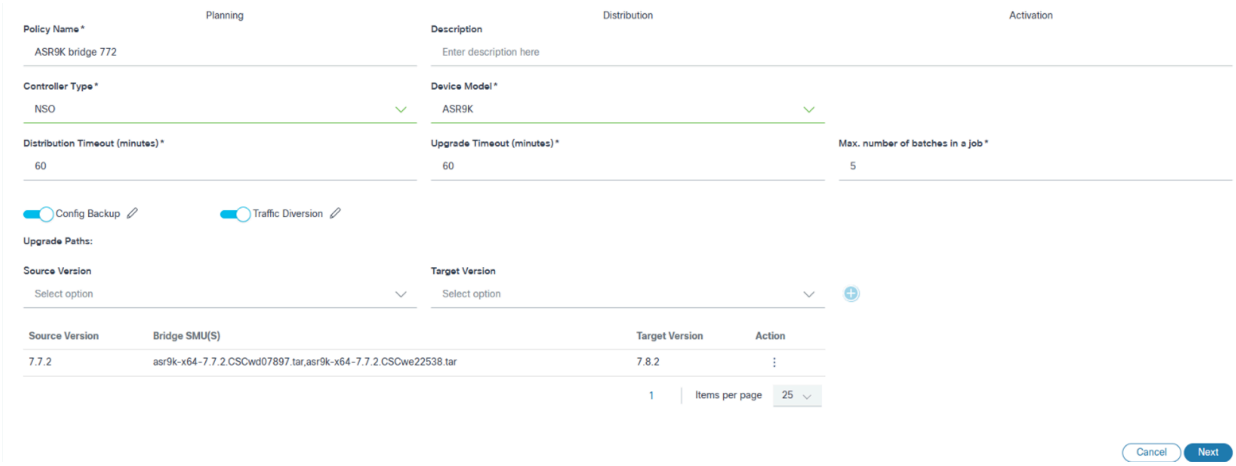

Ruta de actualización con SMU de puente

1. En la sección Upgrade Paths, seleccione el icono More Options > Edit Bridge SMUs. Se abre la ventana Edit Bridge SMUs.




Editar SMU de puente

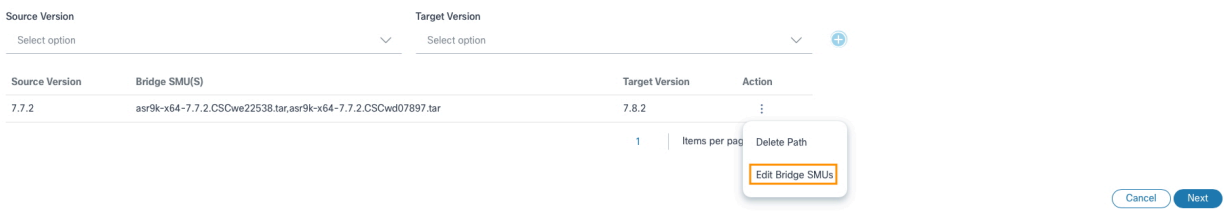
2. Active o desactive las casillas de verificación correspondientes para actualizar las SMU de puente.
3. Click OK. Se muestra un resumen de los cambios.




Resumen de cambios

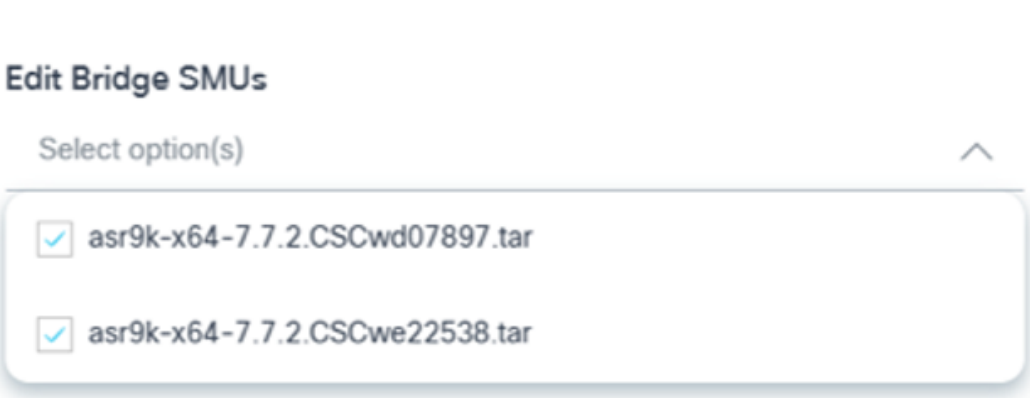
4. Verifique el resumen de los cambios y haga clic en Next.

## Eliminación de SMU de puente



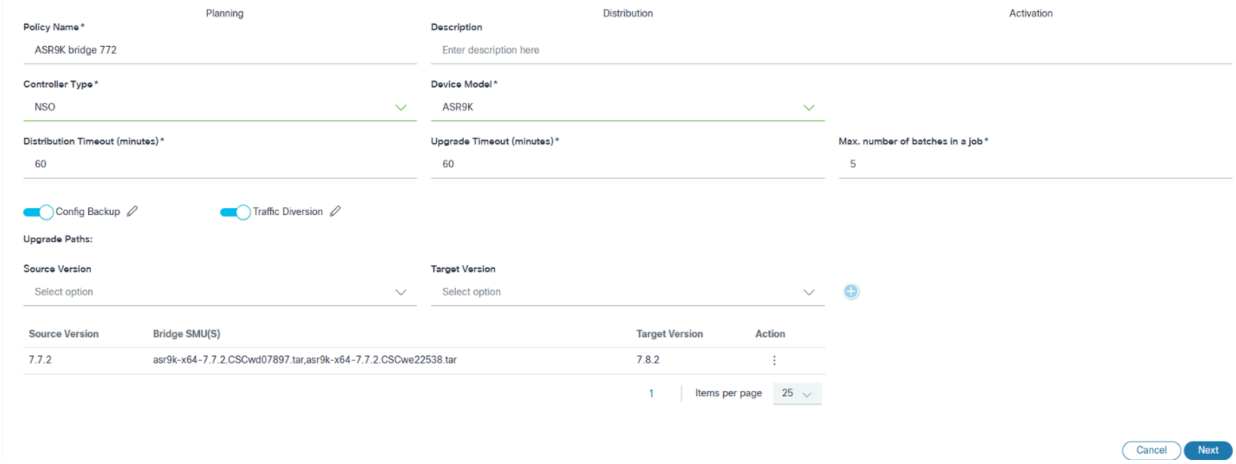

Editar SMU de puente

1. En la sección Upgrade Paths, seleccione el icono More Options > Edit Bridge SMUs. Se abre la ventana Edit Bridge SMUs.




Editar SMU de puente

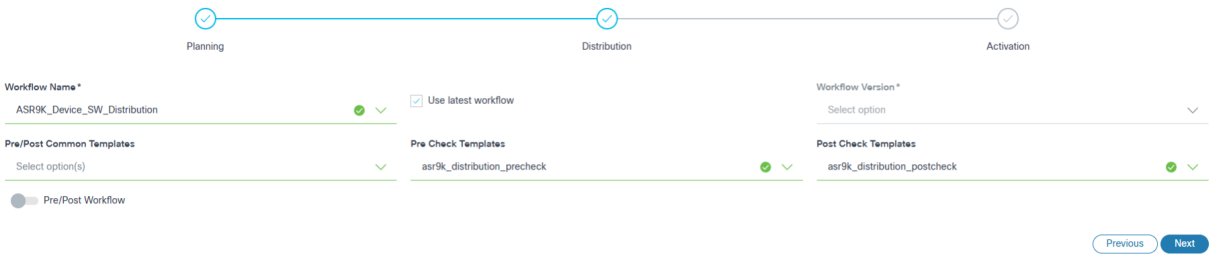
2. Desactive las casillas de verificación correspondientes para quitar SMU de puente.
3. Click OK. Se muestra un resumen de los cambios.



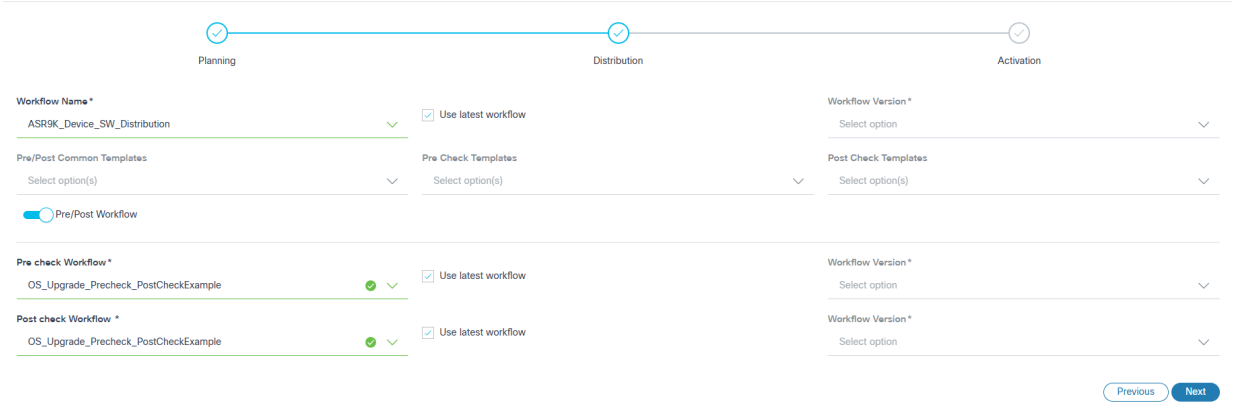

Resumen de cambios

Distribución

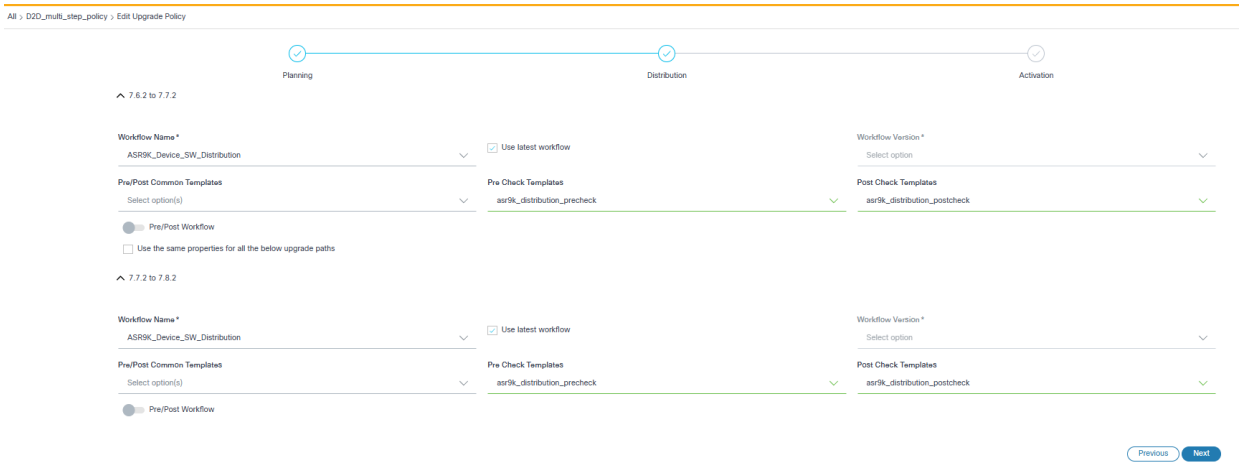
La distribución toma parámetros de entrada relacionados con la distribución de imágenes (es decir, copia de imagen). Las imágenes siguientes son los parámetros de entrada necesarios para cada tipo de ruta de actualización.



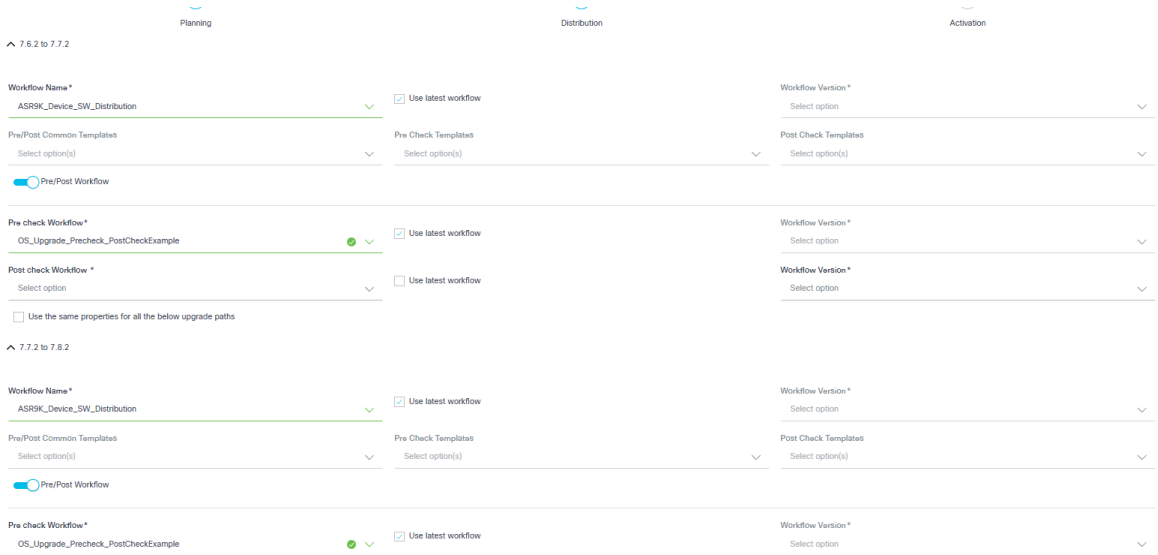

Sección de distribución de imágenes: actualización en un solo paso



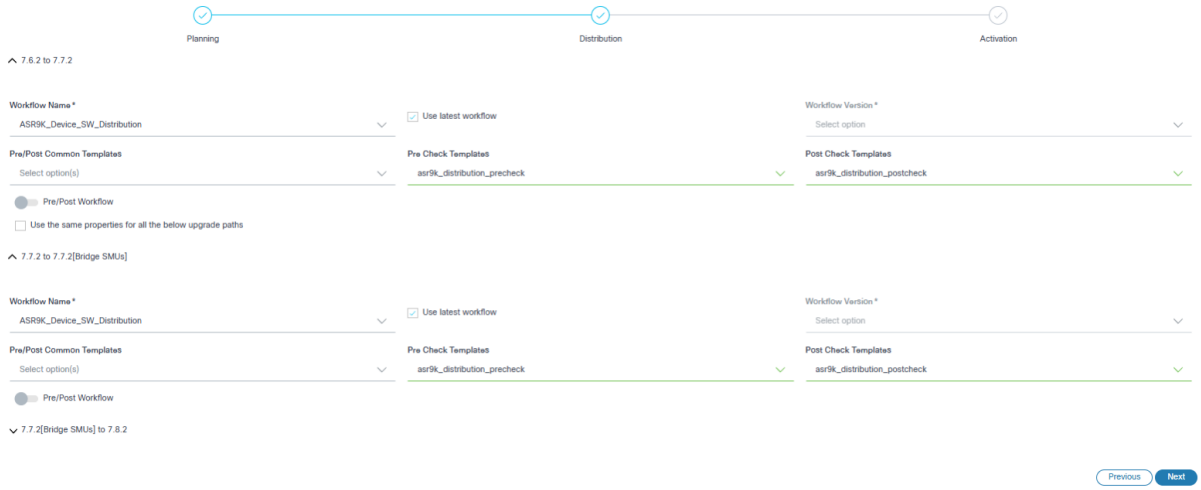

Sección de distribución de imágenes: actualización en un solo paso con la función de flujo de trabajo previo y posterior activada




Sección de distribución: actualización en varios pasos




Sección de distribución: actualización en varios pasos




Sección de distribución: actualización de SMU de puente

1. Configure los parámetros relacionados con la distribución de imágenes.
2. En la tabla siguiente se proporciona una breve descripción de cada campo.

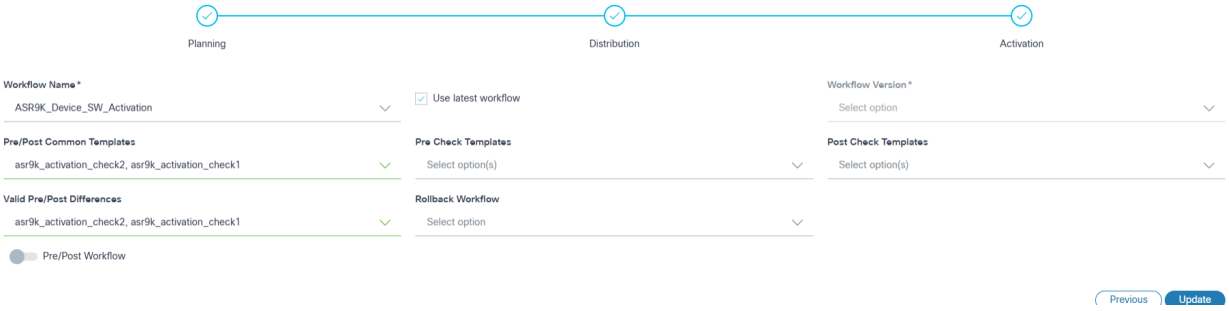
| Campo | Descripción |
|---|---|
| Nombre de flujo de trabajo | El flujo de trabajo de distribución aplicable |
| Utilizar el último flujo de trabajo | Seleccionar la última versión del flujo de trabajo seleccionado |
| Versión de flujo de trabajo | La versión personalizada del flujo de trabajo; sólo se puede seleccionar si la casilla de verificación Usar flujo de trabajo más reciente no está activada |
| Plantillas comunes anteriores y posteriores | Plantillas de proceso que se ejecutan en ambas etapas (es decir, antes y después de la comprobación)<br><br>Nota: Las comprobaciones solo son específicas del hito de distribución.<br><br>Consulte Plantillas de Proceso para obtener más información |
| Alternancia entre el flujo de trabajo anterior y posterior | Permite a los usuarios seleccionar la ejecución de flujos de trabajo anteriores o posteriores a la comprobación en el hito de distribución. Cuando la alternancia está activada, sólo se pueden configurar flujos de trabajo anteriores o posteriores a la comprobación. |
| Flujo de trabajo anterior a la comprobación | Incluye los comandos ejecutados únicamente durante la fase de comprobación previa.<br><br>Nota: Estas comprobaciones son específicas del hito de distribución. |

| Campo | Descripción |
| --- | --- |
| Flujo de trabajo posterior a la comprobación | El flujo de trabajo posterior a la comprobación incluye los comandos ejecutados de forma única durante la fase posterior a la comprobación.<br><br>Nota: Estas comprobaciones son específicas del hito de distribución. |
| Plantillas de comprobación previa | Las plantillas de proceso que contienen comandos exclusivos de comprobación previa; las plantillas solo se ejecutan durante la fase de comprobación previa.<br><br>Nota: Las comprobaciones solo son específicas del hito de distribución. |
| Plantillas posteriores a la comprobación | Las plantillas de proceso que contienen comandos exclusivos posteriores a la comprobación; las plantillas sólo se ejecutan durante la fase posterior a la comprobación.<br><br>Nota: Las comprobaciones solo son específicas del hito de distribución. |
| Utilice las mismas propiedades para todas las siguientes rutas de actualización | Las propiedades uniformes se aplican a través de todas las rutas de actualización en las actualizaciones de selección múltiple.<br><br>Nota: Si se selecciona, se aplican las mismas propiedades a todas las rutas de actualización de la actualización de selección múltiple. |

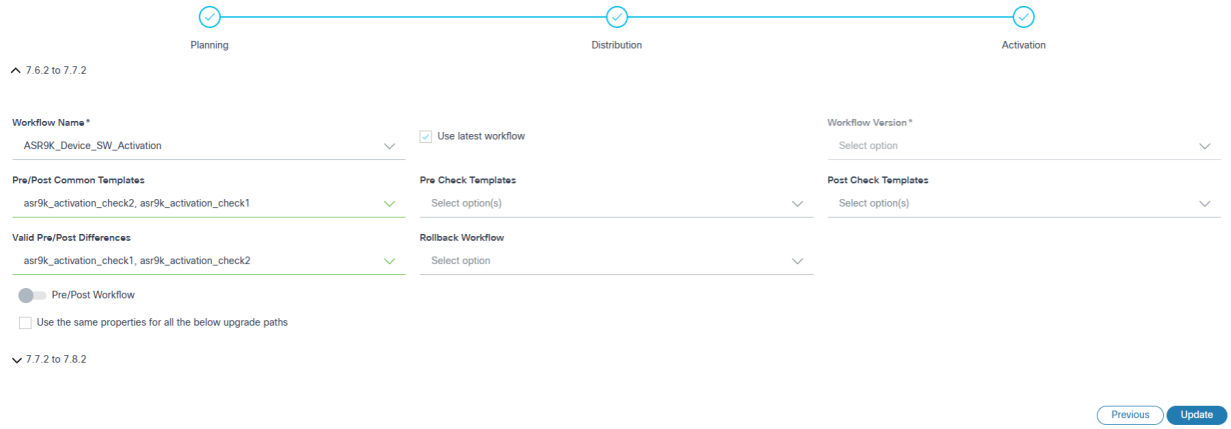
 Nota: Los flujos de trabajo o las plantillas de proceso deben etiquetarse correctamente con la etiqueta Next-Gen (Actualización del sistema operativo).

3. Haga clic en Siguiente para continuar con la sección Activación.

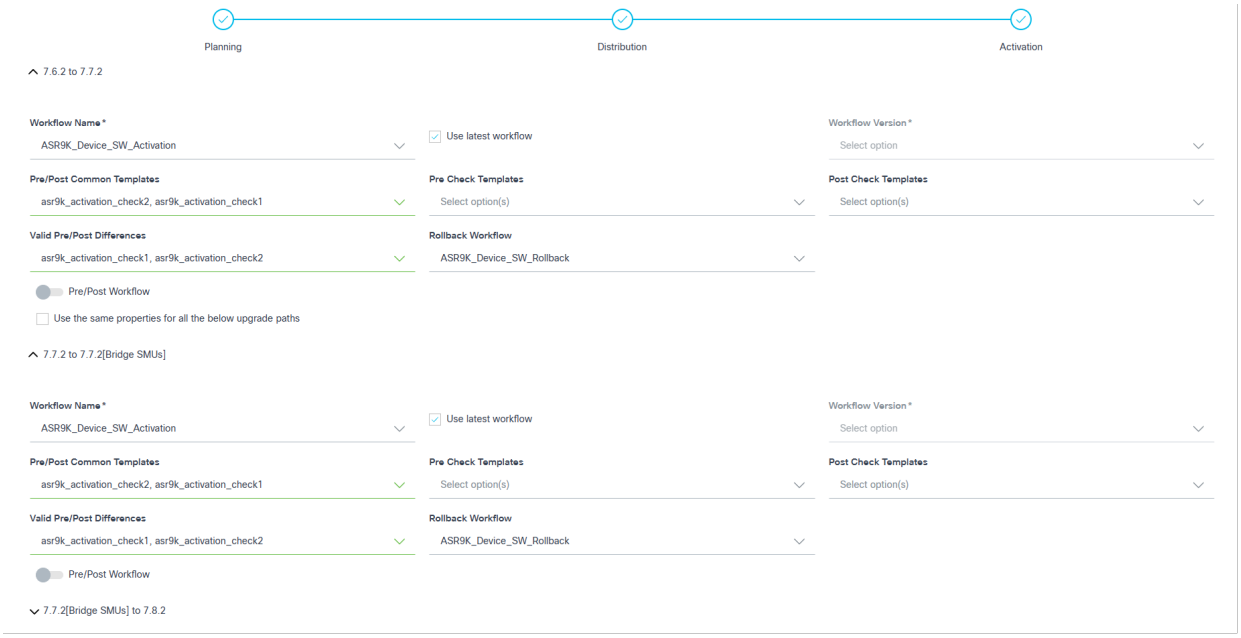
Activación




Sección de activación: actualización en un solo paso




Sección de activación: actualización en varios pasos




Sección de activación - Actualización de Bridge SMU

1. Configure los parámetros relacionados con la activación de la imagen.
2. En la tabla siguiente se proporciona una breve descripción de cada campo.

