Guida per l'utente di BPA Aggiornamento del sistema operativo versione 5.1

Introduzione

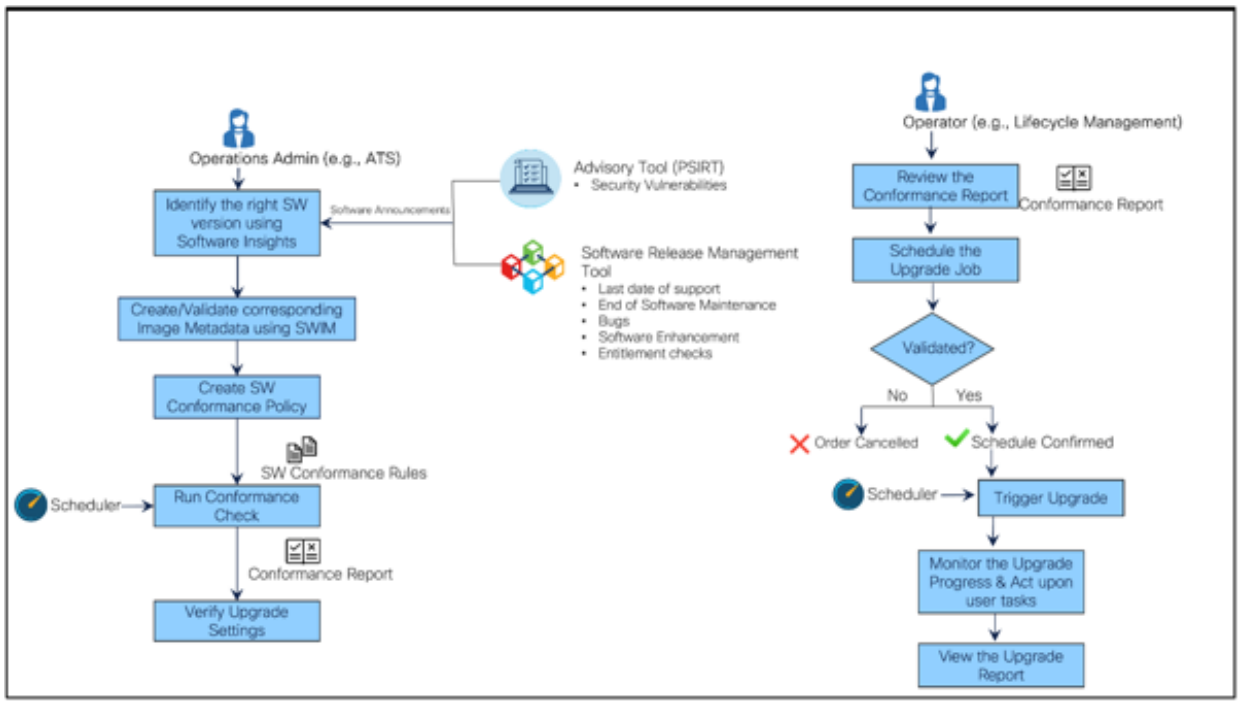
L'applicazione BPA (Business Process Automation) per l'aggiornamento del sistema operativo fornisce una soluzione di automazione completa per l'esecuzione di aggiornamenti e conformità software dei dispositivi di rete su più domini. Supporta più controller di dominio e offre un'esperienza utente unificata. Supporta sia gli aggiornamenti del sistema operativo di base che gli aggiornamenti delle patch SMU (Software Maintenance Update) o RPM (Package Manager).

Funzionalità principali

L'applicazione Aggiornamento sistema operativo fornisce le seguenti funzionalità di automazione chiave:

- Gestione delle immagini software: Elenco centralizzato di immagini software e relative versioni (di tutti i fornitori) per il processo di aggiornamento software da utilizzare
- Informazioni sul software: Identifica i rischi e le vulnerabilità del software esposti agli asset di rete e ottiene informazioni dettagliate sulle versioni software consigliate dal fornitore
- Conformità software: Identifica tutti gli asset della rete di cui è necessario aggiornare le immagini software
- Definizione del metodo di aggiornamento (MOP): Predefinisce il processo di upgrade e i controlli preliminari e successivi per ogni modello o famiglia di dispositivi del fornitore
- Processi di aggiornamento: Pianifica gli aggiornamenti per gli asset non conformi durante le finestre di manutenzione tra aree geografiche, controlla lo stato di avanzamento dell'aggiornamento e ottiene report dettagliati

Flusso end-to-end



Flusso end-to-end

Nella figura precedente sono illustrati i flussi di chiamate dell'applicazione di aggiornamento del sistema operativo per due diversi utenti: Amministratore delle operazioni e operatore di rete, pronto all'uso. Per ulteriori informazioni sui ruoli OOB e sulle autorizzazioni corrispondenti, fare riferimento a Controllo accesso.

Persona	Descrizione	Area di lavoro
Amministratore operazioni	Rileva le vulnerabilità del software (ad esempio, avvertenze, bug, bollettini di fine ciclo di vita) che influiscono sugli asset di rete	BPA: Aggiornamento del sistema operativo/Gestione delle immagini software/Consulenze
Amministratore operazioni	Identifica la versione del software interessata e le risorse interessate e determina la versione di destinazione corretta in base ai suggerimenti forniti dal fornitore	BPA: Aggiornamento del sistema operativo/Gestione delle immagini software/Informazioni approfondite
Amministratore operazioni	Crea i metadati dell'immagine software richiesti	BPA: Upgrade del sistema operativo/Gestione immagini software/Immagini software
Amministratore operazioni	Crea l'intento per i modelli di dispositivo interessati ed esegue il criterio su richiesta o all'esecuzione pianificata del criterio	BPA: Aggiornamento del sistema operativo/criteri di conformità software
Amministratore operazioni	Identifica gli asset non conformi o interessati	BPA: Aggiornamento del sistema operativo/conformità software /Visualizza risultati
Amministratore operazioni	Crea o modifica i criteri di aggiornamento in base al MOP di aggiornamento; ciò include predefinire i controlli preliminari e successivi, i workflow per la distribuzione o l'attivazione, la deviazione o l'inversione del traffico e il rollback per gli aggiornamenti a uno o più passaggi	BPA: Criteri di aggiornamento del sistema operativo
Operatore di rete	Pianifica un processo per aggiornare tutti i dispositivi non conformi	BPA: Processi di aggiornamento del sistema operativo
Operatore di rete	Controlla l'avanzamento del processo di aggiornamento	BPA: Dettagli processo/processo di aggiornamento del sistema operativo
Operatore di rete	Interviene sulle attività utente, se presenti, per risolvere i problemi e consente al processo di procedere al passaggio successivo	BPA: Dettagli processo/aggiornamento del sistema operativo

Proposta di valore

Di seguito sono riportati i valori aggiunti forniti dall'applicazione Aggiornamento sistema operativo:

- Approccio API-first per semplificare l'utilizzo dei servizi da parte dei sistemi di supporto alle operazioni (OSS, Operations Support Systems) e dei sistemi di supporto alle attività (BSS, Business Support Systems) in direzione nord
- Convalida rapida della conformità software dei dispositivi di rete su reti gestite da diversi controller di dominio
- Gli operatori dispongono di un maggiore controllo sui processi di aggiornamento mediante l'utilizzo di meccanismi di batch, accodamento e pianificazione
- I processi di aggiornamento possono essere creati in anticipo per le revisioni ed eseguiti in seguito
- Meccanismo di coda che consente un throughput migliore e più veloce con errori minimi o nulli
- Pre-aggiornamento dei backup di configurazione automatici per il ripristino in caso di guasti
- Esecuzioni di pre- e post-controllo, per garantire la riuscita degli aggiornamenti senza interruzioni del servizio
- Approccio basato su regole che offre la flessibilità necessaria per predefinire il MOP di aggiornamento con controlli pre e post-convalida, distribuzione o attivazione, deviazione o inversione del traffico e processi di rollback, consentendo di personalizzarli in base alle esigenze

Controller e piattaforme di dispositivo supportati

Le seguenti piattaforme sono state convalidate in BPA e sono supportate in OOB. Tuttavia, il quadro è generico e può essere esteso a nuove piattaforme. Nelle versioni future, il supporto OOB per altre piattaforme sarà fornito in base alla priorità.

Controller di dominio	Piattaforme dispositivo
Cisco Catalyst Center v2.3.7.5-70434	- Cisco IOS, Cisco IOS-XE - Cisco IOS, Cisco IOS-XE
vManage v20.12.4	Nota: Affinché la distribuzione remota dei server funzioni correttamente, i dispositivi devono essere v17.9.x o versione successiva
Nexus Dashboard Fabric Controller (NDFC) v12.1.2e e v12.2.2	- Cisco-NXOS (N9k)
Firewall Management Center (FMC) v7.4.1	- Firepower 3140

Controller di dominio	Piattaforme dispositivo
Network Services Orchestrator (NSO) v6.3	- Cisco-IOSXR (NCS540, NCS560, ASR9K) - Cisco-NXOS (N9K) Nota: È richiesto NX-OS NED v5.25.17 o superiore
Cross Network Controller (CNC) v6.0	- Cisco-IOSXR (NCS540, ASR9K)
ANSIBLE v2.9.18 (AWX - 17.1.0)	- Cisco-IOSXR (NCS540, ASR9K)
Direct-to-Device (tramite Telnet e SSH)	- Cisco-IOSXR (NCS540, ASR9K)

Nuove caratteristiche

Per le funzioni incrementali rese disponibili per lo scenario di aggiornamento del sistema operativo per questa release, fare riferimento alle note sulla release di BPA.

Prerequisiti

Prima di utilizzare l'applicazione Aggiornamento sistema operativo, è necessario che siano soddisfatte le seguenti condizioni preliminari:

- Upgrade del sistema operativo, backup e ripristino, servizi di pianificazione e tutti i servizi della piattaforma o dell'agente controller necessari sono attivi e in esecuzione
- Gli artifact richiesti (ad esempio workflow, modelli di processo, criteri di aggiornamento predefiniti e così via) vengono caricati
- Vengono aggiunti i controller necessari e i dispositivi vengono sincronizzati correttamente. per ulteriori informazioni, fare riferimento a Controller supportati e piattaforme di dispositivo

Utilizzo dell'applicazione di aggiornamento del sistema operativo

L'applicazione Aggiornamento sistema operativo è costituita dai seguenti componenti:

- Gestione immagini software (SWIM)
- Gestione server di distribuzione immagini
- Software Insights
- Conformità software
- Criteri di aggiornamento
- Processi di aggiornamento
- Impostazioni

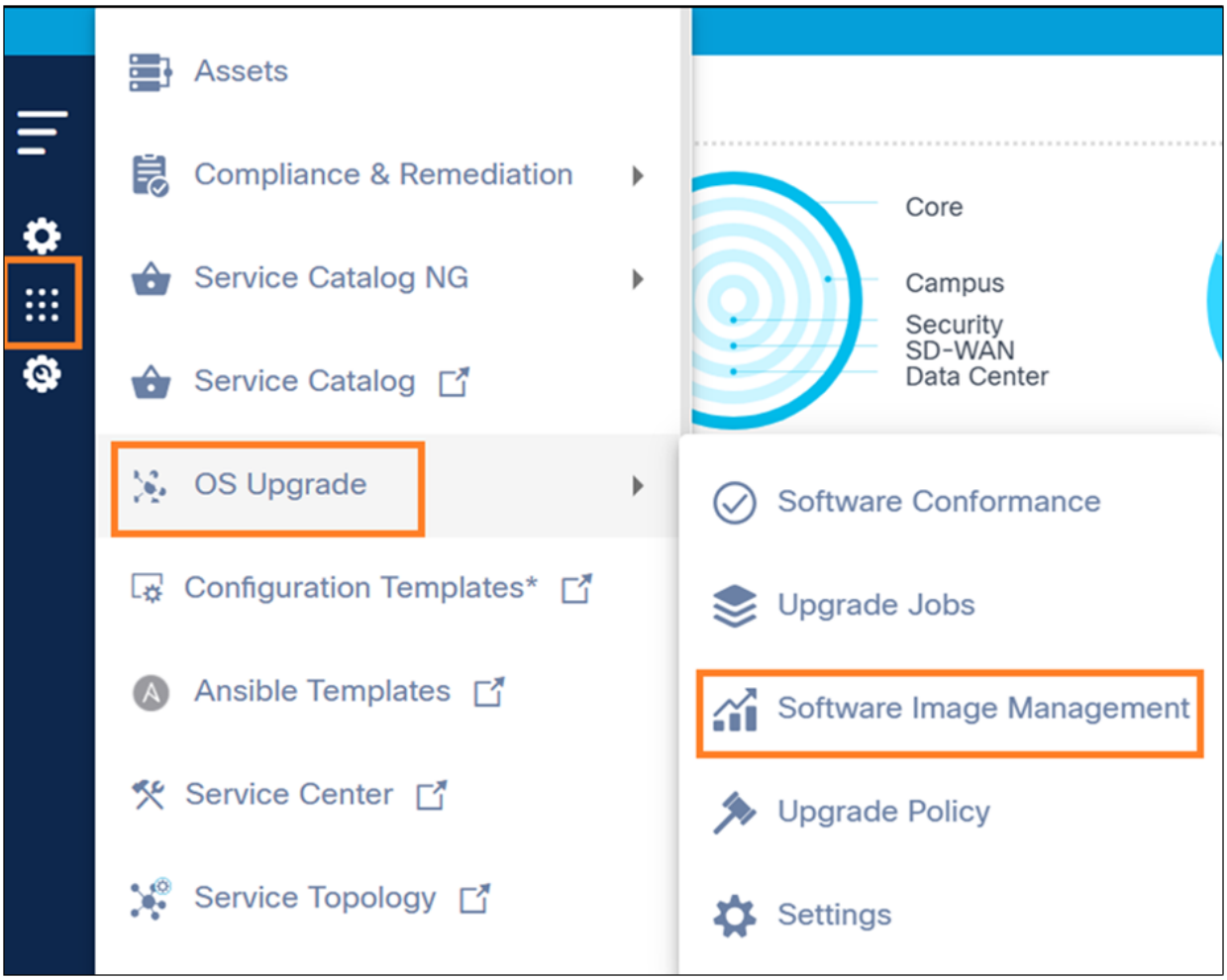
Gestione delle immagini software

Il componente SWIM consente agli utenti di Operations di gestire i dettagli delle immagini software per controller quali NSO, ANSIBLE, CNC, FMC e Direct-to-Device che non dispongono del supporto per la gestione delle immagini OOB. Vengono inoltre elencati i dettagli dell'immagine software gestita da controller quali vManage, NDFC e Cisco Catalyst Center, fornendo un elenco centralizzato di software gestito da tutti i controller di dominio. Le immagini software e il server di distribuzione delle immagini sono i due principali sottocomponenti del modulo SWIM.

Immagini software

Per accedere alla pagina Immagini software:

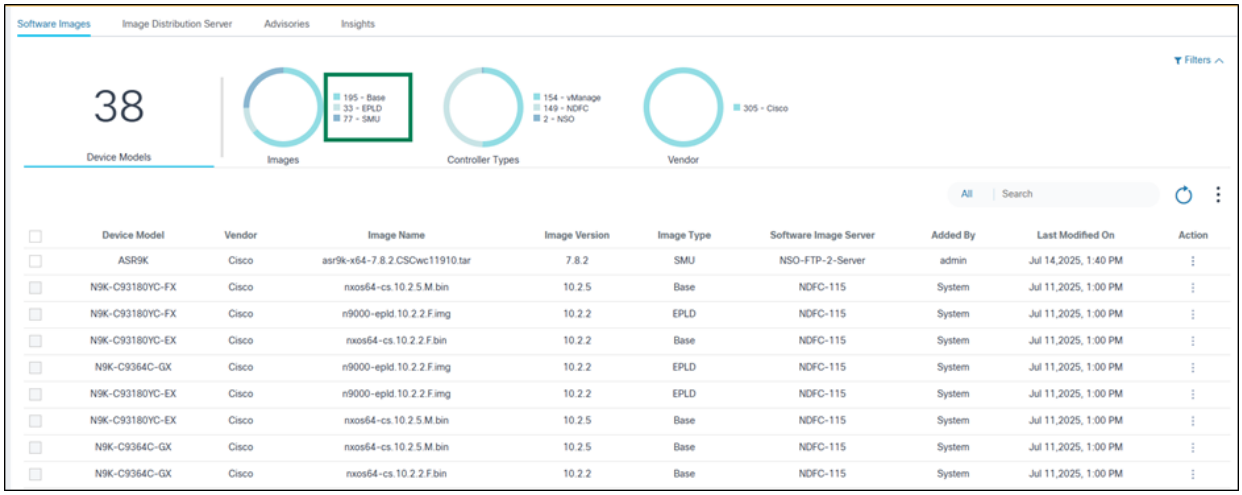
1. Accedere a BPA con le credenziali che hanno accesso a Gestione immagini software.



Navigazione in Software Image Management

2. Selezionare Aggiornamento sistema operativo > Gestione immagini software.

La pagina Gestione immagine visualizza le schede riportate di seguito. Immagini software, Image Distribution Server, avvertenze e informazioni approfondite.



Scheda Immagini software

La scheda Immagini software contiene quanto segue:

- Una sezione di analisi, visualizzata nella parte superiore, che fornisce le informazioni riportate di seguito.
    - Numero totale di modelli di dispositivi e immagini software associate
    - Un filtro rapido Images che consente di filtrare le immagini in base al tipo (ad es. base, SMU); il numero indica il numero totale di immagini associate a un rispettivo tipo di immagine
    - Un filtro rapido Tipi di controller che consente di filtrare le immagini in base al tipo di controller (ad esempio, Cisco Catalyst Center, vManage, NSO o NDFC, Direct-to-Device, CNC, ANSIBLE, FMC) per cui sono ospitate le immagini; il numero indica il numero totale di immagini associate a un rispettivo tipo di controller
    - Un filtro rapido del fornitore che consente di filtrare le immagini in base al fornitore che ha pubblicato il software
- L'icona Altre opzioni fornisce le seguenti funzionalità:
    - Aggiungi dettagli immagine: Aggiungere nuovi metadati dell'immagine
    - Caricamento di massa: Carica in blocco metadati immagine in formato .csv
    - Immagini sincrone: Sincronizza i metadati dell'immagine dai controller (ad esempio, Cisco Catalyst Center, vManage, NDFC e FMC)
    - Elimina tutto: Eliminazione di massa delle immagini selezionate

---

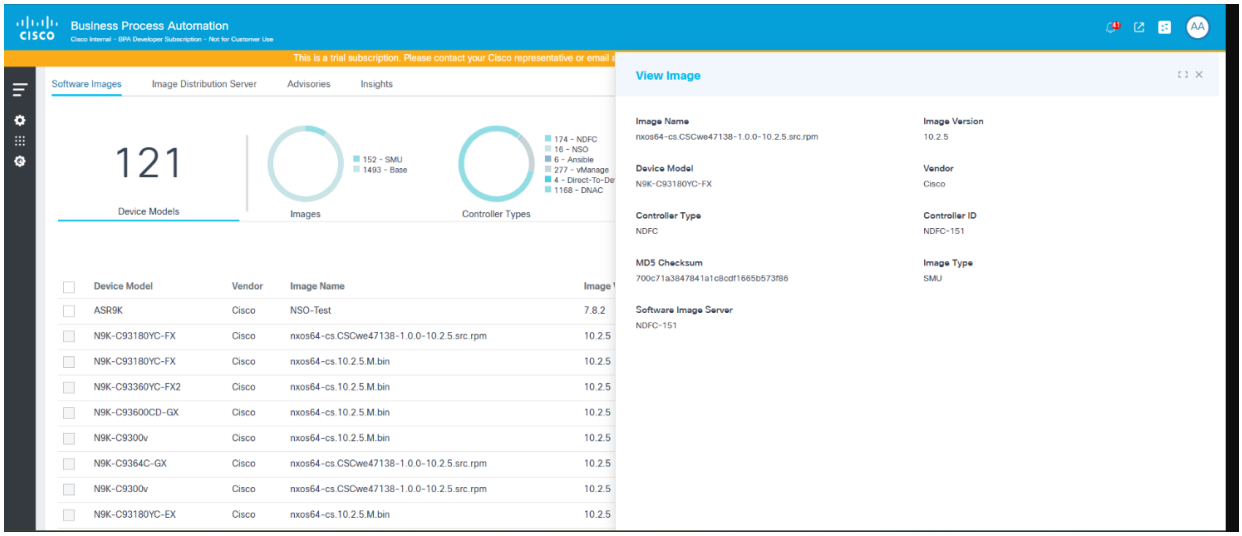
Nota: L'aggiunta, l'eliminazione e il caricamento di massa dei dettagli dell'immagine sono consentiti solo per i controller NSO, ANSIBLE, CNC e Direct-to-Device.

- Il filtro Search (Cerca) può essere utilizzato per la ricerca di immagini e include i seguenti

filtri di ricerca esclusivi:

  - Tutto: Cerca in tutti i campi
  - Nome immagine: Cercare le immagini con un nome specifico
  - Modello dispositivo: Cerca le immagini con un modello specificato
  - Versione immagine: Ricerca di immagini con una versione software specifica
  - Server immagine software: Cercare le immagini associate a un server immagini specifico
- L'icona Aggiorna aggiorna la pagina e cancella i filtri selezionati.
- Le immagini esistenti vengono visualizzate in una tabella griglia con le seguenti colonne:

  - Modello dispositivo: Modello di dispositivo per cui sono applicabili i dettagli dell'immagine
  - Fornitore: Fornitore che pubblica le immagini software
  - Nome immagine: Nome file dell'immagine
  - Versione immagine: Versione software dell'immagine
  - Tipo di immagine: Determina il tipo di immagine (ad esempio, base, SMU, EPLD (Electronic Programmable Logic Device))
  - Server immagine software: Server immagini in cui è presente l'immagine corrente
  - Aggiunto da: Utente che ha aggiunto i metadati dell'immagine
  - Data ultima modifica: Timestamp dell'ultimo aggiornamento dei dettagli immagine
  - Azione: Fornisce un'icona Altre opzioni da cui è possibile selezionare le azioni specifiche della riga (ad esempio, modifica, eliminazione)
- Ordinare le immagini facendo clic sull'intestazione di una colonna



Visualizza immagine

- Facendo clic su una riga viene visualizzata la finestra Visualizza immagine

Sincronizzazione dei metadati delle immagini software

Per eseguire la sincronizzazione su richiesta delle immagini software:

Sincronizza immagini

1. Selezionare l'icona Altre opzioni > Sincronizza immagini. I dettagli dei metadati dell'immagine da vManage, Cisco Catalyst Center, NDFC e FMC vengono rilevati e salvati in BPA.

Nota: Per i controller FMC, i dati esistenti vengono conservati ogni volta che viene eseguita una sincronizzazione. Vengono aggiunte solo le nuove immagini.

---

2. Se il nome dell'immagine dal controller FMC include la parola "FTD" o "Firepower Threat_Defense", il deviceModel per quell'immagine viene mappato come FTD.

O

Se il nome dell'immagine del controller FMC include la parola "FMC", "FW_Mgmt_Center" o "Firewall_Management_Center", l'elemento deviceModel relativo all'immagine viene mappato come FMC.

Nota: FMC non associa le informazioni sul modello ai metadati dell'immagine. Una volta completata la sincronizzazione, modificare i rispettivi metadati dell'immagine e aggiornare il modello come richiesto. Il processo di aggiornamento del CCP non funziona come previsto senza l'aggiornamento del modello.

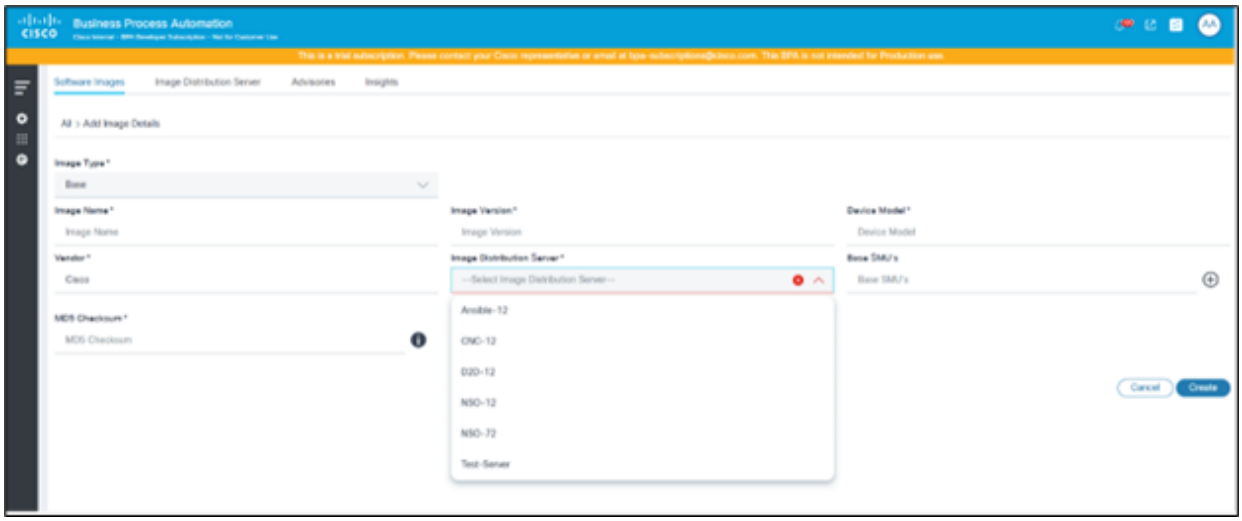
---

3. Nelle immagini dei server remoti vManage l'UUID (Universally Unique Identifier) è inizialmente mappato nella colonna Versione dopo l'operazione di sincronizzazione. Gli operatori devono modificare manualmente i metadati del server remoto richiesti e aggiornarli con la versione dell'immagine appropriata. Se questa mappatura non viene eseguita, gli altri componenti di aggiornamento del sistema operativo (ad esempio, conformità software, criteri di aggiornamento, processi di aggiornamento e così via) non funzionano come previsto.

4. Per pianificare la sincronizzazione automatica dei metadati SWIM a intervalli regolari, fare riferimento a Configurazione distribuzione.

Aggiunta di metadati dell'immagine software

1. Selezionare l'icona Altre opzioni > Aggiungi dettagli immagine. Verrà visualizzata la pagina Aggiungi dettagli immagine.



Aggiungi dettagli immagine

2. Immettere le informazioni nei seguenti campi:

- Tipo di immagine: Tipo di immagine (ad esempio, base, SMU, EPLD)
- Nome immagine: Nome del file di immagine; Gli utenti possono immettere un percorso relativo o assoluto dell'immagine nel campo Nome. Se gli utenti forniscono un percorso assoluto, l'immagine viene recuperata direttamente da tale percorso; se gli utenti forniscono un percorso relativo, il sistema risolve il percorso completo aggiungendo il percorso di base definito nel server del repository durante la distribuzione
- Versione immagine: Versione software dell'immagine
- Modello dispositivo: Il modello di dispositivo per il quale l'immagine viene contrassegnata

---

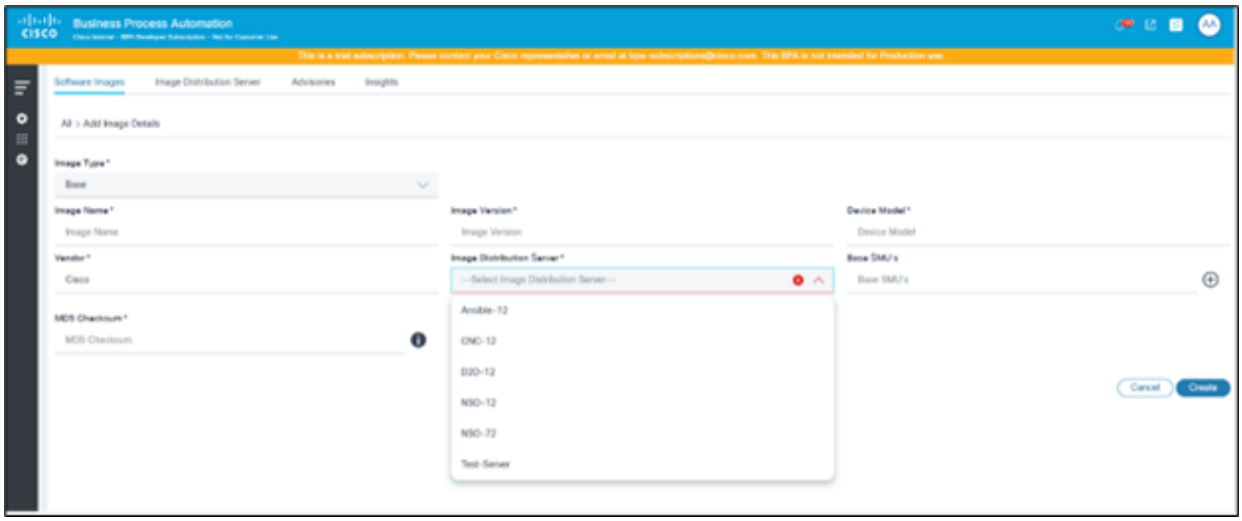
Nota: Il modello del dispositivo deve corrispondere alle informazioni sul modello fornite dal controller CNC, NSO, Direct-To-Device o ANSIBLE per i dispositivi applicabili.

- Fornitore: Il fornitore o il provider che ha pubblicato l'immagine; l'impostazione predefinita è Cisco, ma può essere modificata in base alle esigenze
- Server di distribuzione immagini: Selezionare il server di distribuzione delle immagini che ospita il file software indicato nel campo Nome immagine. Quando si seleziona un server di distribuzione immagini, vengono generate immagini per tutti gli ID controller associati al tipo

di controller specificato definito all'interno del server di distribuzione immagini. Se un utente aggiunge o rimuove istanze di controller nel server di distribuzione immagini, le immagini software corrispondenti vengono aggiunte o rimosse per tali istanze di controller.
- SMU di base: SMU presenti nell'immagine dorata di base; questa opzione è applicabile solo se il tipo di immagine è Base
- Checksum MD5: Checksum MD5 dell'immagine per verifica

3. Fare clic su Crea. Viene visualizzata la notifica Progress seguita da un messaggio di conferma.

Nota: È necessario aggiungere i metadati dell'immagine per le SMU di Bridge prima di utilizzarli in un criterio di aggiornamento. Per aggiungere le SMU Bridge, selezionate SMU dall'elenco a discesa Image Type (Tipo di immagine).



Aggiungi metadati immagine SMU bridge

Caricamento di massa dei metadati dell'immagine software

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

File CSV di esempio con informazioni sull'immagine

1. Preparare un file .csv con i dettagli dell'immagine necessari e i nomi di colonna seguenti:

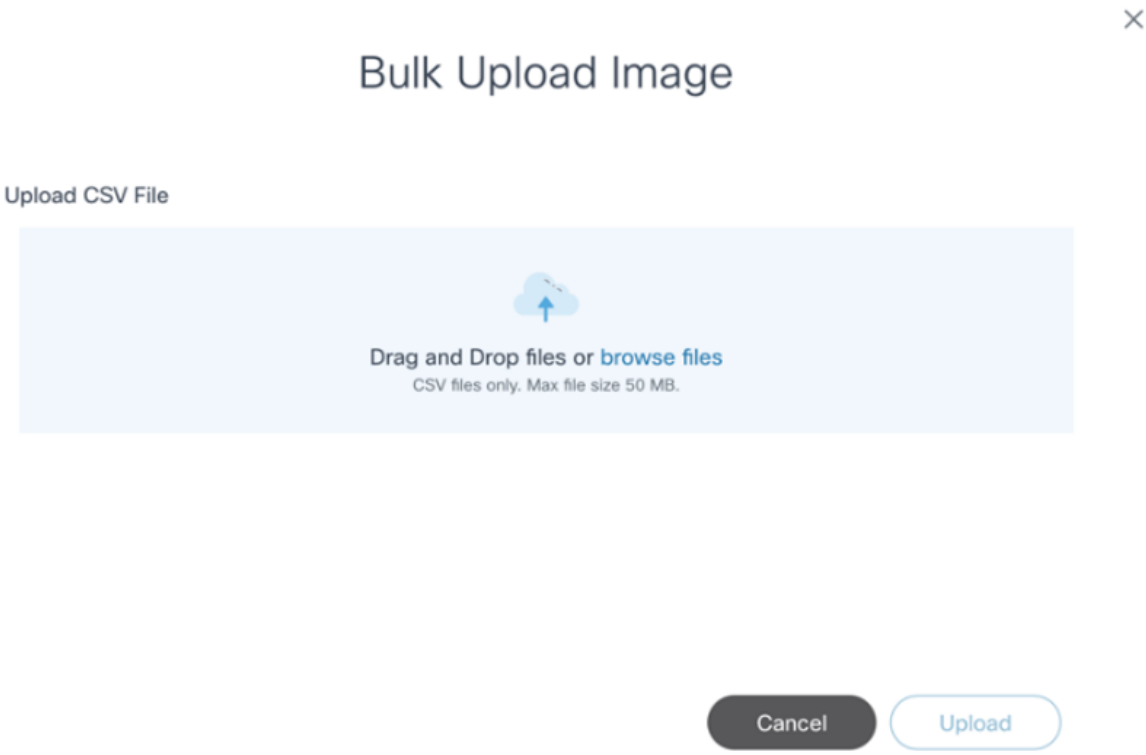
- Nome immagine
- Version
- Modello dispositivo

- Fornitore
- Tipo di immagine

Nota: Sono supportati solo i valori Base, SMU ed EPLD.

- Server di distribuzione immagini
- Checksum MD5

2. Selezionare l'icona Altre opzioni > Caricamento di massa. Viene visualizzata la finestra Bulk Upload Image.



Carica immagine in blocco

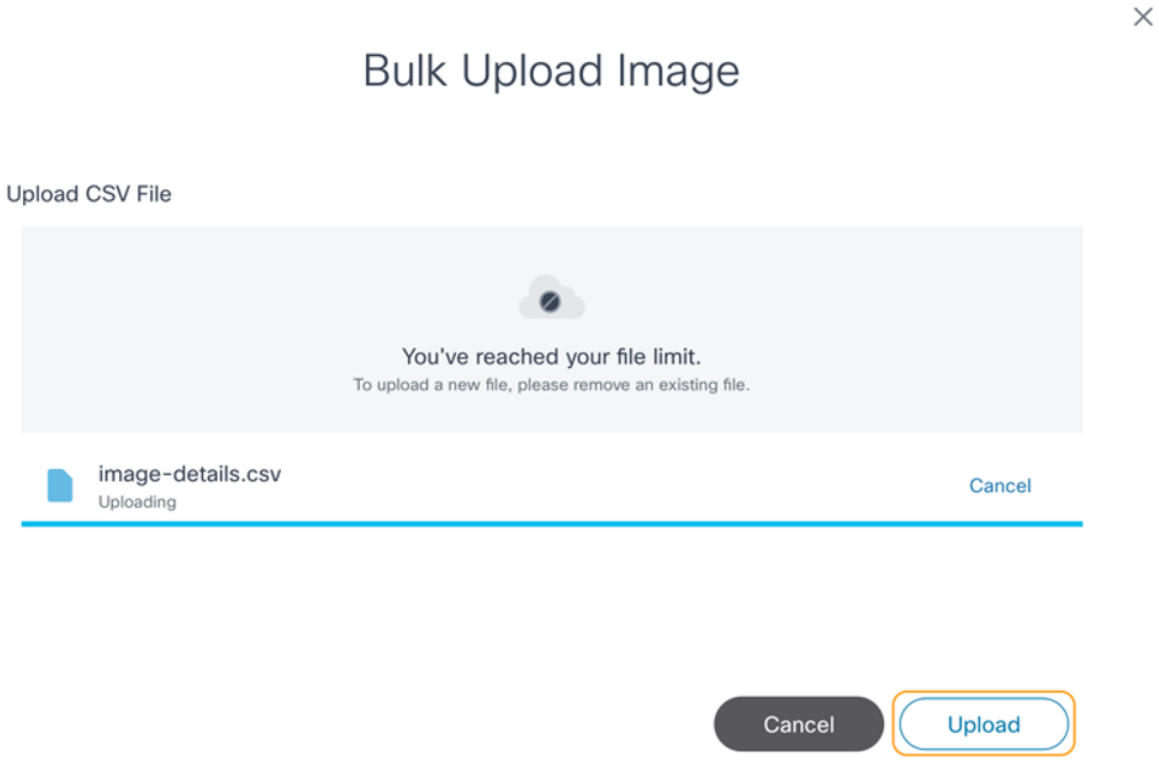
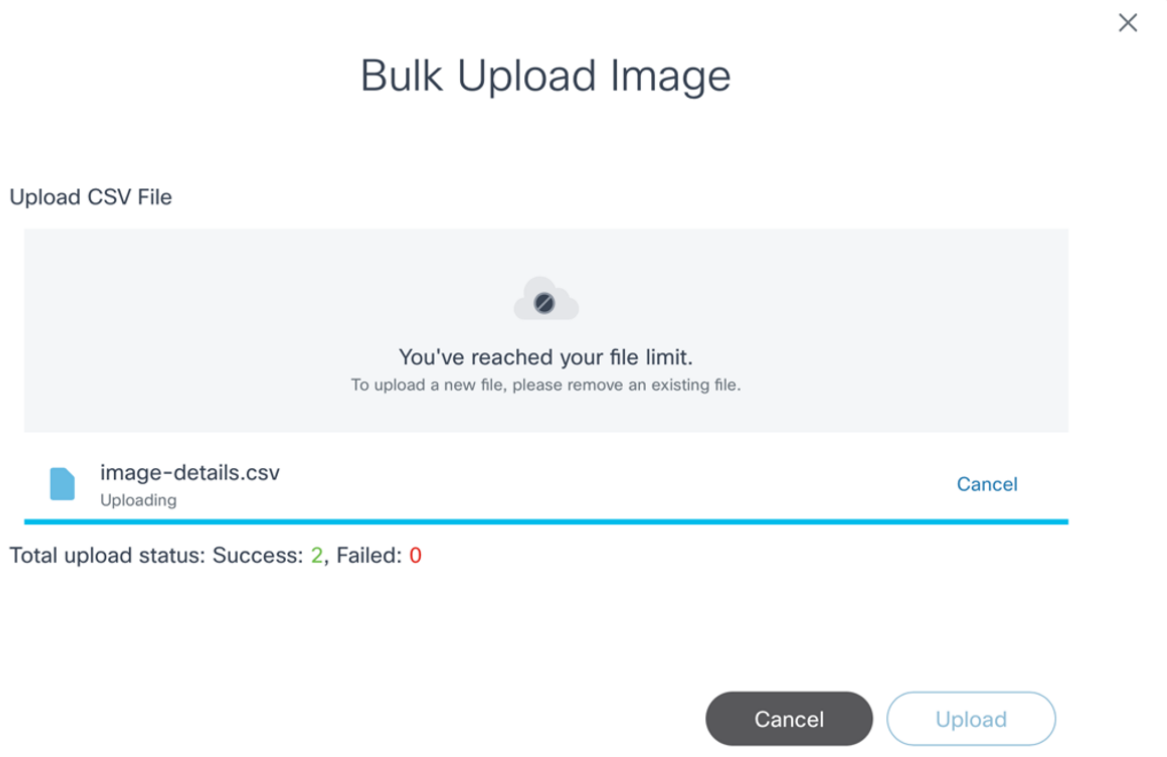


Immagine di caricamento di massa - Caricamento CSV

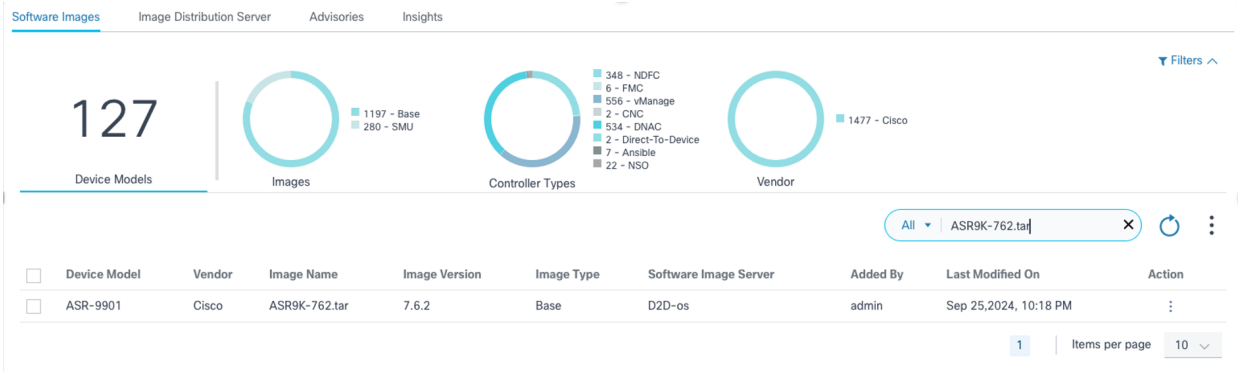
3. Selezionare un file .csv preparato e fare clic su Upload. I dettagli dell'immagine dal file con estensione csv vengono convalidati e quindi elaborati. Una volta caricato il file, viene visualizzato lo stato finale del caricamento di massa.



