Atualização do SO do guia do usuário do BPA v5.1

Introdução

O aplicativo de atualização de SO BPA (Business Process Automation) fornece uma solução de automação abrangente para executar a conformidade de software e atualizações de dispositivos de rede em diferentes domínios. Ele suporta vários controladores de domínio e fornece uma experiência de usuário unificada. Ele suporta atualizações de sistema operacional (SO) base e

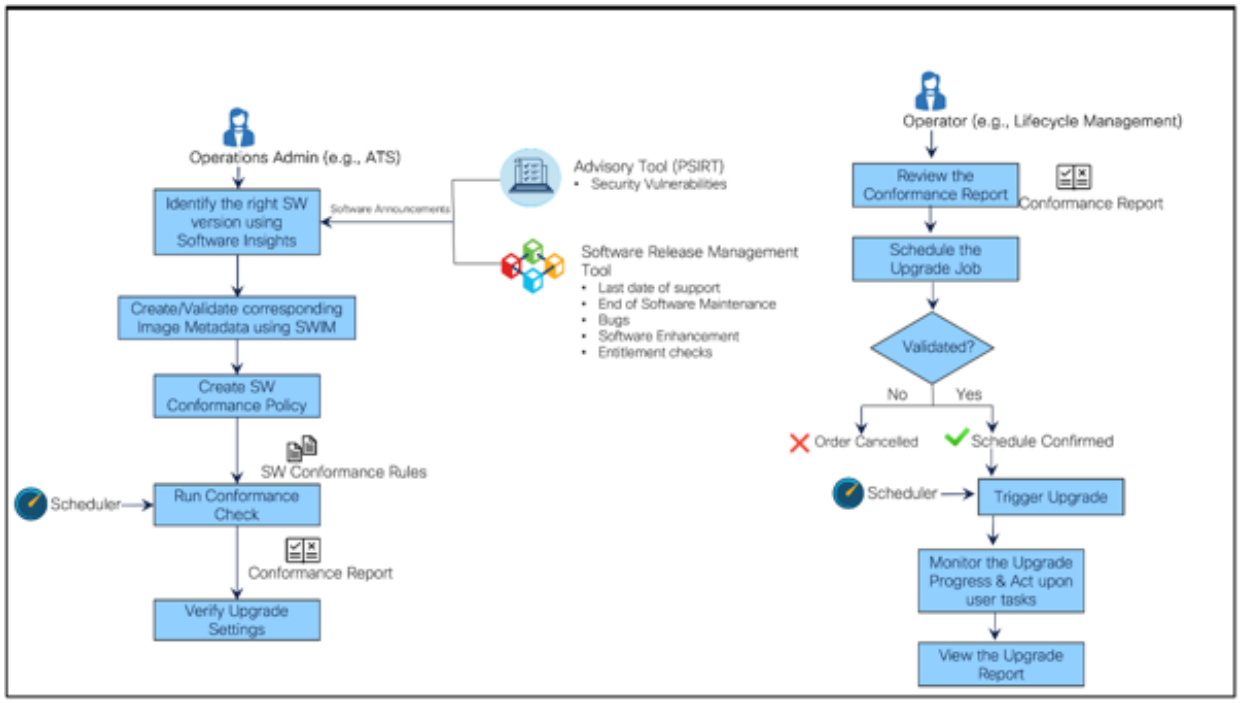
atualizações de patch SMU (Software Maintenance Update) ou RPM Package Manager (RPM).

Principais recursos

O aplicativo de atualização de SO fornece os seguintes recursos principais de automação:

- Gerenciamento de imagens de software: Uma lista centralizada de imagens de software e suas versões (de todos os fornecedores) para o processo de atualização de software usar
- Informações sobre software: Identifica riscos e vulnerabilidades de software expostos a ativos de rede e obtém informações sobre versões de software recomendadas pelo fornecedor
- Conformidade de software: Identifica todos os ativos na rede cujas imagens de software devem ser atualizadas
- Definição de Método de Procedimento de Atualização (MOP): Predefine o processo de atualização junto com verificações prévias e posteriores para cada modelo de dispositivo ou família do fornecedor
- Trabalhos de Atualização: Agenda atualizações para ativos não compatíveis durante as janelas de manutenção nas regiões geográficas, monitora o progresso da atualização e obtém relatórios detalhados

Fluxo de ponta a ponta



Fluxo de ponta a ponta

A figura acima descreve os fluxos de chamadas do aplicativo OS Upgrade para duas personalidades de usuário diferentes: Administrador de operações e operador de rede, que vem

pronto para uso (OOB). Consulte Controle de Acesso para obter mais informações sobre funções OOB e permissões correspondentes.

Persona	Descrição	Espaço de Trabalho
Administrador de operações	Descobre vulnerabilidades de software (por exemplo, avisos, bugs, boletins de fim da vida útil) que afetam os ativos da rede	BPA: Atualização de SO/Gerenciamento de imagem de software/Recomendações
Administrador de operações	Identifica a versão de software e os ativos afetados e determina a versão de destino correta com base nas sugestões fornecidas pelo fornecedor	BPA: Atualização de SO/Gerenciamento de imagem de software/Insights
Administrador de operações	Cria os metadados de imagem de software necessários	BPA: Atualização de SO/Gerenciamento de imagem de software/Imagens de software
Administrador de operações	Cria a intenção para os modelos de dispositivos afetados e executa a política sob demanda ou na execução da política programada	BPA: Política de Conformidade de Software/Atualização do SO
Administrador de operações	Identifica os ativos afetados ou não conformes	BPA: Atualização do SO/conformidade de software/Exibir resultados
Administrador de operações	Cria ou modifica a política de atualização de acordo com o MOP de atualização; isso inclui a predefinição das verificações prévias e posteriores, fluxos de trabalho para distribuição ou ativação, desvio ou reversão de tráfego e reversão para atualizações em uma ou várias etapas	BPA: Política de Upgrade/Atualização do SO
Operador de rede	Agenda um trabalho para atualizar todos os dispositivos não compatíveis	BPA: Trabalhos de Upgrade/Upgrade do SO
Operador de rede	Monitora o progresso do trabalho de atualização	BPA: Atualizar SO/Atualizar trabalhos/Detalhes do trabalho
Operador de rede	Atua nas tarefas do usuário, se houver, para classificar problemas e permite que o processo passe para a próxima etapa	BPA: Atualizar SO/Atualizar trabalhos/Detalhes do trabalho

Proposta de valor

Os seguintes valor agregado abaixo são fornecidos pelo aplicativo OS Upgrade:

- Uma abordagem que prioriza a API para permitir um consumo de serviços mais fácil a partir dos Sistemas de Suporte a Operações (OSS - Operations Support Systems) ascendentes e dos Sistemas de Suporte a Negócios (BSS - Business Support Systems)
- Validação rápida da conformidade de software dos dispositivos de rede em redes gerenciadas por vários controladores de domínio
- Os operadores têm mais controle sobre os trabalhos de atualização usando mecanismos de lote, enfileiramento e agendamento
- Os trabalhos de atualização podem ser criados antecipadamente para revisões e executados posteriormente
- Um mecanismo de enfileiramento que permite um throughput mais rápido e melhor, com falhas mínimas a zero
- Pré-atualize backups de configuração automáticos, permitindo restaurações perfeitas em caso de falhas
- Execuções pré e pós-verificação, garantindo que os upgrades sejam bem-sucedidos sem interrupções de serviço
- Uma abordagem orientada por políticas que oferece a flexibilidade de predefinir o MOP de atualização com verificações de pré e pós-validação, distribuição ou ativação, desvio ou reversão de tráfego e processos de reversão, permitindo que eles sejam personalizados conforme necessário

Controladores e plataformas de dispositivos suportados

As plataformas a seguir foram validadas no BPA e são suportadas no OOB. No entanto, a estrutura é genérica e pode ser estendida para novas plataformas. O suporte OOB para plataformas adicionais será fornecido em versões futuras com base na prioridade.

Controlador(es) de domínio	Plataformas de dispositivo
Cisco Catalyst Center v2.3.7.5-70434	- Cisco IOS, Cisco IOS-XE
vManage v20.12.4	- Cisco IOS, Cisco IOS-XE Note: Os dispositivos devem ser v17.9.x ou superior para que a distribuição do servidor remoto funcione
Nexus Dashboard Fabric Controller (NDFC) v12.1.2e e v12.2.2	- Cisco-NXOS (N9k)

Controlador(es) de domínio	Plataformas de dispositivo
Centro de gerenciamento de firewall (FMC) v7.4.1	- Firepower 3140
Network Services Orchestrator (NSO) v6.3	- Cisco-IOSXR (NCS540, NCS560, ASR9K) - Cisco-NXOS (N9K) Note: NED NX-OS v5.25.17 ou superior é necessário
Cross Network Controller (CNC) v6.0	- Cisco-IOSXR (NCS540, ASR9K)
ANSIBLE v2.9.18 (AWX - 17.1.0)	- Cisco-IOSXR (NCS540, ASR9K)
Direto para dispositivo (via Teletype Network (Telnet) e Secure Shell (SSH))	- Cisco-IOSXR (NCS540, ASR9K)

Novos recursos

Para obter os recursos incrementais disponibilizados para o caso de uso de atualização do SO para esta versão, consulte as Notas de versão do BPA.

Pré-requisitos

As seguintes condições de pré-requisito devem ser atendidas antes de usar o aplicativo de Upgrade do SO:

- Atualização do SO, backup e restauração, serviços do Agendador e todos os serviços de plataforma necessários ou serviços do agente do controlador estão em execução
- Os artefatos necessários (por exemplo, fluxos de trabalho, modelos de processo, políticas de atualização padrão etc.) são carregados
- Os controladores necessários são adicionados e os dispositivos são sincronizados com êxito; consulte Controladores suportados e plataformas de dispositivos para obter mais informações

Trabalhando com o aplicativo de atualização do SO

O aplicativo de atualização de SO é composto pelos seguintes componentes:

- Gerenciamento de imagens de software (SWIM)
- Gerenciamento do servidor de distribuição de imagens
- Informações sobre software
- Conformidade de software

- Política de atualização
- Trabalhos de Atualização
- Configurações

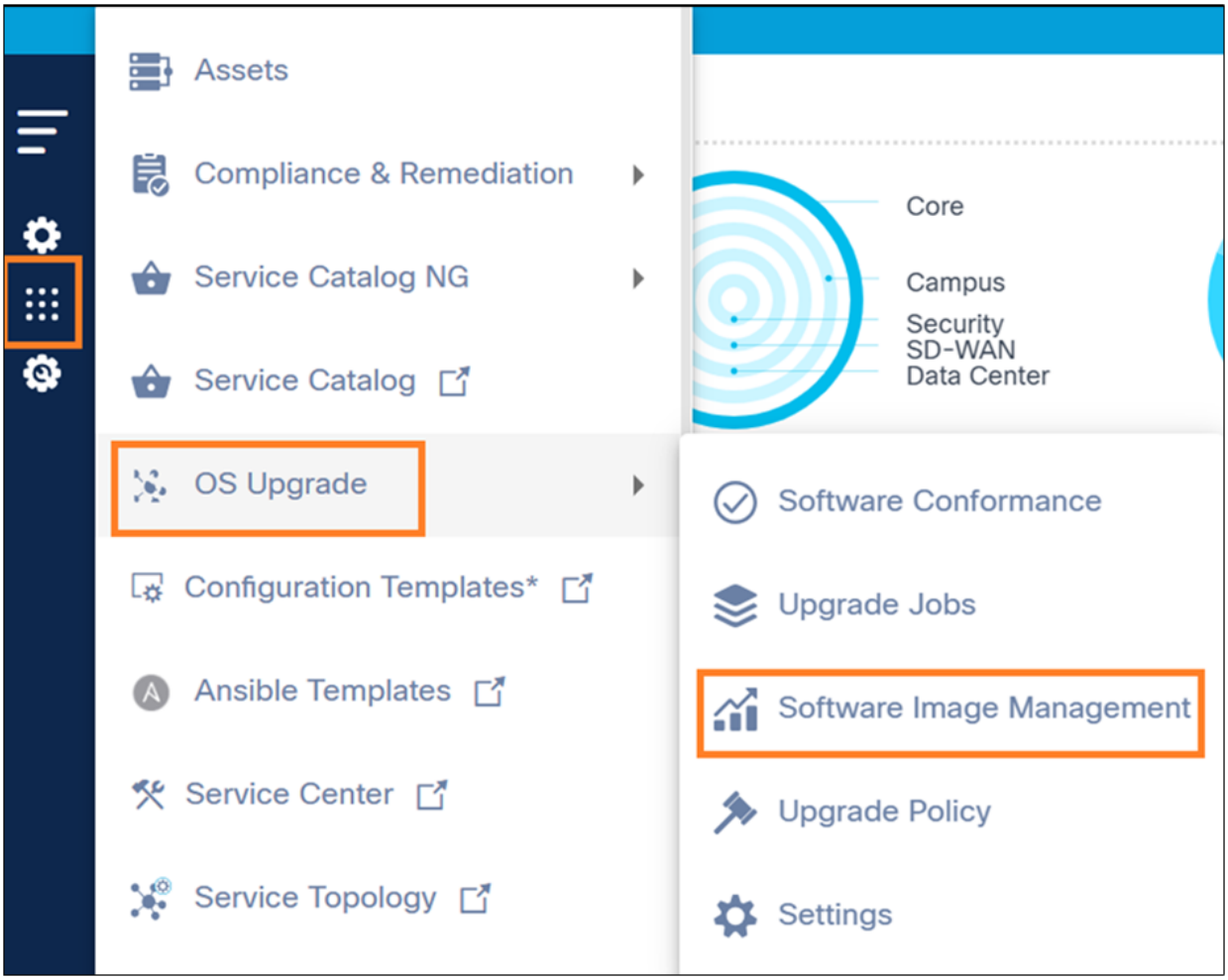
Gerenciamento de imagens de software

O componente SWIM permite que os usuários de operações mantenham detalhes de imagem de software para controladores como NSO, ANSIBLE, CNC, FMC e Direct-to-Device que não têm suporte de gerenciamento de imagem OOB. Ele também lista os detalhes da imagem de software mantida por controladores como vManage, NDFC e Cisco Catalyst Center, fornecendo uma lista centralizada de software mantida em todos os controladores de domínio. As imagens de software e o servidor de distribuição de imagem são os dois principais subcomponentes dentro do módulo SWIM.

Imagens de software

Para acessar a página Imagens de Software:

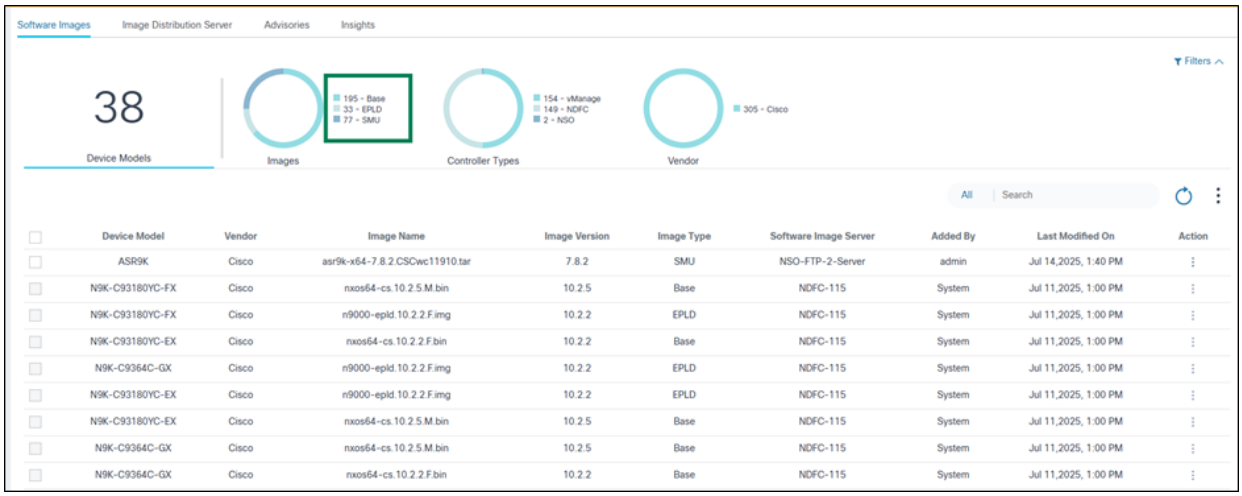
1. Faça login no BPA com credenciais que tenham acesso ao Gerenciamento de imagem de software.



Navegação de gerenciamento de imagem de software

2. Selecione OS Upgrade > Software Image Management.

A página Gerenciamento de imagens exibe as seguintes guias: Imagens de software, Servidor de distribuição de imagens, Recomendações e Informações.



Guia Imagens de software

A guia Imagens de Software contém o seguinte:

- Uma seção de análise, exibida na parte superior, que fornece o seguinte:
    - O número total de modelos de dispositivo e imagens de software associadas
    - Um filtro rápido Imagens que permite filtrar imagens com base no tipo (por exemplo, base, SMU); o número indica o número total de imagens associadas a um tipo de imagem respectivo
    - Um filtro rápido de tipos de controladores que permite filtrar imagens com base no tipo de controlador (por exemplo, Cisco Catalyst Center, vManage, NSO ou NDFC, Direct-to-Device, CNC, ANSIBLE, FMC) para o qual as imagens são hospedadas; o número indica o número total de imagens associadas a um tipo de controlador respectivo
    - Um filtro rápido Vendor que permite filtrar imagens com base no fornecedor que publicou o software
- O ícone Mais opções fornece as seguintes funcionalidades:
    - Adicionar detalhes da imagem: Adicionar novos metadados de imagem
    - Carregamento em massa: Metadados de imagem de carregamento em massa no formato .csv
    - Sincronizar imagens: Sincronizar metadados de imagem de controladores (por exemplo, Cisco Catalyst Center, vManage, NDFC e FMC)
    - Excluir tudo: Exclusão em massa de imagens selecionadas

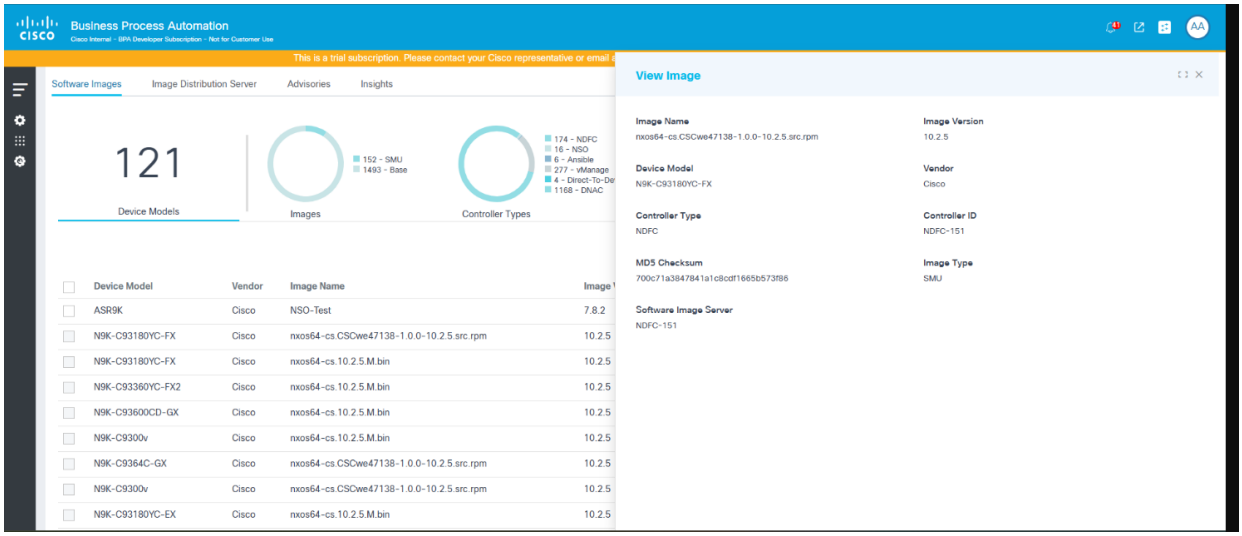
---

Note: A adição, a exclusão e o carregamento em massa de detalhes de imagem são permitidos somente para controladores NSO, ANSIBLE, CNC e Direct-to-Device.

- O filtro Pesquisar pode ser usado para pesquisar imagens e inclui os seguintes filtros de pesquisa exclusivos:
    - Todos: Pesquisar em todos os campos
    - Nome da imagem: Procurar imagens com um nome de imagem específico
    - Modelo do dispositivo: Procurar imagens com um modelo especificado
    - Versão da imagem: Procurar imagens com uma versão de software específica
    - Servidor de imagem de software: Procurar as imagens associadas a um servidor de imagem específico
- O ícone Atualizar atualiza a página e limpa os filtros selecionados.
- As imagens existentes são exibidas em uma tabela de grade com as seguintes colunas:
    - Modelo do dispositivo: Modelo de dispositivo ao qual os detalhes da imagem são aplicáveis
    - Fornecedor: Fornecedor que publica as imagens de software
    - Nome da imagem: Nome do arquivo da imagem
    - Versão da imagem: Versão do software da imagem
    - Tipo de Imagem: Determina o tipo de imagem (por exemplo, base, SMU, dispositivo lógico programável eletrônico (EPLD))

- Servidor de imagem de software: Servidor de imagem onde a imagem atual existe
- Adicionado por: Usuário que adicionou os metadados da imagem
- Última modificação em: Carimbo de data/hora da última atualização de detalhes da imagem
- Ação: Fornece um ícone Mais Opções a partir do qual ações específicas de linha (por exemplo, editar, excluir) podem ser selecionadas

- Classificar imagens clicando no cabeçalho da coluna respectiva



Exibir imagem

- Clicar em uma linha abre a janela Visualizar imagem.

Sincronizando metadados de imagens de software

Para executar a sincronização sob demanda de imagens de software:

Sincronizar imagens

1. Selecione o ícone Mais Opções > Sincronizar Imagens. Os detalhes dos metadados da imagem do vManage, Cisco Catalyst Center, NDFC e FMC são descobertos e persistentes

no BPA.

Note: Para controladores FMC, os dados existentes são retidos toda vez que uma sincronização é executada. Somente imagens novas são acrescentadas.

---

2. Se o nome da imagem do controlador FMC incluir a palavra "FTD" ou "Firepower Threat_Defense", o deviceModel dessa imagem será mapeado como FTD.

OU

Se o nome da imagem do controlador FMC incluir a palavra "FMC", "FW_Mgmt_Center" ou "Firewall_Management_Center", o deviceModel dessa imagem será mapeado como FMC.

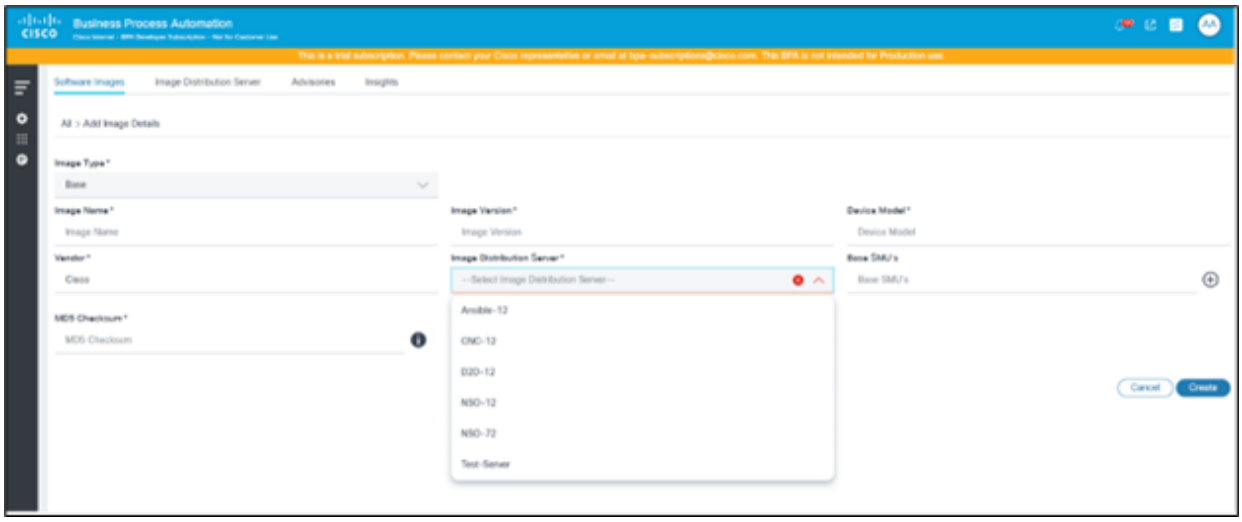
Note: O FMC não associa as informações do modelo aos metadados da imagem. Quando a sincronização estiver concluída, edite os respectivos metadados de imagem e atualize o modelo conforme necessário. O processo de atualização do FMC não funciona como esperado sem a atualização do modelo.

---

3. As imagens dos servidores remotos vManage têm inicialmente o Universally Unique Identifier (UUID) mapeado na coluna Version após a operação de sincronização. Os operadores devem editar manualmente os metadados de servidor remoto necessários e atualizá-los com a versão de imagem apropriada. Se esse mapeamento não for feito, outros componentes de Upgrade do SO (por exemplo, conformidade de software, políticas de upgrade, jobs de upgrade, etc.) não funcionarão como esperado.
4. Para agendar a sincronização automática de metadados SWIM em intervalos regulares, consulte Configuração de Implantação.

Adição de Metadados de Imagem de Software

1. Selecione o ícone More Options > Add Image Details. A página Adicionar detalhes da imagem é exibida.



Adicionar detalhes da imagem

2. Insira informações nos seguintes campos:

- Tipo de Imagem: O tipo de imagem (por exemplo, base, SMU, EPLD)
- Nome da imagem: Nome do arquivo de imagem; os usuários podem inserir um caminho relativo ou absoluto da imagem no campo Nome. Se os usuários fornecerem um caminho absoluto, a imagem é buscada diretamente desse caminho; se os usuários fornecerem um caminho relativo, o sistema resolverá o caminho completo adicionando o caminho base definido no servidor do repositório durante a distribuição
- Versão da imagem: Versão do software da imagem
- Modelo do dispositivo: O modelo de dispositivo para o qual a imagem está sendo marcada

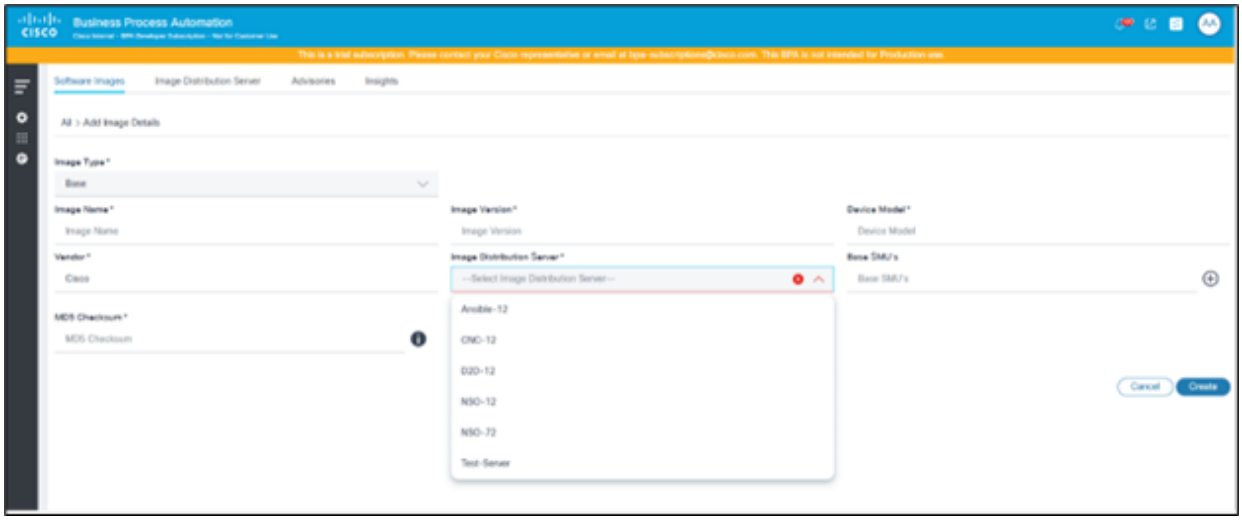
---

Note: O modelo do dispositivo deve corresponder às informações do modelo fornecidas pelo CNC, NSO, Direct-To-Device ou controlador ANSIBLE para dispositivos aplicáveis.

- Fornecedor: O fornecedor ou fornecedor que publicou a imagem; o padrão é Cisco, mas pode ser alterado conforme necessário
- Servidor de distribuição de imagem: Selecione o servidor de distribuição de imagem que hospeda o arquivo de software indicado no campo Nome da imagem. Após a seleção de um servidor de distribuição de imagem, as imagens são geradas para todas as IDs de controlador associadas ao tipo de controlador especificado definido no servidor de distribuição de imagem. Se um usuário adicionar ou remover instâncias de controlador no servidor de distribuição de imagem, as imagens de software correspondentes serão adicionadas ou removidas dessas instâncias de controlador.
- SMUs base: UME presentes na imagem dourada de base; essa opção só será aplicável se o tipo de imagem for Base
- Soma de verificação MD5: Imagem de checksum MD5 para verificação

3. Clique em Criar. A notificação Progress é exibida seguida por uma mensagem de confirmação.

Note: Os metadados de imagem para SMUs de Bridge devem ser adicionados antes de serem usados em uma Política de Atualização. Para adicionar SMUs de ponte, selecione SMU na lista suspensa Tipo de imagem.



Adicionar metadados de imagem SMU de bridge

Metadados de imagem de software para carregamento em massa

	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

Arquivo CSV de exemplo com informações de imagem

1. Prepare um arquivo .csv com os detalhes de imagem necessários e os seguintes nomes de coluna:

- Nome da imagem
- Versão
- Modelo do dispositivo
- Fornecedor
- Tipo de imagem

Note: Somente valores Base, SMU e EPLD são suportados.

- Servidor de distribuição de imagem
- Soma de verificação MD5

2. Selecione o ícone Mais Opções > Carregamento em Massa. A janela Carregar imagem em massa é aberta.

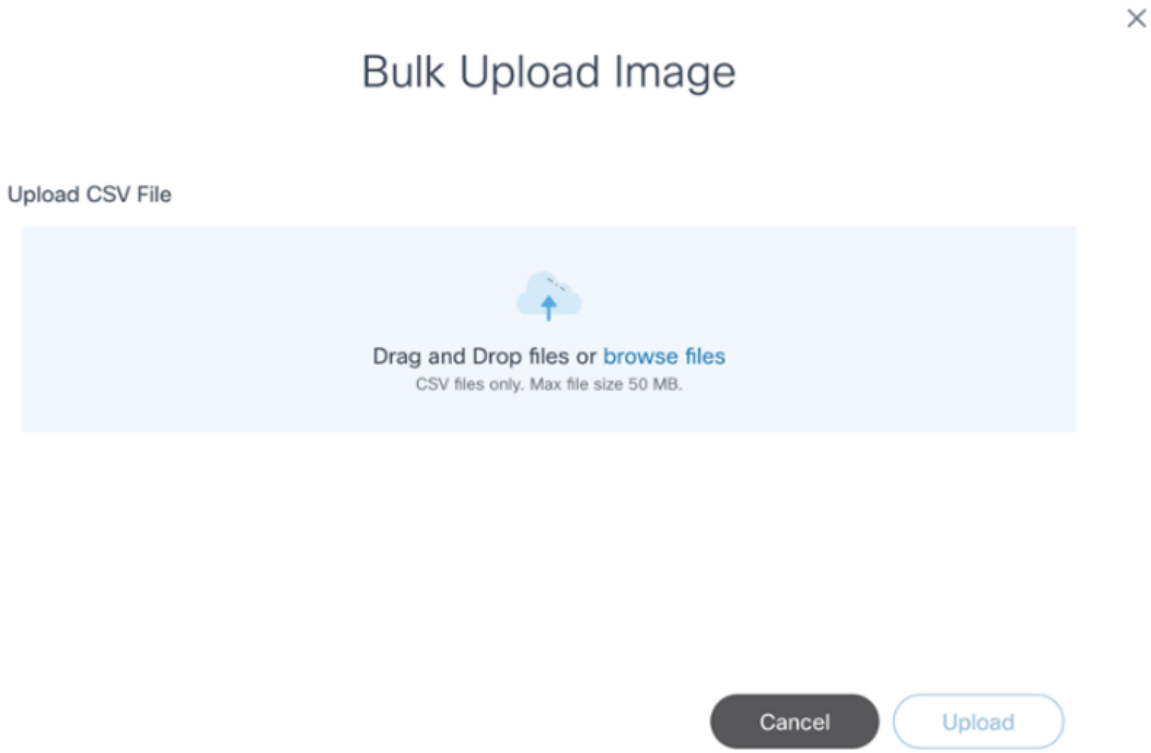


Imagem para carregamento em massa

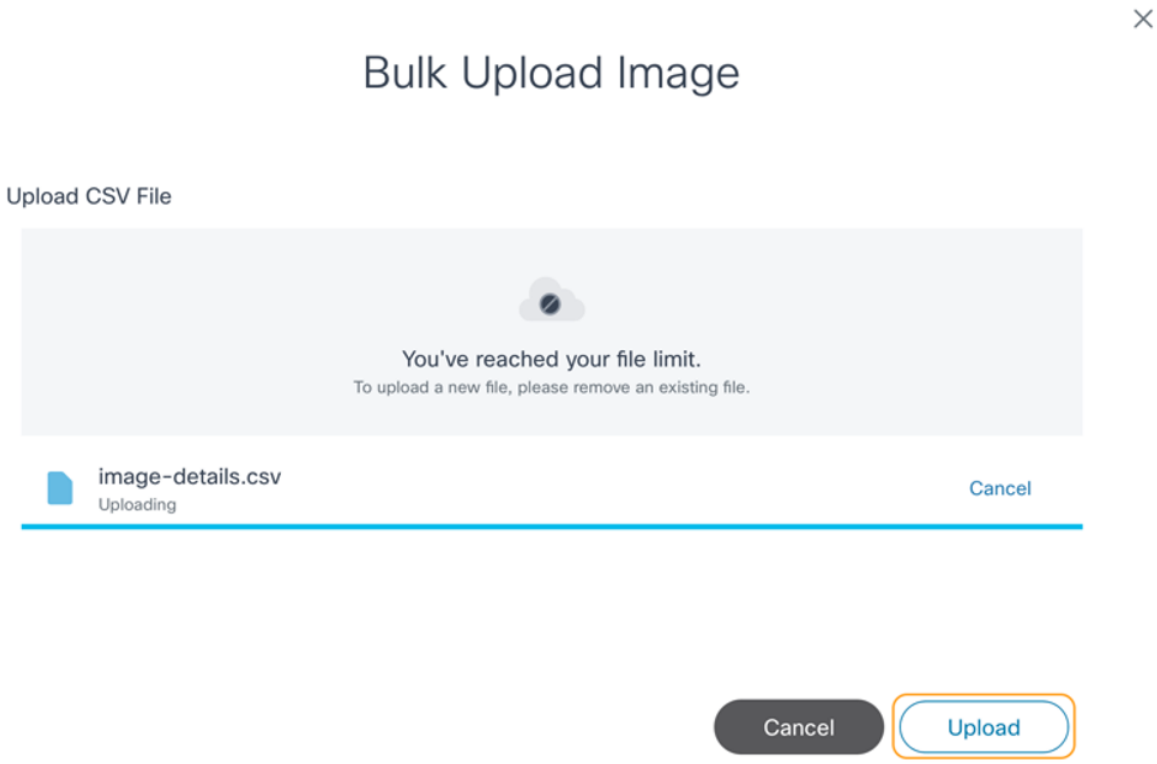
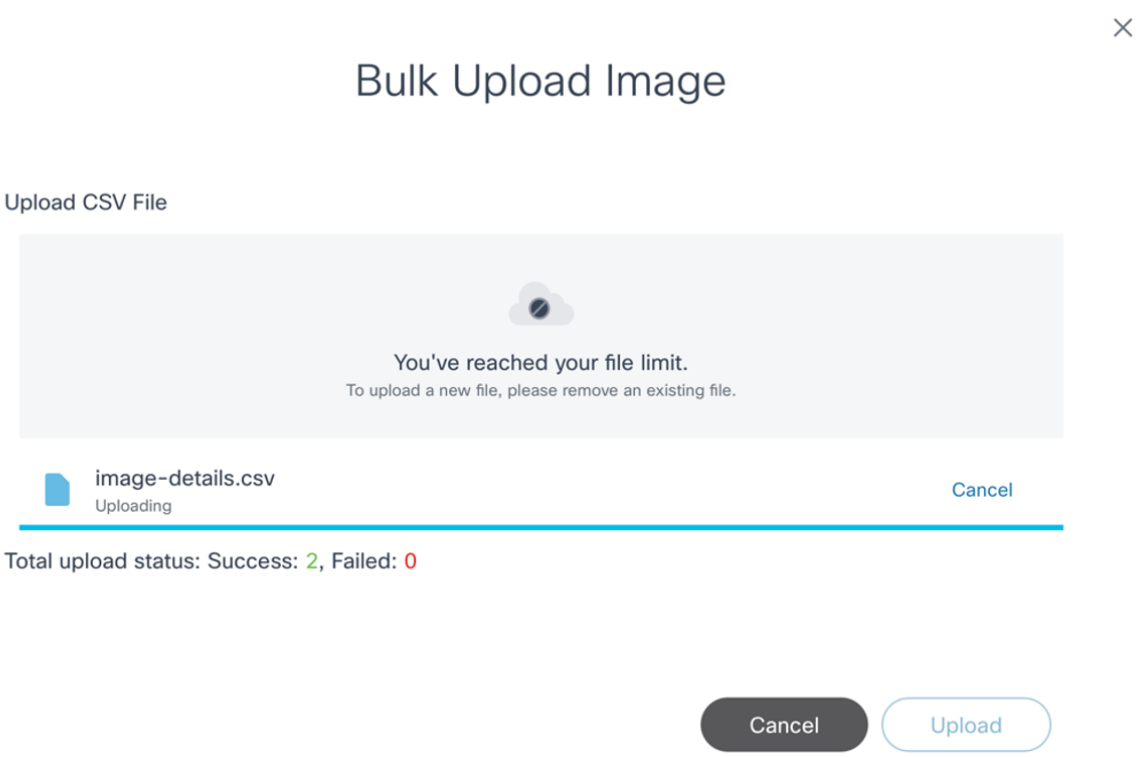


Imagem de carregamento em massa - Carregamento CSV

3. Selecione um arquivo .csv preparado e clique em Carregar. Os detalhes da imagem do .csv

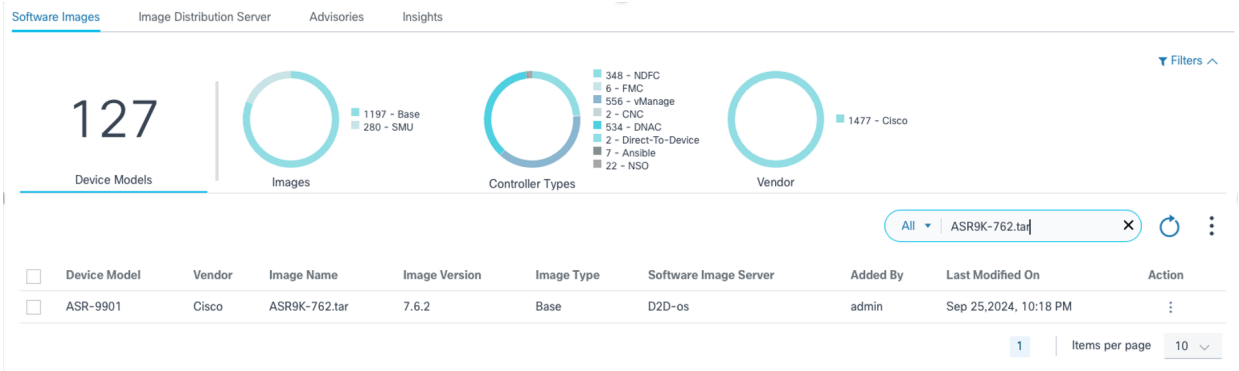
são validados e processados. Quando o arquivo for carregado, o status final do carregamento em massa será exibido.



Status de carregamento de imagem em massa bem-sucedido

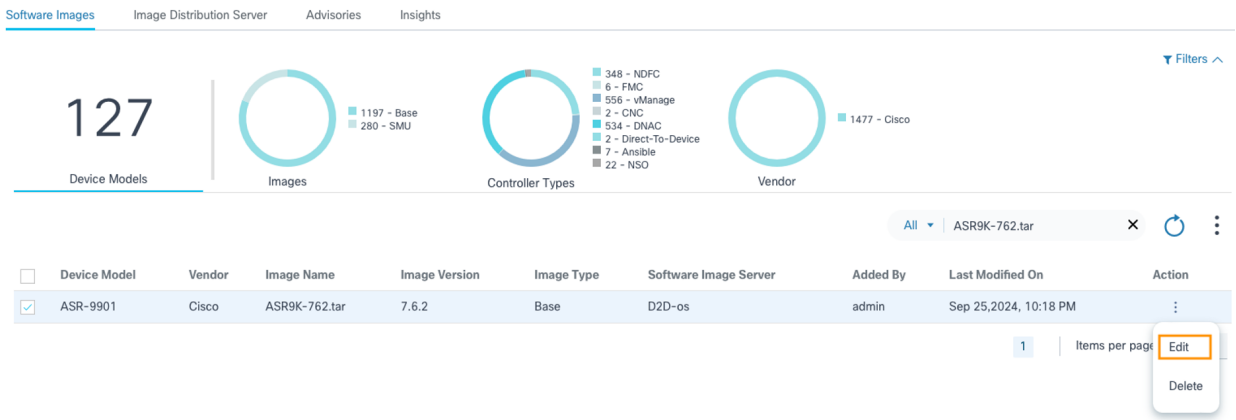
Note: No caso de erros de validação de dados (por exemplo, registros duplicados ou parâmetros inválidos), as mensagens de erro são exibidas como uma grade na janela Bulk Upload Image. Os usuários podem corrigir os valores no arquivo .csv e carregá-lo novamente.

Edição de metadados de imagem de software existentes



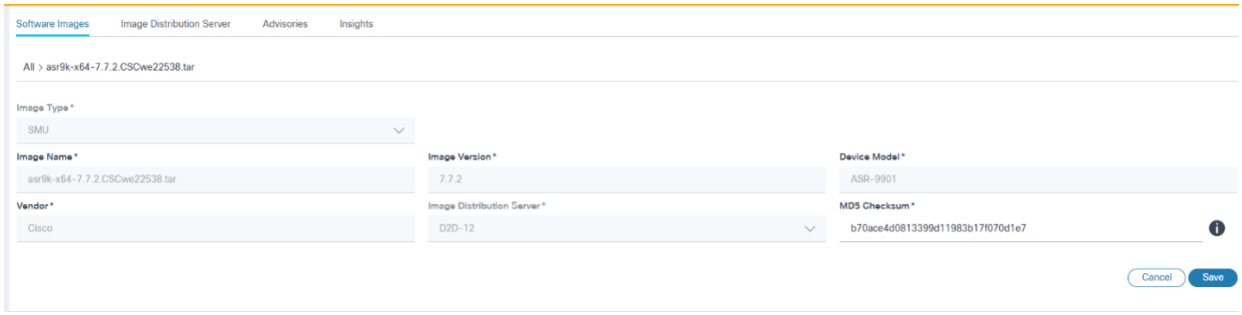
Pesquisar nos metadados da imagem do software

1. Localize a imagem que precisa ser atualizada usando o filtro Search.



Editar

2. Na coluna Ação da imagem desejada, selecione o ícone Mais Opções > Editar.



Editar imagens de software

3. Atualize os parâmetros necessários e clique em Salvar para salvar as alterações ou clique em Cancelar para descartá-las. A notificação de progresso é exibida seguida por uma mensagem de confirmação da atualização da imagem.

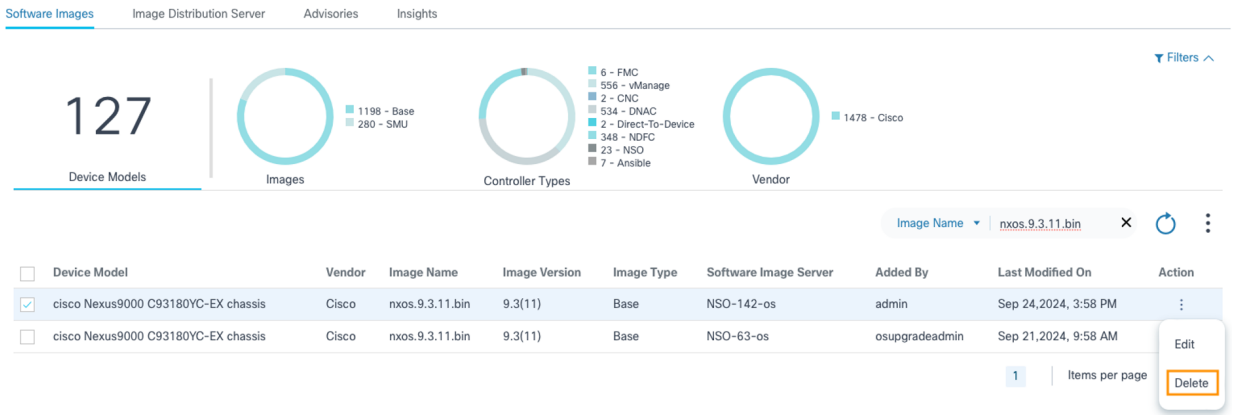
Note: A lista a seguir deve ser anotada.

- A edição está disponível para controladores CNC, NSO, D2D, ANSIBLE, FMC e vManage (aplicável apenas para metadados de imagem de servidor remoto)
- A atualização do modelo de dispositivo só é suportada para imagens de servidor remoto do vManage
- Somente o campo Versão do software pode ser atualizado para metadados de imagem do servidor remoto vManage
- Para imagens vManage, os usuários podem visualizar o servidor de imagens de software no lugar de instâncias do controlador

Excluindo metadados de imagem de software

Pesquisar nos metadados da imagem do software

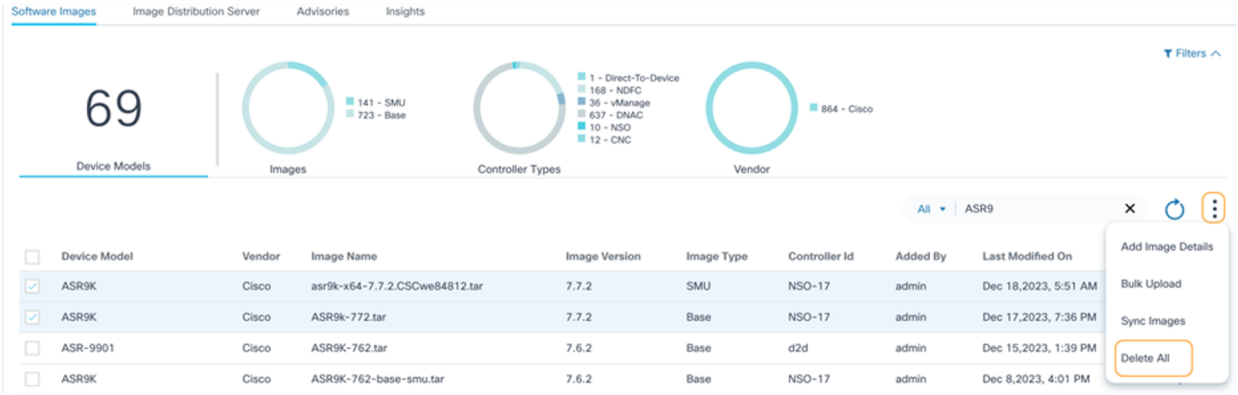
1. Use o campo Pesquisar para localizar uma imagem desejada.



excluir

2. Na coluna Ação da imagem desejada, selecione o ícone Mais Opções > Excluir para excluir uma imagem.

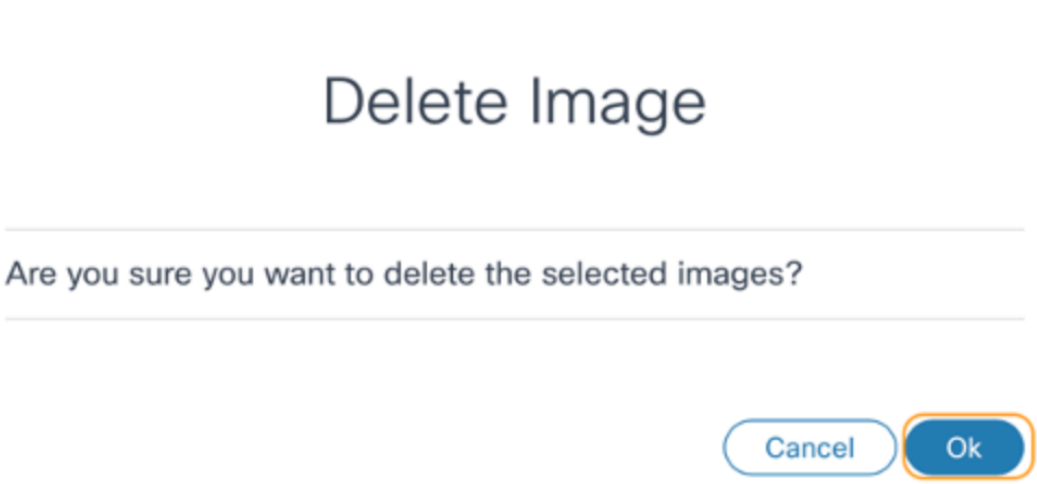
OU



Excluir tudo

Selecione as imagens desejadas e selecione o ícone Mais Opções > Excluir Tudo para excluir várias imagens.

Uma confirmação é exibida.



Confirmação

3. Click OK. Uma notificação de progresso é exibida seguida por uma mensagem de confirmação.

Note: A lista a seguir deve ser anotada.

- Os metadados de imagem só podem ser adicionados para controladores NSO, ANSIBLE, Direct-to-Device e CNC. Para todos os outros controladores corporativos, o recurso SWIM integrado é aproveitado e as imagens são descobertas a partir dos respectivos controladores
- Não há suporte para o recurso de descoberta de imagem nos servidores de imagem das controladoras NSO, ANSIBLE, Direct-to-Device e CNC.
- Por padrão, os metadados da imagem do servidor remoto vManage contêm UUID para o parâmetro de versão pós-sincronização. Os usuários devem editar os metadados e atualizar o UUID com a versão correspondente. A versão de imagem correspondente pode ser identificada no controlador do vManage ou fazendo login no dispositivo onde a imagem existe.

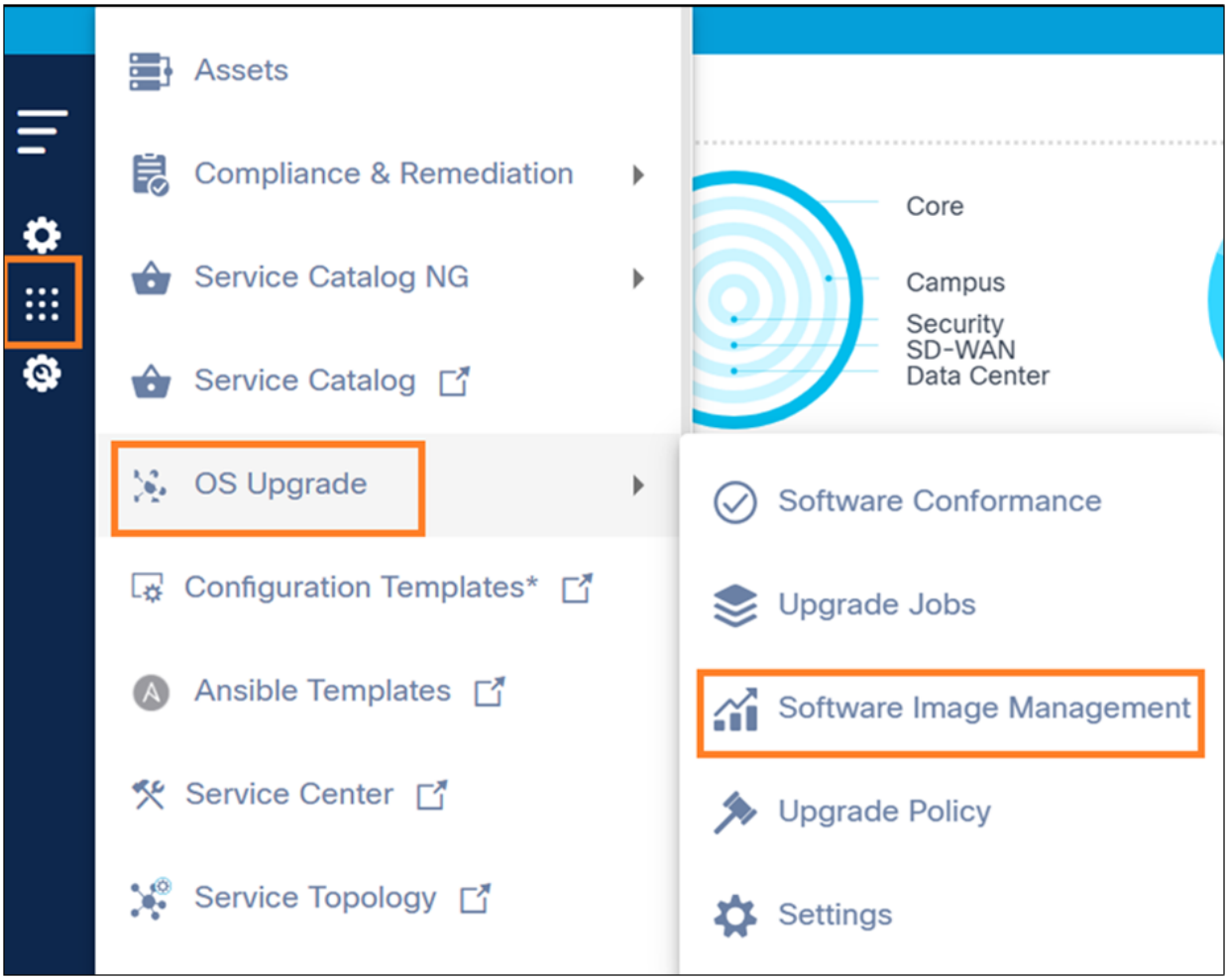
Gerenciamento do servidor de distribuição de imagens

Servidor de distribuição de imagem

O componente permite que os usuários de operações mantenham os detalhes do servidor do repositório de imagens para controladores CNC, NSO, ANSIBLE, FMC e Direct-To-Device que não tenham suporte de gerenciamento do repositório de imagens OOB.