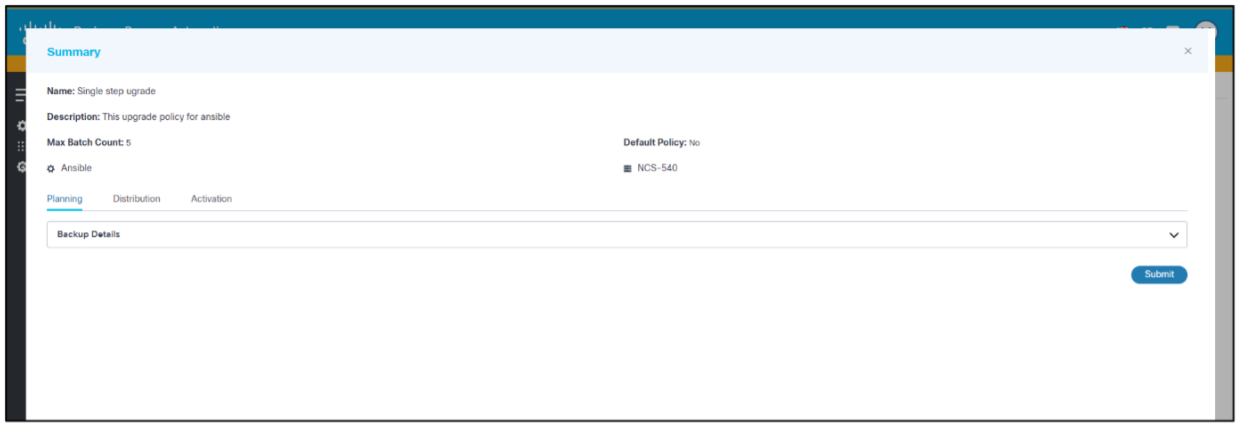
| Campo | Descripción |
| --- | --- |
| Nombre de flujo de trabajo | El flujo de trabajo de activación aplicable |
| Utilizar el último flujo de trabajo | Seleccionar la última versión del flujo de trabajo seleccionado |
| Versión de flujo de trabajo | La versión personalizada del flujo de trabajo; solo se puede seleccionar si la casilla de verificación Usar flujo de trabajo más reciente no está activada |
| Plantillas comunes anteriores y posteriores | Plantillas de proceso que se ejecutan en ambas etapas (es decir, antes y después de la comprobación).<br><br>Nota: Las comprobaciones sólo son específicas del hito de activación.<br><br>Consulte Plantillas de Proceso para obtener más información |
| Plantillas de comprobación previa | Las plantillas de proceso que contienen comandos exclusivos de comprobación previa; las plantillas solo se ejecutan durante la fase de comprobación previa.<br><br>Nota: Las comprobaciones sólo son específicas del hito de activación. |
| Plantillas de cheques postales | Las plantillas de proceso que contienen comandos exclusivos posteriores a la comprobación; las plantillas sólo se ejecutan durante la fase posterior a la comprobación.<br><br>Nota: Las comprobaciones sólo son específicas del hito de activación. |
| Diferencia anterior/posterior válida | Las plantillas de proceso seleccionadas para omitir las diferencias.<br><br>Nota: Las comprobaciones sólo son específicas del hito de activación. |
| Flujo de trabajo de reversión | El flujo de trabajo de reversión aplicable.<br><br>Nota: Si una de las rutas de actualización con el flujo de trabajo de reversión está seleccionada en la actualización de selección múltiple, todos los demás pasos de actualización se seleccionan con el flujo de trabajo de reversión de forma predeterminada. |
| Flujo de trabajo anterior a la comprobación | Este flujo de trabajo de comprobación previa personalizado consta de comandos específicos cuyos resultados de ejecución se pueden seleccionar y revisar. Se lleva a cabo únicamente durante la fase previa al control.<br><br>Nota: Estas comprobaciones son específicas del hito de activación. |
| Flujo de trabajo posterior a la comprobación | Este flujo de trabajo personalizado posterior a la comprobación consta de comandos específicos cuyos resultados de ejecución se pueden seleccionar y revisar. Se lleva a cabo únicamente durante la fase posterior al control.<br><br>Nota: Estas comprobaciones son específicas del hito de activación. |
| Utilice las mismas propiedades para todas las | Las propiedades uniformes se aplican a través de todas las rutas de actualización en las actualizaciones de selección múltiple. |

| Campo | Descripción |
| --- | --- |
| siguientes rutas de actualización | Nota: Si se selecciona, se aplican las mismas propiedades a todas las rutas de actualización de la actualización de selección múltiple. |

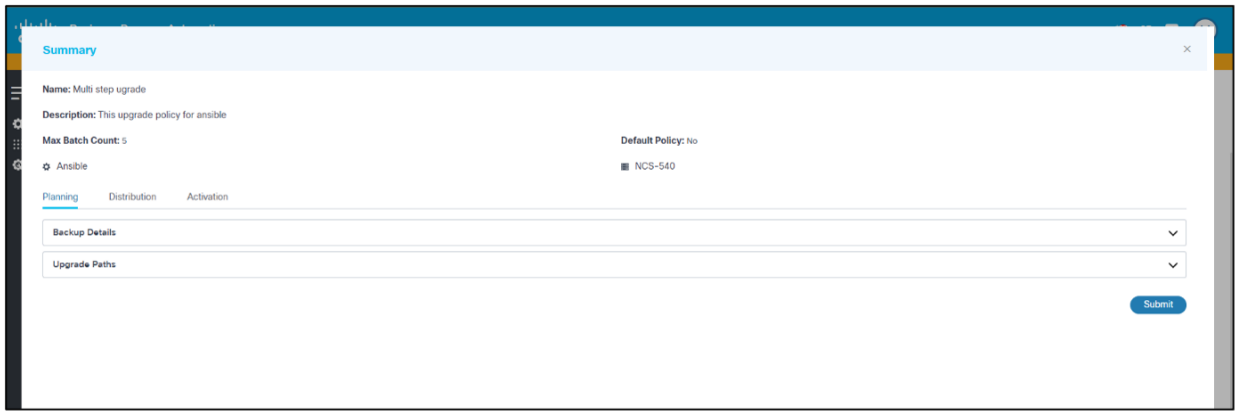
Nota: Debe tenerse en cuenta lo siguiente:

- El algoritmo de clave pública necesario para los dispositivos Nexus se debe configurar en NSO.
- Configure las funciones de bgp, bfd y hsrp para ejecutar plantillas de comprobación previa y posterior en los dispositivos Nexus.

3. Haga clic en Crear. Se muestra un resumen de los campos.




Resumen - Política de actualización en un solo paso




Resumen - Política de actualización en varios pasos

4. Verifique el resumen de los campos y haga clic en Enviar. Aparecerá una notificación de progreso seguida de un mensaje de confirmación. Las políticas son visibles en la página tras la creación correcta.

Se pueden crear políticas de actualización adicionales para otros modelos de dispositivos según sea necesario.

Edición de directivas de actualización

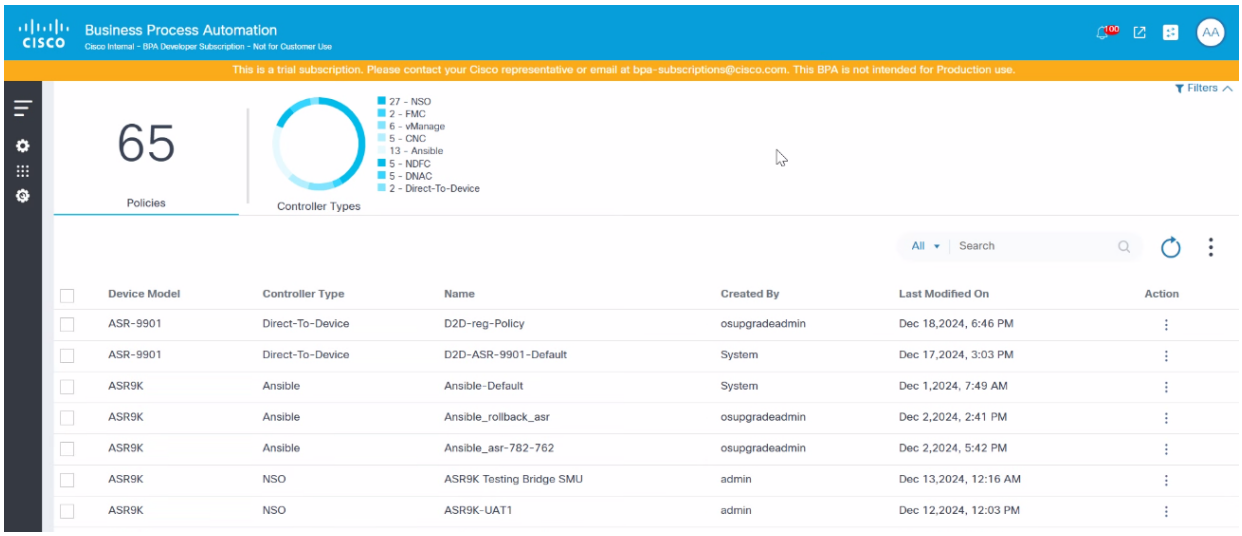

Resultado de la búsqueda de la política de actualización

1. En la página Upgrade Policy, localice la política deseada mediante el campo Search.


Editar directiva de actualización

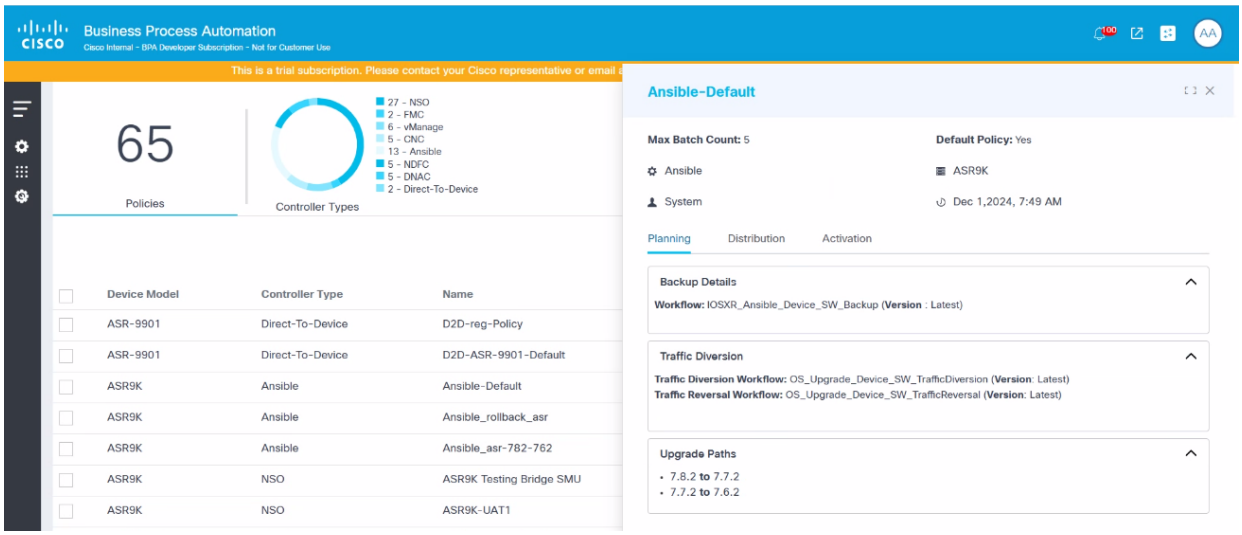
2. En la columna Acción de la política, seleccione el icono Más opciones > Editar.
3. Actualice los campos relevantes y haga clic en Update. Se muestra un resumen de los cambios.
4. Verifique el resumen de los cambios y haga clic en Submit. Las notificaciones de progreso se muestran seguidas de un mensaje de confirmación.

Visualización de directivas de actualización




Política de actualización

1. En la página Upgrade Policy, seleccione la fila de la política de actualización deseada. Se abre la vista detallada de la política.



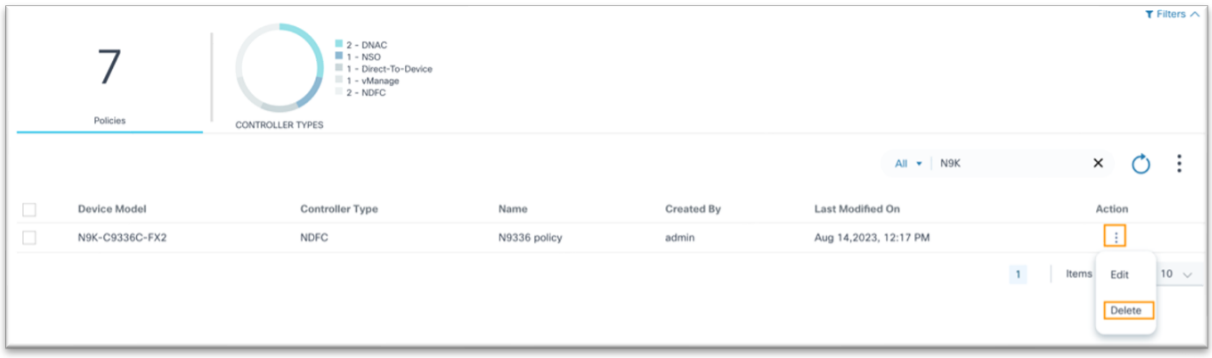

Vista detallada de la política de actualización

## Eliminación de directivas de actualización

Nota: Las directivas predeterminadas no se pueden eliminar, pero los usuarios pueden editar las plantillas de proceso y los flujos de trabajo.

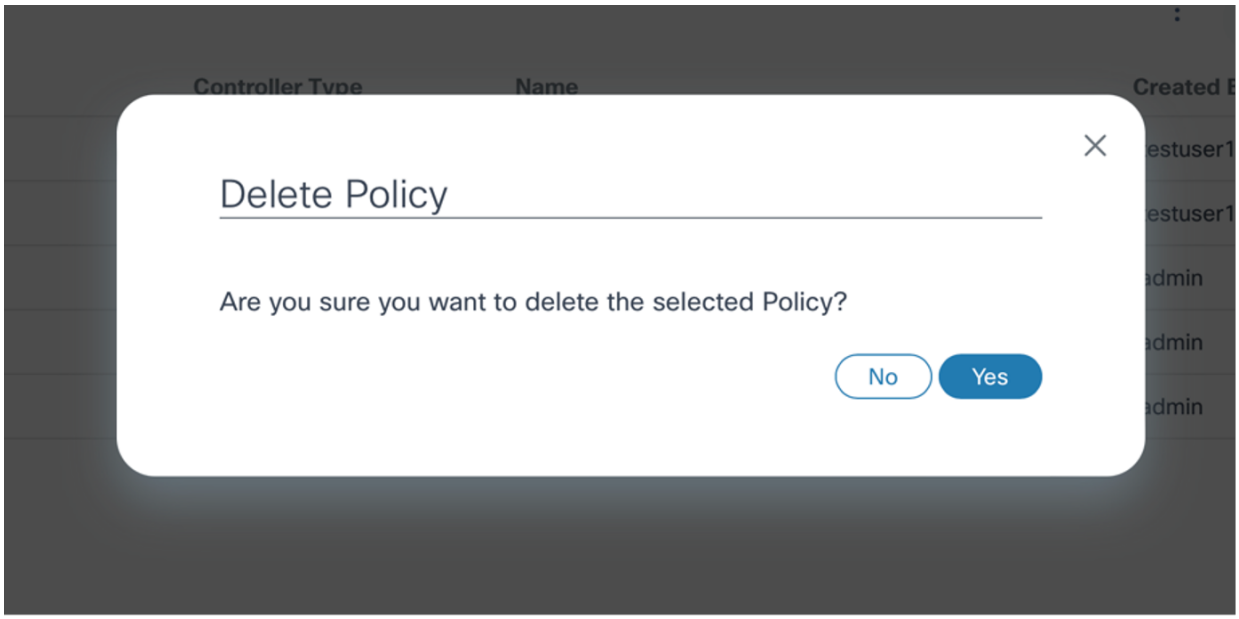

Política de actualización

1. En la página Upgrade Policies, localice la política deseada utilizando el campo Search**.




Eliminar directiva de actualización

2. En la columna Acción de la política, seleccione Más opciones > Eliminar. Se abre una ventana de confirmación




Confirmación de eliminación de política

3. Haga clic en Sí

Control del acceso a las políticas de actualización

Esta función proporciona control de acceso para las directivas de actualización, lo que impide que los usuarios no autorizados actualicen las directivas definidas en la aplicación Actualización del sistema operativo. Los administradores pueden restringir el acceso definiendo un grupo de recursos con directivas accesibles.

Para crear un grupo de recursos:

1. Vaya a Configuración > Grupos de recursos.
2. Cree un grupo de recursos con directivas a las que puedan acceder los usuarios que no sean administradores. Los usuarios que no son administradores y que pertenecen a este grupo de usuarios ahora sólo tienen acceso a las directivas disponibles en este grupo de recursos.
3. Cree una política de acceso para asociar el grupo de recursos a un grupo de usuarios,

Consulte Control de Acceso para obtener más información.

---

Nota: Debe tenerse en cuenta lo siguiente.

---

- Los usuarios pueden seleccionar flujos de trabajo incorrectos para Distribución y activación, lo que provoca un comportamiento no deseado. Es responsabilidad del usuario asignar correctamente el flujo de trabajo y verificar la aplicabilidad para hitos como los modelos de distribución, activación, reversión y dispositivo.
- Los flujos de trabajo y las plantillas de proceso deben asignarse con la etiqueta Next-Gen de actualización del sistema operativo para que estén disponibles para su selección al crear o actualizar políticas.
- Las políticas OOB predeterminadas creadas por el usuario del sistema no se pueden eliminar, pero los usuarios pueden editar las plantillas de proceso y los flujos de trabajo.

## Actualizar trabajos

Las actualizaciones de software se administran mediante la aplicación Upgrade Job, que consta de uno o más lotes, cada uno de los cuales tiene uno o más dispositivos de red. Se puede crear un trabajo en modo borrador y guardarlo varias veces. Las actualizaciones solo pueden comenzar después de que se haya confirmado el trabajo, lo que permite a los operadores planificar el cambio por adelantado.

Prerequisites

- Ventana Mantenimiento reservado para actualizaciones
- Aprobaciones previas para solicitud de cambio de actualización
- El servicio de copia de seguridad y restauración de la configuración debe estar activo y en ejecución
- El servicio de Planificador debe estar activo y en ejecución
- Los adaptadores BPA para sistemas externos (p. ej., un sistema de notificaciones), si los hay, deben estar incorporados

Visualización y gestión de trabajos de actualización

1. Inicie sesión en BPA con credenciales que tengan acceso a los trabajos de actualización.
2. Seleccione OS Upgrade > Upgrade Jobs. Se muestra la página Upgrade Job.

Tarea de actualización

La página Upgrade Job contiene lo siguiente:

---

Nota: De forma predeterminada, se muestran diez trabajos. Los números de página se pueden utilizar para desplazarse a otras páginas de trabajo.

---

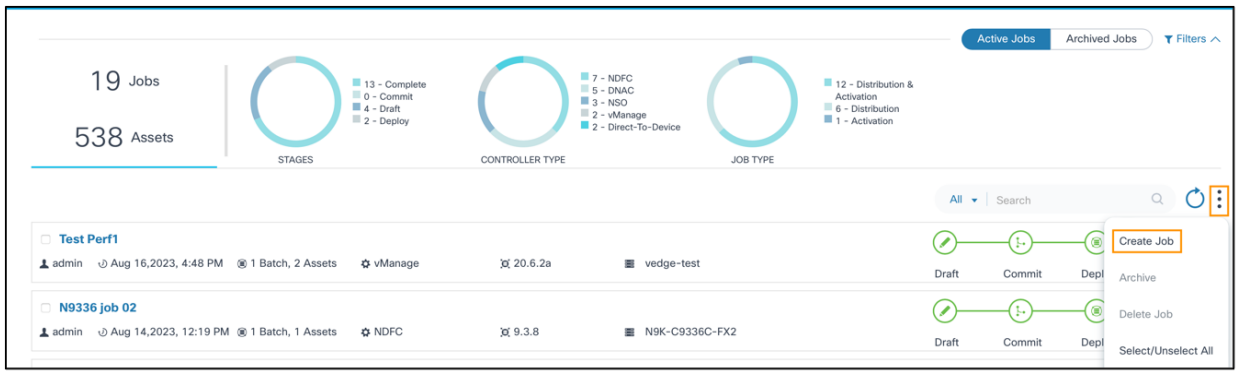
- Un botón Trabajos activos y Trabajos archivados que se puede utilizar para cambiar entre trabajos activos y archivados
- Una sección de análisis, que se muestra en la parte superior, que proporciona lo siguiente:
    - Total de trabajos y activos asociados a los trabajos
    - Gráfico de etapas con los siguientes filtros:
        - Borrador: El trabajo se encuentra en fase de borrador y aún no se ha confirmado

        - Commit: El trabajo se confirma con todos los dispositivos, lotes o programaciones necesarios hasta que se alcanza la programación
        - Implementación: La actividad de actualización se ha iniciado para uno o más lotes
        - Completo: La actividad de actualización ha finalizado para todos los dispositivos que pertenecen a todos los lotes
    - Gráfico Tipo de controlador: Permite el filtrado de tareas mediante los tipos de controlador Cisco Catalyst Center, vManage, NSO, NDFC, Direct-to-Device, CNC, ANSIBLE y FMC
    - Gráfico Tipos de trabajo con los filtros siguientes:
        - Distribución: Trabajos que realizan el almacenamiento provisional o la copia de imágenes de un controlador a dispositivos
        - Activación: Trabajos que realizan la activación o actualización del software de un dispositivo
        - Distribución y activación: Trabajos que realizan el almacenamiento provisional o la copia y la activación o actualización del software de un dispositivo
- El campo Search que se puede utilizar para realizar una búsqueda genérica en todos los metadatos o por los campos Job Name y Created By.
- El icono Actualizar que se puede utilizar para actualizar el resumen del trabajo y borrar los filtros del gráfico o cualquier búsqueda personalizada en el campo Buscar
- El icono Más opciones que proporciona opciones para Crear un nuevo trabajo de actualización y para Archivar o Eliminar trabajos seleccionados; los usuarios pueden seleccionar o anular la selección de Todo
- Los trabajos se muestran como paneles y proporcionan una vista rápida de la siguiente información:
    - El icono Tarea de usuario se muestra con el número de tareas de usuario si hay tareas de usuario disponibles
    - El usuario que creó el trabajo
    - La fecha de creación del trabajo
    - El número de lotes y activos
    - El tipo de controlador (por ejemplo, Cisco Catalyst Center, vManage, NDFC, conexión directa con el dispositivo, CNC, ANSIBLE o FMC)
    - La versión de destino
    - El modelo de dispositivo aplicable
    - Una vista de hitos de las etapas de las tareas (es decir, Borrador, Confirmar, Implementar y Finalizar) con una leyenda de color para cada hito:
        - Gris: El hito no ha comenzado
        - Azul: El hito está en curso
        - Rojo: Emisión hito
        - Verde: Hito completado
    - Leyenda de color al final de los hitos que muestra el estado del trabajo:
        - Verde: El trabajo se ha completado
        - Rojo: El trabajo tiene problemas

- Azul: El trabajo está en curso

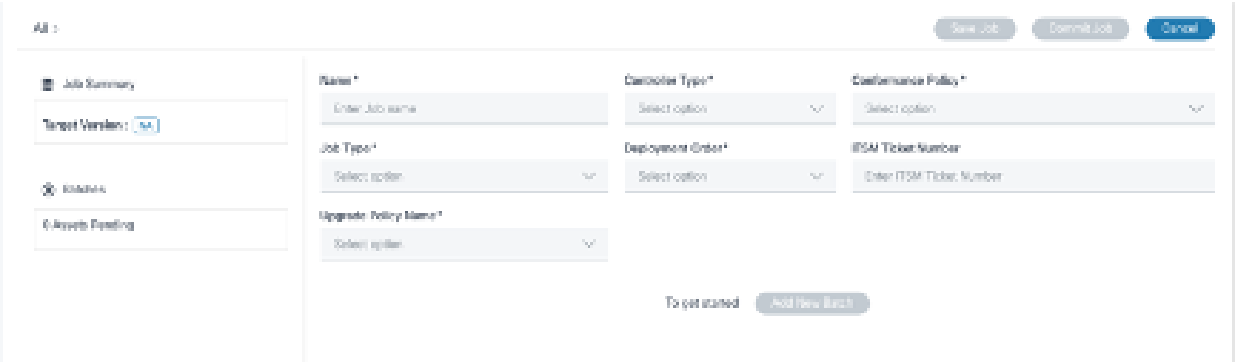
Programación de trabajos de actualización

Para crear un trabajo:




Opción Crear trabajo de actualización

1. En la página Upgrade Job, seleccione el icono More Options > Create Job. Se muestra la página Create Upgrade Job.



Crear trabajo de actualización

2. Introduzca un nombre de trabajo en el campo Nombre.
3. Seleccione el tipo de controlador (por ejemplo, Cisco Catalyst Center, vManage, NDFC, Direct-to-Device, CNC, FMC, ANSIBLE o NSO).
4. Seleccione una política de conformidad que tenga dispositivos no conformes.