Stato caricamento immagine in blocco riuscito

Nota: In caso di errori di convalida dei dati (ad esempio, record duplicati o parametri non validi), i messaggi di errore vengono visualizzati sotto forma di griglia nella finestra Caricamento di massa immagine. Gli utenti possono correggere i valori nel file .csv e caricarlo nuovamente.

Modifica dei metadati delle immagini software esistenti

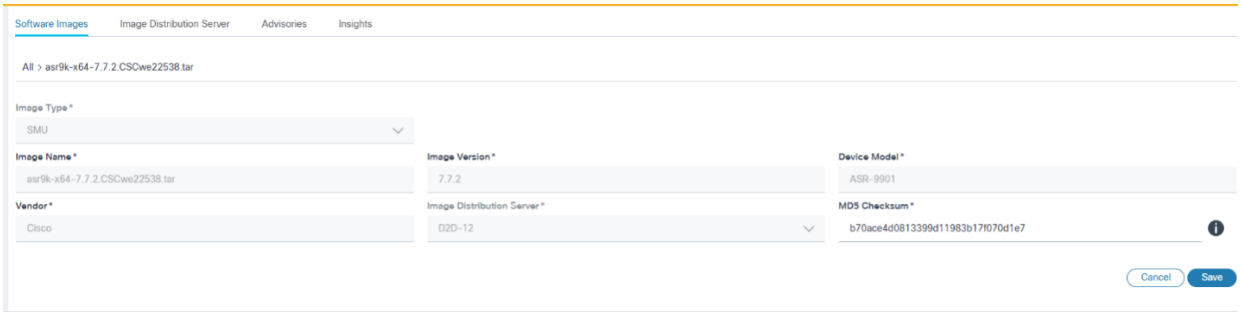


Cerca nei metadati dell'immagine software

1. Individuare l'immagine da aggiornare utilizzando il filtro Cerca.

Modifica

2. Dalla colonna Azione dell'immagine desiderata, selezionare l'icona Altre opzioni > Modifica.



Modifica immagini software

3. Aggiornate i parametri richiesti e fate clic su Salva (Save) per salvare le modifiche oppure su Annulla (Cancel) per annullare le modifiche. Viene visualizzata una notifica di stato seguita da un messaggio di conferma per l'aggiornamento dell'immagine.

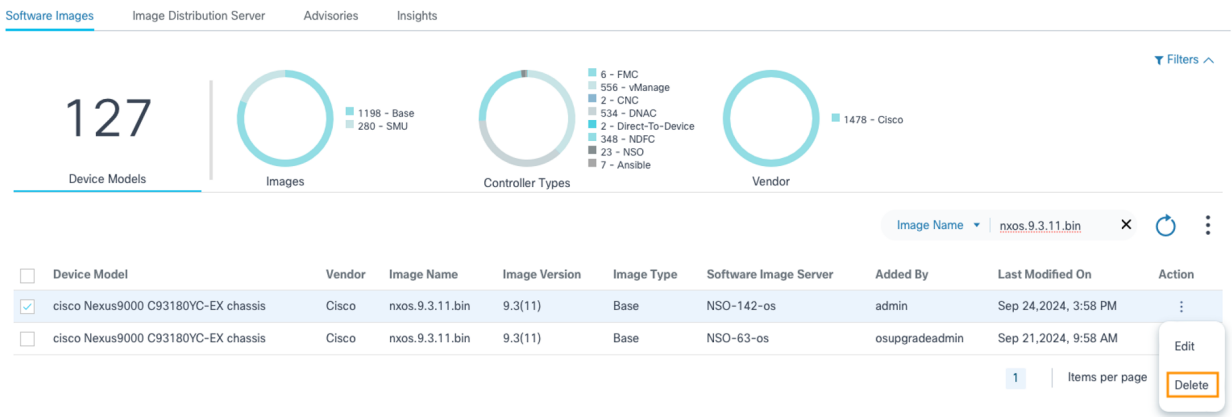
Nota: Occorre prendere nota del seguente elenco.

- La modifica è disponibile per i controller CNC, NSO, D2D, ANSIBLE, FMC e vManage (applicabile solo per i metadati delle immagini server remote)
- L'aggiornamento del modello di dispositivo è supportato solo per le immagini del server remoto vManage
- È possibile aggiornare solo il campo Versione software per i metadati dell'immagine del server remoto vManage
- Per le immagini vManage, gli utenti possono visualizzare il server delle immagini software al posto delle istanze del controller

Eliminazione dei metadati dell'immagine software

Cerca nei metadati dell'immagine software

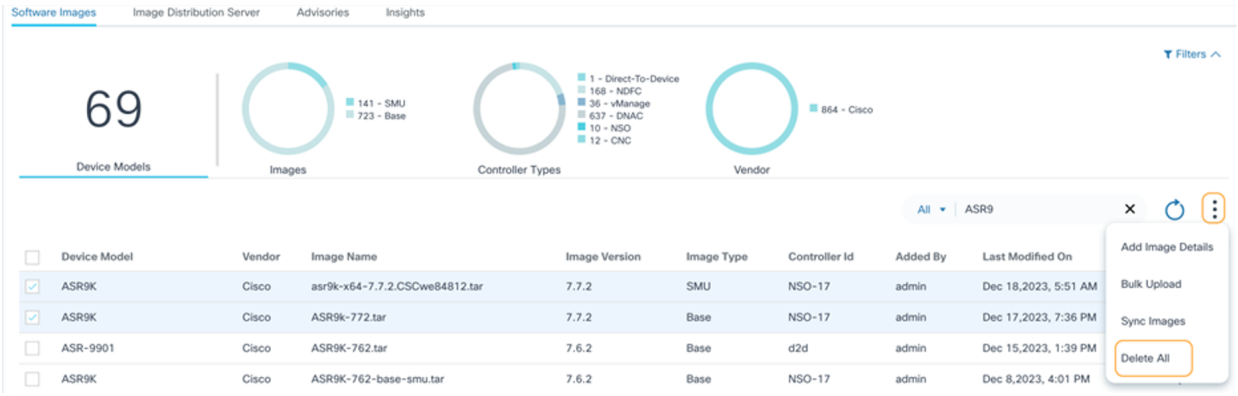
1. Utilizzare il campo Search per individuare l'immagine desiderata.



Elimina

2. Dalla colonna Azione dell'immagine desiderata, selezionare l'icona Altre opzioni > Elimina per eliminare un'immagine.

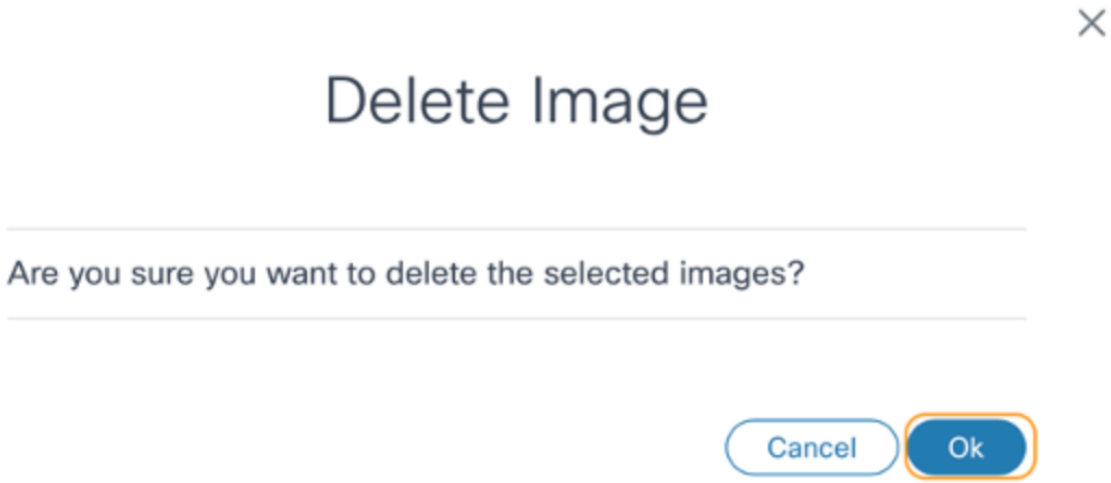
O



Elimina tutto

Selezionare le immagini desiderate e selezionare l'icona Altre opzioni > Elimina tutto per eliminare più immagini.

Viene visualizzata una conferma.



Conferma

3. Fare clic su OK. Viene visualizzata una notifica di stato seguita da un messaggio di conferma.

Nota: Occorre prendere nota del seguente elenco.

- I metadati dell'immagine possono essere aggiunti solo per i controller NSO, ANSIBLE, Direct-to-Device e CNC. Per tutti gli altri controller aziendali, viene utilizzata la funzionalità SWIM integrata e le immagini vengono rilevate dai rispettivi controller
- La funzionalità di rilevamento delle immagini non è supportata per i server di immagine dei controller NSO, ANSIBLE, Direct-to-Device e CNC.
- Per impostazione predefinita, i metadati dell'immagine del server remoto vManage contengono UUID per il parametro della versione post-sincronizzazione. Gli utenti devono

modificare i metadati e aggiornare l'UUID con la versione corrispondente. La versione dell'immagine corrispondente può essere identificata dal controller vManage o accedendo al dispositivo in cui si trova l'immagine.

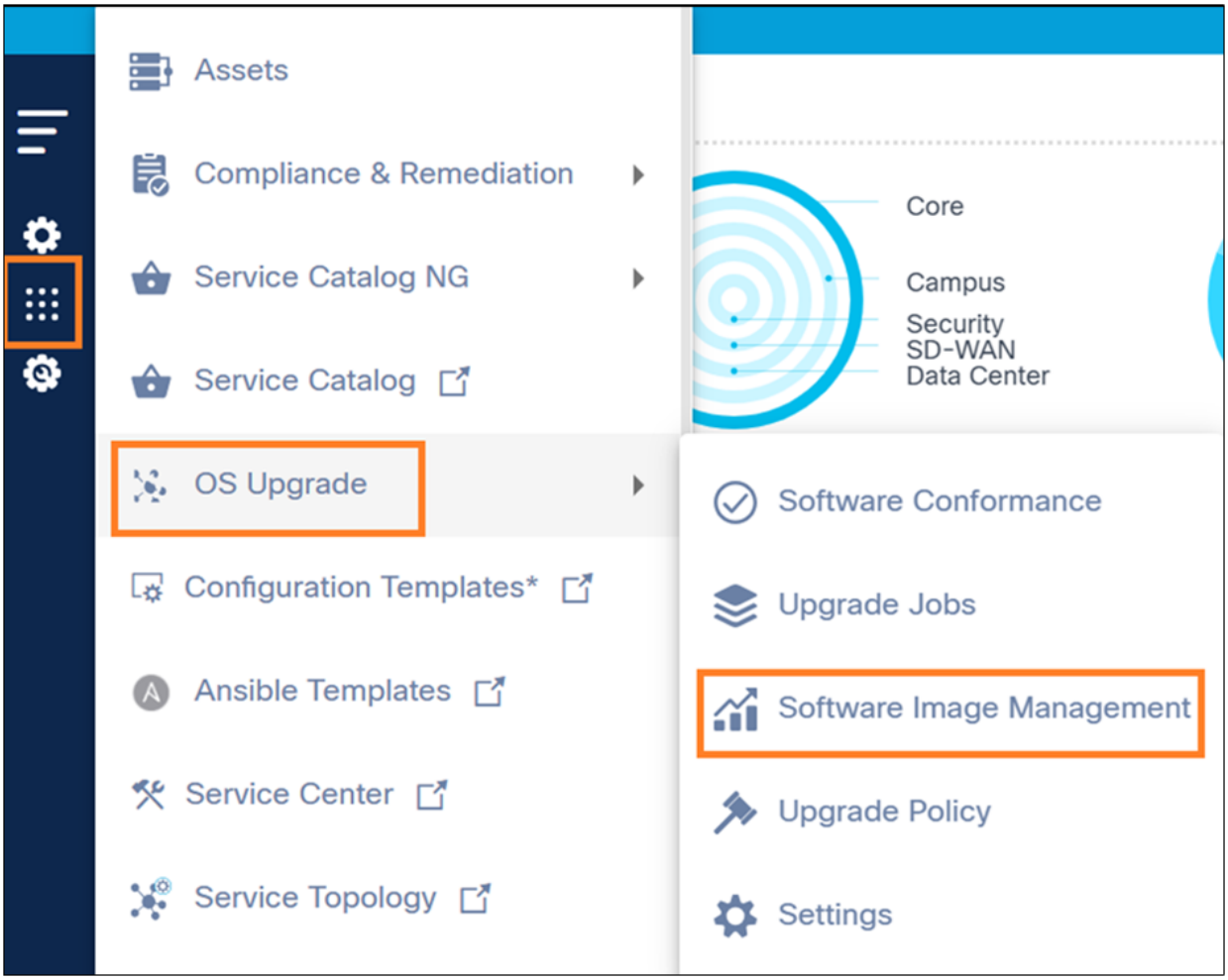
Gestione server di distribuzione immagini

Server di distribuzione immagini

Il componente consente agli utenti di Operations di gestire i dettagli del server del repository di immagini per i controller CNC, NSO, ANSIBLE, FMC e Direct-To-Device che non dispongono del supporto per la gestione del repository di immagini OOB.

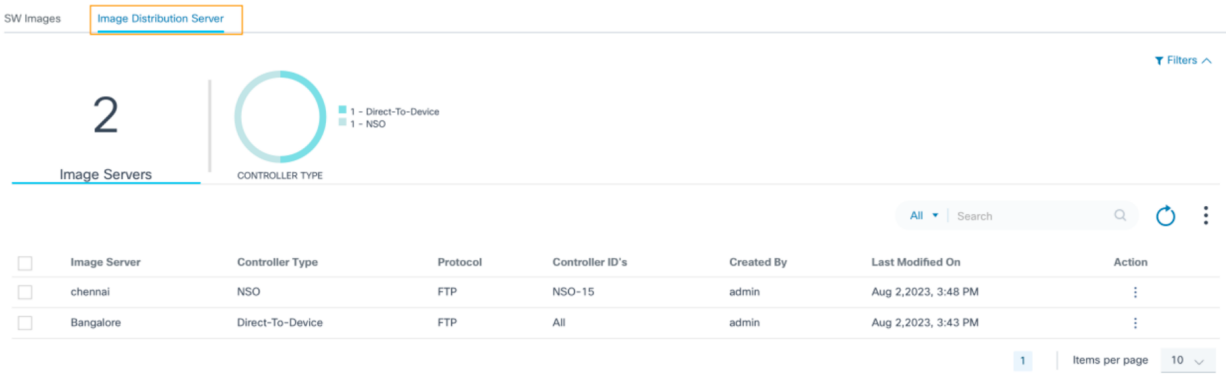
Per accedere alla pagina Image Distribution Server:

1. Accedere a BPA con le credenziali che dispongono dell'accesso di gestione al server di distribuzione delle immagini.



Gestione delle immagini software

2. Selezionare Aggiornamento sistema operativo > Gestione immagini software.



Scheda Server di distribuzione immagini

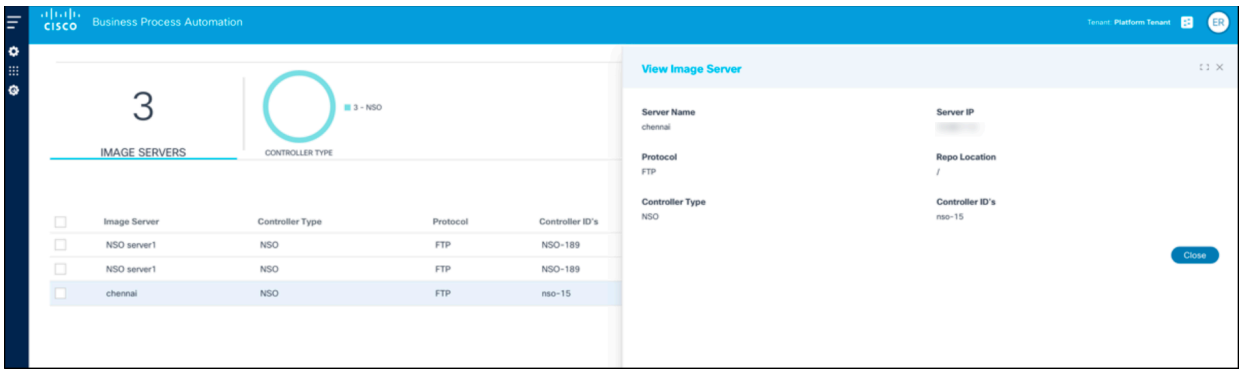
3. Fare clic sulla scheda Server di distribuzione immagini.

La scheda Server di distribuzione immagini contiene le informazioni seguenti:

- Una sezione di analisi, visualizzata nella parte superiore, che fornisce le informazioni riportate di seguito.
    - Numero totale di server di immagini incorporati in questa istanza BPA
    - un filtro rapido di tipo controller che consente di filtrare i server di immagini in base al tipo di controller (ad esempio, NSO, Direct-to-Device, CNC, ANSIBLE, FMC); il numero indica il numero totale di server di distribuzione immagini associati a quel tipo di controller
- Un'icona Altre opzioni che fornisce le seguenti funzionalità:
    - Aggiungi server immagini: Aggiungi nuovo server di distribuzione immagini
    - Elimina tutto: Eliminazione in blocco dei server di distribuzione selezionati
- Filtro di ricerca che può essere utilizzato per la ricerca nei server di distribuzione e include i seguenti filtri di ricerca esclusivi:
    - Tutto: Esegue la ricerca in tutti i campi
    - Server immagine: Cerca server con un nome server specifico
    - ID controller: Cerca i server associati a un ID controller specifico
- Icona Aggiorna che può essere utilizzata per aggiornare la pagina e cancellare i filtri selezionati
- I server di distribuzione esistenti vengono visualizzati in una tabella griglia con le colonne riportate di seguito.
- Server immagine: Nome univoco del server del repository
    - Tipo controller: Tipo di controller a cui è applicabile questo server immagini
    - Protocollo: Protocollo di copia supportato dal server del repository

Nota: Sono supportati solo FTP, SCP e SFTP (Secure File Transfer Protocol)

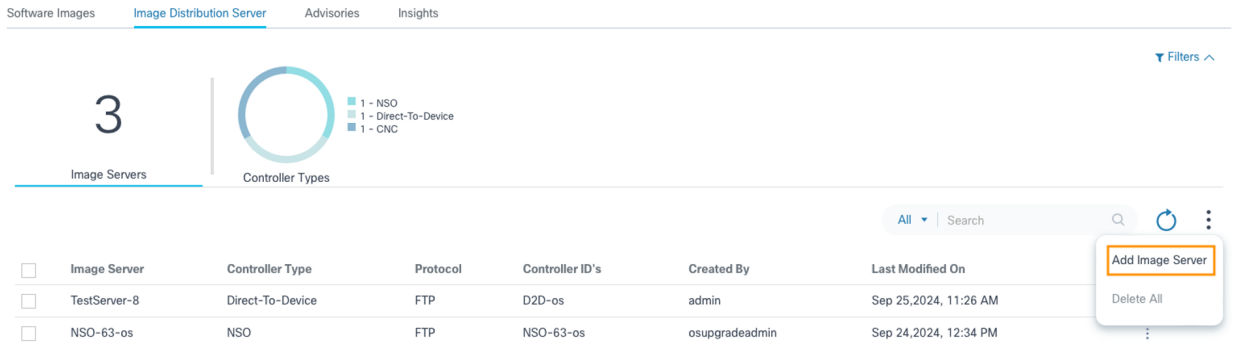
- ID controller: Istanze del controller per le quali il server del repository corrente è utilizzabile o applicabile; l'istanza del controller fa riferimento ai dispositivi gestiti tramite tale controller
- Creato da: Utente che ha eseguito l'accesso al server del repository
- Data ultima modifica: Timestamp dell'ultimo aggiornamento dei dettagli del server
- Azione: Fornisce azioni specifiche per le righe, ad esempio Modifica ed Elimina



Visualizza pannello Image Server

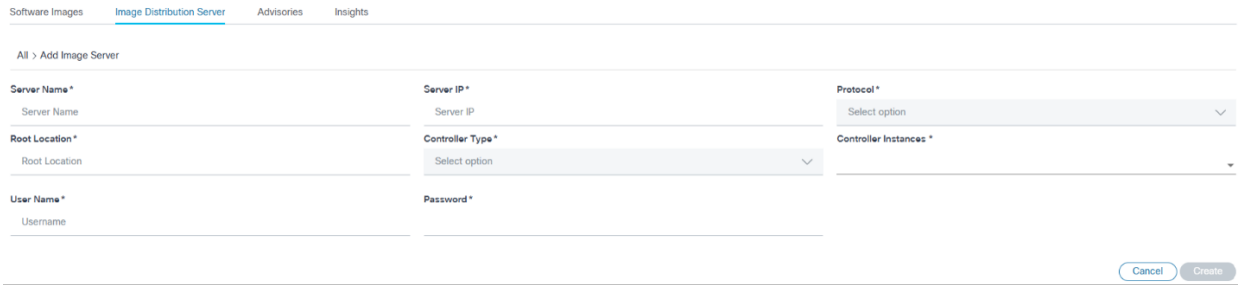
- Se si fa clic su una riga, viene visualizzata la finestra View Image Server

Aggiunta dei dettagli del server di immagini

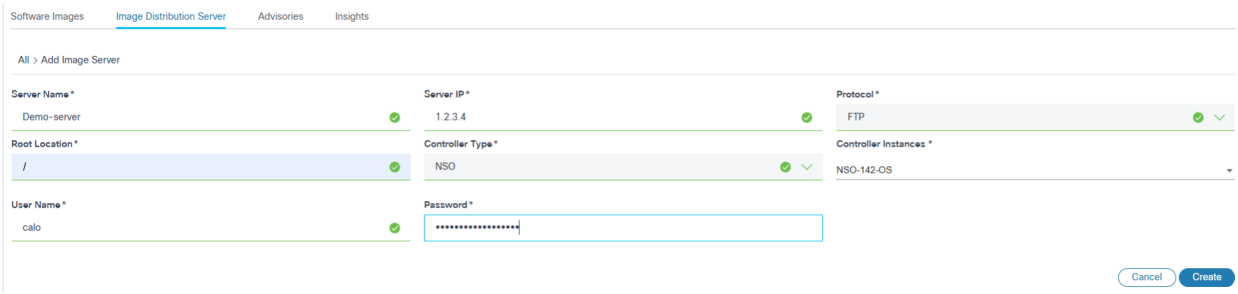


Aggiungi server immagini

4. Selezionare l'icona Altre opzioni > Aggiungi server immagini. Viene visualizzata la pagina Add Image Server.



Aggiungi dettagli server immagini



Aggiungi server immagini con dettagli di esempio

5. Immettere le informazioni nei seguenti campi:

- Nome del server: Nome univoco per il server del repository di immagini
- IP server: Indirizzo IPv4 del server del repository

Nota: Prima di aggiungere, verificare che l'indirizzo IP sia raggiungibile dai dispositivi di rete.

- Protocollo: Supportato dal server del repository immagini per la copia immagine

Nota: Sono supportati solo i protocolli FTP, SCP e SFTP.

- Percorso repository: Percorso di base dei file immagine nel server del repository

Nota: Se i file di immagine sono presenti nella radice della cartella del repository del server di immagini, "/" funziona come un valore.

- Tipo di controller: Tipo di controller a cui è applicabile il server di immagini corrente

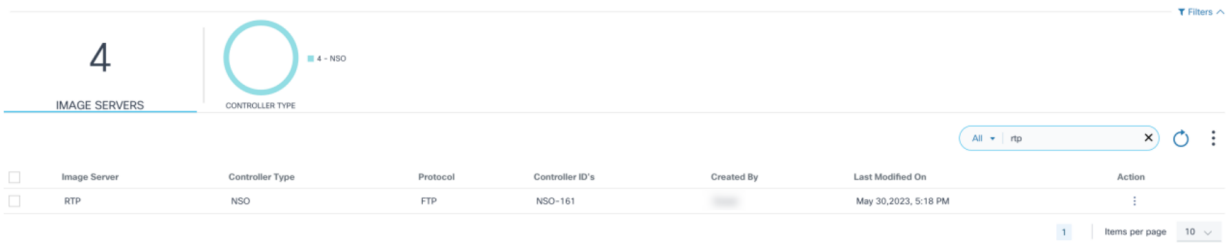
Nota: Sono supportati solo NSO, Direct-To-Device, CNC e ANSIBLE.

- Istanze controller: Una o più istanze di controller applicabili in base ai dispositivi che

gestiscono per i quali utilizzare il server del repository di immagini specificato per copiare l'immagine
- Utente: Credenziali personalizzate da utilizzare per accedere ai file immagine dal repository

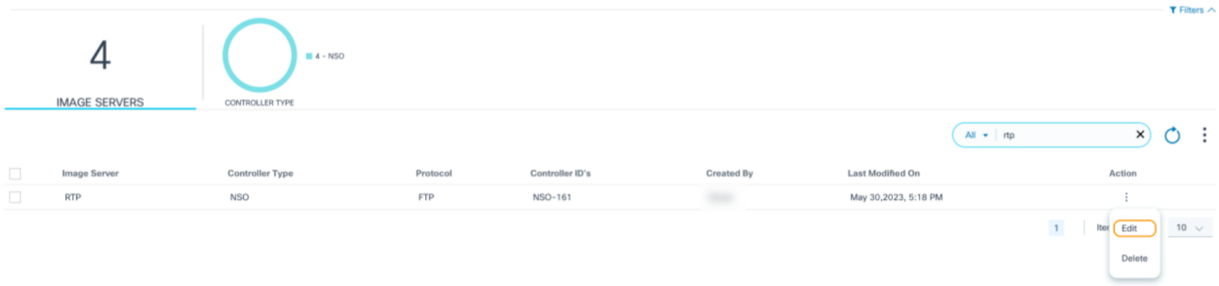
6. Fare clic su Crea. Viene visualizzata la notifica di stato seguita da un messaggio di conferma.

Modifica dei dettagli del server immagini



Ricerca su Image Server

7. Utilizzando il campo Search, individuare il server di distribuzione da aggiornare.

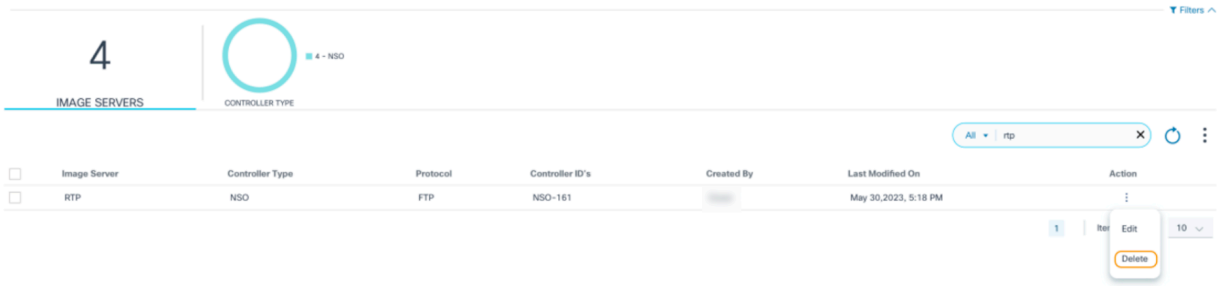


Modifica server immagini

8. Dalla colonna Azione, selezionare l'icona Altre opzioni > Modifica.
9. Aggiornate i parametri richiesti.
10. Fare clic su Save (Salva). Viene visualizzata una notifica di stato seguita da un messaggio di conferma.

Eliminazione dei dettagli del server immagini

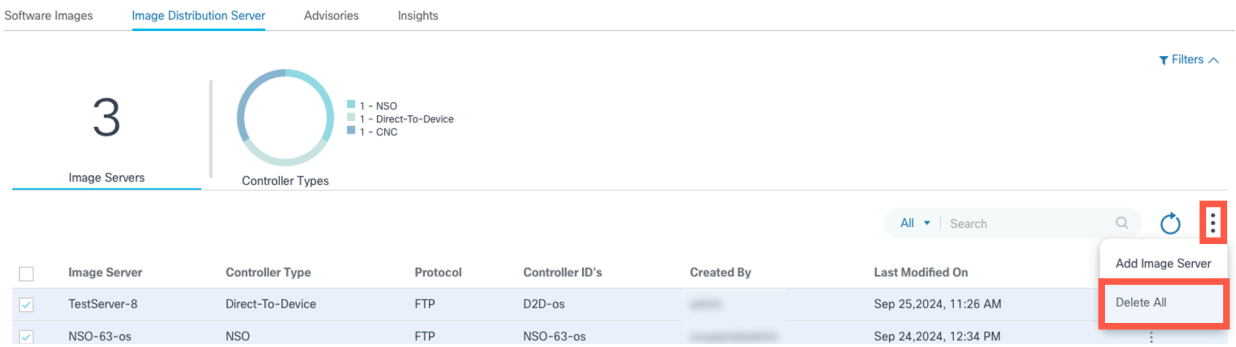
1. Utilizzando il filtro Search, individuare i server desiderati.



Elimina server immagini

2. Dalla colonna Azione, selezionare l'icona Altre opzioni > Elimina per eliminare un singolo server di distribuzione.

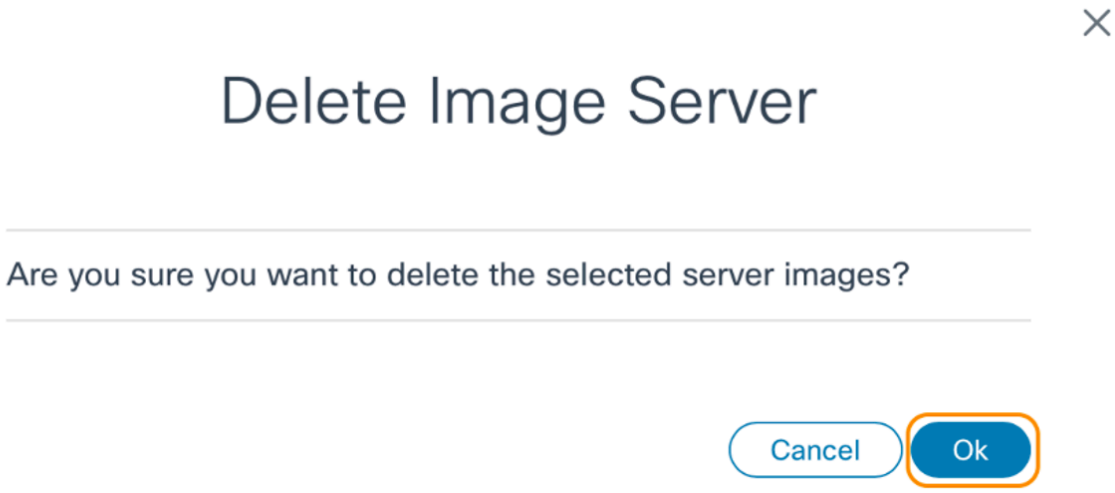
O



Elimina più server di immagini

Selezionare i server desiderati e selezionare l'icona Altre opzioni > Elimina tutto per eliminare più server di distribuzione.

Viene visualizzata una conferma.



Conferma eliminazione

3. Fare clic su OK. Vengono visualizzate notifiche di stato seguite da un messaggio di conferma.

Software Insights

Software Insights individua tutte le vulnerabilità della sicurezza, quali avvertenze sulla sicurezza, bug e fine del ciclo di vita del software esposti dagli asset di rete. Fornisce inoltre suggerimenti software per i modelli di dispositivi gestiti da Cisco Catalyst Center e dai controller NDFC. Consente agli utenti amministratori di selezionare la versione software consigliata per le risorse di rete e crea un criterio di conformità per i modelli di dispositivo, se il suggerimento è disponibile.

Prerequisiti

- Abilitare l'adattatore per informazioni dettagliate. L'adattatore per il server Cisco Insights, denominato "Cisco-Insights-Adapter", è disponibile in modalità OOB. Per l'integrazione con alcuni server Insights esterni, è necessario creare adattatori corrispondenti. Per ulteriori informazioni, fare riferimento a Configuring Insights Adapter nel manuale BPA Developer Guide.
- Per la connessione del sistema BPA al cloud Cisco è necessaria la connettività Internet.
- Verificare che client_id e client_secret siano nella configurazione dell'adattatore prima di procedere con l'operazione di sincronizzazione.
- Se necessario, è possibile configurare il proxy per Internet eseguendo la procedura seguente.
- Per il tipo di sistema operativo IOS-XR, il mapping personalizzato da serie a modello per il dispositivo può essere eseguito in Reference Data Management (RefD) come richiesto. Per ulteriori informazioni sul mapping serie-modello personalizzato, consultare la Guida per gli sviluppatori BPA.
- I BPA Kubernetes Pod richiedono l'accesso a Internet per raccogliere da Cisco le avvertenze, i bug e i dettagli di fine ciclo di vita. Se la rete BPA non ha accesso diretto a Internet, ma è disponibile tramite proxy, utilizzare la procedura seguente per fare in modo che Kubernetes Pods utilizzi il proxy per Internet.

1. Aggiornare lo script con l'indirizzo proxy effettivo anziché <http://proxy-domain.com:port>.
2. Configurare i parametri di ambiente in base a ciascun pod nei grafici YAML o helm di distribuzione.
3. Eseguire lo script seguente nel nodo Kubernetes aggiungendo tutti i nomi di distribuzione nella configurazione NO_PROXY o no_proxy.