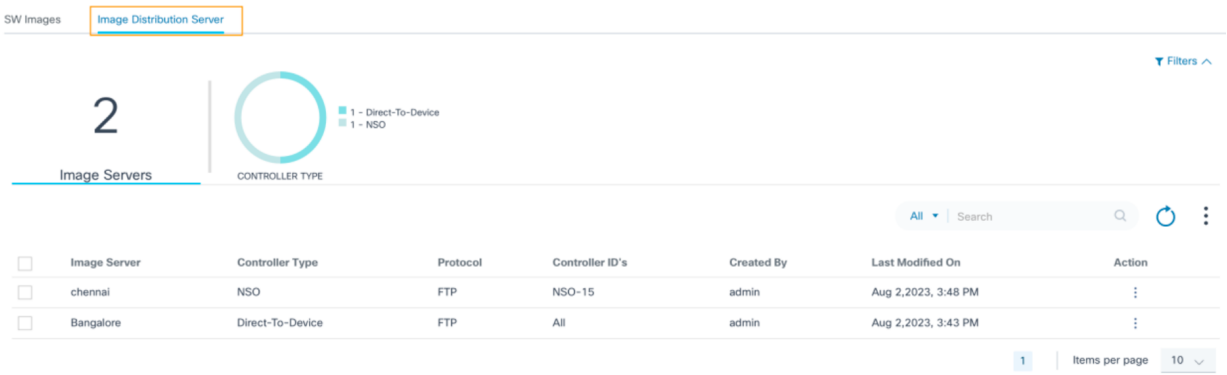
Para acessar a página Servidor de distribuição de imagem:

1. Faça login no BPA com credenciais que tenham acesso de gerenciamento ao Servidor de distribuição de imagem.



Gerenciamento de imagens de software

2. Selecione OS Upgrade > Software Image Management.



Guia Servidor de distribuição de imagens

3. Clique na guia Servidor de distribuição de imagem.

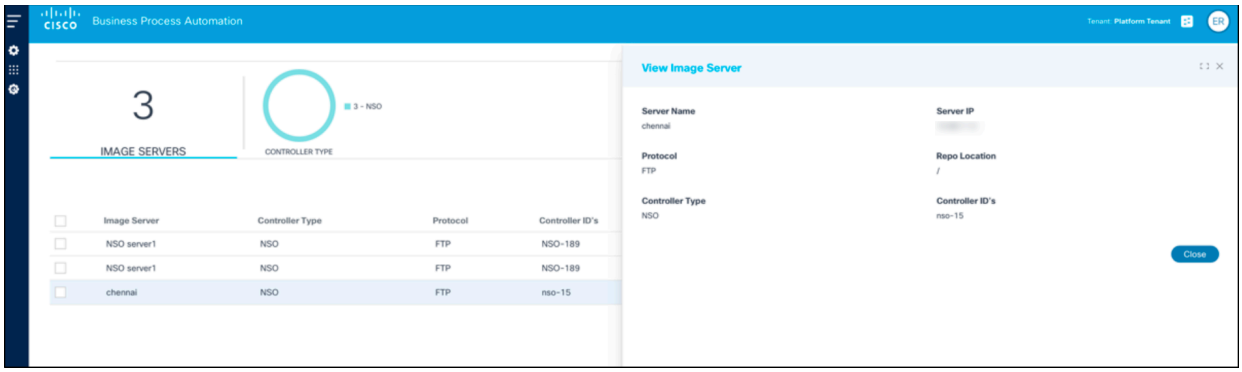
A guia Servidor de distribuição de imagem contém o seguinte:

- Uma seção de análise, exibida na parte superior, que fornece o seguinte:
    - O número total de servidores de imagem integrados nesta instância do BPA
    - Um filtro rápido tipo controlador que permite filtrar servidores de imagem com base no tipo de controlador (por exemplo, NSO, Direct-to-Device, CNC, ANSIBLE, FMC); o número indica o número total de servidores de distribuição de imagem associados a esse tipo de controlador
- Um ícone Mais Opções que fornece as seguintes funcionalidades:
    - Adicionar servidor de imagem: Adicionar novo servidor de distribuição de imagem
    - Excluir tudo: Exclusão em massa de servidores de distribuição selecionados
- Um filtro de Pesquisa que pode ser usado para pesquisar os servidores de distribuição e inclui os seguintes filtros de pesquisa exclusivos:
    - Todos: Pesquisa em todos os campos
    - Servidor de imagem: Procura servidores com um nome de servidor específico
    - ID do controlador: Procura servidores associados a uma ID de controladora específica
- Um ícone Atualizar que pode ser usado para atualizar a página e limpar os filtros selecionados
- Os servidores de distribuição existentes são exibidos em uma tabela de grade com as seguintes colunas:
- Servidor de imagem: Nome exclusivo do servidor do repositório
    - Tipo de controlador: O tipo de controlador ao qual este servidor de imagem é aplicável
    - Protocolo: Protocolo de cópia suportado pelo servidor do repositório

---

Note: Somente FTP, SCP e SFTP são suportados

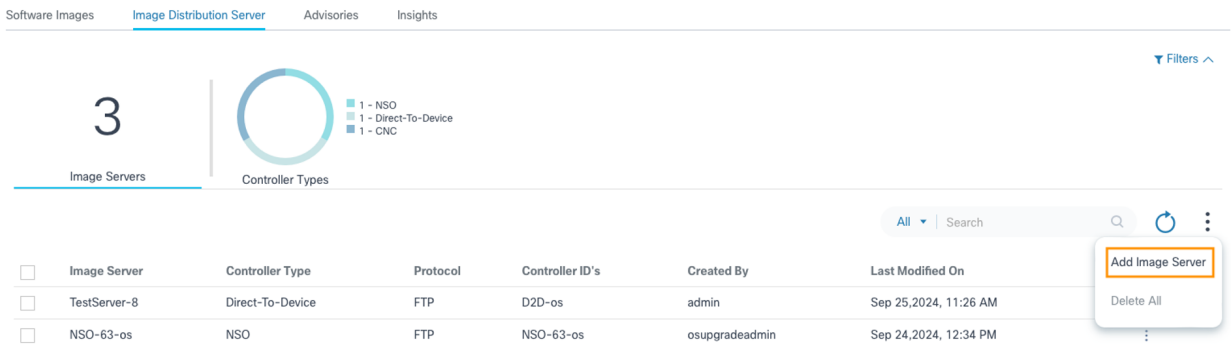
- IDs do controlador: Instâncias do controlador para as quais o servidor de repositório atual é utilizável ou aplicável; instância de controlador refere-se aos dispositivos gerenciados por meio desse controlador
- Criado por: O usuário que integrou o servidor de repositório
- Última modificação em: Carimbo de data/hora de quando os detalhes do servidor foram atualizados pela última vez
- Ação: Fornece ações específicas de linha, como Editar e Excluir



Painel Exibir servidor de imagem

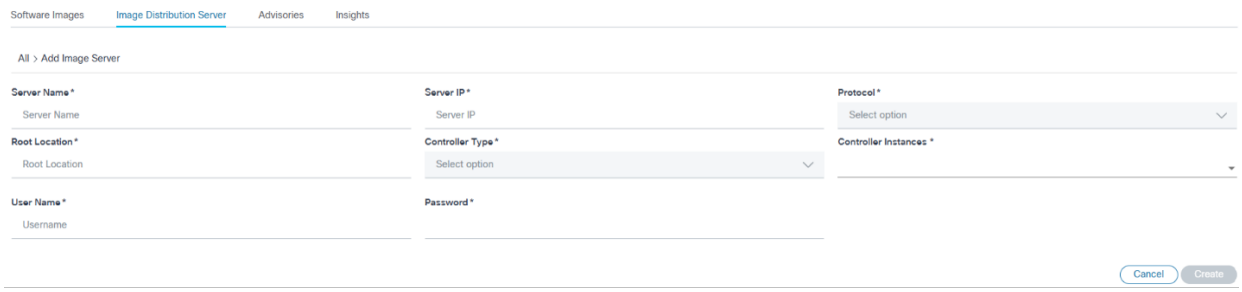
- Clicar em uma linha abre a janela View Image Server

Adicionando detalhes do servidor de imagem

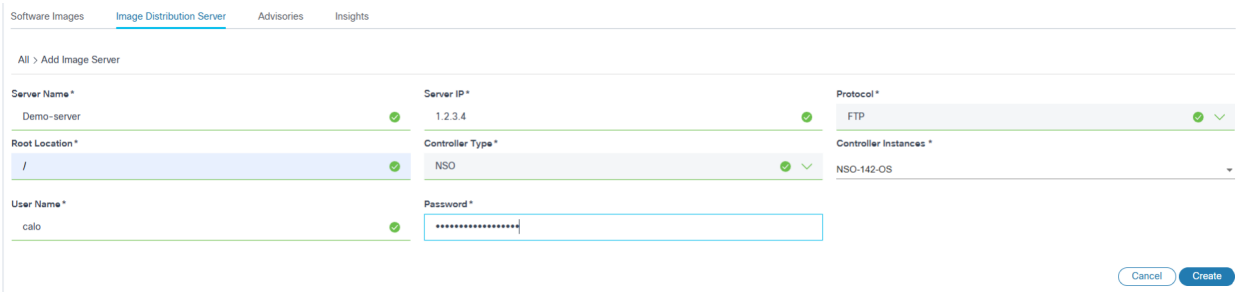


Adicionar servidor de imagem

4. Selecione o ícone More Options > Add Image Server. A página Adicionar servidor de imagem é exibida.



Adicionar detalhes do servidor de imagem



Adicionar servidor de imagem com detalhes de exemplo

5. Insira informações nos seguintes campos:

- Nome do servidor: Nome exclusivo do servidor do repositório de imagens
- IP do servidor: Endereço IPv4 do servidor do repositório

Note: Certifique-se de que esse IP esteja acessível a partir dos dispositivos de rede antes de adicionar.

- Protocolo: Suportado pelo servidor do repositório de imagens para a cópia de imagem

Note: Somente protocolos FTP, SCP e SFTP são suportados.

- Local do repositório: Caminho base dos arquivos de imagem no servidor do repositório

Note: Se os arquivos de imagem estiverem presentes na raiz da pasta do repositório do servidor de imagem, "/" funcionará como um valor.

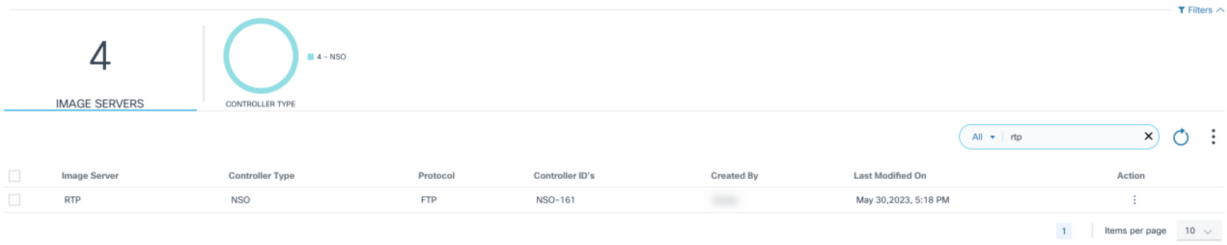
- Tipo de controlador: Tipo de controlador ao qual o servidor de imagem atual é aplicável

Note: Somente NSO, Direct-To-Device, CNC e ANSIBLE são suportados.

- Instâncias do Controlador: Uma ou mais instâncias do controlador aplicáveis com base nos dispositivos que eles gerenciam para os quais o servidor de repositório de imagens fornecido deve ser usado para copiar a imagem
- Usuário: Credenciais personalizadas a serem usadas para acessar os arquivos de imagem do repositório

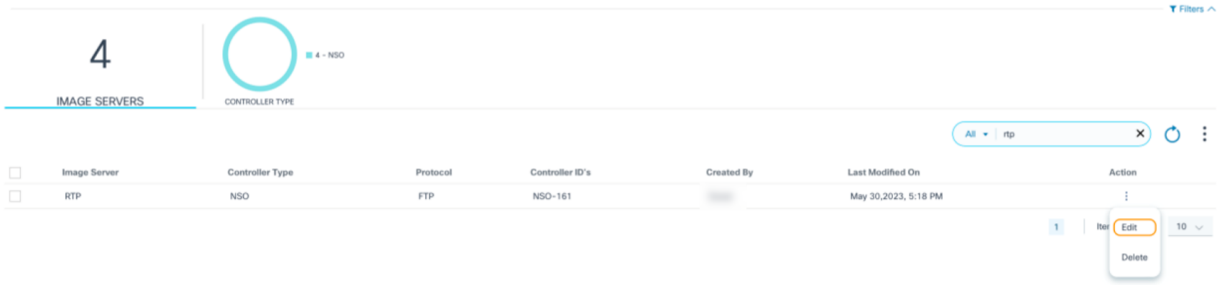
6. Clique em Criar. A notificação do progresso é exibida seguida por uma mensagem de confirmação.

Edição de detalhes do servidor de imagem



Pesquisa do servidor de imagem

7. Usando o campo Pesquisar, localize o servidor de distribuição que precisa ser atualizado.

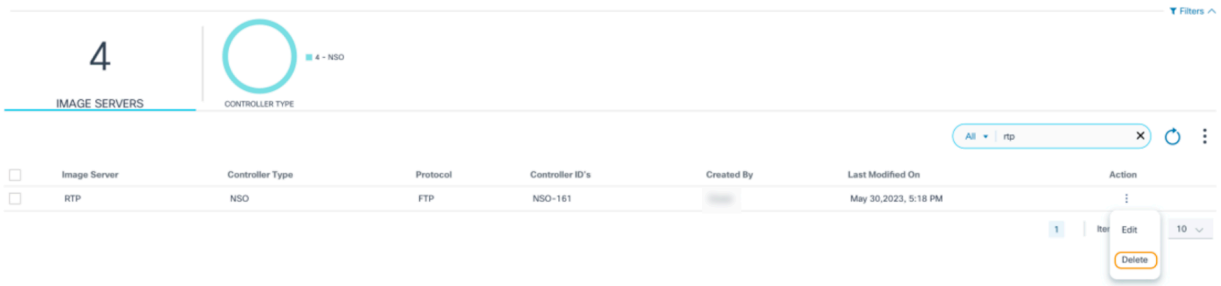


Editar servidor de imagem

8. Na coluna Ação, selecione o ícone Mais Opções > Editar.
9. Atualize os parâmetros necessários.
10. Click Save. A notificação de andamento é exibida seguida por uma mensagem de confirmação.

Excluindo detalhes do servidor de imagem

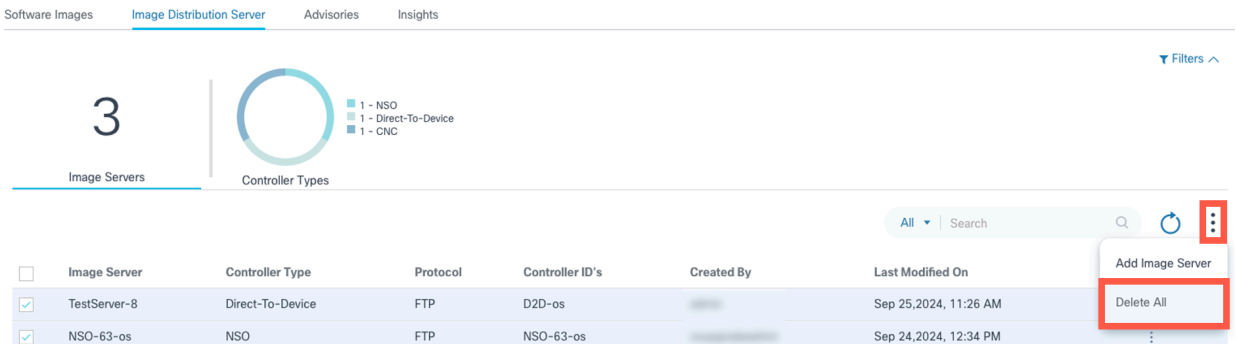
1. Usando o filtro Search, localize o(s) servidor(es) desejado(s).



Excluir servidor de imagem

2. Na coluna Ação, selecione o ícone Mais Opções > Excluir para excluir um único servidor de distribuição.

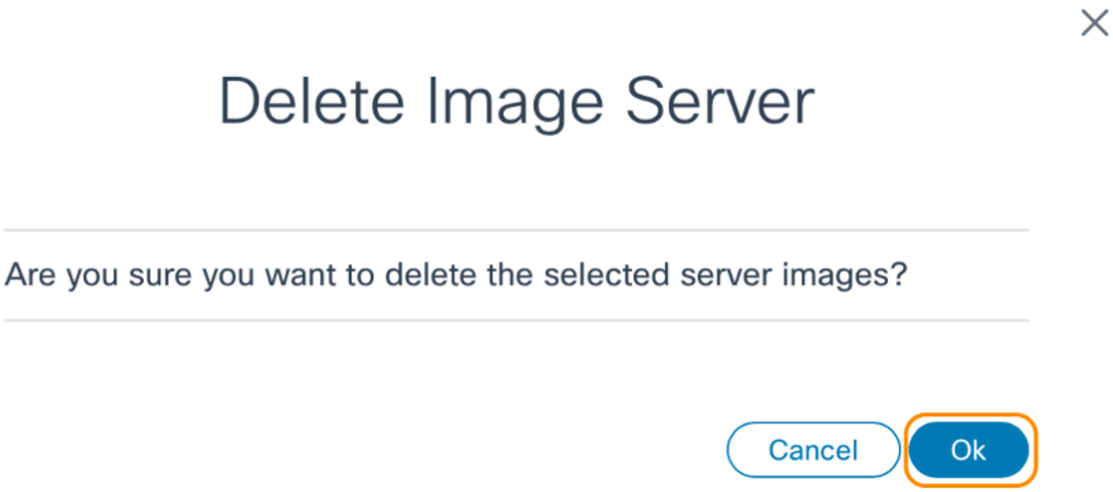
OU



Excluir vários servidores de imagem

Selecione os servidores desejados e selecione o ícone Mais Opções > Excluir Tudo para excluir vários servidores de distribuição.

Uma confirmação é exibida.



Confirmação de exclusão

3. Click OK. As notificações de andamento são exibidas seguidas por uma mensagem de confirmação.

Informações sobre software

O Software Insights descobre todas as vulnerabilidades de segurança, como avisos de segurança, bugs e software no fim da vida útil expostos pelos ativos de rede. Ele também fornece sugestões de software para os modelos de dispositivos gerenciados pelos controladores Cisco Catalyst Center e NDFC. Ele permite que os usuários administradores selecionem a versão de software sugerida para ativos de rede e cria uma política de conformidade para os modelos de

dispositivo, se a sugestão estiver disponível.

Pré-requisitos

- Ative o Adaptador para obter insights. O Adaptador para o servidor de insights da Cisco, chamado "Cisco-Insights-Adapter", está disponível no OOB. Para integrar com alguns servidores externos do Insights de terceiros, os Adaptadores correspondentes precisam ser criados. Consulte Configuring Insights Adapter no Guia do Desenvolvedor BPA para obter mais informações.
- A conectividade com a Internet é necessária para que o sistema BPA se conecte à nuvem da Cisco.
- Verifique se client_id e client_secret estão na configuração do Adaptador antes de continuar com a operação de sincronização.
- Se necessário, o proxy para a Internet pode ser configurado seguindo as etapas abaixo.
- Para o Tipo de SO IOS-XR, o mapeamento personalizado da série para o modelo do dispositivo pode ser feito no Reference Data Management (RefD), conforme necessário. Para obter mais informações sobre o mapeamento personalizado de série para modelo, consulte o Guia do Desenvolvedor BPA.
- Os BPA Kubernetes Pods precisam de acesso à Internet para reunir as recomendações, bugs e detalhes de fim de vida útil da Cisco. Se a rede BPA não tem acesso direto à internet, mas está disponível via proxy, use as etapas abaixo para fazer com que os Kubernetes Pods usem o proxy para internet.

1. Atualize o script com o endereço de proxy real no lugar de **<<**http://proxy-domain.com:port**>>**.
2. Configure os parâmetros de ambiente para cada pod nos gráficos de implantação YAML ou helm.
3. Execute o script abaixo no nó Kubernetes adicionando todos os nomes de deployment na configuração NO_PROXY ou no_proxy.

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



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



      >”
https_proxy=”<



       >”
```

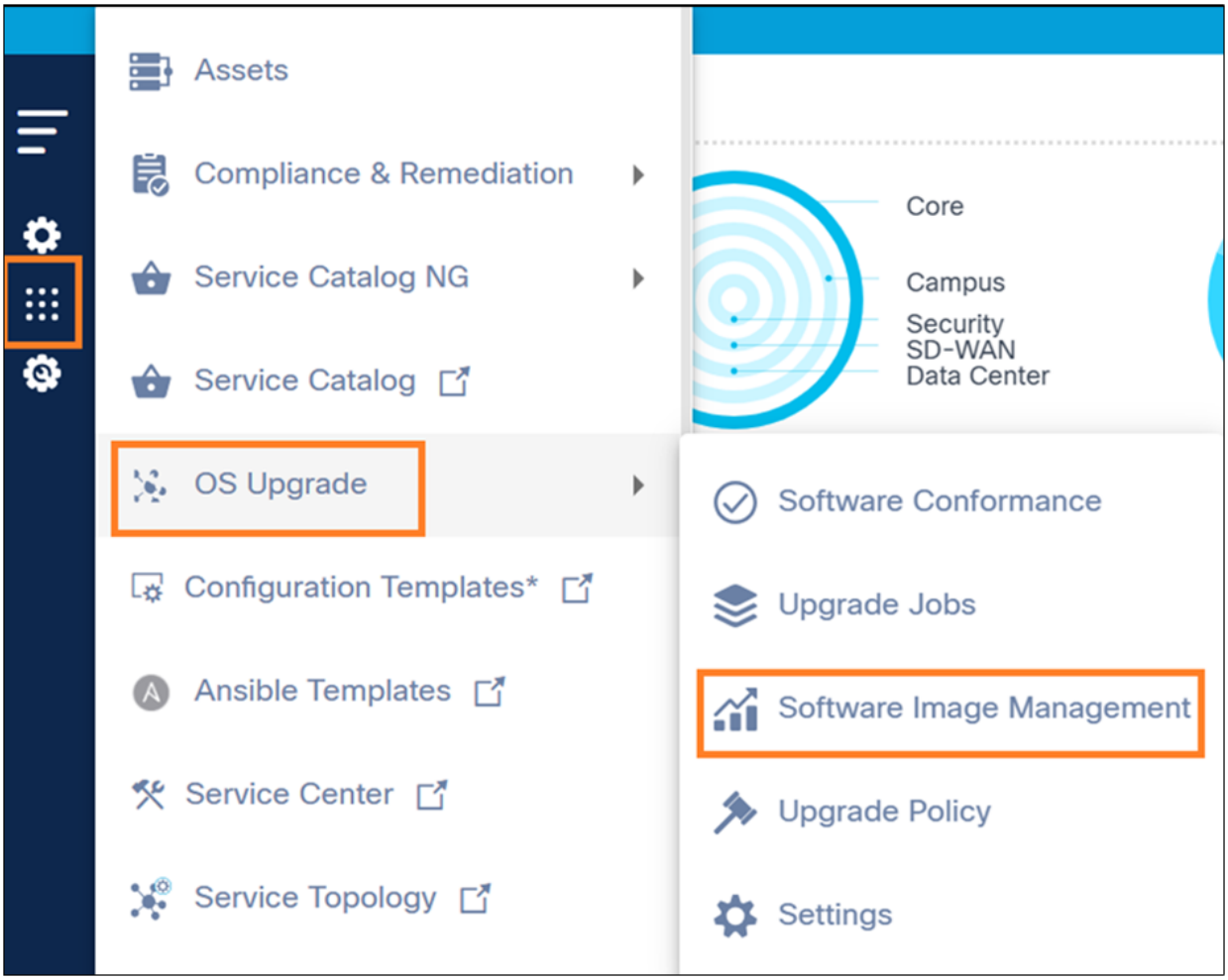
```
NO_PROXY="*.svc,localhost,127.0.0.1,192.168.0.0/16,10.0.0.0/8,172.16 .0.0/12,adaptor-builder,agent-mana