---

Nota: Solo las políticas de conformidad que se ejecutan al menos una vez y tienen al menos un dispositivo no conforme están disponibles en la lista, identificando automáticamente la política de actualización aplicable que se utilizará una vez que se seleccione una política.

---

Los siguientes detalles se muestran en el lado izquierdo del formulario Crear trabajo en Resumen del trabajo:

- Modelos de dispositivo afectados

---

✎ Nota: Se muestran varios modelos de dispositivos cuando la directiva de conformidad seleccionada tiene más de un modelo de dispositivo asociado.

---

- Versión de destino
- Agregado de versiones de lanzamiento existentes y su recuento correspondiente
- Número máximo de lotes permitidos
- Número total de activos no conformes

---

✎ Nota: Si la política de conformidad seleccionada está asociada a varios modelos de dispositivo, muestra la suma de los activos no conformes para todos los modelos asociados.

---

- Opción para agregar lote

5. Seleccione uno de los siguientes tipos de trabajo de actualización:

- Distribución: Los trabajos solo de distribución son útiles cuando el desarrollo de la imagen del software ocurre antes de la activación real
- Activación: Los trabajos de solo activación son útiles para realizar actualizaciones de dispositivos para los que la distribución ya se ha completado mediante un trabajo de solo distribución
- Distribución y activación: Tanto la distribución de imágenes como el montaje y la activación se producen en el mismo trabajo, lo que resulta útil en situaciones en las que hay disponible una amplia ventana de mantenimiento para cubrir tanto la copia de imágenes en un dispositivo como la actualización

6. Seleccione el pedido de actualización. Varios dispositivos se procesan al mismo tiempo en el modo paralelo mientras que los dispositivos se procesan uno por uno en el modo secuencial.

---

✎ Nota: El número máximo de dispositivos que se pueden procesar en modo paralelo depende de la configuración de la implementación. El pedido de actualización seleccionado es aplicable para todo el trabajo, pero se puede sustituir dentro de un lote concreto en función de las necesidades.

---

7. Agregue el número de solicitud de cambio en el campo Número de notificación de ITSM (Administración de servicios de TI).
8. Seleccione el Nombre de la Política de Upgrade. Solo se muestran las políticas de actualización aplicables según el tipo de controlador y el modelo de dispositivo de la política

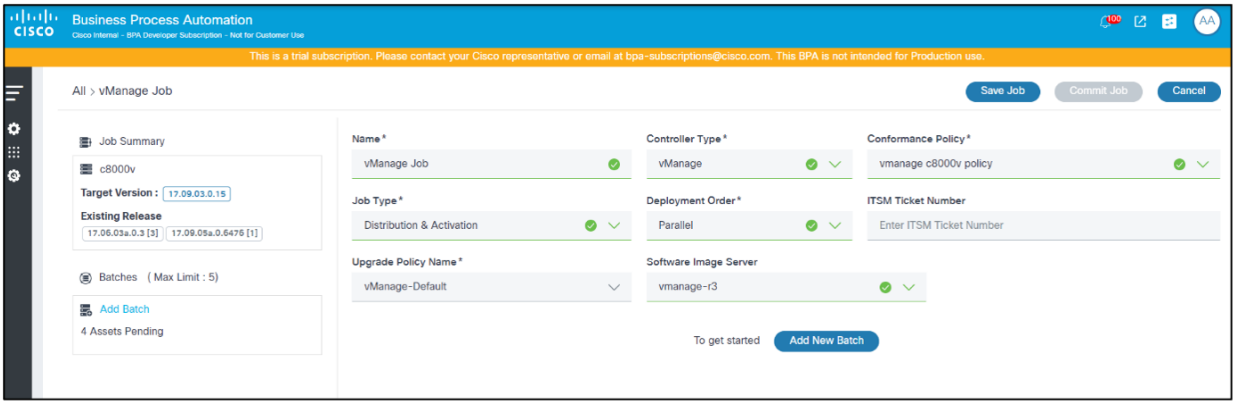
de conformidad; los usuarios pueden seleccionar una de las directivas de actualización. Si la política de conformidad del software tiene más de un modelo asociado, se mostrarán todas las políticas de actualización relevantes asociadas a cada modelo. Los usuarios deben seleccionar cuidadosamente la política de actualización que funciona para todos los modelos.

9. Seleccione Software Image Server para especificar qué repositorio de imágenes de vManage (por ejemplo, local o remoto) se utiliza.

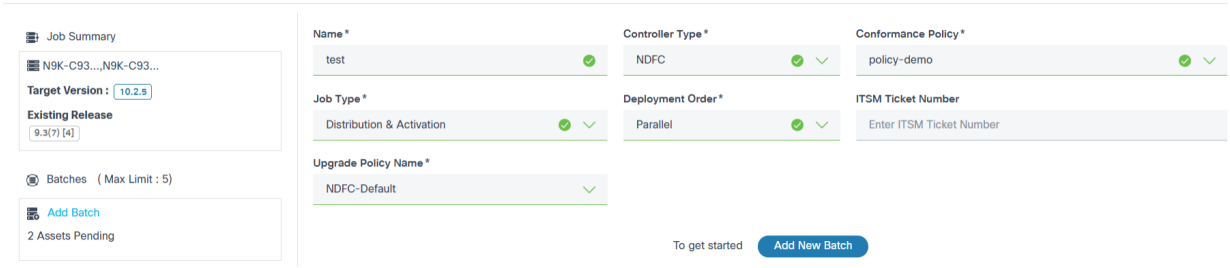
---

Nota: Esta entrada solo se aplica al tipo de controlador vManage.

---

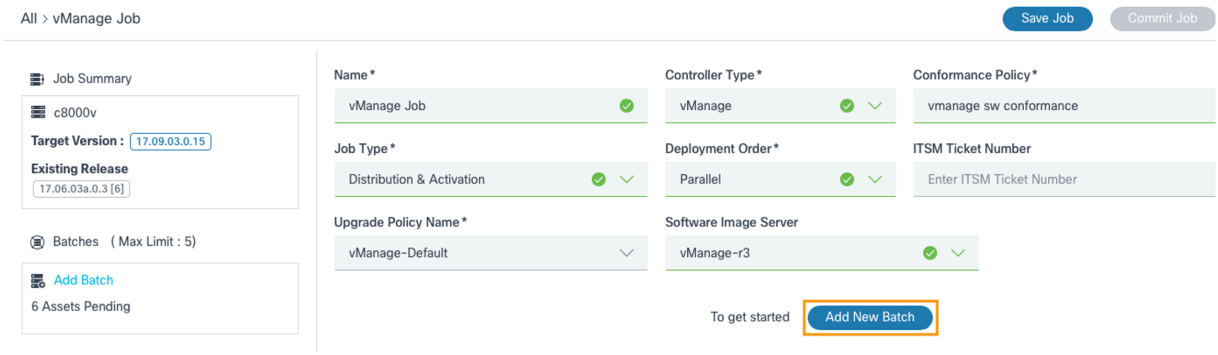



Crear trabajo de actualización con los detalles rellenos (la política de conformidad tiene un modelo)



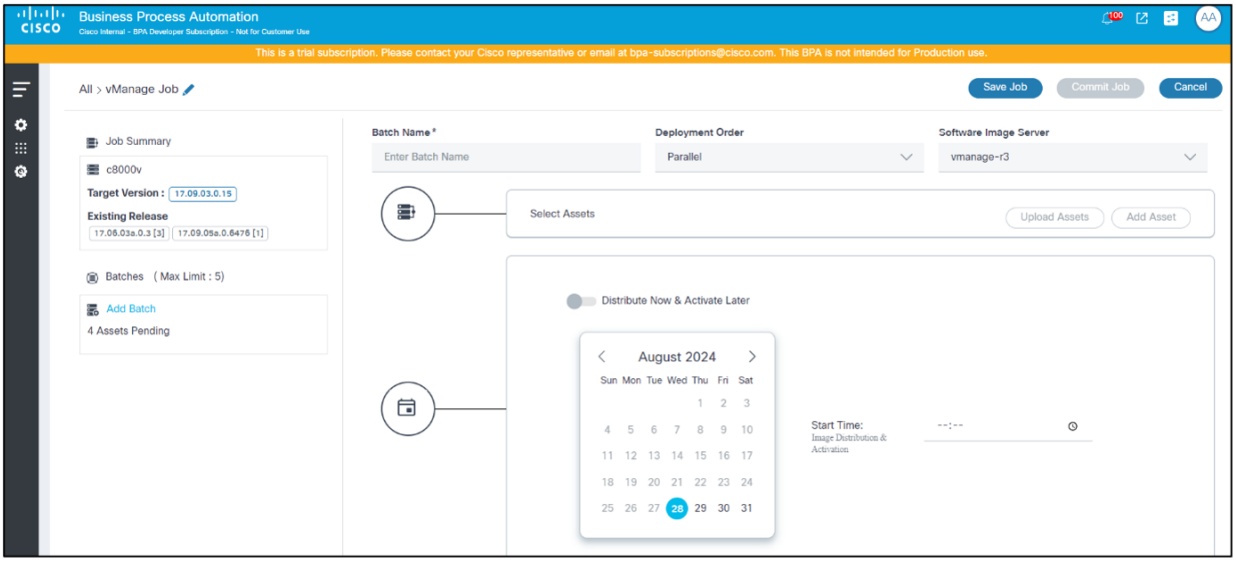

Crear trabajo de actualización con los detalles rellenos (la política de conformidad tiene varios modelos)

10. Haga clic en Save Job para guardar el borrador hasta que el trabajo esté listo para ser confirmado.




Agregar lote y Agregar nuevo lote

11. Para agregar un lote, haga clic en el enlace Agregar lote o en Agregar nuevo lote. Se abre la ventana Creación de lote.




Creación por lotes

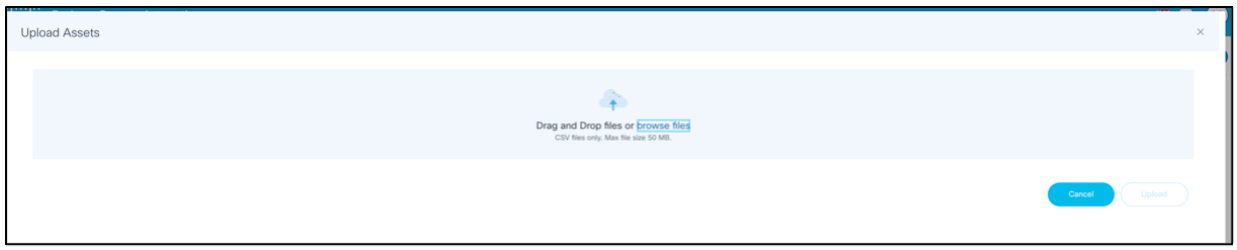
12. Introduzca un nombre de lote relevante y seleccione el pedido de implementación.

Nota: El tipo de actualización seleccionado aquí tiene prioridad sobre el seleccionado en la página Creación de trabajo

13. Seleccione Software Image Server para especificar qué repositorio de vManage (por ejemplo, local o remoto) se utiliza.

Nota: Este campo solo se aplica al tipo de controlador vManage. El Software Image Server seleccionado aquí tiene prioridad sobre el seleccionado en la página Job Creation

14. Añada activos a los lotes. Los activos se pueden añadir a los lotes de dos formas:




Cargar recursos

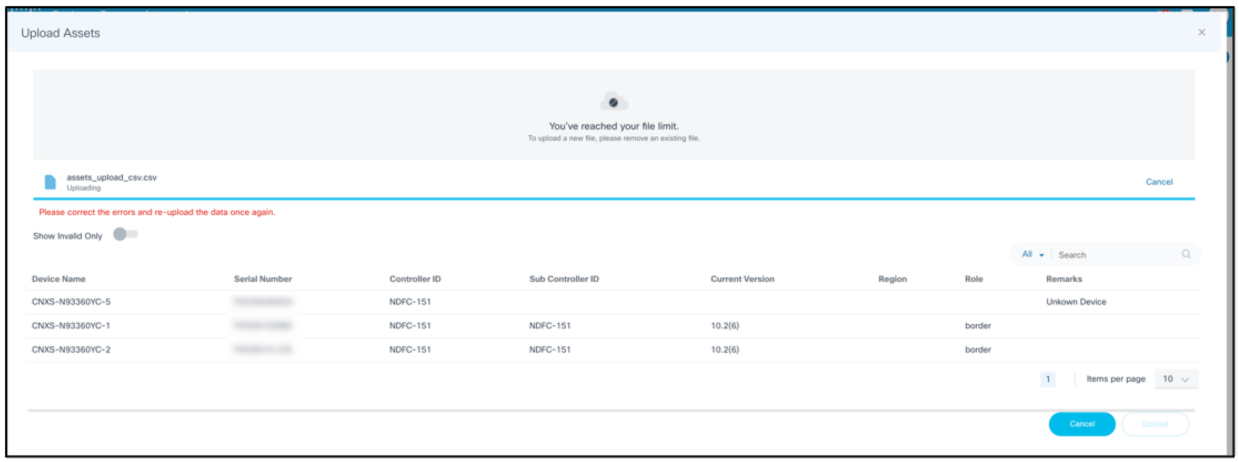
Opción 1:

a. Haga clic en Cargar recursos. Se abre la ventana Cargar activos.
b. Seleccione un archivo .csv para cargarlo.

Nota: El archivo .csv debe tener los siguientes detalles:

- Nombre del dispositivo: Nombre del dispositivo o recurso
- Serial Number: Número de serie del dispositivo
- ID de controlador: Nombre del controlador que administra el dispositivo
- ID de subcontrolador: Nombre del ID del subcontrolador que administra el dispositivo

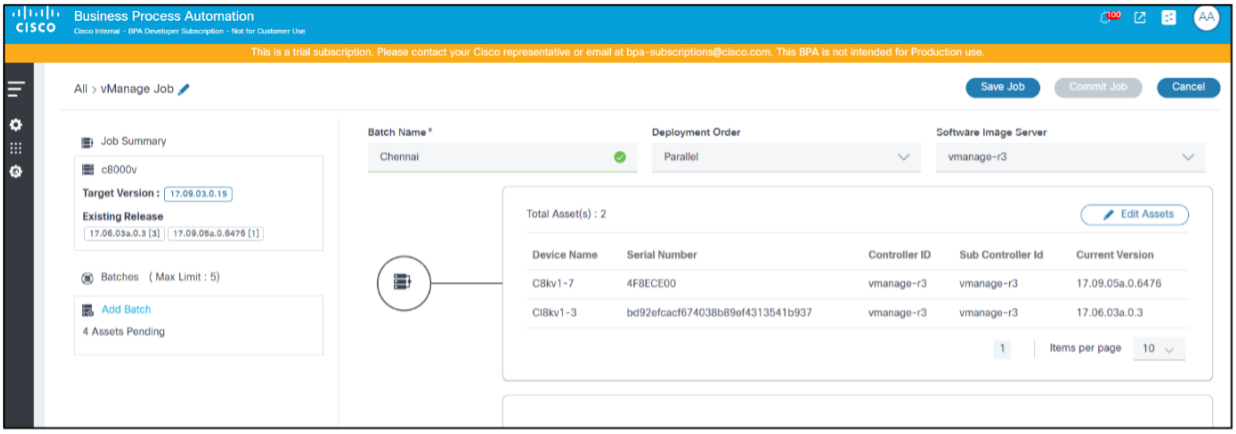
c. Haga clic en Cargar. Se validan los datos del archivo .csv y se muestran tanto los datos válidos como los no válidos. El botón Show Invalid Only se puede utilizar para filtrar los dispositivos no válidos a partir de los detalles de los activos cargados.




Recursos de ejemplo cargados mediante un archivo CSV

d. Si hay errores en el archivo cargado, corríjalos y vuelva a cargarlo.

Nota: Los usuarios solo pueden continuar con la selección de recursos si todos los dispositivos cargados son válidos.




Agregar lote - Activos seleccionados

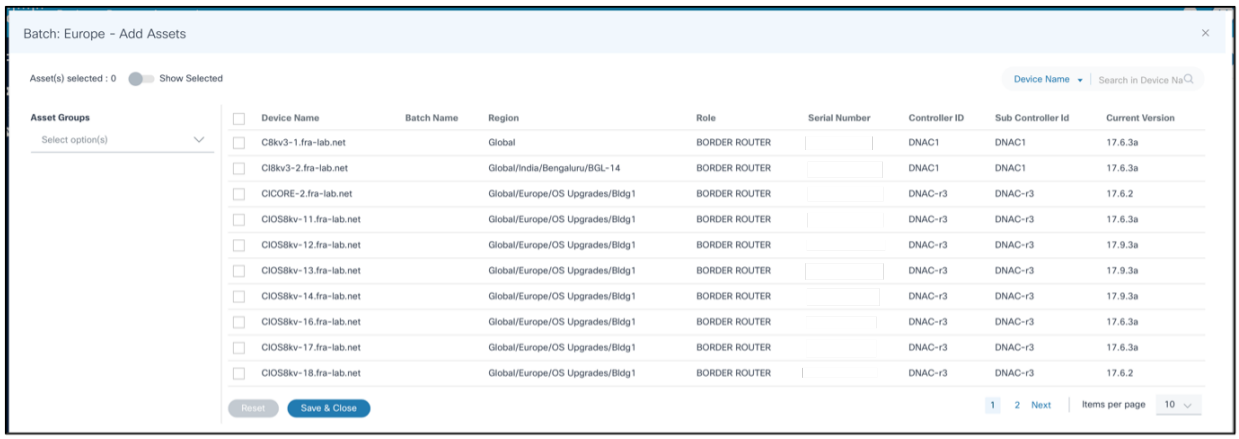
Opción 2:

a. Haga clic en Agregar activos. Se abre la ventana Selección de activos.

Nota: Cargar recursos y Add Assets no se pueden utilizar al mismo tiempo.

b. Para el tipo de controlador FMC únicamente, seleccione el nodo de control o el nodo independiente para realizar la actualización.

Nota: No se permiten dispositivos de datos en el trabajo de actualización porque el nodo de control controla la actualización de los nodos de datos.




Selección de dispositivos

c. Seleccione el dispositivo o dispositivos adecuados para incluirlos en el lote actual.

El filtro Search se puede utilizar para filtrar dispositivos en función de diferentes atributos y todos los dispositivos que coincidan con los criterios de filtrado se pueden seleccionar de forma masiva activando la casilla de verificación del encabezado de columna Device Name. Los usuarios

también tienen la opción de filtrar por grupos de activos.

La opción Mostrar seleccionados se puede habilitar para ver sólo los activos seleccionados.

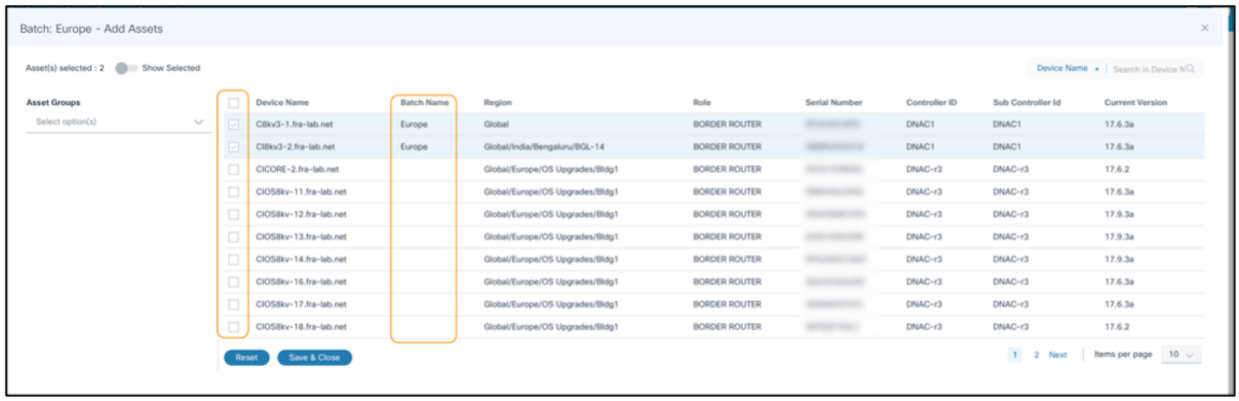
---

Nota: Cuando la opción Mostrar seleccionados está habilitada, el filtro Grupos de activos está deshabilitado.