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

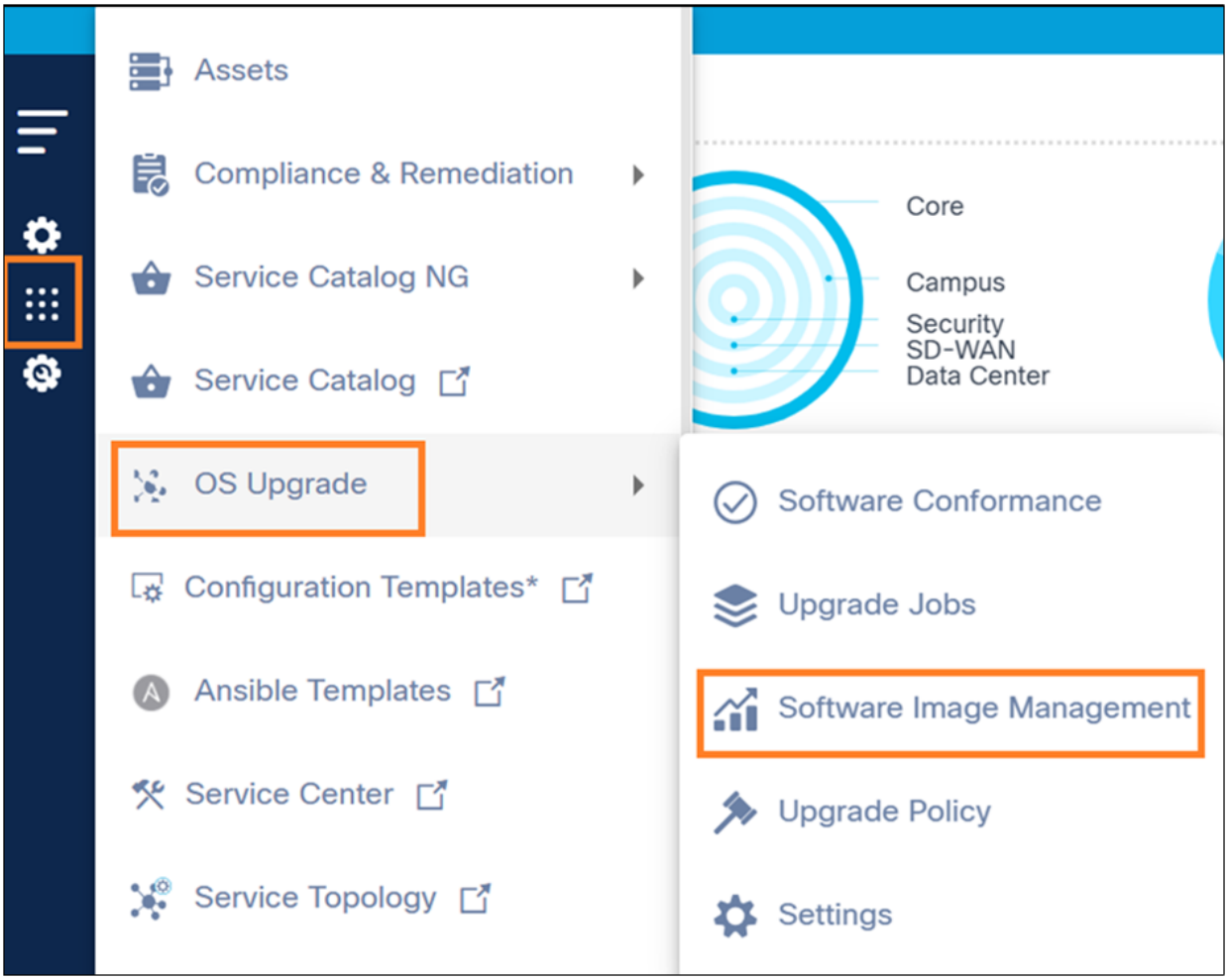
```
     >”
HTTPS_PROXY=”<< http://proxy-domain.com:port>>”
http_proxy=”<



      >”
https_proxy=”<



       >”

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

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

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

Nota: Configurando il proxy come descritto in precedenza, l'Adattatore insights può raggiungere la rete Cisco e scaricare i dati Software Insights richiesti in BPA. Per la connessione diretta a qualsiasi altro server di Insights esterno senza un proxy, assicurarsi di aggiungerli alla variabile no_proxy.

Recupero dei dati di Software Insights in BPA

Per sincronizzare i dati di Software Insights in BPA:

1. Accedere a BPA con le credenziali che hanno accesso ai dati di Sync Software Insights.



Navigazione in Software Image Management

2. Selezionare Aggiornamento sistema operativo > Gestione immagini software dal pannello laterale.

scheda Advisory

3. Fare clic sulla scheda Avvisi.

Sincronizza per recuperare informazioni dettagliate sul software in BPA

Sincronizza per recuperare informazioni dettagliate sul software in BPA

4. Fare clic su Sincronizza.

In questo modo vengono individuati tutti gli avvisi sulla sicurezza, i bug relativi alla priorità, i bollettini di fine ciclo di vita e i suggerimenti software relativi agli asset presenti nell'inventario. Gli avvisi di sicurezza e le date di fine ciclo di vita del software sono determinati in base al tipo di sistema operativo e alla versione del software. I bug relativi alla priorità e i suggerimenti software sono determinati in base all'ID del prodotto e alla versione del software.

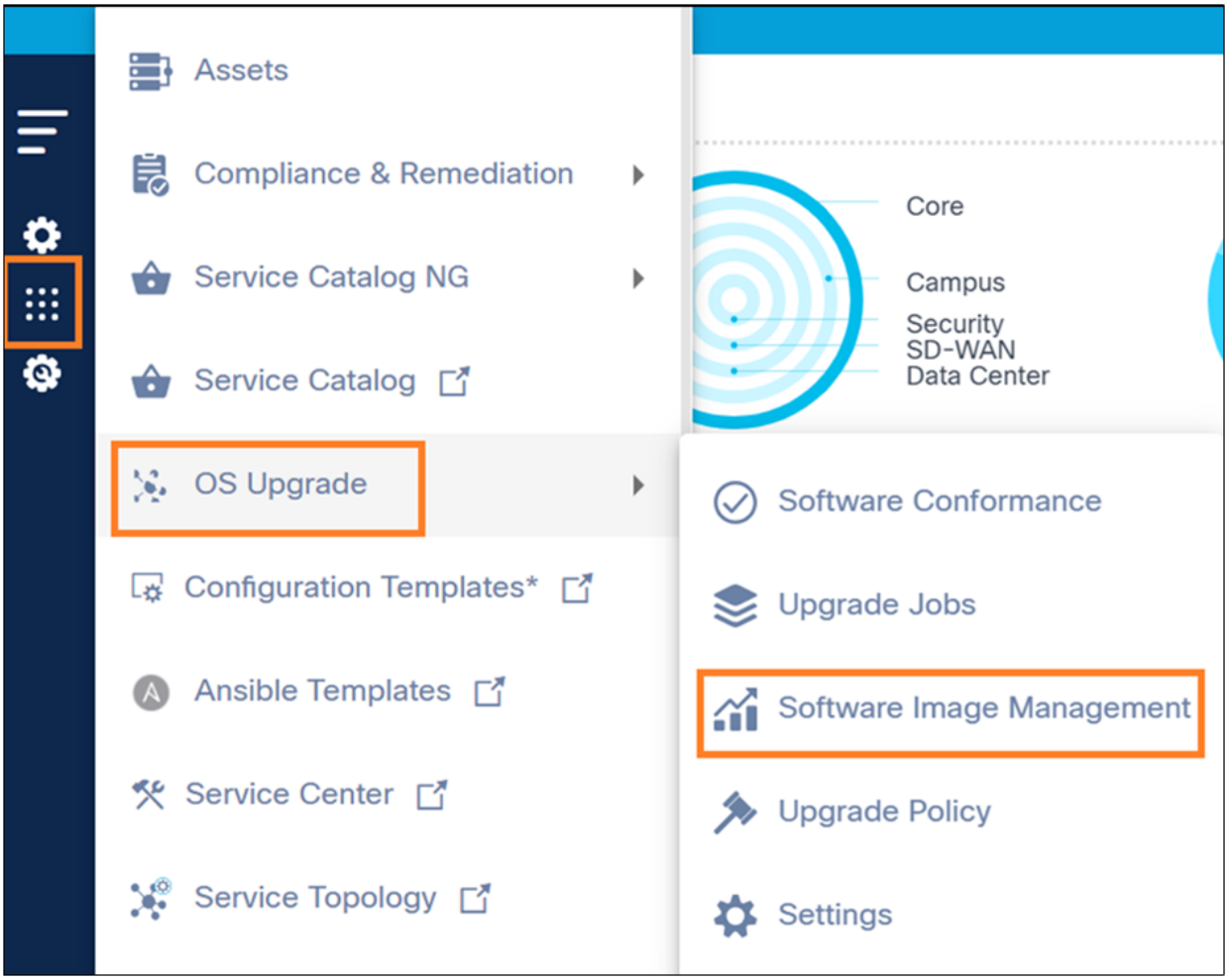
Ultimo aggiornamento mostra la data e l'ora dell'ultima sincronizzazione dei dati di approfondimento e il campo Stato sincronizzazione visualizza lo stato dell'ultima sincronizzazione.

Nota: Tutti gli avvisi, i bug, le note sulla versione e i suggerimenti applicabili vengono recuperati dal cloud Cisco tramite il file "Cisco-Insights-Adapter".

Visualizzazione e gestione degli avvisi di sicurezza

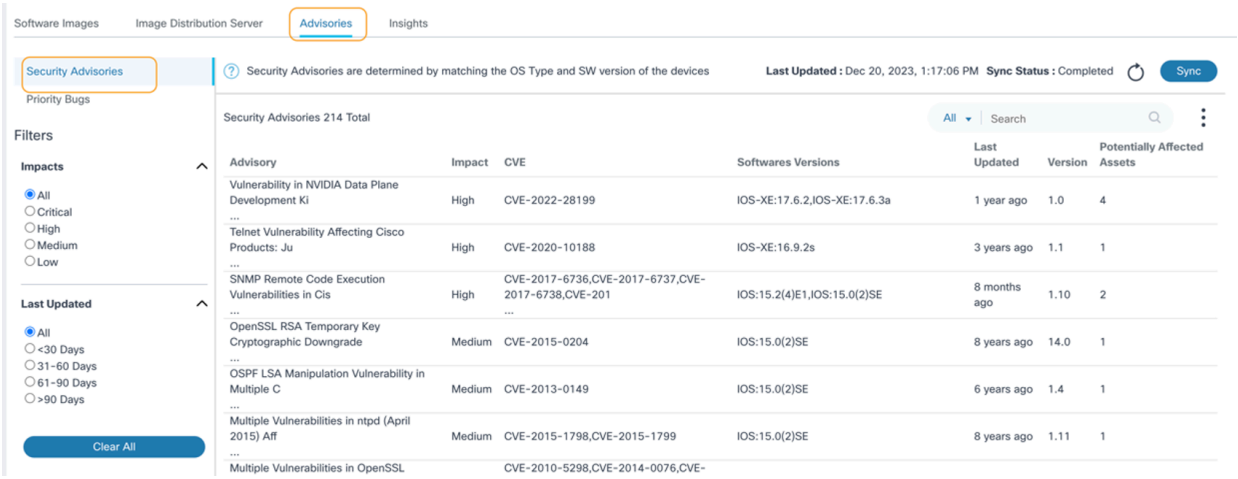
Per accedere alla pagina Advisory:

1. Accedere a BPA con le credenziali che dispongono dell'accesso di gestione agli advisory.



Navigazione in Software Image Management

2. Selezionare Aggiornamento sistema operativo > Gestione immagini software.



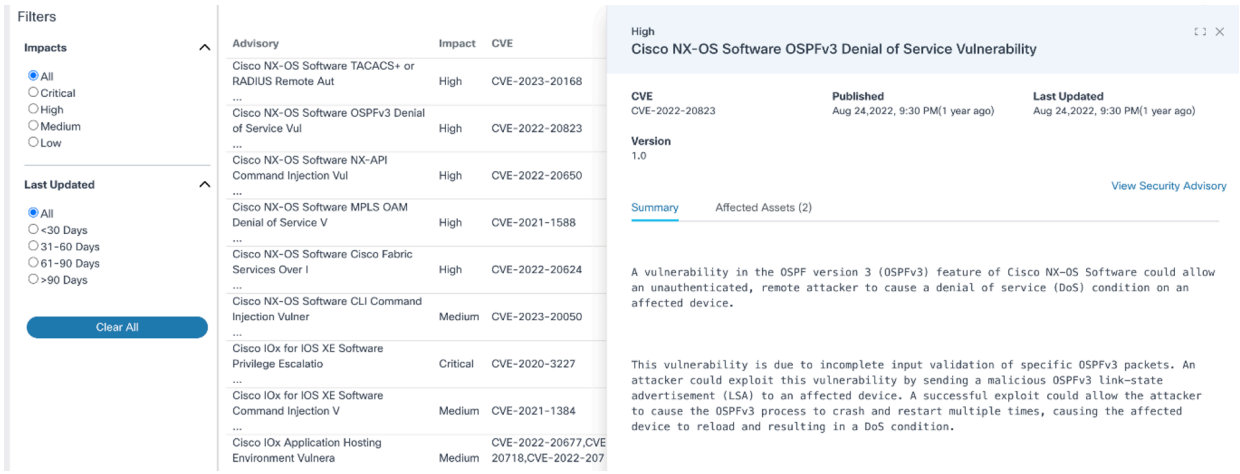
Consulenze sulla sicurezza

3. Fare clic sulla scheda Avvisi. Per impostazione predefinita, viene visualizzata la pagina Consulenze sulla sicurezza.

Per filtrare i dati degli avvisi, vengono visualizzate le opzioni seguenti:

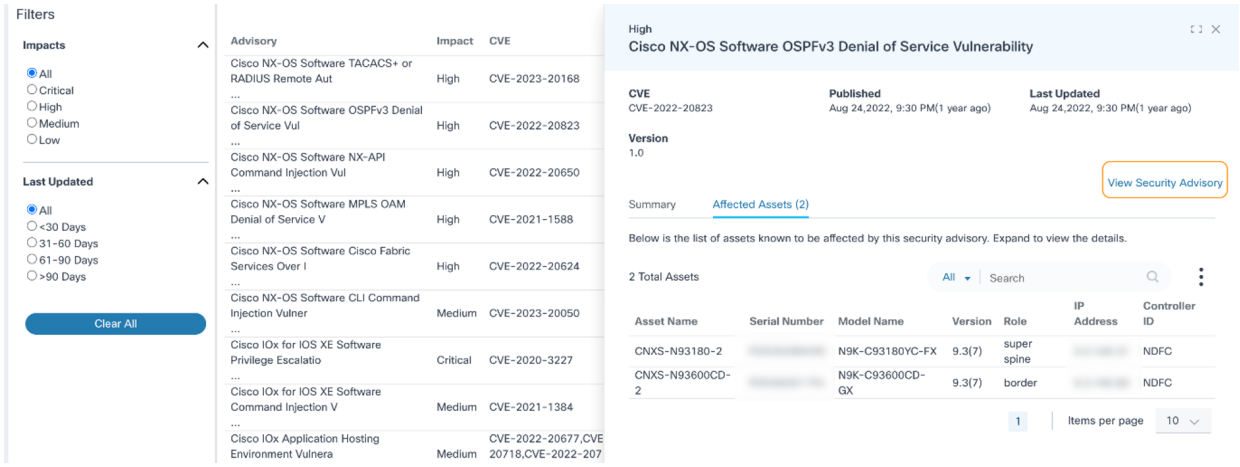
- L'impatto consente il filtraggio in base alla gravità dei consigli. Tutto è selezionato per impostazione predefinita
- Ultimo aggiornamento consente il filtraggio in base alla data dell'ultimo aggiornamento dell'avviso; Tutto è selezionato per impostazione predefinita
- Cancella tutto reimposta i filtri selezionati
- Il filtro di ricerca viene utilizzato per la ricerca degli advisory e include i seguenti filtri di ricerca esclusivi:
- Tutto: Esegue la ricerca in colonne quali Advisory, CVE e versioni software.
- Consulenza: Cerca gli avvisi con i termini specificati nella ricerca
- CVE: Ricerche di consulenze con specifiche vulnerabilità ed esposizioni comuni (CVE)
- Versioni software: Cerca gli avvisi associati a tipi di sistema operativo o versioni software specifici
- L'icona Aggiorna viene utilizzata per aggiornare la pagina e cancellare i filtri selezionati
- Gli advisory esistenti vengono visualizzati con le seguenti colonne:
    - Consulenza: Sintesi dell'avviso
    - Conseguenze: Gravità consulenza
    - CVE CVE assegnate
    - Versioni software: Tipo di sistema operativo e versioni software interessati
    - Ultimo aggiornamento: Data e ora dell'ultimo aggiornamento dell'advisory
    - Version: Versione advisory
    - Asset potenzialmente interessati: Numero di attività che potrebbero essere interessate dall'advisory
- Se si fa clic sul campo dell'intestazione, gli avvisi vengono ordinati

Nota: L'ordinamento non è un'opzione per le risorse potenzialmente interessate.



Visualizzazione dettagli advisory

- Se si seleziona una riga di advisory, viene aperta una vista di dettaglio dell'advisory che include le schede riportate di seguito.
    - Riepilogo: Visualizza un riepilogo dell'avviso selezionato; visualizzazioni predefinite
    - Asset interessati: Visualizza i dettagli degli asset potenzialmente interessati, ad esempio il nome dell'asset, il numero di serie, il nome del modello, la versione del software, l'indirizzo IP e l'ID del controller; in questa scheda è possibile eseguire l'ordinamento e la ricerca delle risorse



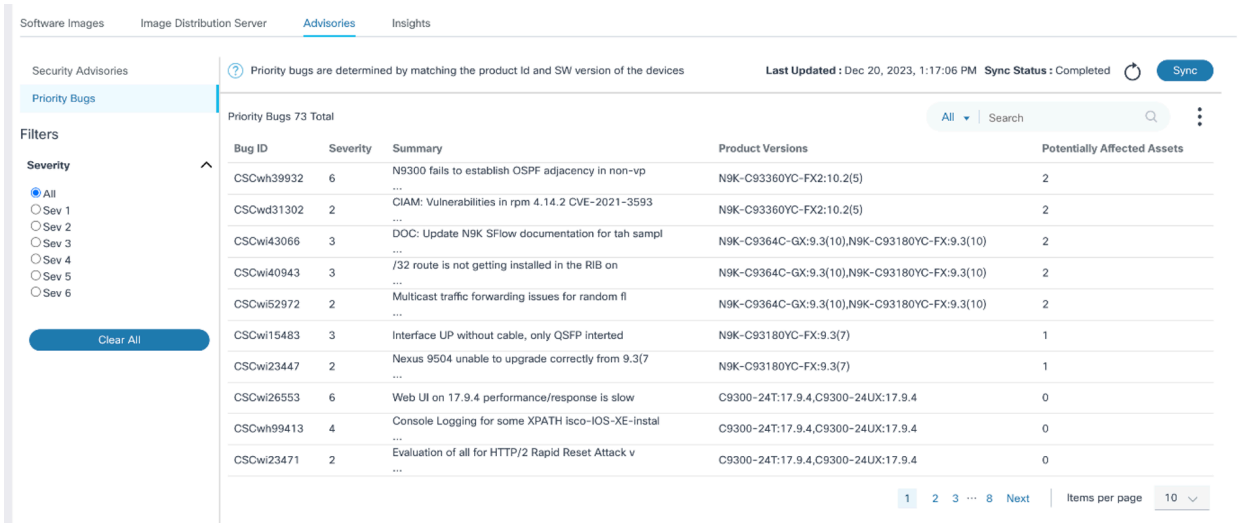
Visualizza Security Advisory

- Collegamento Visualizza Security Advisory: Passa alla pagina Advisory ufficiale

Visualizzazione e gestione dei bug di priorità

Selezione dei bug di priorità

Dopo aver aperto la pagina Advisory come descritto nella sezione precedente, fare clic sulla scheda Priority Bugs (Bug di priorità). Viene visualizzata la pagina Priority Bugs (Bug di priorità).

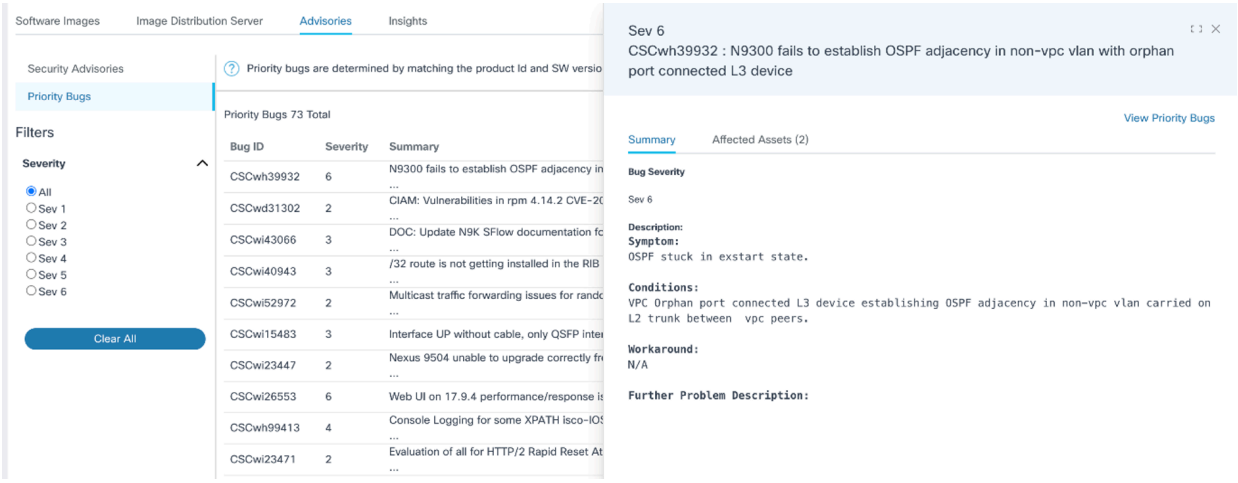


Priorità dei bug

Nella pagina Priorità dei bug sono disponibili le opzioni seguenti:

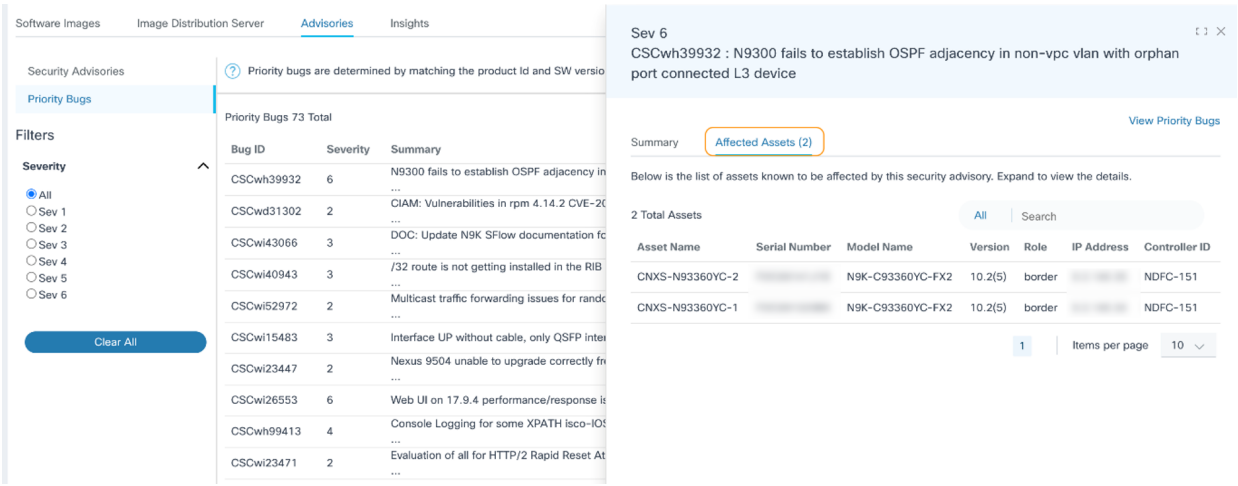
- Un filtro basato sulla gravità che consente di filtrare il bug in base alla gravità; Tutto è selezionato per impostazione predefinita
- Il filtro Search può essere usato per cercare i bug e include i seguenti filtri di ricerca esclusivi:
    - Tutto: Esegue la ricerca in tutti i campi
    - ID bug Cerca i bug con l'ID specificato
    - Riepilogo: Cerca i bug con parole chiave specifiche presenti nel riepilogo
    - Versioni prodotto: Cerca i bug associati a un ID prodotto o a una versione software specifica
- L'icona Aggiorna può essere utilizzata per aggiornare la pagina e cancellare i filtri selezionati
- I bug di priorità vengono visualizzati nella tabella con le seguenti colonne:
    - ID bug
    - Gravità: Gravità del bug
    - Riepilogo: Riepilogo dei dettagli del bug
    - Versioni prodotto: Versioni software e ID prodotto interessate
    - Asset potenzialmente interessati: Numero di risorse che potrebbero essere interessate dal bug

- L'ordinamento può essere eseguito facendo clic su qualsiasi intestazione di colonna, ad eccezione delle risorse potenzialmente interessate



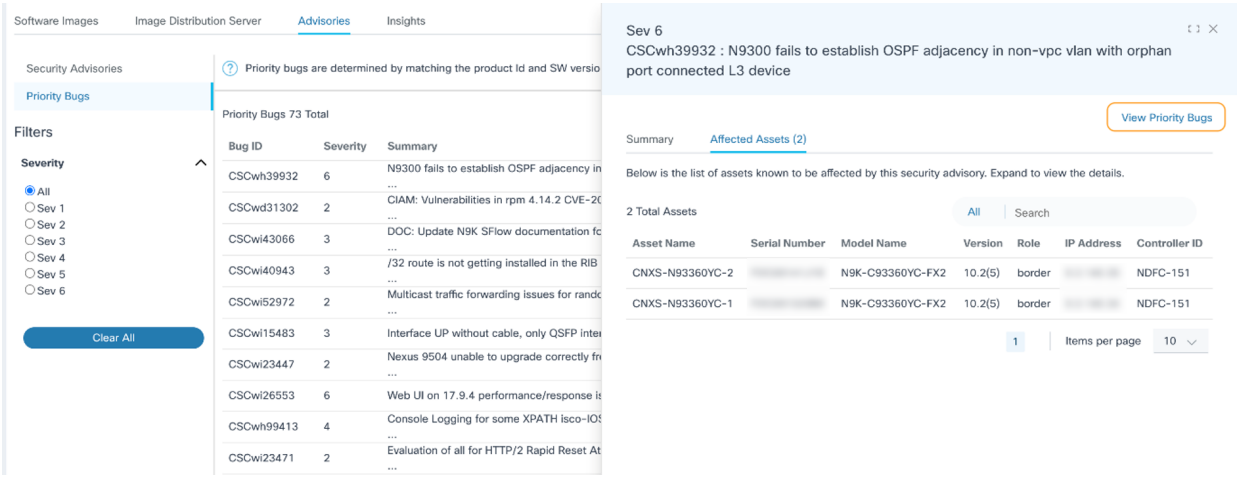
Visualizzazione dei dettagli dei bug

- Se si fa clic su un bug, viene aperta la visualizzazione dettagliata del bug che include quanto segue:
    - Scheda Riepilogo: Visualizza i dettagli sulla gravità, la descrizione e la soluzione alternativa del bug



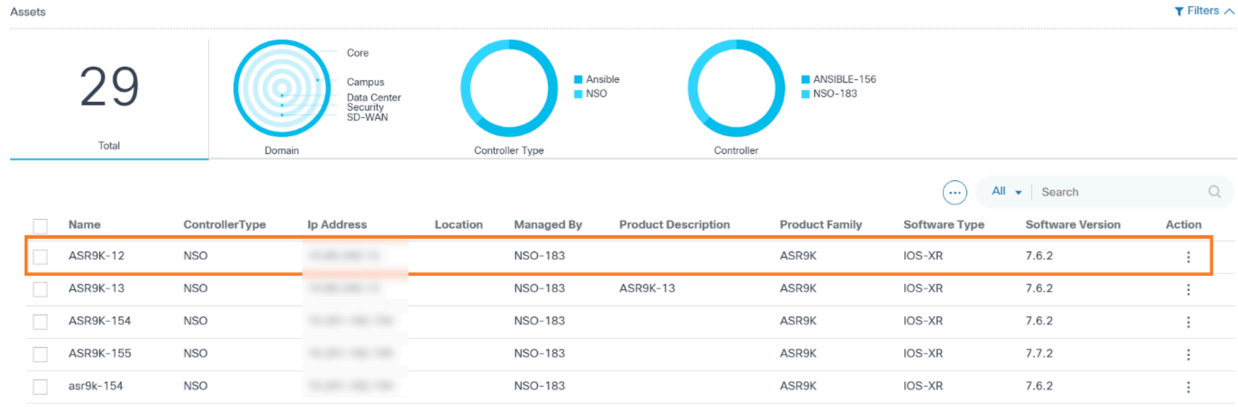
Scheda Cespiti interessati

- Scheda Asset interessati: Visualizza tutti i dettagli sugli asset potenzialmente interessati, ad esempio il nome dell'asset, il numero di serie, il nome del modello, la versione del software, l'indirizzo IP e l'ID del controller; in questa scheda è possibile eseguire l'ordinamento e la ricerca delle risorse



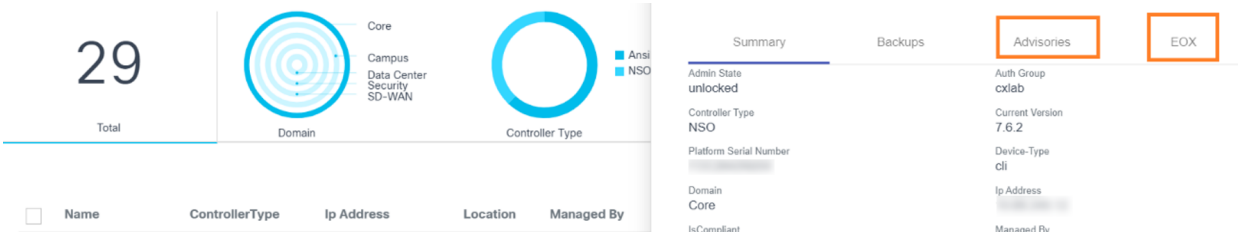
Visualizzazione dei bug di priorità

- Collegamento View Priority Bugs: Passa al Bug Search Tool ufficiale



Attivo

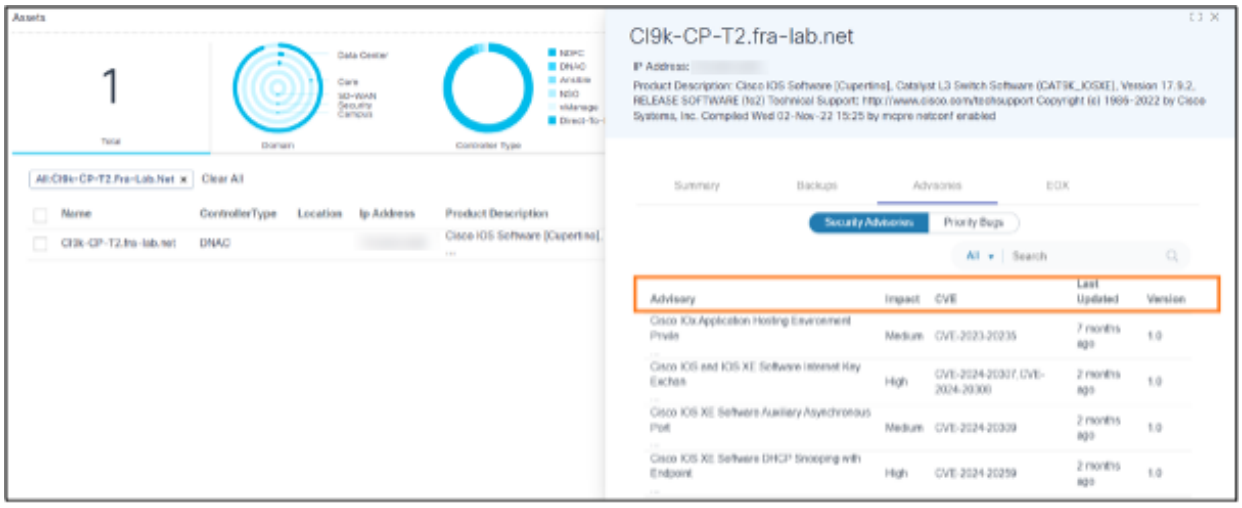
In Asset Manager, gli utenti possono visualizzare un elenco di tutte le risorse. Quando si seleziona una risorsa, in un pannello vengono visualizzate le informazioni a livello di risorsa, che includono i dettagli sulla vulnerabilità del software delle risorse organizzati in due schede: Consulenze ed EOX.



Consigli ed EOX

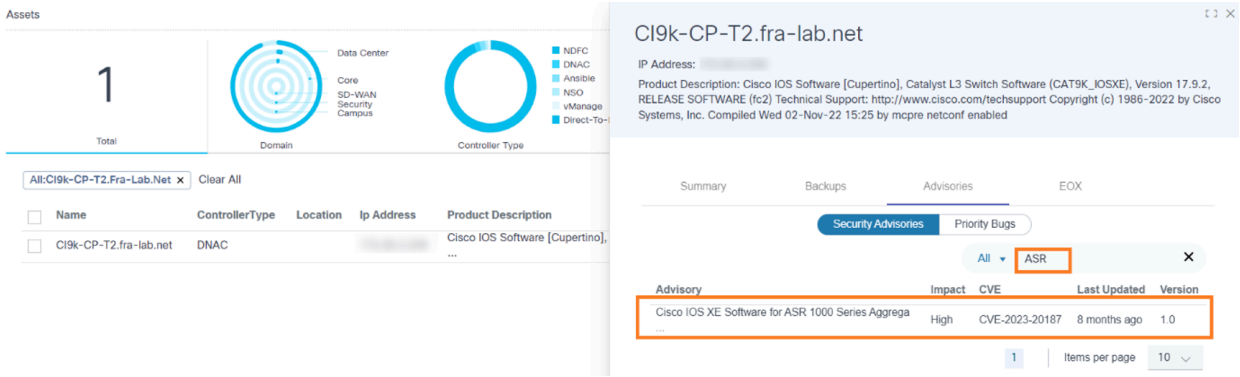
La scheda Advisory contiene due schede secondarie, Security Advisories e Priority Bugs. Per ulteriori informazioni su queste schede, vedere le sezioni seguenti.

Consulenze sulla sicurezza

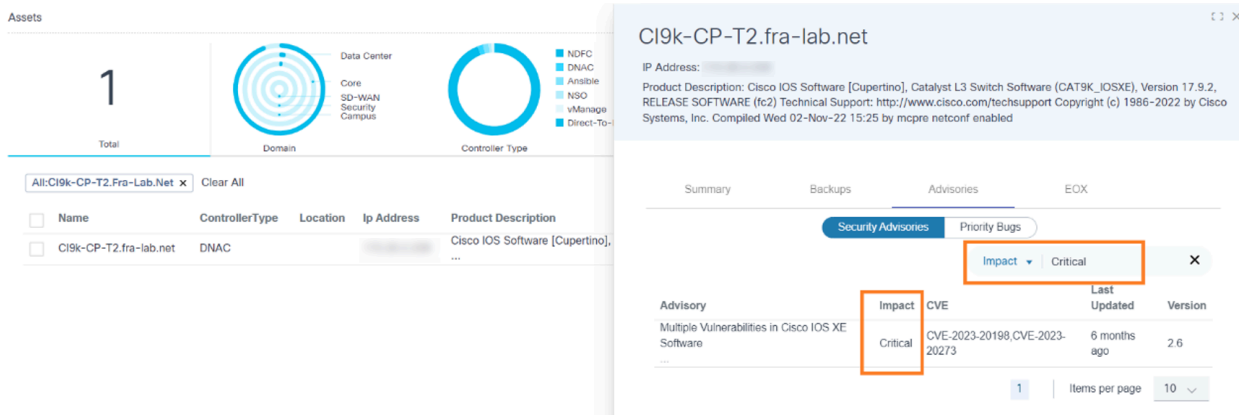


Consulenze sulla sicurezza della risorsa selezionata

Nella scheda secondaria Consigli di sicurezza, gli utenti possono visualizzare tutti gli avvisi di sicurezza che hanno un impatto su una risorsa selezionata. Le colonne della tabella degli avvisi di sicurezza includono Avvisi, Impatto, CVE, Ultimo aggiornamento e Versione.



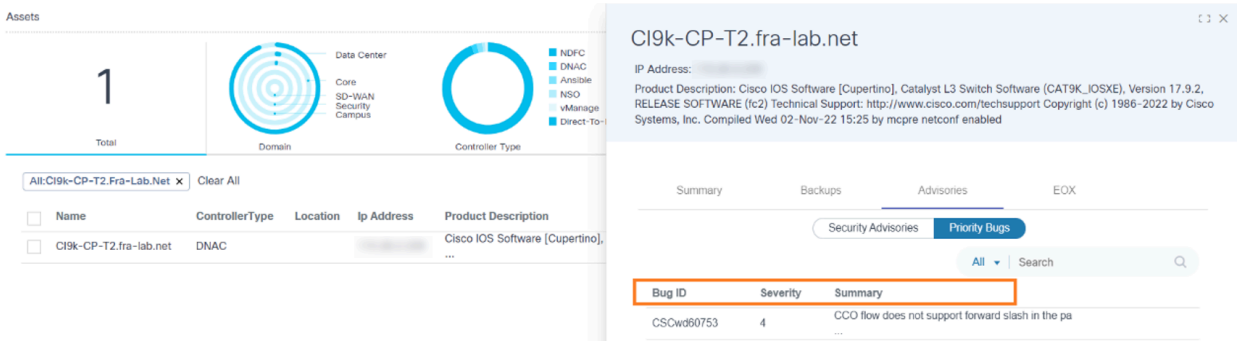
Ricerca consigli sulla sicurezza



Ricerca consigli sicurezza - opzione impatto

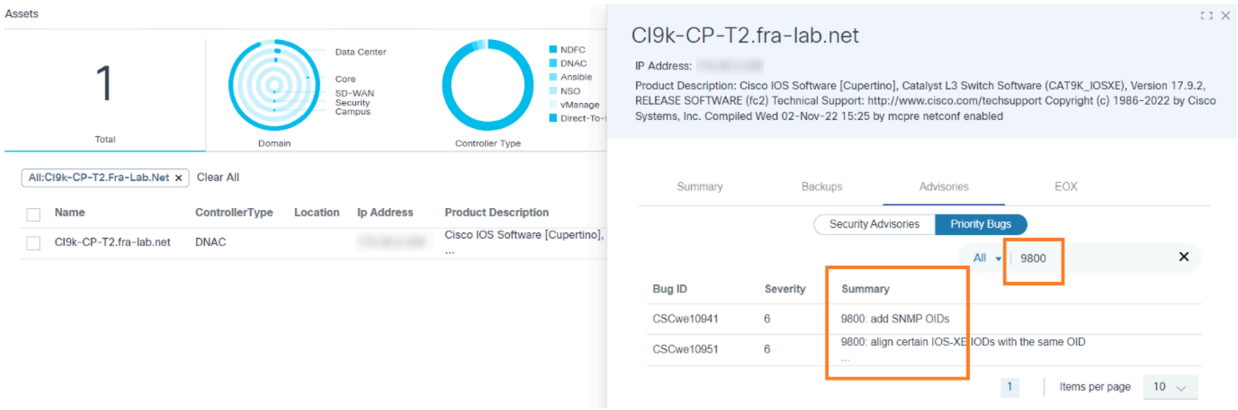
Gli utenti possono cercare gli avvisi in base ai valori delle colonne Avvisi, Impatto, CVE, Ultimo aggiornamento e Versione. L'impaginazione consente agli utenti di spostarsi tra le pagine.

Priorità dei bug

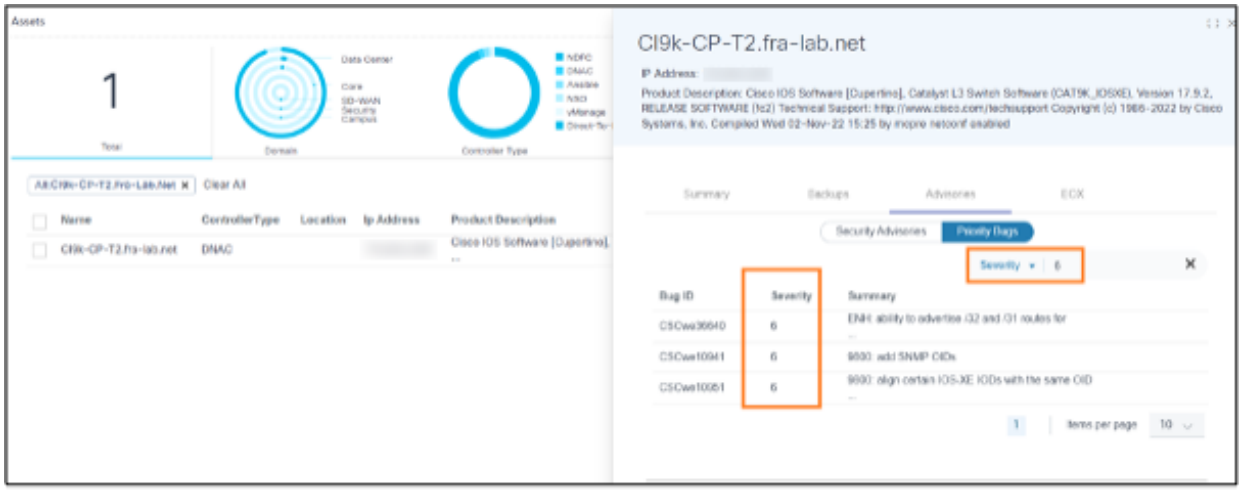


Bug di priorità che influiscono su una risorsa selezionata

Nella scheda secondaria Bug di priorità, gli utenti possono accedere a tutti i bug di priorità che interessano una determinata risorsa. Le colonne della scheda includono ID bug, Gravità e Riepilogo.



Priorità e bug - Ricerca per riepilogo



Priorità nella ricerca dei bug in base alla gravità

Gli utenti possono cercare i bug prioritari in base ai valori specificati nelle colonne ID bug, Gravità e Riepilogo. L'impaginazione facilita lo spostamento tra le pagine.

EOX

Scheda EOX

La scheda EOX visualizza i dati di fine ciclo di vita del software specifici per un asset, incluse tre date importanti:

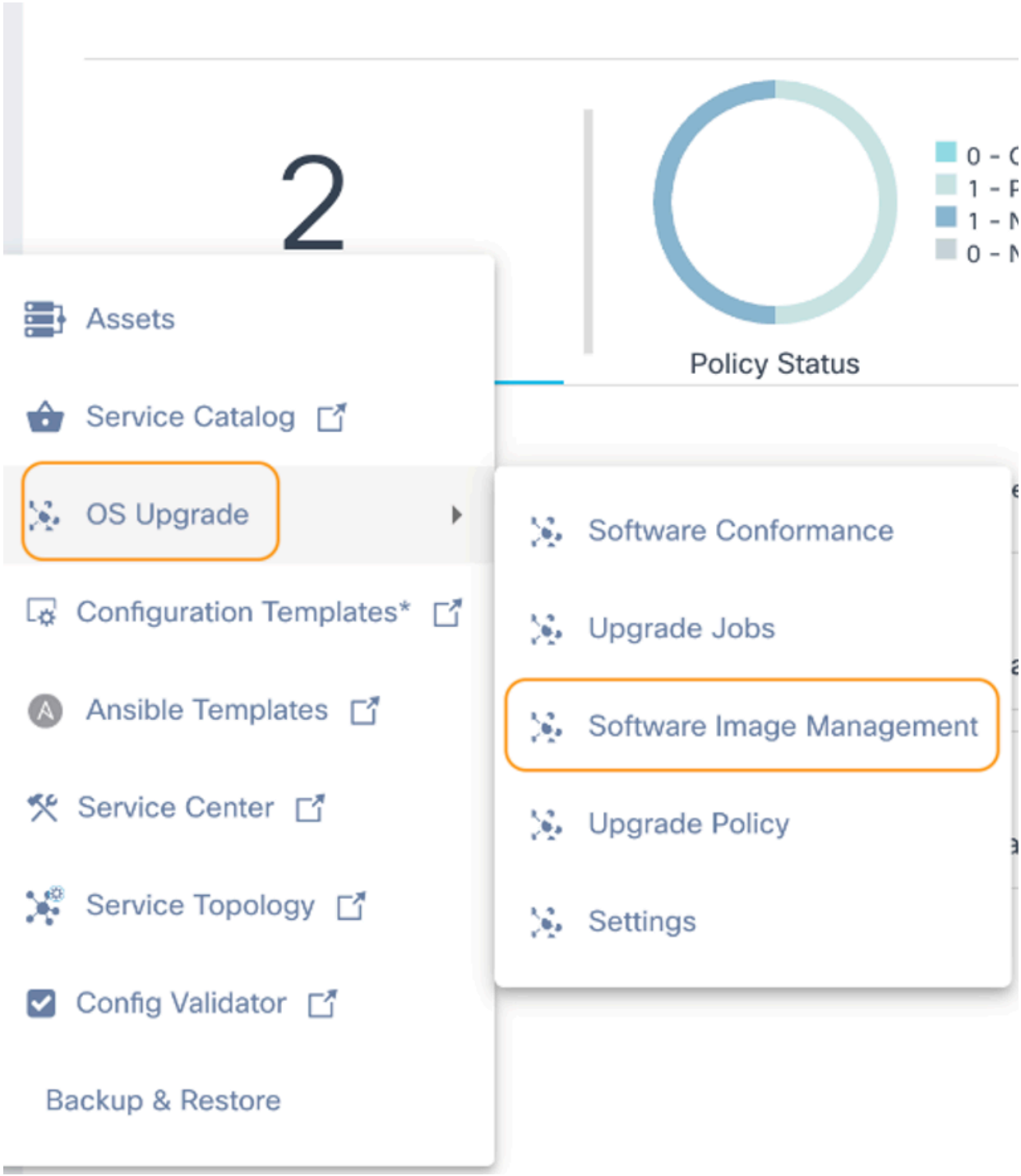
- Fine manutenzione software
- Fine supporto sicurezza
- Ultima data di supporto

Visualizzazione di Software Insights

Software Insights offre suggerimenti software per i modelli di dispositivi gestiti da Cisco Catalyst Center e dai controller NDFC, consentendo agli utenti amministratori di creare un criterio di conformità per i modelli di dispositivi, se il suggerimento è disponibile.

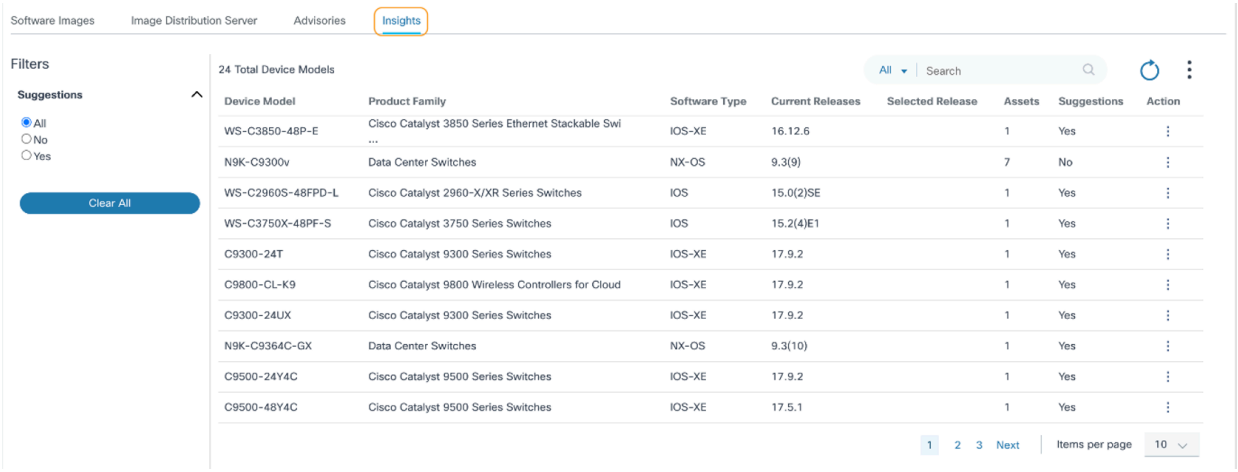
Per accedere a Software Insights:

1. Accedere a BPA con le credenziali che hanno gestito l'accesso a Insights.



Gestione delle immagini software

2. Selezionare Aggiornamento sistema operativo > Gestione immagini software dal pannello laterale.



Scheda Informazioni approfondite

3. Fare clic sulla scheda Informazioni approfondite.

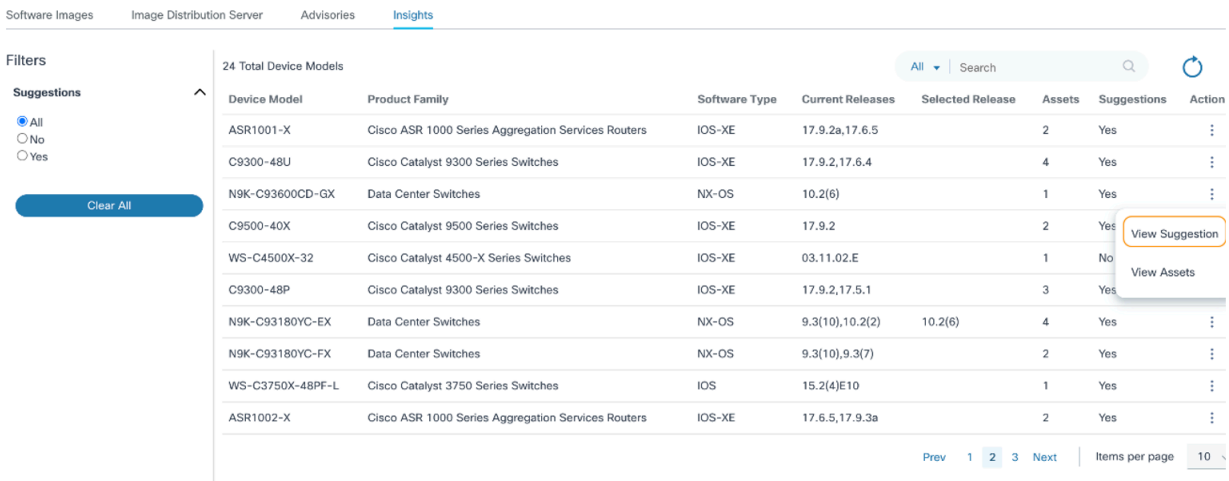
La scheda Informazioni approfondite contiene le informazioni riportate di seguito.

- Filtro che consente agli utenti di filtrare i dati in base ai suggerimenti. Per impostazione predefinita è selezionato Tutto.
    - Sì filtra i dati per i modelli di dispositivo con suggerimenti
    - No filtra i dati per i modelli di dispositivo senza suggerimenti

Esporta in CSV

- L'icona Altre opzioni fornisce un'opzione Esporta in CSV per esportare i dati visualizzati nella pagina
    - L'icona Aggiorna aggiorna la pagina e cancella i filtri selezionati
    - Il filtro di ricerca viene utilizzato per la ricerca dei dati e include i seguenti filtri di ricerca esclusivi:
- Tutto: Esegue la ricerca in tutte le colonne (ad esempio, Modello dispositivo, Famiglia di prodotti e Tipo di software)
- Modello dispositivo: Cerca i dati con un nome di modello di dispositivo specifico
- Famiglia di prodotti Cerca i dati con il nome della famiglia di prodotti specifica
- Tipo di software: Cerca i dati con un nome di tipo di software specifico

- I modelli di dispositivo esistenti sono visualizzati con le seguenti colonne:
- Modello dispositivo: Nome del modello di dispositivo
- Famiglia di prodotti: Nome della famiglia di prodotti a cui appartiene il modello di dispositivo