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
```

Note: Ao configurar o proxy conforme descrito acima, o Adaptador pode acessar a rede da Cisco e baixar os dados necessários do Software Insights no BPA. Para se conectar a qualquer outro servidor externo do Insights diretamente sem um proxy, certifique-se de adicioná-los à variável no_proxy.

Buscando dados de insights de software no BPA

Para sincronizar dados de insights de software no BPA:

1. Faça login no BPA com credenciais que tenham acesso aos dados de insights de software de sincronização.



Navegação de gerenciamento de imagem de software

2. Selecione OS Upgrade > Software Image Management no painel lateral.

Guia Recomendações

3. Clique na guia Recomendações.

Sincronizar para buscar insights de software no BPA

Sincronizar para buscar insights de software no BPA

4. Clique em Sincronizar.

Ele descobre todas as recomendações de segurança, bugs prioritários, boletins de fim da vida útil

e sugestões de software relacionadas aos ativos presentes no inventário. As recomendações de segurança e as datas de fim da vida útil do software são determinadas com base no tipo de SO e na versão do software. Os bugs de prioridade e as sugestões de software são determinados com base na ID do produto e na versão do software.

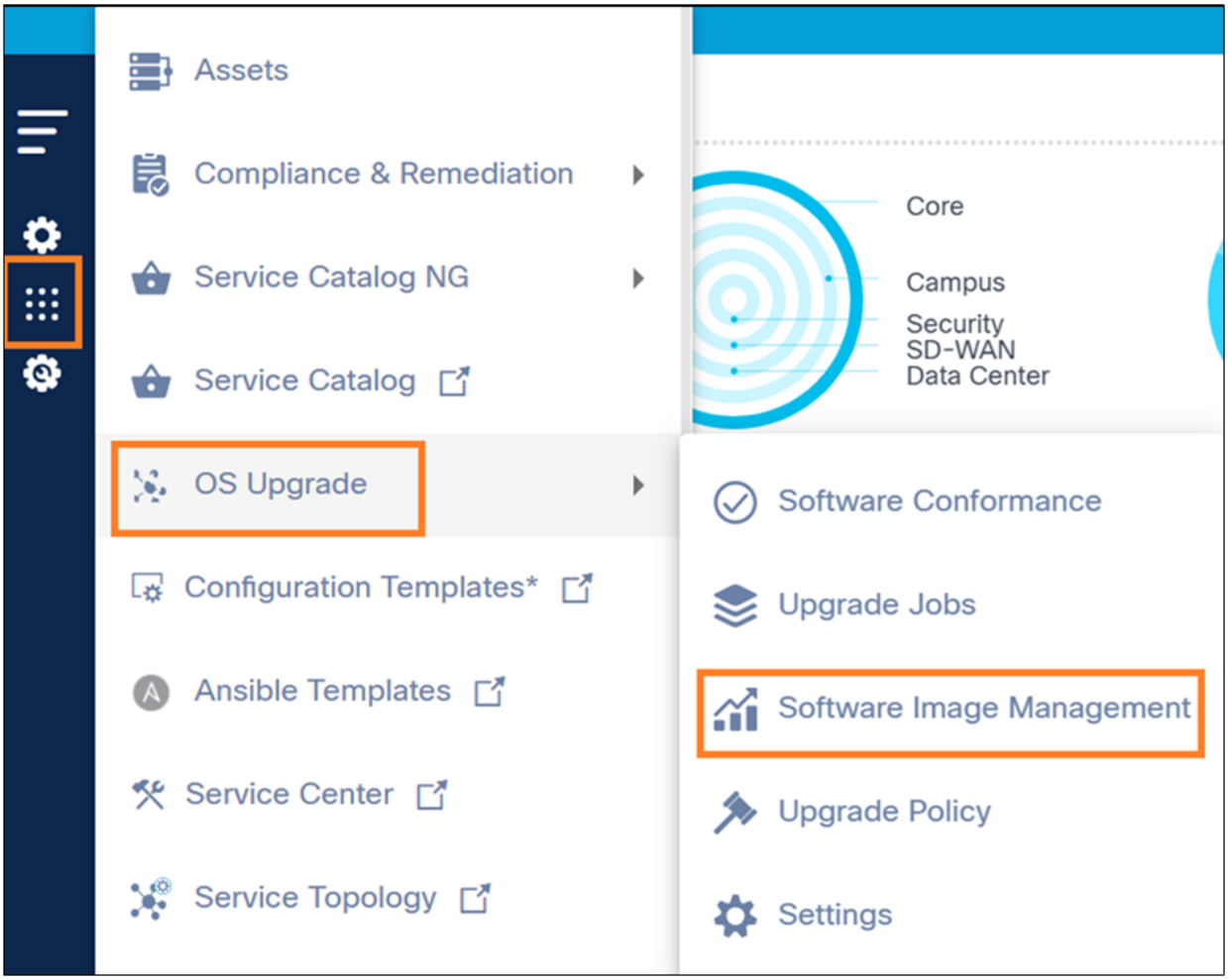
Última atualização mostra a data e a hora em que os dados de insights foram sincronizados pela última vez, e o campo Status da sincronização exibe o último status da sincronização.

Note: Todas as recomendações, bugs, notas de versão e sugestões aplicáveis são buscados na nuvem da Cisco através do arquivo "Cisco-Insights-Adapter".

Exibindo e Gerenciando Recomendações de Segurança

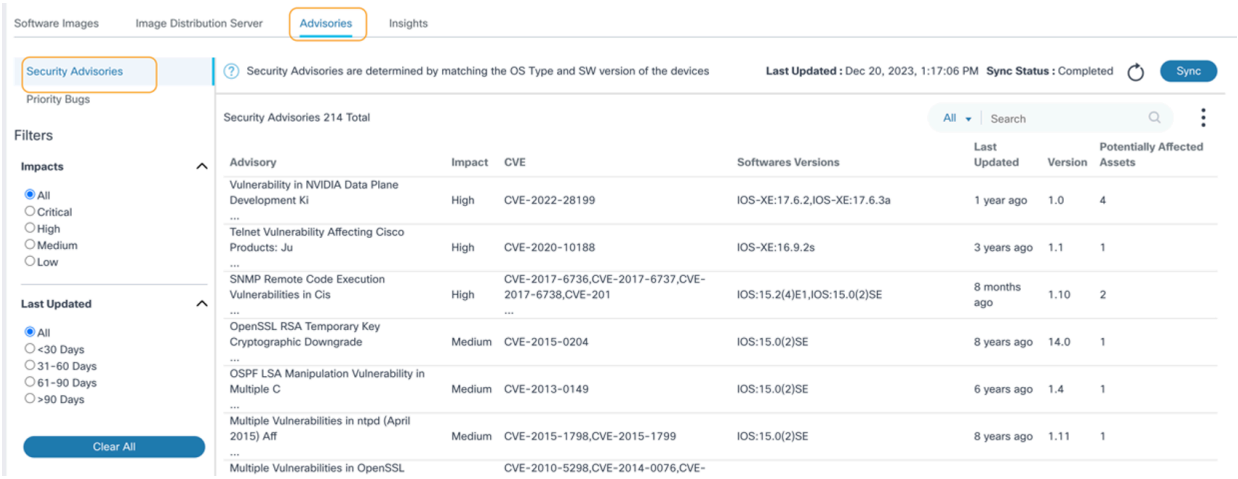
Para acessar a página Recomendações:

1. Efetue login no BPA com credenciais que tenham acesso de gerenciamento aos Supervisores.



Navegação de gerenciamento de imagem de software

2. Selecione OS Upgrade > Software Image Management.



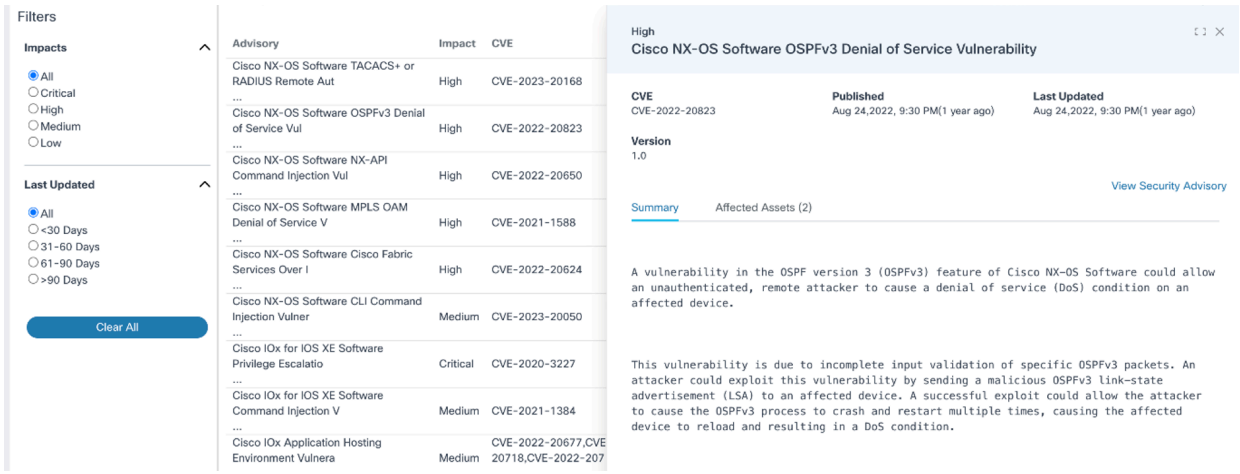
Orientações de Segurança

3. Clique na guia Recomendações. A página Avisos de segurança é aberta por padrão.

As seguintes opções são exibidas para filtrar dados de avisos:

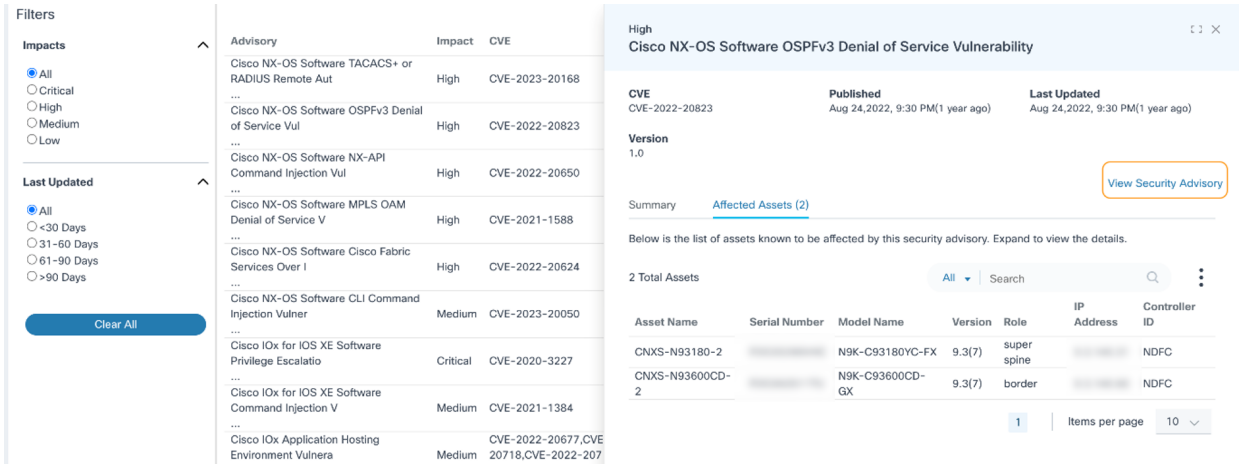
- Impactos permitem filtrar com base na severidade do aviso; Tudo é selecionado por padrão
- Última atualização permite a filtragem com base na data da última atualização do consultivo; Tudo é selecionado por padrão
- Limpar tudo redefine os filtros selecionados
- O filtro Pesquisar é usado para pesquisar as recomendações e inclui os seguintes filtros de pesquisa exclusivos:
- Todos: Pesquisa em colunas como Advisory, CVE e Software Versões
- Consultoria: Procura recomendações com os termos especificados na pesquisa
- CVE: Pesquisa recomendações com Vulnerabilidades e Exposições Comuns (CVE) específicas
- Versões de software: Procura recomendações associadas a tipos específicos de SO ou versões de software
- O ícone Atualizar é usado para atualizar a página e limpar os filtros selecionados
- As recomendações existentes são exibidas com as seguintes colunas:
    - Consultoria: Síntese do parecer
    - Impacto: Severidade de supervisão
    - CVE: CVEs atribuídos
    - Versões de software: Tipo de SO e versões de software afetados
    - Última atualização: Data e hora da última atualização do aviso
    - Versão: Versão consultiva
    - Ativos potencialmente afetados: Número de ativos que podem ser afetados pela consultoria
- Clicar no campo do cabeçalho classifica as recomendações

Note: A classificação não é uma opção para ativos potencialmente afetados.



View Detalhada de Recomendação

- A seleção de uma linha de recomendação abre uma view detalhada de recomendação que inclui as seguintes guias:
    - Resumo: Exibe um resumo da recomendação selecionada; é exibido por padrão
    - Ativos afetados: Exibe detalhes de ativos potencialmente afetados, como Nome do ativo, Número de série, Nome do modelo, Versão do software, Endereço IP e ID do controlador; a classificação e a pesquisa dos ativos podem ser executadas nessa guia



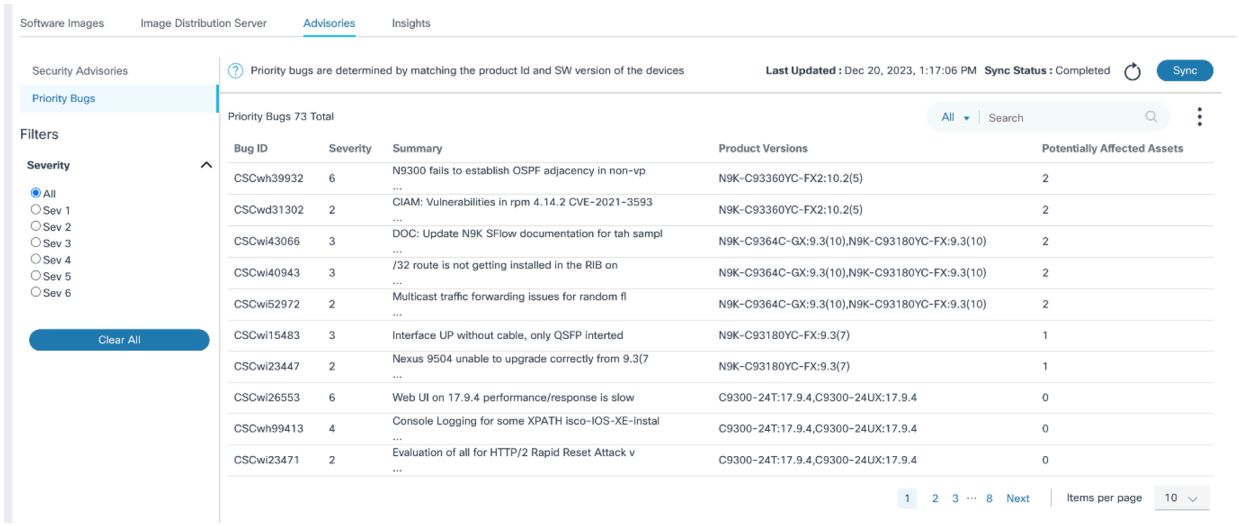
Exibir Consultoria de Segurança

- Link Exibir Aviso de Segurança: Navega para a página oficial Consultoria.

Exibindo e Gerenciando Bugs de Prioridade

Selecionar Erros de Prioridade

Depois de abrir a página Recomendações, conforme descrito na seção anterior, clique na guia Erros de prioridade. A página Erros de prioridade é exibida.

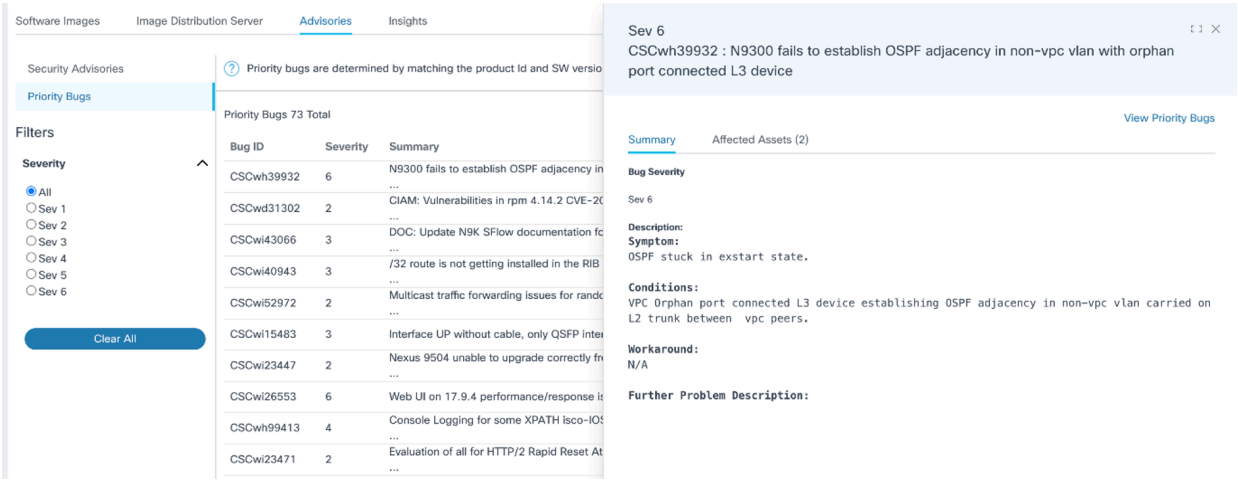


Erros de prioridade

As seguintes opções estão disponíveis na página Erros de prioridade:

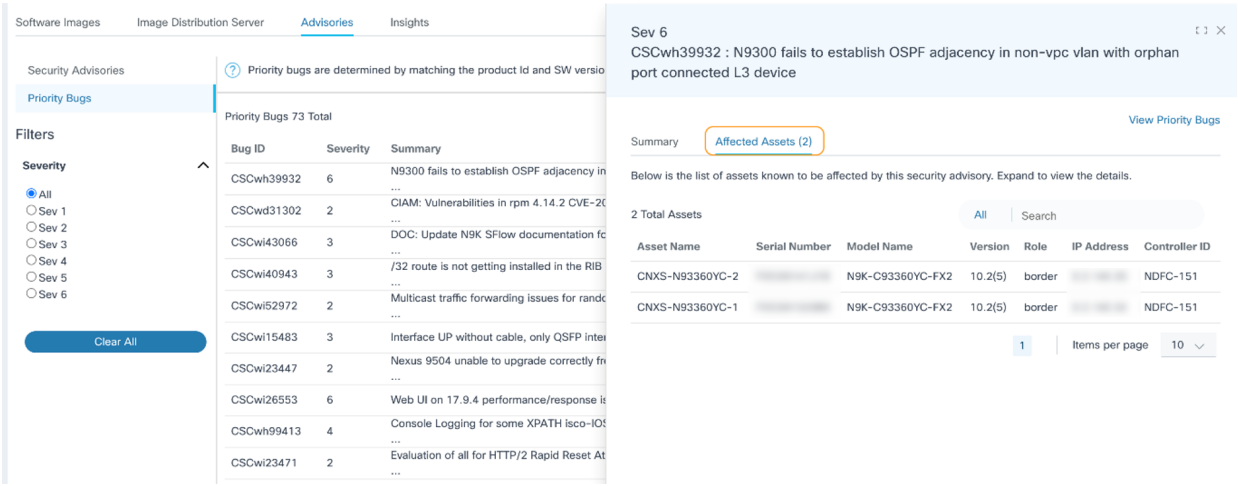
- Um filtro de severidade que permite a filtragem com base na severidade do bug; Tudo é selecionado por padrão
- O filtro Search pode ser usado para pesquisar os bugs e inclui os seguintes filtros de pesquisa exclusivos:
    - Todos: Pesquisa em todos os campos
    - ID do bug: Procura bugs com uma ID de bug especificada
    - Resumo: Procura bugs com palavras-chave específicas presentes no resumo
    - Versões do produto: Procura bugs associados a uma ID de produto ou versão de software específica
- O ícone Atualizar pode ser usado para atualizar a página e limpar os filtros selecionados
- Os bugs de prioridade são exibidos na tabela com as seguintes colunas:
    - ID do bug
    - Severity: Severidade do bug
    - Resumo: Detalhes resumidos do bug
    - Versões do produto: ID do produto e versões de software afetadas
    - Ativos potencialmente afetados: Número de ativos que podem ser afetados pelo bug
- A classificação pode ser feita clicando em qualquer cabeçalho de coluna, exceto Ativos

potencialmente afetados



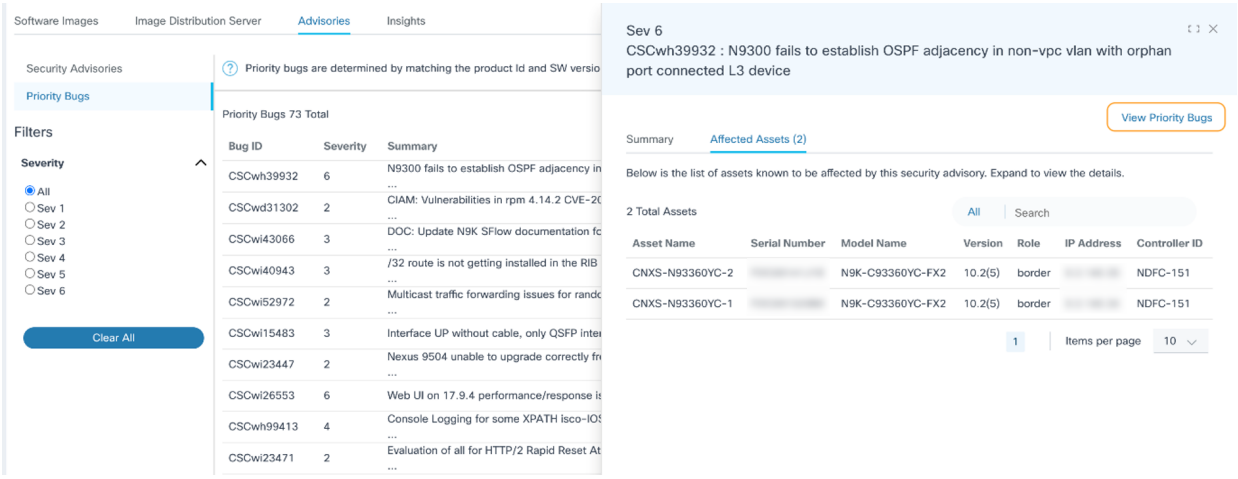
Visão de Detalhes do Erro

- Clicar em um bug abre a visualização detalhada do bug, que inclui o seguinte:
    - Guia Resumo: Exibe detalhes de Severidade do Bug, Descrição e Solução.



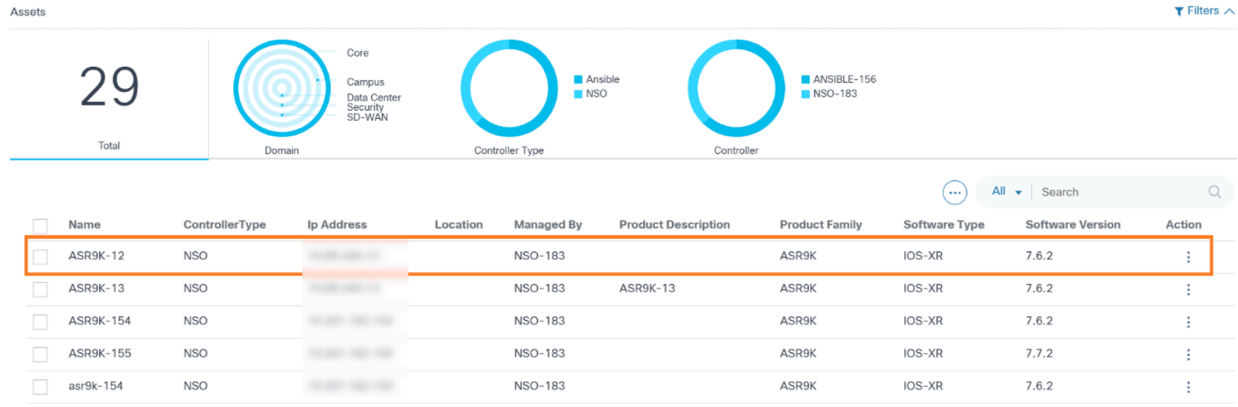
Guia Ativos afetados

- Guia Ativos afetados: Exibe todos os detalhes de ativos potencialmente afetados, como Nome do ativo, Número de série, Nome do modelo, Software Versão, Endereço IP e Controlador ID; a classificação e a pesquisa dos ativos podem ser executadas nessa guia



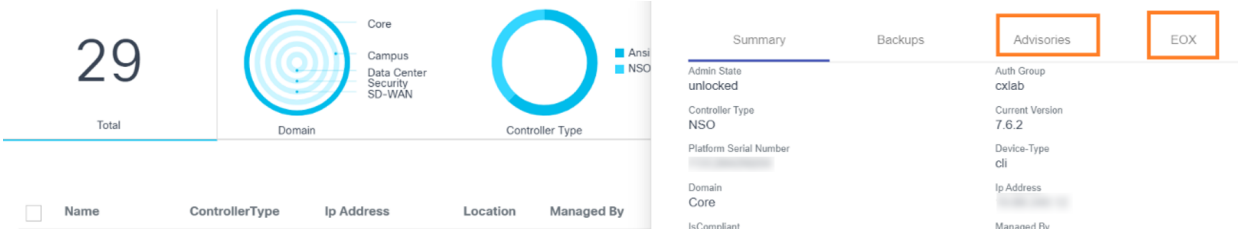
Exibir Erros de Prioridade

- Link Exibir bugs de prioridade: Navega para a ferramenta de pesquisa de erros oficial



Ativos

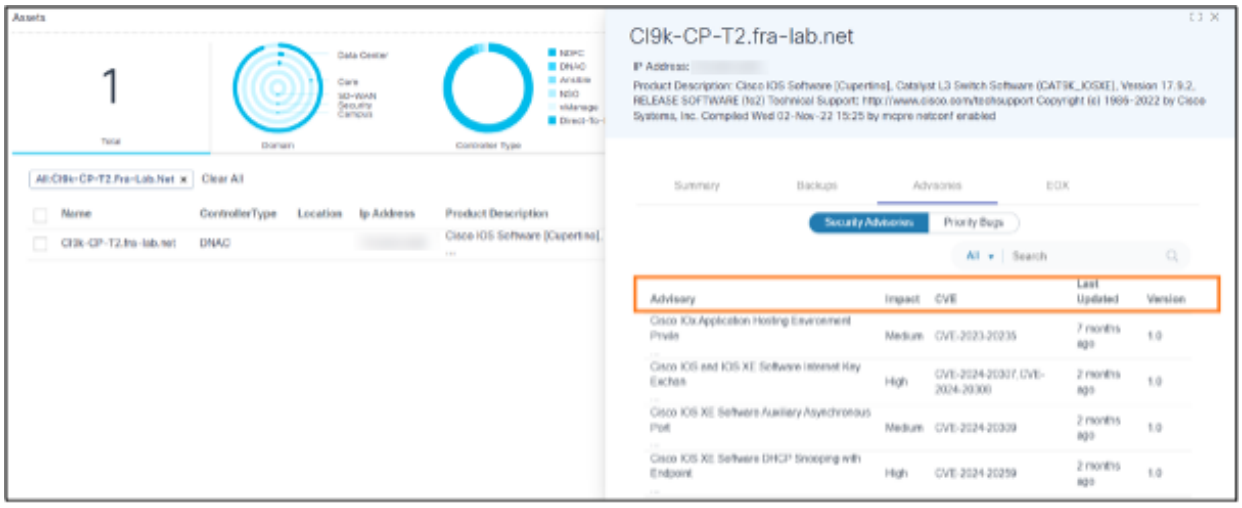
No Gerenciador de ativos, os usuários podem exibir uma lista de todos os ativos. Ao selecionar qualquer ativo, um painel exibe informações no nível do ativo, que incluem detalhes da vulnerabilidade do software do ativo organizados em duas guias: Consultoria e EOX.



Avisos e EOX

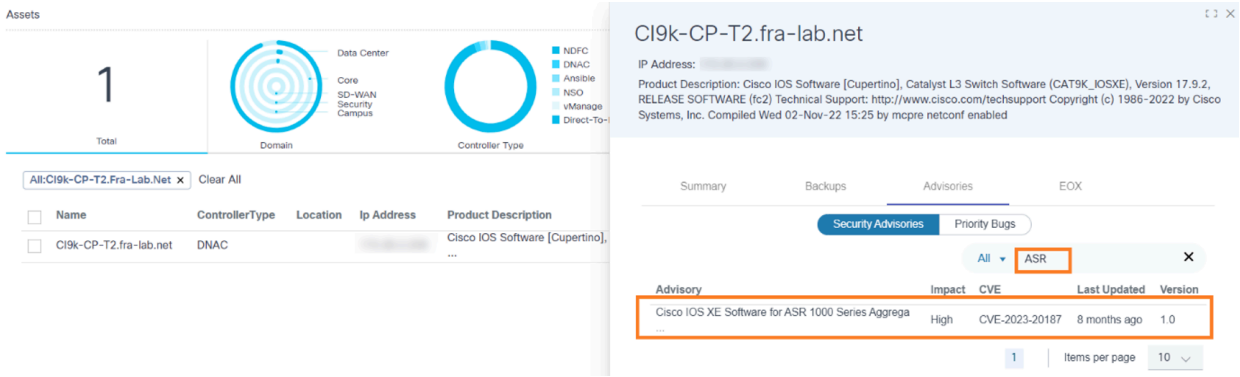
A guia Recomendações contém duas subguias, Recomendações de segurança e Erros de prioridade. Mais detalhes sobre essas guias são fornecidos nas seções abaixo.

Orientações de Segurança

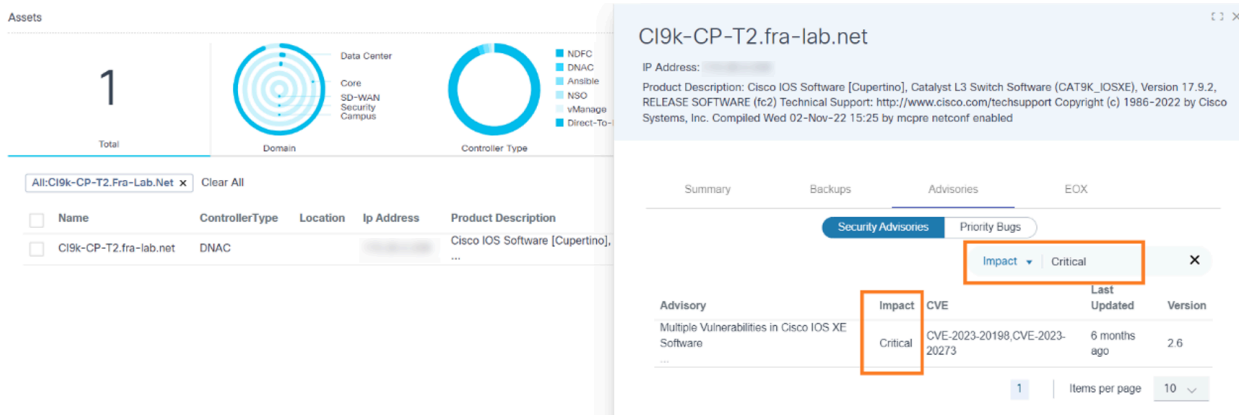


Avisos de segurança do ativo selecionado

Na subguia Recomendações de Segurança, os usuários podem exibir todas as recomendações de segurança que afetam um ativo selecionado. As colunas na tabela de recomendações de segurança incluem Recomendações, Impacto, CVE, Última atualização e Versão.



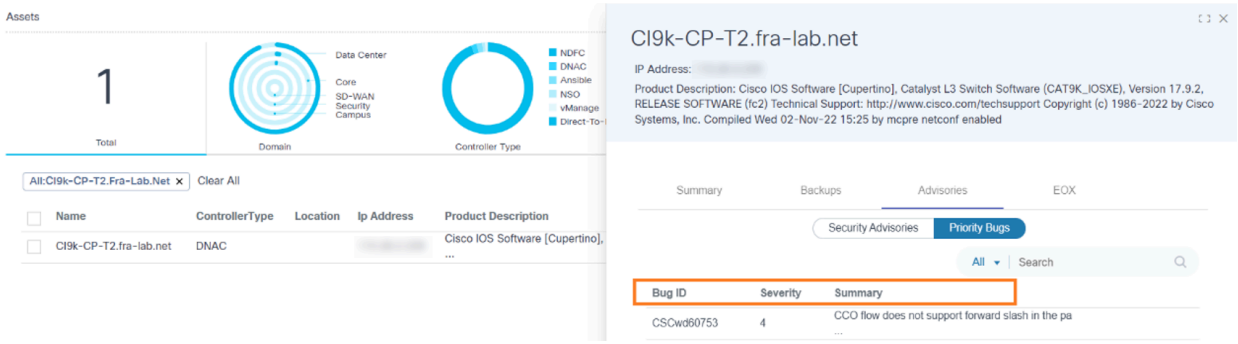
Pesquisa de conselhos de segurança



Pesquisa de conselhos de segurança - Opção de impacto

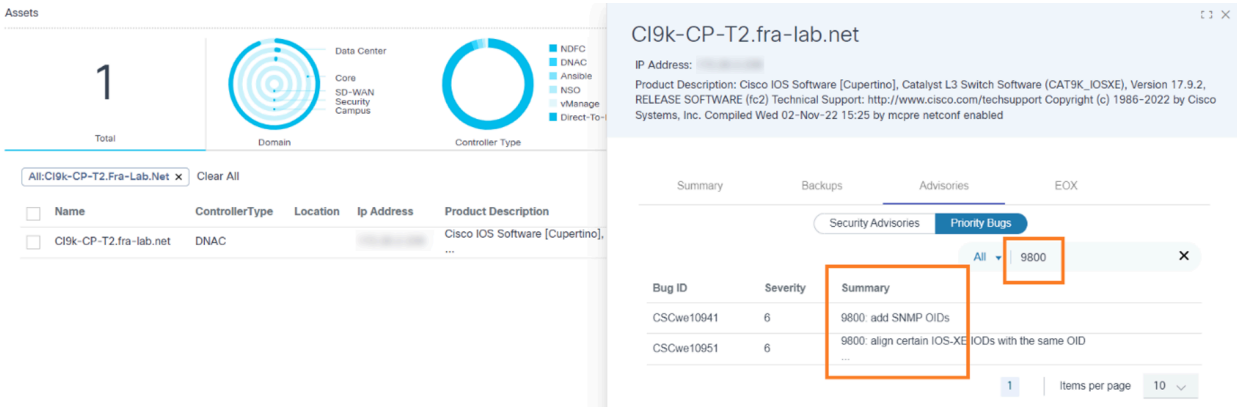
Os usuários podem pesquisar recomendações com base nos valores das colunas Recomendações, Impacto, CVE, Última atualização e Versão. A paginação permite que os usuários naveguem entre as páginas.

Erros de prioridade

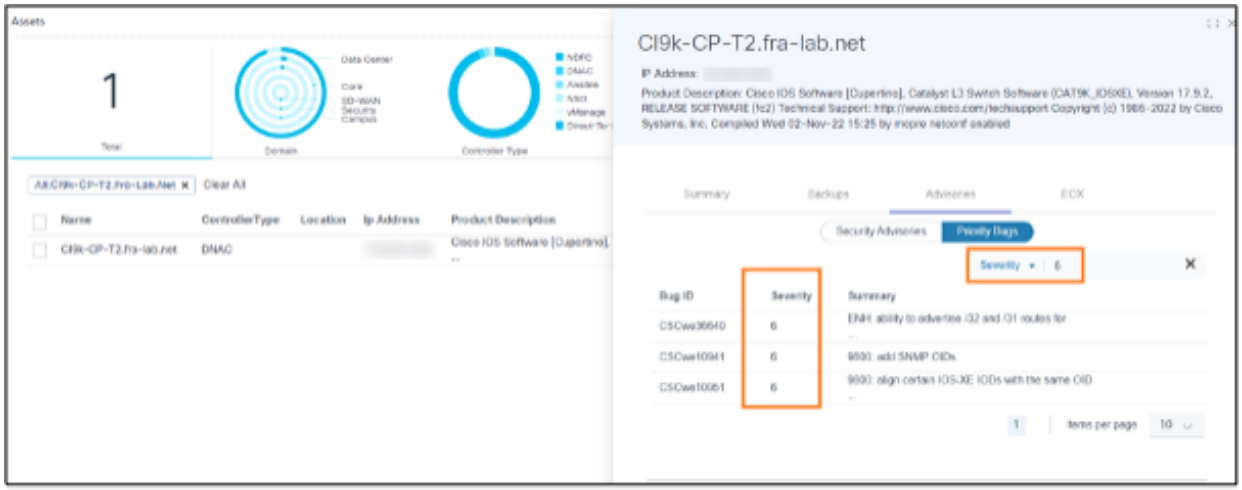


Erros de prioridade que afetam um ativo selecionado

Na subguia Priority Bugs, os usuários podem acessar todos os bugs de prioridade que afetam um determinado ativo. As colunas nesta guia incluem ID do erro, Severidade e Resumo.



Busca de bugs prioritários por resumo



Busca de bugs com prioridade por gravidade

Os usuários podem procurar bugs de prioridade com base nos valores nas colunas Bug ID, Severity e Summary. A paginação facilita a navegação entre as páginas.

EOX

Guia EOX

A guia EOX exibe dados de fim da vida útil do software específicos de um ativo, incluindo três datas importantes:

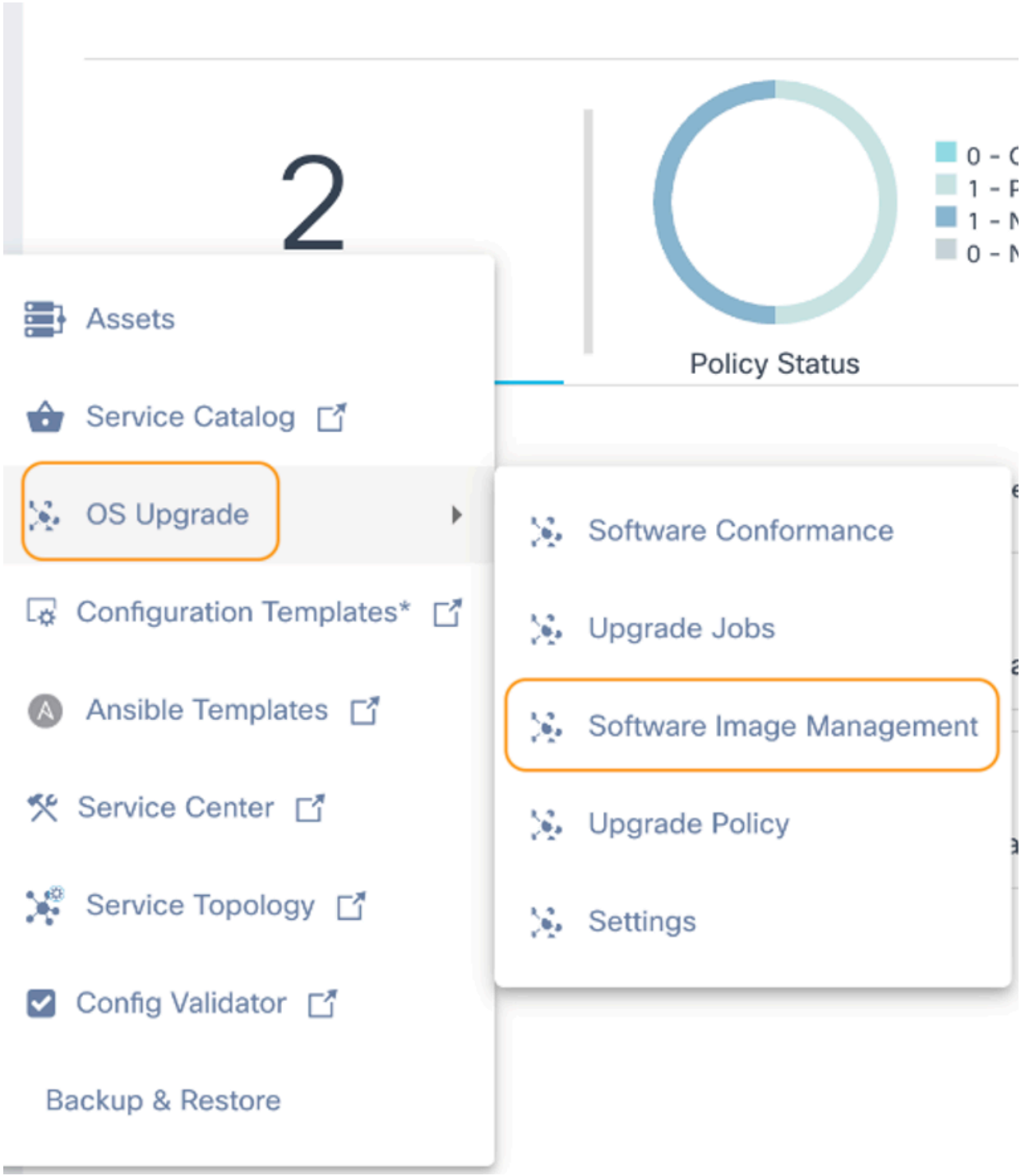
- Fim da manutenção do software
- Fim do suporte de segurança
- Última data de suporte

Exibição de Insights de Software

O Software Insights fornece sugestões de software para os modelos de dispositivo gerenciados pelo Cisco Catalyst Center e pelos controladores NDFC, permitindo que os usuários administradores criem uma política de conformidade para os modelos de dispositivo se a sugestão estiver disponível.

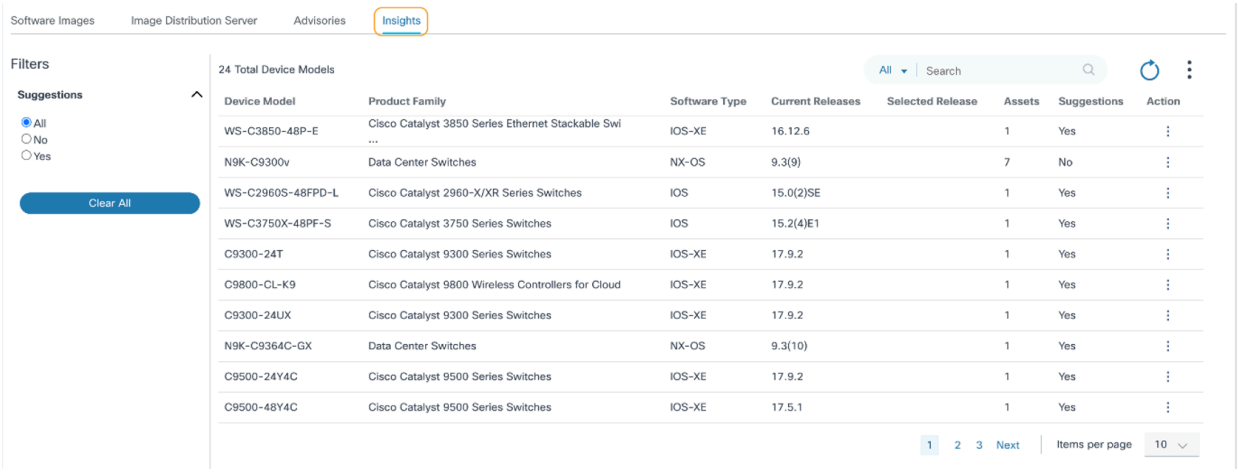
Para acessar o Software Insights:

1. Faça login no BPA com credenciais que tenham acesso de gerenciamento aos Insights.



Gerenciamento de imagens de software

2. Selecione OS Upgrade > Software Image Management no painel lateral.



Guia Insights

3. Clique na guia Insights.

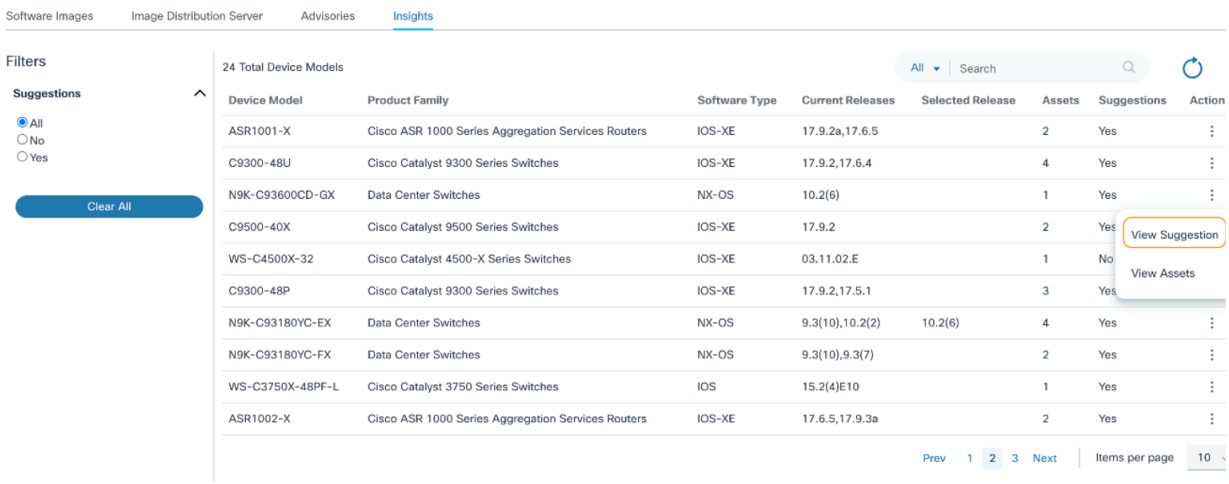
A guia Insights contém o seguinte:

- Um filtro que permite aos usuários filtrar dados com base em Sugestões. Todos é selecionado por padrão.
    - Sim filtra os dados para modelos de dispositivo com sugestões
    - Não filtra os dados para modelos de dispositivo sem sugestões

Exportar para CSV

- O ícone Mais Opções fornece uma opção Exportar para CSV para exportar os dados exibidos na página
    - O ícone Atualizar atualiza a página e limpa os filtros selecionados
    - O filtro Search é usado para pesquisar os dados e inclui os seguintes filtros de pesquisa exclusivos:
- Todos: Pesquisa em todas as colunas (por exemplo, Modelo do dispositivo, Família de produtos e Tipo de software)
- Modelo do dispositivo: Procura dados com um nome de modelo de dispositivo específico
- Família de produtos Pesquisa dados com o nome da família de produtos específica
- Tipo de software: Procura dados com um nome de tipo de software específico

- Os modelos de dispositivos existentes são exibidos com as seguintes colunas:
- Modelo do dispositivo: Nome do modelo do dispositivo
- Linha de produtos: Nome da família de produtos à qual o modelo de dispositivo pertence
- Tipo de software: Nome do tipo de software ao qual o modelo de dispositivo pertence
- Versões atuais: Lista das versões de software exclusivas que estão atualmente presentes no inventário para o modelo de dispositivo
- Versão selecionada: Versão de lançamento sugerida que foi selecionada como uma versão opcional das sugestões fornecidas pela Cisco
- Ativos: Número de ativos presentes no Gerenciador de ativos para o modelo de dispositivo
- Sugestões: Exibe Sim ou Não para todas as sugestões disponíveis para o modelo de dispositivo

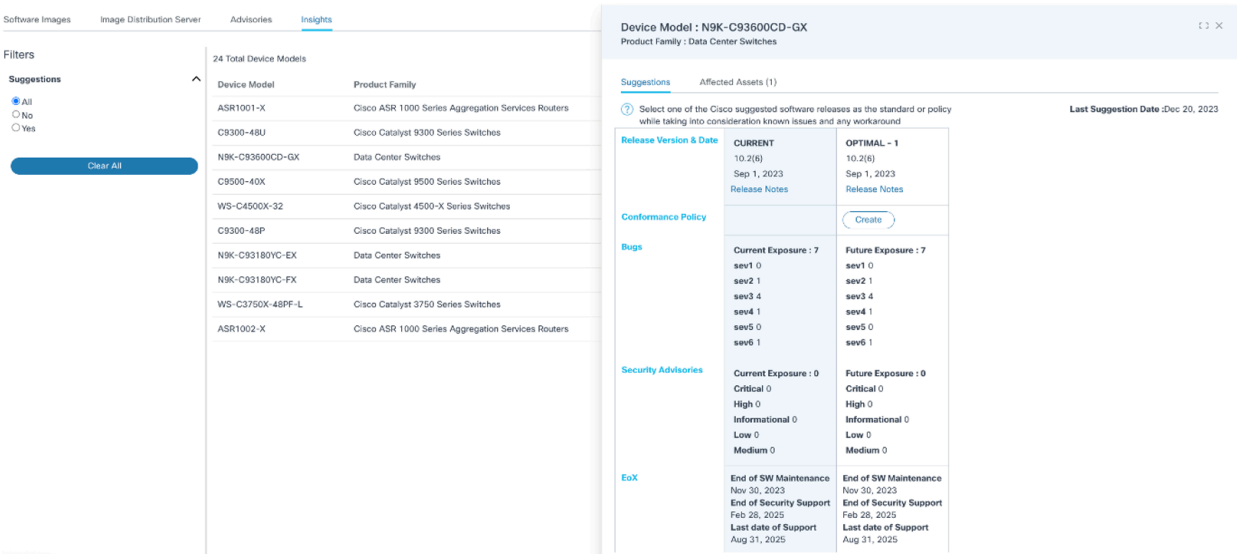


Exibir Navegação de Sugestão

- Ação: Fornece ações específicas de linha por meio do ícone Mais Opções (por exemplo, Exibir Sugestões e Exibir Ativos)

Note: Exibir sugestões estará desabilitado se o modelo do dispositivo não tiver nenhuma sugestão.

Exibindo e escolhendo versões de software sugeridas pelo fornecedor



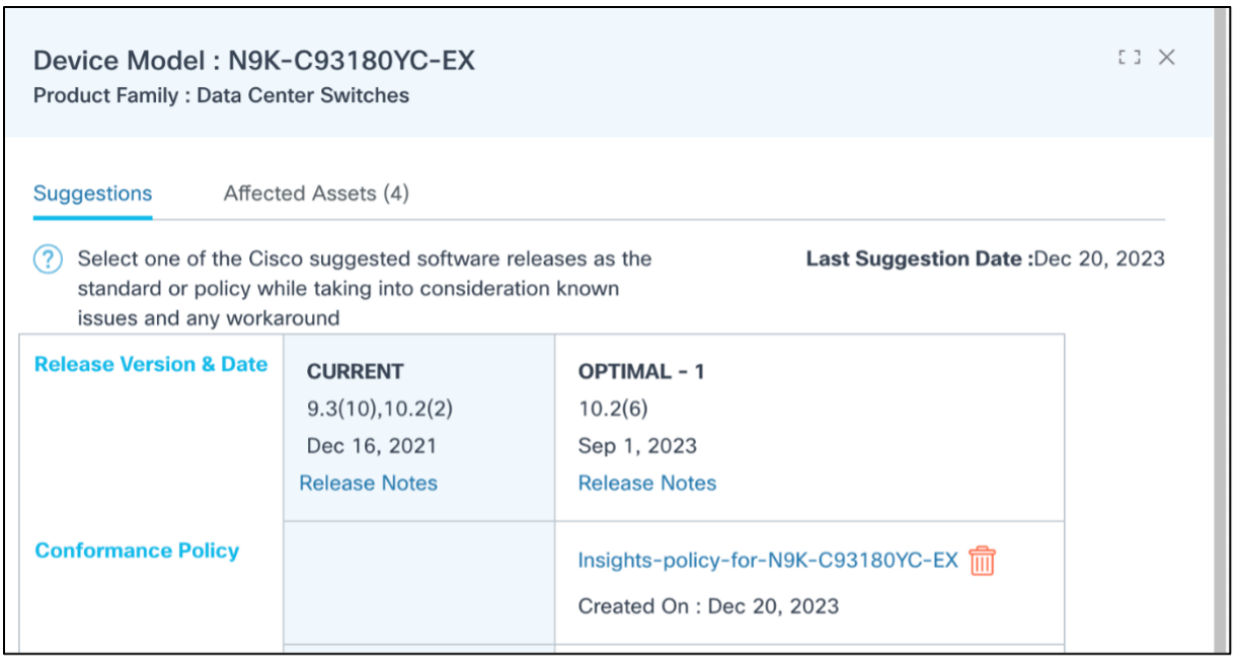
Guia Sugestões

Selecionar o ícone Mais Opções > Exibir Sugestões na coluna Ação abre um painel lateral com todos os detalhes de insight. A guia Sugestões tem os detalhes da versão atual e sugerida para o modelo de dispositivo selecionado; é possível que um modelo de dispositivo tenha mais de uma sugestão. Estão disponíveis os seguintes dados:

- Versão e data da versão: A versão, a data e os detalhes das notas da versão são exibidos para as versões atuais e sugeridas, se disponíveis na nuvem da Cisco; se os ativos no inventário pertencerem a mais de uma versão, todas as versões aplicáveis serão exibidas como valores separados por vírgula na coluna Atual
- Criar política de conformidade: Permite que os administradores criem uma política de conformidade para uma versão específica com a função de dispositivo Qualquer

---

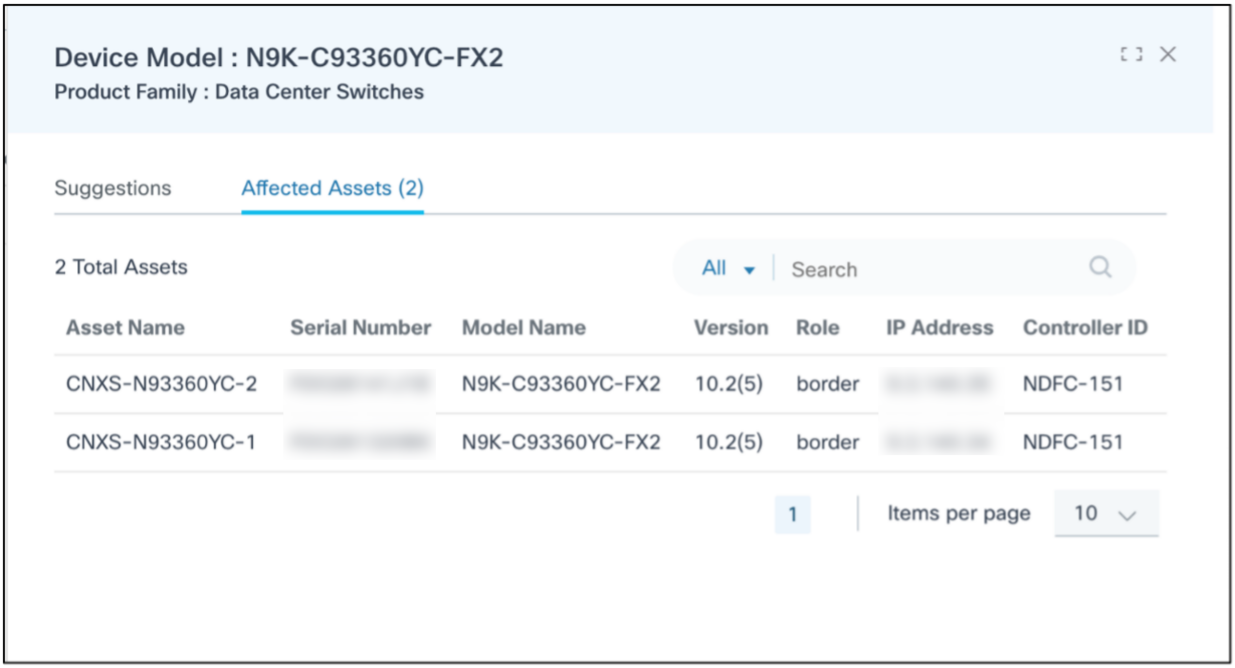
Note: A criação de política de conformidade só tem suporte para modelos de dispositivo de controlador NDFC



Opção Excluir política

Note: Se alguma política já existir para o modelo do dispositivo, um erro será exibido. Se não houver uma política, ela será criada no estado Ativado. Se uma política for criada a partir do Insights, os usuários terão a opção de excluí-la.

- Erros: Exibe uma contagem de bugs consolidada para cada versão
- Avisos de segurança: Exibe uma contagem de recomendações consolidadas para cada versão
- EoX: Exibe as datas de Fim da manutenção do software, Fim do suporte de segurança e Última data de suporte para cada versão



Guia Ativos afetados

A seleção do ícone Mais opções > Exibir ativos na coluna Ação abre um painel lateral onde a guia Ativos afetados é exibida por padrão. A guia Ativos afetados mostra detalhes de ativos potencialmente afetados em colunas como Nome do ativo, Número de série, Nome do modelo, Versão do software, Endereço IP e ID do controlador. A classificação e a pesquisa dos ativos podem ser executadas nessa guia.

Identificação de dispositivos que precisam de atualização de software

Consulte Conformidade de Software para obter mais informações.

Conformidade de software

A conformidade de software ajuda a identificar os ativos em uma rede que não estão em conformidade com a versão de software desejada. A validação é baseada em políticas e regras através das quais os propósitos de conformidade de software são definidos. Essas políticas podem ser executadas de forma programada ou sob demanda. Após a execução bem-sucedida da política de conformidade, é obtido o resultado de conformidade que fornece o status dos ativos aplicáveis. O escopo de conformidade depende de vários critérios, como a função do dispositivo, o gerenciamento da instância do controlador etc.

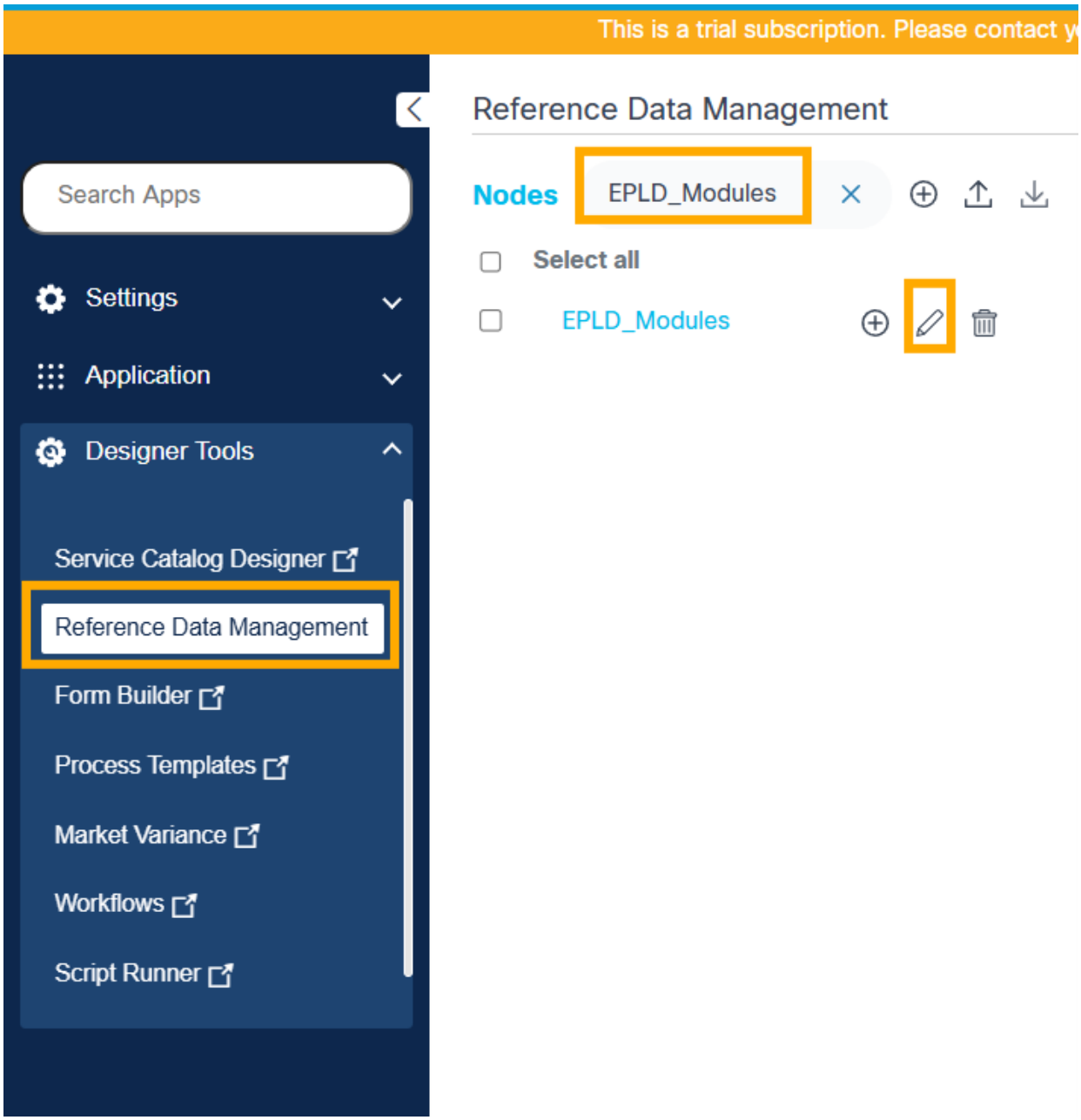
Pré-requisitos

- Imagens de software de controladores como Cisco Catalyst Center, vManage, NDFC e FMC devem estar em sincronia. Consulte Sincronização de Metadados de Imagens de Software para obter mais informações.
- Os metadados de imagem de software necessários para controladores como NSO, CNC, Direct-to-Device e ANSIBLE devem ser adicionados. Consulte Adição de Metadados de Imagem de Software para obter mais informações.
- Os usuários devem ter acesso ao aplicativo RefD para gerenciar os dados do módulo EPLD.
- As informações do módulo EPLD para as versões necessárias devem ser pré-preenchidas no aplicativo RefD
- Os usuários devem adicionar manualmente as informações do módulo EPLD no aplicativo RefD se ele não estiver disponível

Criando Dados do Módulo EPLD no Aplicativo de Gerenciamento de Dados de Referência

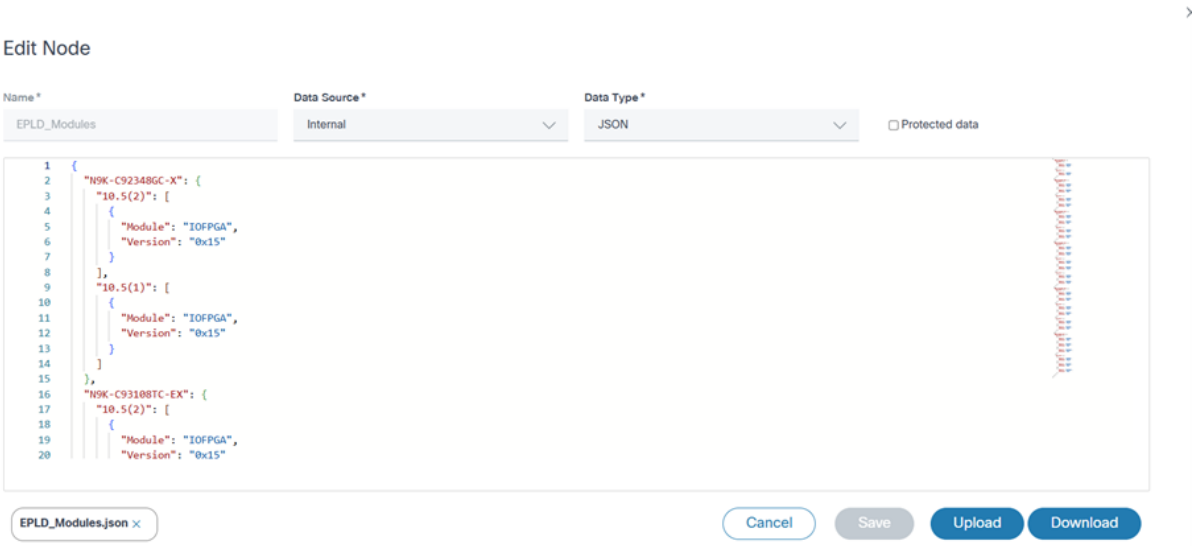
Antes de criar uma política de conformidade, crie os dados de referência do módulo EPLD no aplicativo RefD. O aplicativo RefD inclui informações do módulo EPLD para as versões do software Nexus v10.2(8) e v10.4(5), respectivamente. Para outras versões do dispositivo, as informações do modelo EPLD devem ser adicionadas manualmente no aplicativo RefD.

Conclua as etapas a seguir para adicionar outras versões aos metadados do módulo EPLD:



Gerenciamento de dados de referência

1. Navegue até o aplicativo Reference Data Management e procure por "EPLD_Modules".
2. Selecione o arquivo "EPLD_Modules" e selecione o ícone Editar.



Editar nó

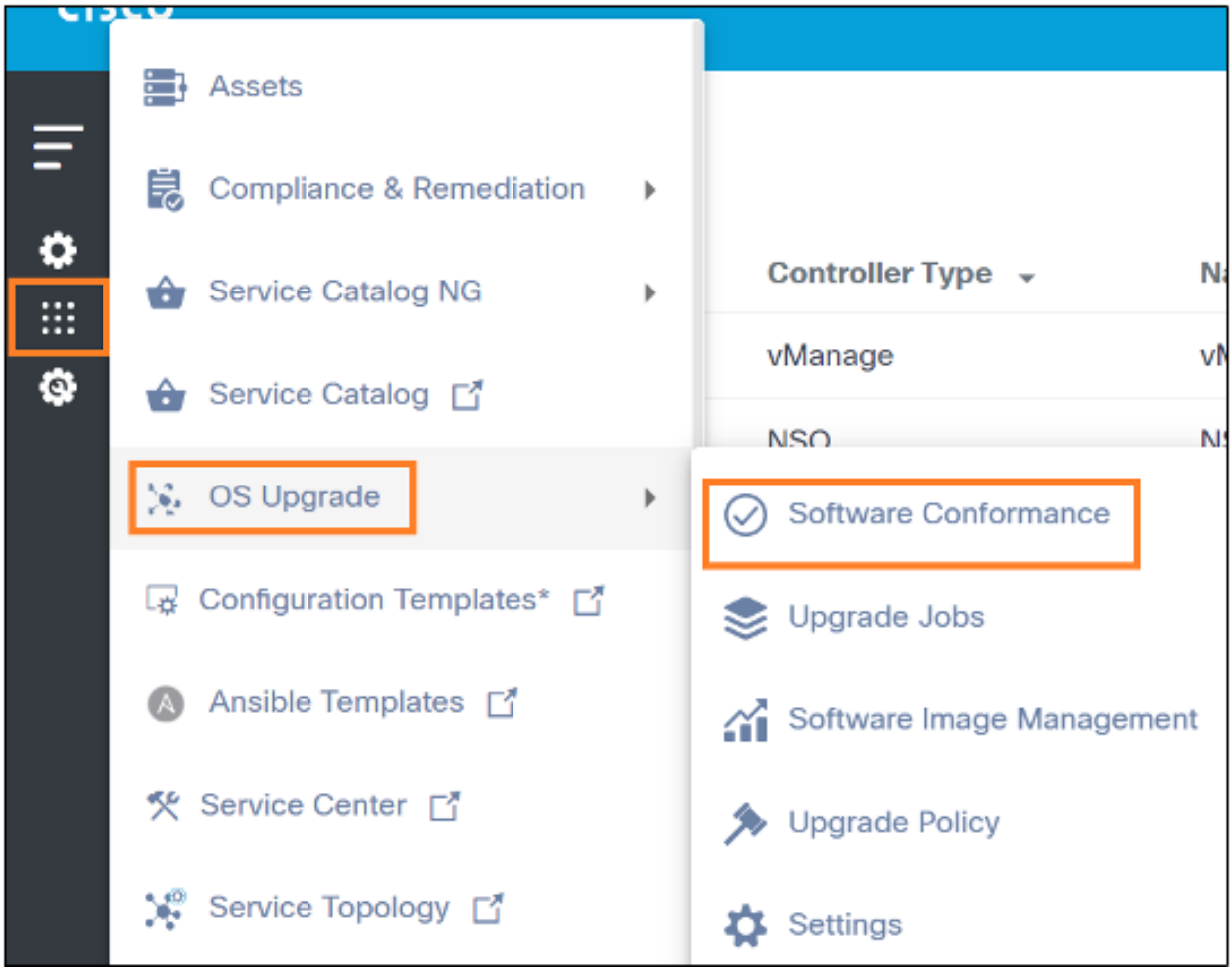
3. Adicione os metadados do módulo EPLD da nova versão anexando uma nova entrada com a seguinte estrutura:

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