---

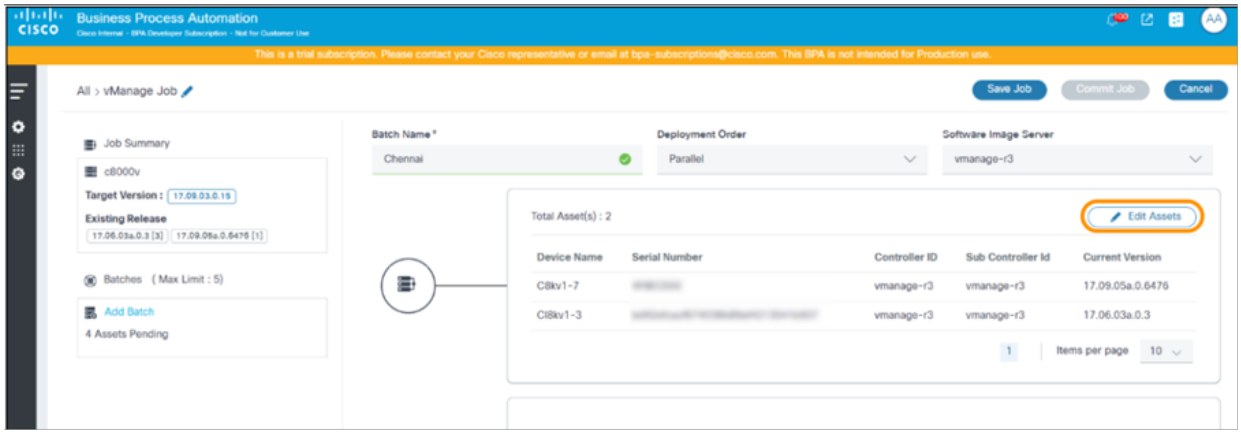
d. Haga clic en Guardar y cerrar.

Al hacer clic en Restablecer, se descartan las selecciones y se conserva el estado original de la selección de activos.



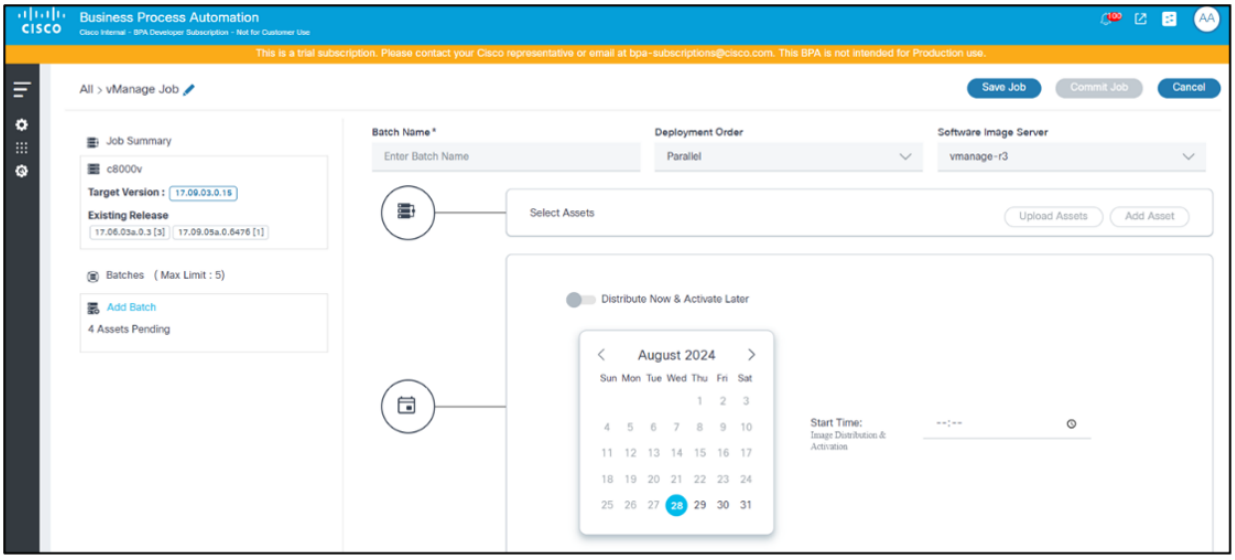

Reiniciar

e. Si es necesario modificar la selección de activos, haga clic en Editar activos.




Edición por lotes de activos

f. Seleccione o borre activos para realizar los cambios necesarios y haga clic en Guardar y cerrar. Al editar los activos del lote, los activos seleccionados actualmente que forman parte de un trabajo y lote diferentes se pueden identificar mediante marcas de verificación y el nombre del lote mostrado en la columna Nombre del Lote.




Actualizar Job Scheduler

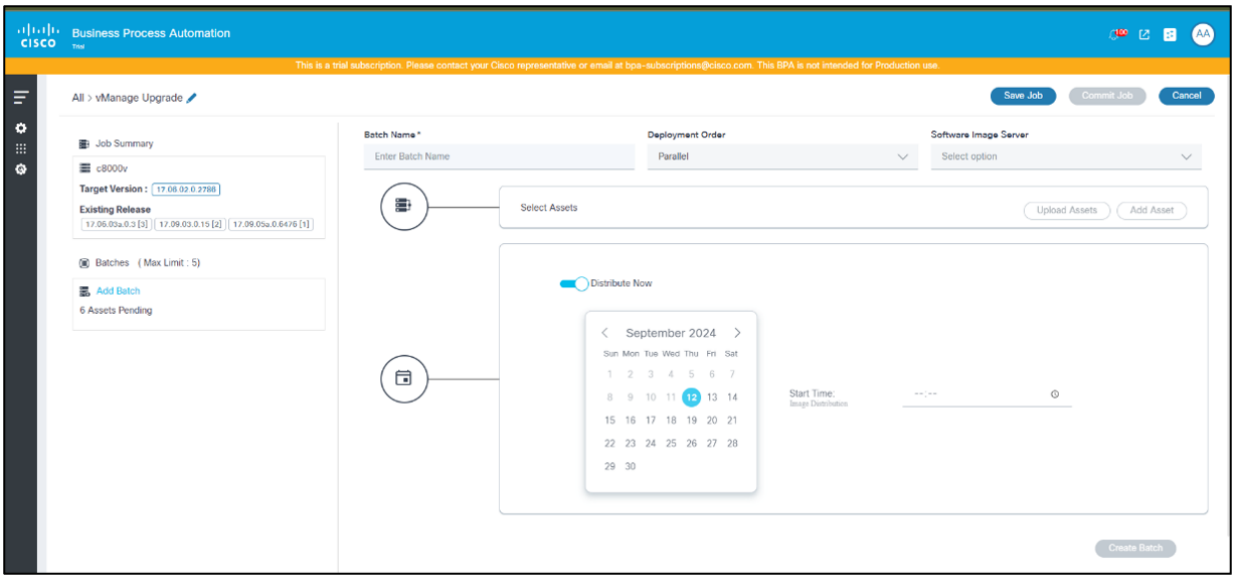
15. Seleccione una fecha del selector de fecha y una hora del selector de hora para programar una hora para activar el tipo de actualización seleccionado para el lote actual.

Nota: El tipo de trabajo seleccionado cambia el tipo de programaciones disponibles.

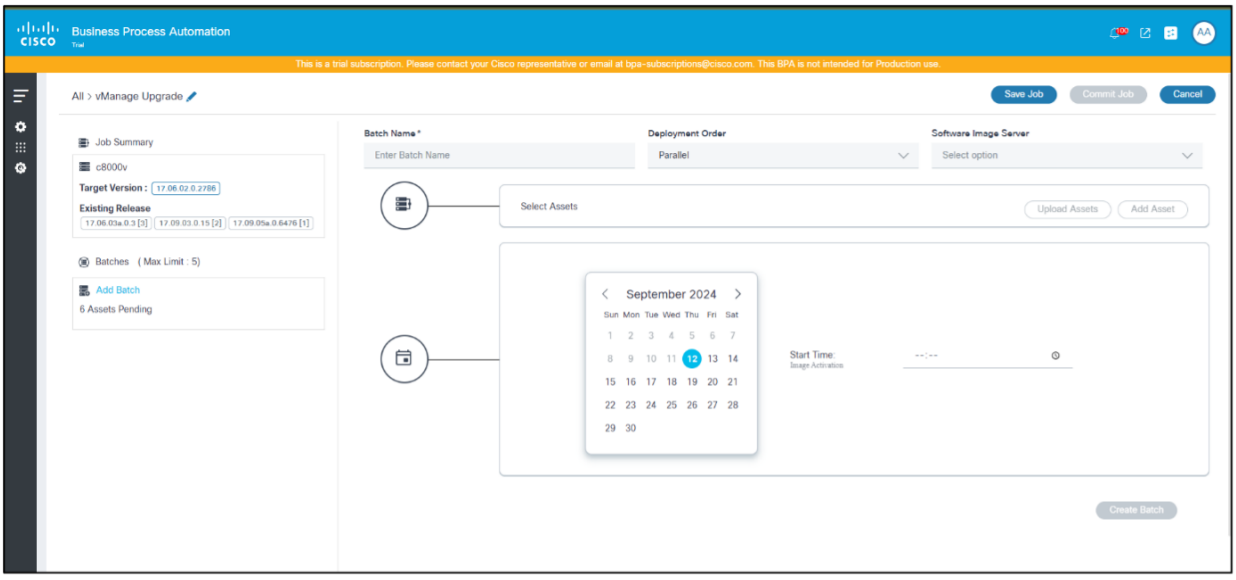
Los escenarios posibles son los siguientes:

| Tipo de trabajo | Distribuir ahora Alternar | Fecha y hora de programación | Detalles de distribución |
|---|---|---|---|
| Distribución | Desactivado de forma predeterminada | Activo | La distribución tiene lugar en la fecha y hora programadas especificadas |
| Distribución | Habilitado | Inhabilitado | La distribución se produce después de confirmar el trabajo |
| Activación | N/A | Activo | La activación tiene lugar en la fecha y hora especificadas |
| Distribución y activación | Desactivado de forma predeterminada | Activo | La distribución y activación se produce en la fecha y hora especificadas |
| Distribución y activación | Habilitado | Activo | La distribución se produce después de la confirmación del trabajo |

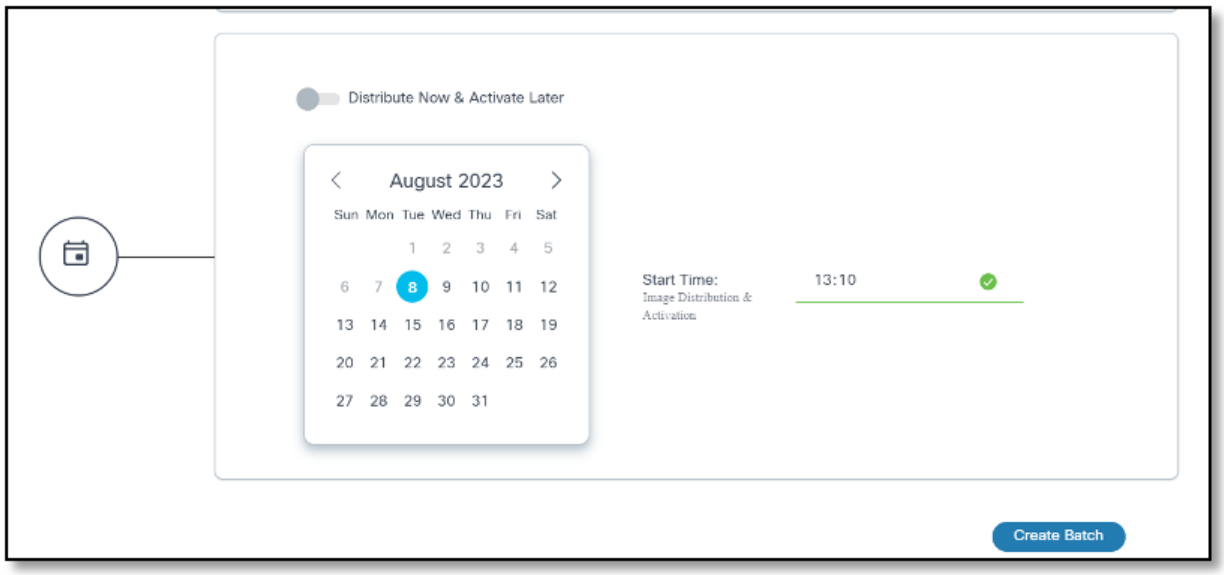
| Tipo de trabajo | Distribuir ahora Alternar | Fecha y hora de programación | Detalles de distribución y los desencadenadores de activación en la fecha y hora programadas especificadas |
| --- | --- | --- | --- |



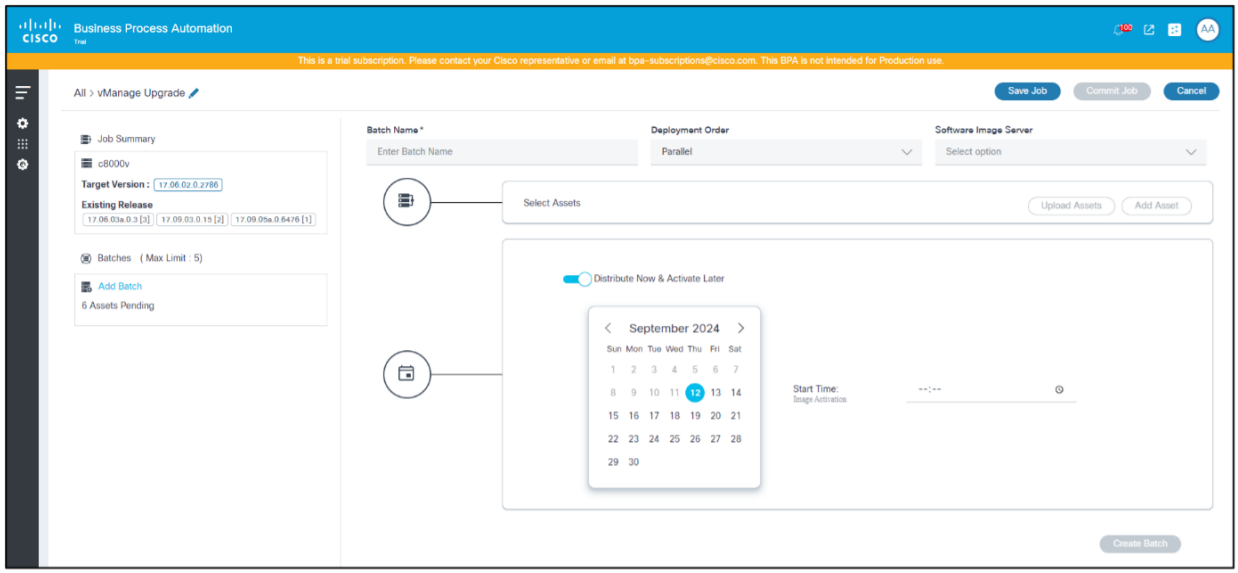

Opciones de programación de tipo de trabajo de distribución




Opciones de programación de tipo de trabajo de activación




Opciones de programación de tipo de trabajo de distribución y activación

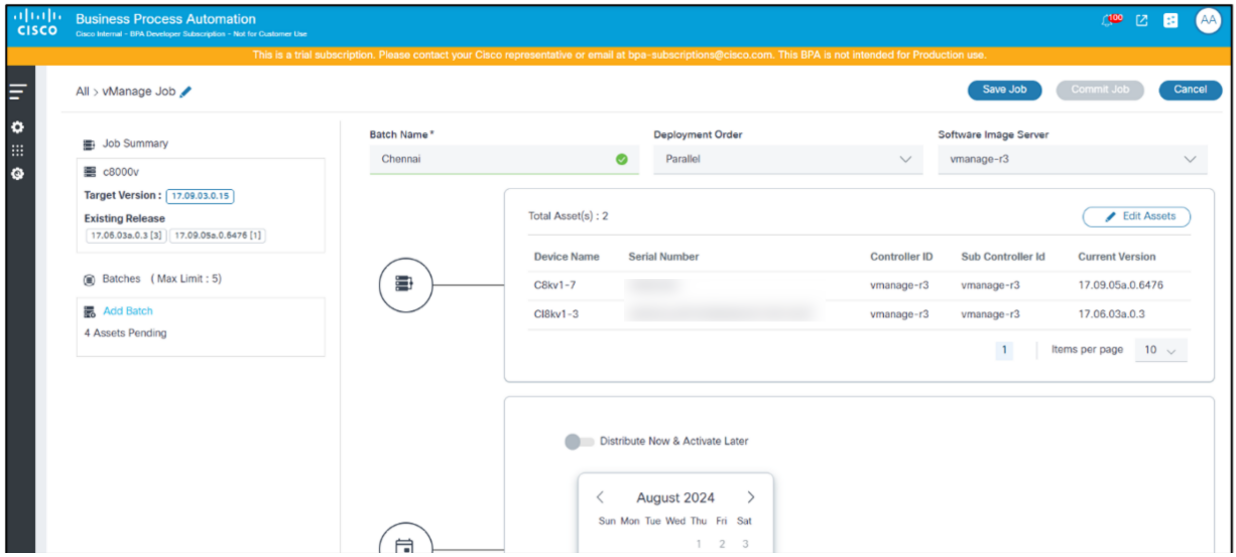



Opciones de programación de tipo de trabajo de distribución y activación con la opción Distribuir ahora y Activar más tarde activada

Nota: Debe tenerse en cuenta la siguiente lista.

- Al programar varios lotes, proporcione un intervalo de tiempo entre los dos lotes para evitar la sobrecarga del sistema. Si se solapan varios lotes, considere la posibilidad de agregarlos a un solo lote.
- Cuando la opción Distribuir ahora y Activar más tarde esté habilitada, proporcione un intervalo de tiempo entre el tiempo de confirmación del trabajo y la programación de activación. De lo contrario, los flujos de trabajo de activación podrían crear tareas de usuario que requieren intervención manual (es decir, los usuarios deben esperar hasta que se complete la distribución y volver a intentarlo).

16. Haga clic en Create Batch. El lote se puede ver en el lado izquierdo de la página.



Crear trabajo: confirmar trabajo

Cree tantos lotes como sea necesario. Un trabajo puede estar en estado Borrador hasta que toda la información necesaria esté disponible.

---

Nota: Para evitar la pérdida de datos del trabajo, haga clic en Guardar trabajo para guardar el borrador.

---

17. Haga clic en Confirmar trabajo para finalizar la creación del trabajo. El trabajo pasa al estado Desplegar cuando se activa la planificación para cualquiera de los lotes.

---

Nota: El umbral para el número máximo de lotes se puede ampliar o actualizar en la página Política de Upgrade.

---

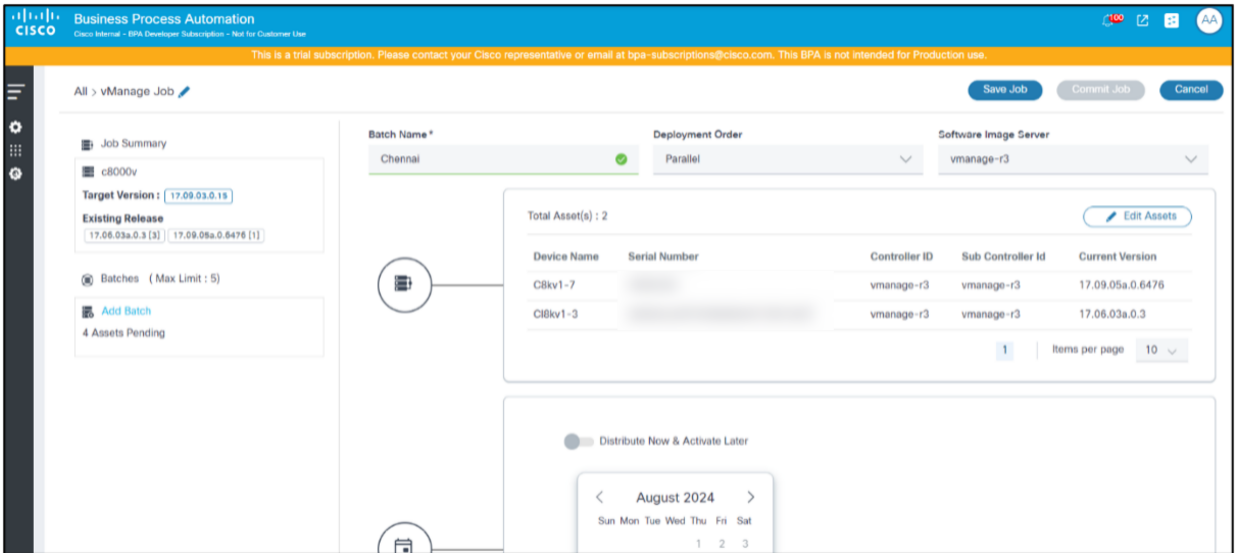
Edición de un lote en un trabajo

---

Nota: Los lotes sólo se pueden actualizar cuando el trabajo se encuentra en la fase Borrador.

---

1. Seleccione el lote deseado en el panel izquierdo.

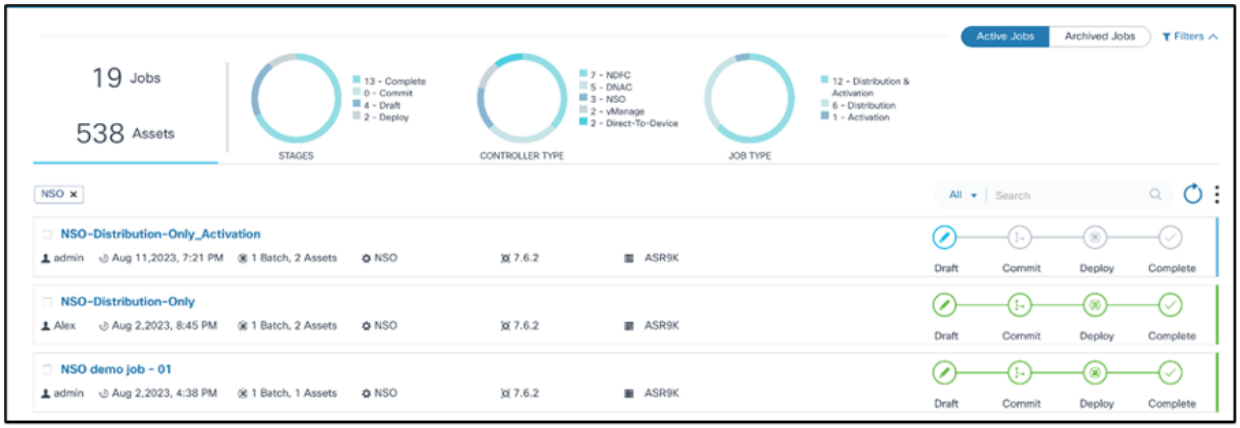



Editar recursos

2. Haga clic en Editar recursos.
3. Realice los cambios necesarios seleccionando o conciliando activos en Añadir activos o Cargar activos o modificando la programación del lote realizando cambios en la fecha o la Hora de inicio.
4. Haga clic en Update Batch.

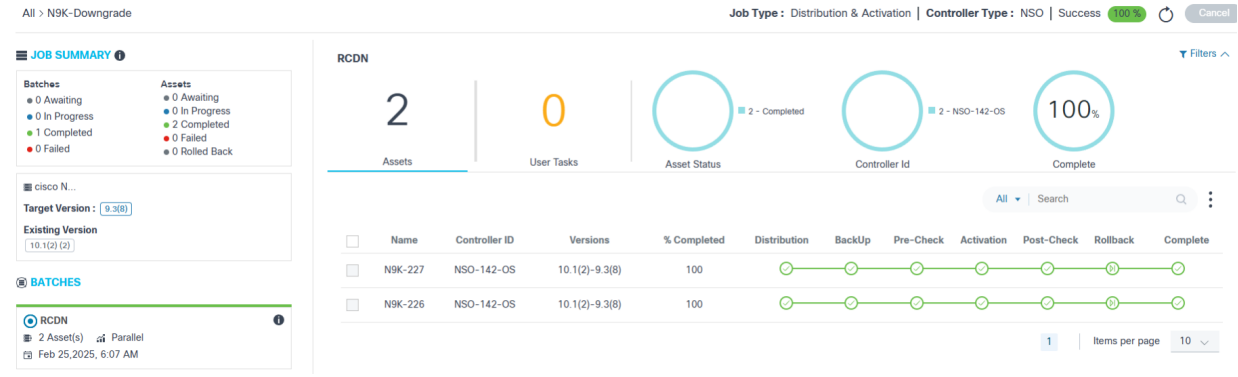
Ejecución de tareas de actualización y supervisión de progreso

1. Inicie sesión en BPA con credenciales que tengan acceso a los trabajos de actualización.
2. Seleccione OS Upgrade > Upgrade Jobs. Se muestra la página Upgrade Job.