- Tipo di software: Nome del tipo di software a cui appartiene il modello di dispositivo
- Versioni correnti: Elenco delle versioni software univoche attualmente presenti nell'inventario per il modello di dispositivo
- Versione selezionata: Versione suggerita che è stata selezionata come versione opzionale tra i suggerimenti forniti da Cisco
- Risorse: Numero di asset presenti in Asset Manager per il modello di dispositivo
- Suggerimenti: Visualizza Sì o No per i suggerimenti disponibili per il modello di dispositivo

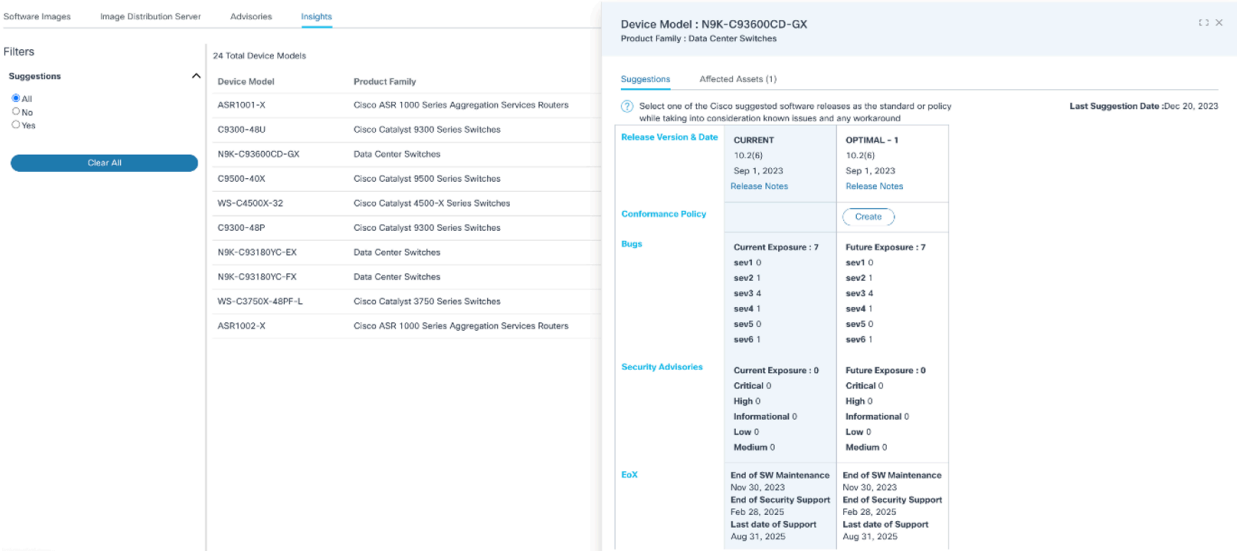


Navigazione suggerimenti visualizzazione

- Azione: Fornisce azioni specifiche per le righe tramite l'icona Altre opzioni (ad esempio, Visualizza suggerimenti e Visualizza risorse)

Nota: Visualizza suggerimenti è disabilitato se il modello di dispositivo non dispone di suggerimenti.

Visualizzazione e scelta delle versioni software suggerite dal fornitore



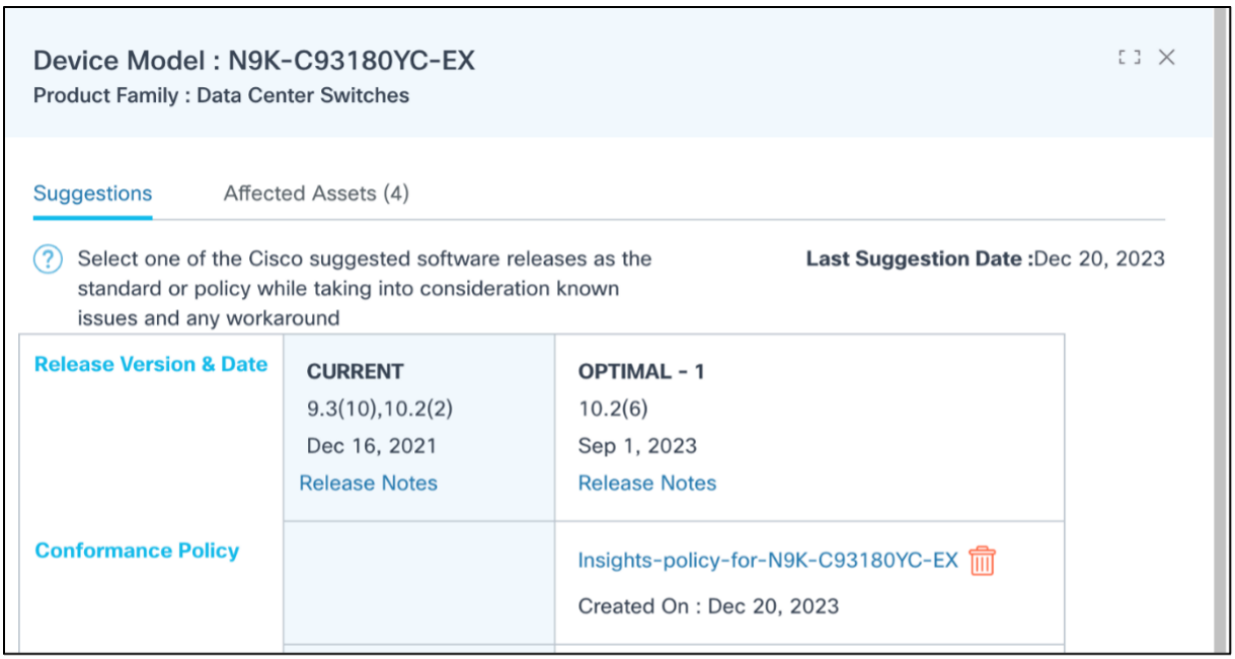
scheda Suggerimenti

Selezionando l'icona Altre opzioni > Visualizza suggerimenti dalla colonna Azione viene visualizzato un pannello laterale con tutti i dettagli di dettaglio. La scheda Suggerimenti contiene i dettagli correnti e consigliati della versione per il modello di dispositivo selezionato; un modello di dispositivo può avere più di un suggerimento. Sono disponibili i seguenti dati:

- Versione e data di rilascio: Versioni, data e note vengono visualizzati i dettagli delle versioni correnti e consigliate, se disponibili nel cloud Cisco; se i cespiti del magazzino appartengono a più versioni, tutte le versioni applicabili vengono visualizzate come valori separati da virgola nella colonna Corrente
- Crea criterio di conformità: Consente agli amministratori di creare un criterio di conformità per una versione specifica con il ruolo di dispositivo Qualsiasi

---

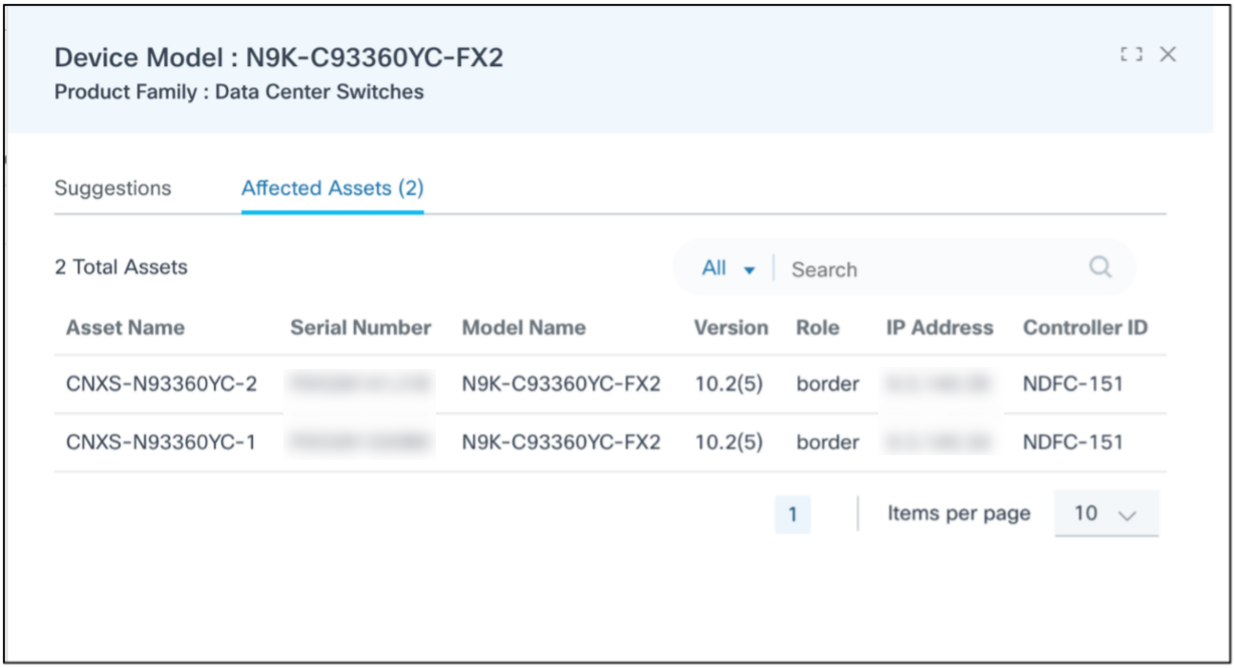
Nota: La creazione di criteri di conformità è supportata solo per i modelli di dispositivi controller NDFC



Opzione Elimina criterio

Nota: Se esistono già criteri per il modello di dispositivo, viene visualizzato un errore. Se non esiste alcun criterio, viene creato un criterio con lo stato Abilitato. Se un criterio viene creato da Insights, gli utenti hanno la possibilità di eliminarlo.

- Bug: Visualizza il numero consolidato di bug di ciascuna release
- Consulenze sulla sicurezza: Visualizza un conteggio di advisory consolidato per ciascuna release
- EoX: Visualizza la fine della manutenzione del software, la fine del supporto di sicurezza e l'ultima data di supporto per ciascuna release



Scheda Cespiti interessati

Se si seleziona l'icona Altre opzioni > Visualizza cespiti dalla colonna Azione, viene visualizzato un pannello laterale in cui per impostazione predefinita viene visualizzata la scheda Cespiti interessati. La scheda Asset interessati mostra i dettagli degli asset potenzialmente interessati in colonne quali Nome asset, Numero di serie, Nome modello, Versione software, Indirizzo IP e ID controller. In questa scheda è possibile eseguire l'ordinamento e la ricerca delle risorse.

Identificazione dei dispositivi che richiedono un aggiornamento software

Per ulteriori informazioni, fare riferimento a Conformità software.

Conformità software

La conformità software consente di identificare gli asset di una rete non conformi alla versione del software di destinazione prevista. La convalida è basata su regole e criteri in base ai quali vengono definiti gli intenti di conformità software. Queste regole possono essere eseguite su base programmata o su richiesta. Una volta eseguita correttamente la regola di conformità, viene ottenuto il risultato che fornisce lo stato delle risorse applicabili. L'ambito di conformità dipende da diversi criteri, ad esempio il ruolo del dispositivo, la gestione dell'istanza del controller e così via.

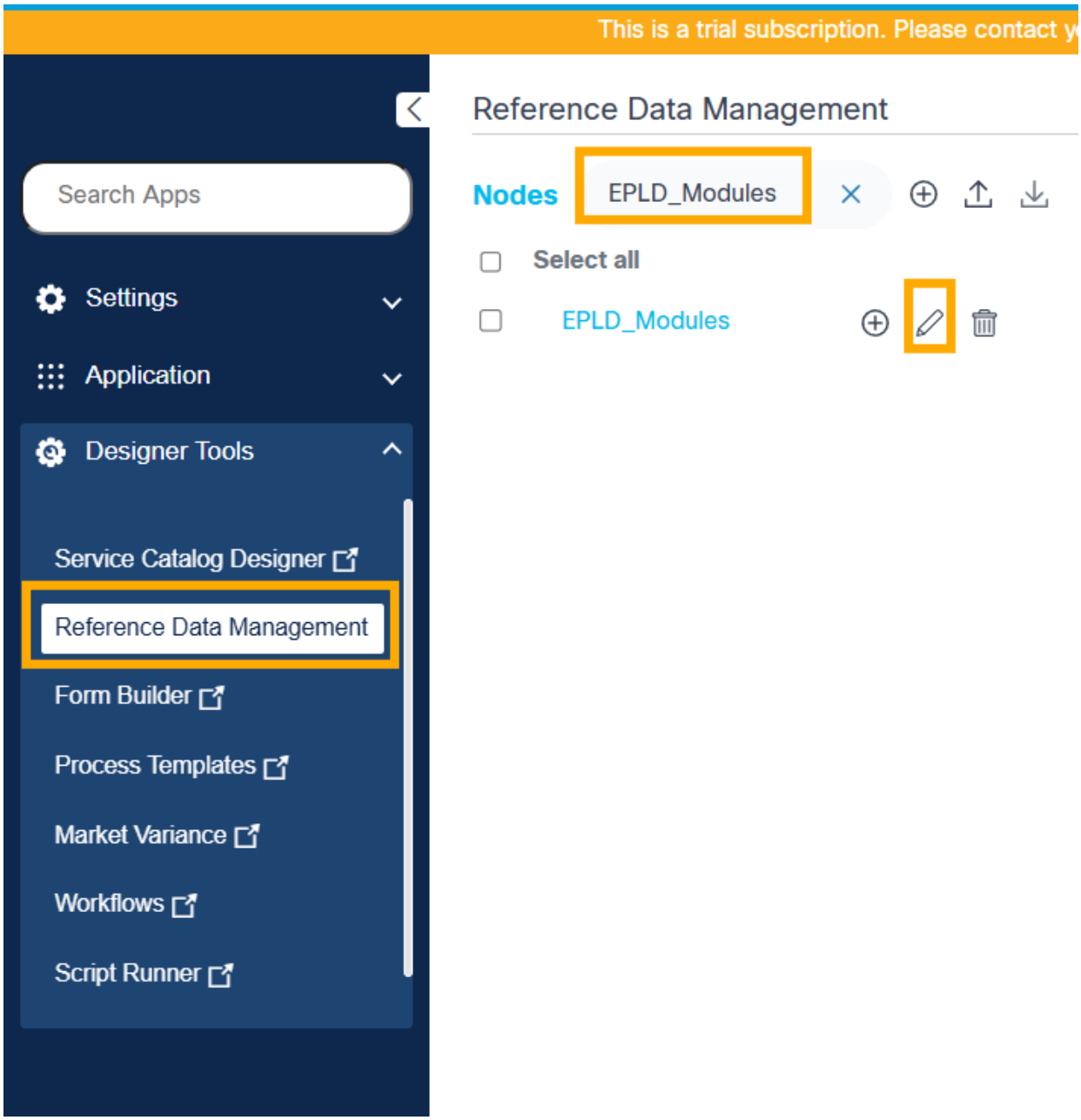
Prerequisiti

- Le immagini software di controller come Cisco Catalyst Center, vManage, NDFC e FMC devono essere sincronizzate. Per ulteriori informazioni, fare riferimento a Sincronizzazione dei metadati delle immagini software.
- È necessario aggiungere i metadati dell'immagine software necessari per controller quali NSO, CNC, Direct-to-Device e ANSIBLE. per ulteriori informazioni, fare riferimento a Aggiunta di metadati dell'immagine software.
- Gli utenti devono avere accesso all'applicazione RefD per gestire i dati del modulo EPLD.
- Le informazioni del modulo EPLD per le release richieste devono essere precompilate nell'applicazione RefD
- Gli utenti devono aggiungere manualmente le informazioni del modulo EPLD nell'applicazione RefD se non è disponibile OOB

Creazione dei dati del modulo EPLD nell'applicazione di gestione dei dati di riferimento

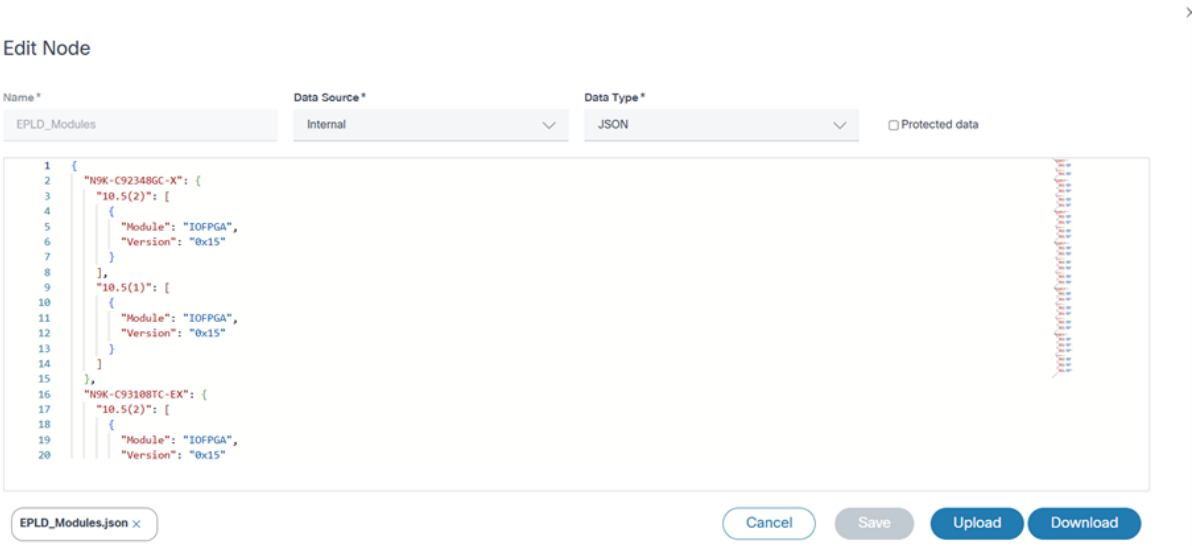
Prima di creare un criterio di conformità, creare i dati di riferimento del modulo EPLD nell'applicazione RefD. L'applicazione RefD include le informazioni del modulo EPLD per le versioni software Nexus rispettivamente v10.2(8) e v10.4(5). Per le altre versioni di dispositivi, le informazioni sul modello EPLD devono essere aggiunte manualmente nell'applicazione RefD.

Per aggiungere altre release ai metadati del modulo EPLD, completare le seguenti operazioni:



Gestione dei dati di riferimento

1. Passare all'applicazione Gestione dati di riferimento e cercare "EPLD_Modules".
2. Selezionare il file "EPLD_Modules" e l'icona Modifica.



Modifica nodo

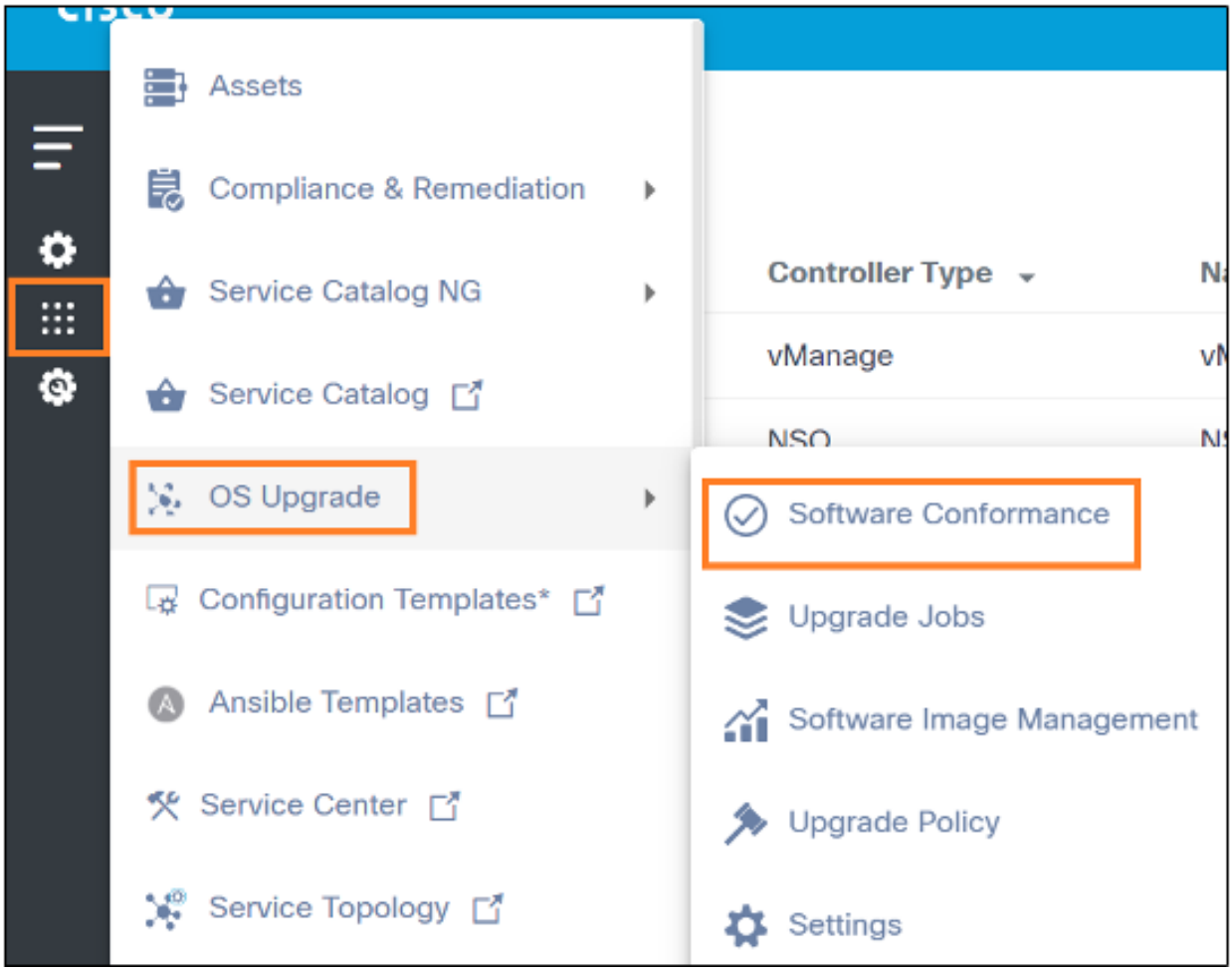
3. Aggiungere i metadati del modulo EPLD della nuova release aggiungendo una nuova voce con la struttura seguente:

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

4. Fare clic su Salva e convalidare i nuovi metadati del modulo EPLD disponibili per la selezione nei criteri di conformità. I dati EPLD per le versioni supportate vengono precompilati.

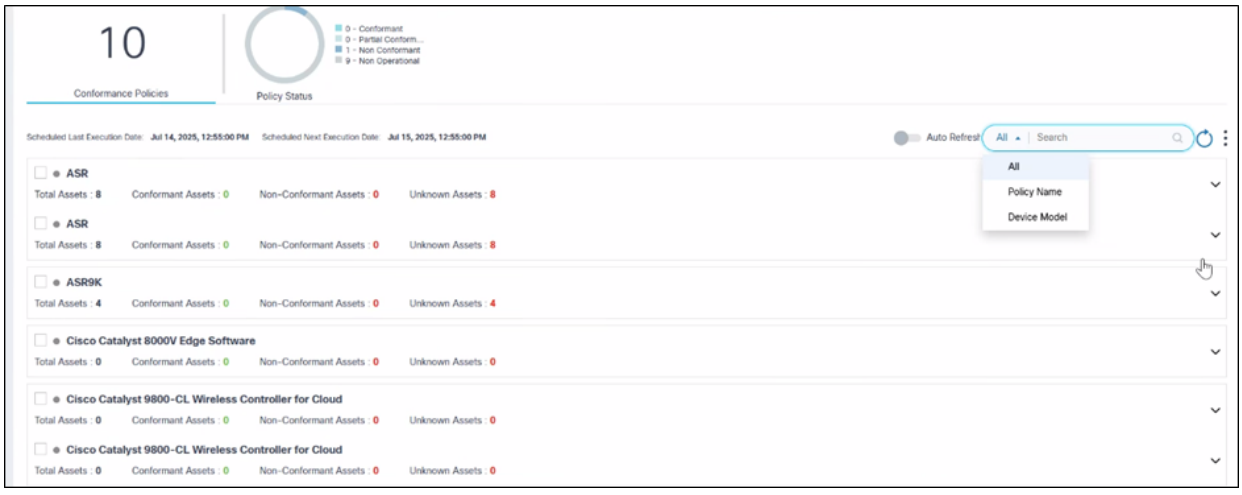
Visualizzazione e gestione della conformità software

1. Accedere a BPA con le credenziali che hanno accesso a Software Conformance.



Navigazione per la conformità software

2. Selezionare Aggiornamento sistema operativo > Conformità software. Viene visualizzata la pagina Software conforme.



Conformità software

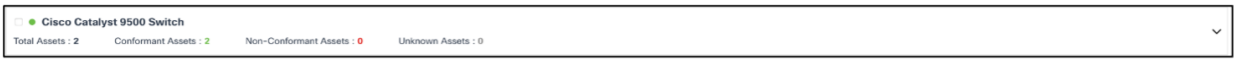
La pagina Software conforme contiene le informazioni riportate di seguito.

- Una sezione di analisi, visualizzata nella parte superiore, che fornisce le informazioni

riportate di seguito.

- Numero totale di criteri di conformità esistenti nel sistema
- Un filtro rapido Stato criteri da filtrare in base ai criteri seguenti:
    - Conforme: Tutti i dispositivi gestiti da BPA con un modello specifico si trovano nella versione software definita
    - Conforme parziale: Alcuni dispositivi gestiti da BPA con un modello specifico si trovano nella versione software definita; i dispositivi rimanenti sono in versioni software diverse
    - Non conforme: Tutti i dispositivi gestiti da BPA con un modello specifico si trovano su versioni software diverse rispetto a una determinata versione software
    - Non operativo: Impossibile trovare dispositivi applicabili in base al modello di dispositivo specificato nel criterio
- Data ultima esecuzione programmata e Data esecuzione successiva programmata che indicano la data e l'ora dei controlli di conformità programmati eseguiti in precedenza e quando il successivo controllo di conformità programmato è per tutti i criteri
- Campo di ricerca utilizzato per filtrare i criteri in base al modello di dispositivo, al nome del criterio o a tutti. Gli utenti possono selezionare Tutto per eseguire la ricerca in tutti i parametri
- L'opzione Aggiornamento automatico consente di aggiornare automaticamente il criterio di conformità In corso a intervalli definiti dall'utente quando è attivata. Per attivare l'interruttore:
    - Selezionare Aggiornamento sistema operativo > Impostazioni per modificare l'intervallo di aggiornamento
    - Modificare l'intervallo di aggiornamento automatico con il valore desiderato
    - Fare clic su Salva.
- Il dashboard dei criteri di conformità software viene aggiornato in base al nuovo intervallo quando è attivato l'interruttore Aggiornamento automatico
- Un'icona Aggiorna per aggiornare la pagina e cancellare i filtri selezionati
- Un'icona Altre opzioni che fornisce le seguenti opzioni:
    - Creare un criterio
    - Esegui tutti i criteri
    - Elimina più criteri selezionati

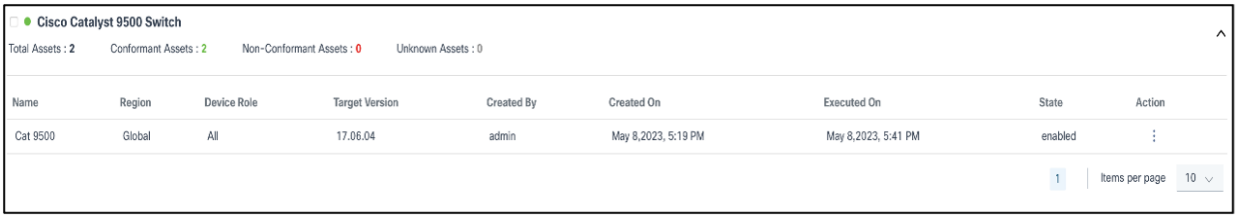
I criteri sono raggruppati in base ai modelli di dispositivo e vengono visualizzati come pannelli espandibili per fornire una singola visualizzazione tra i modelli di dispositivo gestiti da controller diversi.



Visualizzazione compressa dei criteri di conformità

Nella vista compressa, il pannello mostra il modello del dispositivo e rapide statistiche quali Totale

asset, Cespiti conformi, Cespiti non conformi e Cespiti sconosciuti.

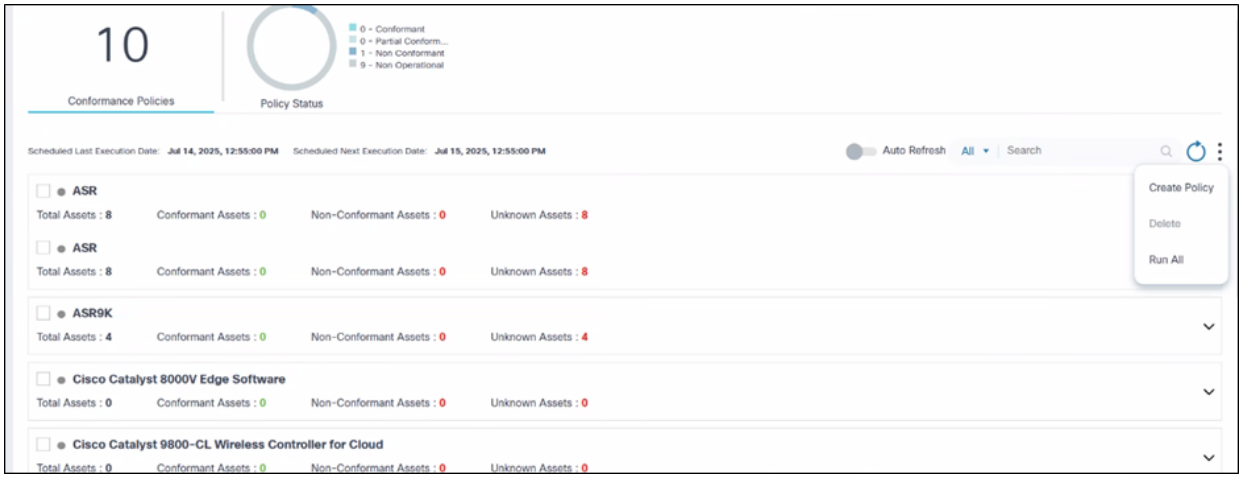


Visualizzazione estesa delle regole di conformità

Nella visualizzazione espansa vengono visualizzati tutti i criteri relativi al modello di dispositivo. Per ogni criterio è possibile eseguire azioni aggiuntive, ad esempio Esegui, Modifica criterio, Visualizza risultati e così via, selezionando l'icona Altre opzioni dalla colonna Azione.

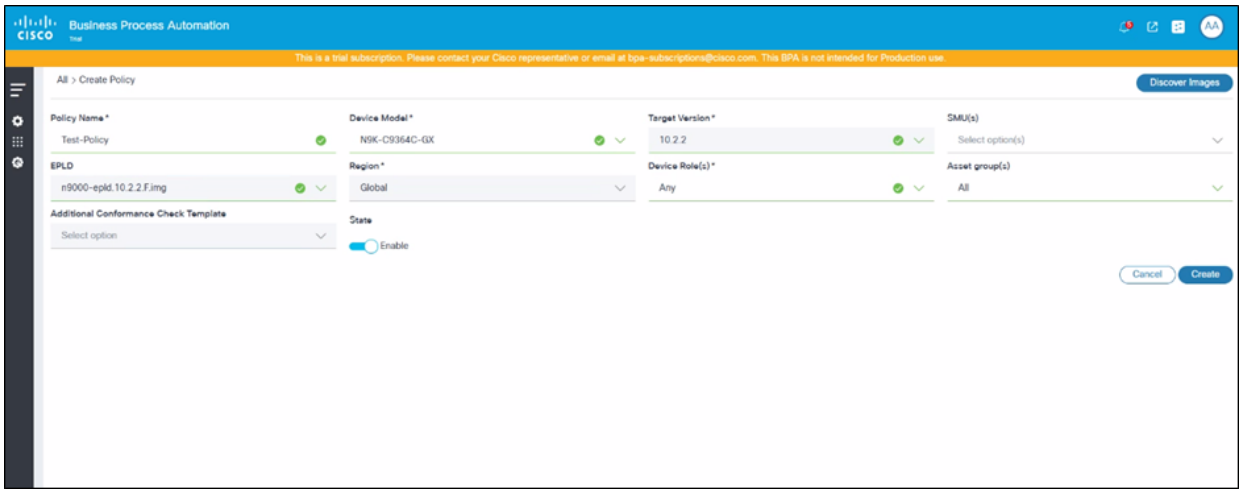
Creazione di criteri di conformità software

1. Accedere a BPA con le credenziali che hanno la gestione dell'accesso a Software Conformance.
2. Selezionare Aggiornamento sistema operativo > Conformità software. Viene visualizzata la pagina Software conforme.



Crea criterio

3. Selezionare l'icona Altre opzioni > Crea criterio.



Crea modulo criteri

4. Immettere le informazioni nei campi Nome criterio, Modello/i dispositivo, Versione di destinazione, SMU, EPLD, Ruolo dispositivo, Gruppi di asset e Modello di controllo di conformità aggiuntivo. SMU, gruppi di asset e modelli di controllo di conformità aggiuntivi sono campi facoltativi.

Nota: È ora possibile selezionare più modelli di dispositivo nel modulo Crea criterio di conformità.

Nota: Il framework di conformità software può eseguire controlli di conformità sulla versione del sistema operativo di base e sulle patch SMU rispetto ai dispositivi di un modello, ruolo o istanza di controller specifici che gestiscono il dispositivo. Se sono necessari ulteriori controlli personalizzati, è possibile creare un modello di processo con i comandi e le regole di convalida necessari che possono essere mappati in base al campo Modello controllo di conformità aggiuntivo.

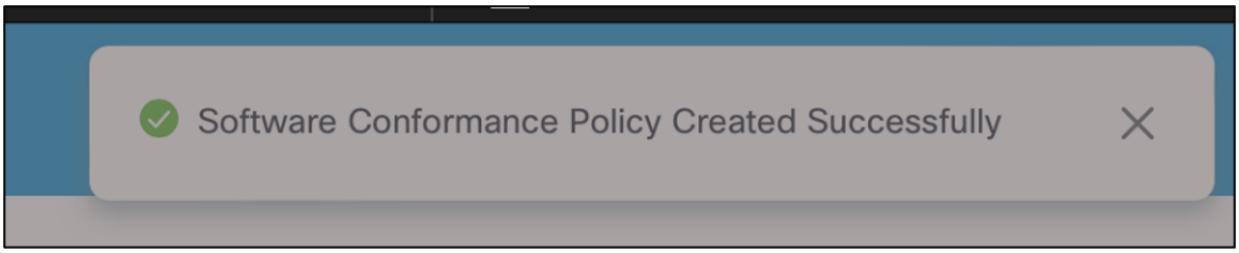
5. Fare clic su Crea. Viene visualizzata una conferma.

Nota: Occorre prendere nota del seguente elenco.

- Gli amministratori Use Case possono creare più criteri con ruoli di dispositivo diversi per un modello di dispositivo selezionato. In un singolo criterio è possibile selezionare più ruoli.
- Se si seleziona Any (Qualsiasi) dall'elenco a discesa Device Role (Ruoli dispositivo), tutti gli altri ruoli del dispositivo (ad esempio, Access, Core, ecc.) vengono disabilitati. Se è selezionato un altro ruolo del dispositivo, Any è disabilitato.
- Per i dispositivi gestiti da controller quali CNC, NSO, ANSIBLE e Direct-to-Device, il ruolo Any (selezionato dall'elenco a discesa Ruoli dispositivo) può essere utilizzato per eseguire il controllo di conformità perché i dispositivi non dispongono di informazioni sul ruolo.