4. Clique em Salvar e valide os novos metadados do módulo EPLD que estão disponíveis para seleção na política de conformidade. Os dados EPLD para as versões suportadas são pré-preenchidos.

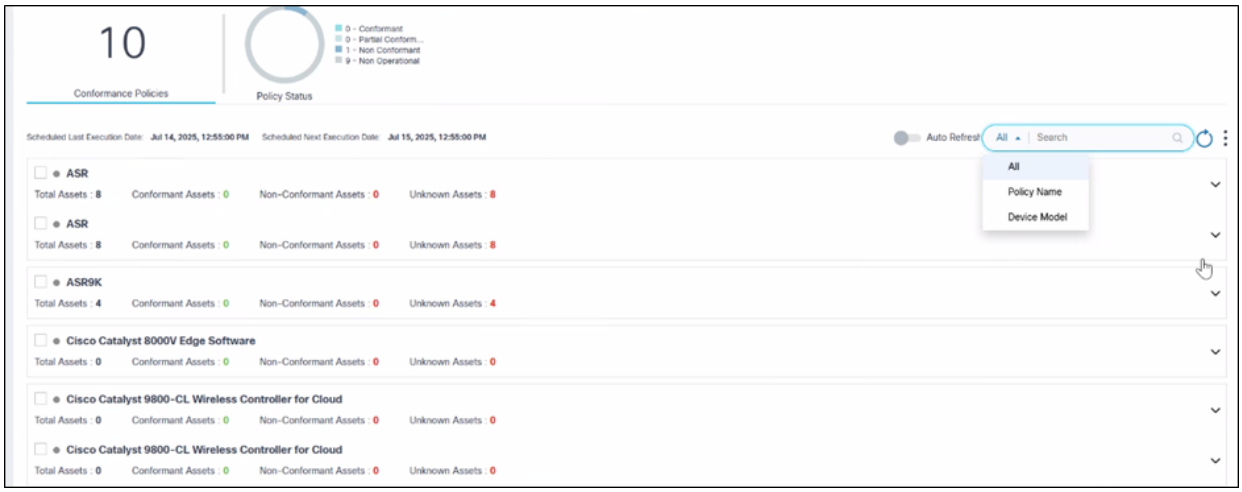
Exibição e gerenciamento da conformidade de software

1. Faça login no BPA com credenciais que tenham acesso à Conformidade de software.



Navegação de conformidade de software

2. Selecione OS Upgrade > Software Conformance. A página Conformidade do software é exibida.



Conformidade de software

A página Conformidade de software contém o seguinte:

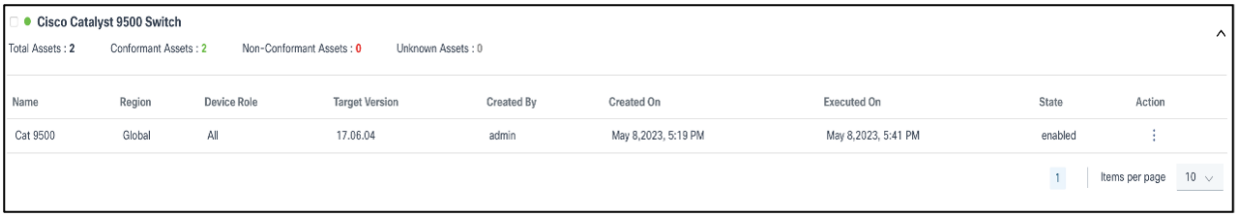
- Uma seção de análise, exibida na parte superior, que fornece o seguinte:

- O número total de políticas de conformidade existentes no sistema
- Um filtro rápido de Status da política para filtrar com base nos seguintes critérios:
    - Conformidade: Todos os dispositivos gerenciados por BPA com um modelo especificado estão na versão de software definida
    - Conformidade parcial: Alguns dispositivos gerenciados por BPA com um modelo especificado estão na versão de software definida; os dispositivos restantes estão em versões de software diferentes
    - Não Conformidade: Todos os dispositivos gerenciados por BPA com um modelo especificado estão em versões de software diferentes quando comparados a uma determinada versão de software
    - Não operacional: Nenhum dispositivo aplicável foi encontrado com base no modelo de dispositivo especificado na política
- Data da Última Execução Programada e Data da Próxima Execução Programada que indicam a data e a hora das verificações de conformidade programadas anteriormente executadas e quando a próxima verificação de conformidade programada é para todas as políticas
- Um campo Pesquisar usado para filtrar políticas com base no modelo do dispositivo, nome da política ou tudo; os usuários podem selecionar All para pesquisar em todos os parâmetros
- Uma alternância de Atualização Automática permite a atualização automática da política de conformidade Em Andamento em intervalos definidos pelo usuário quando habilitada. Para ativar a alternância:
    - Vá para OS Upgrade > Settings para alterar o intervalo de atualização
    - Modificar o intervalo de atualização automática com um valor desejado
    - Clique em Salvar
- O painel de controle da política de conformidade de software é atualizado no novo intervalo quando a alternância Atualização automática está habilitada
- Um ícone Atualizar para atualizar a página e limpar os filtros selecionados
- Um ícone Mais Opções que fornece as seguintes opções:
    - Criar uma política
    - Executar todas as políticas
    - Excluir várias políticas selecionadas

As políticas são agrupadas com base nos modelos de dispositivo e exibidas como painéis expansíveis para fornecer uma única visualização em todos os modelos de dispositivo gerenciados por diferentes controladores.

Exibição Recolhida da Política de Conformidade

Na visualização recolhida, o painel exibe o modelo do dispositivo e estatísticas rápidas, como Total de ativos, Ativos em conformidade, Ativos não em conformidade e Ativos desconhecidos.

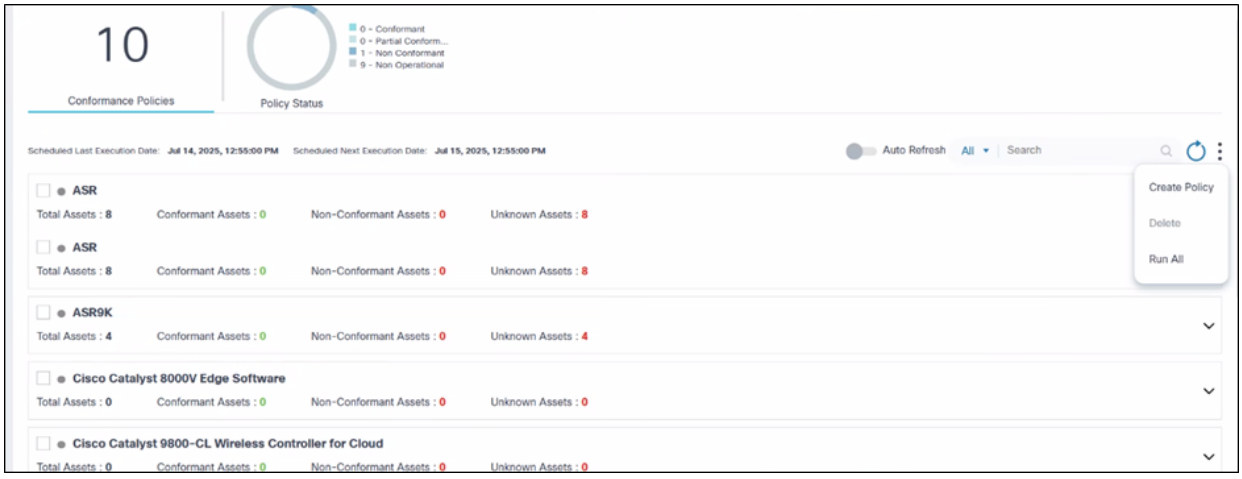


Visão ampliada da política de conformidade

Na visualização expandida, todas as políticas relacionadas ao modelo do dispositivo são exibidas. Para cada política, ações adicionais, incluindo Executar, Editar política, Exibir resultados, etc., podem ser executadas selecionando o ícone Mais opções na coluna Ação.

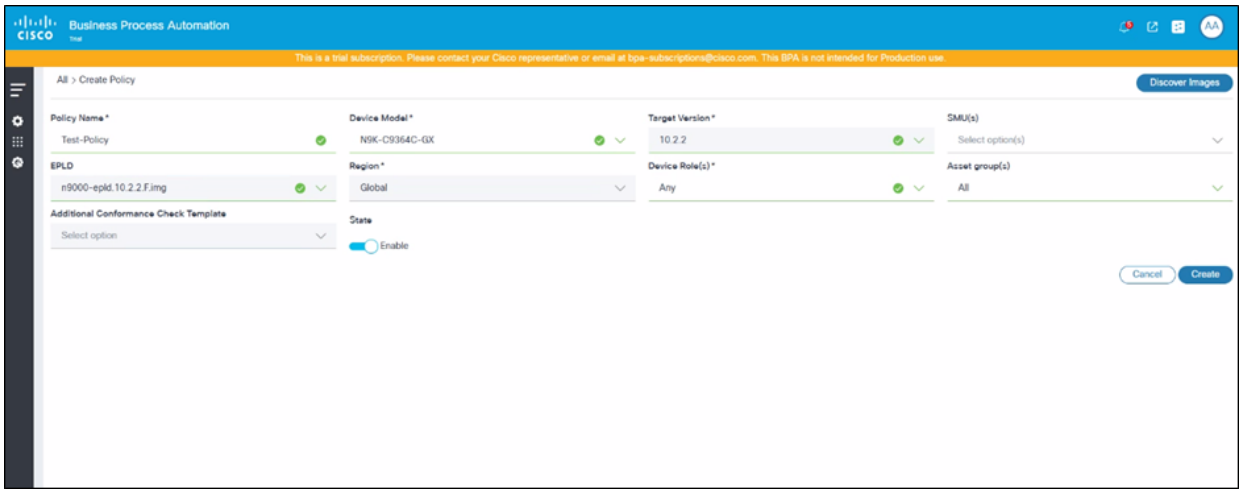
Criação de políticas de conformidade de software

1. Faça login no BPA com credenciais que tenham acesso de gerenciamento à Conformidade de software.
2. Selecione OS Upgrade > Software Conformance. A página Conformidade do software é exibida.



Criar política

3. Selecione o ícone More Options > Create Policy.



Criar Formulário de Política

4. Insira informações nos campos Nome da política, Modelos de dispositivo, Versão de destino, SMU, EPLD, Função do dispositivo, Grupos de ativos e Conformidade adicional Verificar modelo. SMU(s), Grupo(s) de Ativos e Modelo Adicional de Verificação de Conformidade são campos opcionais.

Note: Agora, os usuários podem selecionar mais de um modelo de dispositivo no formulário Criar política de conformidade.

Note: A estrutura de conformidade de software pode executar verificações de conformidade na versão básica do SO e patches SMU em relação aos dispositivos de um modelo, função ou instância de controlador específica que está gerenciando o dispositivo. Se alguma verificação personalizada adicional for necessária, um modelo de processo poderá ser criado com os comandos e as regras de validação necessários que podem ser mapeados no campo Modelo de verificação de conformidade adicional.

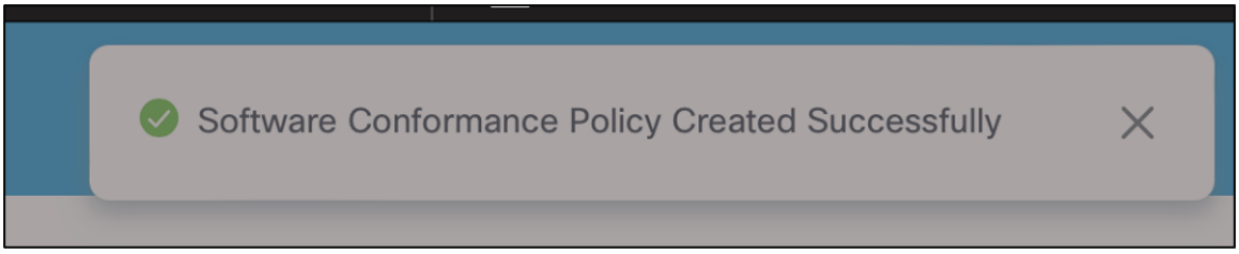
5. Clique em Criar. Uma confirmação é exibida.

Note: A lista a seguir deve ser anotada.

- Os administradores de casos de uso têm a flexibilidade de criar várias políticas com diferentes funções de dispositivo para um modelo de dispositivo selecionado. Mais de uma função pode ser selecionada em uma única política.
- Se Any estiver selecionado na lista suspensa Device Role(s), todas as outras funções de dispositivo (por exemplo, Access, Core, etc.) serão desativadas. Se qualquer outra função do dispositivo for selecionada, Any será desabilitado.
- Para dispositivos gerenciados por controladores como CNC, NSO, ANSIBLE e Direct-to-Device, a função Any (selecionada na lista suspensa Device Role(s)) pode ser usada para executar a verificação de conformidade porque os dispositivos não têm informações de

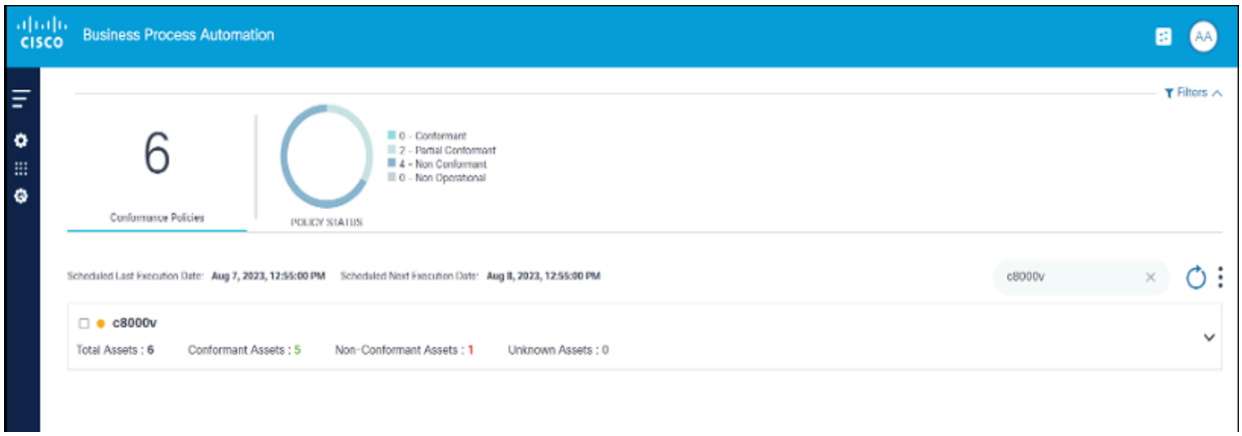
função.

- Se Any for selecionado na lista suspensa Device Role(s) do FMC, a conformidade do software será executada em todos os dispositivos, o que inclui dispositivos autônomos, de controle e de dados.
- A conformidade e as atualizações de SMU(s) são suportadas apenas para controladores CNC, NSO, ANSIBLE, FMC, Direct-to-Device e NDFC.
- Somente Global da lista suspensa Region é suportado nesta versão
- Os usuários podem selecionar Grupo(s) de ativos na lista suspensa. Todos é selecionado por padrão. Os usuários têm a opção de selecionar um ou mais Grupos de ativos. Se um grupo de ativos específico for selecionado, a política será executada apenas nos dispositivos do grupo de ativos selecionado.
- Se os valores esperados para os campos Device Model, Target Version e SMU(s) não forem exibidos, clique em Discover Images e tente novamente.
- Juntos, os campos Modelo de dispositivo, Grupo(s) de ativos e Função formam uma política exclusiva; políticas duplicadas não são permitidas.
- O campo EPLD preenche os valores somente quando os metadados da imagem EPLD estão disponíveis para o(s) modelo(s) de dispositivo selecionado(s) e a versão de destino.
- O Nome da política é exclusivo e nomes de política duplicados não são permitidos.



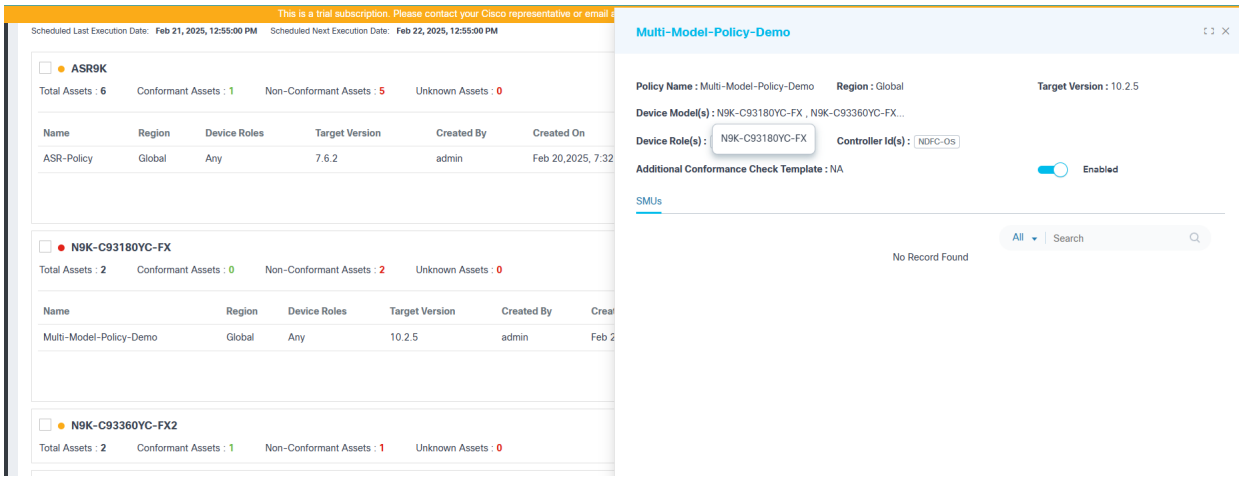
Confirmação de Criação de Política de Conformidade

- Os modelos de processo que são marcados como OS Upgrade Next Generation (Next-Gen) são exibidos no campo Additional Conformance Check Template.



Pesquisar resultado da política de conformidade

6. Localize a política criada inserindo o modelo do dispositivo no campo Pesquisar.

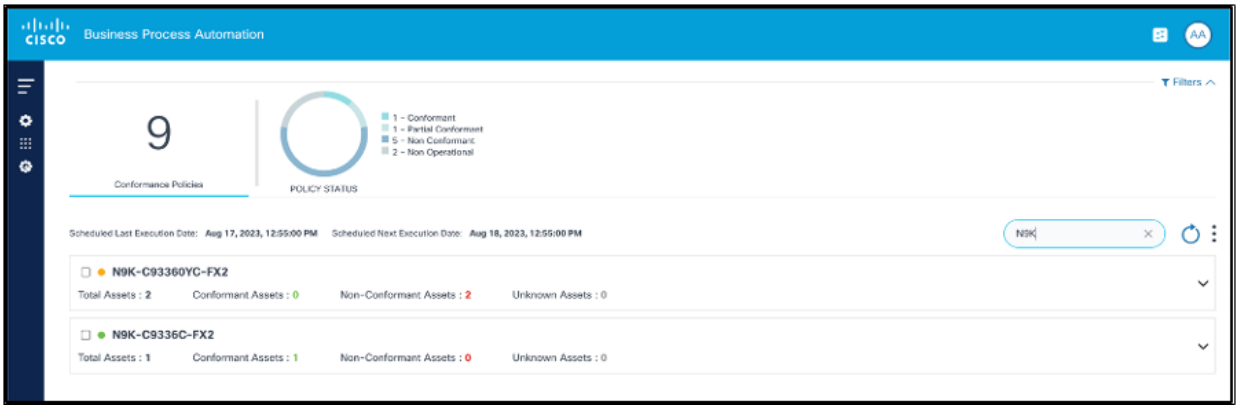


Exibir política de conformidade

7. Clique em Política para exibir a exibição detalhada da política.

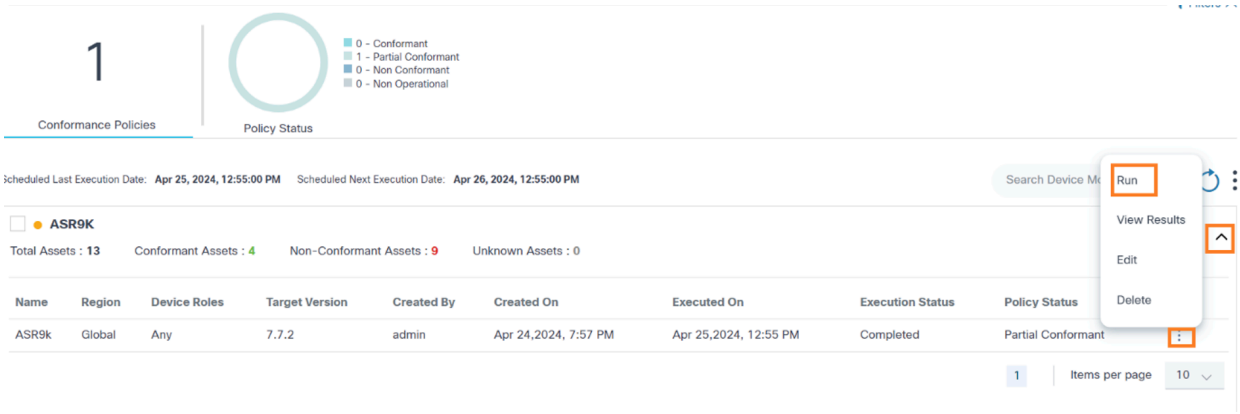
Execução de verificações de conformidade de software sob demanda

1. Faça login no BPA com credenciais que tenham acesso de execução.
2. Selecione OS Upgrade > Software Conformance. A página Conformidade do software é exibida.



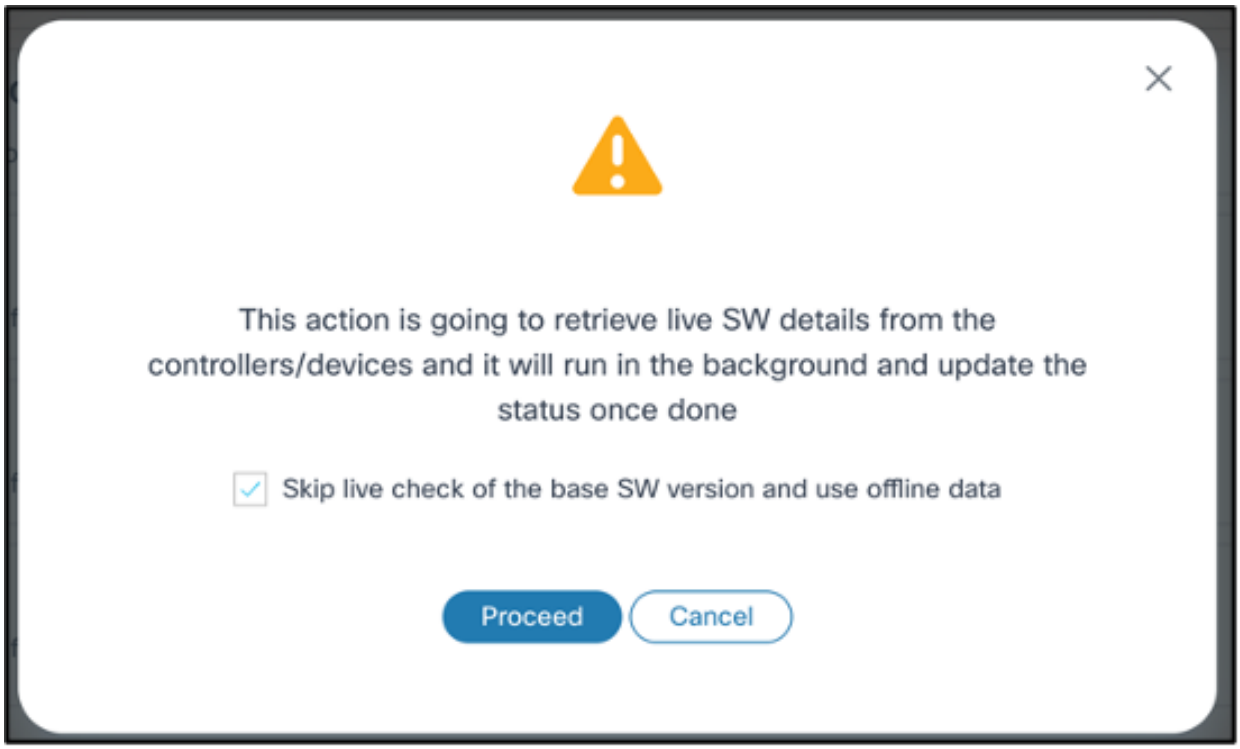
Pesquisa de política

3. Localize a política a ser executada sob demanda usando o campo Pesquisar.



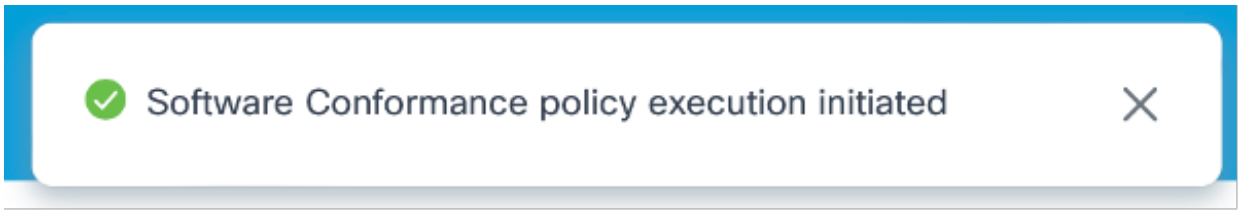
Executar

4. Na coluna Action da política, selecione More Options > Run. Uma confirmação é exibida para validar se uma verificação de inventário em tempo real deve ser executada para os dispositivos.



Confirmação para Executar a Política de Conformidade

5. Se uma sincronização de inventário ao vivo for necessária antes da execução das verificações de conformidade, desmarque a caixa de seleção Ignorar verificação ao vivo da versão básica do software e usar dados offline e clique em Continuar. Nesse caso, a verificação de conformidade é executada apenas após a sincronização. Uma notificação é exibida no canto superior direito.



Notificação de Execução de Política de Conformidade

Note: A lista a seguir deve ser anotada.

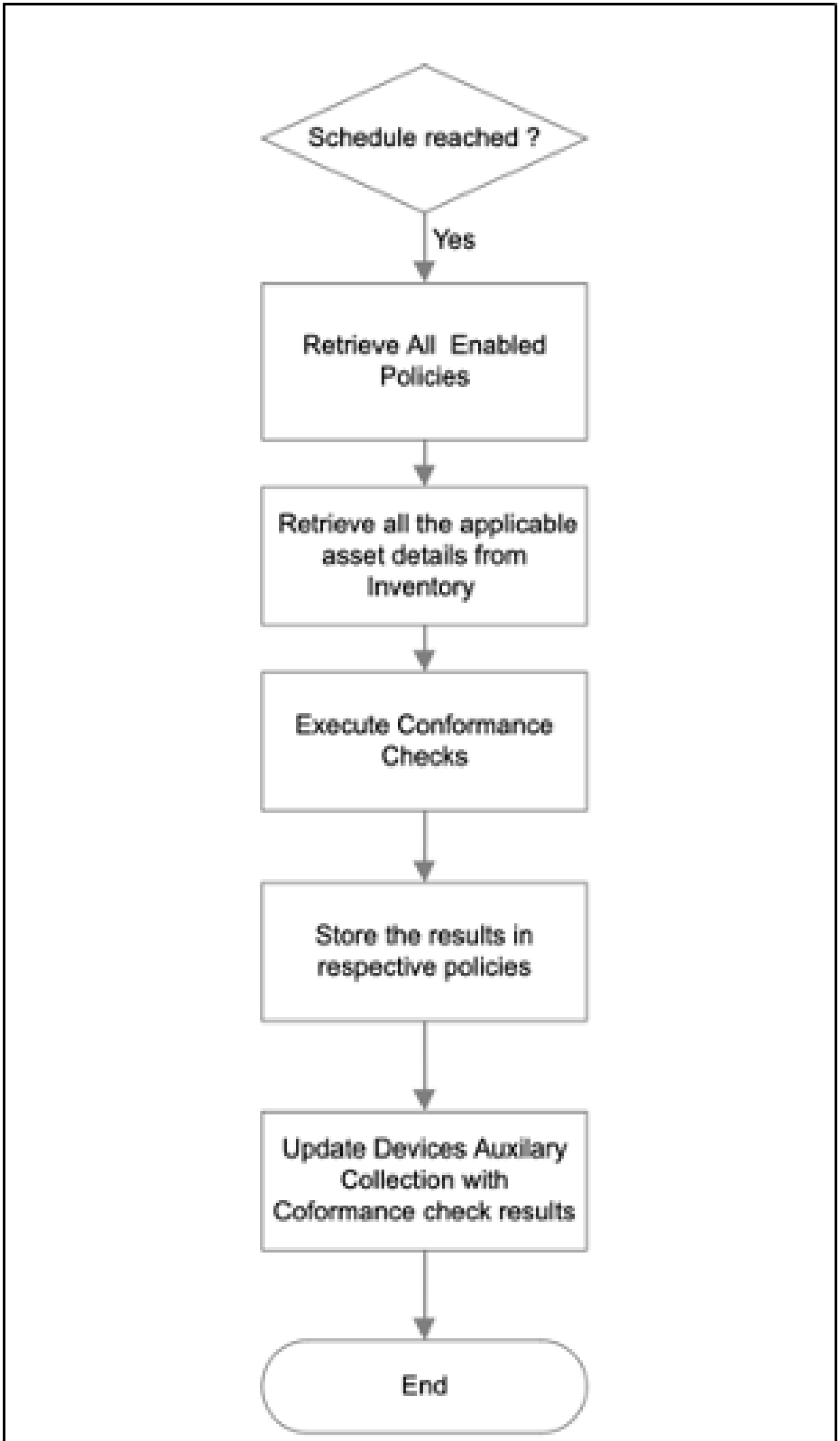
- Uma verificação de conformidade é executada usando dados de inventário de ativos por padrão.
- Durante esse processo, se a sincronização do inventário ou do dispositivo falhar, o respectivo dispositivo de política será marcado como Desconhecido e a verificação SMU será ignorada.
- Para SMUs, os dados em tempo real são recuperados do dispositivo antes de executar verificações de conformidade se a caixa de seleção Ignorar verificação em tempo real da versão básica do SW e usar dados off-line estiver marcada ou não.
- Quando uma política inclui vários modelos de dispositivo, a execução dessa política para um modelo de dispositivo inicia a execução de todas as políticas associadas.

Agendamento da execução das verificações de conformidade de software

As verificações de conformidade de software podem ser executadas automaticamente em intervalos regulares usando o serviço de agendador. As verificações de conformidade programadas podem ser configuradas para execução:

- Diariamente
- Duas vezes por dia
- Semanalmente
- Uma vez

Quando a agenda é atingida, todas as políticas em um estado Habilitado são executadas automaticamente e os resultados de conformidade são armazenados nas respectivas políticas.

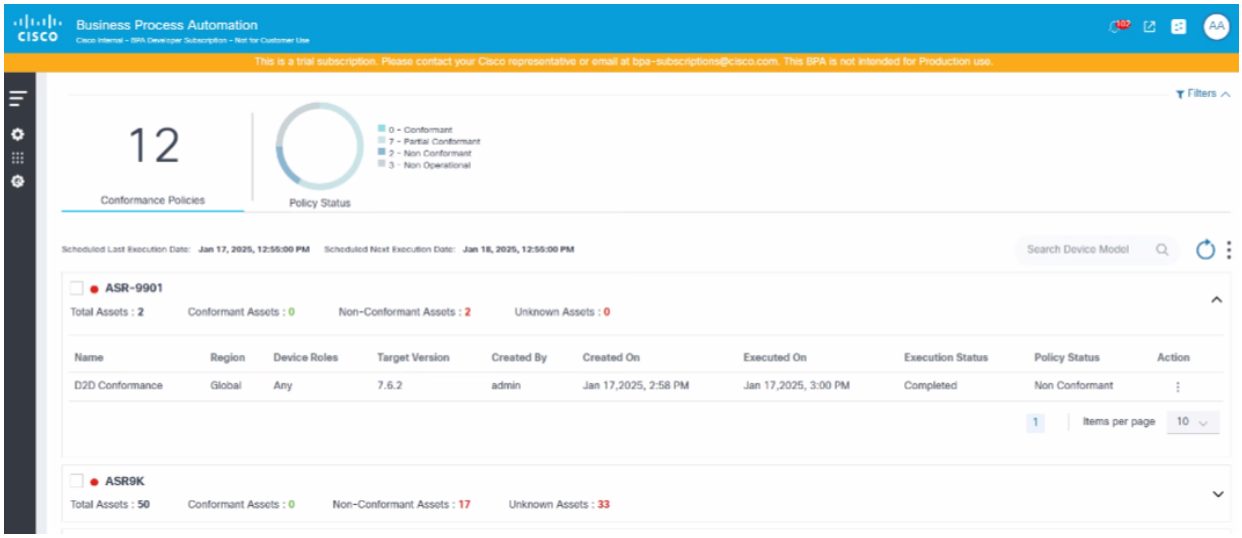

Schedule reached ?
Yes
Retrieve All Enabled Policies
Retrieve all the applicable asset details from Inventory
Execute Conformance Checks
Store the results in respective policies
Update Devices Auxilary Collection with Coformance check results
End

Execução programada de fluxo de chamada de verificações de conformidade de software

Consulte Conformidade de Software para obter mais informações.

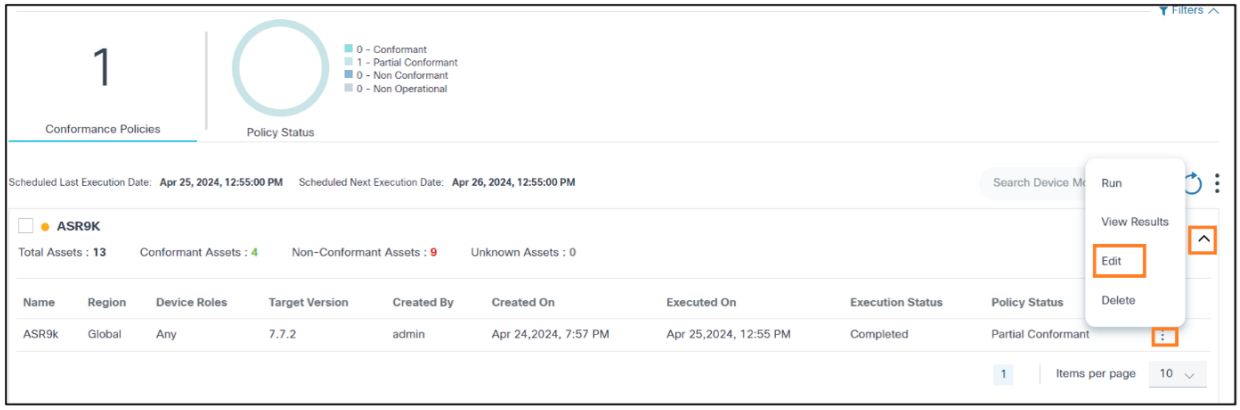
Atualizando Políticas de Conformidade de Software

1. Faça login no BPA com credenciais que tenham acesso de gerenciamento para conformidade de software
2. Selecione OS Upgrade > Software Conformance. A página Conformidade do software é exibida.



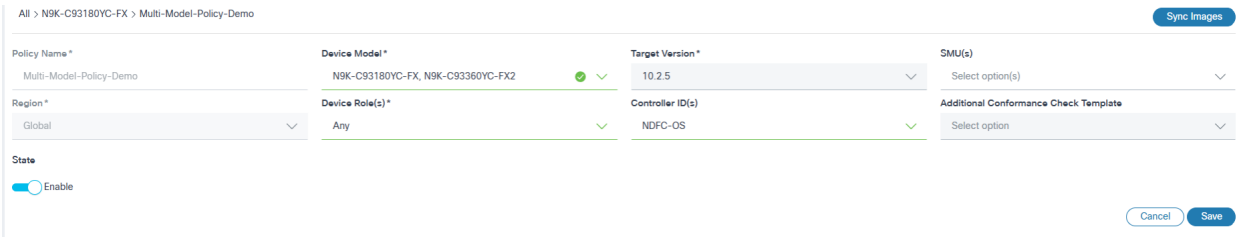
Conformidade de software

3. Use o campo Pesquisar para localizar a política desejada.



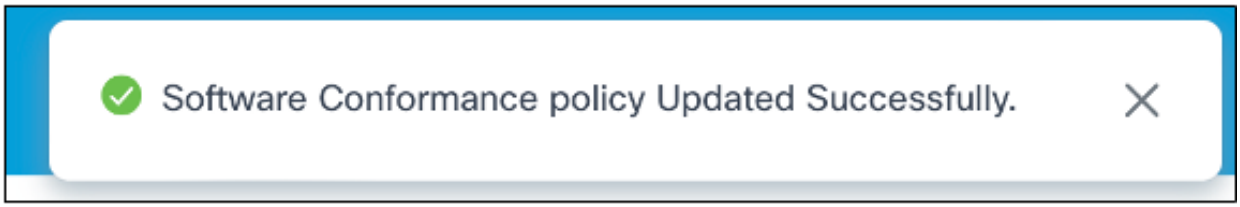
Editar

4. Na coluna Action da política, selecione o ícone More Options > Edit.



Editar política de conformidade com detalhes preenchidos

5. Edite os campos Versão de destino, SMUs, Funções do dispositivo, ID(s) do controlador, Estado da política e Modelo de verificação de conformidade adicional conforme necessário.
6. Click Save. Uma confirmação é exibida.

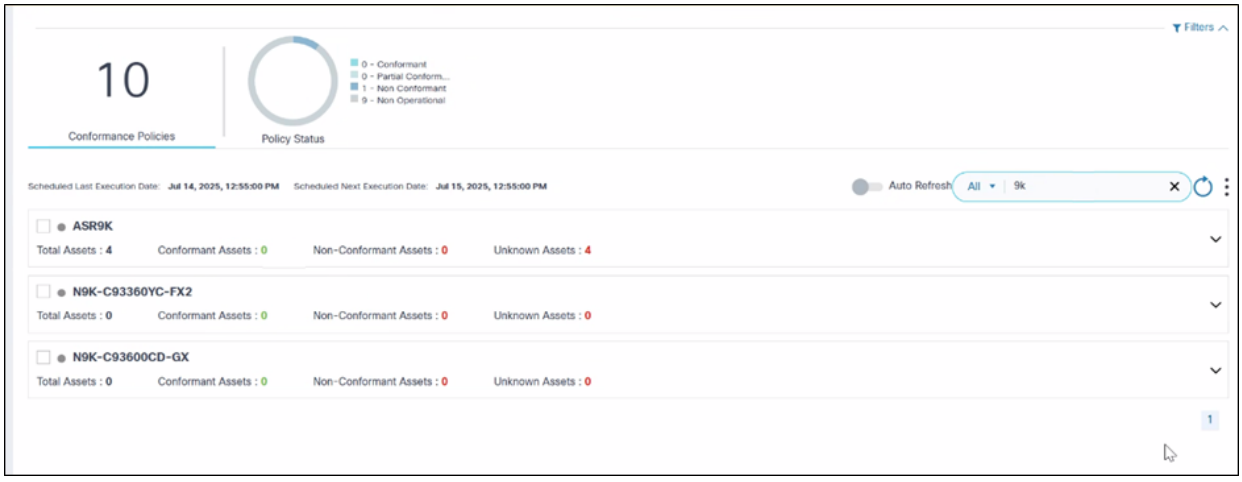


Confirmação de atualização bem-sucedida

Note: Quando a política de Conformidade de Software é usada para um Trabalho de Atualização em andamento, a política não pode ser editada.

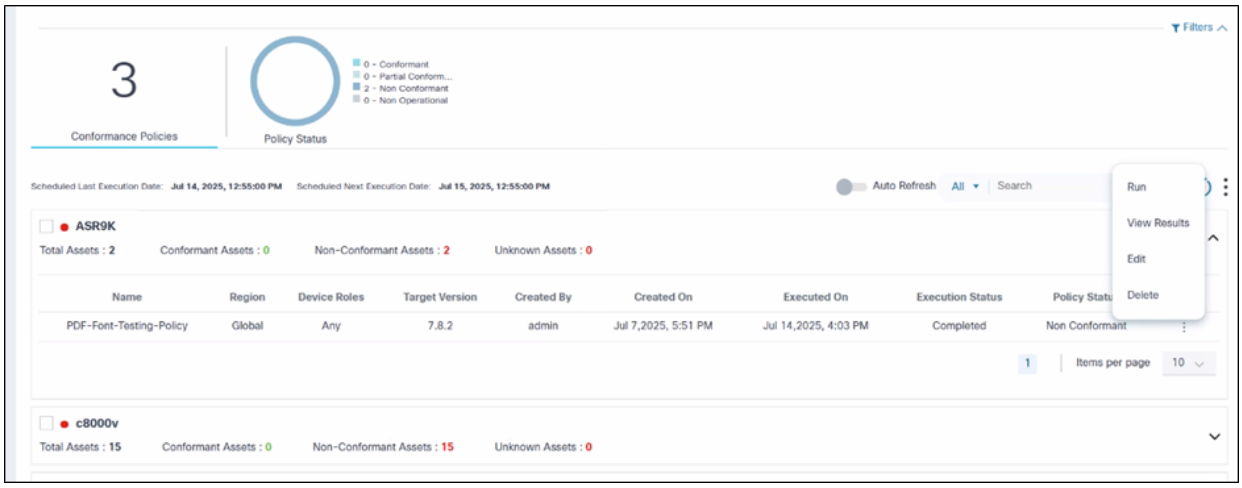
Exclusão de políticas de conformidade de software

1. Faça login no BPA com credenciais que tenham acesso de gerenciamento.
2. Selecione OS Upgrade > Software Conformance. A página Software Conformance é exibida.



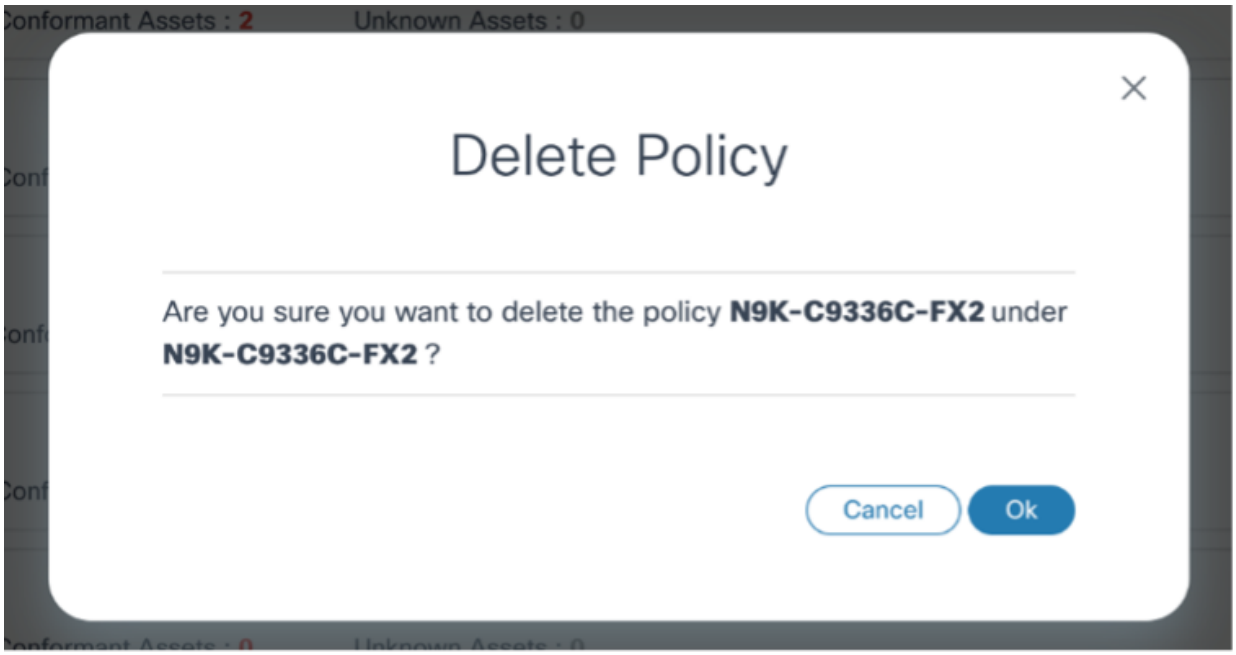
Pesquisar resultado da política de conformidade

3. Use o campo Pesquisar para localizar a política desejada.

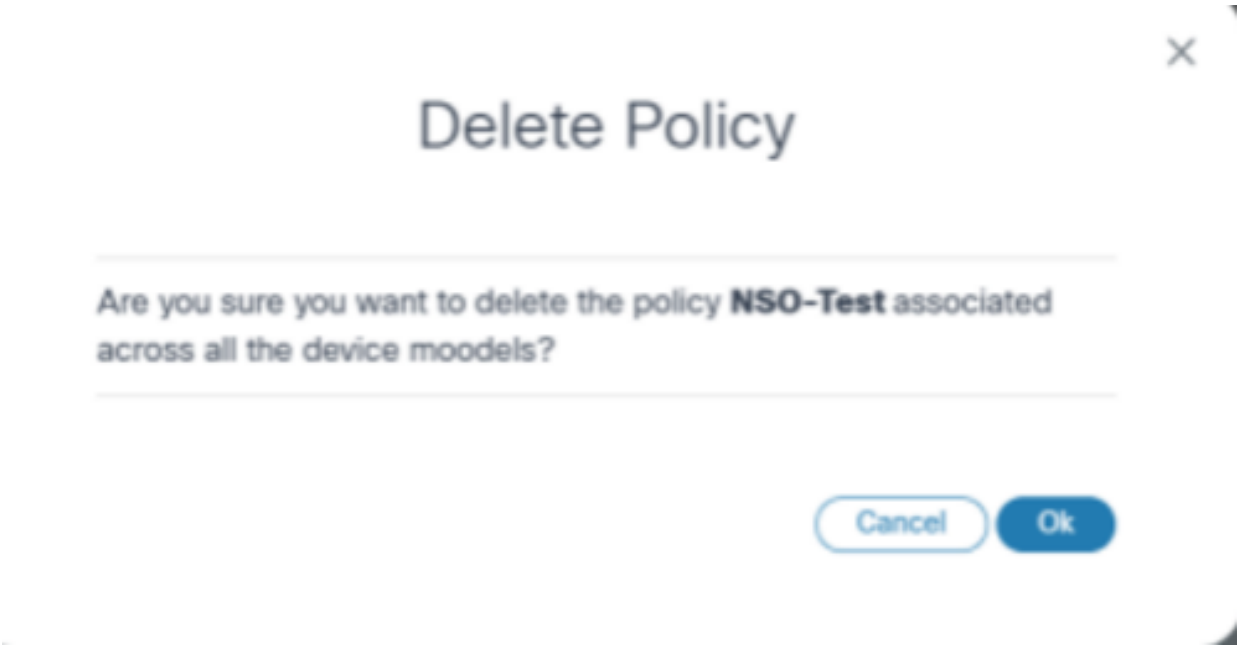


excluir

4. Na coluna Action da política, selecione o ícone More Options > Delete. Uma janela de confirmação será aberta.



Confirmação de Exclusão de Política



Excluir confirmação de política (se a política estiver associada a vários modelos)

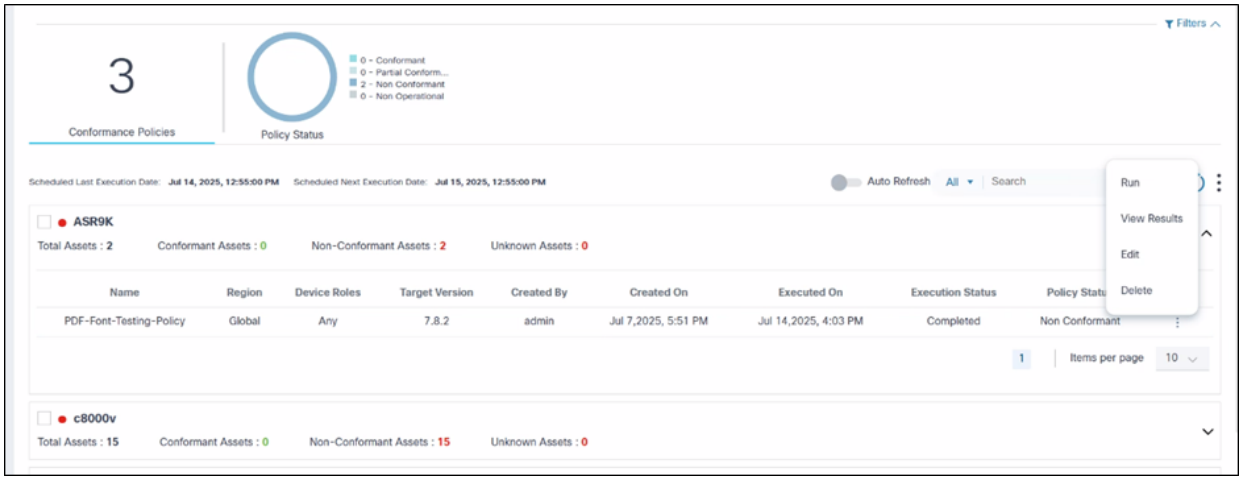
5. Click OK. A política é excluída.

Note: A lista a seguir deve ser anotada.

- Se uma política estiver associada a mais de um modelo de dispositivo, a exclusão de uma política removerá todas as políticas relacionadas para cada modelo associado.
- Quando a política de Conformidade de Software é usada para um Trabalho de Atualização em andamento, a política não pode ser excluída.

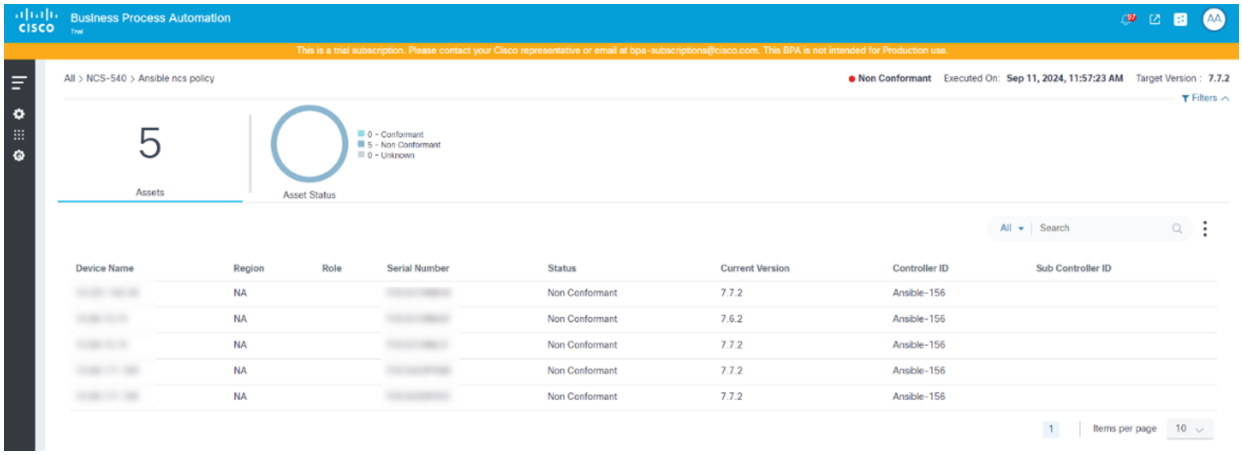
Exibindo e baixando resultados de conformidade

Depois que uma política for executada:

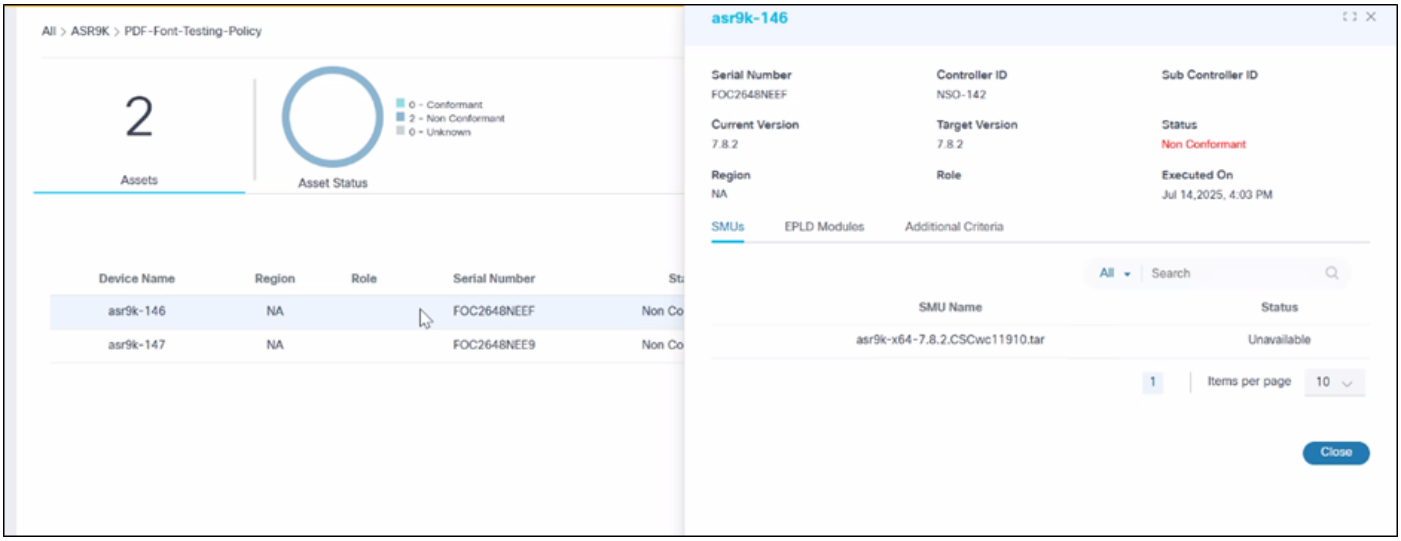


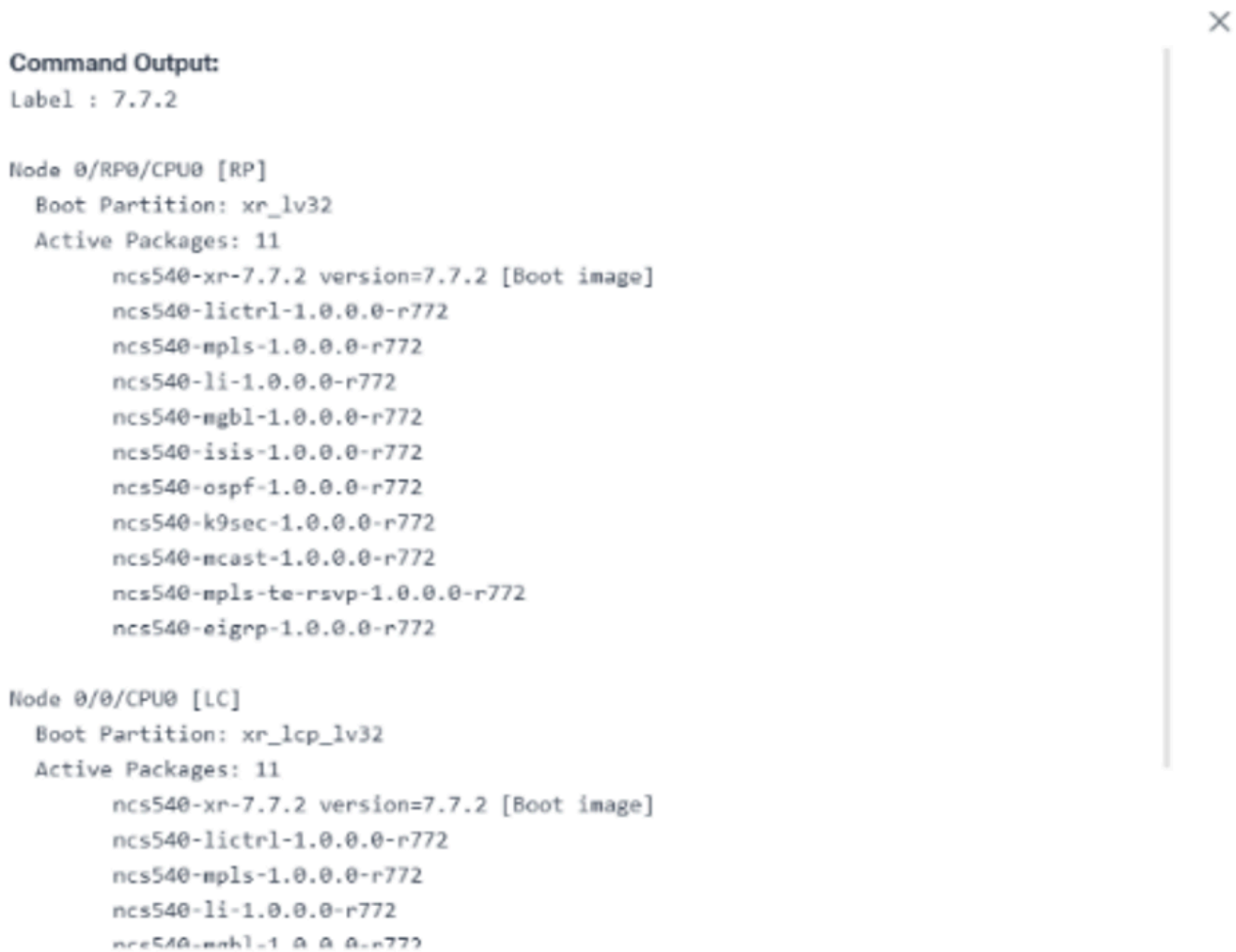
Opção Exibir resultados

1. Na página Software Conformance, selecione o ícone More Options > View Results. A página Resultados é exibida onde os usuários podem exibir o status de conformidade dos dispositivos.



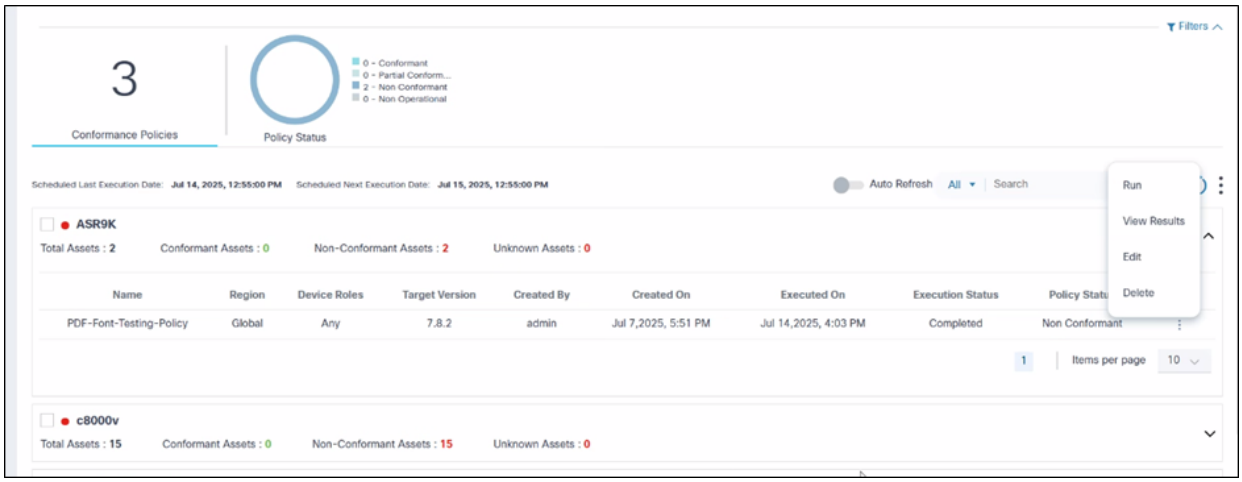
Exibir resultados





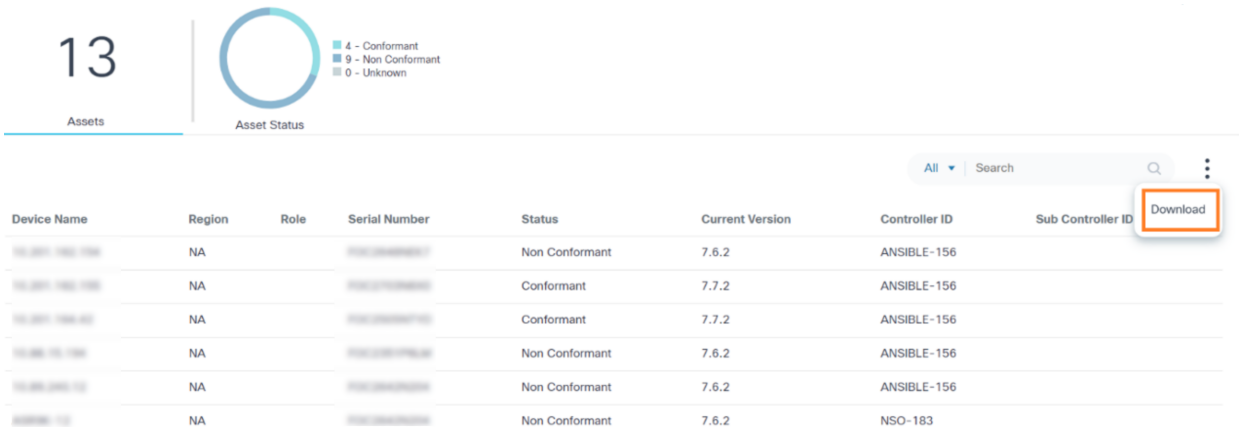
2. Selecione uma linha para exibir detalhes específicos do ativo juntamente com o status SMU e critérios adicionais.

Note: Os detalhes do SMU são exibidos somente para ativos de controladores NSO, CNC, ANSIBLE, Direct-to-Device e NDFC. Os módulos EPLD são exibidos somente para controladores NDFC.



Exibir resultados

3. Na coluna Action de um dispositivo, selecione o ícone More Options > View Results.



Download

4. Selecione o ícone More Options > Download para fazer o download dos resultados no formato .csv com o status de disponibilidade SMU.

Modo de Exibição de Planilha do Excel

Note: Exibir resultados exibe apenas os resultados da verificação de conformidade executada mais recentemente. Os usuários podem apenas exibir os ativos aos quais têm acesso. Para políticas não operacionais, a opção Exibir resultados está desativada.

Possíveis status do dispositivo:

- Conformidade: Indica que o dispositivo está em conformidade com a política definida
- Não Conformidade: Indica que o dispositivo não está em conformidade quando atendido com as seguintes condições:

Versão de Destino	SMU	Verificação de conformidade	Status
Não Conformidade	NA	NA	Não Conformidade
Conformidade	Indisponível	Falha nas Regras	Não Conformidade
Conformidade	Disponível	Falha nas Regras	Não Conformidade
Conformidade	Indisponível	Êxito nas Regras	Não Conformidade

- Desconhecido: Indica que a verificação de conformidade de software do dispositivo não pôde ser executada porque o dispositivo não tem informações de versão de software atuais.

Os critérios para o status Desconhecido incluem:

Versão de Destino	SMU	EPLD	Verificação de conformidade	Status
Não Conformidade	NA	NA	NA	Não Conformidade
Conformidade	Indisponível	Não Conformidade	Falha nas Regras	Não Conformidade
Conformidade	Indisponível	Conformidade	Falha nas Regras	Não Conformidade
Conformidade	Disponível	Conformidade	Falha nas Regras	Não Conformidade
Conformidade	Disponível	Não Conformidade	Falha nas Regras	Não Conformidade
Conformidade	Indisponível	Conformidade	Êxito nas Regras	Não Conformidade
Conformidade	Indisponível	Conformidade	Êxito nas Regras	Não Conformidade

Possíveis status SMU:

- Disponível: Indica que o SMU está presente no dispositivo e em um estado Ativo
- Indisponível: Indica que o SMU pode não existir ou que ele existe, mas está em um estado Inativo

Possíveis status do módulo EPLD:

- Conformidade: Indica que o módulo EPLD está presente no dispositivo com a versão de destino esperada
- Não Conformidade: Indica que o módulo EPLD está presente no dispositivo com a versão de destino esperada incompatível
- Módulo ausente: Indica que os módulos EPLD não estão configurados ou inscritos no dispositivo