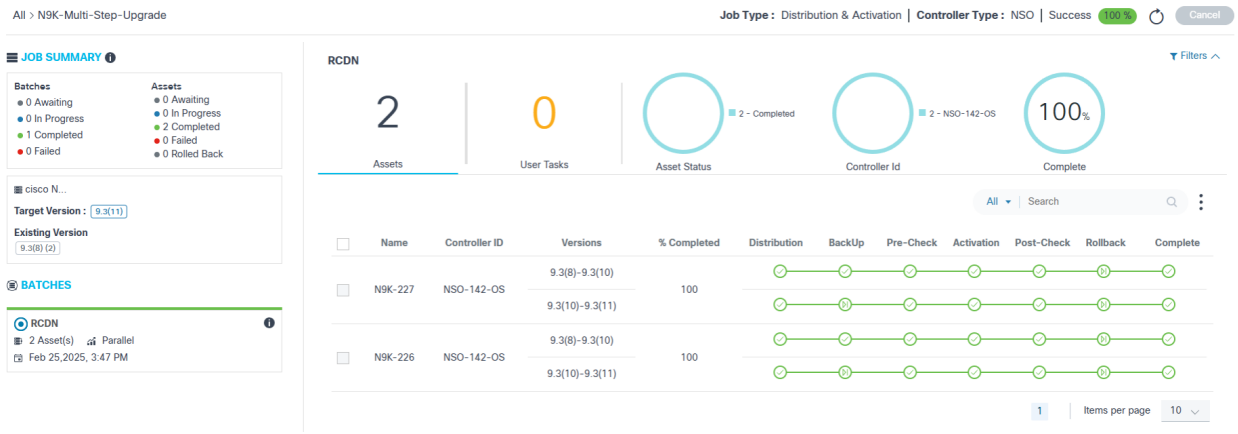



Tarea de actualización

3. Utilice el filtro Buscar en combinación con los filtros de gráfico disponibles para filtrar rápidamente el trabajo.
4. Haga clic en el trabajo deseado. Se muestra la página Resumen del trabajo.

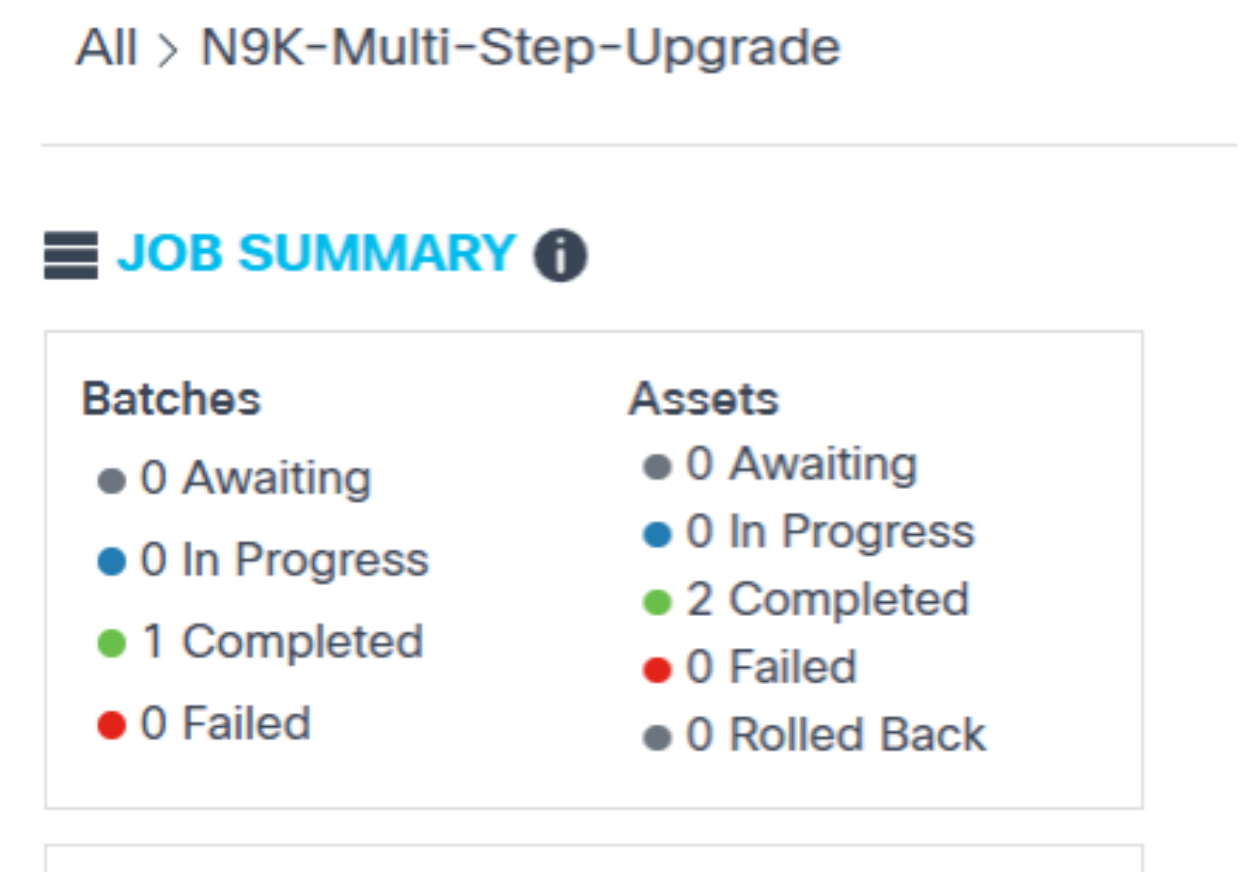



Actualización en un solo paso




Actualización en varios pasos

El panel izquierdo proporciona la siguiente información:



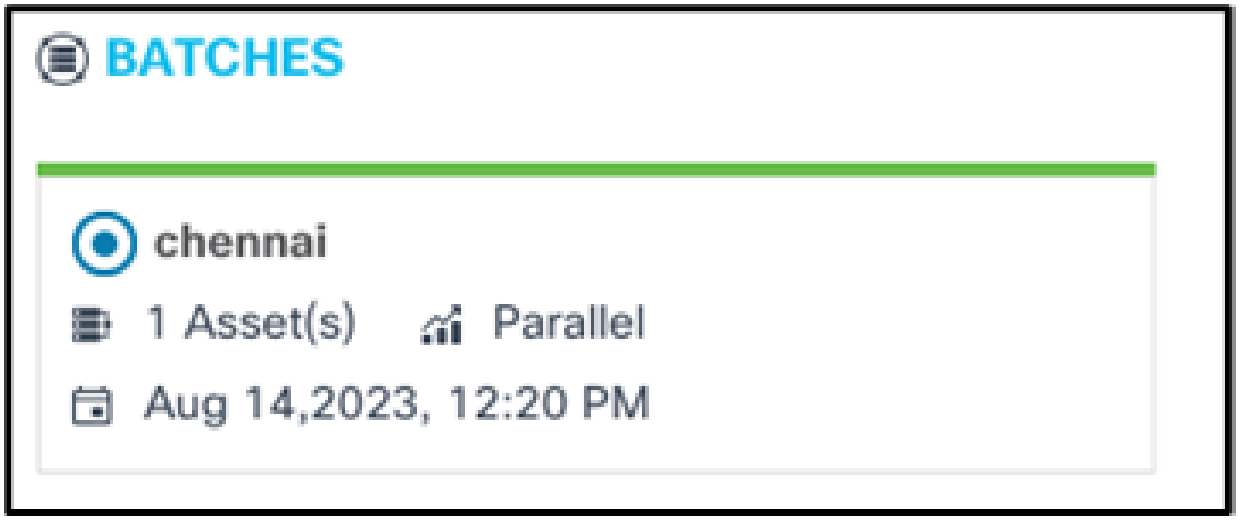

Resumen del trabajo

- Un rápido resumen de los lotes y los activos correspondientes


Detalles de la política de conformidad (si la política tiene un modelo)


Detalles de la política de conformidad (si la política tiene varios modelos)

- Modelo de dispositivo afectado del trabajo, versión de software de destino y versión de versión existente
- Una lista de lotes que forman parte de este trabajo




Detalles del lote

- Detalles del lote:
    - El borde superior gris indica que el lote está esperando la programación
    - El borde superior azul indica que la implementación por lotes está en curso
    - El borde superior verde indica que la implementación por lotes ha finalizado

La siguiente información se muestra en la parte superior de la página Resumen de trabajos:


Parte superior del resumen del trabajo

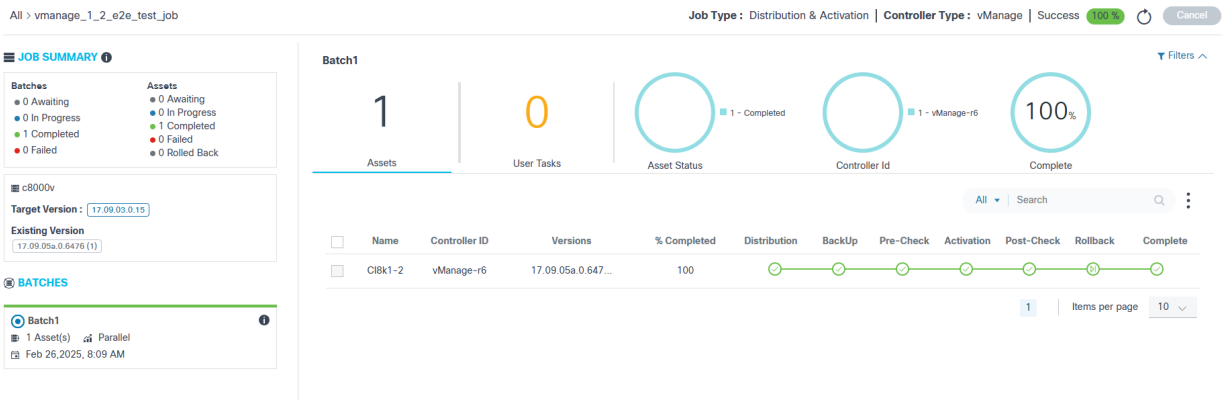
- Navegación de contenido del trabajo actual (por ejemplo, Todos > vmanage_1_2_e2e). La opción All cambia al panel de trabajos
- El tipo de trabajo
- El tipo de controlador
- Estado del trabajo con porcentaje completado:
    - Éxito: El trabajo de actualización se ha realizado correctamente
    - Error: El trabajo de actualización ha fallado por algún motivo
    - En curso: El trabajo de actualización está en curso

---

Nota: El estado del trabajo pasa a En curso aunque se alcance la programación de un lote

---

- Esperando: El trabajo se ha confirmado, pero está a la espera de que se alcance una o varias programaciones de lotes




Resumen del trabajo

Las siguientes opciones están disponibles en la página Resumen del trabajo:

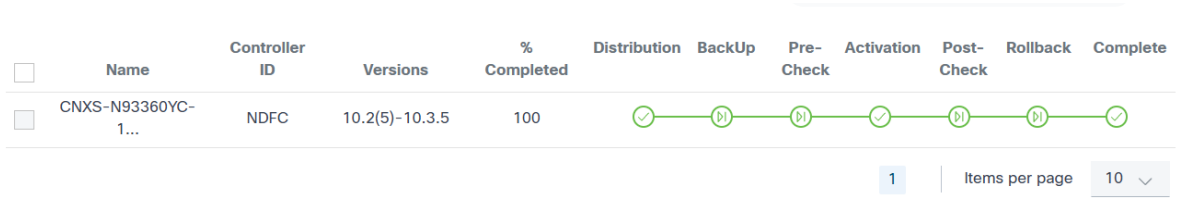
- El icono Refresh permite a los usuarios recuperar actualizaciones a petición
- Cancelar se utiliza para cancelar los trabajos en las fases Borrador y Confirmar a menos que se alcance la programación de cualquiera de los lotes
- Activar crea un nuevo trabajo de activación en el estado Borrador con los mismos lotes y activos que formaban parte del trabajo finalizado anteriormente
    - Activar sólo está disponible si el tipo de trabajo es Distribución y se ha completado correctamente
    - Si el trabajo de activación ya está creado y se hace clic en Activar, se muestra un mensaje con el estado del trabajo creado anteriormente y proporciona una opción para redirigir el trabajo ya creado; en el trabajo recién creado, los usuarios tienen la opción de editar o eliminar los lotes o activos, pero el tipo de trabajo, el tipo de controlador y la directiva de conformidad no se pueden editar.
- Debajo de la sección de análisis se muestra una lista paginada de recursos
- El campo Buscar permite realizar búsquedas generales y específicas de campos para

columnas como:

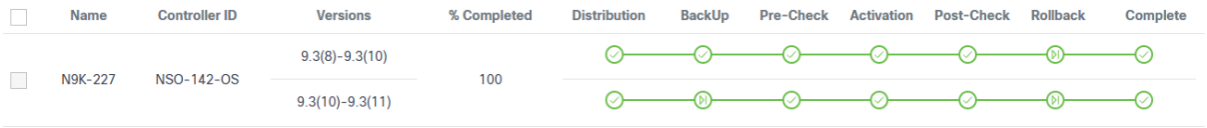
- Nombre del dispositivo
- ID del controlador
- Serial Number


Descargar informe de lotes

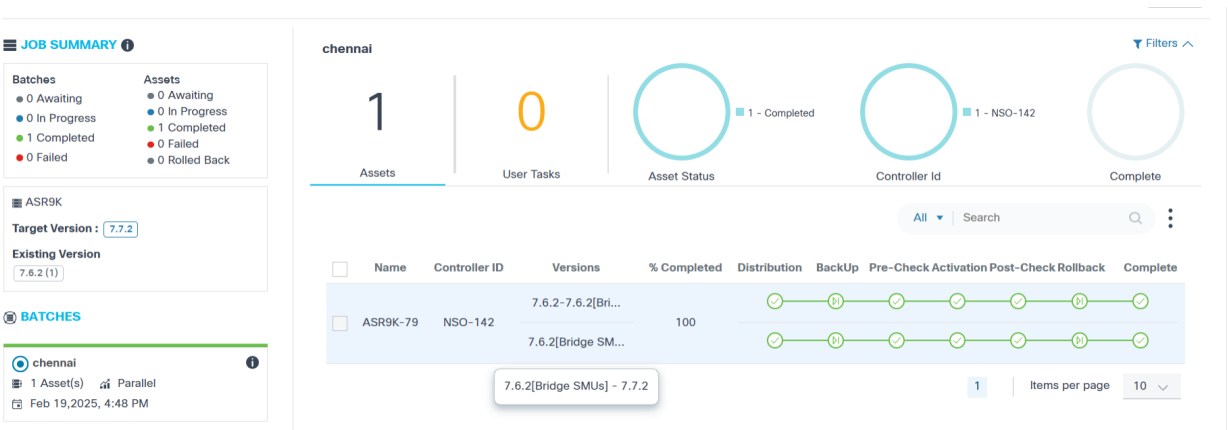
- La opción para descargar el informe de nivel de lote seleccionando el icono Más opciones > Descargar; el informe consta de los detalles de nivel de lote con los detalles del dispositivo




Ordenar: actualización en un solo paso




Ordenar: actualización en varios pasos




Ordenar - Actualización de Bridge SMU

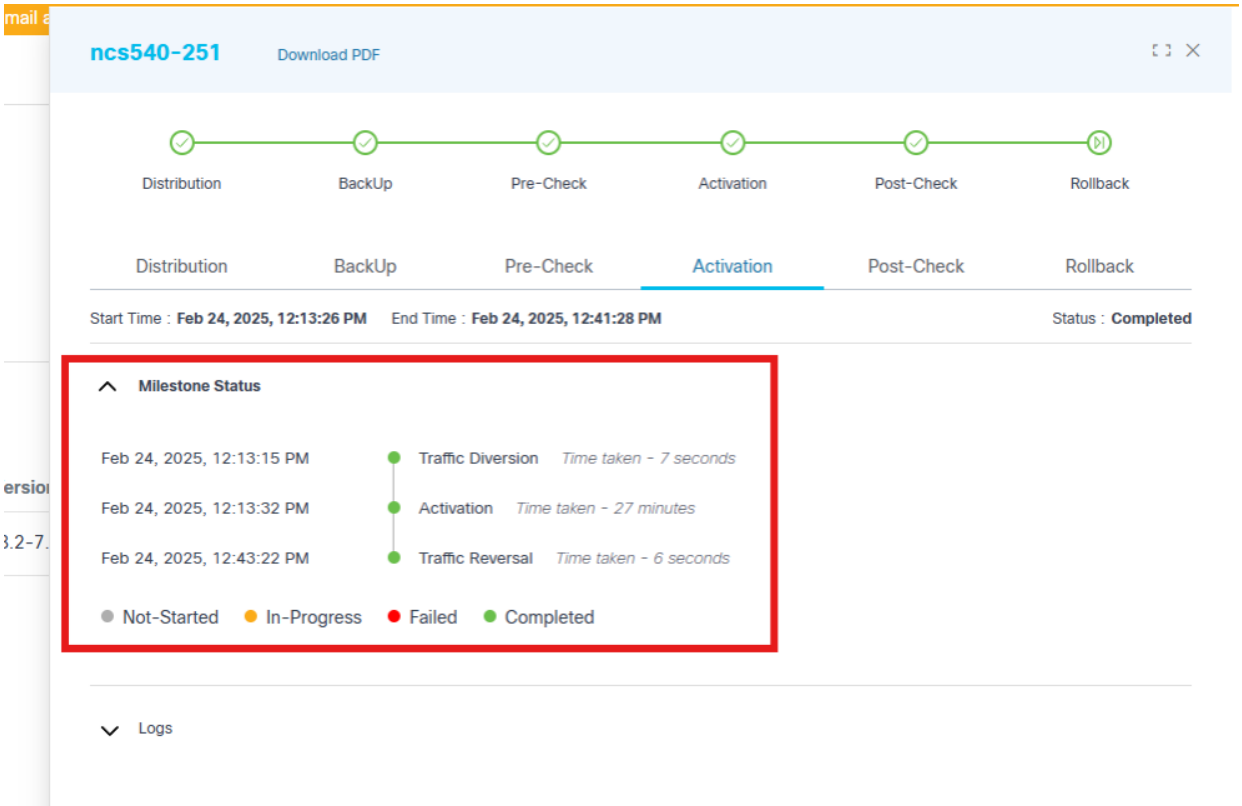
- La ordenación se puede realizar haciendo clic en los nombres de las columnas
- Se muestran los siguientes hitos de actualización para cada dispositivo junto con Name, Controller ID, Versions y % Completed:
    - Distribución
    - Respaldo
    - Comprobación previa
    - Tráfico-Desviación
    - Activación
    - Comprobación posterior
    - Traffic-Reversal
    - Rollback
    - Completo

---

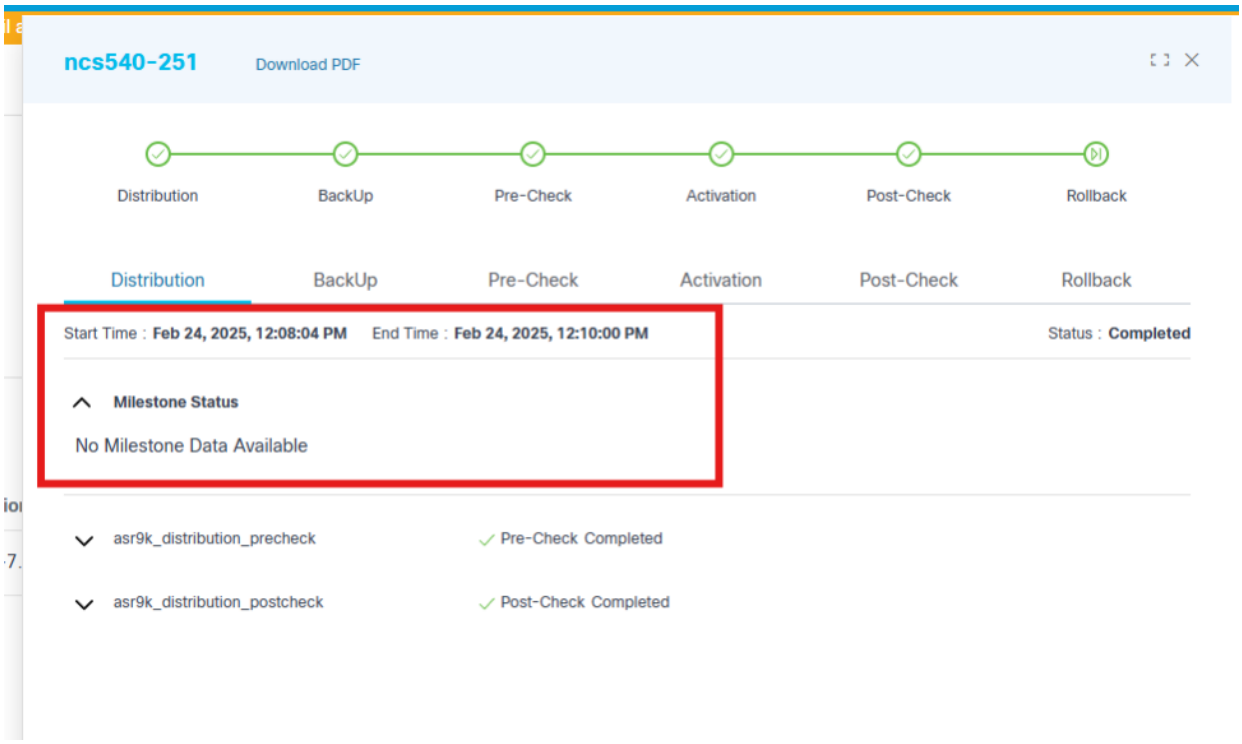
Nota: % completado muestra el progreso en función del número de hitos completados para un dispositivo. Todos los porcentajes de finalización a nivel de dispositivo dentro de un lote se agregan para calcular el porcentaje de finalización del lote. A su vez, todos los porcentajes de finalización de lotes se agregan para calcular el porcentaje de finalización de nivel de trabajo.

---

Los subhitos también conocidos como hitos personalizados son los pasos intermedios significativos que se ejecutan y ven bajo el hito estándar cuando se agregan. Para obtener más información sobre cómo agregar hitos personalizados, consulte la Guía del desarrollador de BPA.