- Se si seleziona Qualsiasi dall'elenco a discesa Ruoli dispositivo per FMC, la conformità

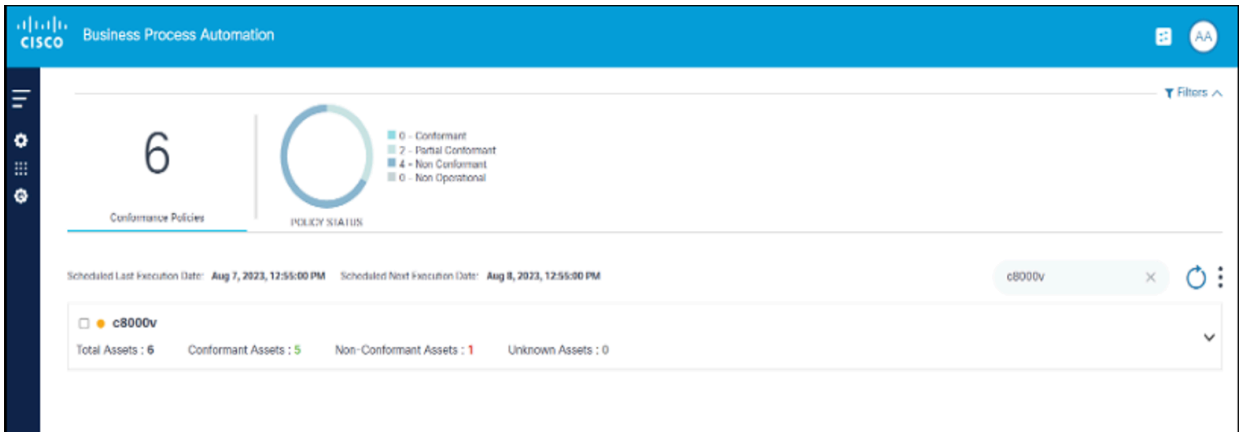
software viene eseguita su tutti i dispositivi, inclusi i dispositivi autonomi, di controllo e dati.

- La conformità e gli aggiornamenti SMU sono supportati solo per i controller CNC, NSO, ANSIBLE, FMC, Direct-to-Device e NDFC.
- In questa release è supportato solo l'opzione Globale (Global) dall'elenco a discesa Regione (Region)
- Gli utenti possono selezionare i gruppi di asset dall'elenco a discesa. Per impostazione predefinita è selezionato Tutto. Gli utenti hanno la possibilità di selezionare uno o più gruppi di asset. Se viene selezionato un gruppo di asset specifico, il criterio viene eseguito solo sui dispositivi del gruppo selezionato.
- Se i valori previsti per i campi Device Model, Target Version e SMU(s) non sono visualizzati, fare clic su Discover Images (Trova immagini) e riprovare.
- I campi Modello dispositivo, Gruppo/i di asset e Ruolo costituiscono una regola univoca; i criteri duplicati non sono consentiti.
- Il campo EPLD popola i valori solo quando i metadati dell'immagine EPLD sono disponibili per i modelli di dispositivo e la versione di destinazione selezionati.
- Il nome del criterio è univoco e non sono consentiti nomi di criteri duplicati.



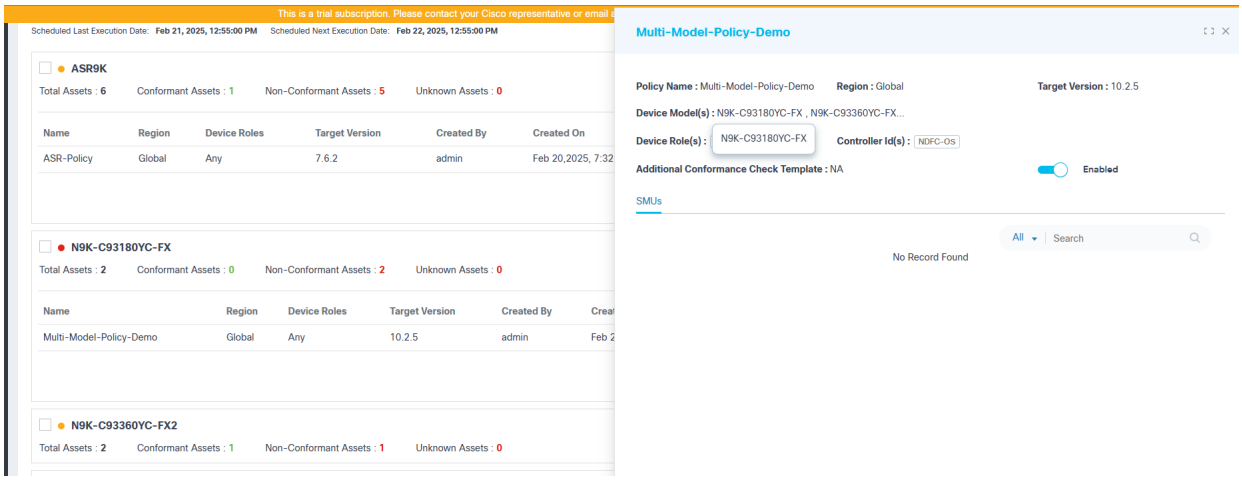
Conferma creazione criteri di conformità

- I modelli di processo contrassegnati per l'aggiornamento del sistema operativo di nuova generazione (Next-Gen) vengono visualizzati nel campo Modello di controllo di conformità aggiuntivo.



Risultati della ricerca dei criteri di conformità

6. Individuare il criterio creato immettendo il modello di dispositivo nel campo Cerca.

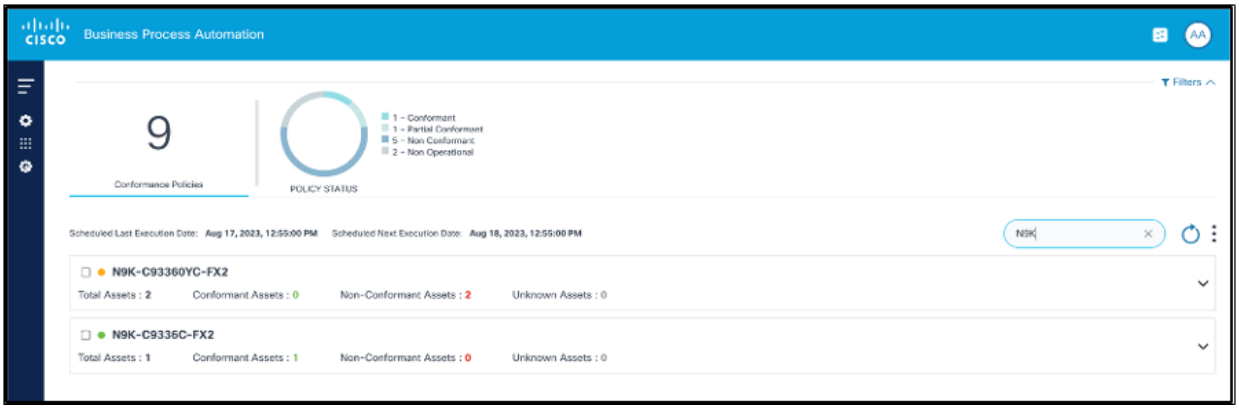


Visualizza criteri di conformità

7. Fare clic su Criterio per visualizzare i dettagli del criterio.

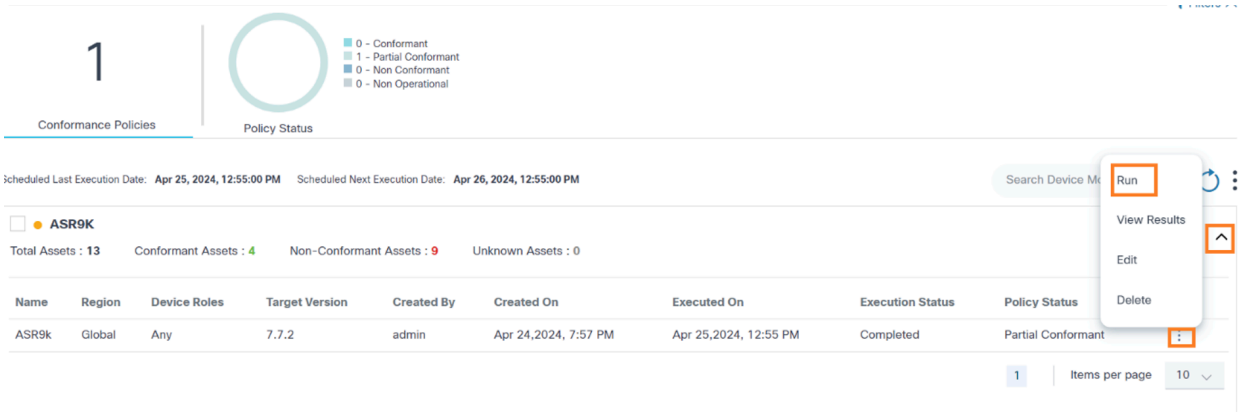
Esecuzione dei controlli di conformità software su richiesta

1. Accedere a BPA con le credenziali con accesso in esecuzione.
2. Selezionare Aggiornamento sistema operativo > Conformità software. Viene visualizzata la pagina Software conforme.



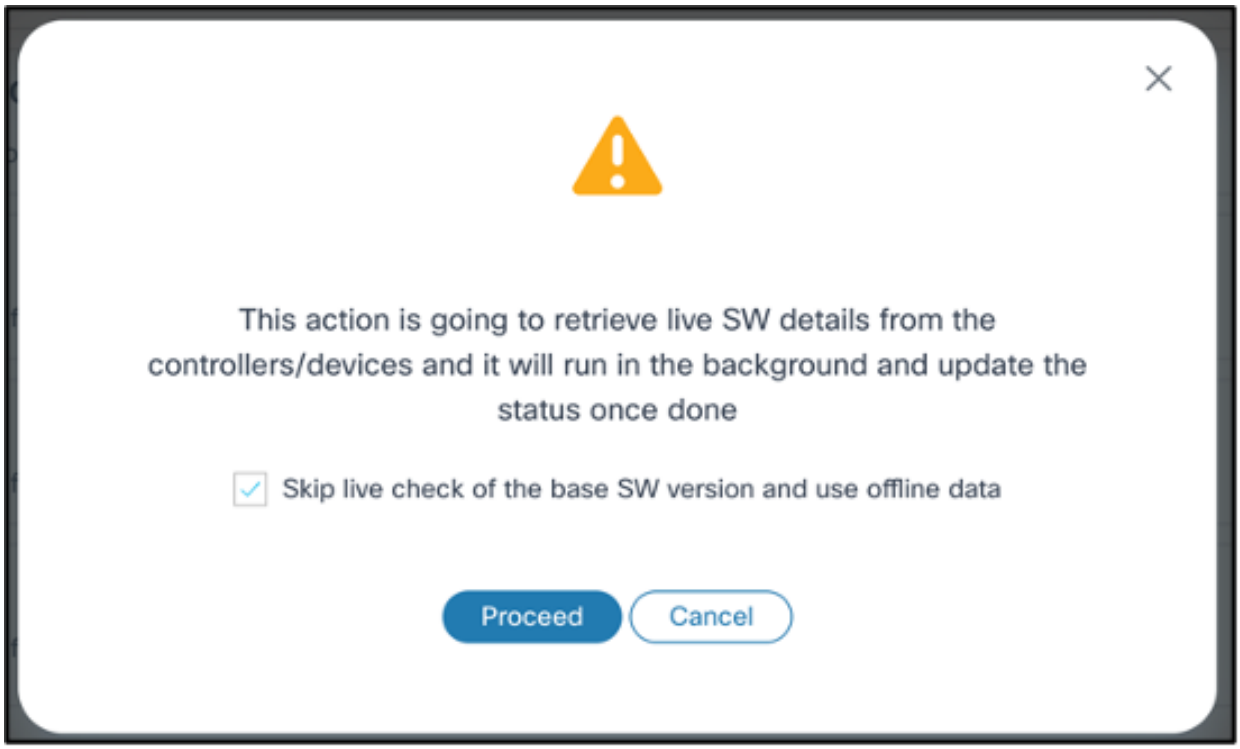
Ricerca criteri

3. Individuare il criterio da eseguire su richiesta utilizzando il campo Cerca.



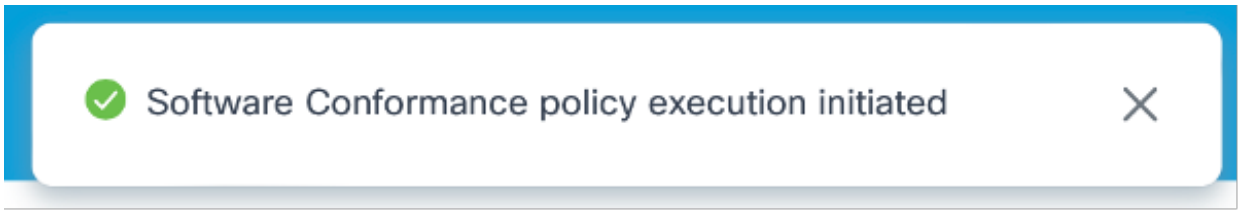
Lanciare

4. Dalla colonna Azione del criterio, selezionare Altre opzioni > Esegui. Viene visualizzata una conferma per verificare se è necessario eseguire un controllo dell'inventario dinamico per i dispositivi.



Conferma dell'esecuzione dei criteri di conformità

5. Se è necessaria la sincronizzazione dell'inventario prima di eseguire i controlli di conformità, deselezionare la casella di controllo Ignora controllo dinamico della versione del software di base e usa dati non in linea e fare clic su Continua. In questo caso, il controllo di conformità viene eseguito solo dopo la sincronizzazione. Nell'angolo superiore destro viene visualizzata una notifica.



Notifica di esecuzione criteri di conformità

Nota: Occorre prendere nota del seguente elenco.

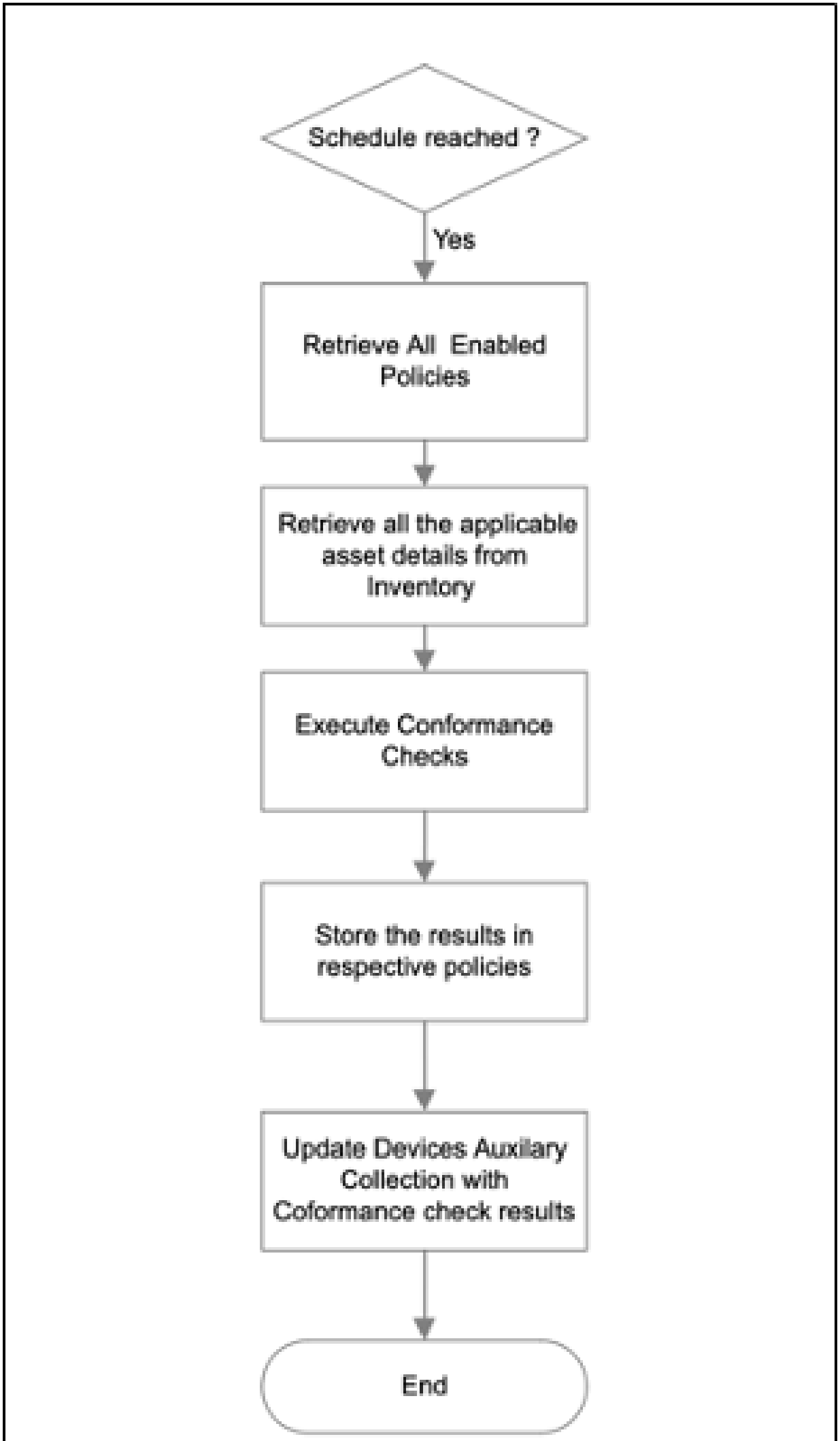
- Per impostazione predefinita, il controllo di conformità viene eseguito utilizzando i dati di inventario delle risorse.
- Durante questo processo, se la sincronizzazione dell'inventario o del dispositivo ha esito negativo, il relativo dispositivo di criteri viene contrassegnato come Sconosciuto e la verifica SMU viene ignorata.
- Per le SMU, i dati in tempo reale vengono recuperati dal dispositivo prima di eseguire i controlli di conformità per verificare se la casella di controllo Ignora controllo dinamico della versione del software di base e usa dati non in linea è selezionata o meno.
- Quando un criterio include più modelli di dispositivo, l'esecuzione del criterio per un modello di dispositivo avvia l'esecuzione di tutti i criteri associati.

Pianificazione dell'esecuzione dei controlli di conformità software

I controlli di conformità software possono essere eseguiti automaticamente a intervalli regolari utilizzando il servizio di pianificazione. I controlli di conformità programmati possono essere configurati per l'esecuzione di:

- Giornaliero
- Due volte al giorno
- Settimanale
- Una volta

Una volta raggiunta la pianificazione, tutti i criteri con stato Abilitato vengono eseguiti automaticamente e i risultati della conformità vengono memorizzati nei rispettivi criteri.

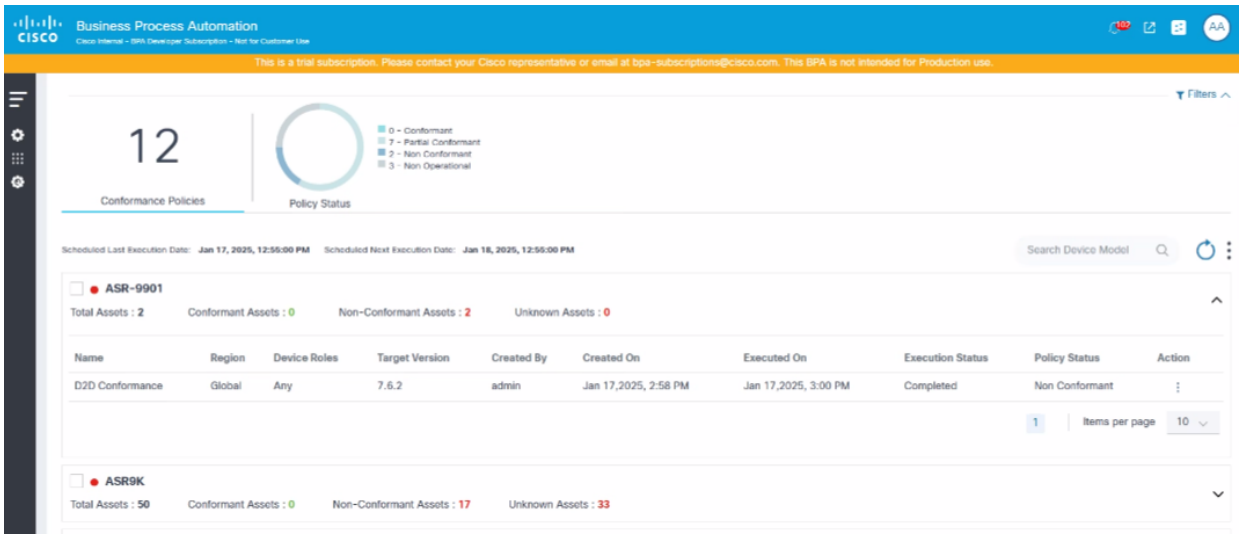

Schedule reached ?
Yes
Retrieve All Enabled Policies
Retrieve all the applicable asset details from Inventory
Execute Conformance Checks
Store the results in respective policies
Update Devices Auxilary Collection with Coformance check results
End

Esecuzione pianificata dei controlli di conformità software Flusso delle chiamate

Per ulteriori informazioni, fare riferimento a Conformità software.

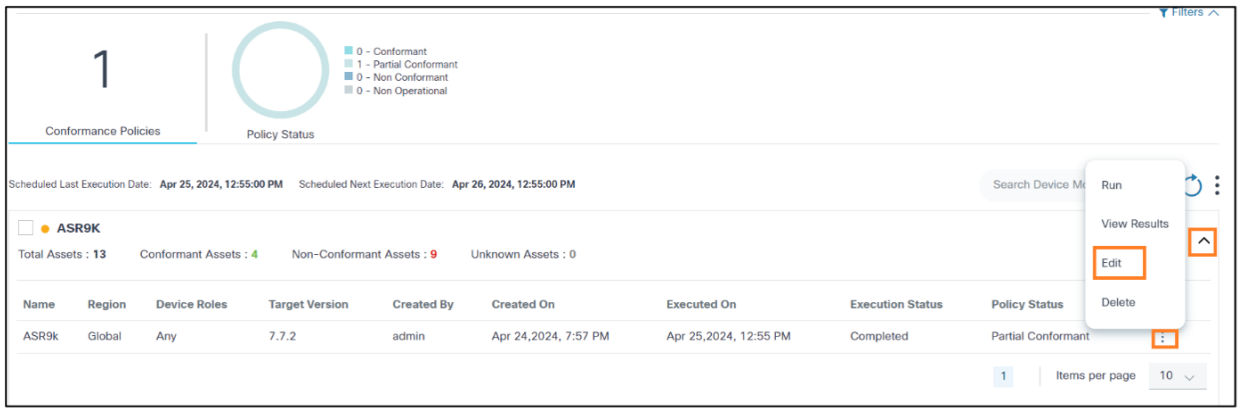
Aggiornamento dei criteri di conformità software

1. Accedere a BPA con credenziali che dispongono dell'accesso di gestione per la conformità software
2. Selezionare Aggiornamento sistema operativo > Conformità software. Viene visualizzata la pagina Software conforme.



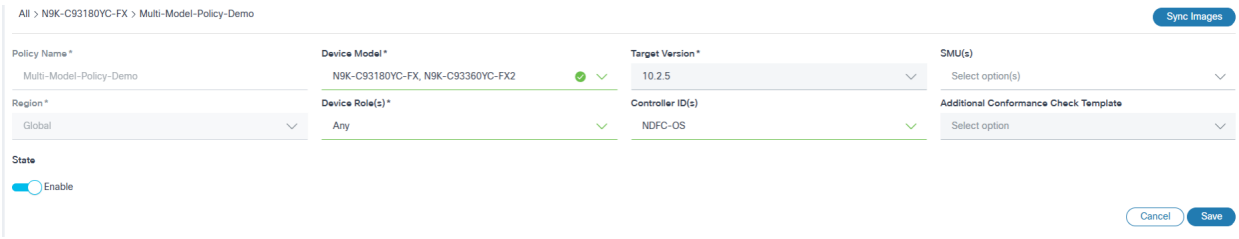
Conformità software

3. Utilizzare il campo Search per individuare il criterio desiderato.



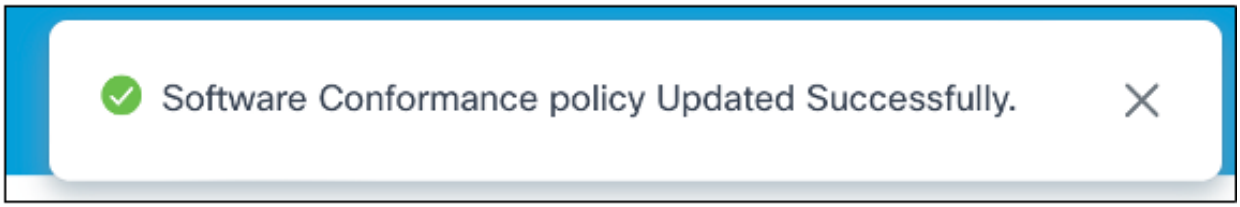
Modifica

4. Dalla colonna Azione del criterio, selezionare l'icona Altre opzioni > Modifica.



Modifica criteri di conformità con dettagli completati

5. Modificare la versione di destinazione, le SMU, i ruoli dei dispositivi, gli ID dei controller, lo stato dei criteri e i modelli aggiuntivi di controllo di conformità come necessario.
6. Fare clic su Save (Salva). Viene visualizzata una conferma.

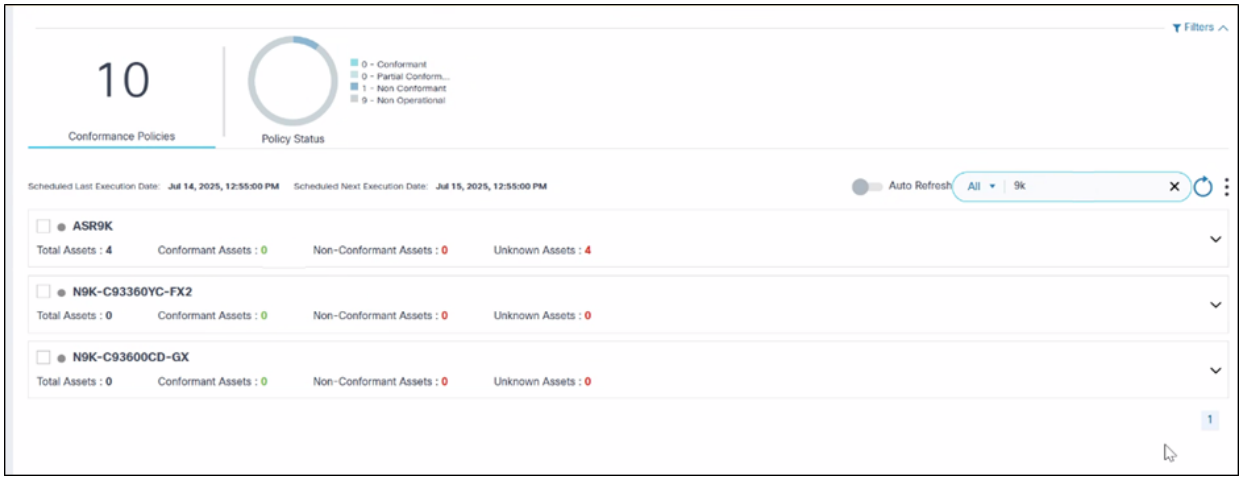


Conferma dell'esito positivo dell'aggiornamento

Nota: Quando il criterio di conformità software viene utilizzato per un processo di aggiornamento in corso, il criterio non può essere modificato.

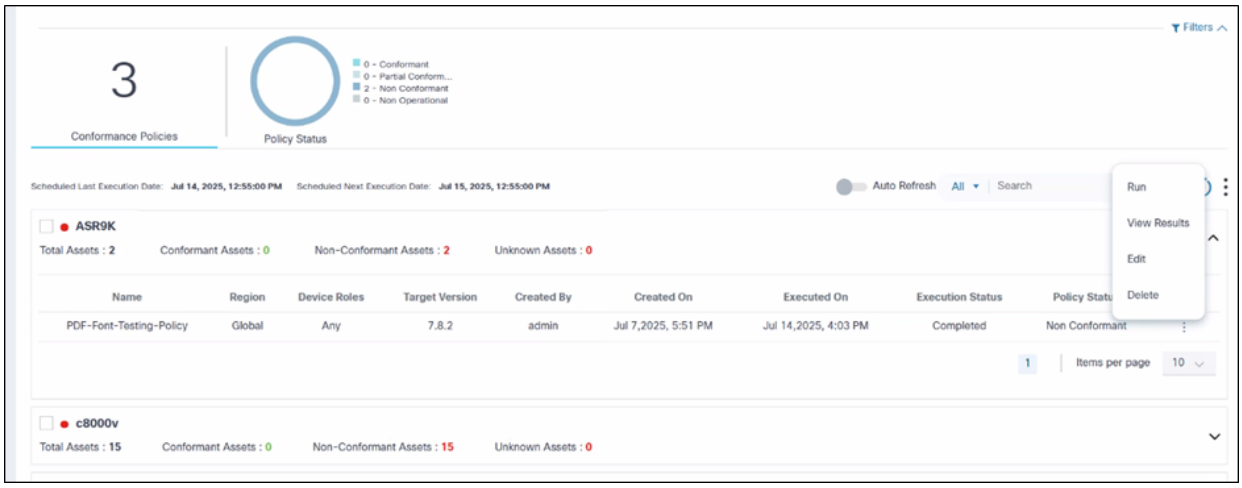
Eliminazione dei criteri di conformità software

1. Accedere a BPA con le credenziali che dispongono dell'accesso di gestione.
2. Selezionare Aggiornamento sistema operativo > Conformità software. Viene visualizzata la pagina Software conforme.



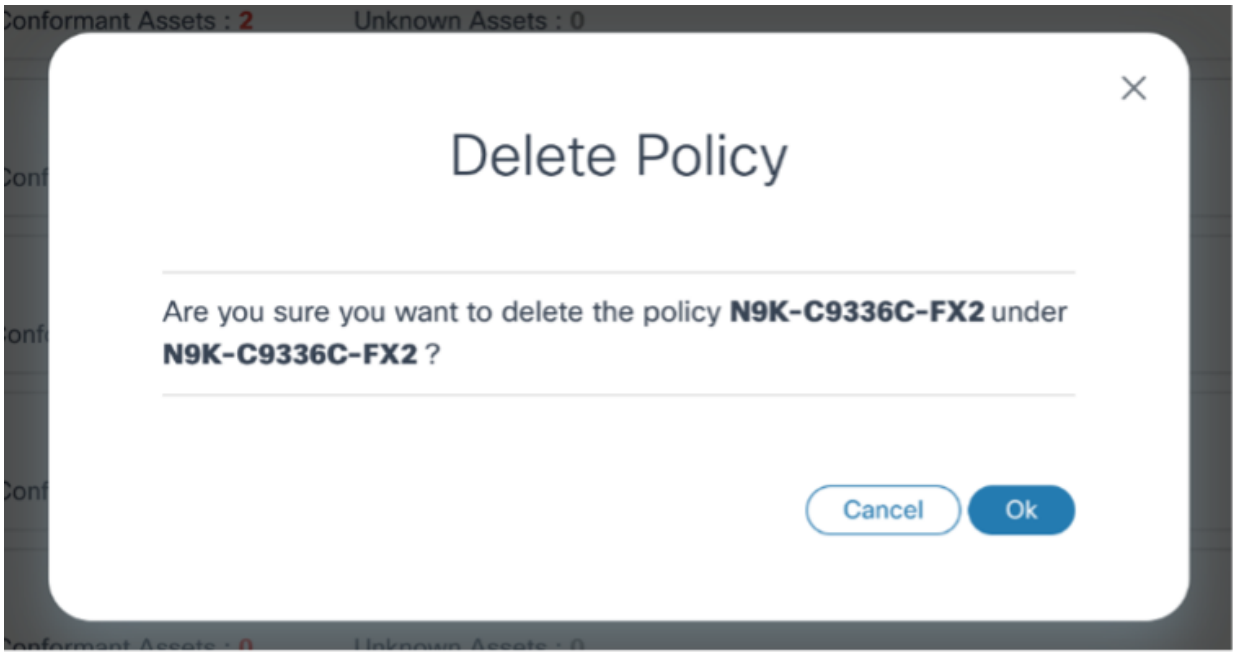
Risultati della ricerca dei criteri di conformità

3. Utilizzare il campo Search per individuare il criterio desiderato.

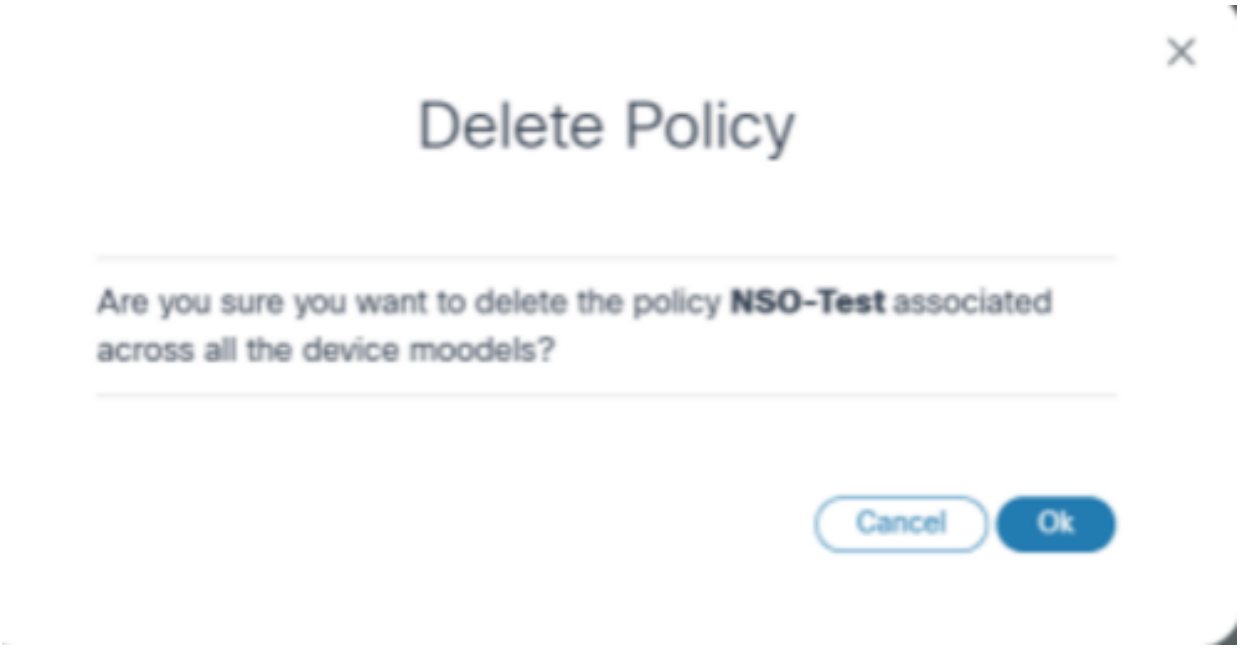


Elimina

4. Dalla colonna Azione del criterio, selezionare l'icona Altre opzioni > Elimina. Viene visualizzata una finestra di conferma.



Conferma eliminazione criterio



Conferma eliminazione criterio (se il criterio è associato a più modelli)

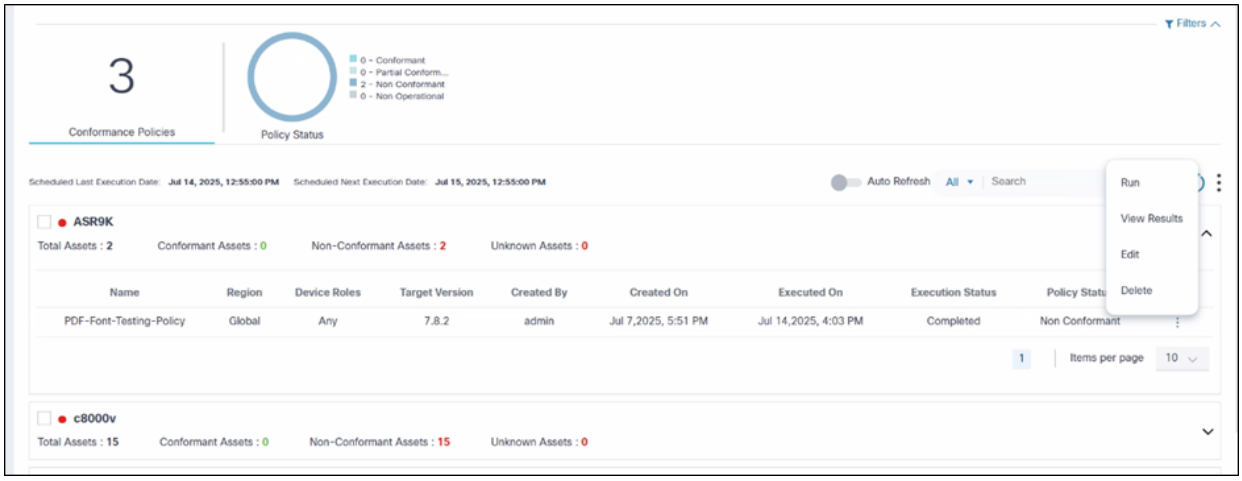
5. Fare clic su OK. Il criterio viene eliminato.

Nota: Occorre prendere nota del seguente elenco.

- Se un criterio è associato a più modelli di dispositivo, l'eliminazione di un criterio comporta la rimozione di tutti i criteri correlati per ogni modello associato.
- Quando il criterio di conformità software viene utilizzato per un processo di aggiornamento in corso, non è possibile eliminarlo.

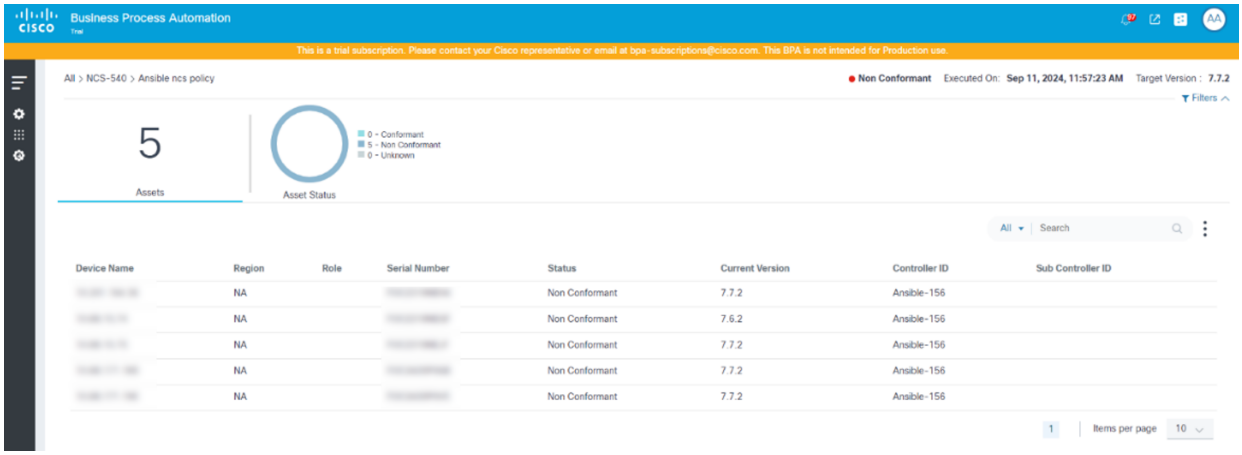
Visualizzazione e download dei risultati di conformità

Dopo l'esecuzione di un criterio:

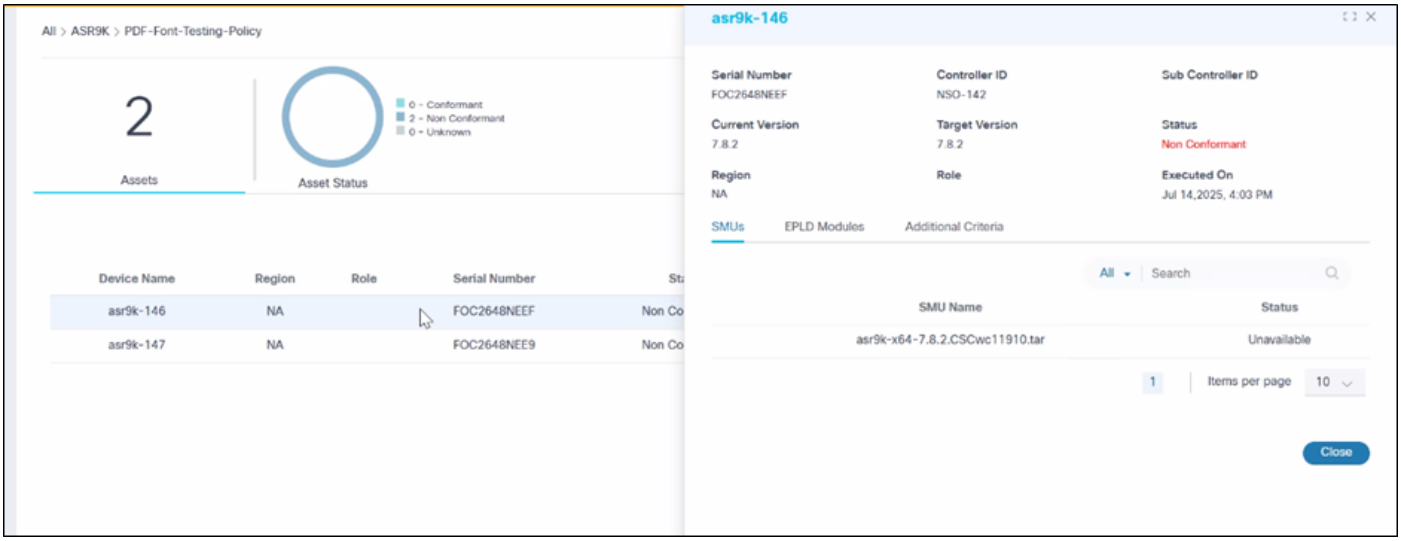


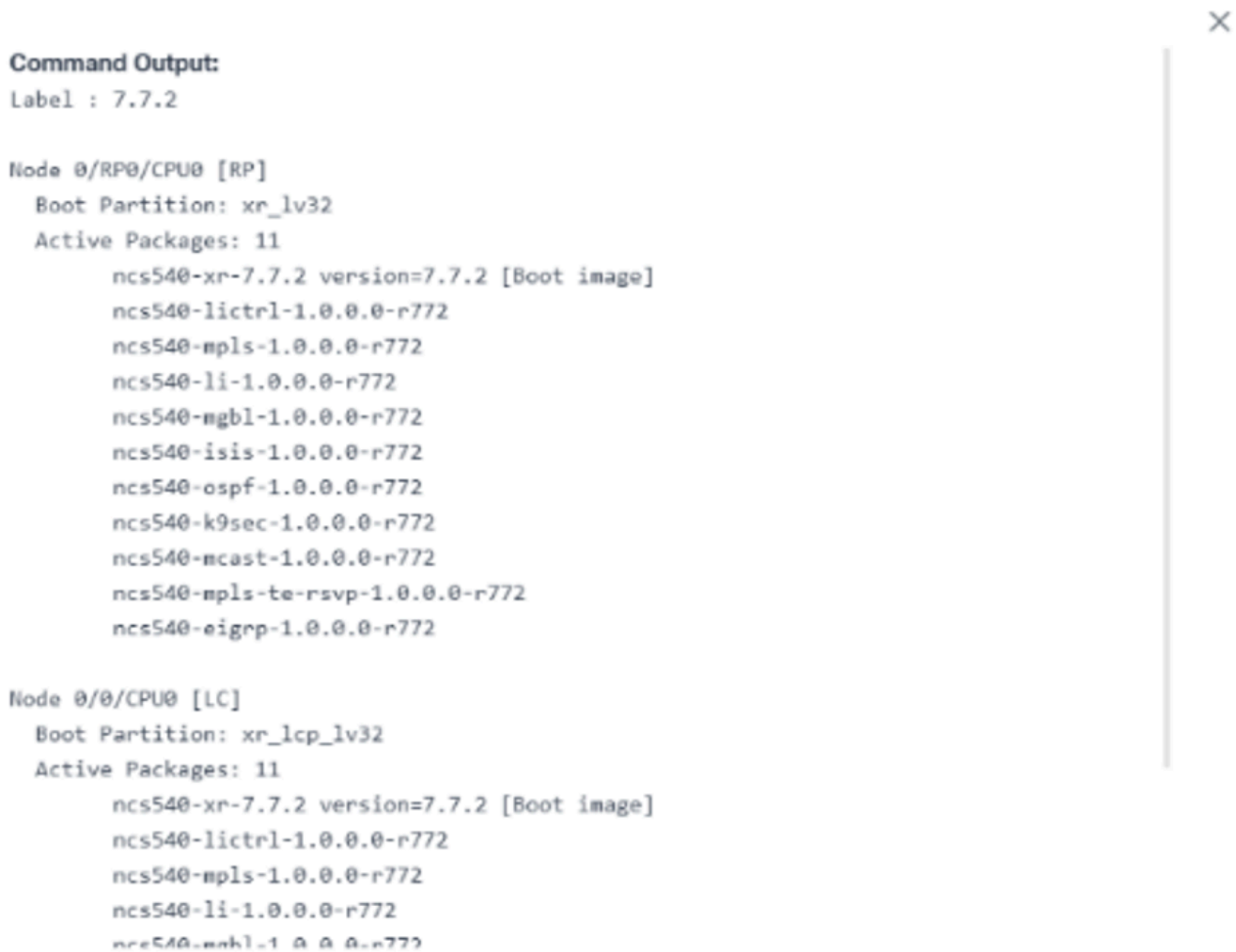
Opzione Visualizza risultati

1. Nella pagina Software conforme, selezionare l'icona Altre opzioni > Visualizza risultati. Nella pagina Risultati viene visualizzata la posizione in cui gli utenti possono visualizzare lo stato di conformità dei dispositivi.



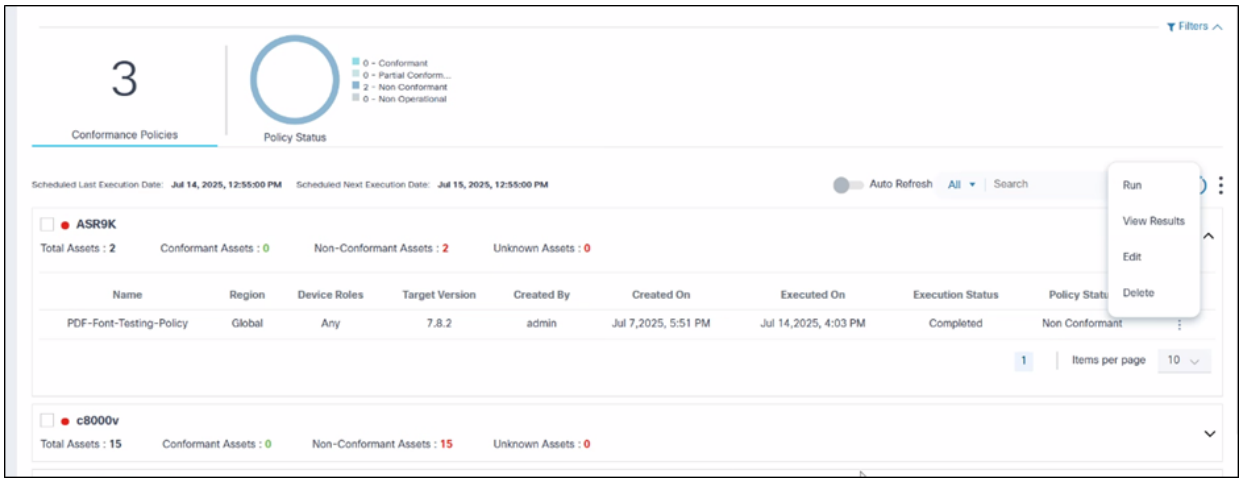
Visualizza risultati





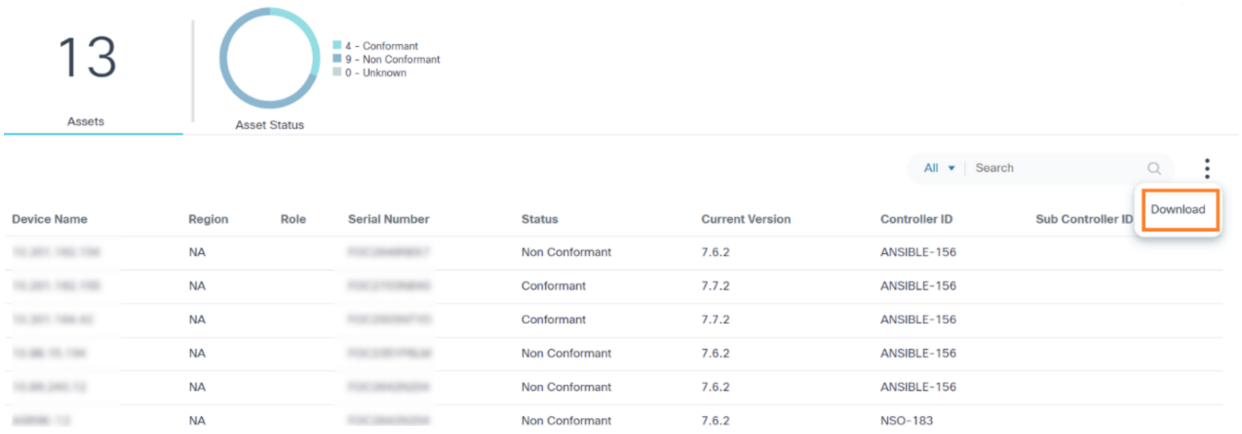
2. Selezionare una riga per visualizzare i dettagli specifici del cespite insieme allo stato SMU e ai criteri aggiuntivi.

Nota: I dettagli SMU vengono visualizzati solo per le risorse dei controller NSO, CNC, ANSIBLE, Direct-to-Device e NDFC. I moduli EPLD vengono visualizzati solo per i controller NDFC.



Visualizza risultati

3. Dalla colonna Azione di un dispositivo, selezionare l'icona Altre opzioni > Visualizza risultati.



Scarica

4. Selezionate l'icona Altre opzioni (More Options) > Scarica (Download) per scaricare i risultati in formato .csv con lo stato di disponibilità SMU.

Visualizzazione Foglio di Excel

Nota: Visualizza risultati visualizza solo i risultati dell'ultimo controllo di conformità eseguito. Gli utenti possono visualizzare solo le risorse per le quali hanno accesso. Per i criteri non operativi, Visualizza risultati è disabilitato.

Possibili stati del dispositivo:

- Conforme: Indica che il dispositivo è conforme al criterio definito
- Non conforme: Indica che il dispositivo non è conforme quando vengono soddisfatte le seguenti condizioni:

Versione di destinazione	SMU	Controllo di conformità	Stato
Non conforme	N/D	N/D	Non conforme
Conforme	Non disponibile	Regole non riuscite	Non conforme
Conforme	Disponibile	Regole non riuscite	Non conforme
Conforme	Non disponibile	Regole riuscite	Non conforme

- Sconosciuto: Indica che non è stato possibile eseguire il controllo di conformità del software del dispositivo perché il dispositivo non dispone delle informazioni sulla versione del software corrente.

I criteri per lo stato Sconosciuto includono:

Versione di destinazione	SMU	EPLD	Controllo di conformità	Stato
Non conforme	N/D	N/D	N/D	Non conforme
Conforme	Non disponibile	Non conforme	Regole non riuscite	Non conforme
Conforme	Non disponibile	Conforme	Regole non riuscite	Non conforme
Conforme	Disponibile	Conforme	Regole non riuscite	Non conforme
Conforme	Disponibile	Non conforme	Regole non riuscite	Non conforme
Conforme	Non disponibile	Conforme	Regole riuscite	Non conforme
Conforme	Non disponibile	Conforme	Regole riuscite	Non conforme

Possibili stati SMU:

- Disponibile: Indica che l'unità SMU è presente nel dispositivo e in stato Attivo
- Non disponibile: Indica che la SMU potrebbe non esistere o che esiste ma è in stato Inactive

Possibili stati del modulo EPLD:

- Conforme: Indica che il modulo EPLD è presente nel dispositivo con la versione di destinazione prevista
- Non conforme: Indica che il modulo EPLD è presente nel dispositivo con la versione di destinazione prevista non corrispondente
- Modulo mancante: Indica che i moduli EPLD non sono configurati o sottoscritti nel dispositivo

Possibili stati dei modelli di controllo di conformità:

- Operazione riuscita: Indica che il dispositivo ha eseguito correttamente il modello di processo con comandi e regole validi
- Operazione non riuscita: Indica che il dispositivo non è riuscito a eseguire il modello di processo (ad esempio, quando i comandi non sono corretti)
- N/D: Indica che il dispositivo non è idoneo per l'esecuzione del modello di processo, ad esempio quando il dispositivo non è conforme alla versione di destinazione definita.

Nota: Occorre prendere nota del seguente elenco.

- I controlli di conformità software funzionano solo con i dispositivi appartenenti al tenant predefinito
- I controlli di conformità software si basano sull'inventario degli asset come fonte di informazioni per le versioni software correnti dei dispositivi. Se i dati di inventario degli asset non sono aggiornati, i risultati dei controlli di conformità software non sono aggiornati. Per evitare il problema dei dati non aggiornati, utilizzare la funzione di controllo dell'inventario dinamico all'avvio dell'esecuzione dei criteri di conformità