Possíveis status do modelo de verificação de conformidade:

- Sucesso: Indica que o dispositivo executou com êxito o modelo de processo com comandos e regras válidos
- Falha: Indica que o dispositivo falhou ao executar o modelo de processo (por exemplo, quando os comandos estão incorretos)
- NA: Indica que o dispositivo não está qualificado para executar o modelo de processo (por exemplo, quando o dispositivo não está em conformidade com a versão de destino definida)

Note: A lista a seguir deve ser anotada.

- As verificações de conformidade de software funcionam somente com dispositivos pertencentes ao espaço padrão
- As verificações de conformidade de software dependem do inventário de ativos como a fonte verdadeira das versões de software atuais dos dispositivos. Se os dados do inventário de ativos estiverem obsoletos, os resultados das verificações de conformidade de software ficarão obsoletos. Para evitar o problema de dados obsoletos, use o recurso de verificação de inventário em tempo real ao iniciar a execução da política de conformidade
- O agendamento padrão pode ser alterado em Atualização de SO > Configurações > Conformidade de software
- Após a atualização para o BPA 5.1, todas as políticas preexistentes são movidas para um estado desativado; os usuários devem editar cada política, selecionar os valores apropriados, ativá-la e salvar as alterações para uso posterior

Política de atualização

O componente de política de atualização suporta dois tipos de políticas:

- Política em uma única etapa:
  - Qualquer um
  - <versão de origem específica (7.7.1)> - <versão de destino específica (7.7.2)>
- Política em várias etapas:
  - v7.7.1 - 7.7.2
  - v7.7.2 - 7.7.8
- A atualização em várias etapas pode incluir SMUs de bridge, como mostrado no exemplo abaixo:
  - v7.7.1 - v7.7.1[SMUs de ponte]
  - V7.7.1[SMUs de Bridge] - 7.7.8

O componente de política de atualização oferece a flexibilidade de predefinir os seguintes artefatos específicos da plataforma:

- Caminhos de upgrade
- Modelos ou fluxos de trabalho de pré e pós-validação
- Fluxo de trabalho de distribuição
- Fluxo de trabalho de ativação
- Fluxo de trabalho de backup
- Valores de tempo limite
- Reverter fluxo de trabalho
- Diferenças anteriores e posteriores válidas
- Fluxo de trabalho de desvio de tráfego ou fluxo de trabalho de reversão de tráfego

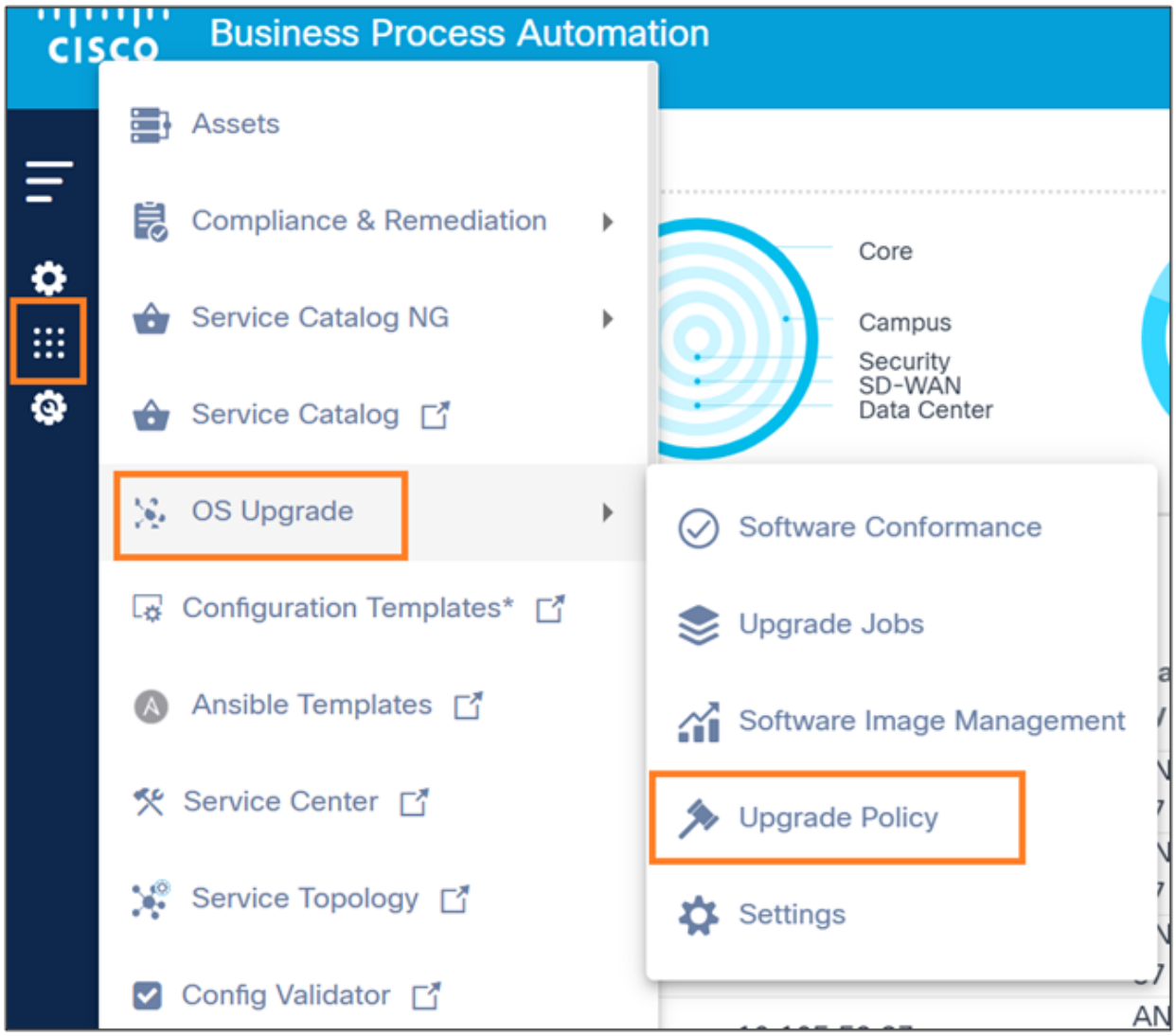
Pré-requisitos

- Modelos ou fluxos de trabalho de processo de pré e pós-validação necessários
- Fluxos de trabalho de backup, distribuição, ativação e reversão necessários
- Metadados de imagem necessários

Exibindo e Gerenciando Políticas de Atualização

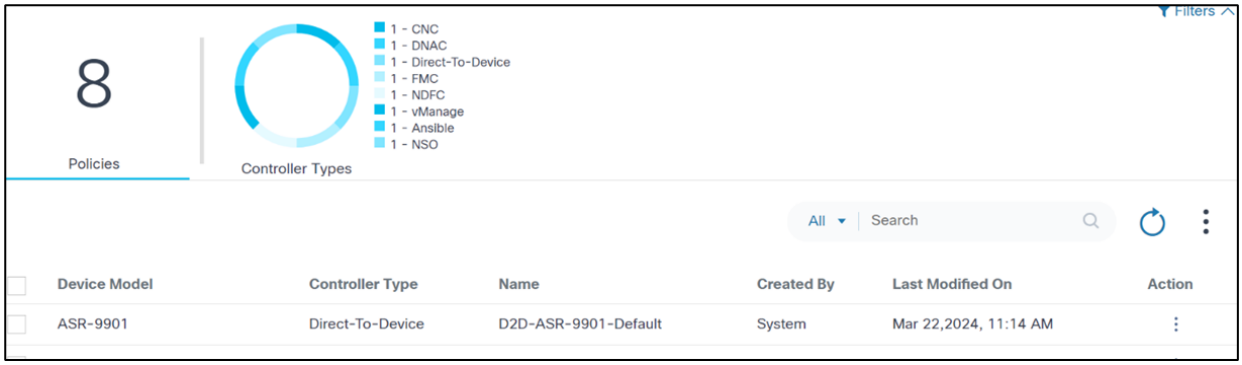
Para acessar a página Política de Upgrade:

1. Faça login no BPA com credenciais que tenham acesso suficiente à Política de atualização.



Navegação da Política de Atualização

2. Selecione OS Upgrade > Upgrade Policy. A página Atualizar Política é exibida.

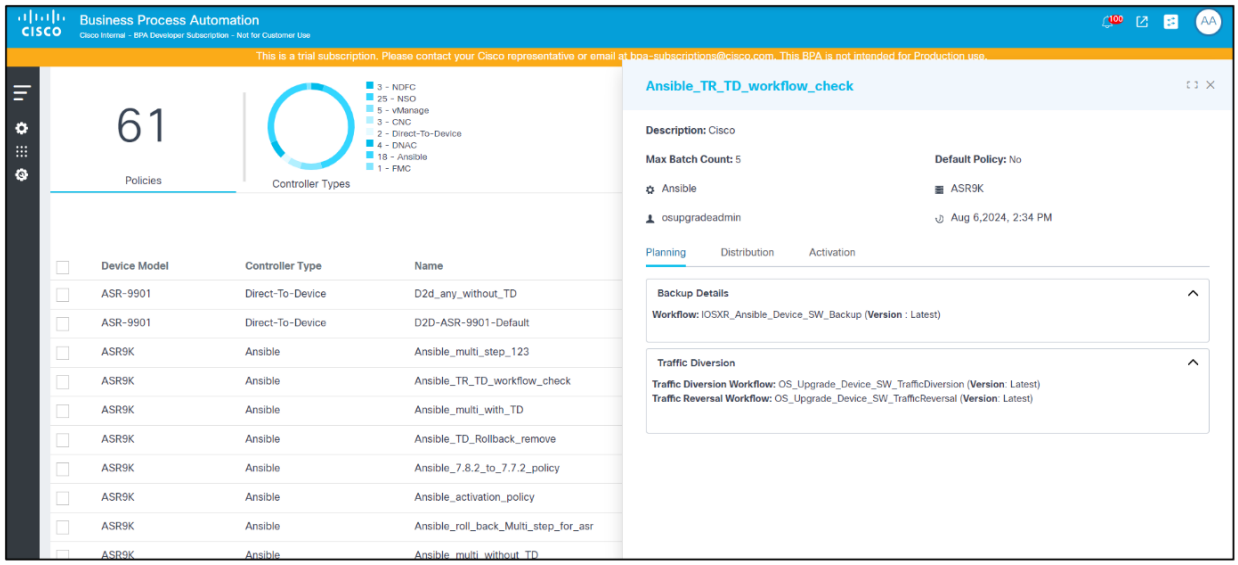


Política de atualização

A página Política de Upgrade contém o seguinte:

- Uma seção de análise, exibida na parte superior, que fornece o seguinte:

    - O número total de políticas de atualização no sistema
    - Um filtro rápido Tipos de controlador que fornece a capacidade de filtrar por tipo de controlador
- Um ícone de Mais opções que fornece a opção de Criar política e as ações de processamento em massa, como Excluir todas as políticas selecionadas
- Um filtro Pesquisar para pesquisar políticas que podem ser filtradas da seguinte maneira:
    - Todos: Pesquisar em todos os campos
    - Modelo do dispositivo: Procurar políticas com um modelo especificado
    - Nome: Procurar políticas com um nome de política especificado
    - Criado por: Procurar políticas com um usuário especificado
- Classificar políticas clicando nos respectivos nomes de coluna ou campos de tabela



Exibição de Detalhes da Política

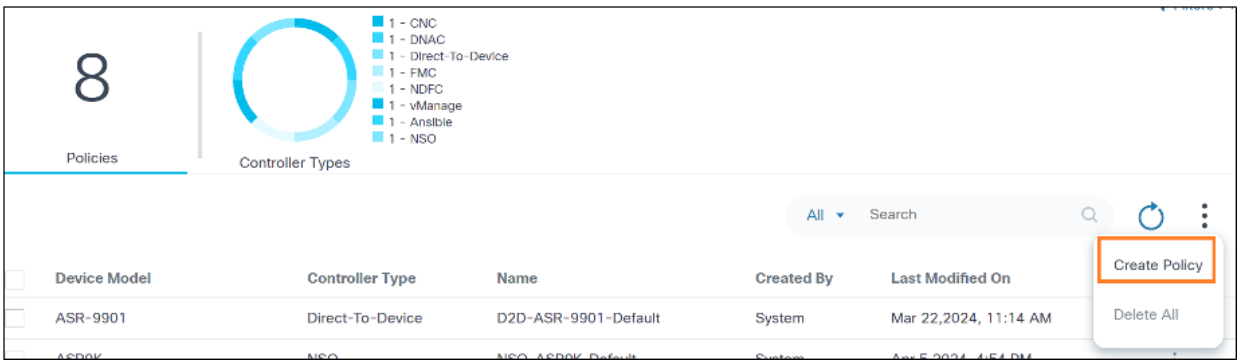
- Clicar em uma política específica ou exibir os detalhes de uma política

---

Note: O mesmo modelo de dispositivo e tipo de controlador pode ter qualquer número de políticas se os nomes das políticas forem exclusivos.

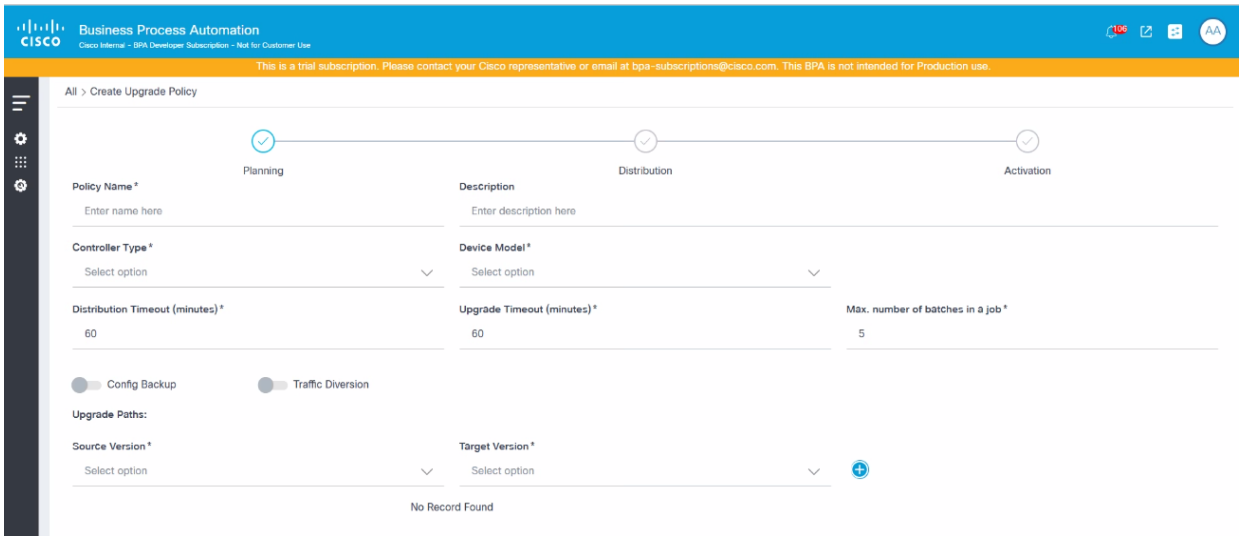
Criando políticas de atualização

1. Faça login no BPA com credenciais que tenham acesso de gerenciamento para Políticas de atualização.
2. Selecione OS Upgrade > Upgrade Policy. A página Atualizar Política é exibida.



Criar política

3. Selecione More Options > Create Policy. A página Criar Política de Atualização é exibida.



Criar Política de Atualização

Planejamento

1. Configure os parâmetros relacionados à política geral. A tabela abaixo fornece uma breve descrição de cada campo.

Campo	Descrição
Nome da política	Nome da política
Descrição	Breve descrição da política
Tipo de controlador	Controlador apropriado que é usado para realizar o upgrade do SO
Modelo do dispositivo	Modelo de dispositivo usado para executar a atualização do sistema operacional
Tempo limite de distribuição (minutos)	Tempo de espera máximo em minutos para a atividade de distribuição de imagem

Campo	Descrição
Tempo Limite de Atualização(minutos)	Tempo de espera máximo em minutos para a atividade de ativação de imagem
Número máximo de lotes em um trabalho	Número de lotes que podem ser adicionados a um trabalho; o número máximo de lotes permitidos é 20
Alternar backup de configuração	Ative esta opção se o backup for necessário e preencha os seguintes campos na janela para controladores vManage e Direct-to-Device: - Nome do fluxo de trabalho: O fluxo de trabalho de backup aplicável Note: Se não for possível encontrar os fluxos de trabalho, verifique se eles estão marcados corretamente com a marca OS Upgrade NextGen - Usar fluxo de trabalho mais recente: Se selecionado, a versão mais recente do fluxo de trabalho selecionado será usada - Versão do fluxo de trabalho: A versão personalizada do fluxo de trabalho; só pode ser selecionado se Usar fluxo de trabalho mais recente não estiver selecionado. Para controladores NDFC, NSO, CNC e Cisco Catalyst Center, o backup é feito por meio do serviço Backup and Restore. Portanto, uma política de backup e restauração deve ser selecionada na janela Detalhes do backup. Note: Os usuários devem selecionar a política apropriada para o tipo de controlador. Consulte a seção Backup and Restore para obter mais informações sobre políticas de backup e restauração.
Alternar desvio de tráfego	Para ativar o backup para dispositivos Nexus, a configuração do servidor scp do recurso deve estar presente nos dispositivos de destino. Ative esta opção se o desvio de tráfego for necessário e preencha os seguintes campos na janela Desvio de tráfego:

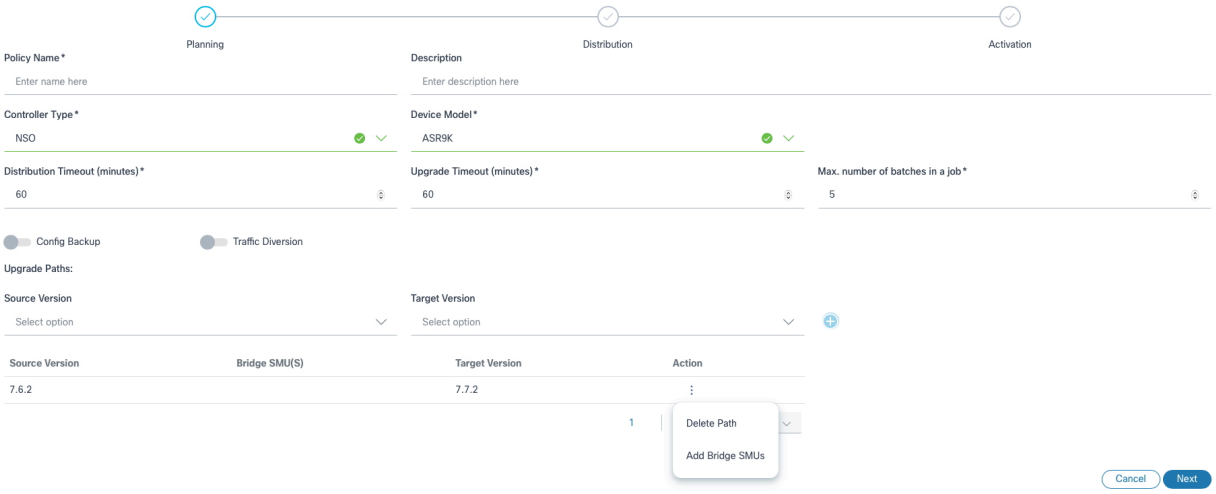
Campo	Descrição
	- Fluxo de trabalho de desvio de tráfego: O fluxo de trabalho de desvio de tráfego aplicável. Note: Se não for possível encontrar os fluxos de trabalho, verifique se eles estão marcados corretamente com a marca OS Upgrade NextGen - Fluxo de trabalho de inversão de tráfego: O fluxo de trabalho de reversão de tráfego aplicável. Note: Se não for possível encontrar os fluxos de trabalho, verifique se eles estão marcados corretamente com a marca OS Upgrade NextGen - Usar fluxo de trabalho mais recente: A versão mais recente do fluxo de trabalho selecionado acima - Versão do fluxo de trabalho: A versão personalizada do fluxo de trabalho; só pode ser selecionado se Usar fluxo de trabalho mais recente não estiver selecionado
Caminhos de atualização	Os caminhos de upgrade definem os caminhos de upgrade de etapa aplicáveis; várias versões de origem e destino podem ser adicionadas nos campos a seguir para acomodar demandas variáveis - Versão de Origem: A versão inicial do caminho de atualização - Versão de Destino: A versão final do caminho de atualização - Versão de Origem (Qualquer) para Versão de Destino (Qualquer): Isso é disponibilizado selecionando Any para os campos Source Version e Target Version, que é o valor padrão para todos os modelos de dispositivo; neste cenário, as páginas Distribuição e Ativação fornecem um processo unificado para a atualização - Versão de Origem (Versão Específica) para Versão de Destino (Versão Específica): Isso é disponibilizado selecionando versões de imagem específicas disponíveis para o modelo do dispositivo; várias versões de origem e destino podem ser adicionadas; o número de entradas do processo de atualização de ativação e distribuição corresponde ao número de versões de origem e destino adicionadas, e cada uma

Campo	Descrição
	é apresentada como uma seção recolhível rotulada com as versões de origem e destino correspondentes. Um caminho de atualização exige que as SMUs obrigatórias sejam aplicadas na versão de origem antes de atualizar para a versão de destino, adicionando-as como SMUs de ponte ao respectivo caminho de atualização. Para obter mais detalhes sobre SMUs de Bridge, consulte a próxima seção.

SMUs de bridge

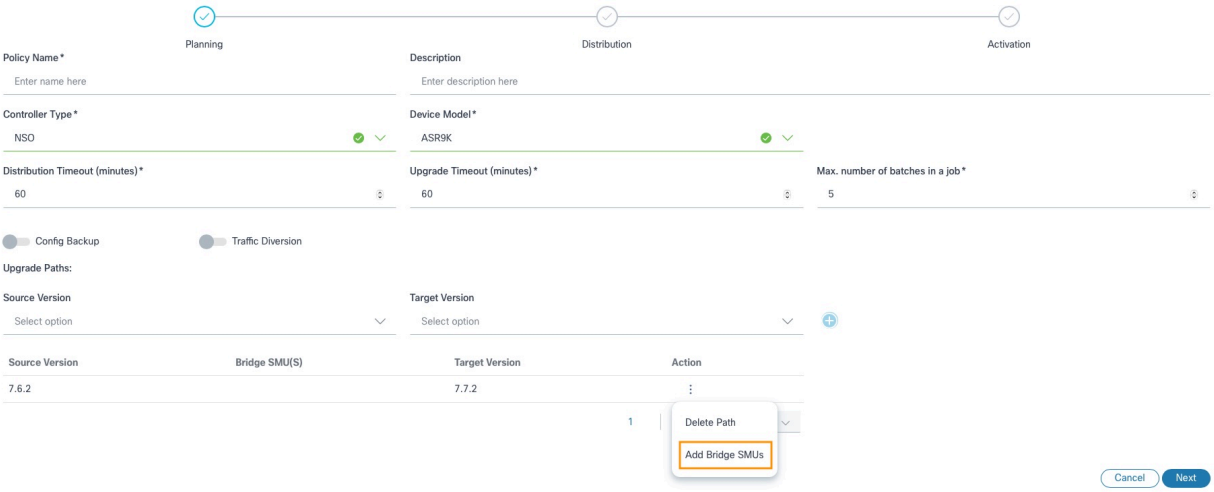
As SMUs de ponte, também chamadas de SMUs de atualização ou downgrade obrigatórias, são um pré-requisito e devem ser instaladas antes da atualização ou downgrade para outra versão de software da mesma plataforma ou modelo.

Adicionando SMUs de Bridge em um Caminho de Upgrade



Opções de caminho de atualização

1. Após adicionar um Caminho de Upgrade, selecione o ícone Mais Opções. As opções Delete Path e Add Bridge SMUs são exibidas.

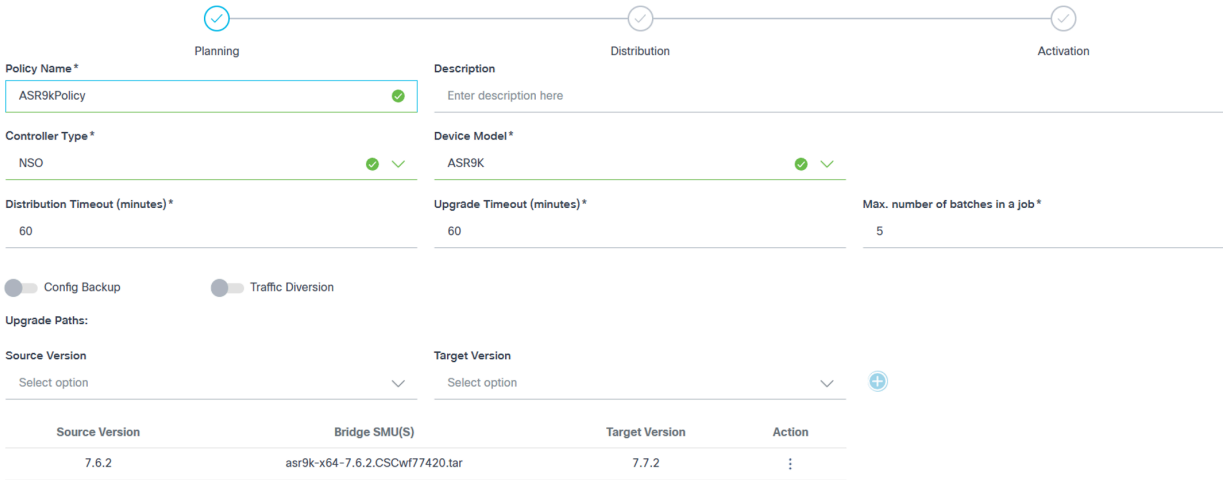


Adicionar SMUs de Bridge

2. Selecione Add Bridge SMUs. A janela Add Bridge SMUs é aberta. Todas as SMUs de Bridge disponíveis são exibidas para o caminho de atualização especificado.

Adicionar SMUs de Bridge

3. Na janela Add Bridge SMUs, marque as caixas de seleção apropriadas para adicionar Bridge SMUs ou desmarque as caixas de seleção para removê-las. Depois de adicionar os SMUs de Bridge, o caminho de upgrade é atualizado com os detalhes do SMU de Bridge selecionado.



Caminho de atualização com SMUs de ponte

Note: Cada caminho de upgrade que inclui SMU(s) de Bridge é considerado um upgrade de duas etapas na jornada de upgrade. Para o caminho de atualização mostrado na figura acima, o caminho de atualização final é:

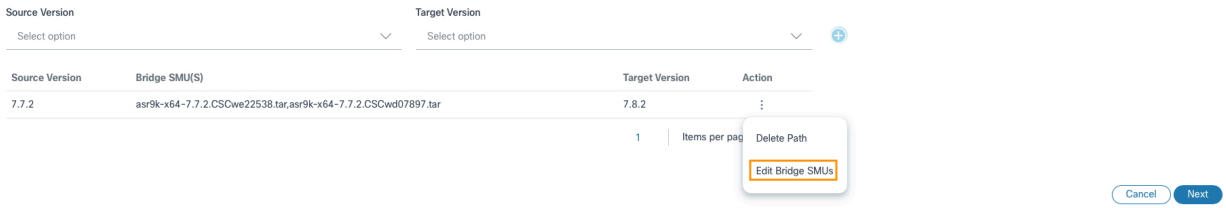
- 7.6.2 - 7.6.2 [SMUs de ponte]

Esse caminho representa a atualização do dispositivo em execução na v7.6.2 com as SMUs da Bridge.

- 7.6.2 [SMUs de ponte] - 7.7.2

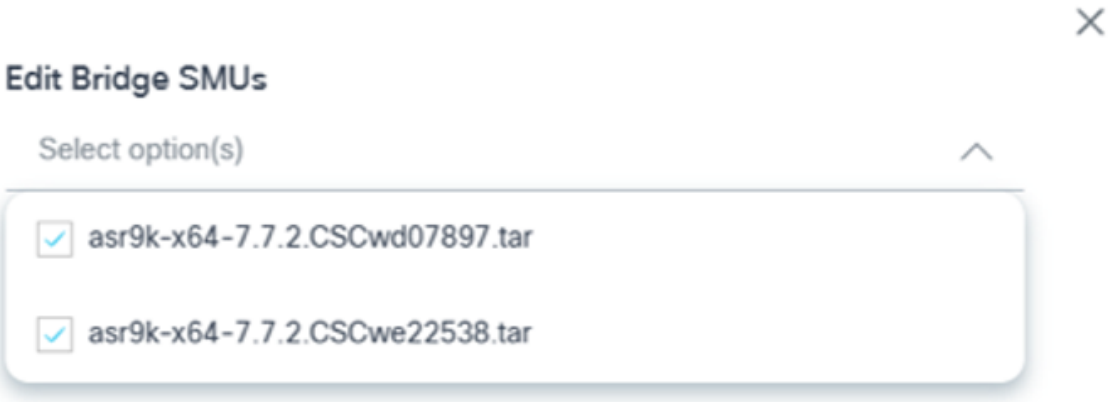
Esse caminho representa a atualização do dispositivo de v7.6.2 para v7.7.2. Nesse caso, a versão de origem do dispositivo é 7.6.2, incluindo as SMUs de Bridge aplicadas a ele.

Editando SMUs de Bridge



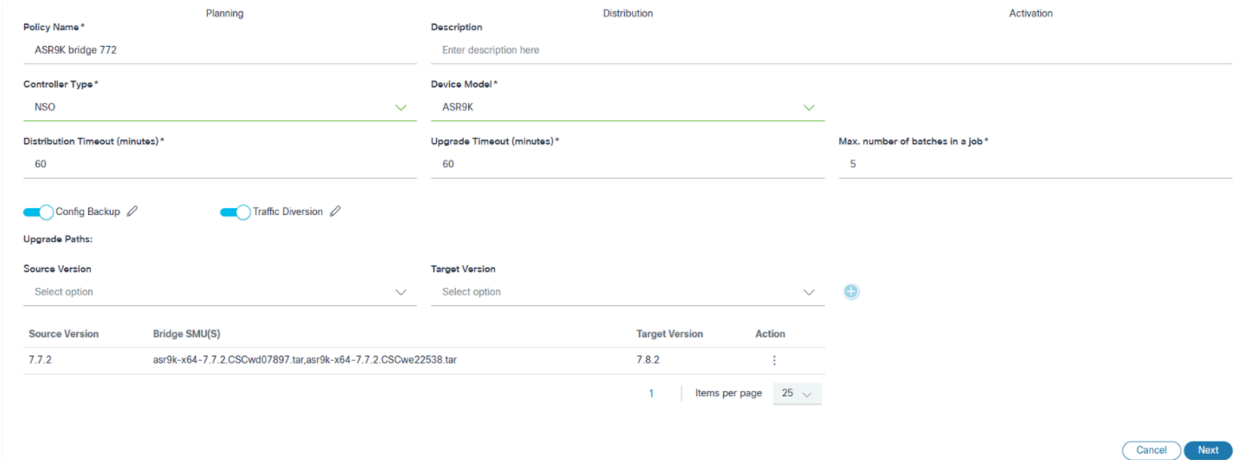
Caminho de atualização com SMUs de ponte

1. Na seção Upgrade Paths, selecione o ícone More Options > Edit Bridge SMUs. A janela Edit Bridge SMUs é aberta.



Editar SMUs de Bridge

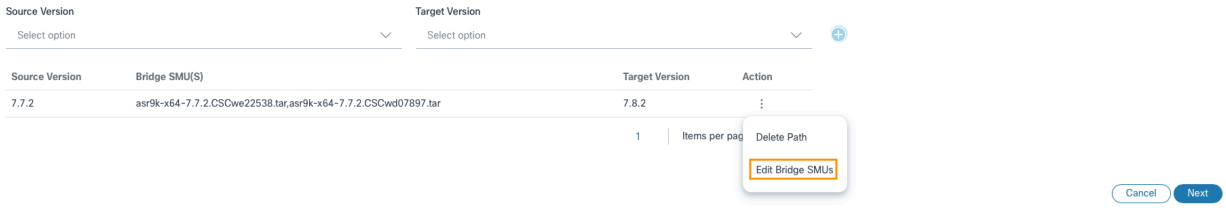
2. Marque ou desmarque as caixas de seleção apropriadas para atualizar os SMUs da Bridge.
3. Click OK. Um resumo das alterações é exibido.



Resumo das alterações

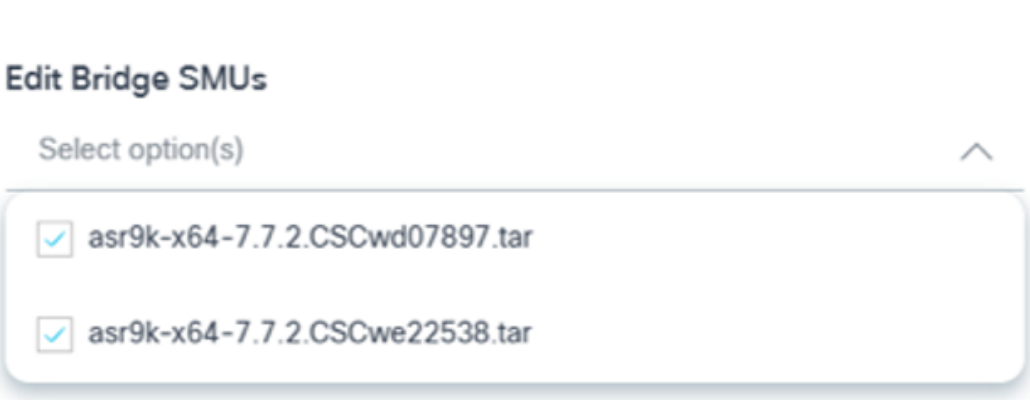
4. Verifique o resumo das alterações e clique em Avançar.

Excluindo SMUs de Bridge



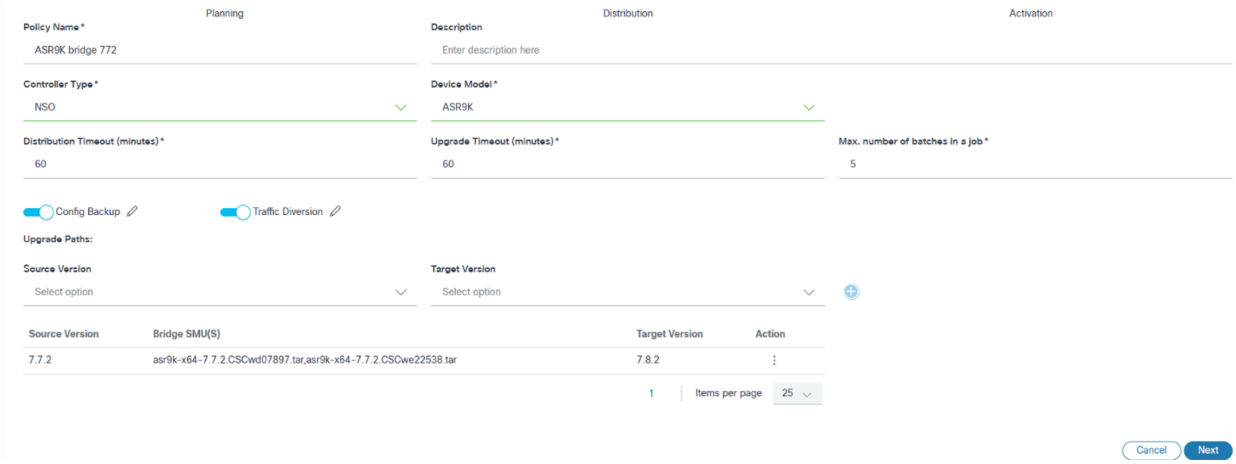
Editar SMUs de Bridge

1. Na seção Upgrade Paths, selecione o ícone More Options > Edit Bridge SMUs. A janela Edit Bridge SMUs é aberta.



Editar SMUs de Bridge

2. Desmarque as caixas de seleção apropriadas para remover as SMUs da Bridge.
3. Click OK. Um resumo das alterações é exibido.

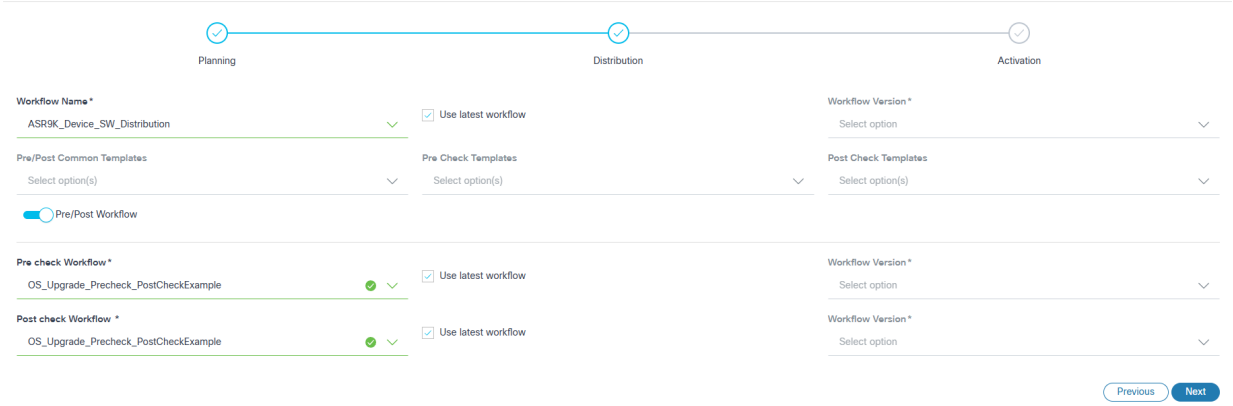


Resumo das alterações

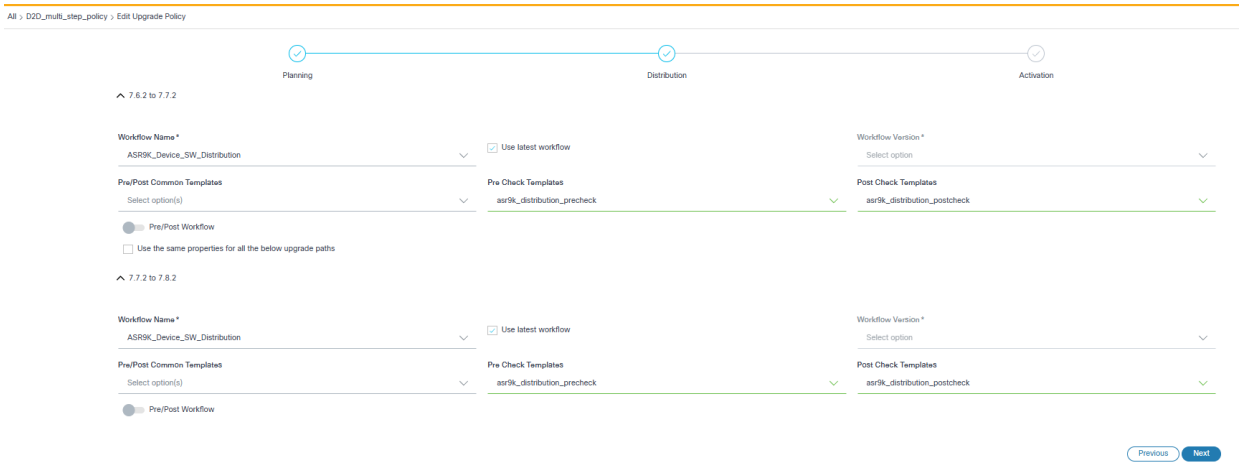
Distribuição

A distribuição utiliza parâmetros de entrada relacionados à distribuição de imagem (ou seja, cópia de imagem). As imagens a seguir são os parâmetros de entrada necessários para cada tipo de caminho de atualização.

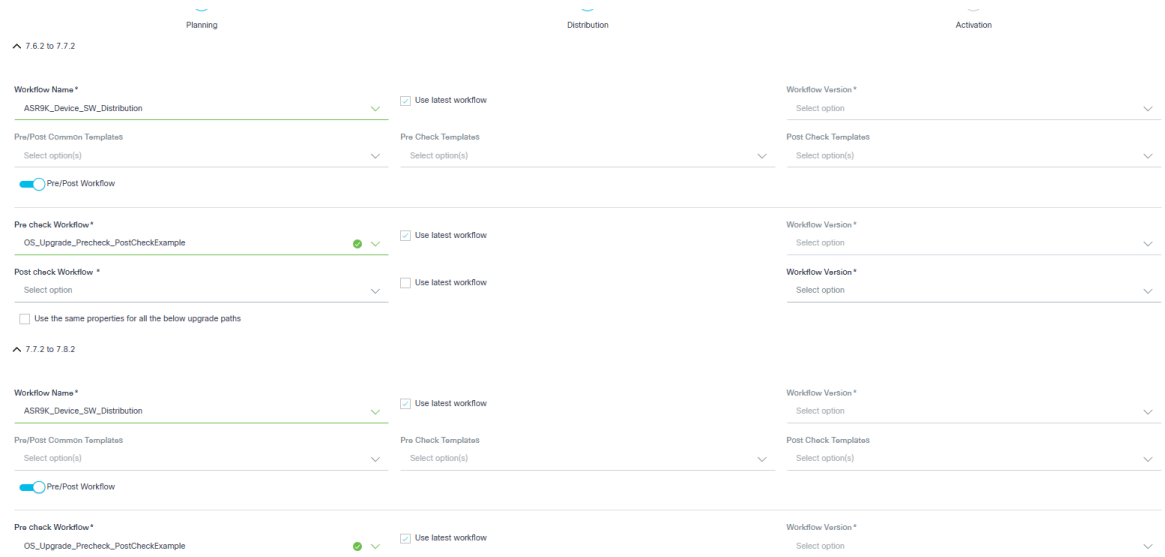
Seção de distribuição de imagem - Atualização de etapa única



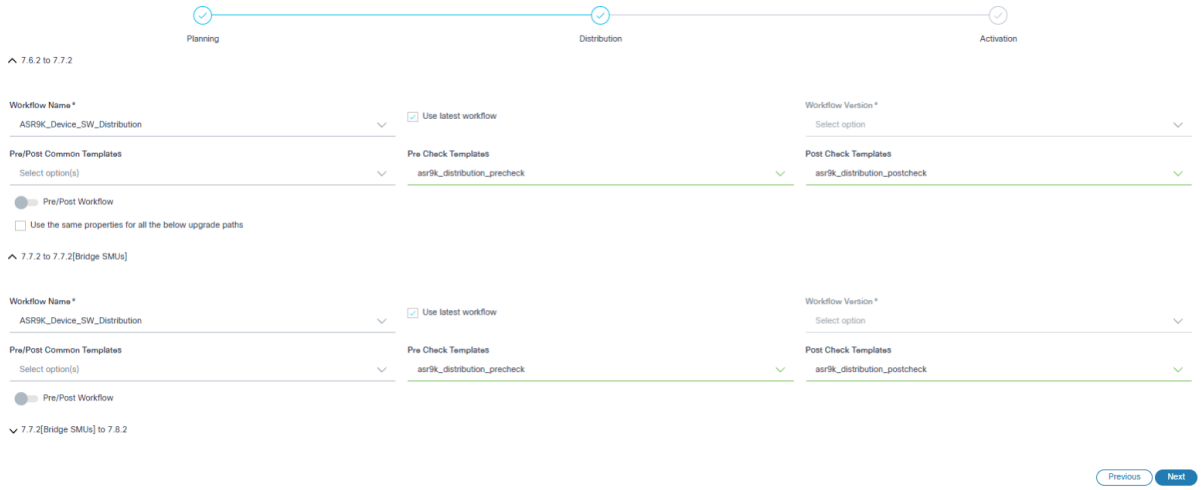
Seção de distribuição de imagem - Atualização de etapa única com alternância de pré/pós fluxo de trabalho ativada



Seção de distribuição - Atualização em várias etapas



Seção de distribuição - Atualização em várias etapas



Seção de distribuição - Atualização da ponte SMU

1. Configure os parâmetros relacionados à distribuição da imagem.
2. A tabela a seguir fornece uma breve descrição de cada campo.

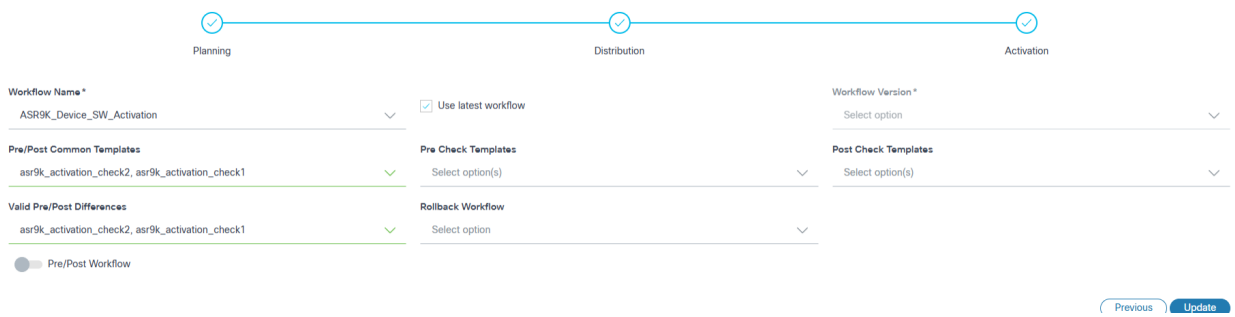
Campo	Descrição
Nome do Fluxo de Trabalho	O fluxo de trabalho de distribuição aplicável
Usar fluxo de trabalho mais recente	Selecionar a versão mais recente do fluxo de trabalho selecionado
Versão do Fluxo de Trabalho	A versão personalizada do fluxo de trabalho; isso só poderá ser selecionado se a caixa de seleção Usar fluxo de trabalho mais recente não estiver marcada
Modelos pré/pós-comuns	Os modelos de processo que são executados em ambos os estágios (isto é, pré-verificação e pós-verificação) Note: As verificações são específicas apenas para a Etapa de distribuição. Consulte Modelos de Processo para obter mais informações
Alternar Fluxo de Trabalho Pré/Pós	Permite que os usuários selecionem a execução de fluxos de trabalho pré ou pós-verificação dentro da Etapa de distribuição. Quando a alternância está ativada, somente os fluxos de trabalho pré ou pós-verificação podem ser configurados.
Fluxo de Trabalho de Pré-Verificação	Inclui os comandos executados somente durante a etapa de pré-verificação. Note: Essas verificações são específicas para a Etapa de distribuição.

Campo	Descrição
Fluxo de trabalho pós-verificação	O Fluxo de trabalho pós-verificação compreende os comandos executados exclusivamente durante a etapa pós-verificação. Note: Essas verificações são específicas para a Etapa de distribuição.
Modelos de pré-verificação	Os modelos de processo que contêm comandos exclusivos de pré-verificação; os modelos são executados somente durante a etapa de pré-verificação. Note: As verificações são específicas apenas para a Etapa de distribuição.
Modelos de pós-verificação	Os modelos de processo que contêm comandos exclusivos de pós-verificação; os modelos são executados somente durante a etapa pós-verificação. Note: As verificações são específicas apenas para a Etapa de distribuição.
Usar as mesmas propriedades para todos os caminhos de upgrade abaixo	Propriedades consistentes são aplicadas em todos os caminhos de upgrade em upgrades de várias seleções. Note: Se for selecionada, as mesmas propriedades serão aplicadas a todos os caminhos de upgrade na atualização de seleção múltipla.

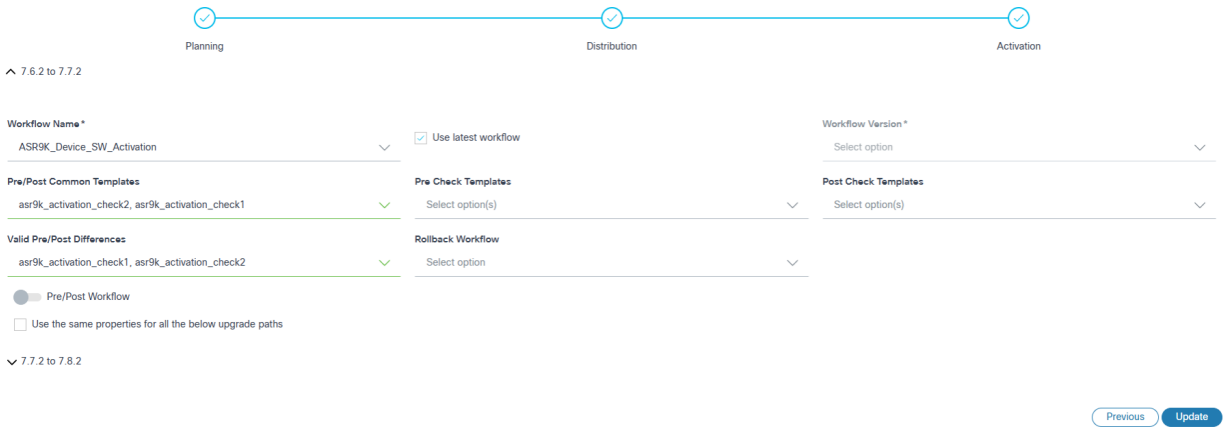
Note: Os fluxos de trabalho ou modelos de processo devem ser marcados adequadamente com a marca OS Upgrade Next-Gen.

3. Clique em Avançar para continuar na seção Ativação.

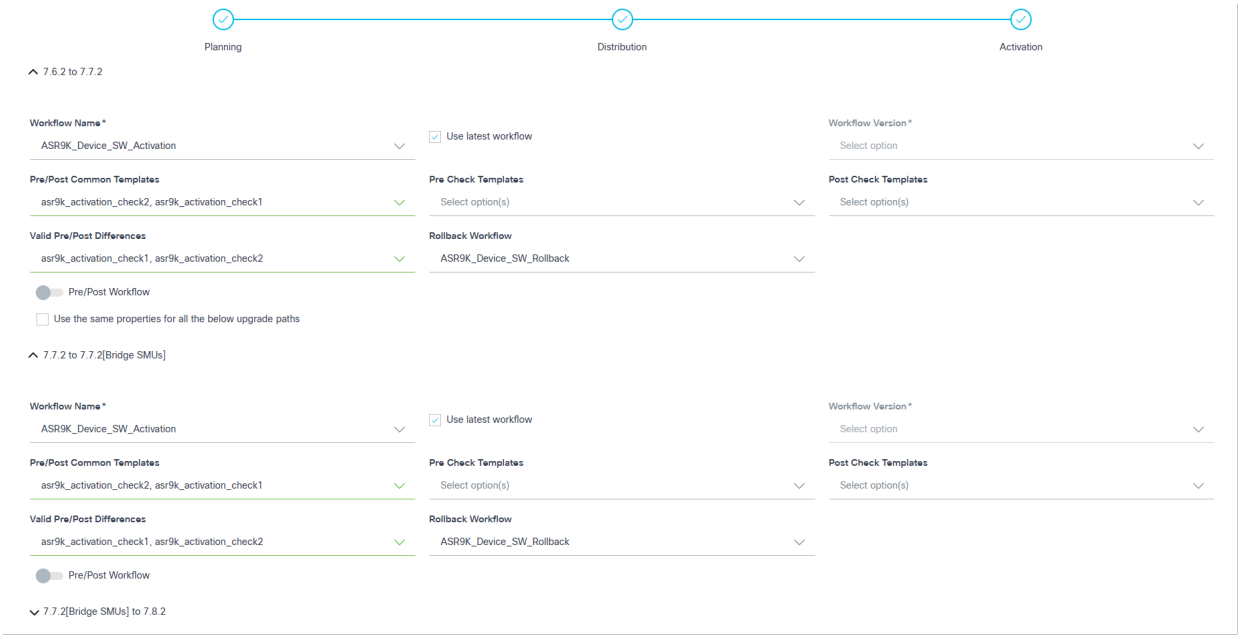
Ativação



Seção de Ativação - Atualização de Etapa Única



Seção de ativação - Atualização em várias etapas



Seção de Ativação - Atualização do SMU da Bridge

1. Configure os parâmetros relacionados à ativação da imagem.
2. A tabela abaixo fornece uma breve descrição de cada campo.

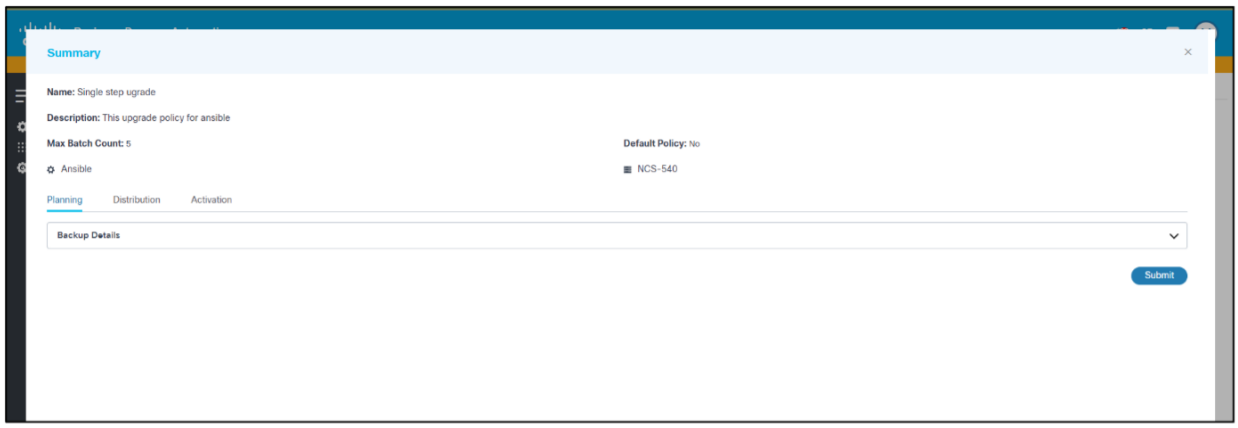
Campo	Descrição
Nome do Fluxo de Trabalho	O fluxo de trabalho de ativação aplicável
Usar fluxo de trabalho mais recente	Selecionar a versão mais recente do fluxo de trabalho selecionado
Versão do Fluxo de Trabalho	A versão personalizada do fluxo de trabalho; só pode ser marcada se a caixa de seleção Usar fluxo de trabalho mais recente não estiver marcada

Campo	Descrição
Modelos pré/pós-comuns	Os modelos de processo que são executados em ambos os estágios (isto é, pré-verificação e pós-verificação). Note: As verificações são específicas apenas para a etapa de Ativação. Consulte Modelos de Processo para obter mais informações