Vista de subhitos (si los subhitos se agregan bajo el nombre de hito estándar)

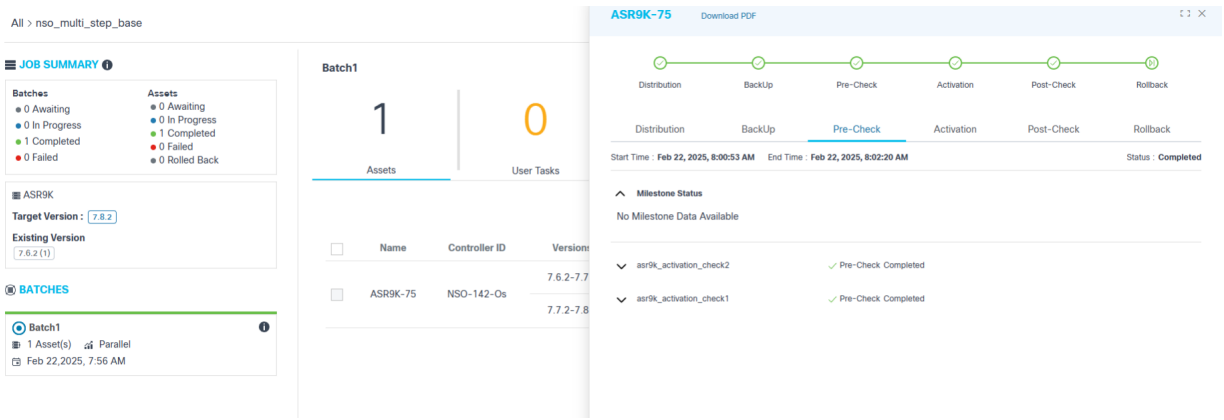



Vista de subhitos (si los subhitos no se agregan bajo el nombre de hito estándar)

Nota: Los hitos varían según el tipo de trabajo seleccionado. El hito TrafficReversal no está disponible para los trabajos de distribución.

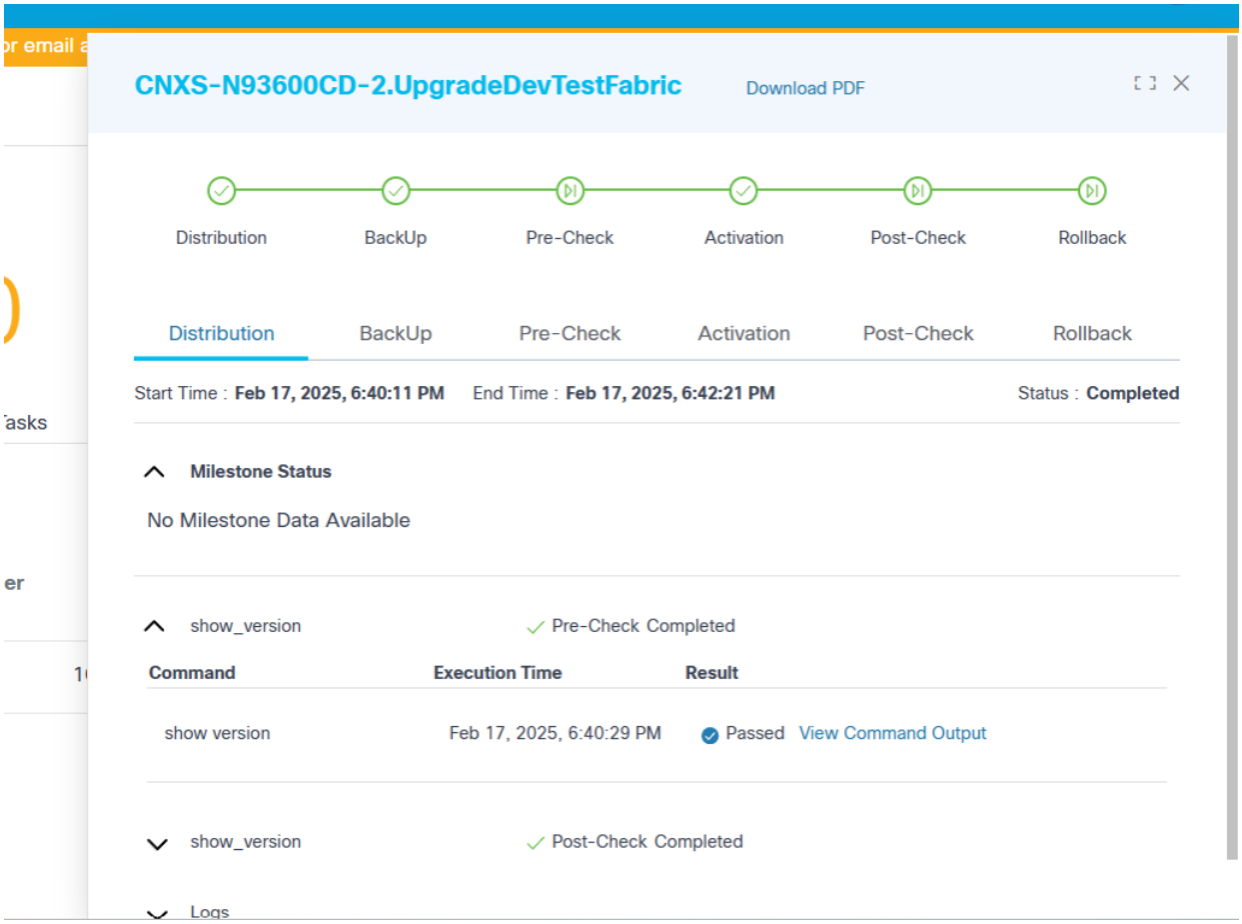
El desvío y la inversión del tráfico se mueven por debajo del hito de activación.

- Una leyenda de color de hito que consta de lo siguiente:
  - Cheque gris: Pendiente
  - Marca azul: En curso
  - Indicador verde: Omitido
  - Cheque verde: Completado
  - Cheque naranja: Tarea de usuario
  - Marca roja: Error



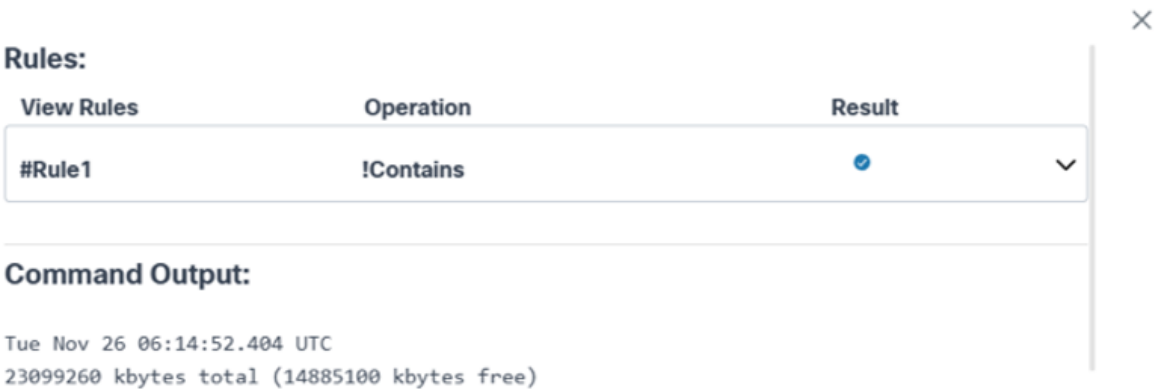

Vista de hitos previa y posterior a la comprobación

Para los hitos con ejecución previa o posterior a la comprobación, los usuarios pueden ver el resultado completo del comando junto con las reglas de validación y sus estados para todos los comandos configurados en la plantilla de proceso correspondiente.



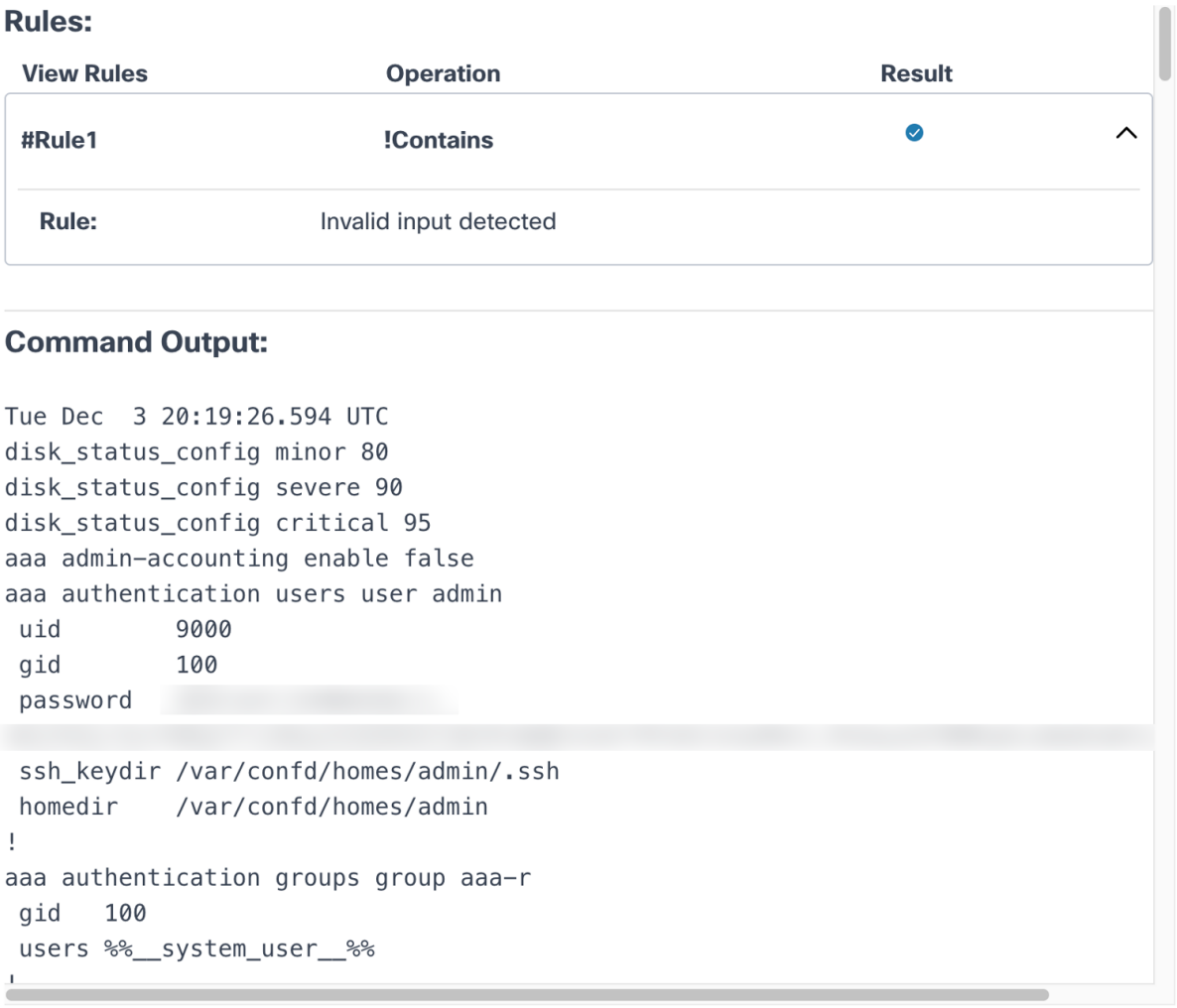

Vista de hito de distribución con resultado de comando de comprobación previa

1. Para ver el resultado del comando y las reglas asociadas con los comandos anteriores y posteriores a la comprobación, haga clic en el enlace Ver resultado del comando.

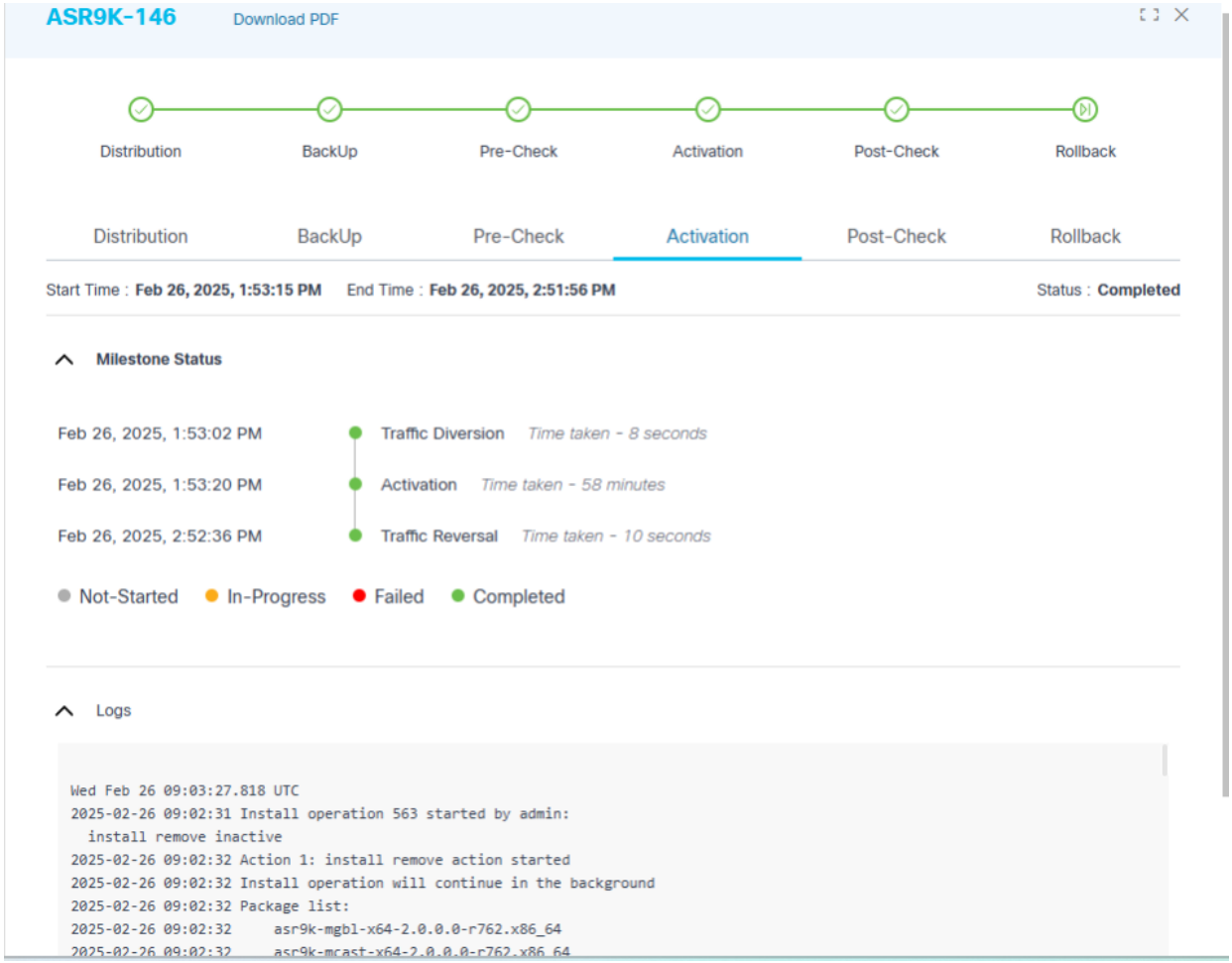



Resultado de los comandos de comprobación previa y posterior y reglas asociadas

2. Seleccione el icono Expandir para ver todos los detalles de cada regla.



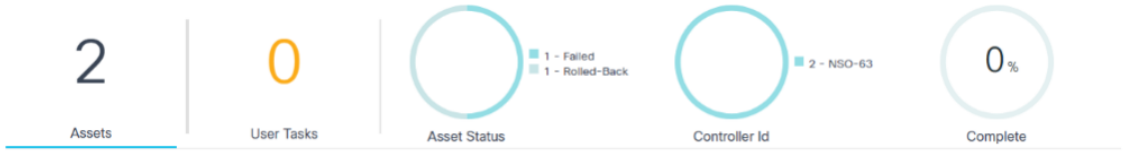

Resultado de los comandos de comprobación previa y posterior con reglas de validación




Vista de hito de activación con registros en directo

La figura anterior proporciona detalles del hito de activación, que incluye registros en vivo para ayudar a monitorear el progreso de la activación de software de un dispositivo en particular.

Cuando un hito se inicia o finaliza, al hacer clic en el hito se muestra más información.



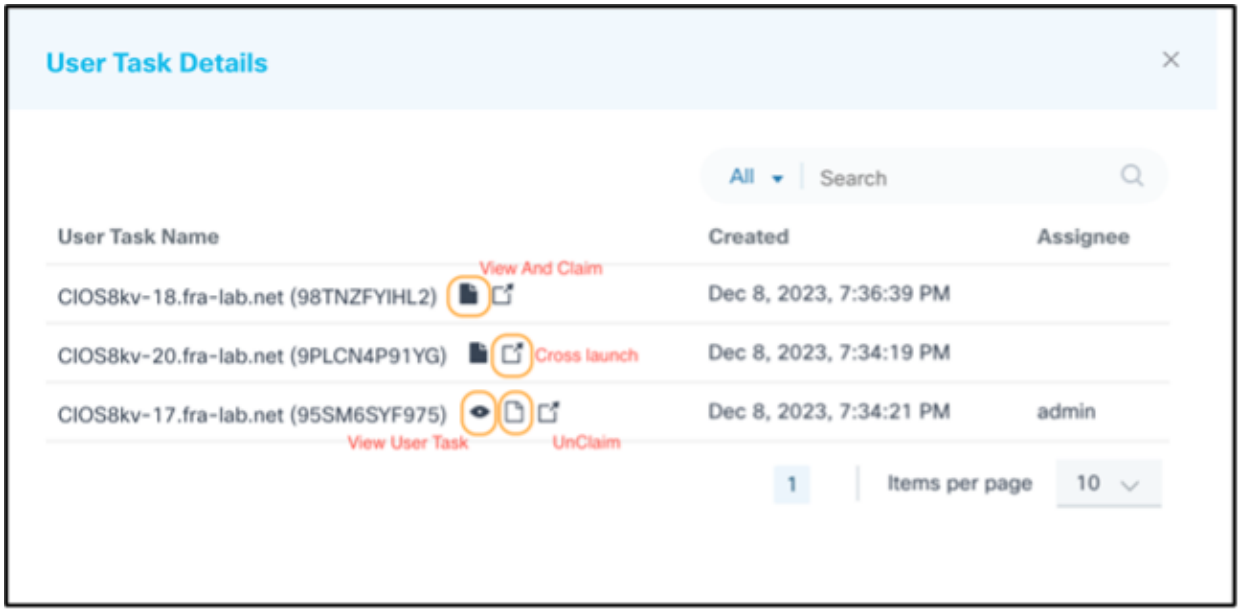

Sección Análisis

Una sección de análisis, que se muestra en la parte superior de la página Resumen de Trabajo, muestra la siguiente información relacionada con el trabajo seleccionado actualmente:

- El nombre del lote (p. ej., Asia)
- Filtra ^ contrae y expande la sección de análisis
- Los siguientes detalles del lote se muestran en orden:
    - Recursos: Número total de activos

- Tareas de usuario: Número total de tareas de usuario que esperan la entrada del usuario de operaciones o del administrador
- Estado del activo: Filtra los dispositivos por lotes según su estado. El filtro Rollback se ha agregado para ayudar a identificar los dispositivos que se han revertido correctamente.
- ID de controlador: Filtra los dispositivos por lotes que pertenecen a la ID del controlador seleccionado
- Completo: Porcentaje total de finalización del lote

Para actuar sobre cualquier tarea de usuario, haga clic en el número Tareas de usuario. La ventana Detalles de Tarea de Usuario se abre con lo siguiente:




Detalles de tarea de usuario

- Una lista de tareas de usuario que corresponden a los dispositivos respectivos que requieren atención
- Los siguientes iconos para las opciones de tareas de usuario:

  - Ver y reclamar: Ver los detalles de la tarea de usuario
  - Lanzamiento cruzado: Vea las tareas de flujo de trabajo de BPA en la interfaz de usuario clásica
  - Cancelar reclamación: Quitar la asignación de tarea de usuario
  - Ver tarea de usuario: Ver los detalles de la tarea de usuario


Tarea de usuario

Opción Ver de tarea de usuario

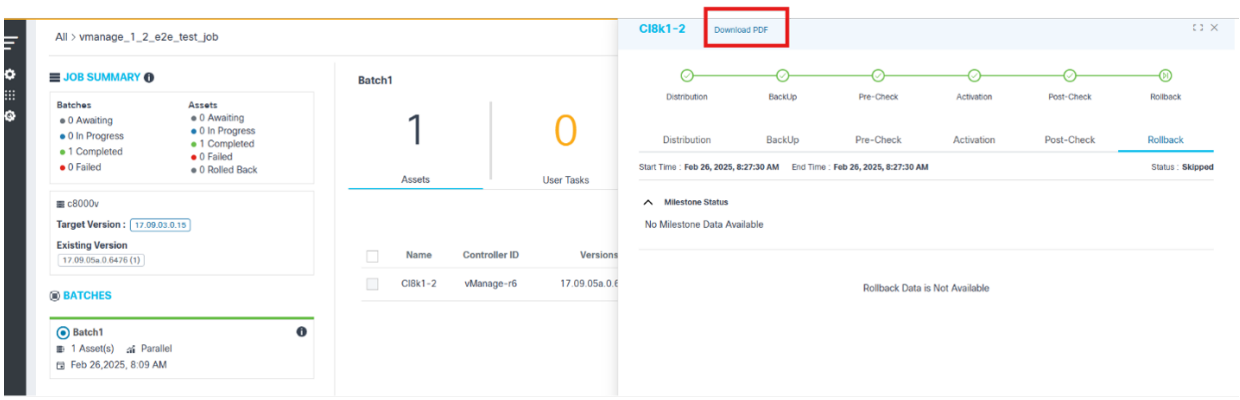
- Las siguientes opciones se muestran en función del contexto de la tarea:
    - Reintentar: Vuelve a ejecutar la tarea
    - Reintentar todo: Reejecuta todas las comprobaciones previas y posteriores
    - Continúe: Continúa con la siguiente tarea
    - Reversión: Vuelve a la versión anterior; Esta opción está disponible cuando falla la activación o la comprobación posterior o cuando se encuentran diferencias no válidas entre las comprobaciones anteriores y posteriores
    - Cancelar: Cancela el trabajo actual
    - Cierre: Cierra la ventana Tarea de usuario.
- Actúe con las tareas de usuario, si las hay, y seleccione el icono Actualizar para actualizar el recuento total de tareas de usuario
- Porcentaje total de finalización del lote
- Gráfico en el que se puede hacer clic para filtrar por ID de controlador

---

Nota: El número antes del ID del controlador indica el número total de dispositivos administrados por el controlador respectivo.