- La pianificazione predefinita può essere modificata in Aggiornamento sistema operativo > Impostazioni > Conformità software
- Dopo l'aggiornamento a BPA 5.1, tutte le policy preesistenti vengono spostate in uno stato disabilitato; gli utenti devono modificare ogni criterio, selezionare i valori appropriati, attivarlo e quindi salvare le modifiche per un ulteriore utilizzo

Criteri di aggiornamento

Il componente criteri di aggiornamento supporta due tipi di criteri:

- Regola in un unico passaggio:
  - Any-Any
  - <versione origine specifica (7.7.1)> - <versione destinazione specifica (7.7.2)>
- Regola in più passaggi:
  - v7.7.1 - 7.7.2
  - v7.7.2 - 7.7.8
- L'aggiornamento in più passaggi può includere SMU Bridge, come illustrato nell'esempio

seguente:
    - v7.7.1 - v7.7.1 [Bridge SMU]
    - V7.7.1[Bridge SMU] - 7.7.8

Il componente criteri di aggiornamento offre la flessibilità necessaria per predefinire i seguenti artifact specifici della piattaforma:

- Percorsi aggiornamento
- Modelli o workflow di pre e post-convalida
- Workflow di distribuzione
- Flusso di lavoro attivazione
- Flusso di lavoro di backup
- Valori di timeout
- Ripristina flusso di lavoro
- Differenze valide precedenti e successive
- Flusso di lavoro di deviazione del traffico o di inversione del traffico

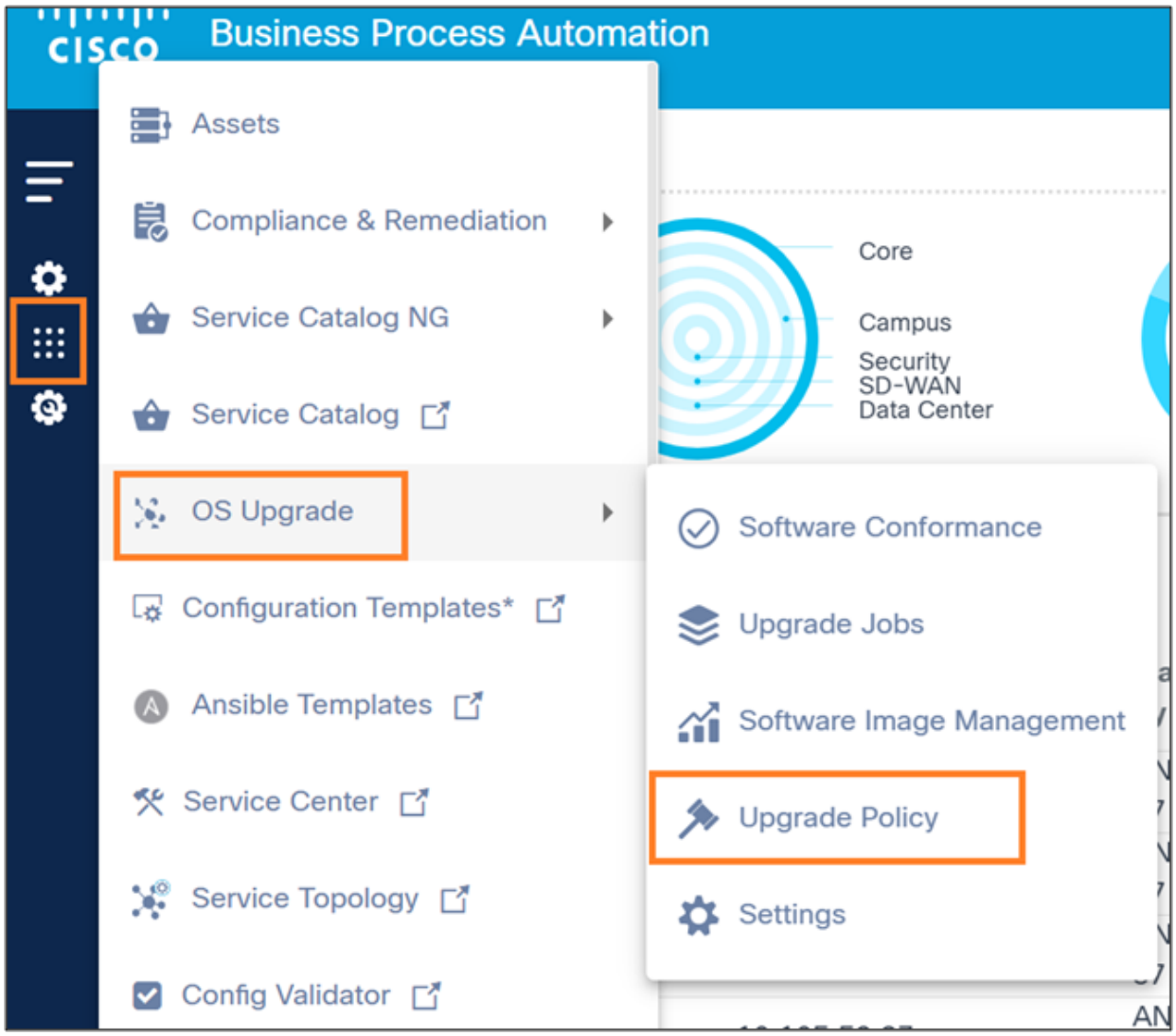
Prerequisiti

- Modelli di processo o workflow richiesti prima e dopo la convalida
- Workflow di backup, distribuzione, attivazione e rollback richiesti
- Metadati immagine richiesti

Visualizzazione e gestione dei criteri di aggiornamento

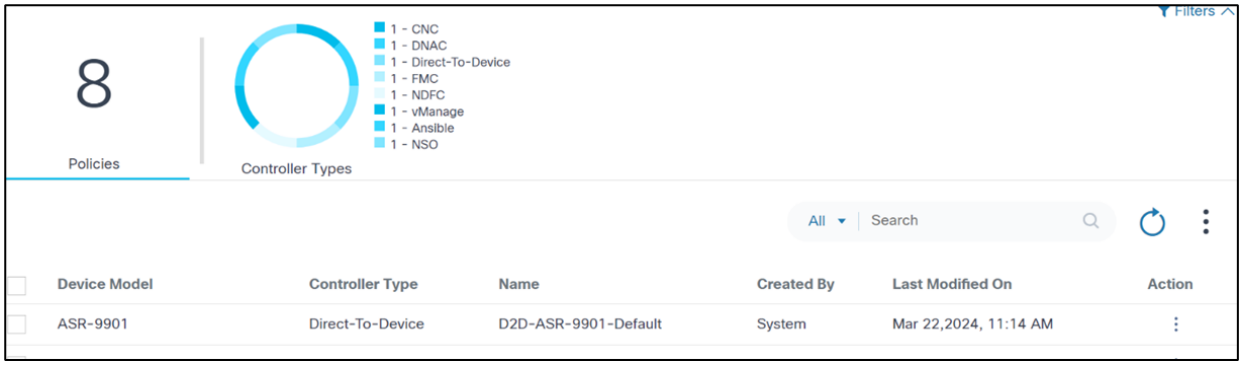
Per accedere alla pagina Criteri di aggiornamento:

1. Accedere a BPA con credenziali che dispongano di diritti di accesso sufficienti per i criteri di aggiornamento.



Spostamento tra i criteri di aggiornamento

2. Selezionare Aggiornamento sistema operativo > Criteri di aggiornamento. Viene visualizzata la pagina Criteri di aggiornamento.



Criteri di aggiornamento

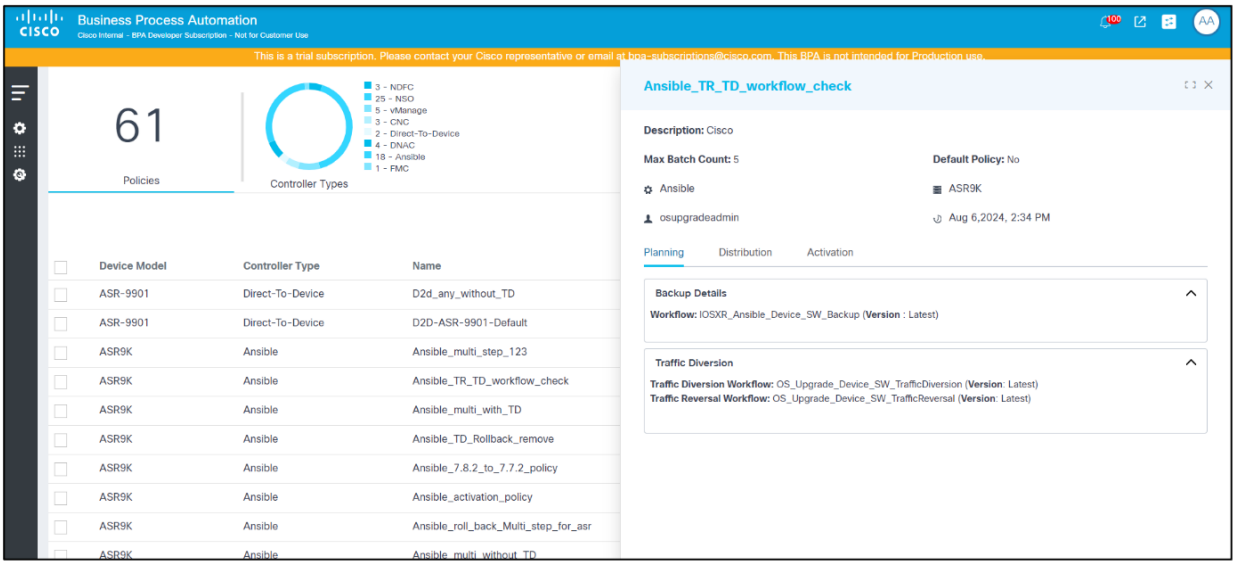
La pagina Criteri di aggiornamento contiene le informazioni riportate di seguito.

- Una sezione di analisi, visualizzata nella parte superiore, che fornisce le informazioni

riportate di seguito.

    - Numero totale di criteri di aggiornamento nel sistema
    - Un filtro rapido Tipi di controller che consente di filtrare per tipo di controller
- Un'icona Altre opzioni che fornisce l'opzione per creare criteri e azioni di elaborazione in blocco, ad esempio Elimina tutti i criteri selezionati
- Un filtro di ricerca per cercare criteri che possono essere filtrati come segue:

    - Tutto: Cerca in tutti i campi
    - Modello dispositivo: Cerca criteri con un modello specificato
    - Nome: Cerca criteri con un nome di criterio specificato
    - Creato da: Cerca criteri con un utente specificato
- Ordinare i criteri facendo clic sui rispettivi nomi di colonna o campi di tabella



Visualizzazione dettagli criteri

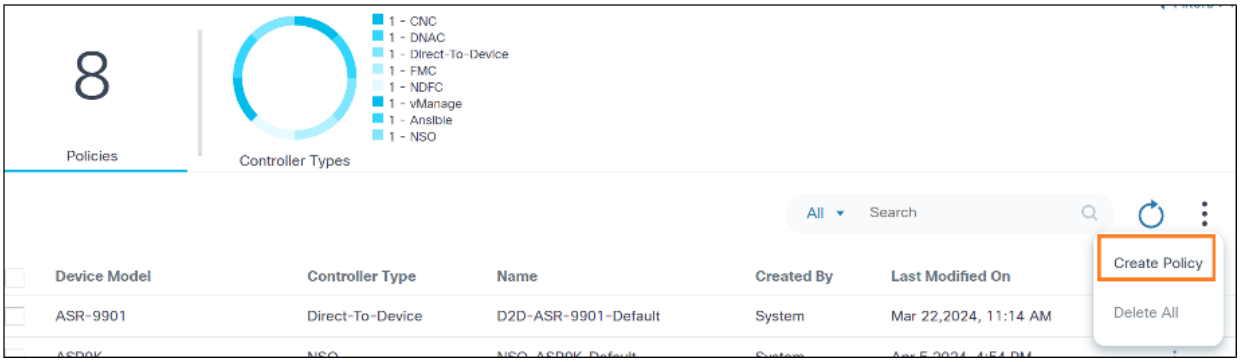
- Facendo clic su un criterio specifico o su una riga nella visualizzazione dei dettagli di un criterio

---

Nota: Se i nomi dei criteri sono univoci, lo stesso modello di dispositivo e lo stesso tipo di controller possono avere un numero qualsiasi di criteri.

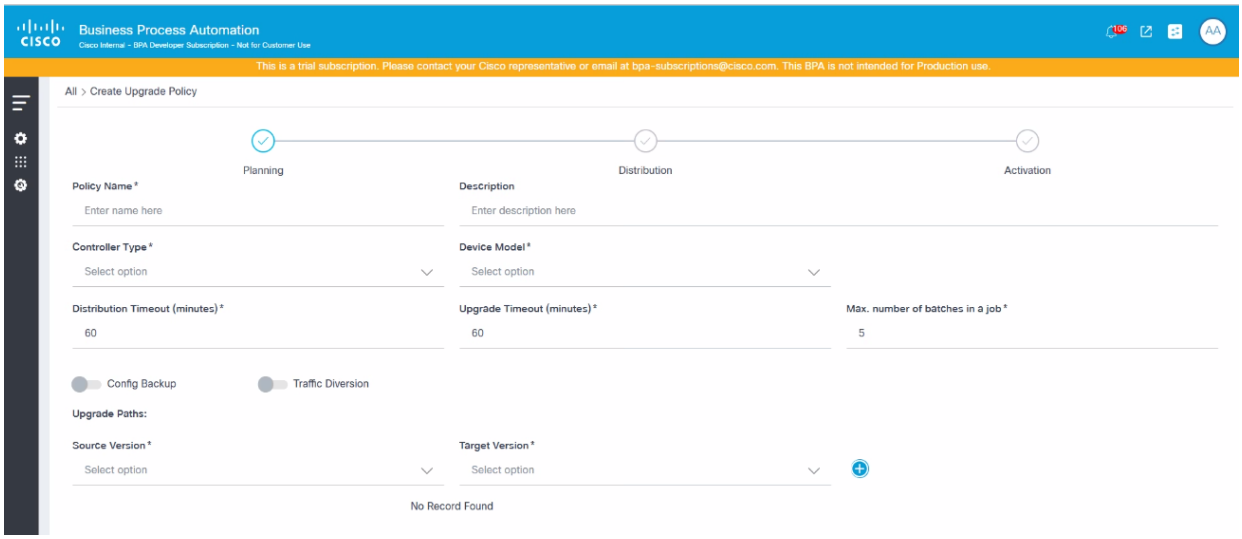
Creazione dei criteri di aggiornamento

1. Accedere a BPA con le credenziali che dispongono dell'accesso di gestione per i criteri di aggiornamento.
2. Selezionare Aggiornamento sistema operativo > Criteri di aggiornamento. Viene visualizzata la pagina Criteri di aggiornamento.



Crea criterio

3. Selezionare Altre opzioni > Crea criterio. Viene visualizzata la pagina Crea criterio di aggiornamento.



Crea criteri di aggiornamento

Pianificazione

1. Configurare i parametri correlati al criterio generale. Nella tabella seguente viene fornita una breve descrizione di ogni campo.

Campo	Descrizione
Nome criterio	Nome del criterio
Descrizione	Breve descrizione del criterio
Tipo di controller	Controller appropriato utilizzato per eseguire l'aggiornamento del sistema operativo
Modello dispositivo	Modello di dispositivo utilizzato per eseguire l'aggiornamento del sistema operativo
Timeout distribuzione (minuti)	Tempo di attesa massimo in minuti per l'attività di

Campo	Descrizione
	distribuzione delle immagini
Timeout aggiornamento (minuti)	Tempo di attesa massimo in minuti per l'attività di attivazione dell'immagine
Numero massimo di batch in un processo	Numero di batch che possono essere aggiunti in un processo; il numero massimo di batch consentiti è 20
Attiva/disattiva backup configurazione	Attivare questa opzione se è necessario eseguire il backup e completare i seguenti campi nella finestra per i controller vManage e Direct-to-Device: - Nome workflow: Flusso di lavoro di backup applicabile Nota: Se non è possibile trovare i workflow, assicurarsi che siano contrassegnati correttamente con il tag NextGen di Aggiornamento del sistema operativo - Ultimo flusso di lavoro: Se l'opzione è selezionata, viene utilizzata l'ultima versione del flusso di lavoro selezionato - Versione flusso di lavoro: La versione personalizzata del workflow; può essere selezionato solo se non è selezionata l'opzione Usa flusso di lavoro più recente. Per i controller NDFC, NSO, CNC e Cisco Catalyst Center, il backup viene eseguito tramite il servizio Backup e ripristino. È pertanto necessario selezionare un criterio di backup e ripristino nella finestra Dettagli backup. Nota: Gli utenti devono selezionare il criterio appropriato per il tipo di controller. Per ulteriori informazioni sui criteri di backup e ripristino, consultare la sezione Backup e ripristino.
Attiva/disattiva deviazione traffico	Per abilitare il backup per i dispositivi Nexus, è necessario che la configurazione del server scp della funzionalità sia presente nei dispositivi di destinazione. Abilitare questa opzione se la deviazione del traffico è obbligatoria e completare i seguenti campi nella finestra Deviazione traffico:

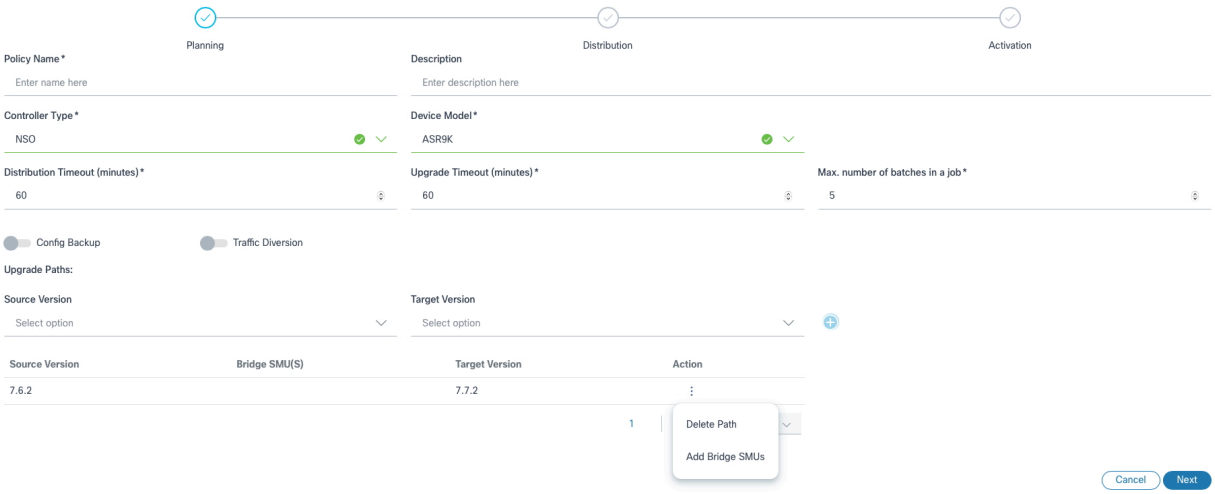
Campo	Descrizione
	- Workflow di deviazione del traffico: Flusso di lavoro di deviazione del traffico applicabile. Nota: Se non è possibile trovare i workflow, assicurarsi che siano contrassegnati correttamente con il tag NextGen di Aggiornamento del sistema operativo - Workflow di inversione del traffico: Flusso di lavoro di inversione del traffico applicabile. Nota: Se non è possibile trovare i workflow, assicurarsi che siano contrassegnati correttamente con il tag NextGen di Aggiornamento del sistema operativo - Ultimo flusso di lavoro: Versione più recente del flusso di lavoro selezionato in precedenza - Versione flusso di lavoro: La versione personalizzata del workflow; può essere selezionato solo se non è selezionato Usa flusso di lavoro più recente
Percorsi aggiornamento	I percorsi di aggiornamento definiscono i percorsi di aggiornamento dei passaggi applicabili; è possibile aggiungere più versioni di origine e di destinazione nei campi seguenti per soddisfare domande variabili - Versione di origine: Versione iniziale del percorso di aggiornamento - Versione di destinazione: Versione finale del percorso di aggiornamento - Versione di origine (Any) per versione di destinazione (Any): A tale scopo, selezionare Any (Qualsiasi) sia per i campi Source Version (Versione di origine) che per i campi Target Version (Versione di destinazione), che rappresenta il valore predefinito per tutti i modelli di dispositivi. in questo scenario, le pagine Distribuzione e Attivazione forniscono un processo unificato per l'aggiornamento - Versione di origine (versione specifica) alla versione di destinazione (versione specifica): Ciò è reso disponibile selezionando specifiche versioni di immagini disponibili per il modello di dispositivo; è possibile aggiungere più versioni di origine e di destinazione; il numero di input

Campo	Descrizione
	del processo di aggiornamento della distribuzione e dell'attivazione corrisponde al numero di versioni di origine e di destinazione aggiunte e ognuna di esse viene presentata come una sezione comprimibile etichettata con le versioni di origine e di destinazione corrispondenti. Un percorso di aggiornamento richiede l'applicazione di SMU obbligatori nella versione di origine prima dell'aggiornamento alla versione di destinazione aggiungendoli come SMU bridge al rispettivo percorso di aggiornamento. Per ulteriori informazioni sulle SMU Bridge, fate riferimento alla sezione successiva.

SMU bridge

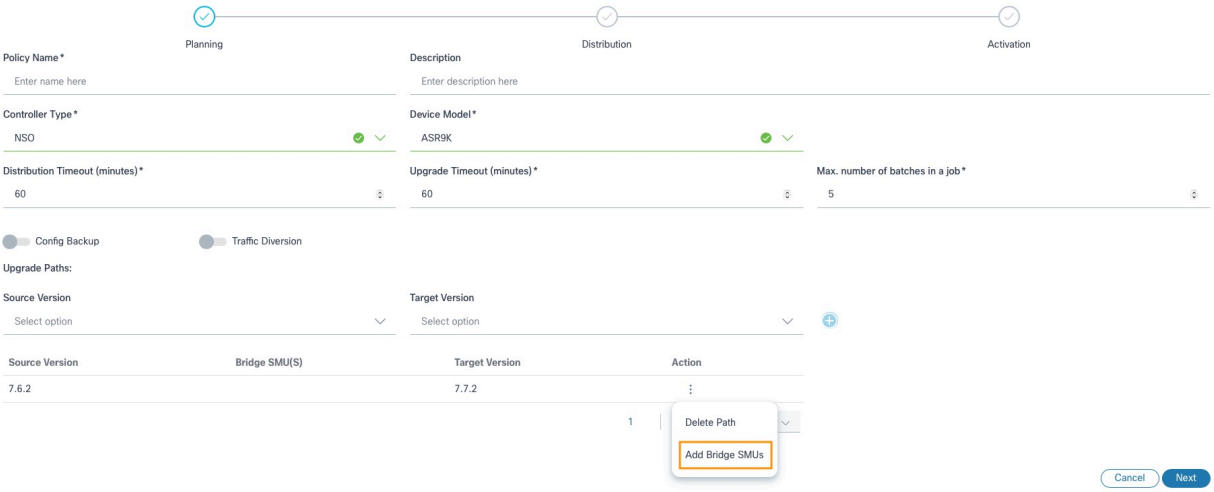
Le SMU bridge, dette anche SMU di aggiornamento o downgrade obbligatori, sono un prerequisito e devono essere installate prima di eseguire l'aggiornamento o il downgrade a un'altra versione software della stessa piattaforma o dello stesso modello.

Aggiunta di SMU bridge in un percorso di aggiornamento



Opzioni percorso di aggiornamento

1. Dopo aver aggiunto un percorso di aggiornamento, selezionare l'icona Altre opzioni. Vengono visualizzate le opzioni Elimina percorso (Delete Path) e Aggiungi SMU bridge (Add Bridge SMUs).

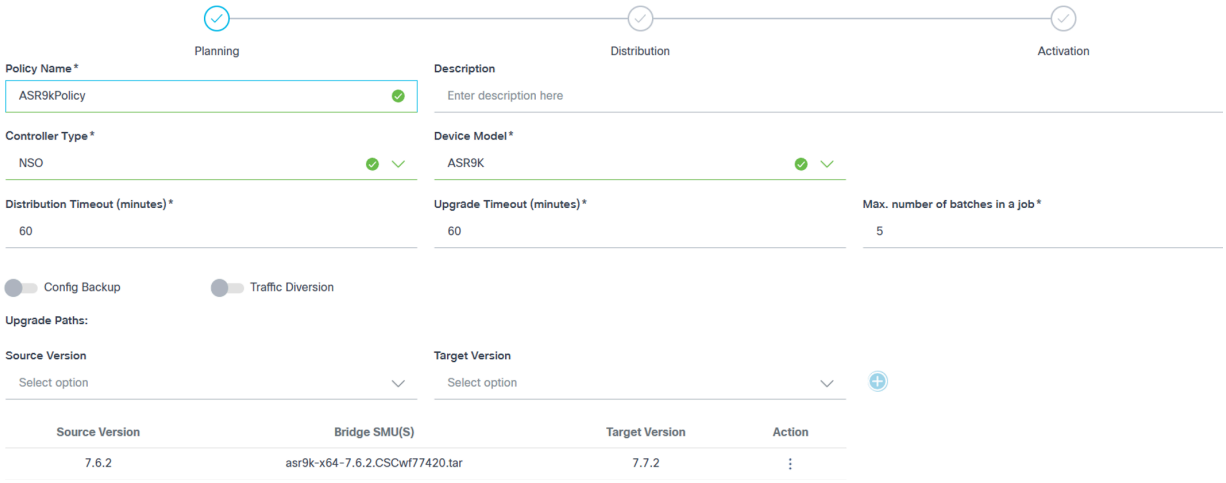


Aggiungi SMU bridge

2. Selezionate Aggiungi SMU bridge. Viene visualizzata la finestra Aggiungi SMU bridge. Tutte le SMU di Bridge disponibili vengono visualizzate per il percorso di aggiornamento specificato.

Aggiungi SMU bridge

3. Nella finestra Add Bridge SMUs, selezionate le caselle di controllo appropriate per aggiungere le SMU Bridge o deselezionate le caselle di controllo per rimuoverle. Dopo aver aggiunto le SMU del bridge, il percorso di aggiornamento viene aggiornato con i dettagli selezionati per le SMU del bridge.



Percorso di aggiornamento con SMU Bridge

Nota: Ogni percorso di aggiornamento che include Bridge SMU è considerato un aggiornamento in due fasi nel percorso di aggiornamento. Per il percorso di aggiornamento illustrato nella figura precedente, il percorso di aggiornamento finale è:

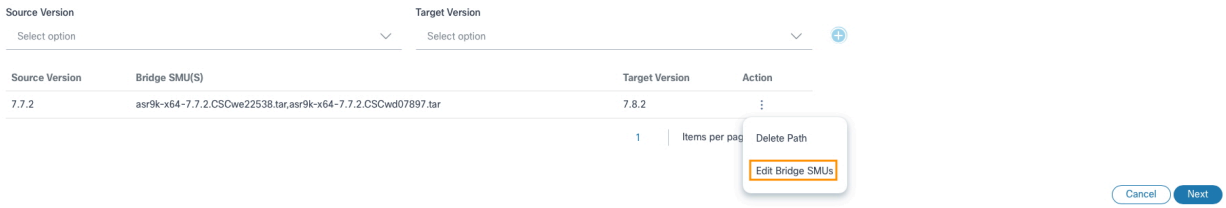
- 7.6.2 - 7.6.2 [SMU ponte]

Questo percorso rappresenta l'aggiornamento del dispositivo in esecuzione sulla versione 7.6.2 con le SMU di Bridge.

- 7.6.2 [SMU ponte] - 7.7.2

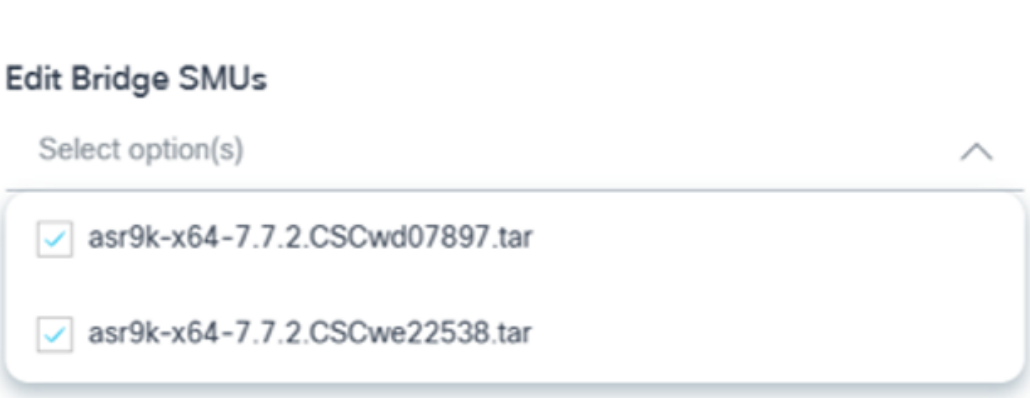
Questo percorso rappresenta l'aggiornamento del dispositivo dalla versione 7.6.2 alla versione 7.7.2. In questo caso, la versione di origine del dispositivo è la 7.6.2, inclusi i Bridge SMU applicati.

Modifica di SMU bridge



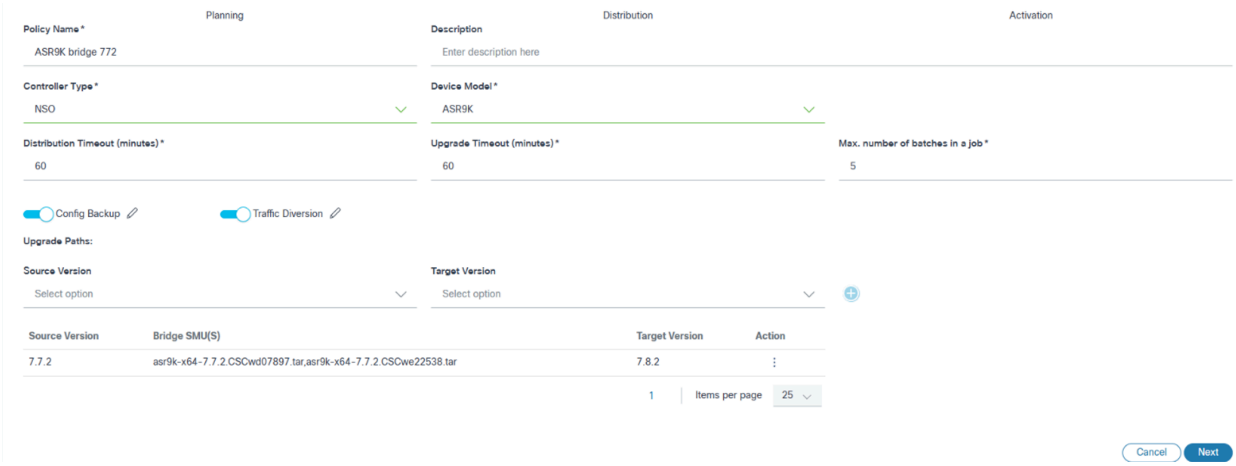
Percorso di aggiornamento con SMU Bridge

1. Nella sezione Percorsi di aggiornamento, selezionate l'icona Altre opzioni > Modifica SMU Bridge. Viene visualizzata la finestra Modifica SMU Bridge.



Modifica SMU bridge

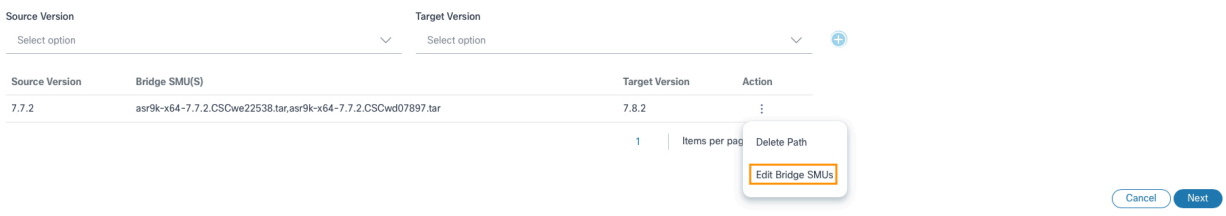
2. Selezionate o deselezionate le caselle di controllo appropriate per aggiornare le SMU di Bridge.
3. Fare clic su OK. Viene visualizzato un riepilogo delle modifiche.



Riepilogo delle modifiche

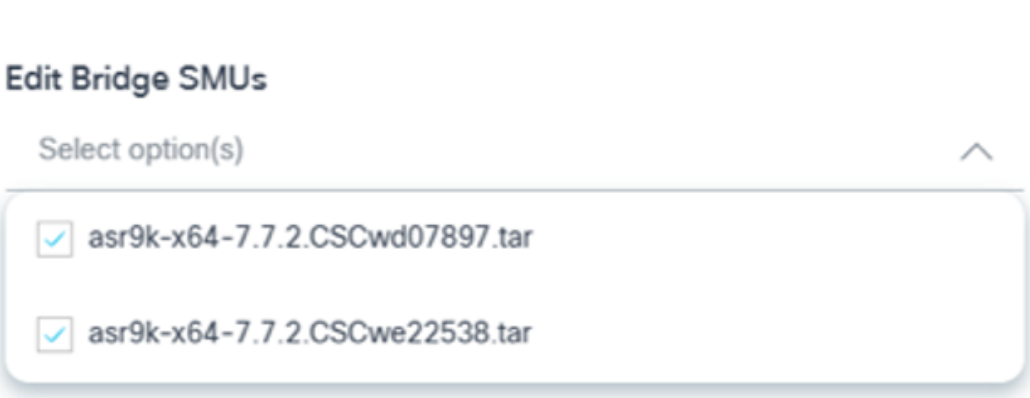
4. Verificare il riepilogo delle modifiche e fare clic su Avanti.

Eliminazione di SMU bridge



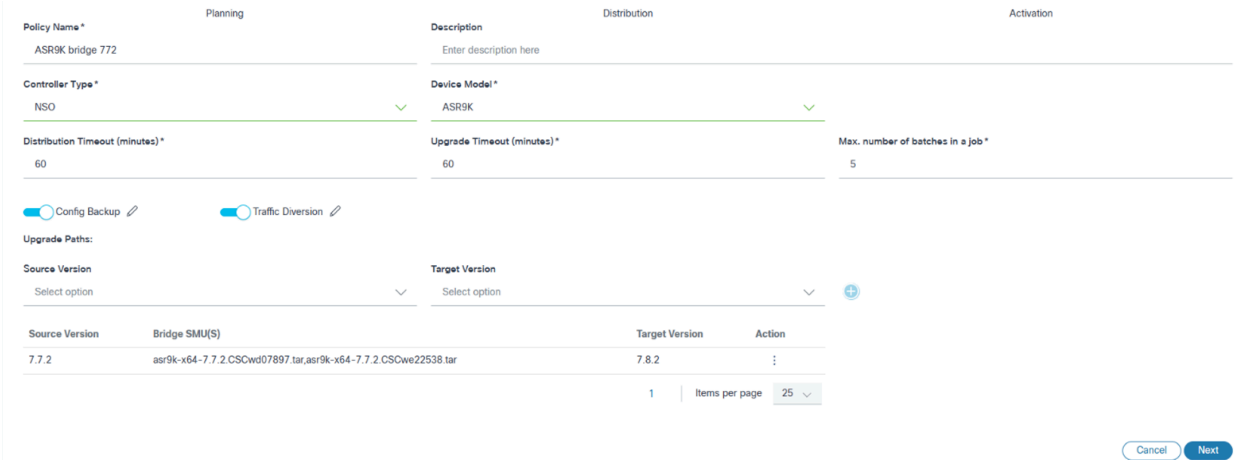
Modifica SMU bridge

1. Nella sezione Percorsi di aggiornamento, selezionate l'icona Altre opzioni > Modifica SMU Bridge. Viene visualizzata la finestra Modifica SMU Bridge.



Modifica SMU bridge

2. Deselezionate le caselle di controllo appropriate per rimuovere le SMU Bridge.
3. Fare clic su OK. Viene visualizzato un riepilogo delle modifiche.

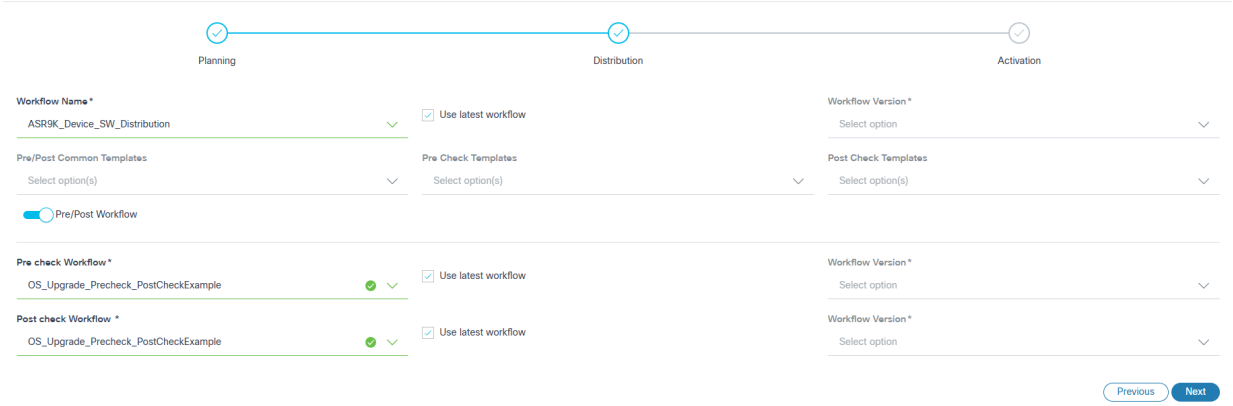