Modelos de pré-verificação	Os modelos de processo que contêm comandos exclusivos de pré-verificação; os modelos são executados somente durante a etapa de pré-verificação. Note: As verificações são específicas apenas para a etapa de Ativação.
Modelos de pós-verificação	Os modelos de processo que contêm comandos exclusivos de pós-verificação; os modelos são executados somente durante a etapa pós-verificação. Note: As verificações são específicas apenas para a etapa de Ativação.
Diferença Válida Pré/Pós	Os modelos de processo selecionados para ignorar as diferenças. Note: As verificações são específicas apenas para a etapa de Ativação.
Reverter Fluxo de Trabalho	O fluxo de trabalho de reversão aplicável. Note: Se um dos caminhos de atualização com o fluxo de trabalho de reversão for selecionado na atualização de seleção múltipla, todas as outras etapas de atualização serão selecionadas com o fluxo de trabalho de reversão por padrão.
Fluxo de Trabalho de Pré-Verificação	Esse fluxo de trabalho de pré-verificação personalizado consiste em comandos específicos cujos resultados de execução podem ser selecionados e revisados. É efetuada apenas durante a fase de pré-controlo. Note: Essas verificações são específicas para a Etapa de ativação.
Fluxo de trabalho pós-verificação	Esse fluxo de trabalho personalizado de pós-verificação consiste em comandos específicos cujos resultados de execução podem ser selecionados e revisados. É efetuada apenas durante a fase de pós-controlo. Note: Essas verificações são específicas para a Etapa de ativação.
Usar as mesmas propriedades para todos os caminhos de upgrade abaixo	Propriedades consistentes são aplicadas em todos os caminhos de upgrade em upgrades de várias seleções. Note: Se for selecionada, as mesmas propriedades serão aplicadas a todos os caminhos de upgrade na atualização de seleção múltipla.

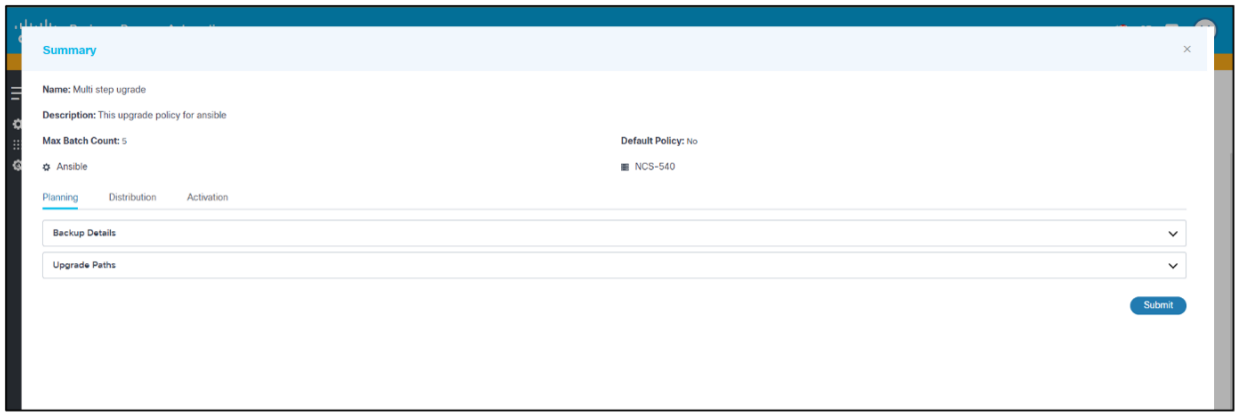
Note: Deve notar-se o seguinte:

- O algoritmo de chave pública necessário para dispositivos Nexus deve ser configurado no NSO.
- Configure os recursos de bgp, bfd e hsrp para executar modelos de pré e pós-verificação nos dispositivos Nexus.

3. Clique em Criar. Um resumo dos campos é exibido.



Resumo - Política de atualização em uma única etapa



Resumo - Política de atualização em várias etapas

4. Verifique o resumo dos campos e clique em Enviar. Uma notificação de progresso é exibida seguida por uma mensagem de confirmação. As políticas ficam visíveis na página após a criação bem-sucedida.

Políticas de atualização adicionais para outros modelos de dispositivo podem ser criadas conforme necessário.

Editando políticas de atualização

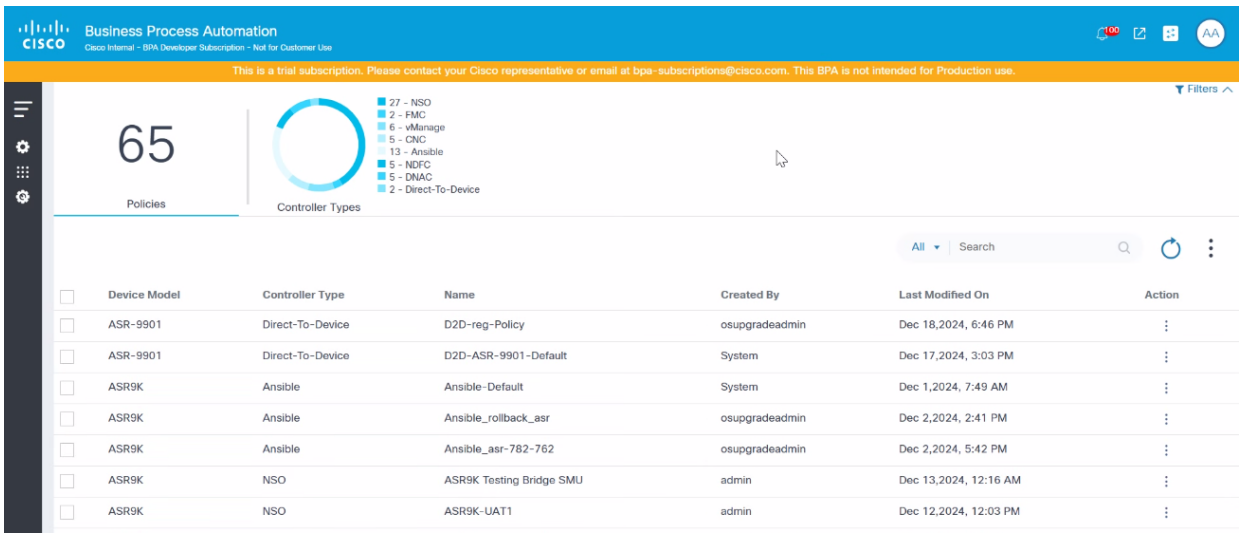
Resultado da Pesquisa de Política de Atualização

1. Na página Upgrade Policy, localize a política desejada usando o campo Search.

Editar política de atualização

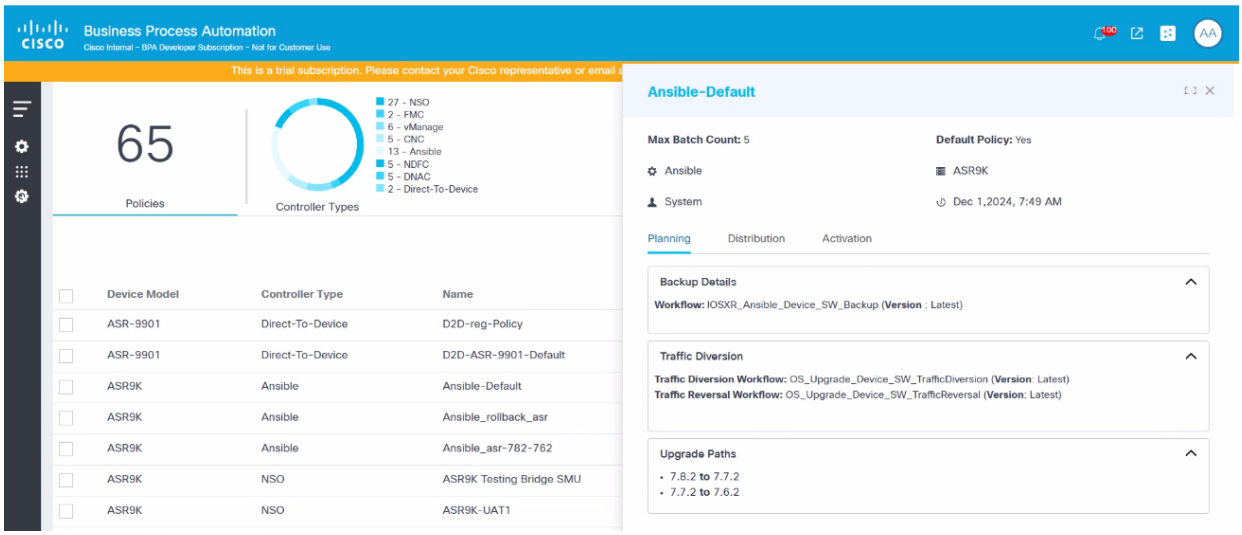
2. Na coluna Action da política, selecione o ícone More Options > Edit.
3. Atualize os campos relevantes e clique em Atualizar. Um resumo das alterações é exibido.
4. Verifique o resumo das alterações e clique em Enviar. As notificações de andamento são exibidas seguidas por uma mensagem de confirmação.

Exibindo Políticas de Atualização



Política de atualização

1. Na página Política de Upgrade, selecione a linha da política de upgrade desejada. A exibição de detalhes da política é aberta.



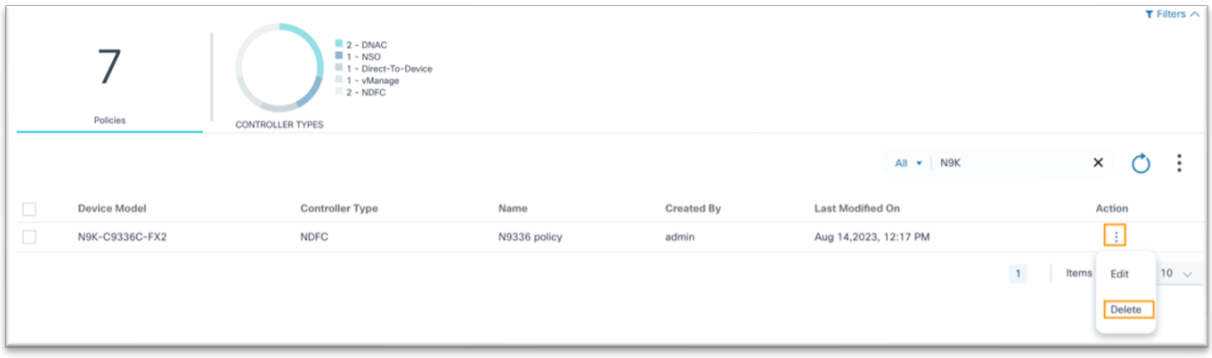
Atualizar Exibição de Detalhes da Política

Excluindo políticas de atualização

Note: As políticas padrão não podem ser excluídas, mas os usuários podem editar os modelos de processo e fluxos de trabalho.

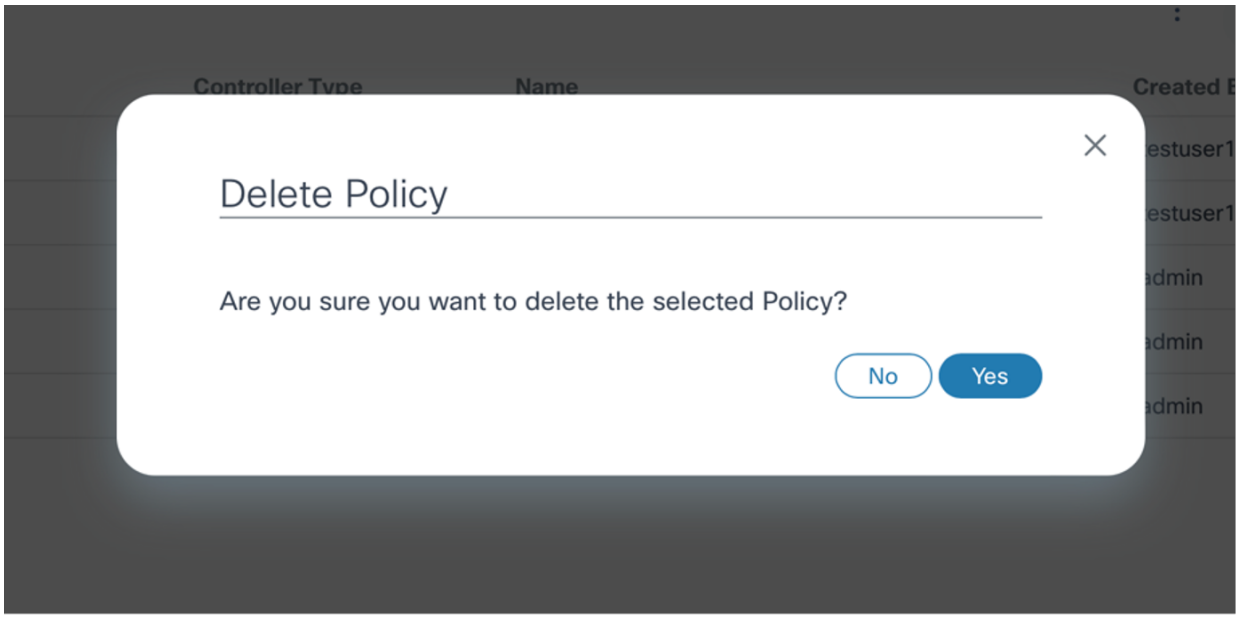
Política de atualização

1. Na página Atualizar Políticas, localize a política desejada usando o campo Pesquisar**.



Excluir Política de Atualização

2. Na coluna Action da política, selecione More Options > Delete. Uma janela de confirmação será aberta



Confirmação de Exclusão de Política

3. Clique em Sim.

Controlando o acesso a políticas de atualização

Este recurso fornece controle de acesso para políticas de atualização, restringindo que usuários não autorizados atualizem as políticas definidas no aplicativo de atualização do SO. Os administradores podem restringir o acesso definindo um grupo de recursos com políticas acessíveis.

Para criar um grupo de recursos:

1. Navegue até Configurações > Grupos de recursos.

2. Crie um grupo de recursos com políticas que usuários não administradores possam acessar. Os usuários não administradores que pertencem a este grupo de usuários agora têm acesso apenas às políticas disponíveis neste grupo de recursos.
3. Crie uma política de acesso para associar o grupo de recursos a um grupo de usuários,

Consulte Controle de Acesso para obter mais informações.

Note: É de notar o seguinte.

- É possível que os usuários selecionem os fluxos de trabalho incorretos para Distribuição e Ativação, resultando em comportamento não intencional. É responsabilidade do usuário mapear corretamente o fluxo de trabalho e verificar a aplicabilidade de marcos como Distribuição, Ativação, Reversão e Modelos de Dispositivo.
- Fluxos de trabalho e modelos de processo devem ser mapeados com a marca de próxima geração de atualização de SO para que estejam disponíveis para seleção ao criar ou atualizar políticas.
- As políticas OOB padrão criadas pelo usuário do sistema não podem ser excluídas, mas os usuários podem editar os modelos de processo e fluxos de trabalho.

Trabalhos de Atualização

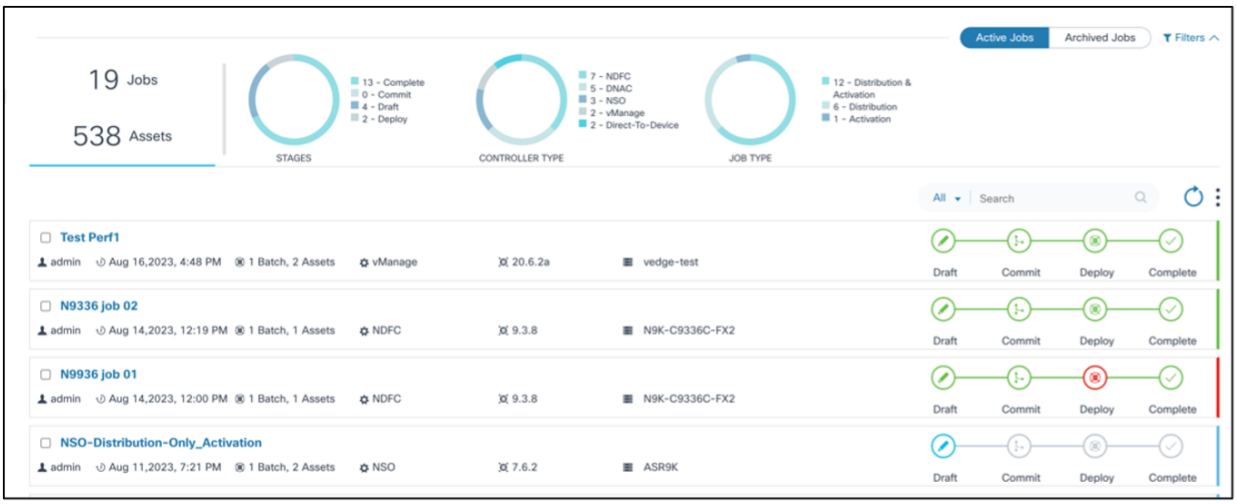
As atualizações de software são gerenciadas usando o aplicativo Trabalho de atualização, que é composto de um ou mais lotes com cada lote tendo um ou mais dispositivos de rede. Um trabalho pode ser criado no modo de rascunho e salvo várias vezes. As atualizações podem começar somente após o trabalho ser confirmado, permitindo que as operadoras planejem a alteração com antecedência.

Pré-requisitos

- Janela Manutenção Reservada para atualizações
- Pré-aprovações para Solicitação de Alteração de Atualização
- O serviço Backup e Restauração da Configuração deve estar ativo e em execução
- O serviço Agendador deve estar ativo e em execução
- Adaptadores BPA para sistemas externos (por exemplo, um sistema de tíquetes), se houver, devem ser integrados

Exibindo e Gerenciando Jobs de Atualização

1. Faça login no BPA com credenciais que tenham acesso a Jobs de Atualização.
2. Selecione OS Upgrade > Upgrade Jobs. A página Atualizar Job é exibida.



Trabalho de Atualização

A página Atualizar Job contém o seguinte:

Note: Por padrão, dez trabalhos são exibidos. Os números de página podem ser usados para navegar para outras páginas de trabalho.

- Uma alternância de Trabalhos Ativos e Trabalhos Arquivados que pode ser usada para alternar entre trabalhos ativos e arquivados
- Uma seção de análise, exibida na parte superior, que fornece o seguinte:
    - Total de trabalhos e ativos associados aos trabalhos
    - Gráfico de estágios com os seguintes filtros:
        - Rascunho: O trabalho está na fase de rascunho e ainda não foi comprometido
        - Consolidação: O trabalho é confirmado com todos os dispositivos, lotes ou agendamentos necessários até que o agendamento seja atingido
        - Implantar: A atividade de atualização foi iniciada para um ou mais lotes
        - Completo: A atividade de atualização foi concluída para todos os dispositivos que pertencem a todos os lotes
    - Gráfico de tipo de controlador: Permite a filtragem de tarefas por tipos de controladores Cisco Catalyst Center, vManage, NSO, NDFC, Direct-to-Device, CNC, ANSIBLE e FMC
    - Gráfico de tipos de tarefa com os seguintes filtros:
        - Distribuição: Trabalhos que executam preparo ou cópia de imagens do controlador para os dispositivos
        - Ativação: Trabalhos que executam a ativação ou atualização do software de um dispositivo
        - Distribuição e ativação: Trabalhos que executam a preparação ou a cópia e a ativação ou atualização do software de um dispositivo
- O campo Search que pode ser usado para executar uma pesquisa genérica em todos os metadados ou pelos campos Job Name e Created By

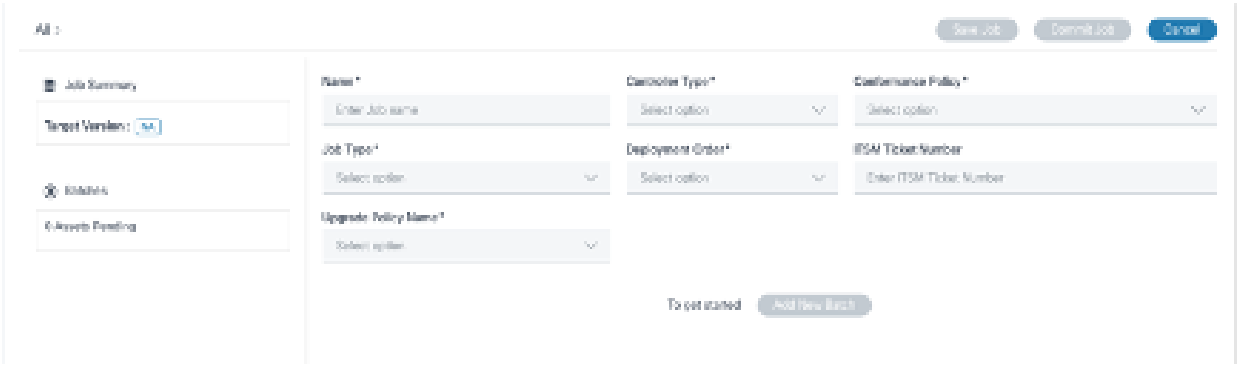
- O ícone Atualizar que pode ser usado para atualizar o resumo do trabalho e limpar os filtros do gráfico ou qualquer pesquisa personalizada no campo Pesquisar
- O ícone Mais opções que fornece opções para Criar um novo trabalho de atualização e para Arquivar ou Excluir trabalhos selecionados; os usuários podem selecionar ou cancelar a seleção de Todos
- As tarefas são exibidas como painéis e fornecem uma visão rápida das seguintes informações:
    - O ícone User Task será exibido com o número de tarefas de usuário se houver tarefas de usuário disponíveis
    - O usuário que criou o trabalho
    - A data de criação do trabalho
    - O número de lotes e ativos
    - O tipo de controlador (por exemplo, Cisco Catalyst Center, vManage, NDFC, Direct-to-Device, CNC, ANSIBLE ou FMC)
    - A versão de destino
    - O modelo de dispositivo aplicável
    - Uma exibição de etapa do projeto dos estágios do trabalho (isto é, Rascunho, Confirmar, Implantar e Concluir) com uma legenda de cor para cada etapa do projeto:
        - Cinza: A etapa não foi iniciada
        - Azul: Etapa do projeto em andamento
        - Vermelho: Questão de marco
        - Verde: Etapa concluída
    - Uma legenda colorida no final das etapas do projeto que exibe o status da tarefa:
        - Verde: O trabalho foi concluído
        - Vermelho: O trabalho tem problemas
        - Azul: Trabalho em andamento

Agendando Trabalhos de Atualização

Para criar um job:

Criar Opção de Trabalho de Atualização

1. Na página Atualizar Job, selecione o ícone Mais Opções > Criar Job. A página Criar Job de Atualização é exibida.



Criar Trabalho de Atualização

2. Insira um nome de trabalho no campo Nome.
3. Selecione o tipo de controlador (por exemplo, Cisco Catalyst Center, vManage, NDFC, Direct-to-Device, CNC, FMC, ANSIBLE ou NSO).
4. Selecione uma Política de conformidade que tenha dispositivos não compatíveis.

Note: Somente as políticas de conformidade que são executadas pelo menos uma vez e têm pelo menos um dispositivo não compatível estão disponíveis na lista, identificando automaticamente a política de atualização aplicável a ser usada quando uma política for selecionada.

Os detalhes a seguir são exibidos no lado esquerdo do formulário Criar Job em Resumo do Job:

- Modelo(s) de dispositivo afetado(s)

Note: Vários modelos de dispositivos são exibidos quando a política de conformidade selecionada tem mais de um modelo de dispositivo associado.

- Versão de destino
- Agregação de versões existentes e sua contagem correspondente
- Número máximo de lotes permitidos
- Número total de ativos não conformes

Note: Se a política de conformidade selecionada estiver associada a vários modelos de dispositivo, ela exibirá o agregado de ativos não compatíveis para todos os modelos associados.

- Opção de adicionar lote

5. Selecione um dos seguintes tipos de trabalho de atualização:

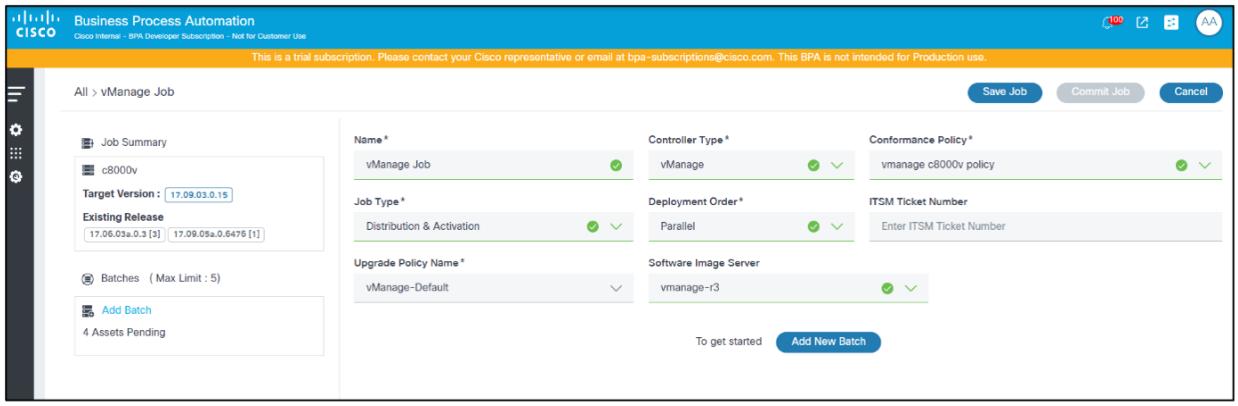
- Distribuição: Os trabalhos somente de distribuição são úteis quando a preparação da imagem do software ocorre antes da ativação real
- Ativação: As tarefas somente de ativação são úteis para executar atualizações de dispositivos para os quais a distribuição já foi concluída por meio de uma tarefa somente de distribuição
- Distribuição e ativação: A distribuição ou a preparação e a ativação de imagens ocorrem no mesmo trabalho, o que é útil em cenários em que uma ampla janela de manutenção está disponível para cobrir a cópia de imagens para um dispositivo e a atualização

6. Selecione o pedido de atualização. Vários dispositivos são processados ao mesmo tempo no modo Paralelo, enquanto os dispositivos são processados um por um no modo Sequencial.

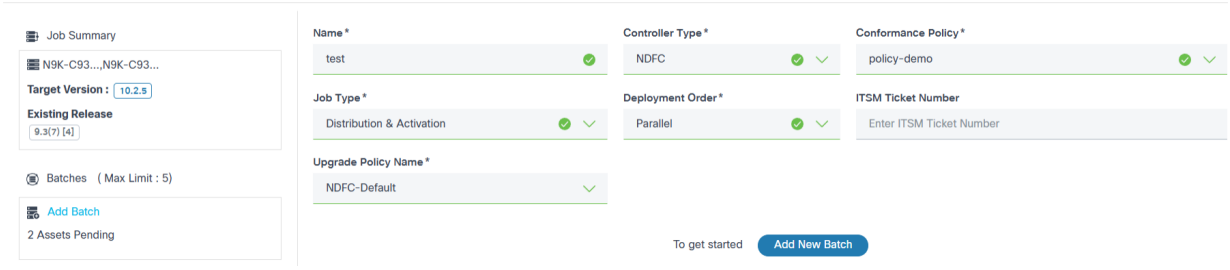
Note: O número máximo de dispositivos que podem ser processados no modo paralelo depende da configuração de implantação. A ordem de atualização selecionada é aplicável a todo o trabalho, mas pode ser substituída em um lote específico com base na necessidade.

7. Adicione o número da solicitação de alteração no campo IT Service Management (ITSM) Ticket Number.
8. Selecione o Nome da Política de Atualização. Somente as políticas de atualização aplicáveis são exibidas com base no tipo de controlador e no modelo de dispositivo de política de conformidade; os usuários podem selecionar uma das políticas de atualização. Se a política de conformidade de software tiver mais de um modelo associado, todas as políticas de atualização relevantes associadas a cada modelo serão exibidas. Os usuários devem selecionar cuidadosamente a política de atualização que funciona para todos os modelos.
9. Selecione o Servidor de imagem do software para especificar qual repositório de imagem do vManage (por exemplo, local ou remoto) é usado.

Note: Essa entrada só se aplica ao tipo de controlador do vManage.

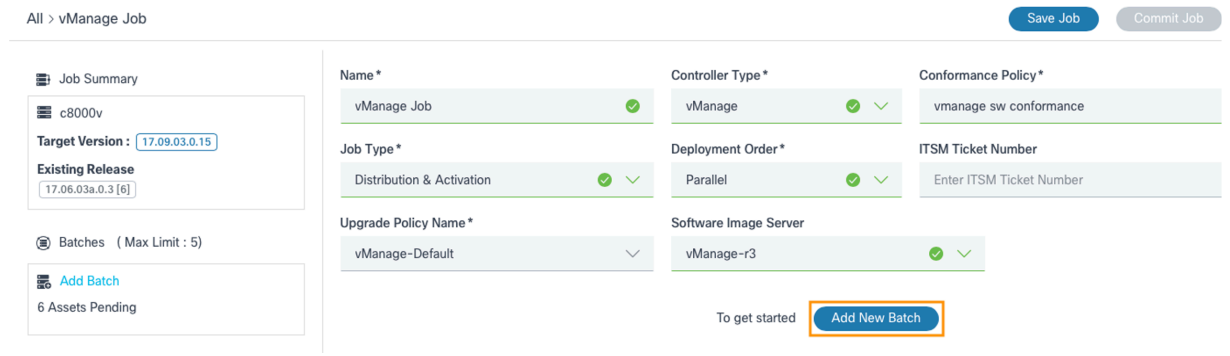


Criar Trabalho de Atualização com Detalhes Preenchidos (a política de conformidade tem um modelo)



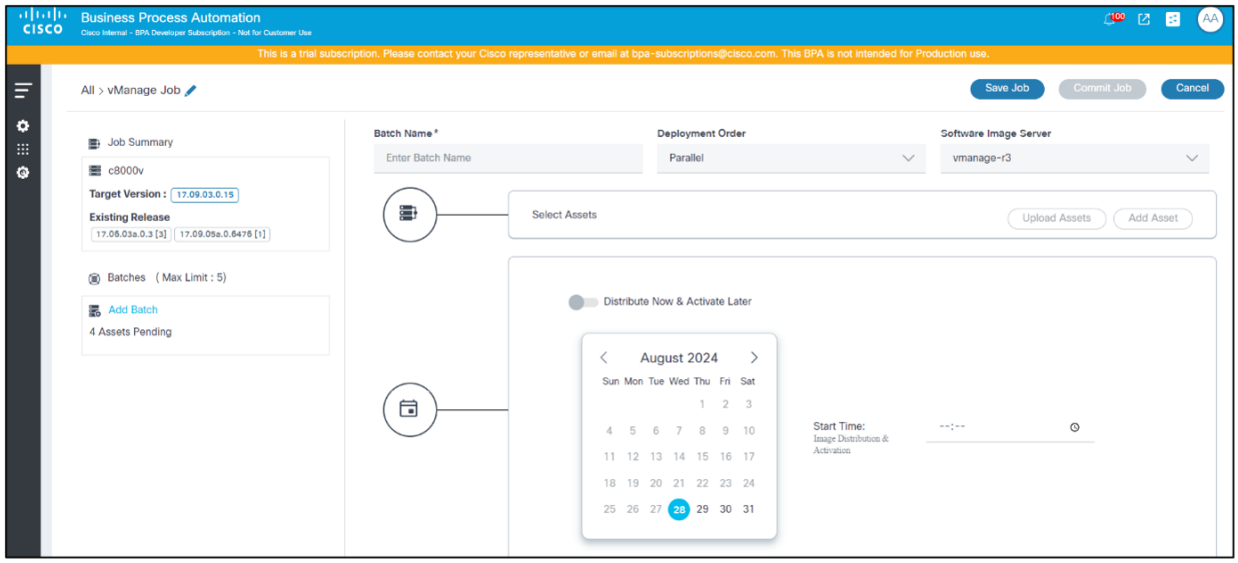
Criar Trabalho de Atualização com Detalhes Preenchidos (a política de conformidade tem vários modelos)

10. Clique em Salvar trabalho para salvar o rascunho até que o trabalho esteja pronto para ser confirmado.



Adicionar lote e Adicionar novo lote

11. Para adicionar um lote, clique no link Adicionar lote ou Adicionar novo lote. A janela Criação de lote é aberta.



Criação de Lote

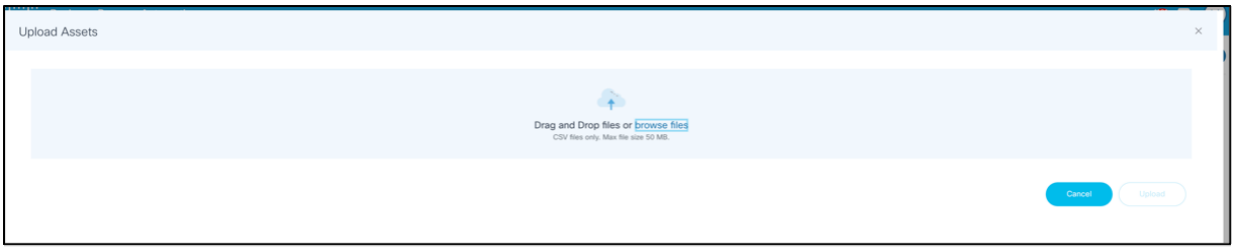
12. Insira um Nome do Lote relevante e selecione a Ordem de Implantação.

Note: O Tipo de Atualização selecionado aqui tem precedência sobre o selecionado na página Criação de Tarefa

13. Selecione o Servidor de imagem do software para especificar qual repositório do vManage (por exemplo, local ou remoto) é usado.

Note: Esse campo só se aplica ao tipo de controlador do vManage. O Servidor de imagem do software selecionado aqui tem precedência sobre aquele selecionado na página Criação de tarefa

14. Adicione ativos aos lotes. Os ativos podem ser adicionados a lotes de duas maneiras:



Fazer upload de ativos

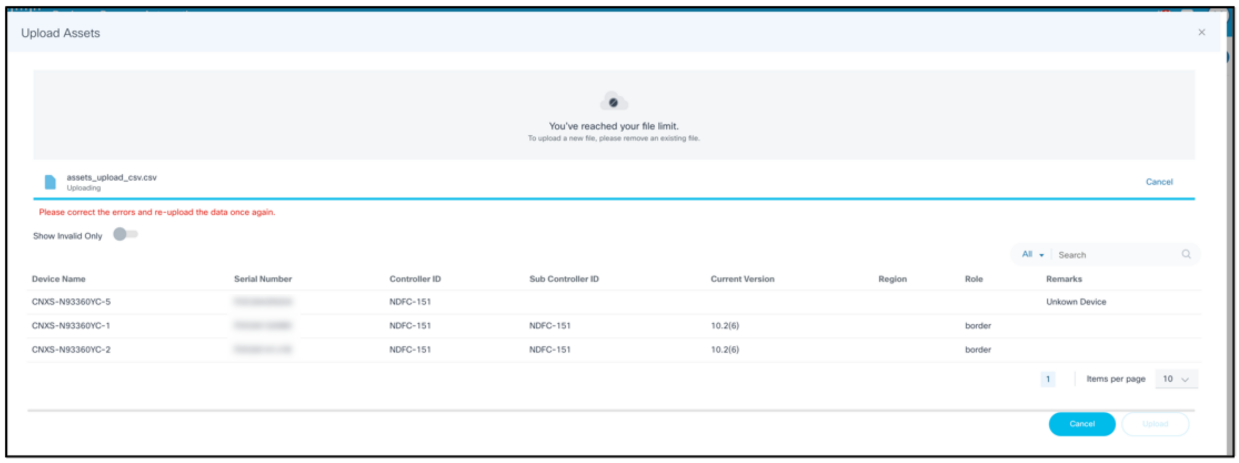
Opção 1:

a. Clique em Upload Assets. A janela Fazer upload de ativos é aberta.
b. Selecione um arquivo .csv para carregar.

Note: O arquivo .csv deve ter os seguintes detalhes:

- Nome de dispositivo: Nome do dispositivo ou ativo
- Número de série: Número de série do dispositivo
- ID do controlador: Nome do controlador que gerencia o dispositivo
- ID do subcontrolador: Nome da ID do subcontrolador que gerencia o dispositivo

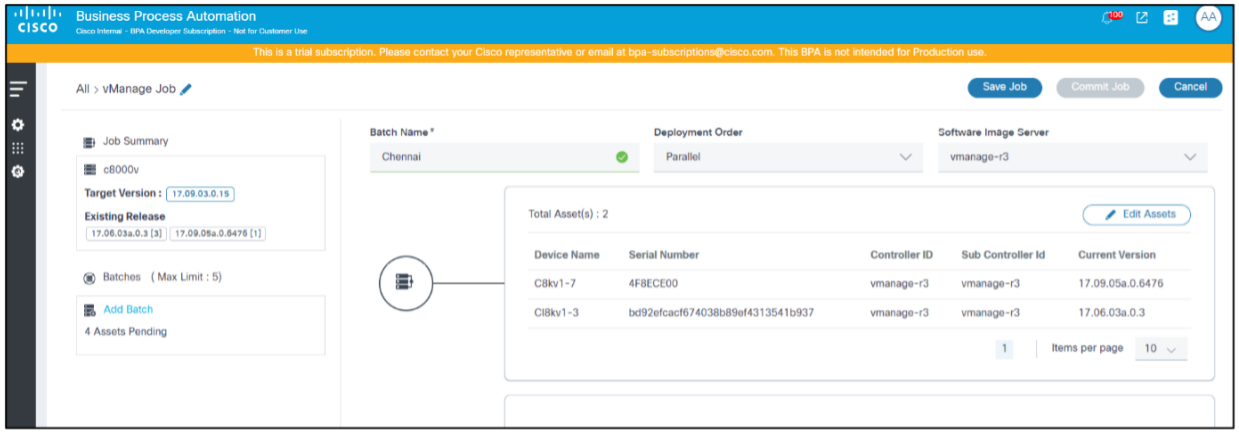
c. Clique em Fazer upload. Os dados do arquivo .csv são validados e os dados válidos e inválidos são exibidos. A opção Show Invalid Only pode ser usada para filtrar os dispositivos inválidos dos detalhes de ativos carregados.



Amostra de ativos carregados através do arquivo CSV

d. Se houver erros no arquivo carregado, corrija-os e carregue-o novamente.

Note: Os usuários só poderão prosseguir com a seleção de ativos se todos os dispositivos carregados forem válidos.



Adicionar lote - Ativos selecionados

Opção 2:

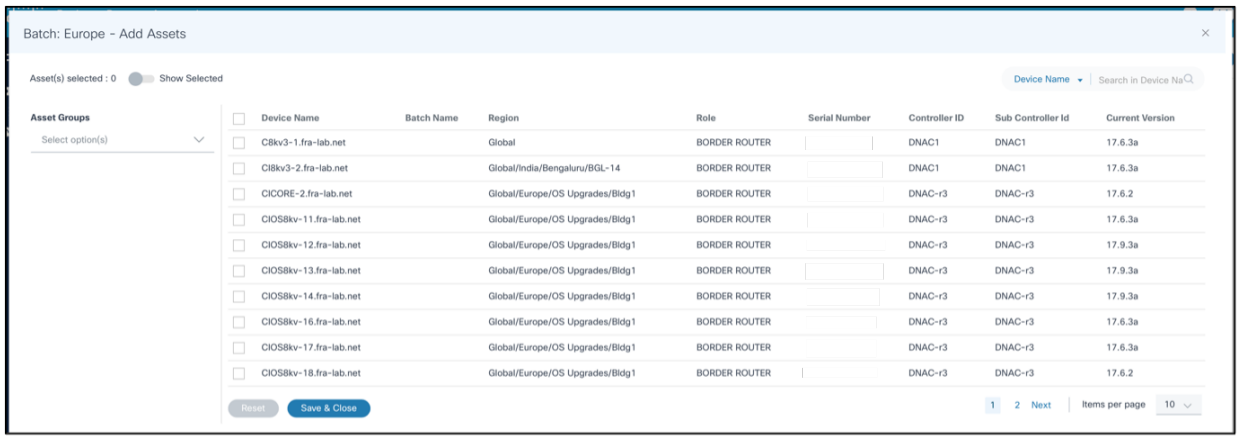
a. Clique em Add Assets. A janela Seleção de ativos é aberta.

Note: Fazer upload de ativos e Adicionar ativos não podem ser usados ao mesmo tempo.

b. Apenas para o tipo de controlador do FMC, selecione o nó de controle ou o nó autônomo para fazer a atualização.

Note: Dispositivos de dados não são permitidos no Trabalho de Atualização porque a