---

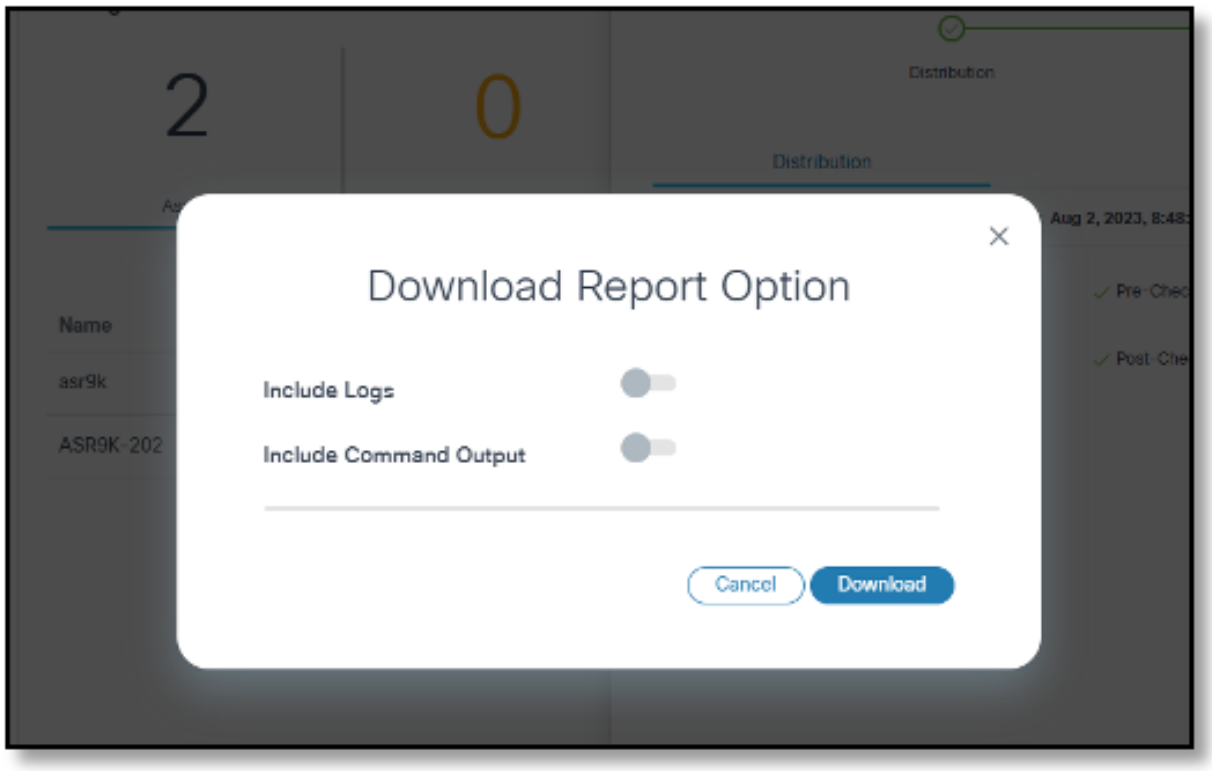
Descargando informe de actualización de software




Descargar PDF

Se muestra el nombre del dispositivo seguido de Download PDF en el encabezado de la vista de detalles. Los usuarios pueden generar y descargar el informe de actualización en formato PDF para el dispositivo seleccionado actualmente. Para descargar el informe de actualización en formato PDF:

1. Haga clic en Descargar PDF. Se abre la ventana Descargar opción de informe.



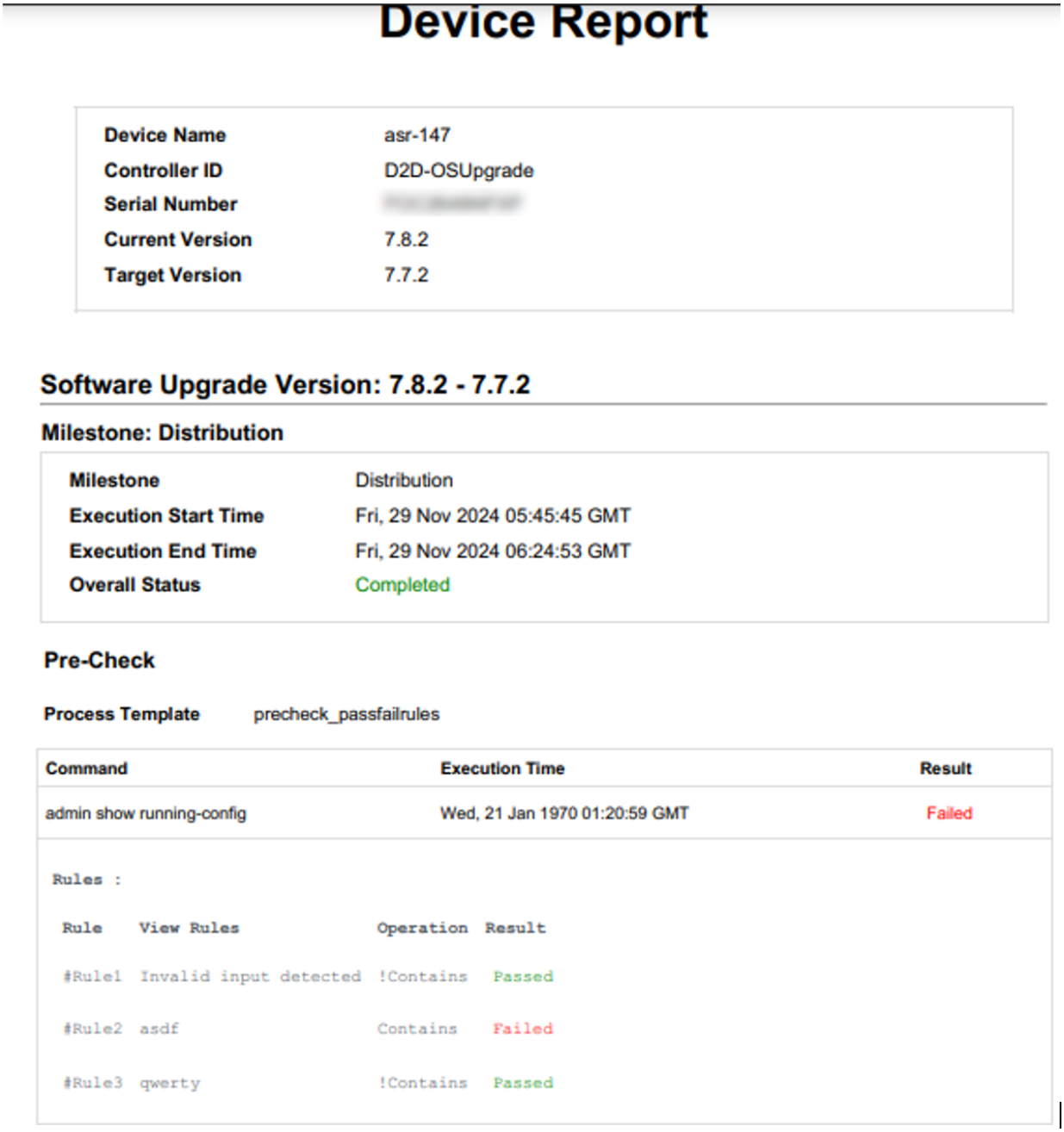

Descargar opción de informe

2. Habilite los modificadores Incluir registros e Incluir salidas de comando.
    - Incluir registros: Incluye registros activos, si los hay, en el informe
    - Resultado del comando Include: Incluye la salida de comando de las comprobaciones previas y posteriores en el informe; En este caso, las reglas son seguidas por el resultado del comando
3. Haga clic en Descarga. Comienza la generación de informes.

---

Nota: La habilitación de las opciones Incluir registros e Incluir salida de comando aumenta el tiempo de procesamiento para la generación y el tamaño del informe. Utilice estas alternancias sólo cuando necesite un informe detallado. Las reglas de comandos se incluyen en el informe independientemente de que la alternancia de resultados del comando esté activada o desactivada.

---



# Device Report

| | |
|---|---|
| **Device Name** | asr-147 |
| **Controller ID** | D2D-OSUpgrade |
| **Serial Number** | [redacted] |
| **Current Version** | 7.8.2 |
| **Target Version** | 7.7.2 |

## Software Upgrade Version: 7.8.2 - 7.7.2

### Milestone: Distribution

| | |
|---|---|
| **Milestone** | Distribution |
| **Execution Start Time** | Fri, 29 Nov 2024 05:45:45 GMT |
| **Execution End Time** | Fri, 29 Nov 2024 06:24:53 GMT |
| **Overall Status** | Completed |

### Pre-Check

**Process Template** precheck_passfailrules

| Command | Execution Time | Result |
|---|---|---|
| admin show running-config | Wed, 21 Jan 1970 01:20:59 GMT | Failed |

Rules :

| Rule | View Rules | Operation | Result |
|---|---|---|---|
| #Rule1 | Invalid input detected | !Contains | Passed |
| #Rule2 | asdf | Contains | Failed |
| #Rule3 | qwerty | !Contains | Passed |

Informe de dispositivo

Trabajos de archivado

1. Inicie sesión en BPA con credenciales que tengan acceso suficiente a los trabajos de actualización.
2. Seleccione OS Upgrade > Upgrade Jobs. Se muestra la página Upgrade Job.
3. Utilice el filtro Buscar en combinación con los filtros de gráfico disponibles para filtrar los trabajos.
4. Seleccione uno o varios trabajos.


Trabajo de archivo

5. Seleccione el icono Más opciones > Archivar.

---

Nota: Sólo se pueden archivar los trabajos completados.

---

Supresión de trabajos

1. Inicie sesión en BPA con credenciales que tengan acceso suficiente a los trabajos de actualización.
2. Seleccione OS Upgrade > Upgrade Jobs. Se muestra la página Upgrade Job.
3. Utilice el filtro Buscar en combinación con los filtros de gráfico disponibles para filtrar los trabajos.
4. Seleccione uno o varios trabajos.


Eliminar trabajo

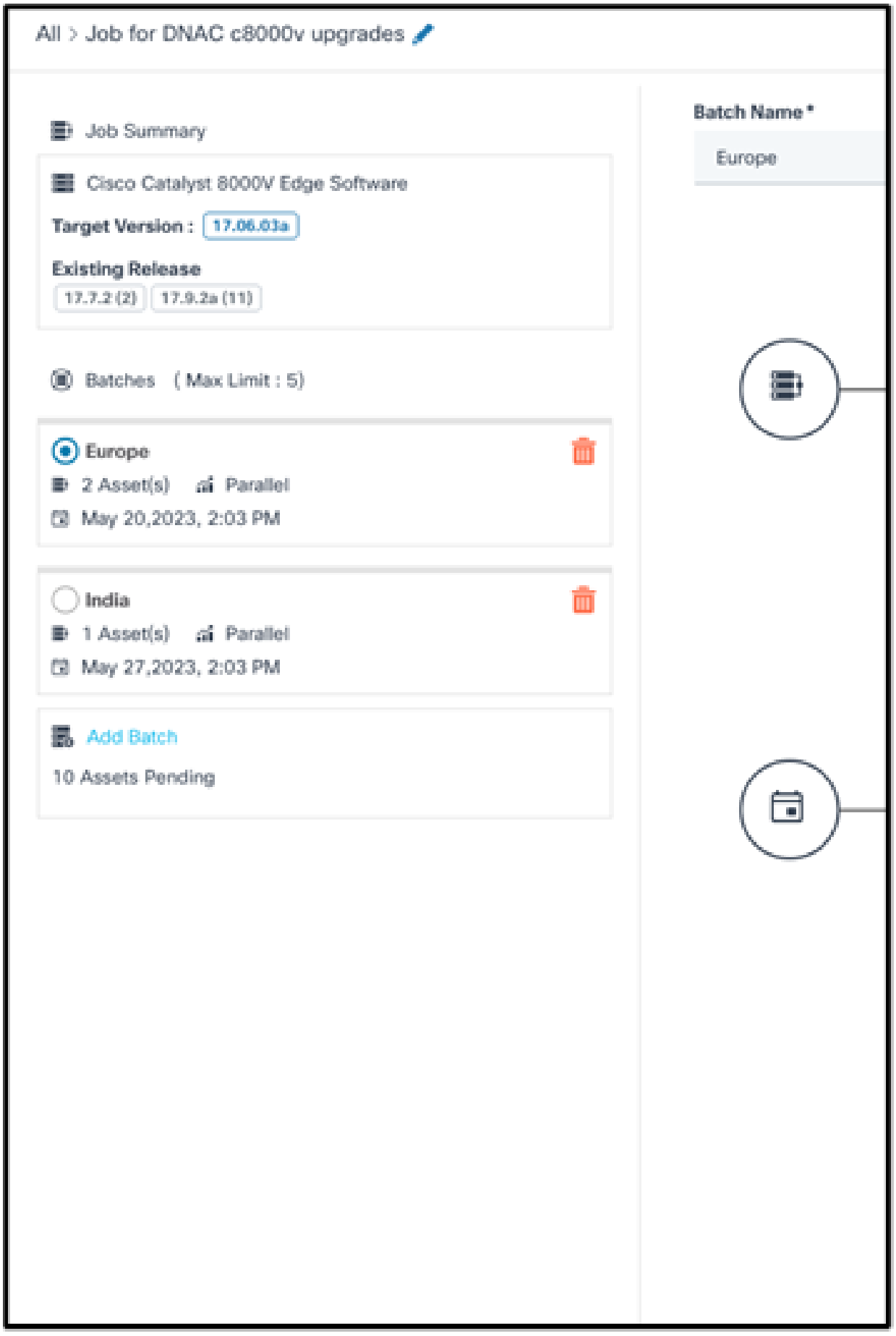
5. Seleccione el icono Más opciones > Eliminar trabajo.

---

Nota: Los trabajos sólo se pueden eliminar cuando se encuentran en la fase Borrador.

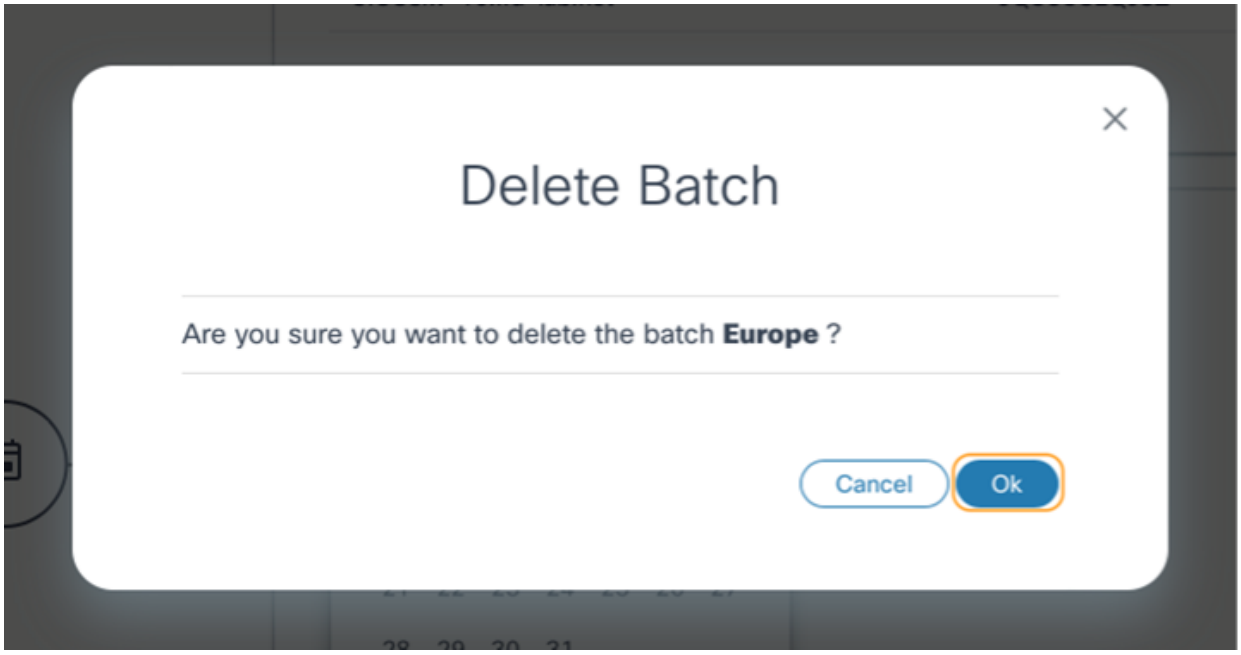
---

Supresión de Lotes en Trabajos




Eliminar un lote en un trabajo

1. Seleccione el icono Eliminar del lote deseado en el panel lateral. Se abrirá una ventana de confirmación.



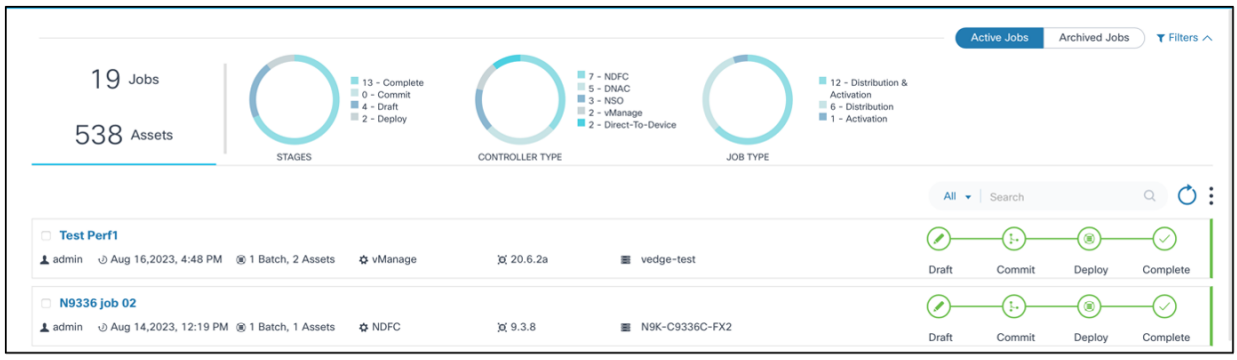

Confirmación de eliminación de lote

2. Click OK.

Los activos asociados al lote eliminado vuelven al grupo de activos pendientes y están disponibles para su selección en lotes nuevos o existentes.

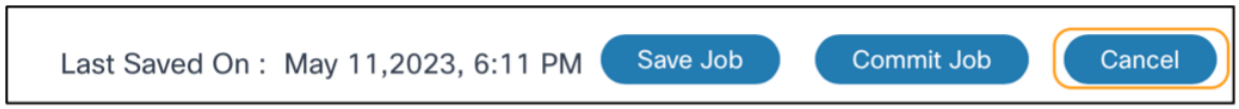
Cancelación de trabajos

1. Inicie sesión en BPA con credenciales que tengan acceso suficiente a los trabajos de actualización.
2. Seleccione OS Upgrade > Upgrade Jobs. Se muestra la página Upgrade Job.




Tarea de actualización

3. Utilice el filtro Buscar en combinación con los filtros de gráfico disponibles para filtrar el trabajo deseado.
4. Haga clic en el trabajo deseado. Se muestra la página Resumen del trabajo.

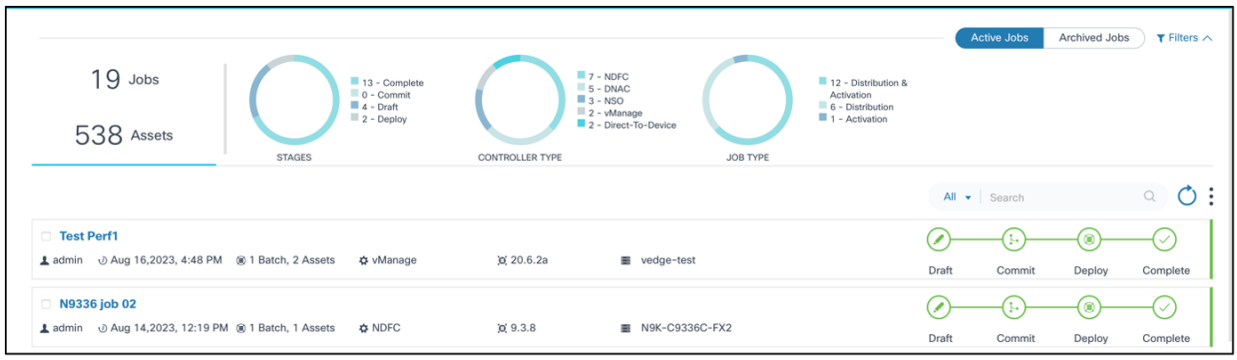



Cancelar

5. Haga clic en Cancel (Cancelar).

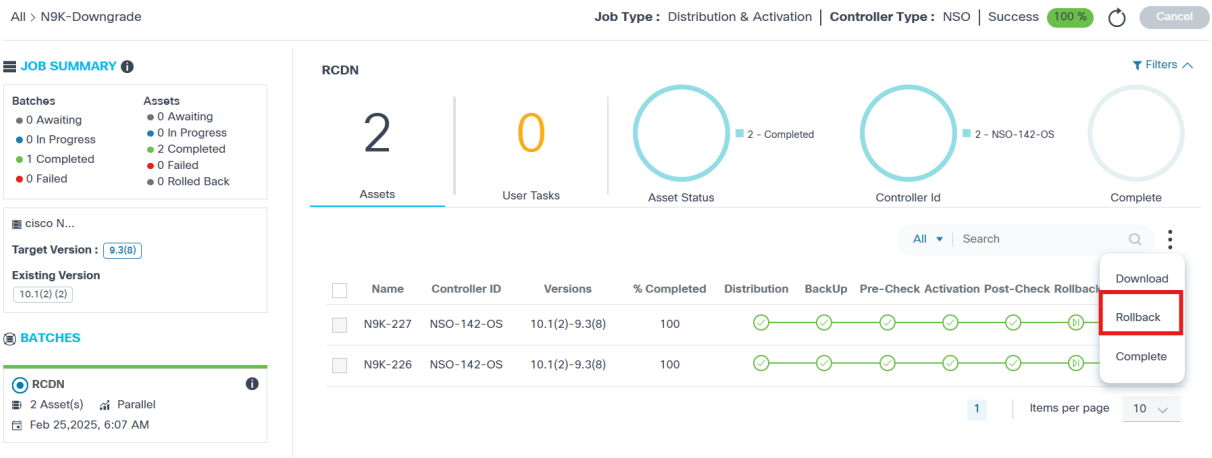
Reversión de trabajos o actualizaciones completados

1. Inicie sesión en BPA con credenciales que tengan acceso suficiente a los trabajos de actualización.
2. Seleccione OS Upgrade > Upgrade Jobs. Se muestra la página Upgrade Job.




Tarea de actualización

3. Utilice el filtro Buscar en combinación con los filtros de gráfico disponibles para filtrar el trabajo deseado.
4. Haga clic en el trabajo deseado. Se muestra la página Resumen del trabajo. Seleccione el lote necesario en el panel del lado izquierdo y seleccione los dispositivos deseados que necesitan confirmación completa / Rollback en el panel del lado derecho
5. Seleccione el icono Más opciones y haga clic en las acciones de menú Deshacer o Finalizar según los requisitos.