Riepilogo delle modifiche

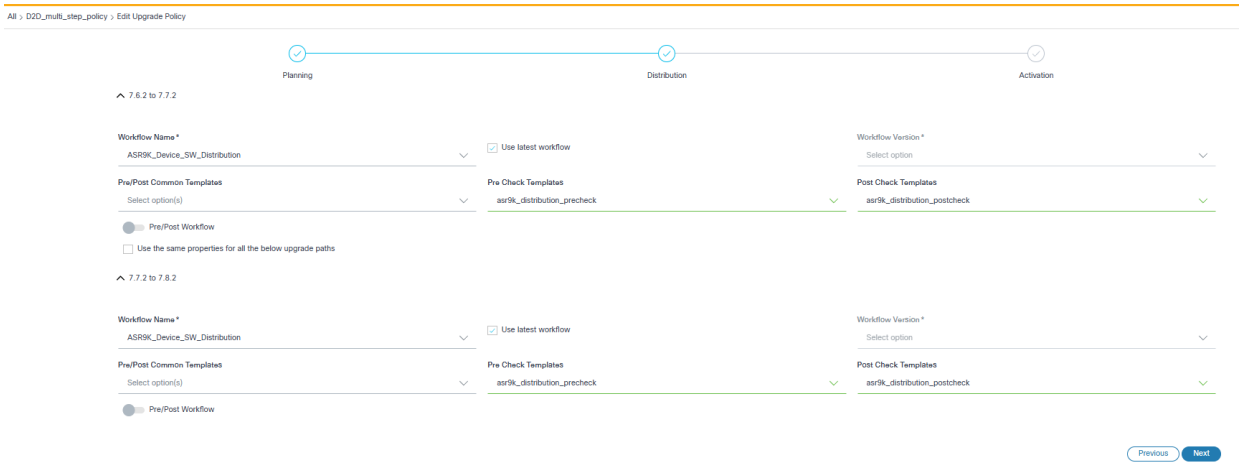
Distribuzione

La distribuzione accetta i parametri di input relativi alla distribuzione dell'immagine (ad esempio, la copia dell'immagine). Le immagini seguenti rappresentano i parametri di input necessari per ogni tipo di percorso di aggiornamento.

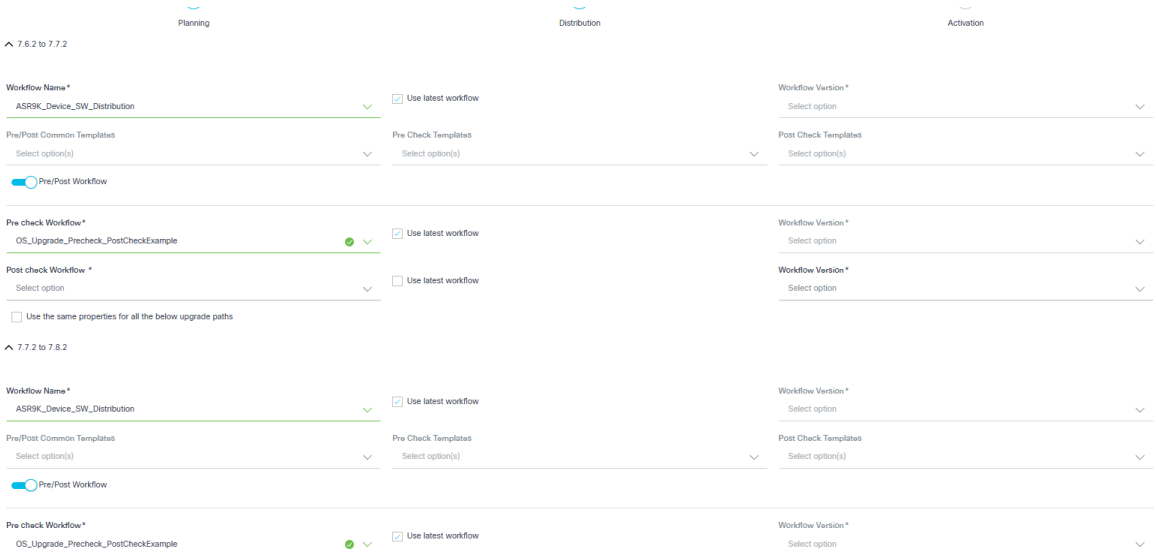
Sezione Distribuzione immagini - Aggiornamento in un unico passaggio



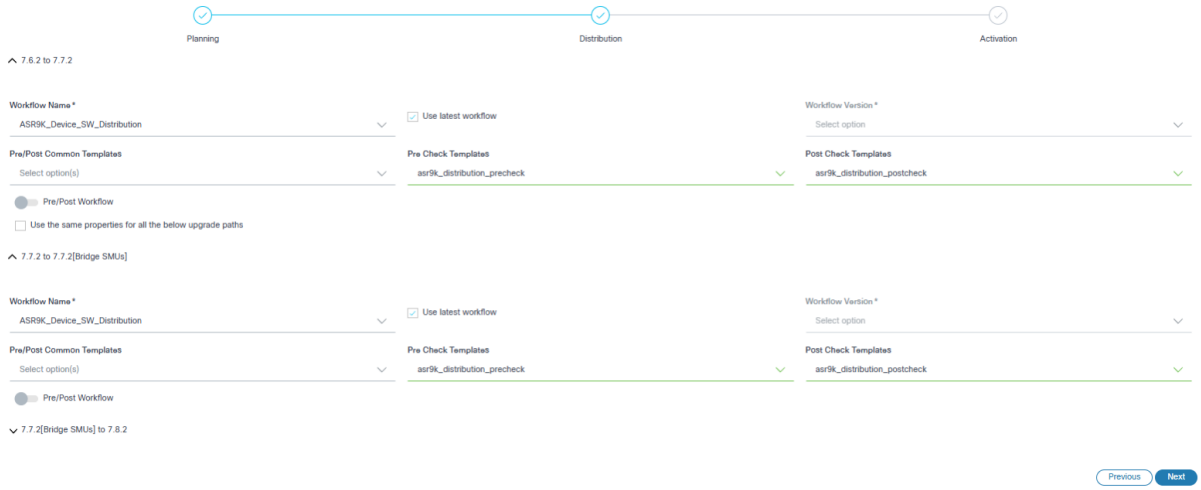
Sezione Distribuzione delle immagini - Aggiornamento in un unico passaggio con attivazione/disattivazione del flusso di lavoro precedente/successivo



Sezione Distribuzione - Aggiornamento in più passaggi



Sezione Distribuzione - Aggiornamento in più passaggi



Sezione Distribuzione - Aggiornamento Bridge SMU

1. Configurare i parametri relativi alla distribuzione delle immagini.
2. Nella tabella seguente viene fornita una breve descrizione di ogni campo.

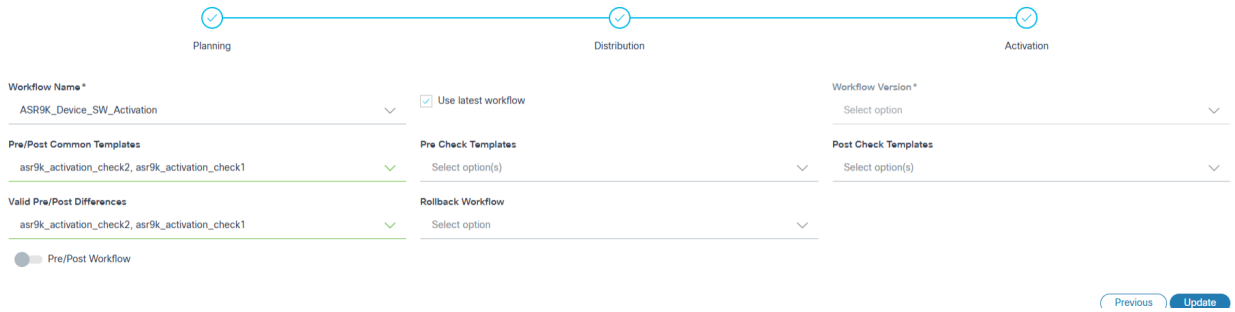
Campo	Descrizione
Nome workflow	Flusso di lavoro di distribuzione applicabile
Usa flusso di lavoro più recente	Selezionare la versione più recente del flusso di lavoro selezionato
Versione flusso di lavoro	La versione personalizzata del workflow; Questa opzione può essere selezionata solo se non è selezionata la casella di controllo Usa flusso di lavoro più recente
Modelli comuni pre/post	I modelli di processo eseguiti in entrambe le fasi (pre-controllo e post-controllo) Nota: I controlli sono specifici solo per la fase cardine di distribuzione. Fare riferimento ai modelli di processo per ulteriori informazioni
Attiva/disattiva flusso di lavoro pre/post	Consente agli utenti di selezionare l'esecuzione dei flussi di lavoro di pre- o post-controllo all'interno della fase cardine di distribuzione. Quando l'interruttore è attivato, è possibile configurare solo i flussi di lavoro pre- o post-controllo.
Flusso di lavoro pre-controllo	Include i comandi eseguiti esclusivamente durante la fase di pre-controllo. Nota: Questi controlli sono specifici della fase cardine di distribuzione.

Campo	Descrizione
Flusso di lavoro post-controllo	Il flusso di lavoro post-controllo comprende i comandi eseguiti in modo univoco durante la fase di post-controllo. Nota: Questi controlli sono specifici della fase cardine di distribuzione.
Modelli di pre-controllo	i modelli di processo che contengono comandi di pre-controllo esclusivi; i modelli vengono eseguiti solo durante la fase di pre-controllo. Nota: I controlli sono specifici solo per la fase cardine di distribuzione.
Modelli post-controllo	I modelli di processo che contengono comandi di post-controllo esclusivi; i modelli vengono eseguiti solo durante la fase successiva al controllo. Nota: I controlli sono specifici solo per la fase cardine di distribuzione.
Utilizzare le stesse proprietà per tutti i percorsi di aggiornamento seguenti	Le proprietà coerenti vengono applicate a tutti i percorsi di aggiornamento in aggiornamenti a selezione multipla. Nota: Se l'opzione è selezionata, le stesse proprietà vengono applicate a tutti i percorsi di aggiornamento nell'aggiornamento a selezione multipla.

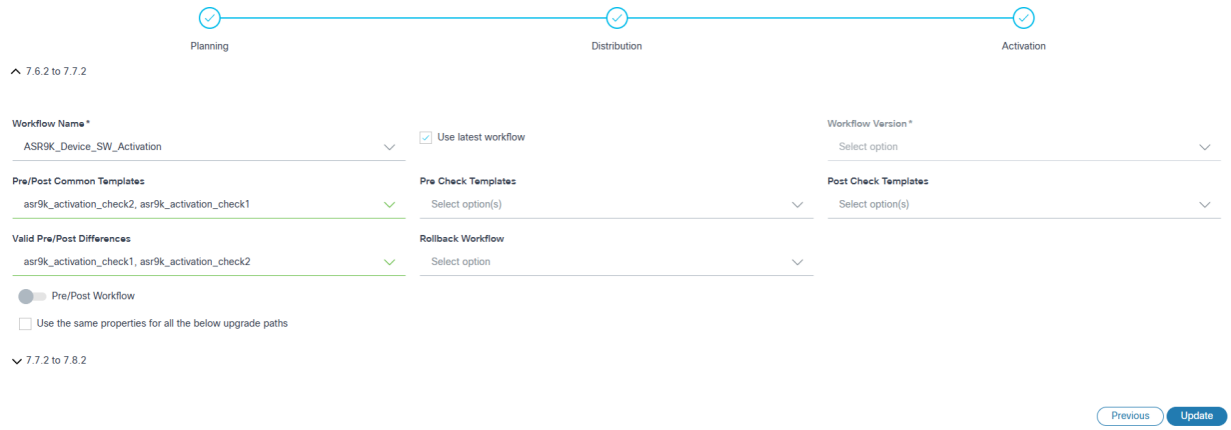
Nota: I workflow o i modelli di processo devono essere contrassegnati correttamente con il tag di aggiornamento del sistema operativo di nuova generazione.

3. Fare clic su Next (Avanti) per passare alla sezione Activation (Attivazione).

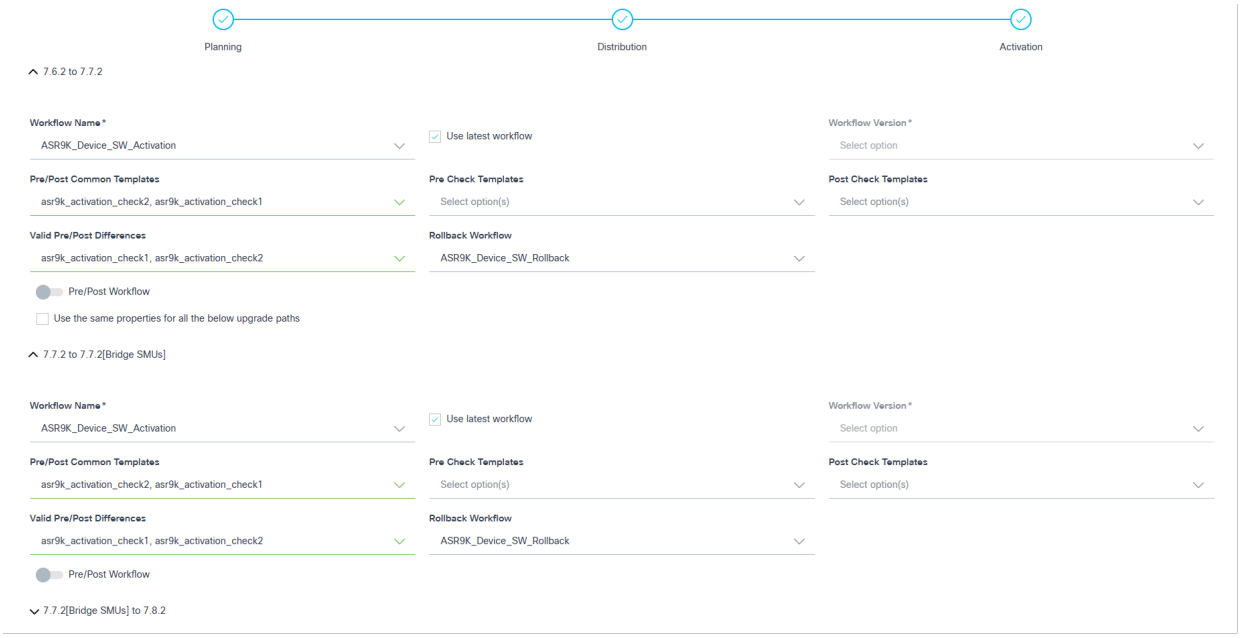
Attivazione



Sezione Attivazione - Aggiornamento in un unico passaggio



Sezione Attivazione - Aggiornamento in più passaggi



Sezione Attivazione - Aggiornamento Bridge SMU

1. Configurare i parametri relativi all'attivazione dell'immagine.
2. Nella tabella seguente viene fornita una breve descrizione di ogni campo.

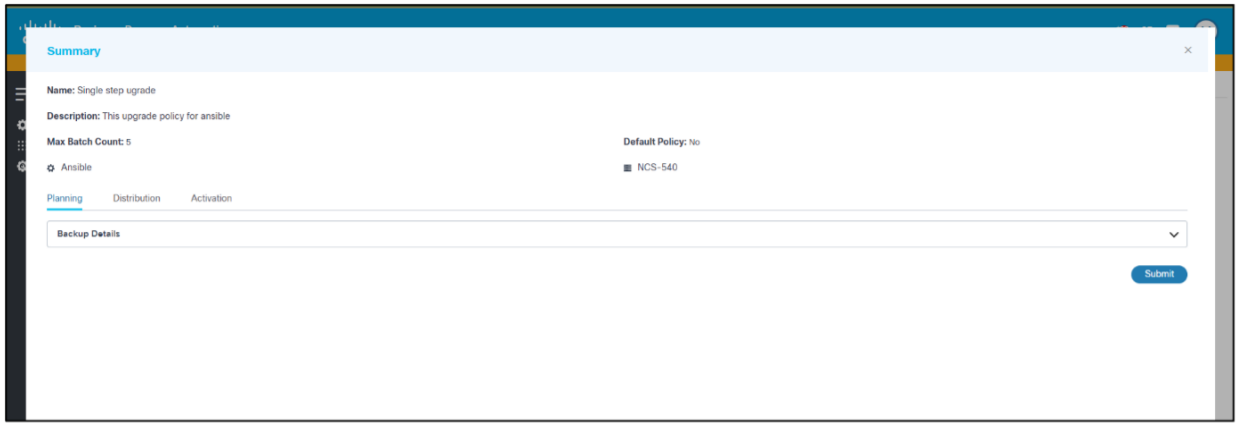
Campo	Descrizione
Nome workflow	Flusso di lavoro di attivazione applicabile
Usa flusso di lavoro più recente	Selezionare la versione più recente del flusso di lavoro selezionato
Versione flusso di lavoro	La versione personalizzata del workflow; può essere selezionato solo se non è selezionata la casella di controllo Usa il flusso di lavoro più recente
Modelli comuni pre/post	I modelli di processo eseguiti in entrambe le fasi (pre-controllo e post-controllo). Nota: I controlli sono specifici solo della fase cardine Attivazione.

Campo	Descrizione
Modelli di pre-controllo	Fare riferimento ai modelli di processo per ulteriori informazioni i modelli di processo che contengono comandi di pre-controllo esclusivi; i modelli vengono eseguiti solo durante la fase di pre-controllo. Nota: I controlli sono specifici solo della fase cardine Attivazione.
Modelli assegno post	I modelli di processo che contengono comandi di post-controllo esclusivi; i modelli vengono eseguiti solo durante la fase successiva al controllo. Nota: I controlli sono specifici solo della fase cardine Attivazione.
Differenza pre/post valida	I modelli di processo selezionati per ignorare le differenze. Nota: I controlli sono specifici solo della fase cardine Attivazione.
Ripristina flusso di lavoro	Flusso di lavoro di rollback applicabile. Nota: Se uno dei percorsi di aggiornamento con il flusso di lavoro di rollback è selezionato nel processo di aggiornamento a selezione multipla, tutti gli altri passaggi dell'aggiornamento vengono selezionati con il flusso di lavoro di rollback per impostazione predefinita.
Flusso di lavoro pre-controllo	Questo flusso di lavoro di pre-controllo personalizzato è costituito da comandi specifici i cui risultati di esecuzione possono essere selezionati ed esaminati. Essa è effettuata soltanto durante la fase di pre-controllo. Nota: Questi controlli sono specifici della fase cardine di attivazione.
Flusso di lavoro post-controllo	Questo flusso di lavoro personalizzato post-controllo è costituito da comandi specifici i cui risultati di esecuzione possono essere selezionati e rivisti. Essa è effettuata soltanto nella fase successiva al controllo. Nota: Questi controlli sono specifici della fase cardine di attivazione.
Utilizzare le stesse proprietà per tutti i percorsi di aggiornamento seguenti	Le proprietà coerenti vengono applicate a tutti i percorsi di aggiornamento in aggiornamenti a selezione multipla. Nota: Se l'opzione è selezionata, le stesse proprietà vengono applicate a tutti i percorsi di aggiornamento nell'aggiornamento a selezione multipla.

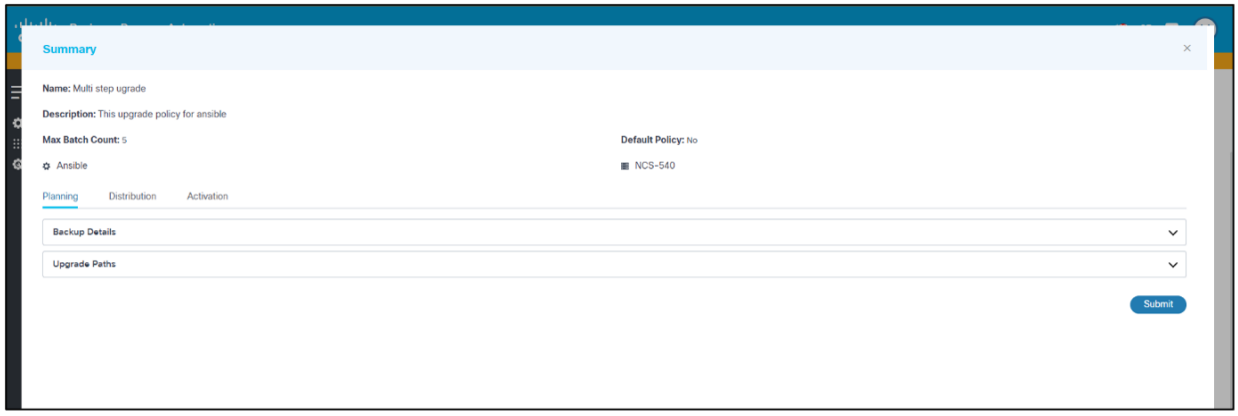
Nota: Si noti quanto segue:

- L'algoritmo a chiave pubblica richiesto per i dispositivi Nexus deve essere configurato in NSO.
- Configurare le funzionalità di bgp, bfd e hsrp in modo da eseguire i modelli di pre- e post-controllo nei dispositivi Nexus.

3. Fare clic su Crea. Verrà visualizzato un riepilogo dei campi.



Riepilogo - Criteri di aggiornamento in un unico passaggio



Riepilogo - Criteri di aggiornamento in più passaggi

4. Verificare il riepilogo dei campi e fare clic su Invia. Viene visualizzata una notifica di stato seguita da un messaggio di conferma. I criteri sono visibili nella pagina al momento della creazione.

Se necessario, è possibile creare ulteriori criteri di aggiornamento per altri modelli di dispositivi.

Modifica dei criteri di aggiornamento

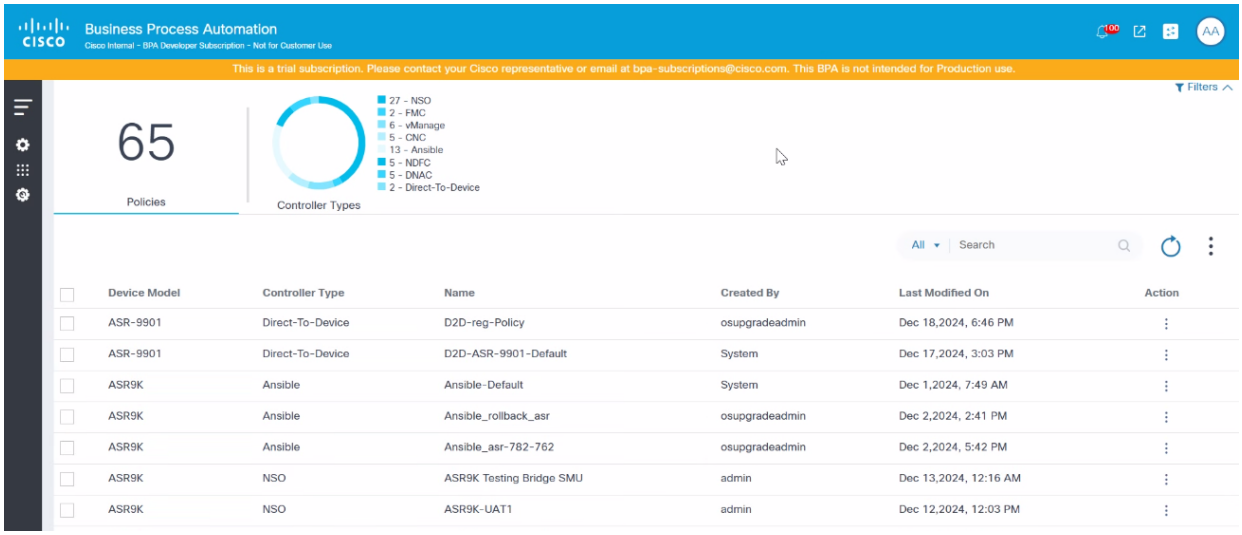
Risultati della ricerca dei criteri di aggiornamento

1. Dalla pagina Criteri di aggiornamento, individuare il criterio desiderato utilizzando il campo Cerca.

Modifica criteri di aggiornamento

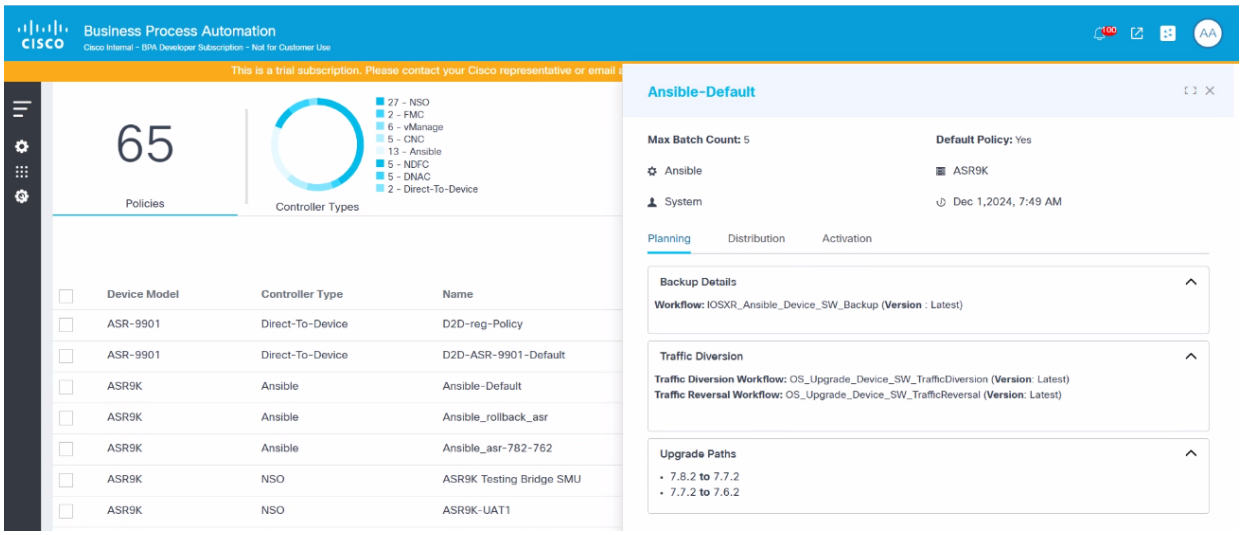
2. Dalla colonna Azione del criterio, selezionare l'icona Altre opzioni > Modifica.
3. Aggiornare i campi pertinenti e fare clic su Aggiorna. Viene visualizzato un riepilogo delle modifiche.
4. Verificare il riepilogo delle modifiche e fare clic su Invia. Vengono visualizzate notifiche di stato seguite da un messaggio di conferma.

Visualizzazione dei criteri di aggiornamento



Criteri di aggiornamento

1. Dalla pagina Criteri di aggiornamento, selezionare la riga del criterio di aggiornamento desiderato. Viene visualizzata la vista dei dettagli del criterio.



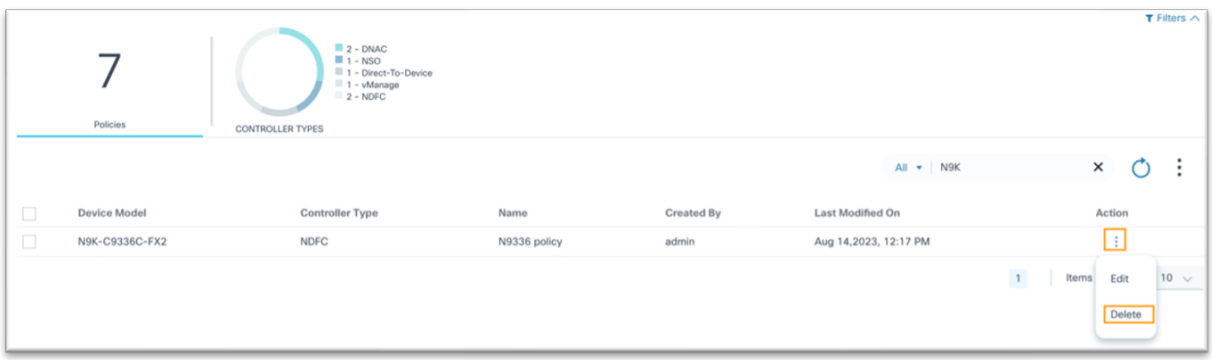
Visualizzazione dettagli criteri di aggiornamento

Eliminazione dei criteri di aggiornamento

Nota: I criteri predefiniti non possono essere eliminati, ma gli utenti possono modificare i modelli di processo e i workflow.

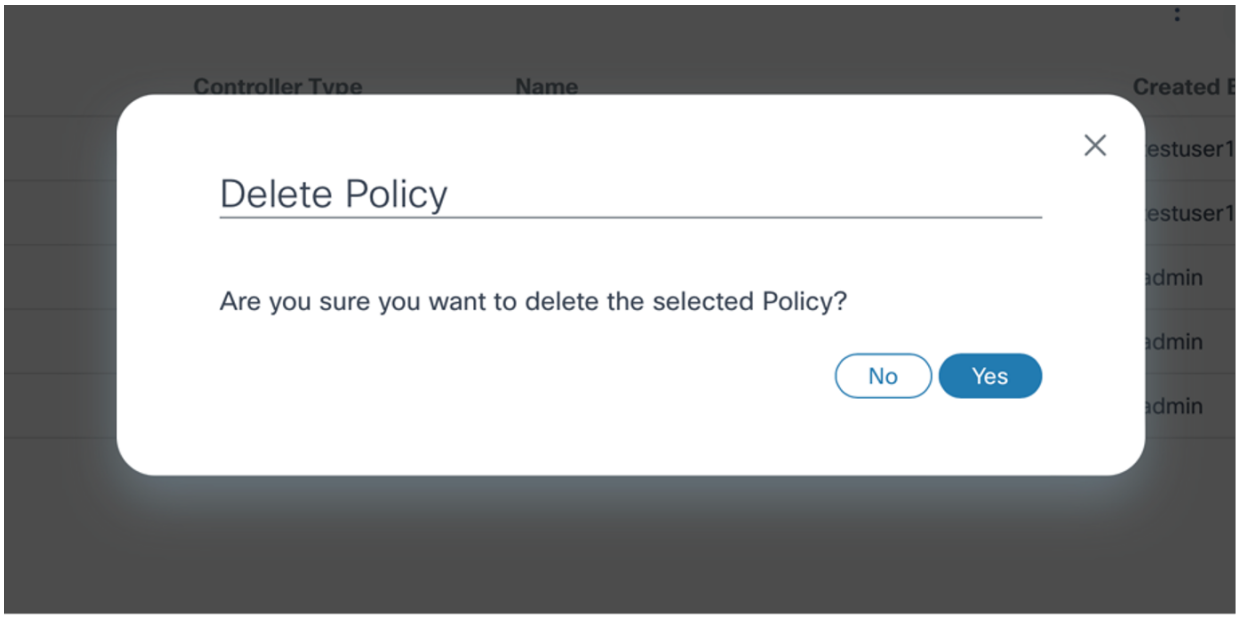
Criteri di aggiornamento

1. Dalla pagina Criteri di aggiornamento, individuare il criterio desiderato utilizzando il campo Cerca**.



Elimina criterio di aggiornamento

2. Dalla colonna Azione del criterio, selezionare Altre opzioni > Elimina. Viene visualizzata una finestra di conferma



Conferma eliminazione criterio

3. Fare clic su Sì.

Controllo dell'accesso ai criteri di aggiornamento

Questa funzionalità fornisce il controllo dell'accesso per i criteri di aggiornamento, limitando gli utenti non autorizzati ad aggiornare i criteri definiti nell'applicazione Aggiornamento del sistema operativo. Gli amministratori possono limitare l'accesso definendo un gruppo di risorse con criteri accessibili.

Per creare un gruppo di risorse:

1. Passare a Impostazioni > Gruppi di risorse.
2. Crea un gruppo di risorse con criteri a cui possono accedere utenti non amministratori. Gli utenti non amministratori che appartengono a questo gruppo di utenti possono ora accedere solo ai criteri disponibili in questo gruppo di risorse.
3. Creare un criterio di accesso per associare il gruppo di risorse a un gruppo di utenti,

Per ulteriori informazioni, fare riferimento a Controllo di accesso.

Nota: Si noti quanto segue.

- È possibile che gli utenti selezionino i flussi di lavoro non corretti per la distribuzione e l'attivazione, determinando un comportamento non intenzionale. È responsabilità dell'utente mappare correttamente il flusso di lavoro e verificare l'applicabilità per fasi cardine quali distribuzione, attivazione, rollback e modelli di dispositivo.
- I workflow e i modelli di processo devono essere mappati con il tag di aggiornamento del sistema operativo di nuova generazione affinché siano disponibili per la selezione durante la creazione o l'aggiornamento dei criteri.
- I criteri OOB predefiniti creati dall'utente di sistema non possono essere eliminati, ma gli utenti possono modificare i modelli di processo e i workflow.

Processi di aggiornamento

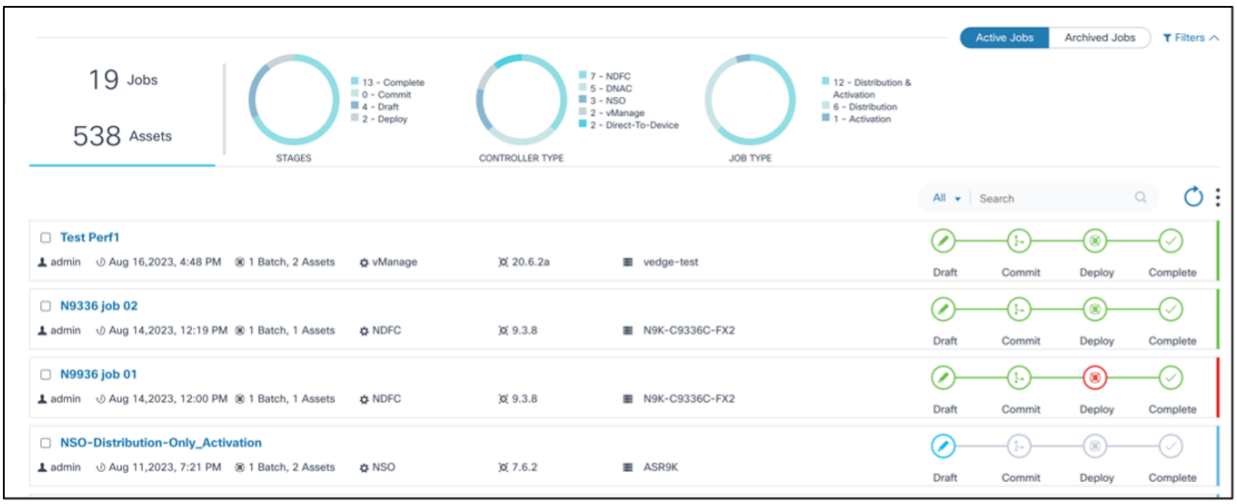
Gli aggiornamenti software vengono gestiti tramite l'applicazione Processo di aggiornamento, costituita da uno o più batch con uno o più dispositivi di rete per ogni batch. È possibile creare un processo in modalità bozza e salvarlo più volte. Gli aggiornamenti possono iniziare solo dopo il commit del job, consentendo agli operatori di pianificare in anticipo le modifiche.

Prerequisiti

- Finestra Manutenzione riservata per gli aggiornamenti
- Approvazioni preliminari per Richiesta di modifica aggiornamento
- Il servizio Backup e ripristino configurazione deve essere attivo e in esecuzione
- Il servizio di pianificazione deve essere attivo e in esecuzione
- Eventuali adattatori BPA per sistemi esterni (ad es., un sistema di biglietteria) devono essere integrati

Visualizzazione e gestione dei job di aggiornamento

1. Accedere a BPA con le credenziali che hanno accesso ai processi di aggiornamento.
2. Selezionare Aggiornamento sistema operativo > Processi di aggiornamento. Viene visualizzata la pagina Job di aggiornamento.



Processo di aggiornamento

La pagina Job di aggiornamento contiene le informazioni riportate di seguito.