atualização de nós de dados é tratada pelo nó de controle.



Seleção de dispositivo

c. Selecione os dispositivos apropriados a serem incluídos no lote atual.

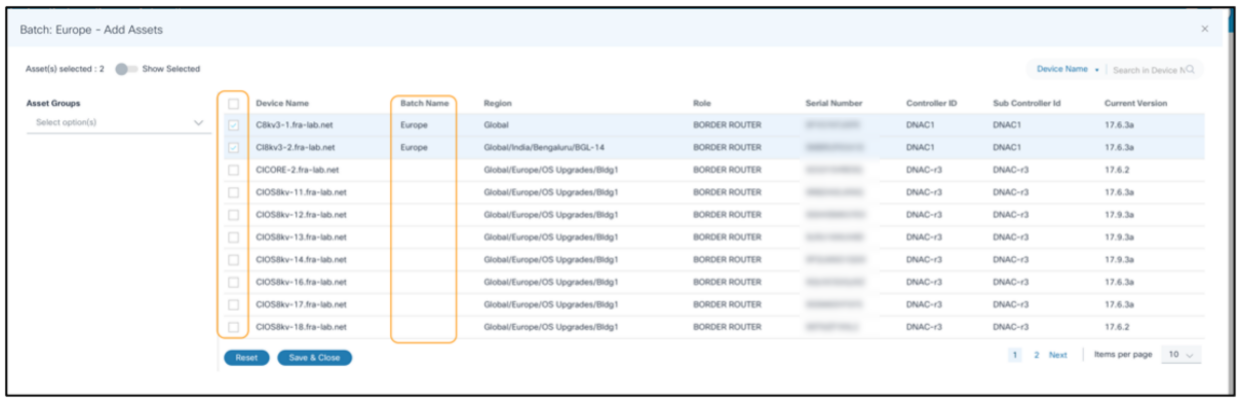
O filtro Search pode ser usado para filtrar dispositivos com base em diferentes atributos e todos os dispositivos que correspondem aos critérios de filtragem podem ser selecionados em massa marcando a caixa de seleção no cabeçalho da coluna Device Name. Os usuários também têm a opção de filtrar por Grupos de ativos.

A alternância Mostrar selecionado pode ser habilitada para exibir somente os ativos selecionados.

Note: Quando a alternância Mostrar selecionado está habilitada, o filtro Grupos de ativos está desabilitado.

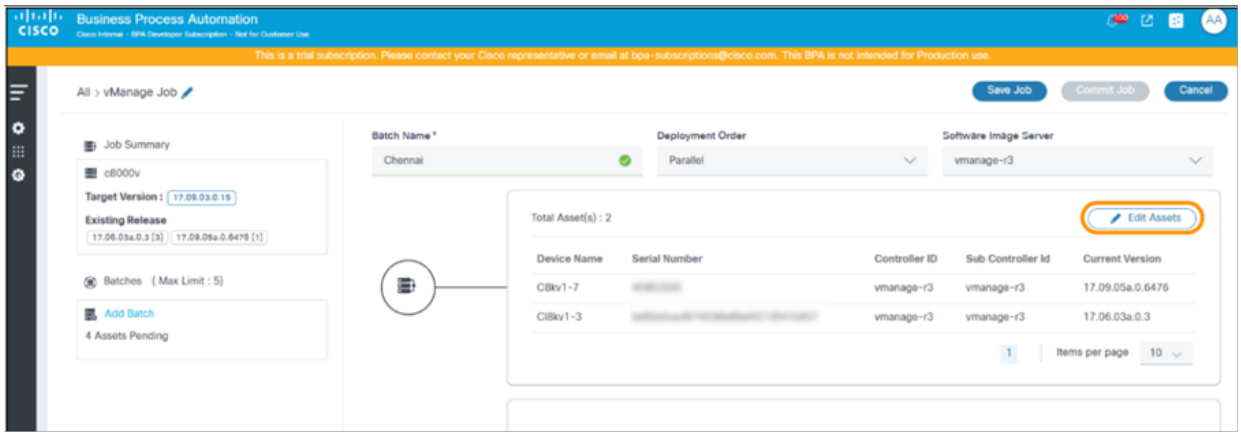
d. Clique em Salvar e Fechar.

Clicar em Redefinir descarta as seleções e mantém o estado original da seleção de ativos.



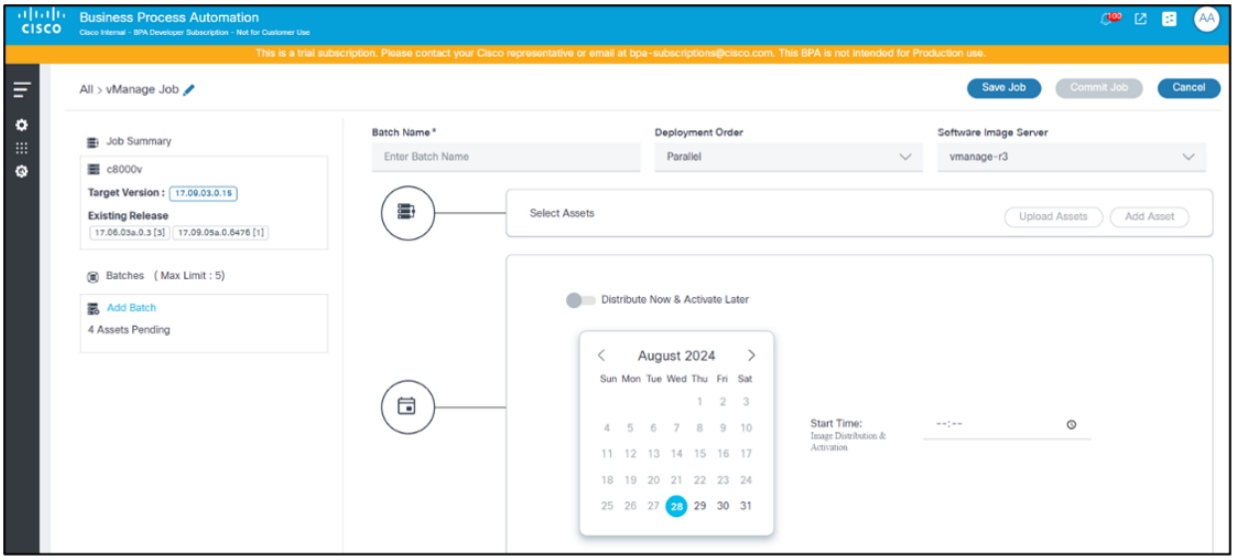
Reinicialização

e. Se a seleção de ativos precisar de modificação, clique em Editar ativos.



Ativos de edição em lote

f. Selecione ou limpe os ativos para fazer as alterações necessárias e clique em Salvar e fechar. Durante a edição dos ativos de lote, os ativos atualmente selecionados que fazem parte de um trabalho e lote diferentes podem ser identificados usando marcas de seleção e o nome do lote exibido na coluna Nome do lote.



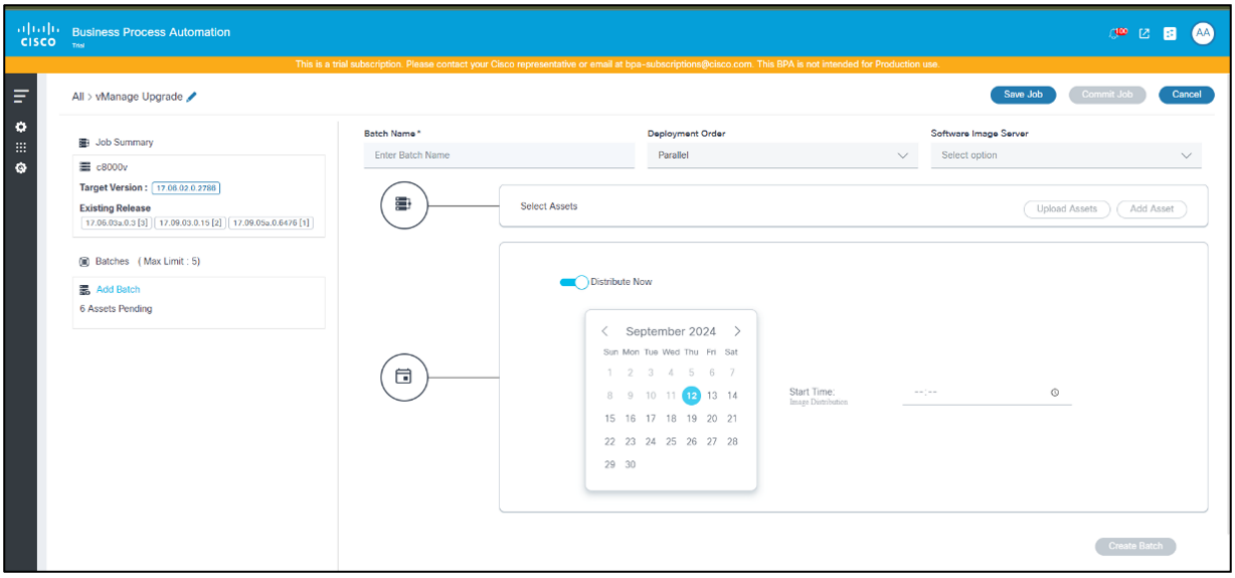
Atualizar Agendador de Trabalhos

15. Selecione uma data no selecionador de data e uma hora no selecionador de hora para agendar uma hora para disparar o tipo de atualização selecionado para o lote atual.

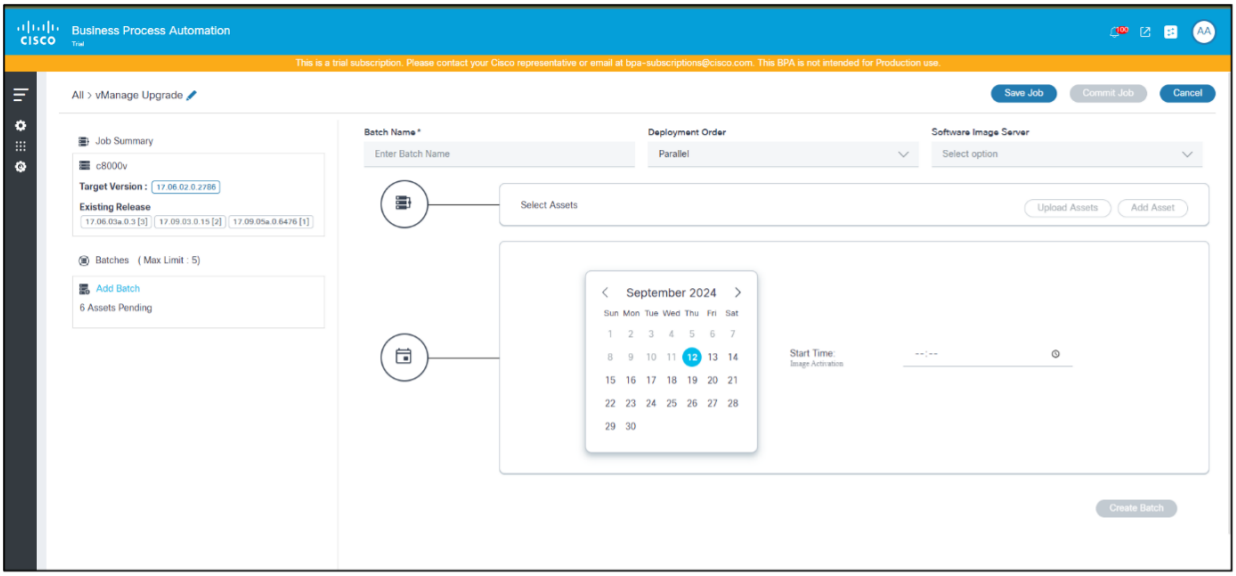
Note: O tipo de trabalho selecionado altera o tipo de agendamentos disponíveis.

Os cenários possíveis são os seguintes:

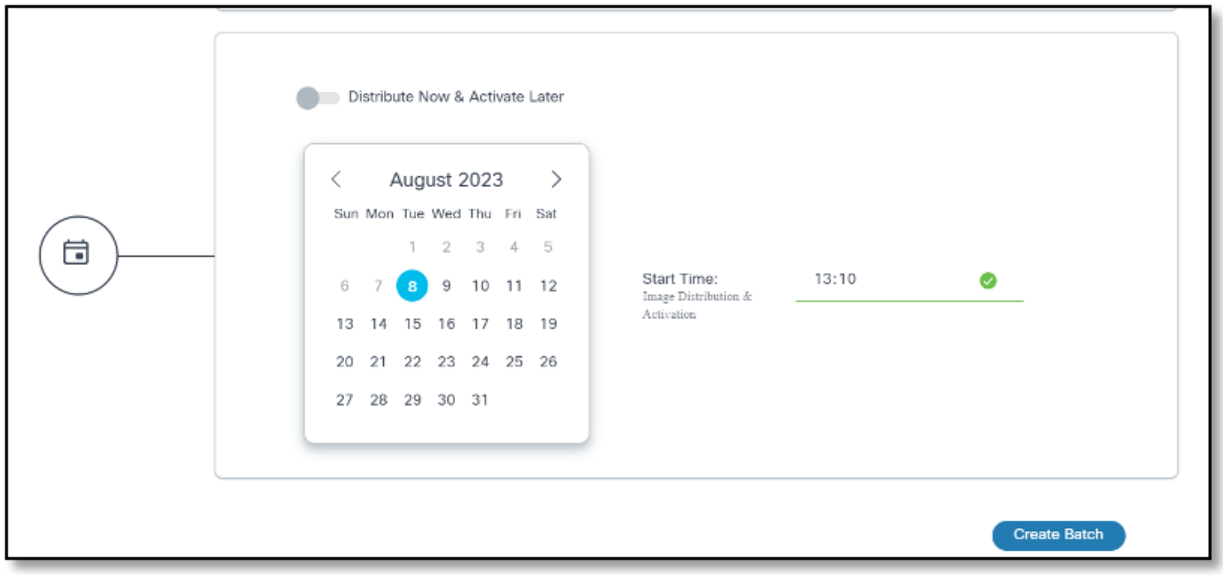
Tipo de Trabalho	Alternar Distribuir Agora	Data e Hora da Programação	Detalhes da distribuição
Distribuição	Desabilitado por padrão	Ativo	A distribuição ocorre na data e na hora agendadas especificadas
Distribuição	Habilitado	Desabilitado	A distribuição ocorre após a confirmação do trabalho
Ativação	N/A	Ativo	A ativação ocorre na data e na hora especificadas
Distribuição e ativação	Desabilitado por padrão	Ativo	A distribuição e a ativação ocorrem na data e na hora especificadas
Distribuição e ativação	Habilitado	Ativo	A distribuição ocorre após a confirmação do trabalho e os gatilhos de ativação na data e hora agendadas especificadas



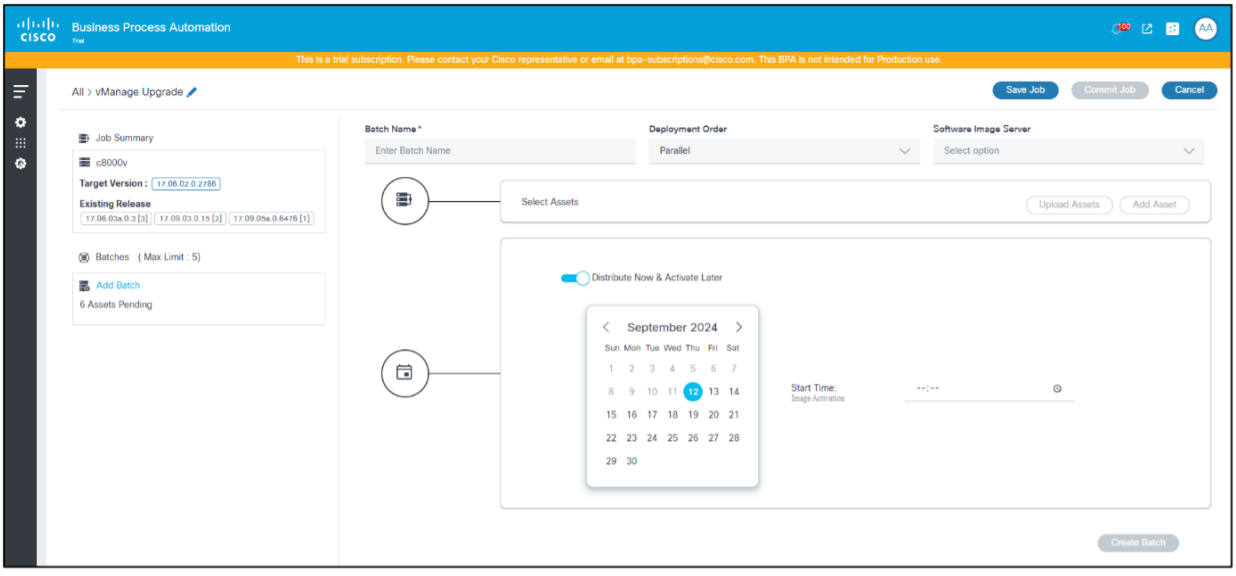
Opções de Programação do Tipo de Ordem de Produção de Distribuição



Opções de Programação do Tipo de Job de Ativação



Opções de agendamento do tipo de tarefa de distribuição e ativação

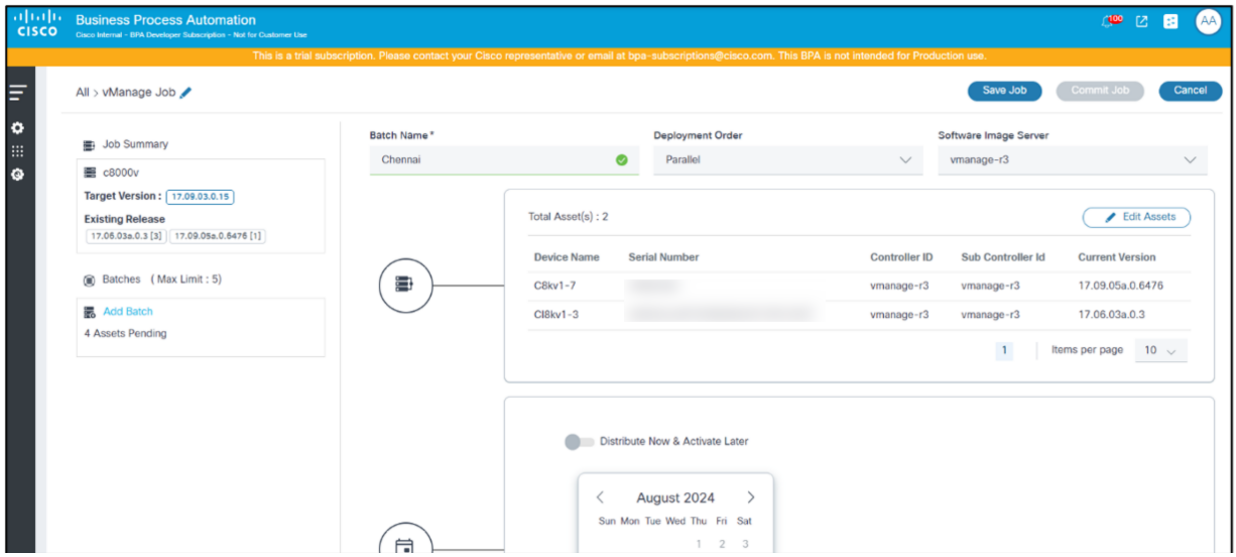


Tipo de tarefa de distribuição e ativação Opções de agenda com a opção Distribuir agora e ativar depois ativada

Note: A lista a seguir deve ser anotada.

- Ao agendar vários lotes, forneça um intervalo de tempo entre os dois lotes para que a sobrecarga do sistema possa ser evitada. Se os vários lotes estiverem sobrepostos, considere adicioná-los a um único lote.
- Quando a alternância Distribuir Agora e Ativar Depois estiver ativada, forneça um intervalo de tempo entre o horário de confirmação do job e o agendamento de ativação. Caso contrário, os fluxos de trabalho de ativação podem criar tarefas de usuário que exigem intervenção manual (ou seja, os usuários devem aguardar até a conclusão da distribuição e tentar novamente).

16. Clique em Criar lote. O lote pode ser exibido no lado esquerdo da página.



Criar Trabalho - Confirmar Trabalho

Crie quantos lotes forem necessários. Um trabalho pode estar no estado Rascunho até que todas as informações necessárias estejam disponíveis.

Note: Evite a perda de dados do trabalho clicando em Salvar trabalho para salvar o rascunho.

17. Clique em Confirmar trabalho para finalizar a criação do trabalho. O trabalho passa para o estado Implantar quando o agendamento é disparado para qualquer um dos lotes.

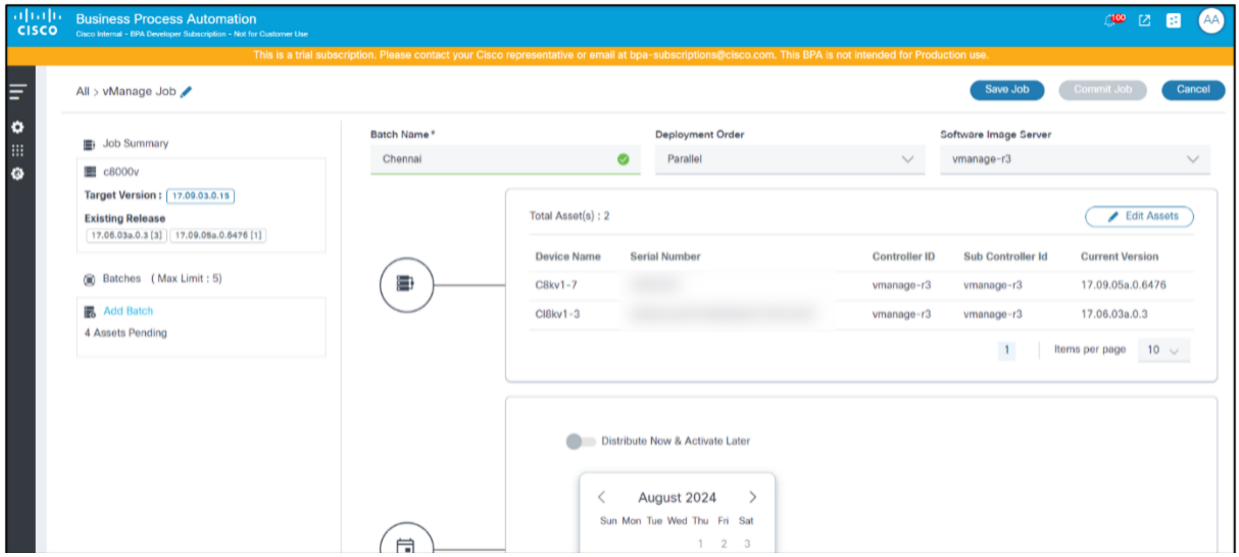
Note: O limite para o número máximo de lotes pode ser estendido ou atualizado na página

Política de Upgrade.

Edição de um Lote em um Job

Note: Os lotes só podem ser atualizados quando o trabalho está no estágio Rascunho.

1. Selecione o lote desejado no painel esquerdo.

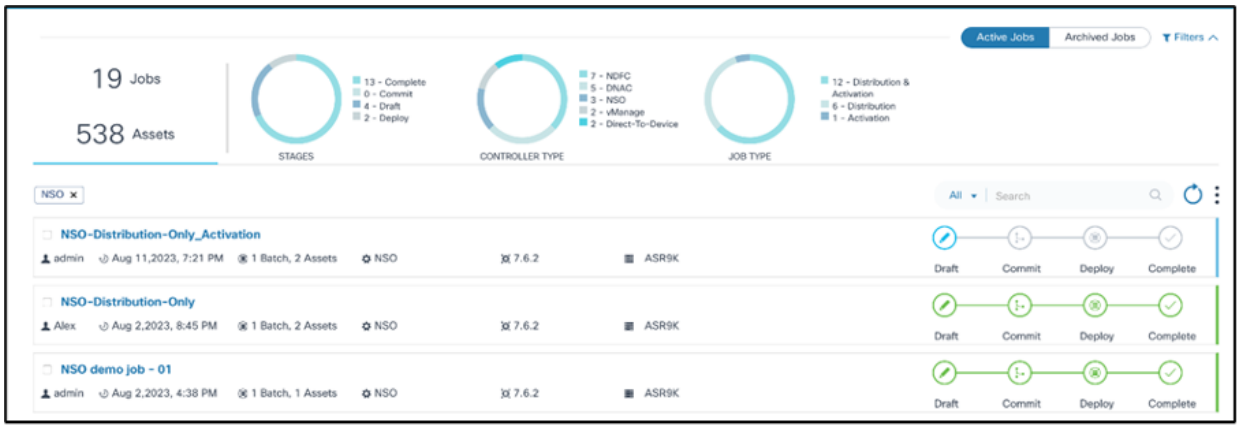


Editar ativos

2. Clique em Edit Assets.
3. Faça as alterações necessárias selecionando ou compensando ativos em Adicionar Ativos ou Fazer Upload de Ativos ou modificando a programação do lote fazendo alterações na data ou na Hora Inicial.
4. Clique em Atualizar lote.

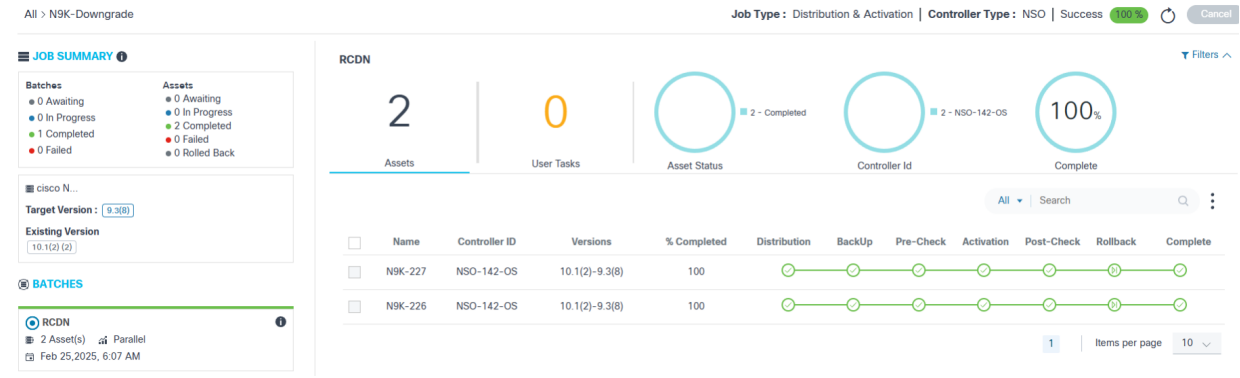
Atualizar Execução de Trabalho e Monitoramento de Andamento

1. Faça login no BPA com credenciais que tenham acesso a Jobs de Atualização.
2. Selecione OS Upgrade > Upgrade Jobs. A página Atualizar Job é exibida.

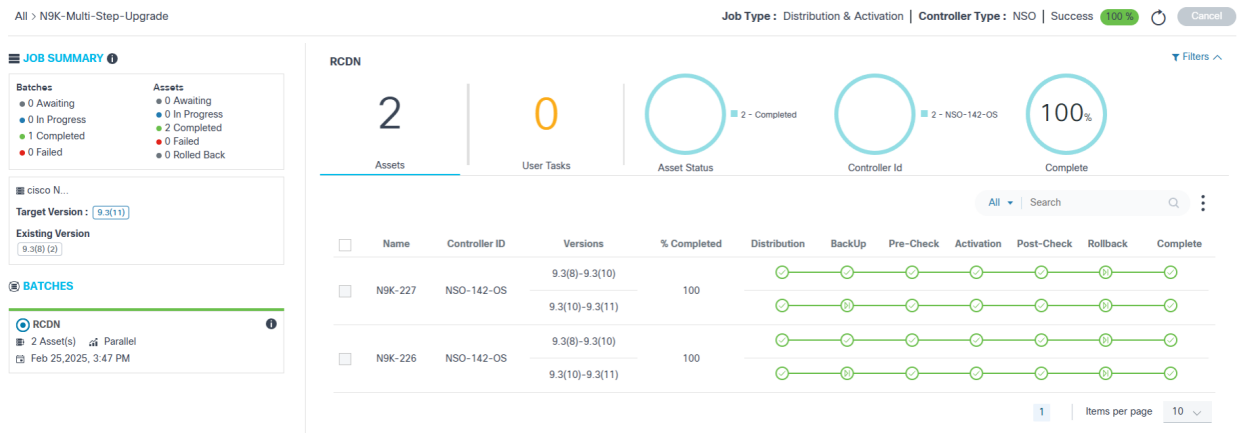


Trabalho de Atualização

3. Use o filtro Pesquisar em combinação com os filtros de gráfico disponíveis para filtrar rapidamente o trabalho.
4. Clique no trabalho desejado. A página Resumo da tarefa é exibida.

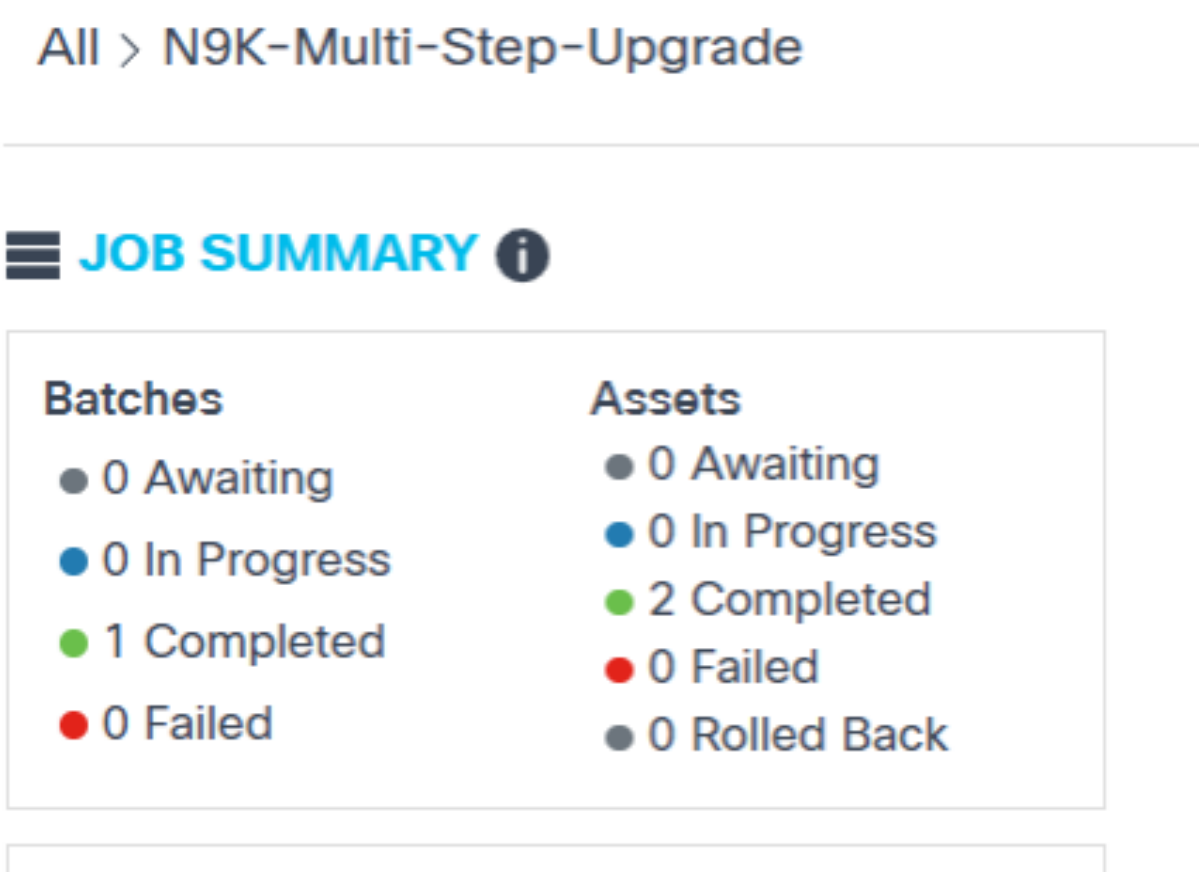


Atualização de etapa única



Atualização em várias etapas

O painel esquerdo fornece as seguintes informações:



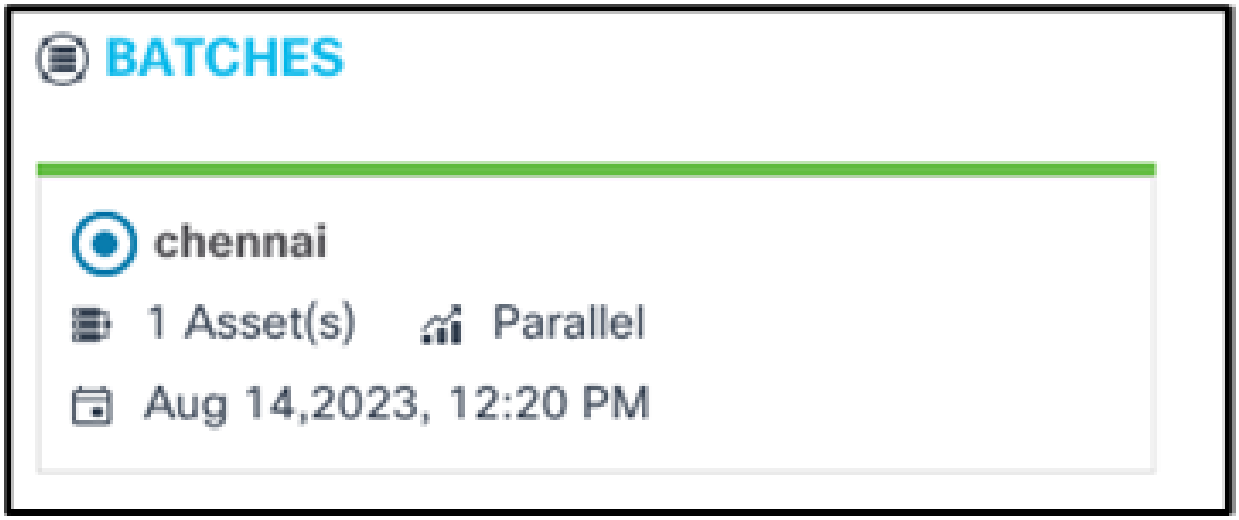
Resumo do Trabalho

- Um rápido resumo de lotes e respectivos ativos

Detalhes da política de conformidade (se a política tiver um modelo)

Detalhes da política de conformidade (se a política tiver vários modelos)

- O modelo do dispositivo afetado pelo trabalho, a versão do software de destino e a versão da versão existente
- Uma lista de lotes que fazem parte deste trabalho



Detalhes do lote

- Detalhes do lote:
  - A borda superior cinza indica que o lote está aguardando a programação
  - A borda superior azul indica que a implantação do lote está em andamento
  - A borda superior verde indica que a implantação do lote foi concluída

As informações a seguir são exibidas na parte superior da página Resumo da tarefa:

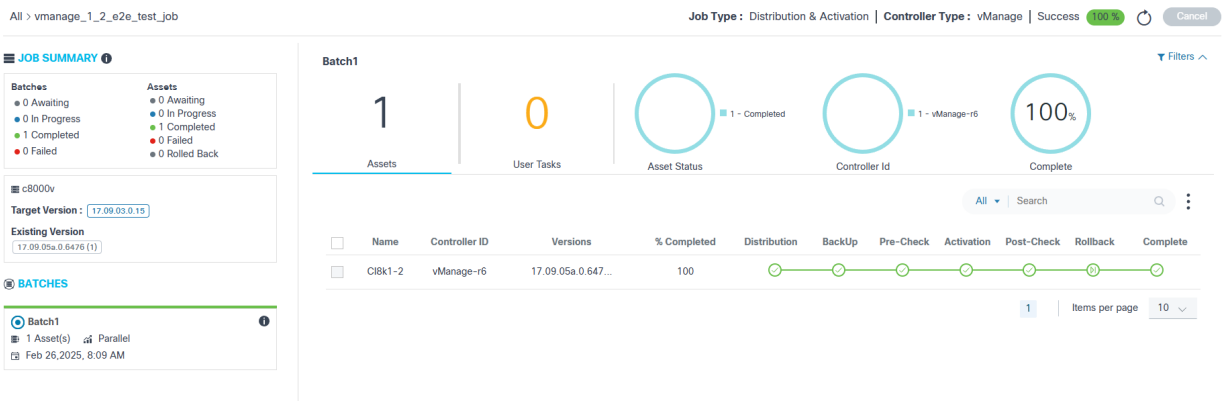
Resumo do Início do Trabalho

- A navegação de trilha do trabalho atual (por exemplo, Todos > manage_1_2_e2e). A opção All alterna para o painel Jobs
- O tipo de trabalho
- O tipo da controladora
- Status do trabalho com porcentagem de conclusão:
    - Sucesso: Trabalho de atualização bem-sucedido
    - Falha: Falha no trabalho de atualização por algum motivo
    - Em andamento: Trabalho de atualização em andamento

Note: O status do trabalho será movido para em andamento mesmo que o agendamento de um lote seja atingido

---

- Aguardando: O trabalho foi confirmado, mas está aguardando que um ou mais agendamentos de lote sejam alcançados



Resumo do Trabalho

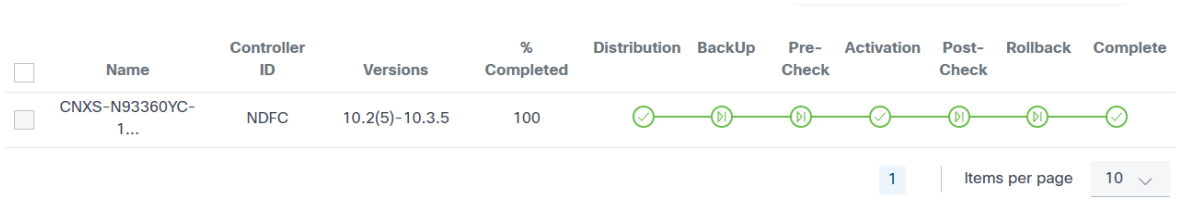
As seguintes opções estão disponíveis na página Resumo da tarefa:

- O ícone Atualizar permite que os usuários recuperem atualizações sob demanda
- Cancelar é usado para cancelar os trabalhos nos estágios Rascunho e Confirmar, a menos que o agendamento de qualquer um dos lotes seja atingido
- Ativar cria um novo trabalho de ativação no estado Rascunho com os mesmos lotes e ativos que faziam parte do trabalho concluído anteriormente
    - Ativar só estará disponível se o tipo de trabalho for Distribuição e for concluído com êxito
    - Se o trabalho de ativação já tiver sido criado e Ativar for clicado, uma mensagem será exibida com o status do trabalho criado anteriormente e oferecerá uma opção para redirecionar o trabalho já criado; na tarefa recém-criada, os usuários têm a opção de editar ou excluir os lotes ou ativos, mas o tipo de tarefa, o tipo de controlador e a política de conformidade não são editáveis.
- Uma lista paginada de ativos é exibida abaixo da seção de análise

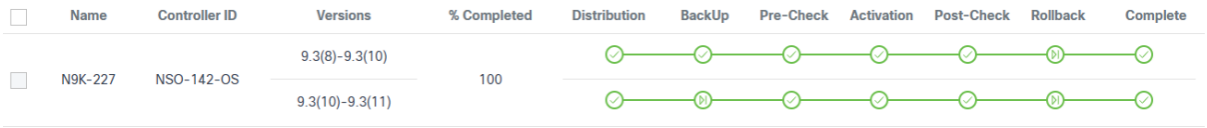
- O campo Pesquisar permite pesquisas gerais e específicas de campo para colunas como:
    - Nome de dispositivo
    - ID do controlador
    - Serial Number

Download do relatório em lote

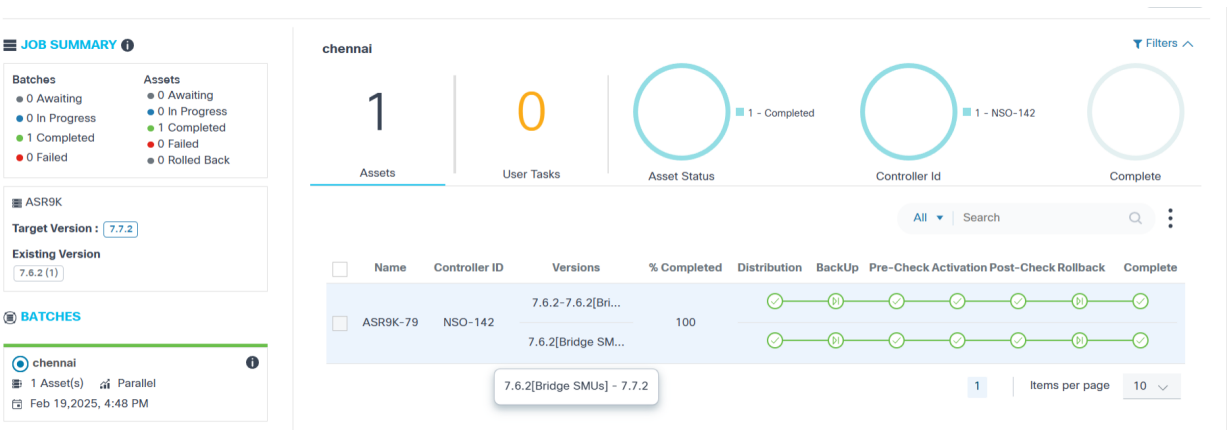
- A opção de fazer download do relatório em nível de lote selecionando o ícone Mais Opções > Download; o relatório consiste nos detalhes em nível de lote com detalhes do dispositivo



Classificar - Atualização em Etapa Única



Classificação - Atualização em Várias Etapas

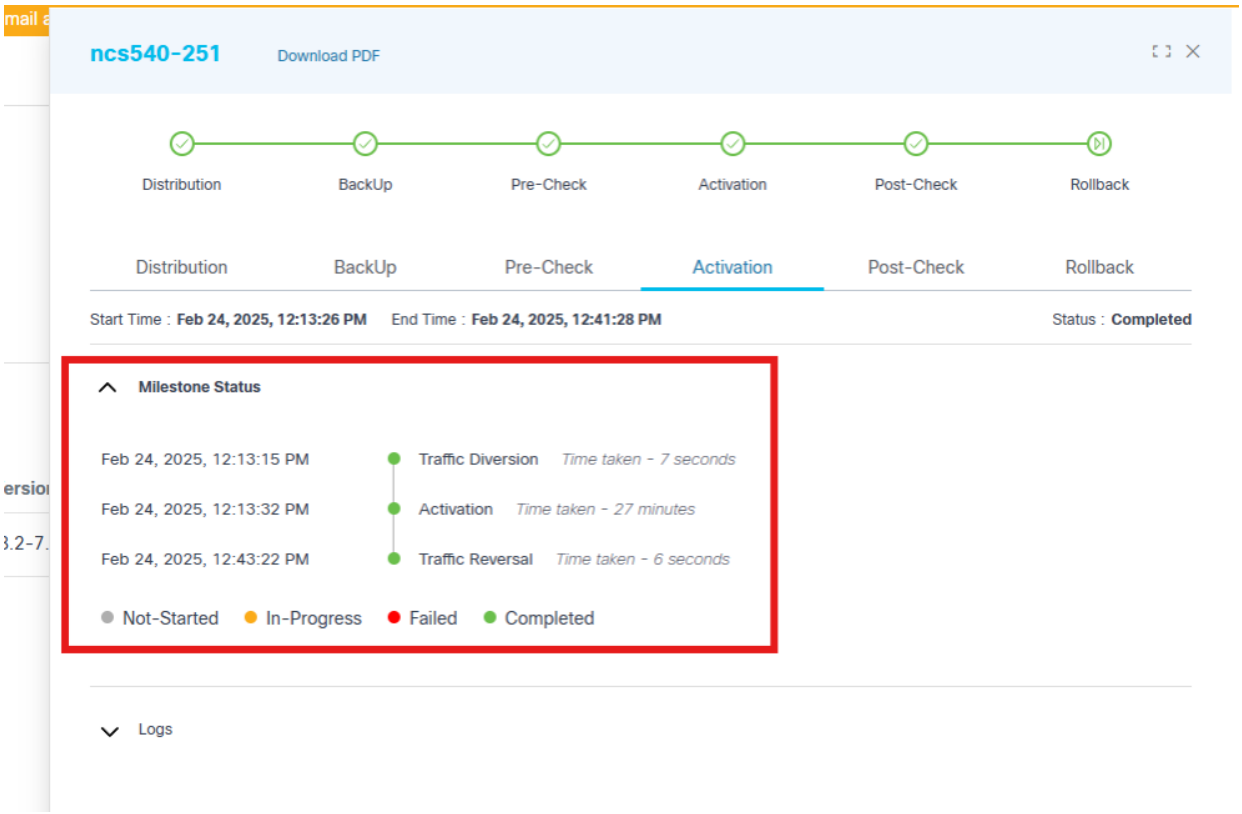


Classificar - Atualização do SMU da Bridge

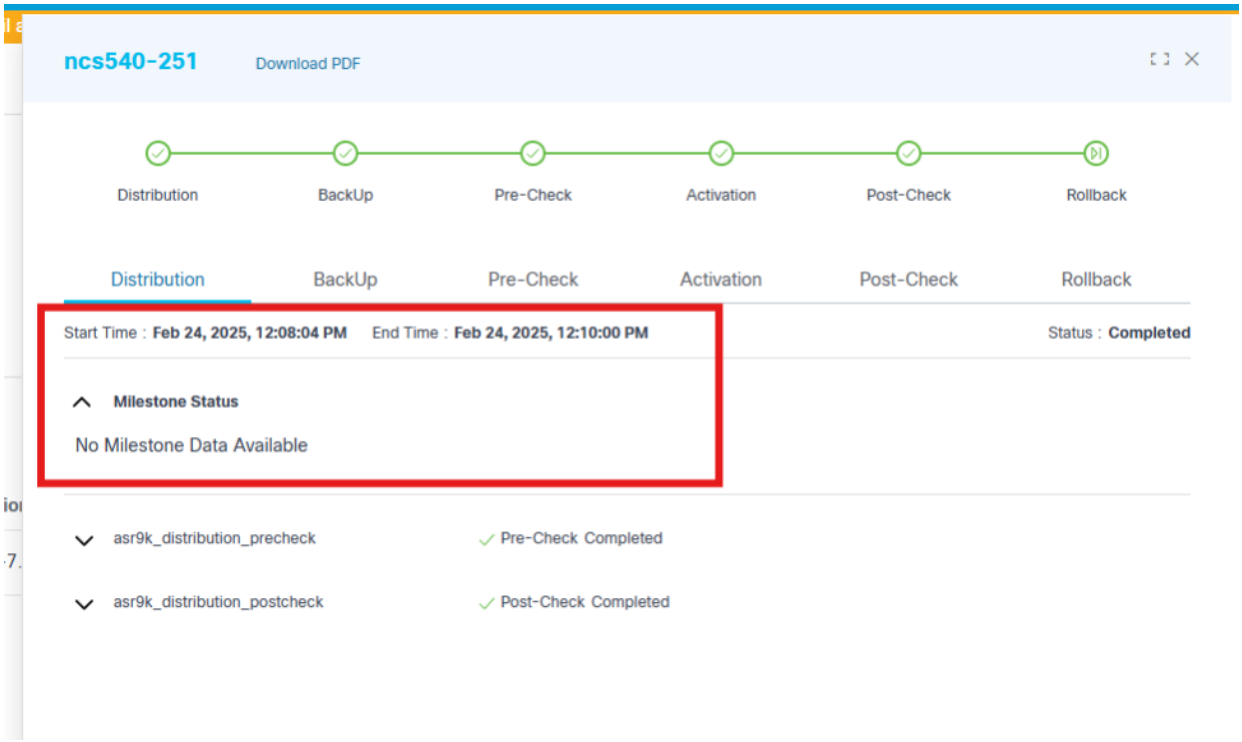
- A classificação pode ser feita clicando nos nomes das colunas
- Os seguintes marcos de atualização são exibidos para cada dispositivo junto com Nome, ID do controlador, Versões e % Concluído:
    - Distribuição
    - Fazer backup
    - Pré-verificação
    - Desvio de tráfego
    - Ativação
    - Pós-verificação
    - Traffic-Reversal
    - Reverter
    - Completo

Note: % concluído exibe o progresso com base no número de etapas concluídas para um dispositivo. Todos os percentuais de conclusão em nível de dispositivo dentro de um lote são agregados para calcular o percentual de conclusão do lote. Por sua vez, todas as porcentagens de conclusão de lote são agregadas para calcular a porcentagem de conclusão em nível de trabalho.

As etapas secundárias também conhecidas como etapas personalizadas são as etapas intermediárias significativas executadas e visualizadas sob a etapa padrão quando adicionadas. Para obter mais informações sobre a adição de marcos personalizados, consulte o Guia do desenvolvedor BPA.



Exibição de submarco (se submarcos forem adicionados sob o nome padrão do marco)

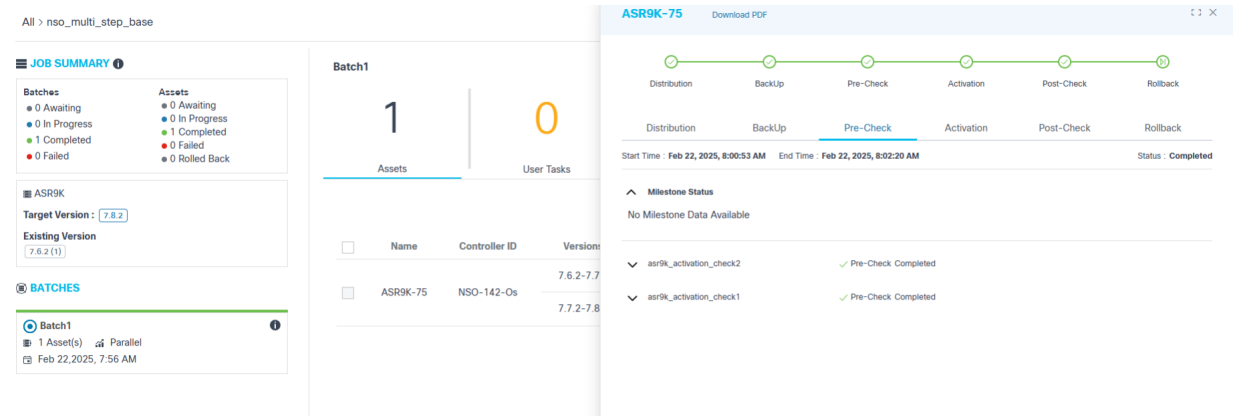


Exibição de submarco (se os submarcos não forem adicionados sob o nome padrão do marco)

Note: As etapas variam de acordo com o tipo de tarefa selecionado. A etapa do projeto TrafficReversal não está disponível para trabalhos de distribuição.

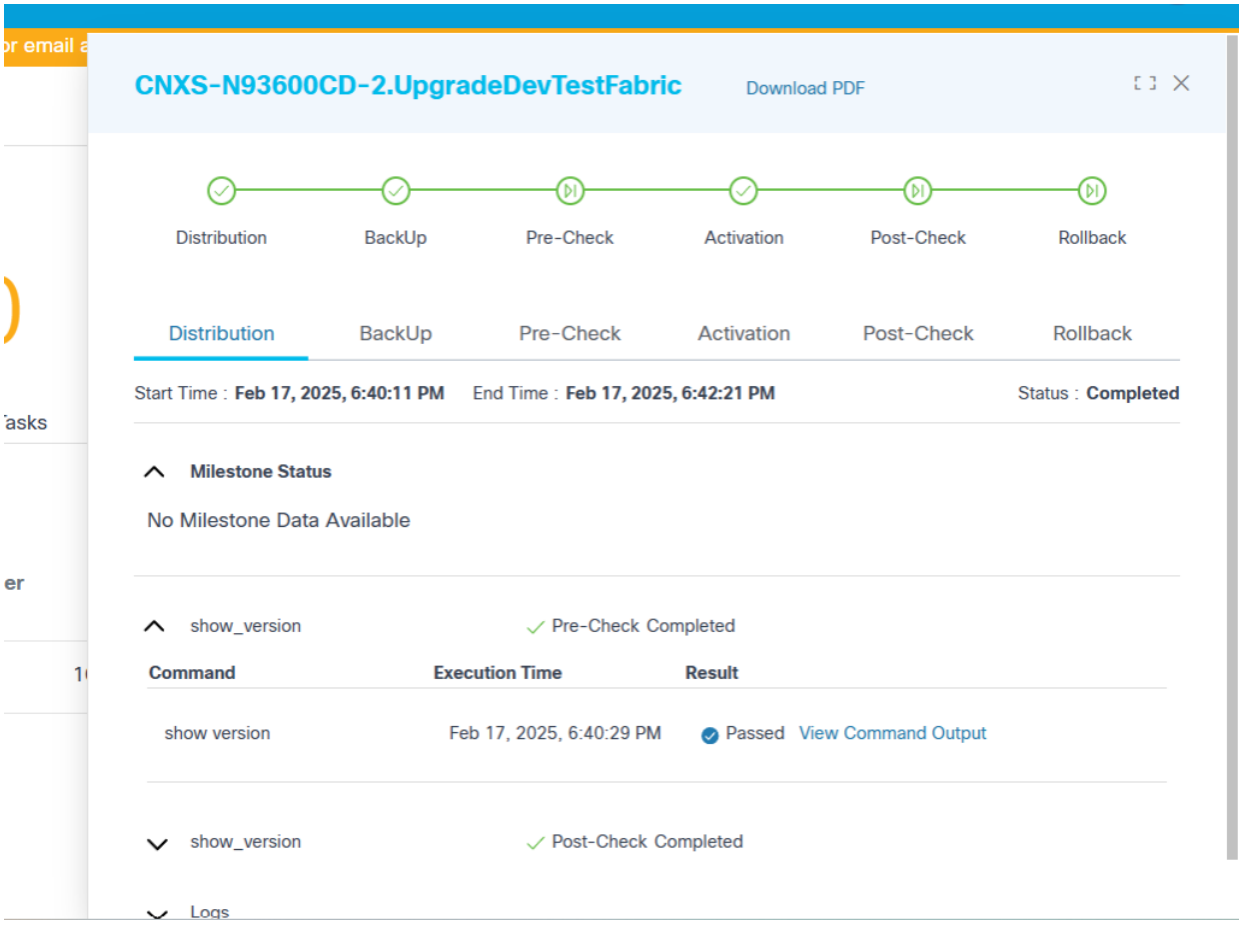
O desvio de tráfego e a reversão de tráfego são movidos para a etapa de ativação.

- Uma legenda de cor de marco que consiste no seguinte:
  - Verificação de Cinza: Pendente
  - Verificação Azul: Em andamento
  - Sinalizador Verde: Ignorado
  - Verificação verde: Concluído
  - Cheque Laranja: Tarefa do usuário
  - Cheque vermelho: Falha



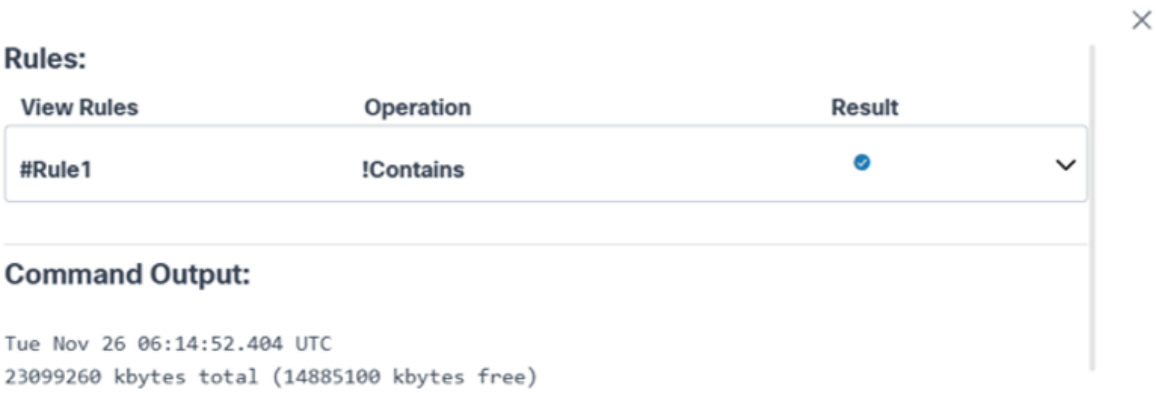
Visualização de etapas pré e pós-verificação

Para marcos com execução pré ou pós-verificação, os usuários podem exibir a saída completa do comando junto com as regras de validação e seus status para todos os comandos configurados no respectivo modelo de processo.



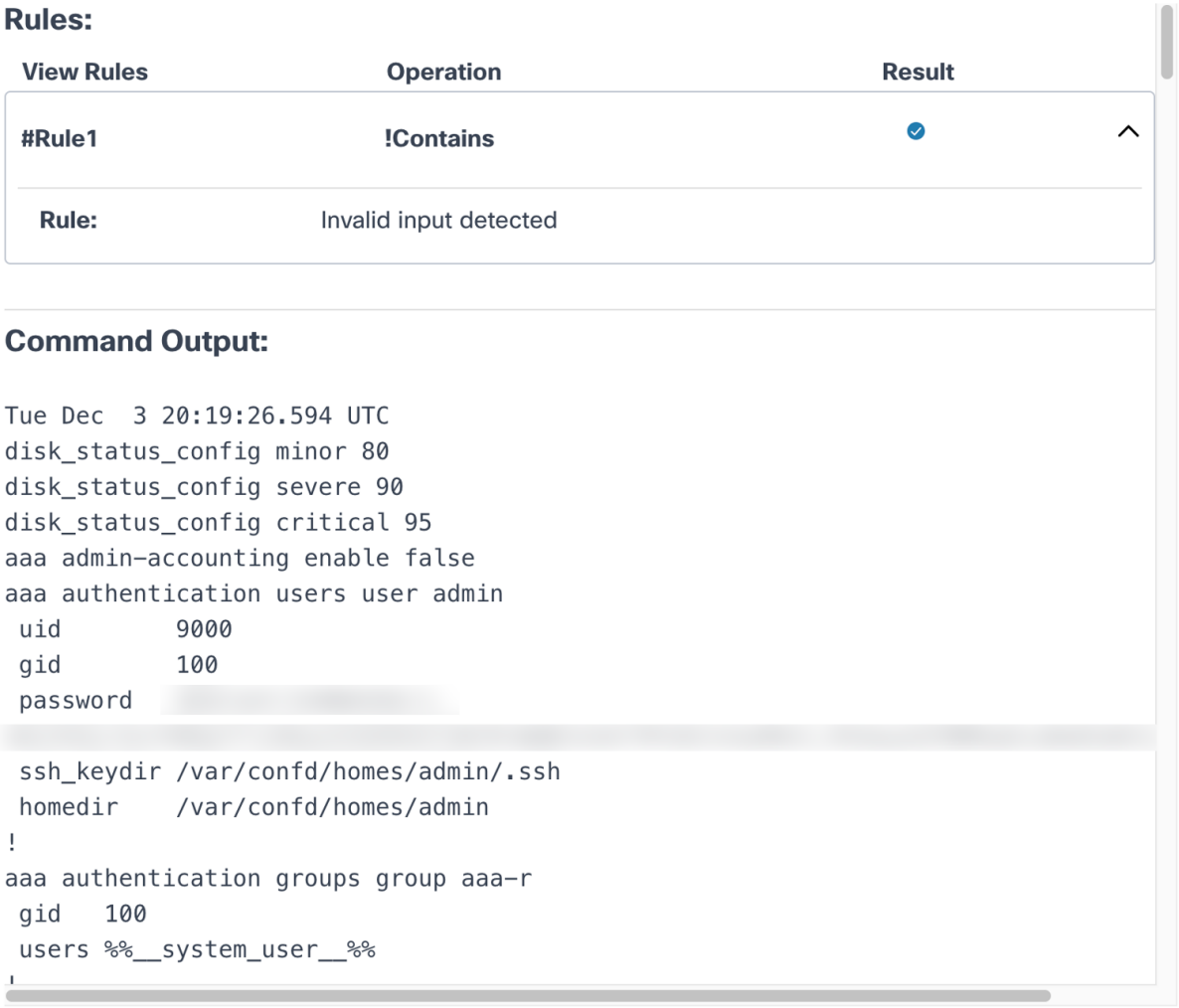
Exibição de Marco de Distribuição com Saída de Comando de Pré-Verificação

1. Para exibir a saída do comando e as regras associadas aos comandos de pré e pós-verificação, clique no link Exibir Saída do Comando.

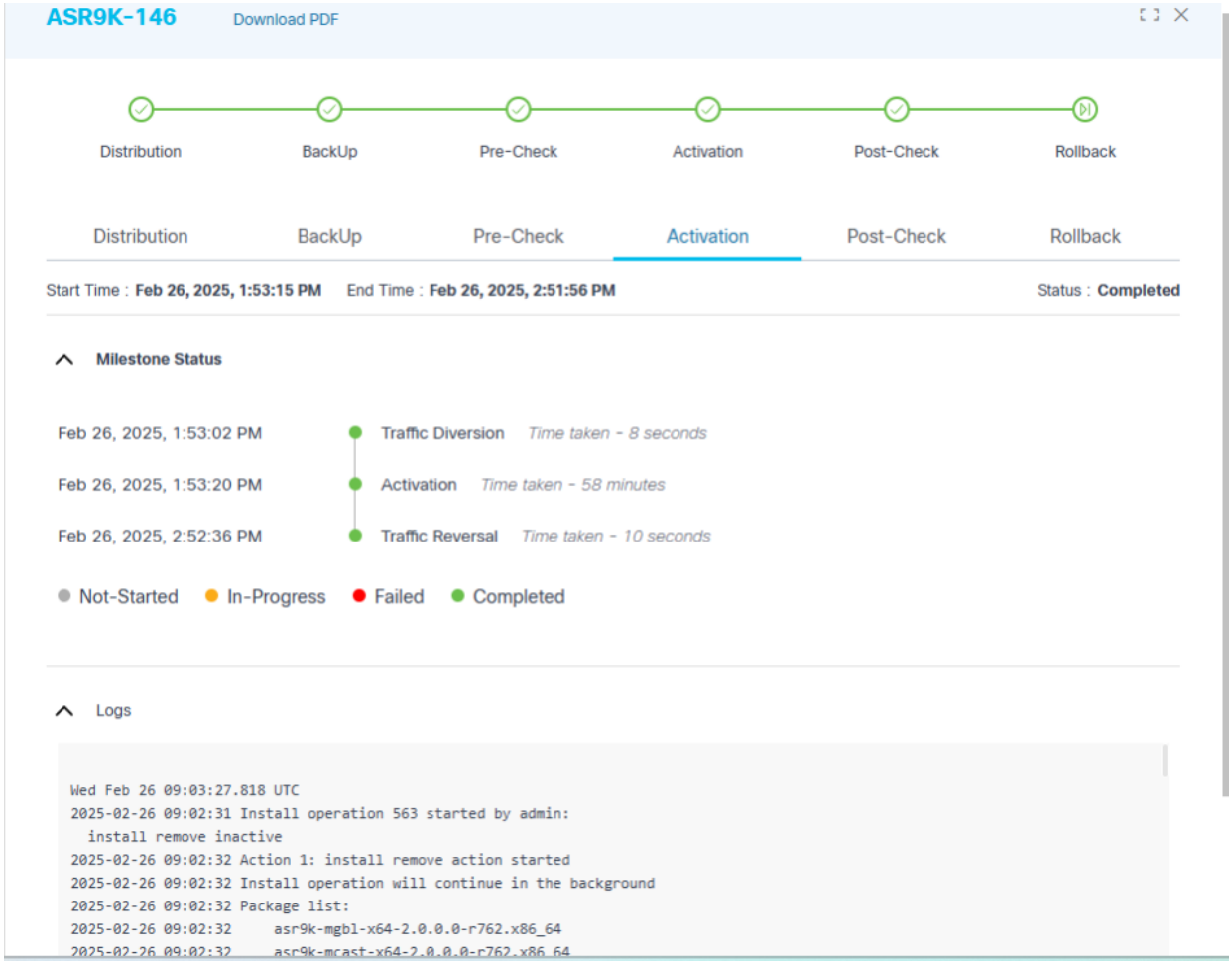


Saída do comando de pré e pós-verificação e regras associadas

2. Selecione o ícone Expandir para exibir todos os detalhes de cada regra.



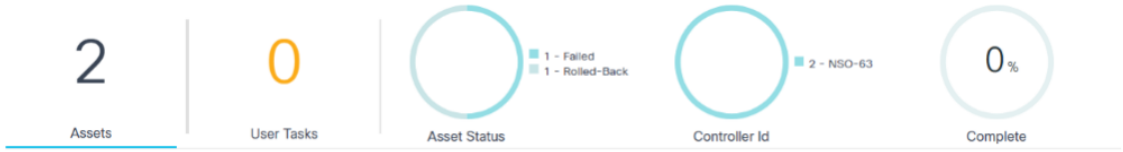
Saída do comando de pré e pós-verificação com regras de validação



Exibição do marco de ativação com registros em tempo real

A figura acima fornece detalhes do marco de ativação, que inclui logs ao vivo para ajudar a monitorar o progresso da ativação de software de um dispositivo específico.

Quando uma etapa do projeto for iniciada ou concluída, clicar nela exibirá mais informações.



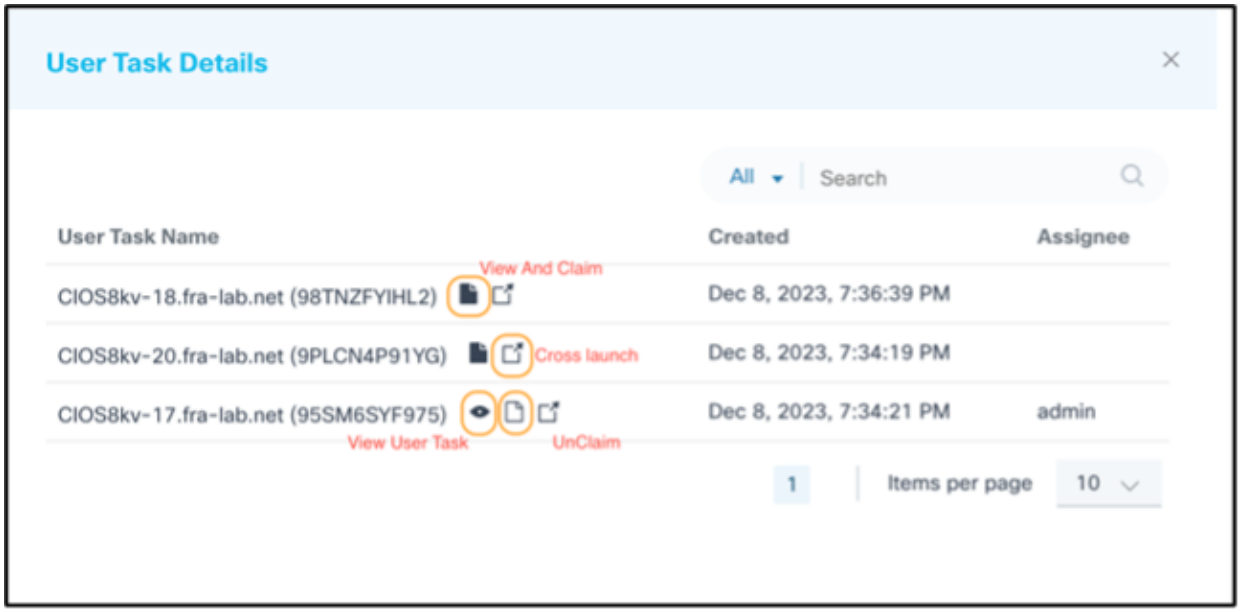
Seção de análise

Uma seção de análise, exibida na parte superior da página Resumo da tarefa, exibe as seguintes informações relacionadas à tarefa selecionada no momento:

- O nome do lote (por exemplo, Ásia)
- Filtros ^ recolhe e expande a seção de análise
- Os seguintes detalhes do lote são mostrados na ordem:
    - Ativos: Número total de ativos

- Tarefas do usuário: Número total de tarefas do usuário aguardando a entrada do usuário de Operações ou do Administrador
- Status do ativo: Filtra os dispositivos de lote de acordo com seu status. O filtro Rollback foi adicionado para ajudar a identificar os dispositivos que foram revertidos com êxito.
- ID do controlador: Filtra os dispositivos de lote que pertencem à ID de controlador selecionada
- Completo: Percentual de conclusão de lote geral

Para agir sobre qualquer tarefa de usuário, clique na contagem Tarefas de Usuário. A janela Detalhes da tarefa do usuário é aberta com o seguinte:



Detalhes da Tarefa do Usuário

- Uma lista de tarefas do usuário que correspondem aos respectivos dispositivos que exigem atenção
- Os seguintes ícones para as opções de tarefas do usuário:

  - Exibir e reivindicar: Exibir os detalhes da tarefa do usuário
  - Lançamento Cruzado: Exibir as tarefas de fluxo de trabalho do BPA na interface de usuário clássica
  - Não reivindicar: Remover a atribuição de tarefa do usuário
  - Tarefa Exibir Usuário: Exibir os detalhes da tarefa do usuário

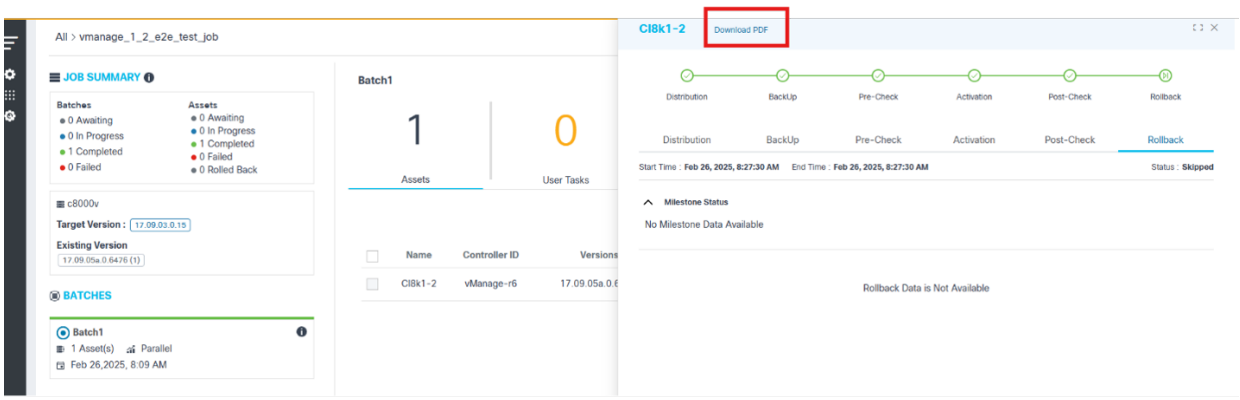
Tarefa do usuário

Opção Exibir da Tarefa do Usuário

- As seguintes opções são exibidas com base no contexto da tarefa:
    - Repetir: Reexecuta a tarefa
    - Repetir Tudo: Reexecuta todas as verificações prévias e posteriores
    - Continuar: Continua para a próxima tarefa
    - Reversão: Retorna à versão anterior; Essa opção está disponível quando a ativação ou pós-verificação falha ou diferenças inválidas são encontradas entre as pré e pós-verificações
    - Cancel: Cancela o trabalho atual
    - Fechar: Fecha a janela User Task.
- Aja nas tarefas do usuário, se houver, e selecione o ícone Atualizar para atualizar a contagem total de tarefas do usuário
- Porcentagem total de conclusão de lote
- Gráfico clicável para filtrar por IDs de controlador

Note: O número antes do ID do controlador indica o número total de dispositivos gerenciados pelo respectivo controlador.

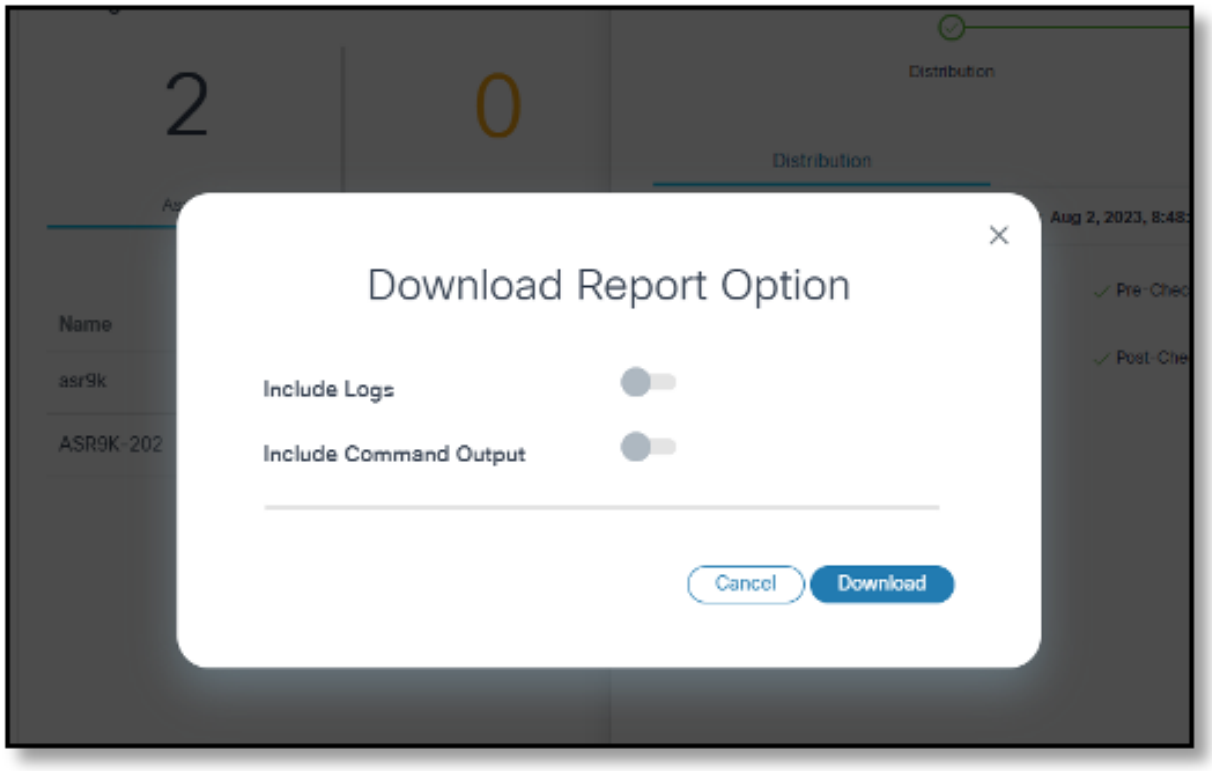
Download do relatório de atualização de software



Faça o download do PDF

O nome do dispositivo é exibido seguido por Download PDF no cabeçalho da exibição detalhada. Os usuários podem gerar e baixar o relatório de atualização em formato PDF para o dispositivo selecionado no momento. Para fazer o download do relatório de atualização em formato PDF:

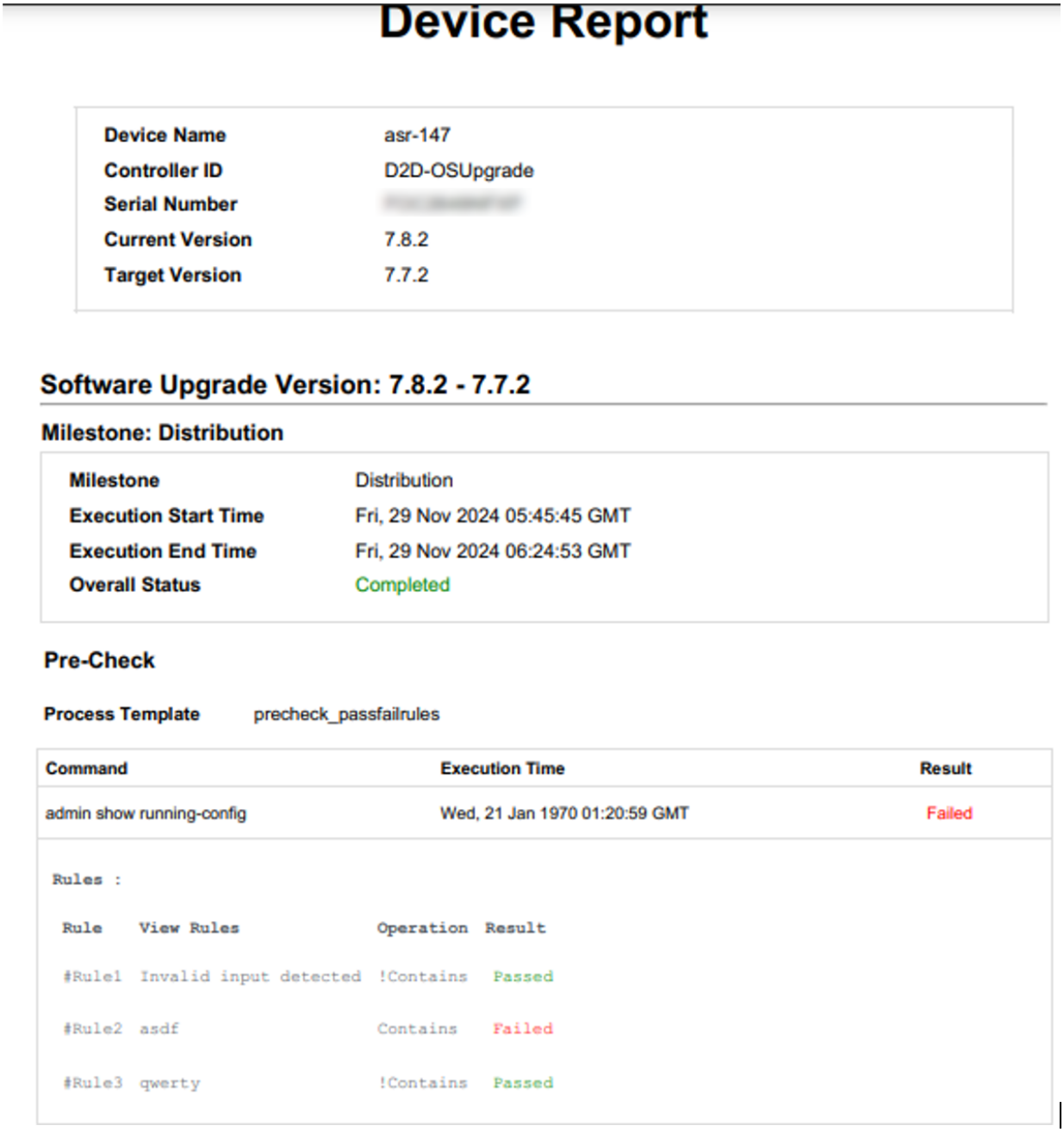
1. Clique em Download de PDF. A janela Download Report Option é aberta.



Opção de Download de Relatório

2. Ative as opções Include Logs e Include Command Outputs.
    - Incluir logs: Inclui logs dinâmicos, se houver, no relatório
    - Incluir saída do comando: Inclui no relatório os resultados dos controlos prévios e posteriores; Nesse caso, as regras são seguidas pela saída do comando
3. Clique em Download. A geração do relatório é iniciada.

Note: A habilitação das alternâncias Incluir Logs e Incluir Saída de Comando aumenta o tempo de processamento para a geração de relatórios e o tamanho dos relatórios. Use essas opções somente quando um relatório detalhado for necessário. As regras de comando são incluídas no relatório independentemente da alternância de saída de comando ser Ativado ou Desativado.



Device Report

Device Name	asr-147
Controller ID	D2D-OSUpgrade
Serial Number	
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

Relatório do dispositivo

Trabalhos de arquivamento

1. Faça login no BPA com credenciais que tenham acesso suficiente aos Jobs de Atualização.
2. Selecione OS Upgrade > Upgrade Jobs. A página Atualizar Job é exibida.
3. Use o filtro Pesquisar em combinação com os filtros de gráfico disponíveis para filtrar o(s) trabalho(s).
4. Selecione um ou mais trabalhos.

Trabalho de Arquivo Morto

5. Selecione o ícone Mais Opções > Arquivo.

Note: Somente trabalhos concluídos podem ser arquivados.