Rollback

---

Nota: Los dispositivos solo se pueden seleccionar cuando se cumplen los siguientes requisitos previos:

---

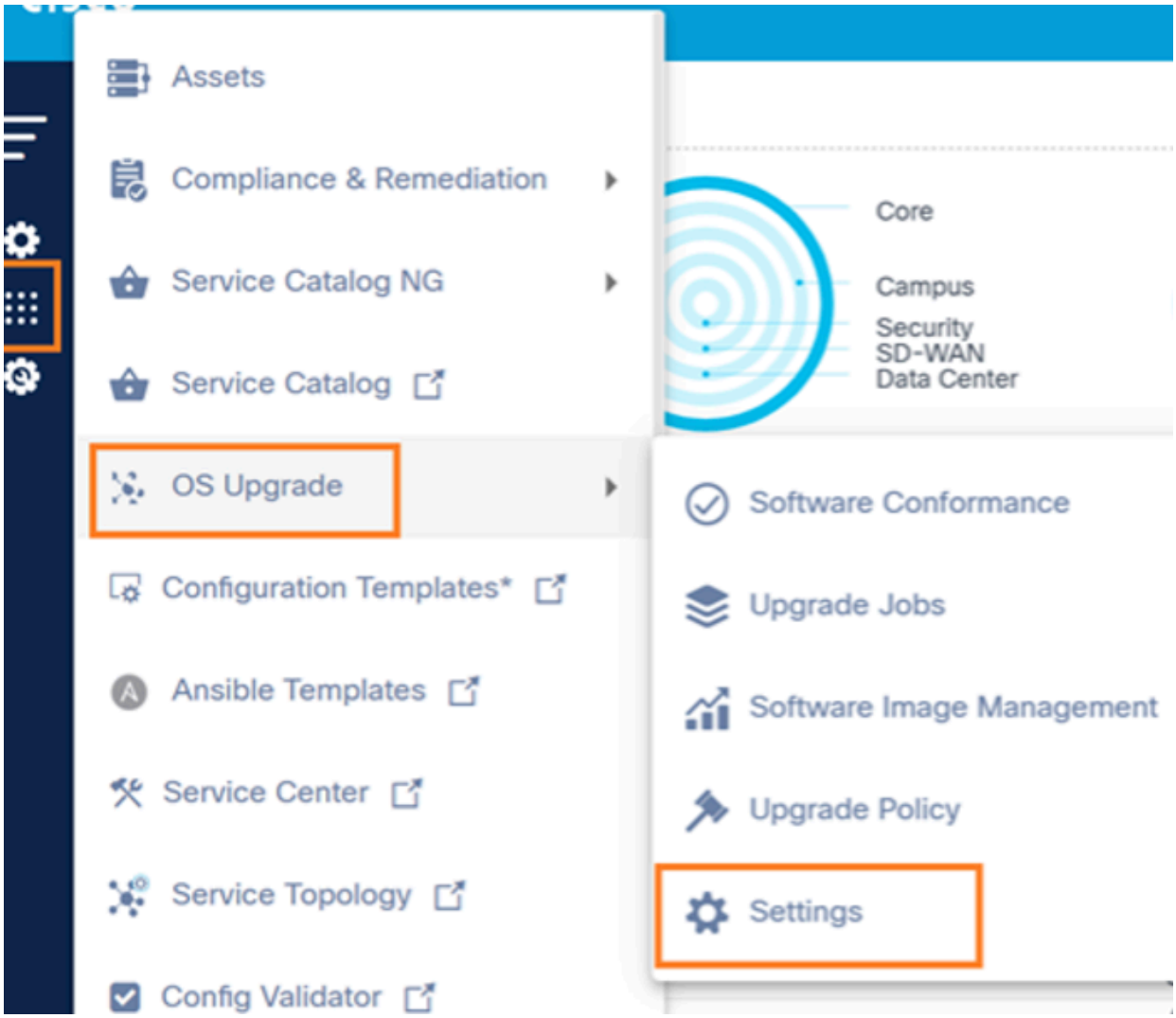
- Se deben configurar las opciones para habilitar la opción de reversión de un trabajo actualizado completado; consulte Configuración para obtener más información.
- Si no se lleva a cabo ninguna acción en el tiempo, los dispositivos pasan automáticamente al estado Completo
- Los dispositivos están disponibles para la acción de reversión bajo demanda si la reversión se ha completado anteriormente o si el hito de reversión está en estado Esperando

# Configuración

La configuración de actualización del sistema operativo proporciona un marcador de posición para mantener la configuración común utilizada en otros componentes de la aplicación Actualización del sistema operativo.

Para acceder a la página Configuración:

1. Inicie sesión en BPA con credenciales que tengan acceso de administrador a la configuración.



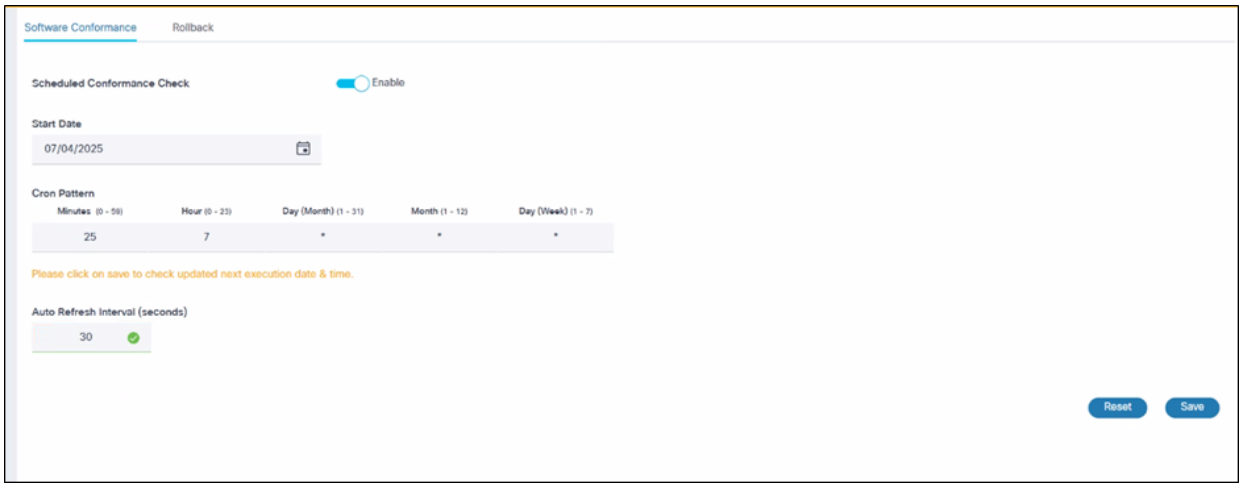
Configuración

2. Seleccione OS Upgrade > Settings. Se abre la página Settings.

La página Configuración tiene las dos fichas siguientes:

- Conformidad de software: En esta ficha se pueden actualizar las configuraciones que permiten la ejecución de planificaciones de conformidad automática
- Reversión: Las configuraciones que permiten la reversión de una actualización de dispositivo completa se pueden actualizar en esta ficha

## Conformidad de software




Ficha Conformidad de software

La ficha Software Conformance proporciona lo siguiente:

- Comprobación de conformidad programada: Activar o desactivar la planificación
- Fecha de inicio: Seleccione el MM/DD/AAAA.

---

Nota: La fecha de inicio debe ser una fecha futura.

---

- Patrón crónico: Proporcione los siguientes detalles:
  - Minutos (0-59)
  - Hora (0-23)
  - Día (mes) (1-31)
  - Mes (1-12)
  - Día (semana) (1-7)
- Agregar intervalo de actualización automática: El valor predeterminado es 30 segundos
- Guardar: Guardar cambios

## Rollback


Ficha Deshacer

La ficha Rollback proporciona lo siguiente:

- Alternancia de verificación de usuario: Habilitar o deshabilitar la verificación de usuario
    - Estado habilitado: Los dispositivos en el trabajo de actualización esperan la confirmación del usuario para revertir o completar la actualización hasta que se alcance el tiempo de umbral configurado en Configuration Threshold Time (hrs); cuando se alcanza, los dispositivos pasan automáticamente al estado Completado
    - Estado deshabilitado: Los dispositivos del trabajo de actualización completan automáticamente la actualización sin esperar la confirmación del usuario
- Tiempo de umbral de confirmación: Agregar un tiempo de umbral para esperar en horas
- Guardar: Guardar cambios

## Configuración de implementación

- Las programaciones predeterminadas para la comprobación de la política de conformidad y los metadatos SWIM se configuran diariamente a las 7:25 a.m. hora local.
- Para cambiar las programaciones predeterminadas de la sincronización de metadatos de la imagen SWIM, navegue hasta el directorio instalado BPA "<directorio de instalación BPA>/conf/@cisco-bpa-platform/mw-osupgrade-nxtgen/config.json" y actualice la propiedad schedule.swimSchedule con la expresión Cron. Las programaciones se pueden actualizar después de la implementación. Consulte Conformidad de Software para obtener más información.
- Para aumentar o disminuir el número máximo de dispositivos procesados en modo paralelo para diferentes tipos de controladores:

1. Actualice los siguientes archivos:
    - Archivo de Cisco Catalyst Center: "<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-dnac-agent/config.json"
    - Archivo vManage: "<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-vmanage-agent/config.json"
    - Archivo NDFC: "<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-ndfc-agent/config.json"
    - Archivo FMC: "<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-fmc-agent/config.json"
2. Navegue hasta Límite de actualización > Capacidades > Activación de imagen, Distribución de imagen para aumentar el límite de activación o distribución concurrente.

---

Nota: Consulte las Plataformas de Dispositivos y Controladores Soportados antes de actualizar estos límites.

---

## Control de acceso

## Control de acceso basado en roles

BPA admite el control de acceso basado en roles (RBAC). En el modelo RBAC, una función encapsula un conjunto de permisos (es decir, acciones) que un usuario puede realizar. Para el control de acceso, los administradores pueden asignar funciones predefinidas o funciones recién creadas con permisos para grupos de usuarios. Un usuario puede pertenecer a uno o más grupos de usuarios y cada grupo de usuarios puede asignarse a una o más funciones, lo que otorga a los usuarios de ese grupo determinados permisos de acceso.

En la tabla siguiente se describen las funciones de actualización del sistema operativo OOB y los permisos asociados.

| Servicio | Grupo | Intención | Superadministrador | Administrador de casos prácticos | Usuario de solo lectura (caso práctico de actualización del SO: usuario de solo lectura) |
|---|---|---|---|---|---|
| OSUpgradeService | ui_app | Mostrar u ocultar la aplicación Actualizar trabajos | Yes | Yes | Yes |
| OSUpgradeService | ui_app | Mostrar u ocultar la aplicación Conformidad de software | Yes | Yes | Yes |
| OSUpgradeService | ui_app | Mostrar u ocultar la aplicación SWIM | Yes | Yes | Yes |
| OSUpgradeService | ui_app | Mostrar u ocultar la aplicación Directivas de actualización de software | Yes | Yes | Yes |
| OSUpgradeService | ui_app | Mostrar u ocultar la configuración de actualización de software | Yes | Yes | Yes |
| OSUpgradeService | Actualizar trabajos | Administrar trabajos de | Yes | Yes | No |

| Servicio | Grupo | Intención | Superadministrador | Administrador de casos prácticos | Usuario de solo lectura (caso práctico de actualización del SO: usuario de solo lectura) |
|---|---|---|---|---|---|
| | | actualización (p. ej., crear, actualizar, eliminar y confirmar) | | | |
| OSUpgradeService | Actualizar trabajos | Cancelar trabajos de actualización | Yes | Yes | No |
| OSUpgradeService | Actualizar trabajos | Archivado a demanda de los trabajos | Yes | Yes | No |
| OSUpgradeService | Actualizar trabajos | Aprobación manual | Yes | Yes | No |
| OSUpgradeService | Política de conformidad del software | Ver políticas de conformidad de software y resultados de ejecución | Yes | Yes | Yes |
| OSUpgradeService | Política de conformidad del software | Crear, actualizar y eliminar directivas de conformidad de software | Yes | Yes | No |
| OSUpgradeService | Política de conformidad del software | Ejecución a demanda de políticas de conformidad del software | Yes | Yes | No |
| OSUpgradeService | Política de actualización | Ver políticas de actualización del SO | Yes | Yes | Yes |
| OSUpgradeService | Política de actualización | Gestionar políticas de actualización del SO | Yes | Yes | No |
| OSUpgradeService | Swim-image-management | Creación, actualización y eliminación de | Yes | Yes | No |

| Servicio | Grupo | Intención | Superadministrador | Administrador de casos prácticos | Usuario de solo lectura (caso práctico de actualización del SO: usuario de solo lectura) |
|---|---|---|---|---|---|
| | | imágenes de software | | | |
| OSUpgradeService | Swim-image-management | Ver SWIM | Yes | Yes | Yes |
| OSUpgradeService | Swim-image-management | Sincronizar imágenes de software | Yes | Yes | No |
| OSUpgradeService | Recomendaciones de software | Sincronizar metadatos de recomendaciones de software | Yes | Yes | No |
| OSUpgradeService | Recomendaciones de software | Ver recomendaciones o perspectivas | Yes | Yes | Yes |
| OSUpgradeService | Recomendaciones de software | Administrar la directiva de conformidad | Yes | Yes | No |
| OSUpgradeService | Configuración de la conformidad del software | Ver configuración de conformidad del software | Yes | Yes | Yes |
| OSUpgradeService | Configuración de la conformidad del software | Administrar configuración de conformidad de software | Yes | Yes | No |

Nota: Los roles personalizados y la asignación de permisos se pueden realizar según los requisitos. Consulte Grupos de Recursos.

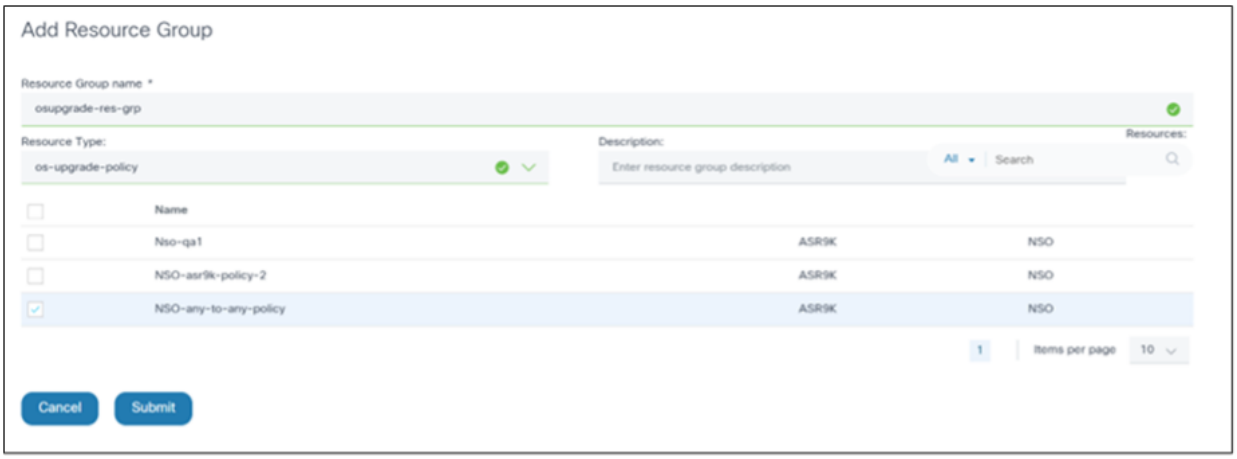
## Grupos de recursos

Esta función proporciona un control de acceso granulado preciso para los recursos de BPA, como las directivas de actualización, lo que impide que los usuarios no autorizados actualicen las directivas definidas en la aplicación Actualización del sistema operativo. Los administradores

pueden restringir el acceso definiendo un grupo de recursos con directivas accesibles.

Para crear un grupo de recursos:

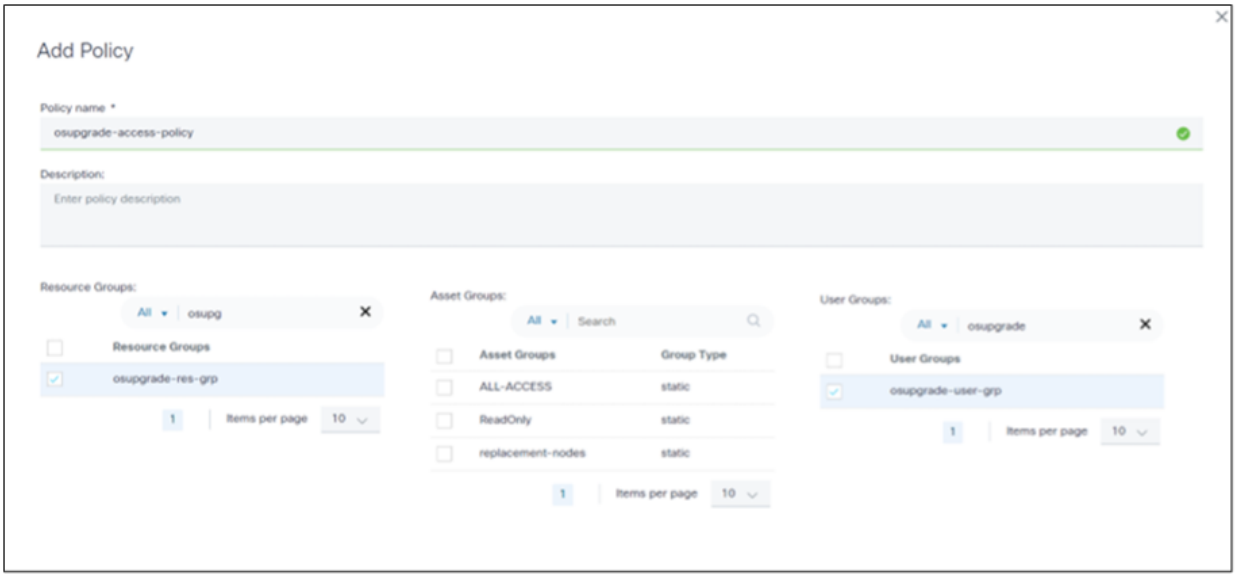
1. Vaya a Configuración > Grupos de recursos.




Agregar grupo de recursos

2. Cree un grupo de recursos con directivas a las que puedan acceder los usuarios que no sean administradores.
3. Seleccione os-upgrade-policy como Resource Type. Se muestran los recursos correspondientes.
4. Seleccione las directivas de actualización necesarias.
5. Haga clic en Submit (Enviar). Los usuarios que no sean administradores y que pertenezcan a este grupo de usuarios tendrán acceso a las directivas disponibles únicamente en el grupo de recursos seleccionado.

Para asociar el grupo de recursos a un grupo de usuarios, cree una directiva de acceso.



Agregar política de acceso

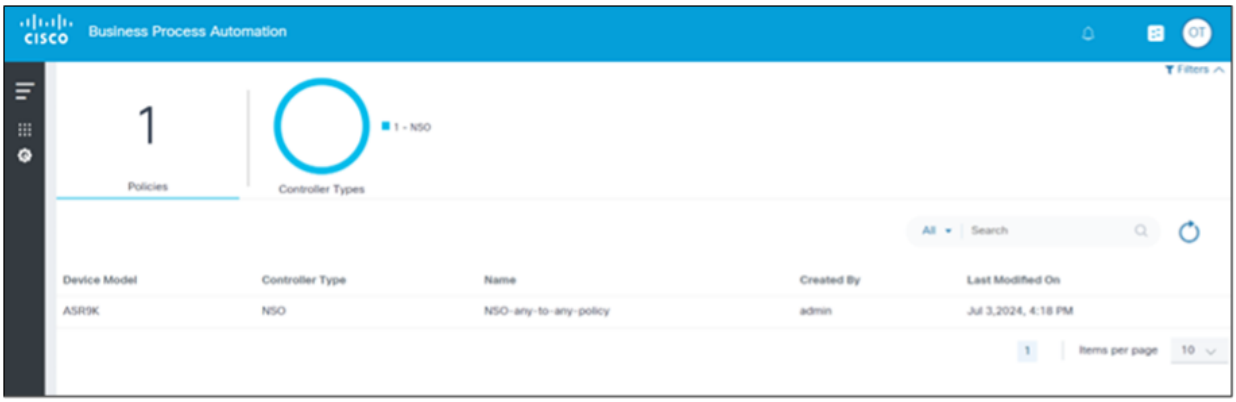
---

Nota: Una vez creado el grupo de recursos, debe asociarse a un grupo de usuarios mediante directivas de acceso. Consulte Control de Acceso para obtener más información sobre lo siguiente:

---

- Usuarios
- Funciones
- Grupos de usuarios
- Políticas de acceso
- Grupos de recursos
- Grupos de activos

A continuación se muestra un ejemplo de un usuario no administrador que tiene acceso a recursos restringidos:




Usuario no administrador con restricciones de recursos

Configuración del indicador de confianza cero

Los recursos accesibles para un usuario pueden variar en función de la configuración del indicador de confianza cero. El indicador de confianza cero se puede establecer en true o false. En la tabla siguiente se resumen las posibilidades de acceso a los recursos en función de la configuración del indicador de confianza cero.

| Usuario | Grupo de usuarios | Política de acceso | Grupo de recursos | Recursos | Confianza cero | Habilitado |
|---|---|---|---|---|---|---|
| Usuario 1 | UG1 | AP1 | RG1 | 2 recursos | 2 recursos | 2 recursos |
| Usuario | UG1 | AP2 | RG2 | 0 recursos | 0 recursos | 0 recursos |

| Usuario | Grupo de usuarios | Política de acceso | Grupo de recursos | Recursos | Confianza cero | Habilitado |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| Usuario 1 | UG1 | AP3 | Nulo | | 0 recursos | Todos los recursos |
| Usuario 1 | UG1 | Nulo | Nulo | | 0 recursos | Todos los recursos |

Para habilitar o deshabilitar el indicador de confianza cero:

1. Vaya a la siguiente ruta de configuración:

```
cd /opt/bpa/bpa-helm-chart-

      /charts/cisco-bpa-platform-mw-auth/public_conf/config.json
```

2. Modifique el valor zeroTrustPolicies.
3. Navegue hasta el siguiente paquete principal:

```
cd /opt/bpa/bpa-helm-chart-
```

4. Ejecute el siguiente comando para eliminar el casco principal:

```
helm delete bpa-rel -n bpa-ns
```

5. Ejecute el siguiente comando para verificar el estado de las vainas

```
kubectl get pods -n bpa-ns
```

6. Ejecute el siguiente comando para instalar el núcleo helm después de que se hayan terminado todos los pods:

```
helm install bpa-rel --create-namespace --namespace bpa-ns
```

7. Ejecute el siguiente comando para verificar el estado de las vainas que aparecen:

```
kubectl get pods -n bpa-ns
```

# Solución de problemas de actualización del SO

Esta sección proporciona consejos para la resolución de problemas relacionados con los problemas observados con la aplicación Actualización del SO en BPA.

## No se puede ver el modelo de dispositivo de destino al crear una directiva de conformidad

Asegúrese de que los metadatos de imagen correspondientes estén disponibles en Imágenes de software en SWIM. Si no se encuentra, realice una de las siguientes opciones:

- Sincronizar imágenes para recuperar metadatos de imagen de controladores como Cisco Catalyst Center, NDFC, vManage y FMC
- Crear los metadatos de imagen necesarios para controladores como NSO, CNC, Direct-to-Device y ANSIBLE

## La conformidad del software muestra un estado no operativo

Esto podría deberse a las siguientes razones:

- No se encontraron recursos con el modelo seleccionado al crear la directiva de conformidad de software
- El nombre del modelo en SWIM no coincide con el modelo del dispositivo de conformidad en el inventario de dispositivos para todos los dispositivos
- Si se eligió SMU como parte de la creación de conformidad de software y la detección de SMU falló para todos los dispositivos
- Error o no se encontró la plantilla de proceso seleccionada para la ejecución de la plantilla de comprobación de conformidad
- El número de serie o la versión actual no están disponibles para todos los dispositivos del modelo seleccionado al crear la conformidad de software

## El estado del resultado de conformidad de software de ciertos dispositivos es desconocido

Esto podría deberse a las siguientes razones:

- El nombre del modelo en SWIM no coincide con el modelo de dispositivo de conformidad en el inventario de dispositivos
- Si se eligió SMU como parte de la creación de conformidad de software y la detección de SMU falló para un dispositivo
- Error o no se encontró la plantilla de proceso seleccionada para la ejecución de la plantilla de comprobación de conformidad
- El número de serie o la versión actual no están disponibles para los dispositivos

## Porcentaje de progreso de finalización de tarea de actualización

Si el porcentaje de progreso de finalización del trabajo de actualización es inferior a 100 aunque se haya completado la actualización, confirme que la configuración de Espera para Rollback esté habilitada en OS Upgrade > Settings > Rollback y que la opción de verificación de usuario esté activada. Si el porcentaje de finalización general permanece por debajo de 100, seleccione Rollback o Complete.

## Se ha alcanzado la programación del trabajo, los dispositivos están atascados en estado de espera

Si los dispositivos se quedan en estado de espera después de que se inicie el trabajo programado, intente reiniciar los microservicios Kafka, Camunda, Scheduler y Actualización del SO.

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).

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).