Exclusão de Trabalhos

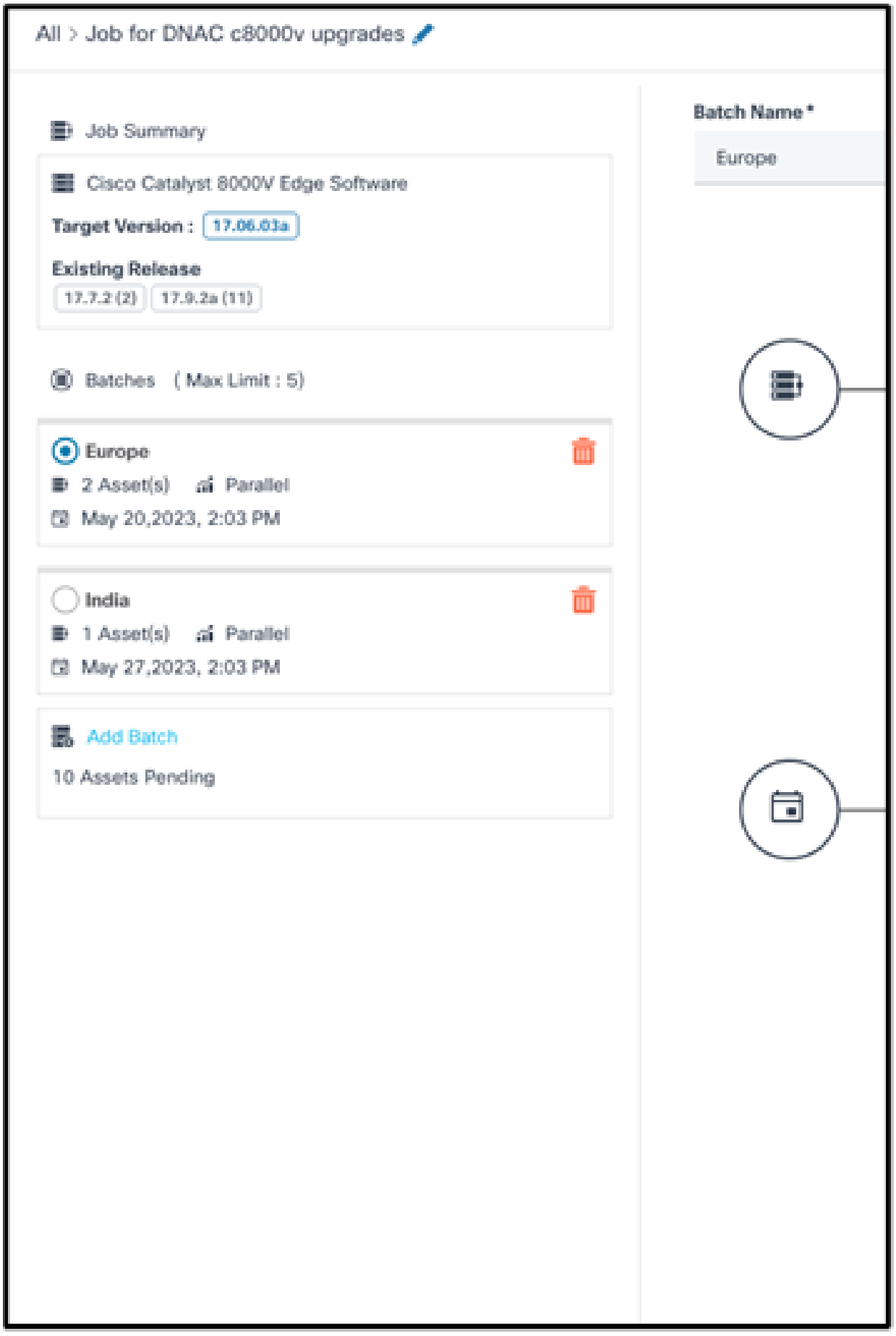
1. Faça login no BPA com credenciais que tenham acesso suficiente aos Jobs de Atualização.
2. Selecione OS Upgrade > Upgrade Jobs. A página Atualizar Job é exibida.
3. Use o filtro Pesquisar em combinação com os filtros de gráfico disponíveis para filtrar o(s) trabalho(s).
4. Selecione um ou mais trabalhos.

Excluir Trabalho

5. Selecione o ícone Mais Opções > Excluir Job.

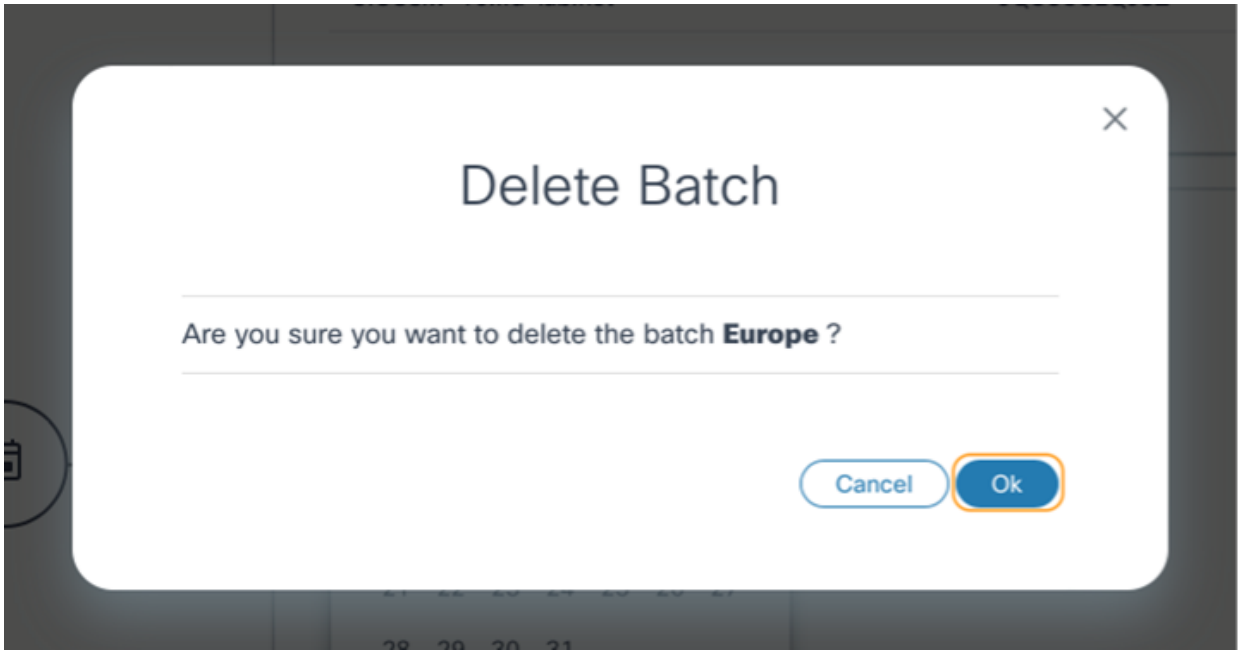
Note: Os trabalhos só podem ser excluídos quando estiverem no estágio Rascunho.

Exclusão de Lotes em Jobs



Deletar um Lote em um Job

1. Selecione o ícone Excluir do lote desejado no painel lateral. Uma janela de confirmação será aberta.



Confirmação de Exclusão de Lote

2. Click OK.

Os ativos associados ao lote excluído retornam ao grupo de ativos pendentes e estão disponíveis para seleção em lotes novos ou existentes.

Cancelando Trabalhos

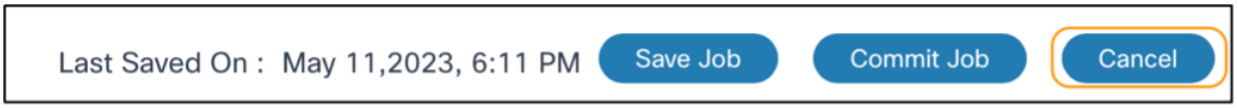
1. Faça login no BPA com credenciais que tenham acesso suficiente aos Jobs de Atualização.
2. Selecione OS Upgrade > Upgrade Jobs. A página Atualizar Job é exibida.

Trabalho de Atualização

3. Use o filtro Pesquisar em combinação com os filtros de gráfico disponíveis para filtrar o

trabalho desejado.

4. Clique no trabalho desejado. A página Resumo da tarefa é exibida.

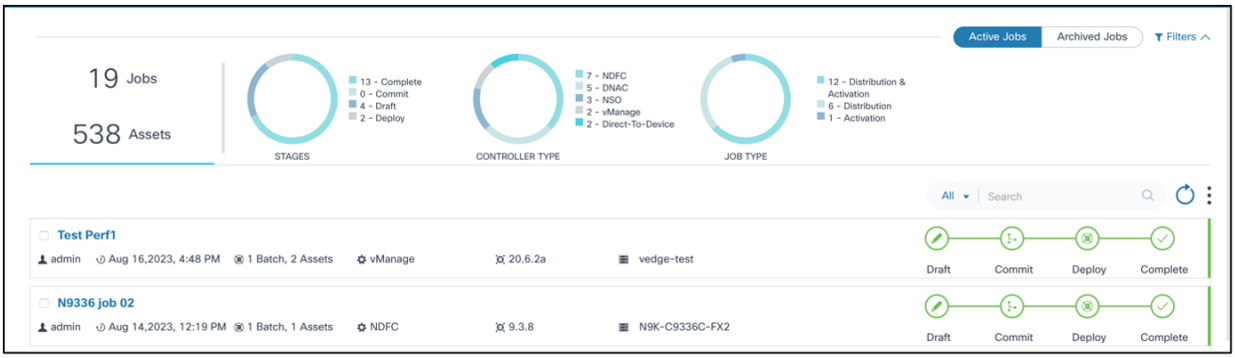


Cancel

5. Clique em Cancel.

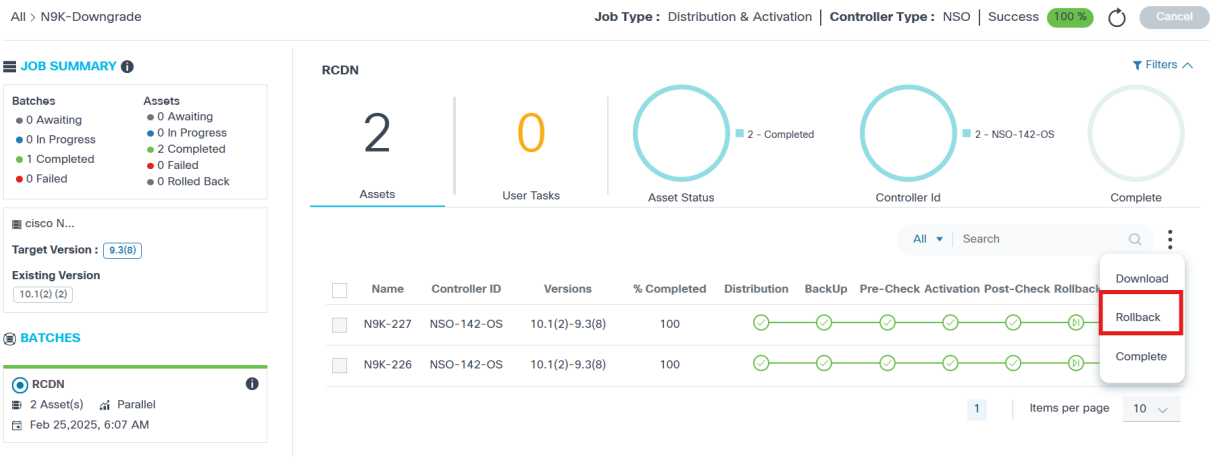
Revertendo Ordens de Produção ou Atualizações Concluídas

1. Faça login no BPA com credenciais que tenham acesso suficiente aos Jobs de Atualização.
2. Selecione OS Upgrade > Upgrade Jobs. A página Atualizar Job é exibida.



Trabalho de Atualização

3. Use o filtro Pesquisar em combinação com os filtros de gráfico disponíveis para filtrar o trabalho desejado.
4. Clique no trabalho desejado. A página Resumo da tarefa é exibida. Selecione o lote necessário no painel do lado esquerdo e selecione os dispositivos desejados que precisam de confirmação completa/reversão no painel do lado direito
5. Selecione o ícone Mais Opções e clique nas ações de menu Reverter ou Concluir de acordo com o requisito.



Reverter

Note: Os dispositivos só podem ser selecionados quando os seguintes pré-requisitos forem atendidos:

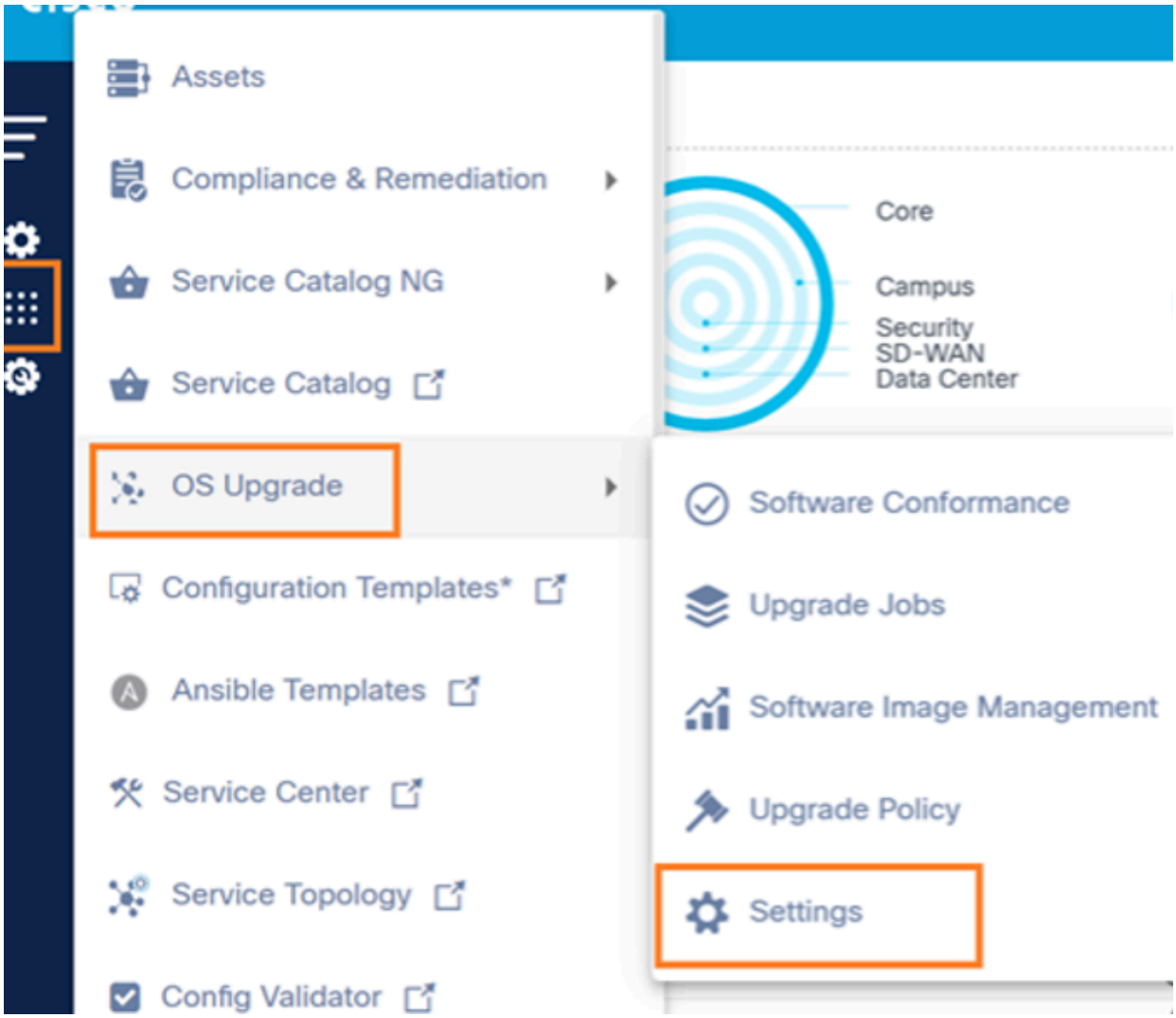
- As configurações devem ser configuradas para ativar a opção de reversão de um trabalho atualizado concluído; consulte Configurações para obter mais informações.
- Se nenhuma ação for executada dentro do tempo, os dispositivos automaticamente passam para o estado Completo
- Os dispositivos estarão disponíveis para a ação de reversão sob demanda se a reversão tiver sido concluída anteriormente ou se o marco de reversão estiver no estado Aguardando

Configurações

As configurações de Atualização de SO fornecem um espaço reservado para armazenar configurações comuns usadas em outros componentes do aplicativo de Atualização de SO.

Para acessar a página Configurações:

1. Faça login no BPA com credenciais que tenham acesso de gerenciamento às Configurações.



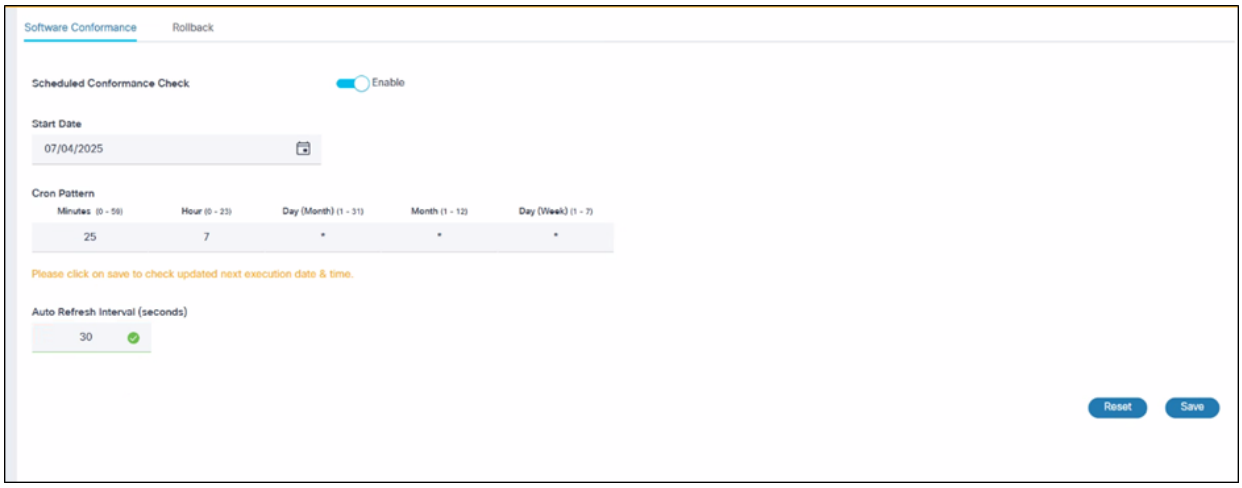
Configurações

2. Selecione OS Upgrade > Settings. A página Configurações é aberta.

A página Configurações tem as duas guias a seguir:

- Conformidade de software: As configurações que permitem programações de execução de conformidade automática podem ser atualizadas nesta guia
- Reversão: As configurações que permitem a reversão de uma atualização completa do dispositivo podem ser atualizadas nesta guia

Conformidade de software



Guia Conformidade de software

A guia Conformidade de software fornece o seguinte:

- Verificação de conformidade programada: Habilitar ou desabilitar a agenda
- Data de início: Selecione DD/MM/AAAA

Note: A Data de Início deve ser uma data futura.

- Padrão Cron: Forneça os seguintes detalhes:
  - Minutos (0-59)
  - Hora (0-23)
  - Dia (Mês) (1-31)
  - Mês (1-12)
  - Dia (Semana) (1-7)
- Adicionar intervalo de atualização automática: O valor padrão é 30 segundos
- Save: Salvar alterações

Reverter

Guia Reverter

A guia Rollback fornece o seguinte:

- Alternar verificação de usuário: Habilitar ou desabilitar verificação do usuário
    - Estado Habilitado: Os dispositivos no trabalho de atualização aguardam a confirmação do usuário para reverter ou concluir a atualização até que o tempo limite configurado em Tempo Limite de Configuração (h) seja atingido; quando alcançados, os dispositivos automaticamente entram no estado Concluído
    - Estado Desabilitado: Dispositivos no trabalho de atualização concluem automaticamente a atualização sem aguardar a confirmação do usuário
- Tempo limite de confirmação: Adicionar um tempo limite de espera em horas
- Save: Salvar alterações

Configuração de Implantação

- Os agendamentos padrão para a verificação de política de conformidade e os metadados SWIM são configurados diariamente às 7h25, horário local.
- Para alterar as agendas padrão da sincronização de metadados da imagem SWIM, navegue para o diretório instalado BPA "<BPA install diretory>/conf/@cisco-bpa-platform/mw-osupgrade-nxtgen/config.json" e atualize a propriedade schedule.swimSchedule com a expressão Cron. As programações podem ser atualizadas após a implantação. Consulte Conformidade de Software para obter mais informações.
- Para aumentar ou diminuir o número máximo de dispositivos processados em modo paralelo para diferentes tipos de controladores:

1. Atualize os seguintes arquivos:
    - Arquivo do Cisco Catalyst Center: "<DIRETÓRIO_INSTALAÇÃO_BPA>/conf/@cisco-bpa-platform/mw-dnac-agent/config.json"
    - Arquivo vManage: "<DIRETÓRIO_INSTALAÇÃO_BPA>/conf/@cisco-bpa-platform/mw-vmanage-agent/config.json"
    - Arquivo NDFC: "<DIRETÓRIO_INSTALAÇÃO_BPA>/conf/@cisco-bpa-platform/mw-ndfc-agent/config.json"
    - Arquivo FMC: "<DIRETÓRIO_INSTALAÇÃO_BPA>/conf/@cisco-bpa-platform/mw-fmc-agent/config.json"
2. Navegue para Update throttling > capabilities > image-ativation, image-distribute para aumentar o limite de ativação ou distribuição simultânea.

Note: Consulte as controladoras suportadas e plataformas de dispositivos antes de atualizar esses limites.

Controle de acesso

Controle de Acesso Baseado em Função

O BPA suporta RBAC (controle de acesso baseado em funções). No modelo RBAC, uma função encapsula um conjunto de permissões (ou seja, ações) que um usuário pode executar. Para controle de acesso, os administradores podem atribuir funções predefinidas ou funções recém-criadas com permissões para grupos de usuários. Um usuário pode pertencer a um ou mais grupos de usuários e cada grupo de usuários pode ser atribuído a uma ou mais funções que concedem aos usuários desse grupo determinadas permissões de acesso.

A tabela abaixo descreve as funções de Atualização do SO OOB e as permissões associadas.

Serviço	Grupo	Intenção	Super administrador	Administrador de caso de uso	Usuário somente leitura (Caso de uso de atualização do SO Usuário somente leitura)	Operador
OSUpgradeService	ui_app	Mostrar ou ocultar o aplicativo Atualizar Trabalhos	Yes	Yes	Yes	Yes
OSUpgradeService	ui_app	Mostrar ou ocultar o aplicativo de Conformidade de Software	Yes	Yes	Yes	Yes
OSUpgradeService	ui_app	Mostrar ou ocultar o aplicativo SWIM	Yes	Yes	Yes	Yes
OSUpgradeService	ui_app	Mostrar ou ocultar o aplicativo de Políticas de Atualização de Software	Yes	Yes	Yes	Yes
OSUpgradeService	ui_app	Mostrar ou	Yes	Yes	Yes	Yes

Serviço	Grupo	Intenção	Super administrador	Administrador de caso de uso	Usuário somente leitura (Caso de uso de atualização do SO Usuário somente leitura)	Operador
		ocultar as configurações de Atualização de Software				
OSUpgradeService	Trabalhos de Atualização	Gerenciar trabalhos de atualização (por exemplo, criar, atualizar, excluir e confirmar)	Yes	Yes	No	Yes
OSUpgradeService	Trabalhos de Atualização	Cancelar trabalhos de atualização	Yes	Yes	No	Yes
OSUpgradeService	Trabalhos de Atualização	Arquivamento sob demanda dos trabalhos	Yes	Yes	No	Yes
OSUpgradeService	Trabalhos de Atualização	Aprovação manual	Yes	Yes	No	Yes
OSUpgradeService	Política de conformidade de software	Exibir políticas de conformidade de software e resultados de execução	Yes	Yes	Yes	Yes
OSUpgradeService	Política de conformidade de software	Criar, atualizar e excluir políticas de conformidade de software	Yes	Yes	No	No
OSUpgradeService	Política de conformidade de software	Execução sob demanda de políticas de conformidade de software	Yes	Yes	No	Yes

Serviço	Grupo	Intenção	Super administrador	Administrador de caso de uso	Usuário somente leitura (Caso de uso de atualização do SO Usuário somente leitura)	Operador
OSUpgradeService	Política de atualização	Exibir políticas de atualização de SO	Yes	Yes	Yes	Yes
OSUpgradeService	Política de atualização	Gerenciar políticas de atualização de SO	Yes	Yes	No	No
OSUpgradeService	Gerenciamento de imagens do Swim	Criar, atualizar e excluir imagens de software	Yes	Yes	No	Yes
OSUpgradeService	Gerenciamento de imagens do Swim	Exibir SWIM	Yes	Yes	Yes	Yes
OSUpgradeService	Gerenciamento de imagens do Swim	Sincronizar imagens de software	Yes	Yes	No	Yes
OSUpgradeService	Recomendações de software	Sincronizar metadados de recomendações de software	Yes	Yes	No	No
OSUpgradeService	Recomendações de software	Exibir recomendações ou insights	Yes	Yes	Yes	Yes
OSUpgradeService	Recomendações de software	Gerenciar a política de conformidade	Yes	Yes	No	No
OSUpgradeService	Configuração de conformidade de software	Exibir configurações de conformidade de software	Yes	Yes	Yes	Yes
OSUpgradeService	Configuração de conformidade de software	Gerenciar configurações de	Yes	Yes	No	No

Serviço	Grupo	Intenção	Super administrador	Administrador de caso de uso	Usuário somente leitura (Caso de uso de atualização do SO Usuário somente leitura)	Operador
		conformidade de software				

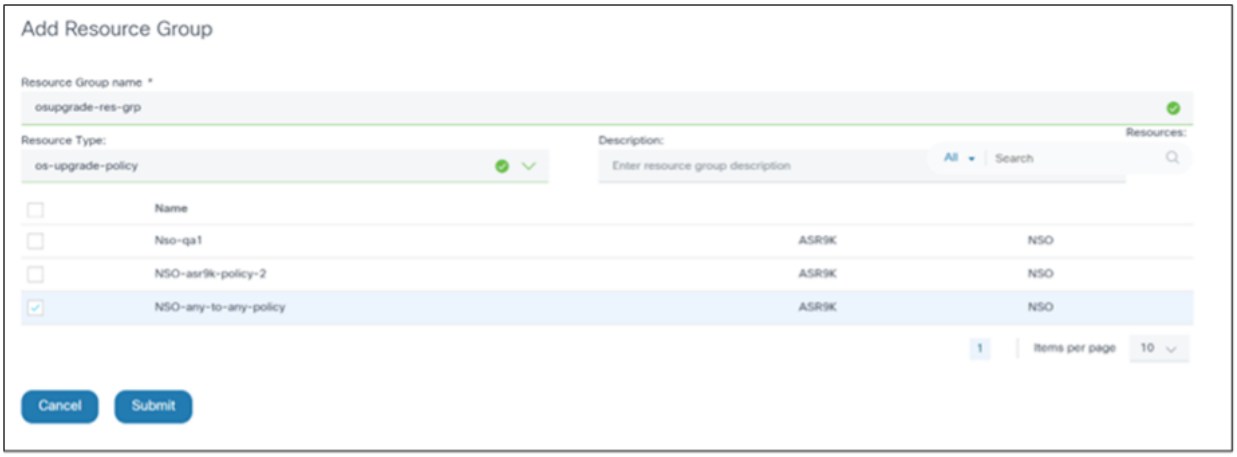
Note: Funções personalizadas e mapeamento de permissão podem ser feitos de acordo com os requisitos. Consulte Grupos de Recursos.

Grupos de recursos

Esse recurso fornece controle de acesso detalhado para recursos BPA, como políticas de upgrade, restringindo que usuários não autorizados atualizem as políticas definidas no aplicativo OS Upgrade. Os administradores podem restringir o acesso definindo um grupo de recursos com políticas acessíveis.

Para criar um grupo de recursos:

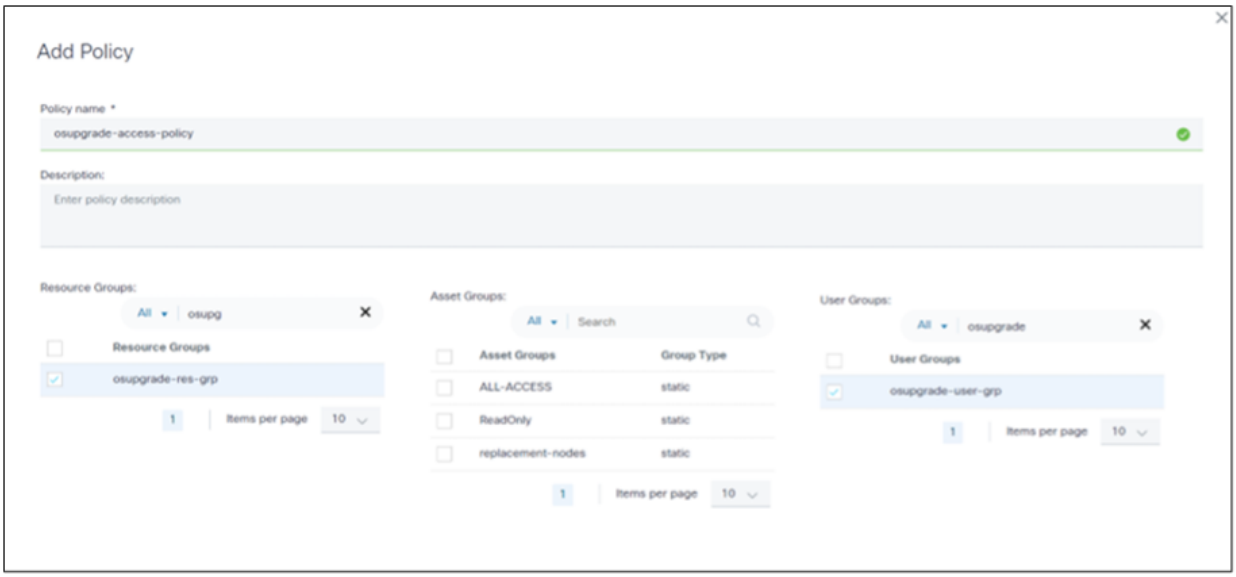
1. Navegue até Configurações > Grupos de recursos.



Adicionar grupo de recursos

2. Crie um grupo de recursos com políticas que usuários não administradores possam acessar.
3. Selecione os-upgrade-policy como o Tipo de recurso. Os recursos correspondentes são exibidos.
4. Selecione as políticas de atualização necessárias.
5. Clique em Submit. Os usuários não administradores que pertencem a este grupo de usuários agora têm acesso às políticas disponíveis somente no grupo de recursos selecionado.

Para associar o grupo de recursos a um grupo de usuários, crie uma política de acesso.

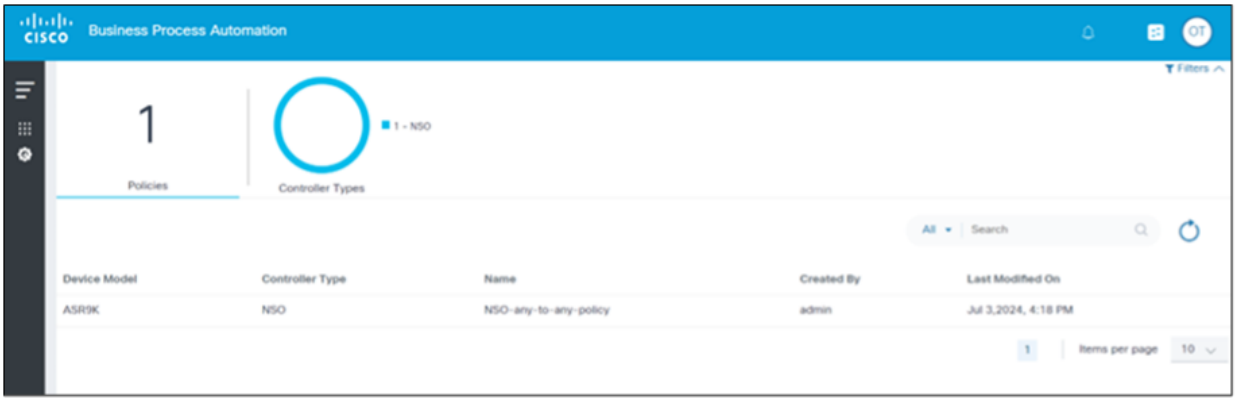


Adicionar política de acesso

Note: Depois que o grupo de recursos for criado, ele deverá ser associado a um grupo de usuários por meio de políticas de acesso. Consulte Controle de Acesso para obter mais informações sobre o seguinte:

- Usuários
- Funções
- Grupos de usuários
- Políticas de acesso
- Grupos de recursos
- Grupos de ativos

Abaixo está um exemplo de um usuário não-administrador que tem acesso a recursos restritos:



Usuário Não-Administrador Com Restrições De Recursos

Configuração de Sinalizador de Confiança Zero

Os recursos acessíveis por um usuário podem variar com base na configuração de flag zero-trust. O sinalizador zero-trust pode ser definido como verdadeiro ou falso. A tabela a seguir resume as possibilidades de acesso a recursos com base na configuração de flag zero-trust.

Usuário	Grupo de usuários	Política de acesso	Grupo de recursos	Recursos	Confiança zero	Habilitado
Usuário 1	UG1	AP1	RG1	2 recursos	2 recursos	2 recursos
Usuário 1	UG1	AP2	RG2	0 recursos	0 recursos	0 recursos
Usuário 1	UG1	AP3	Nulo		0 recursos	Todos os recursos
Usuário 1	UG1	Nulo	Nulo		0 recursos	Todos os recursos

Para habilitar ou desabilitar o sinalizador zero-Trust:

1. Navegue até o seguinte caminho de configuração:

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

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

2. Modifique o valor zeroTrustPolicies.
3. Navegue até o seguinte pacote principal:

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

4. Execute o seguinte comando para excluir o leme principal:

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

5. Execute o seguinte comando para verificar o status dos pods

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

6. Execute o seguinte comando para instalar o leme do núcleo após a terminação de todos os pods:

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

7. Execute o seguinte comando para verificar o status dos pods que aparecem:

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

Solução de problemas de atualização de SO

Esta seção fornece dicas de troubleshooting relacionadas aos problemas observados com o aplicativo OS Upgrade no BPA.

O Modelo de Dispositivo de Destino Não Pode Ser Visto ao Criar uma Política de Conformidade

Verifique se os metadados de imagem correspondentes estão disponíveis em Imagens de

software em SWIM. Se não for encontrado, execute uma das seguintes opções:

- Sincronizar imagens para recuperar metadados de imagem de controladores como Cisco Catalyst Center, NDFC, vManage e FMC
- Crie metadados de imagem necessários para controladores como NSO, CNC, Direct-to-Device e ANSIBLE

A conformidade de software mostra um status não operacional

Isso pode ocorrer devido aos seguintes motivos:

- Nenhum ativo foi encontrado com o modelo selecionado ao criar a política de conformidade de software
- O nome do modelo no SWIM não corresponde ao modelo de dispositivo de conformidade no inventário de dispositivos para todos os dispositivos
- Se o SMU foi escolhido como parte da criação de conformidade de software e a descoberta SMU falhou para todos os dispositivos
- O modelo de processo selecionado para a execução do modelo de verificação de conformidade falhou ou não foi encontrado
- O número de série ou a versão atual não está disponível para todos os dispositivos no modelo selecionado ao criar conformidade de software

O Status do Resultado de Conformidade de Software de Determinados Dispositivos É Desconhecido

Isso pode ocorrer devido aos seguintes motivos:

- O nome do modelo no SWIM não corresponde ao modelo de dispositivo de conformidade no inventário de dispositivos
- Se o SMU foi escolhido como parte da criação de conformidade de software e a descoberta SMU falhou para um dispositivo
- O modelo de processo selecionado para a execução do modelo de verificação de conformidade falhou ou não foi encontrado
- O número de série ou a versão atual não está disponível para os dispositivos

Porcentagem do Andamento da Conclusão do Trabalho de Atualização

Se o percentual de progresso da conclusão do trabalho de atualização for menor que 100, mesmo que a atualização esteja concluída, confirme se as configurações Aguardar Reversão estão habilitadas em Atualização do SO > Configurações > Reversão e se a alternância Verificação do

Usuário está ativada. Se o percentual de conclusão geral permanecer abaixo de 100, selecione Reverter ou Concluir.

Agendamento do Trabalho Atingido, Dispositivos estão Parados no Estado Aguardando

Se os dispositivos estiverem presos em um estado Aguardando após o início do trabalho agendado, tente reiniciar os microsserviços Kafka, Camunda, Scheduler e OS Upgrade.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.