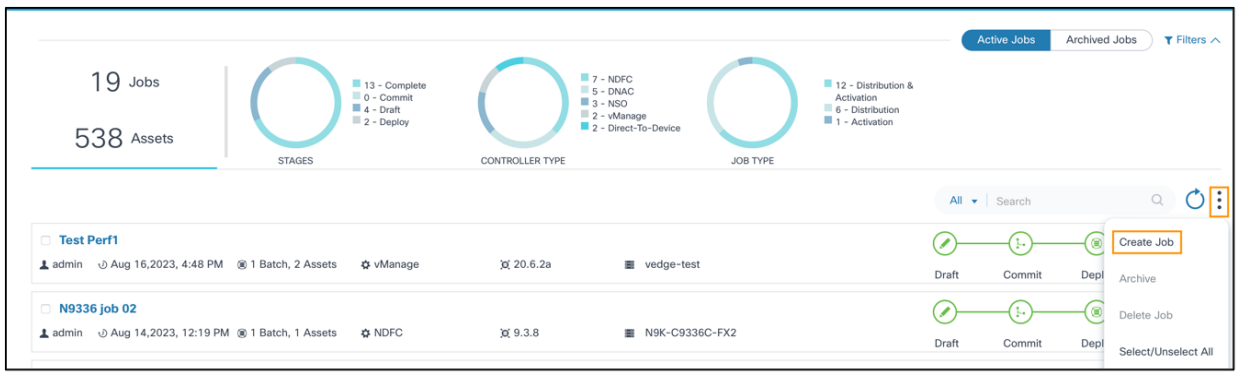
Nota: Per impostazione predefinita, vengono visualizzati dieci processi. I numeri di pagina possono essere utilizzati per passare ad altre pagine di job.

- Un'opzione Job attivi e Job archiviati può essere utilizzata per passare da un job attivo a uno archiviato e viceversa
- Una sezione di analisi, visualizzata nella parte superiore, che fornisce le informazioni riportate di seguito.
    - Totale processi e cespiti associati ai processi
    - Grafico Stadi con i filtri seguenti:
        - Bozza: Il processo è in fase di bozza e non è stato ancora eseguito
        - Commit: Il job viene eseguito con tutti i dispositivi, i batch o i programmi necessari fino al raggiungimento della programmazione
        - Implementazione: Attività di aggiornamento avviata per uno o più batch
        - Completa: Attività di aggiornamento completata per tutti i dispositivi appartenenti a tutti i batch
    - Grafico Tipo di controller: Consente di filtrare i processi per tipi di controller Cisco Catalyst Center, vManage, NSO, NDFC, Direct-to-Device, CNC, ANSIBLE e FMC
    - Grafico Tipi di job con i seguenti filtri:
        - Distribuzione: Processi che eseguono il posizionamento nell'area intermedia o la copia di immagini dal controller ai dispositivi
        - Attivazione: Processi che eseguono l'attivazione o l'aggiornamento del software di un dispositivo
        - Distribuzione e attivazione: Processi che eseguono sia la gestione temporanea o la copia che l'attivazione o l'aggiornamento del software di un dispositivo
- Il campo Cerca che può essere utilizzato per eseguire una ricerca generica tra tutti i metadati o dai campi Nome processo e Creato da

- L'icona Aggiorna che può essere utilizzata per aggiornare il riepilogo del job e cancellare i filtri del grafico o qualsiasi ricerca personalizzata nel campo Cerca
- L'icona Altre opzioni che fornisce le opzioni per creare un nuovo job di aggiornamento e per archiviare o eliminare i job selezionati; gli utenti possono selezionare o deselezionare Tutto
- I job vengono visualizzati come pannelli e forniscono una rapida visualizzazione delle seguenti informazioni:
    - L'icona Task utente viene visualizzata con il numero di task utente se sono disponibili task utente.
    - Utente che ha creato il processo
    - Data di creazione del processo
    - Numero di batch e cespiti
    - Tipo di controller (ad esempio, Cisco Catalyst Center, vManage, NDFC, Direct-to-Device, CNC, ANSIBLE o FMC)
    - Versione di destinazione
    - Il modello di dispositivo applicabile
    - Una vista cardine delle fasi del job (ad esempio Bozza, Conferma, Distribuisci e Completa) con una legenda a colori per ciascuna fase cardine:
        - Grigio: Cardine non avviata
        - Blu: Cardine in corso
        - Rosso: Problema cardine
        - Verde: Attività cardine completata
    - Una legenda a colori alla fine delle fasi cardine che visualizza lo stato del processo:
        - Verde: Processo completato
        - Rosso: Problemi del processo
        - Blu: Processo in corso

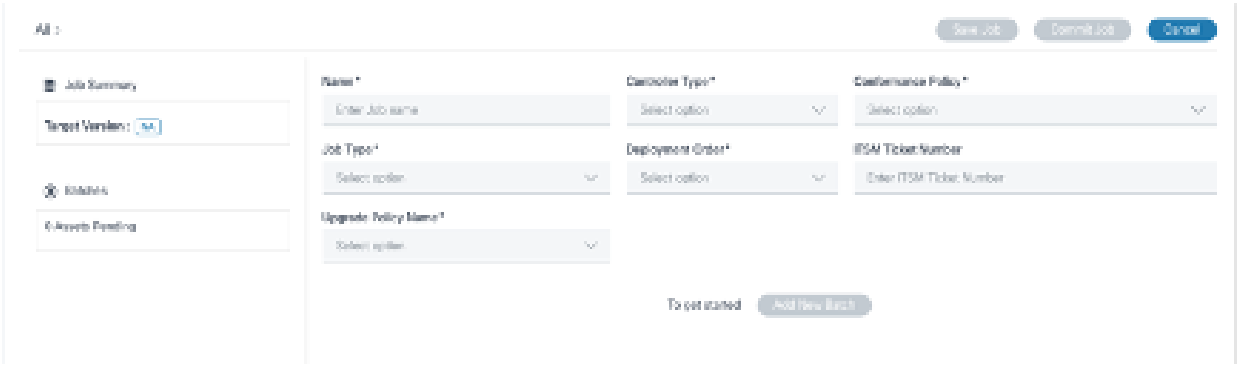
Pianificazione dei job di aggiornamento

Per creare un job:



Opzione Crea processo di aggiornamento

1. Dalla pagina Aggiorna job, selezionare l'icona Altre opzioni > Crea job. Viene visualizzata la pagina Crea job di aggiornamento.



Crea processo di aggiornamento

2. Immettere un nome di processo nel campo Nome.
3. Selezionare il tipo di controller (ad esempio, Cisco Catalyst Center, vManage, NDFC, Direct-to-Device, CNC, FMC, ANSIBLE o NSO).
4. Selezionare un criterio di conformità con dispositivi non conformi.

Nota: Nell'elenco sono disponibili solo i criteri di conformità che vengono eseguiti almeno una volta e che hanno almeno un dispositivo non conforme, identificando automaticamente i criteri di aggiornamento applicabili da utilizzare dopo la selezione di un criterio.

I dettagli riportati di seguito vengono visualizzati sul lato sinistro del modulo Crea processo in Riepilogo processo:

- Modelli di dispositivo interessati

Nota: Quando al criterio di conformità selezionato è associato più di un modello di dispositivo, vengono visualizzati più modelli di dispositivo.

- Versione di destinazione
- Aggregazione delle versioni di release esistenti e del numero corrispondente
- Numero massimo di batch consentiti
- Numero totale di attività non conformi

Nota: Se il criterio di conformità selezionato è associato a più modelli di dispositivo, visualizza l'aggregazione delle risorse non conformi per tutti i modelli associati.

- Opzione per l'aggiunta del batch

5. Selezionare uno dei tipi di processo di aggiornamento seguenti:

- Distribuzione: I job di sola distribuzione sono utili quando la gestione temporanea dell'immagine software avviene prima dell'attivazione effettiva
- Attivazione: I job di sola attivazione sono utili per eseguire gli aggiornamenti dei dispositivi la cui distribuzione è già stata completata tramite un job di sola distribuzione
- Distribuzione e attivazione: Sia la distribuzione che l'installazione di appoggio e l'attivazione delle immagini avvengono nell'ambito dello stesso processo, il che è utile negli scenari in cui è disponibile un'ampia finestra di manutenzione che copre sia la copia delle immagini su un dispositivo che l'aggiornamento

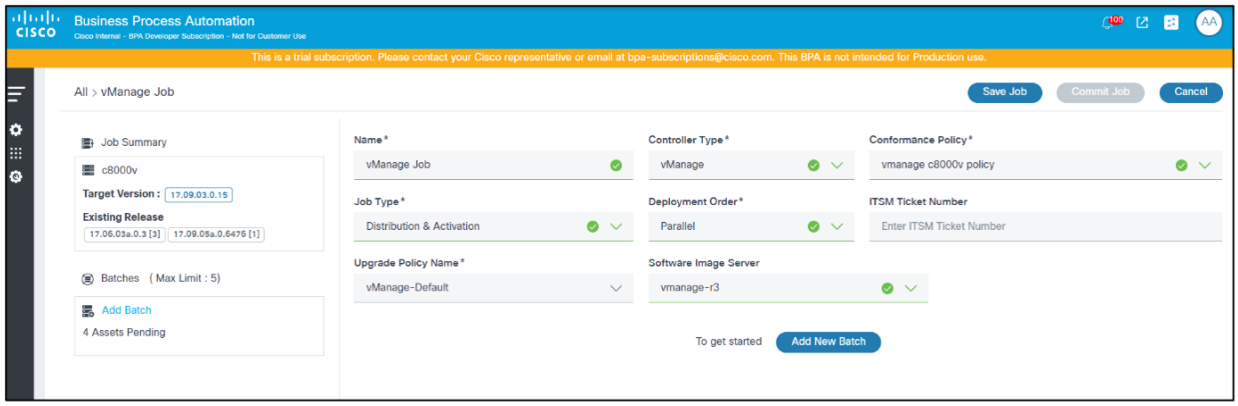
6. Selezionare l'ordine di aggiornamento. Più dispositivi vengono elaborati contemporaneamente in modalità parallela, mentre i dispositivi vengono elaborati singolarmente in modalità sequenziale.

Nota: Il numero massimo di dispositivi che possono essere elaborati in modalità parallela dipende dalla configurazione della distribuzione. L'ordine di aggiornamento selezionato è applicabile per l'intero processo, ma può essere ignorato all'interno di un batch specifico in base alle esigenze.

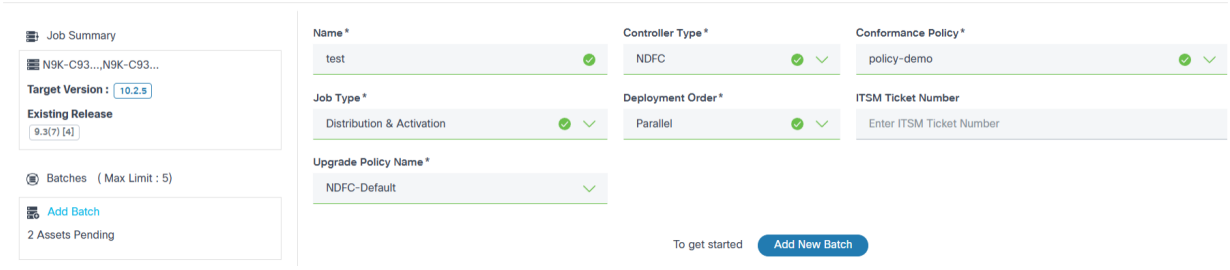
---

7. Aggiungere il numero di richiesta di modifica nel campo Numero ticket Gestione servizi IT (ITSM).
8. Selezionare il nome del criterio di aggiornamento. Vengono visualizzati solo i criteri di aggiornamento applicabili in base al tipo di controller e al modello di dispositivo dei criteri di conformità. gli utenti possono selezionare uno dei criteri di aggiornamento. Se al criterio di conformità software sono associati più modelli, verranno visualizzati tutti i criteri di aggiornamento associati a ogni modello. Gli utenti devono selezionare con attenzione il criterio di aggiornamento che funziona per tutti i modelli.
9. Selezionare il Software Image Server per specificare quale repository di immagini vManage (ad esempio, locale o remoto) utilizzare.

Nota: Questo input è applicabile solo al tipo di controller vManage.

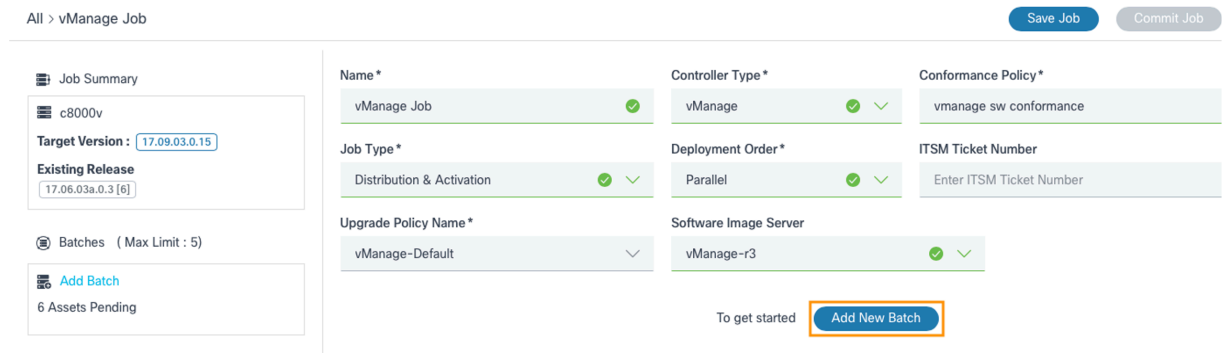


Crea processo di aggiornamento con dettagli completati (il criterio di conformità ha un modello)



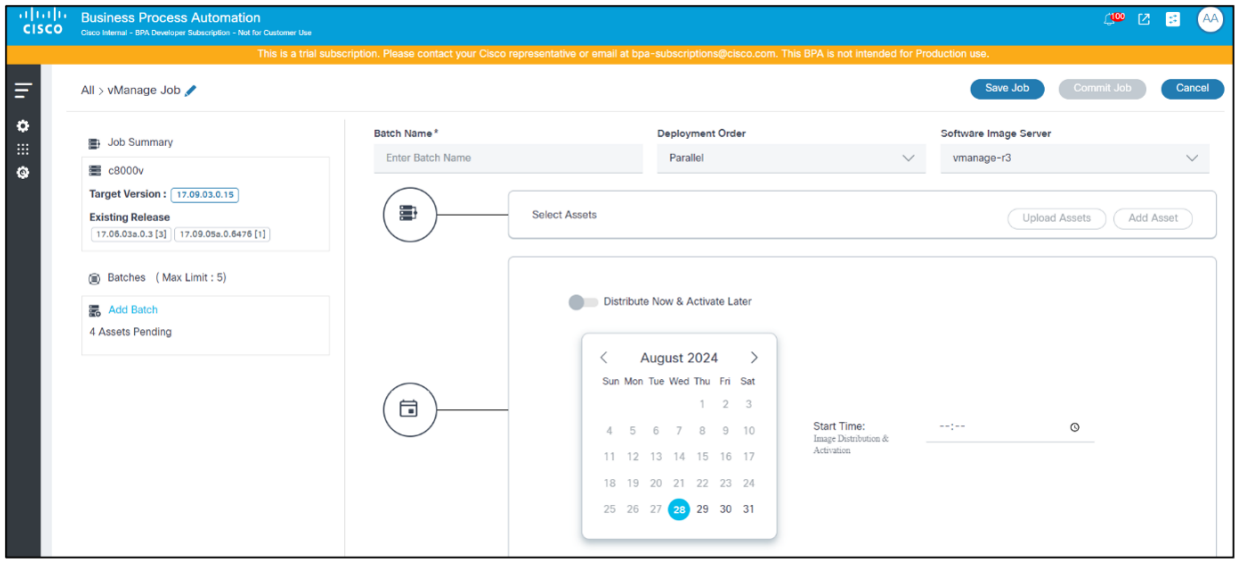
Crea processo di aggiornamento con dettagli completati (i criteri di conformità hanno più modelli)

10. Fare clic su Salva job per salvare la bozza fino a quando il job non è pronto per essere eseguito.



Aggiungi batch e Aggiungi nuovo batch

11. Per aggiungere un batch, fare clic sul collegamento Aggiungi batch o Aggiungi nuovo batch. Viene visualizzata la finestra Creazione batch.



Creazione batch

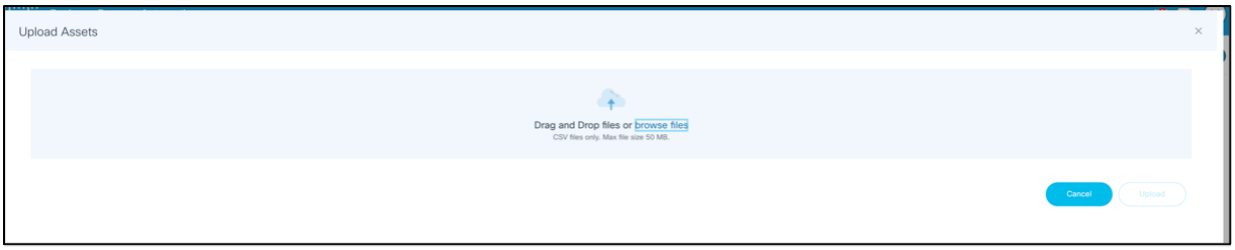
12. Immettere il nome del batch desiderato e selezionare l'ordine di distribuzione.

Nota: Il tipo di aggiornamento selezionato in questo punto ha la precedenza su quello selezionato nella pagina Creazione processo

13. Selezionare il Software Image Server per specificare quale repository vManage (ad esempio, locale o remoto) utilizzare.

Nota: Questo campo è valido solo per il tipo di controller vManage. Il Software Image Server selezionato in questo punto ha la precedenza su quello selezionato nella pagina Creazione processo

14. Aggiungere risorse ai batch. Gli asset possono essere aggiunti ai batch in due modi:



Carica risorse

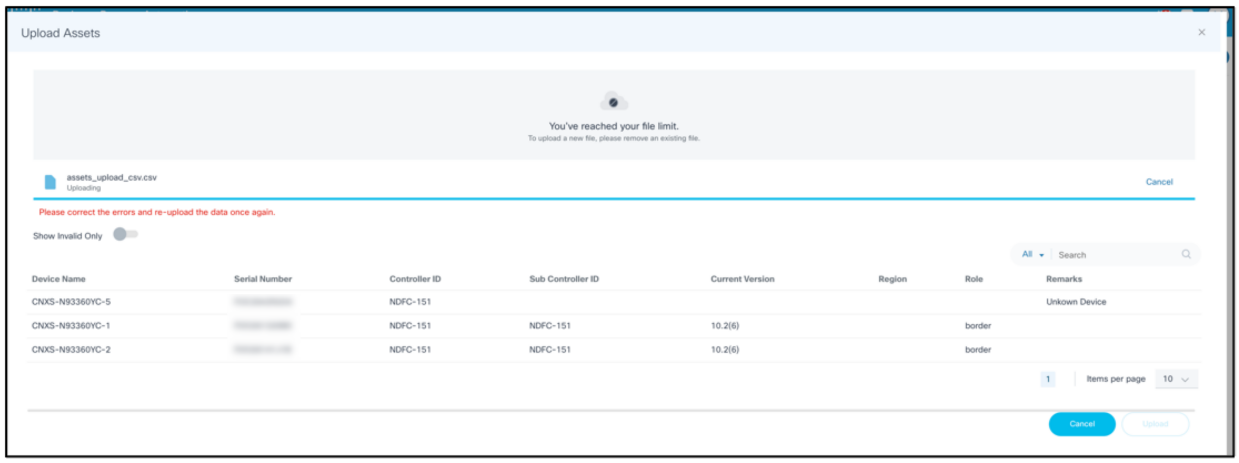
Opzione 1:

a. Fare clic su Carica risorse. Viene visualizzata la finestra Carica cespiti.
b. Selezionare un file CSV da caricare.

Nota: Il file .csv deve contenere i seguenti dettagli:

- Nome dispositivo: Nome del dispositivo o della risorsa
- Numero di serie: Numero di serie del dispositivo
- ID controller: Nome del controller che gestisce il dispositivo
- ID controller secondario: Nome dell'ID del controller secondario che gestisce il dispositivo

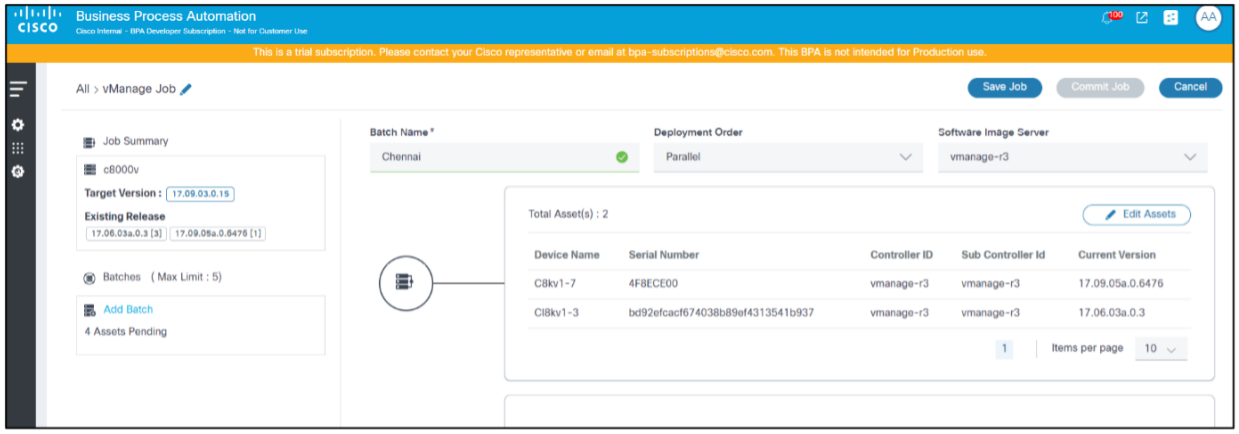
c. Fare clic su Upload. I dati del file con estensione csv vengono convalidati e vengono visualizzati sia i dati validi che quelli non validi. L'opzione Mostra solo non validi può essere utilizzata per filtrare i dispositivi non validi dai dettagli della risorsa caricata.



Risorse di esempio caricate tramite file CSV

d. In caso di errori nel file caricato, correggerli e caricarli nuovamente.

Nota: Gli utenti possono procedere con la selezione degli asset solo se tutti i dispositivi caricati sono validi.



Aggiungi batch - Risorse selezionate

Opzione 2:

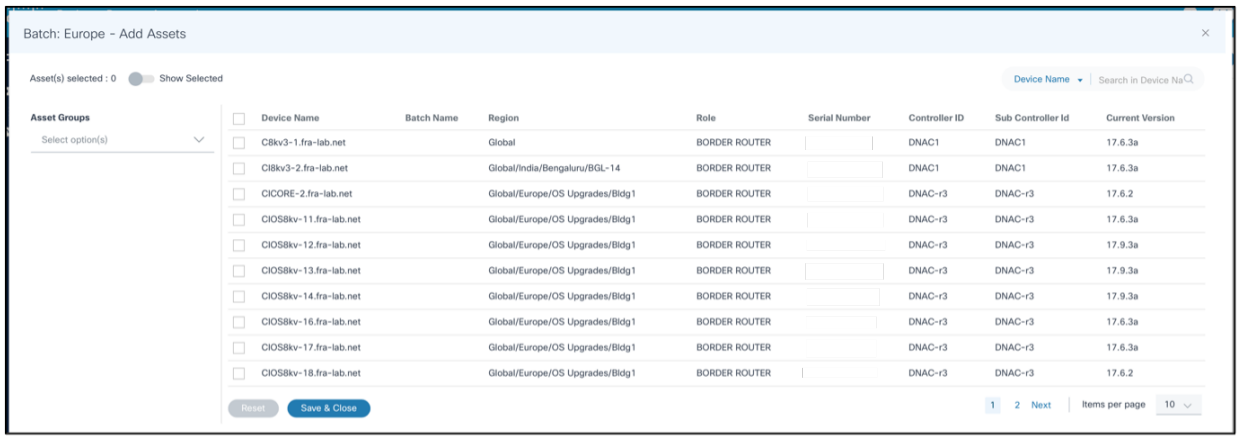
a. Fare clic su Aggiungi risorse. Viene visualizzata la finestra Selezione cespite.

Nota: Carica risorse e Aggiungi asset non possono essere utilizzati contemporaneamente.

b. Solo per il tipo di controller FMC, selezionare il nodo di controllo o il nodo autonomo per eseguire l'aggiornamento.

Nota: I dispositivi dati non sono consentiti nel processo di aggiornamento perché

l'aggiornamento dei nodi dati è gestito dal relativo nodo di controllo.



Selezione dispositivo

c. Selezionare i dispositivi appropriati da includere nel batch corrente.

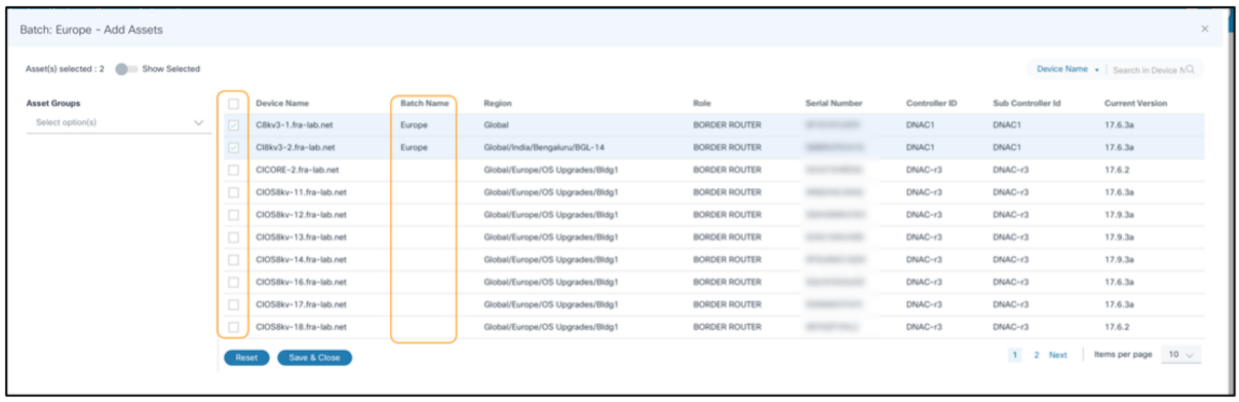
Il filtro Search (Cerca) può essere usato per filtrare i dispositivi in base ad attributi diversi e tutti i dispositivi che corrispondono ai criteri di filtraggio possono essere selezionati in blocco selezionando la casella di controllo nell'intestazione della colonna Device Name (Nome dispositivo). Gli utenti possono inoltre filtrare in base ai gruppi di asset.

L'opzione Mostra selezione (Show Selected) può essere attivata per visualizzare solo le risorse selezionate.

Nota: Quando l'interruttore Mostra selezione è abilitato, il filtro Asset Groups è disabilitato.

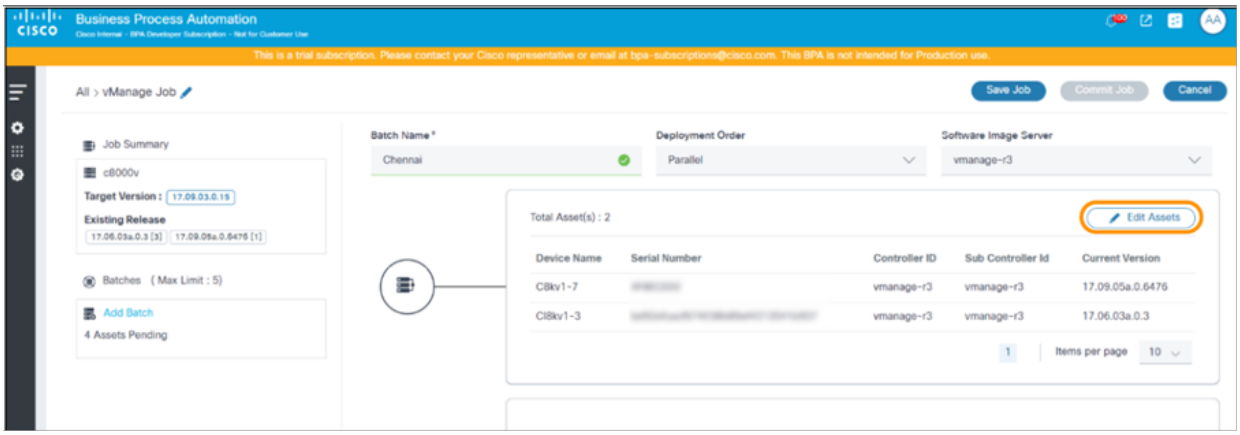
d. Fare clic su Salva e chiudi.

Se si fa clic su Reimposta, le selezioni vengono annullate e viene mantenuto lo stato originale della selezione di risorsa.



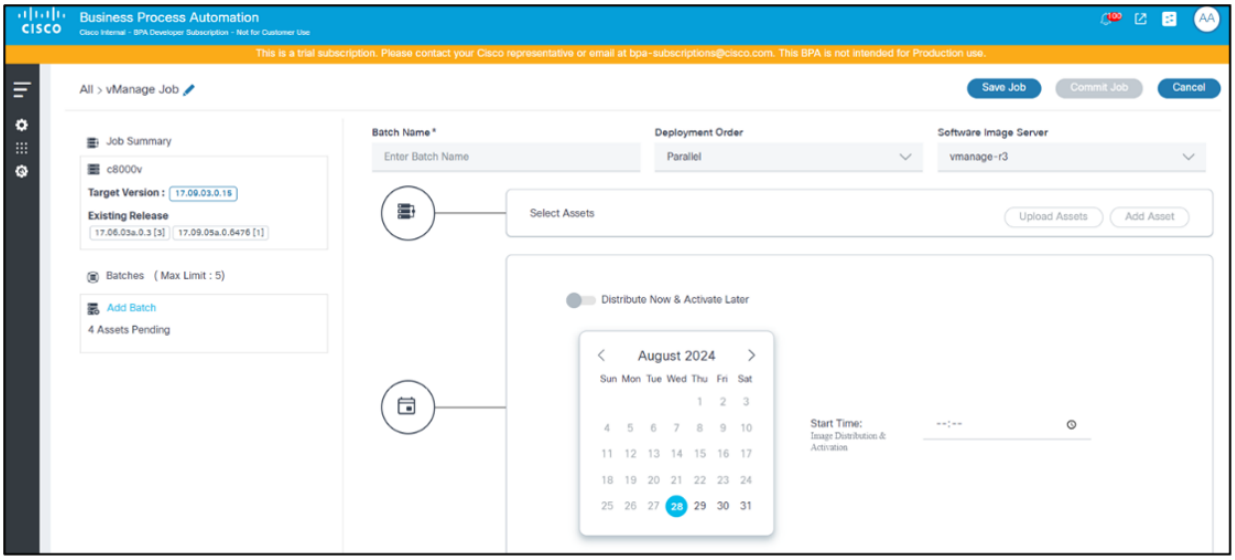
Reset

e. Se è necessario modificare la selezione delle risorse, fare clic su Modifica risorse.



Modifica in batch delle risorse

f. Selezionate o deselezionate le risorse per apportare le modifiche necessarie e fate clic su Salva e chiudi (Save and Close). Durante la modifica dei cespiti batch, i cespiti attualmente selezionati che fanno parte di un processo e di un batch diversi possono essere identificati mediante segni di spunta e il nome del batch visualizzato nella colonna Nome batch.



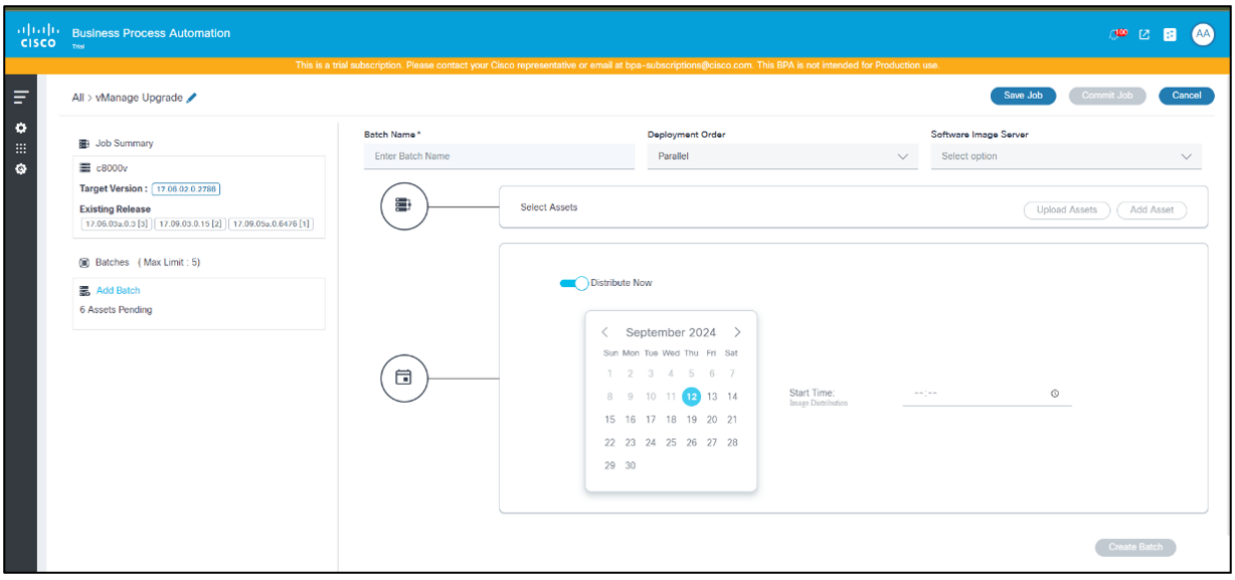
Pianificazione processi di aggiornamento

15. Selezionare una data dal controllo selezione data e un'ora dal controllo selezione ora per pianificare un'ora per attivare il tipo di aggiornamento selezionato per il batch corrente.

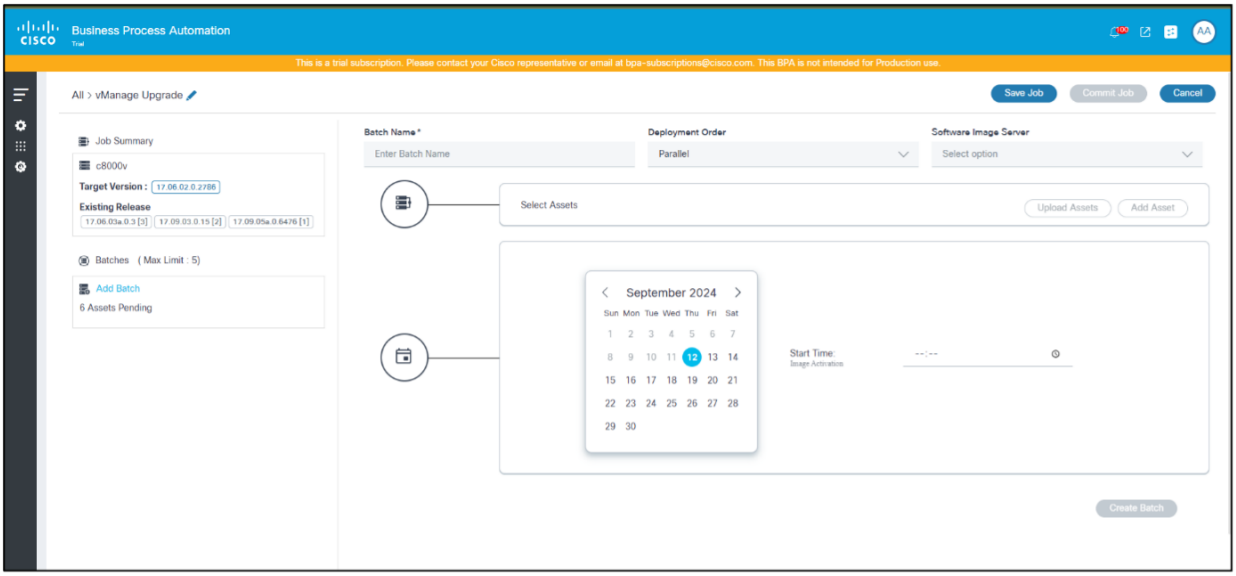
Nota: Il tipo di processo selezionato modifica il tipo di pianificazioni disponibili.

Gli scenari possibili sono i seguenti:

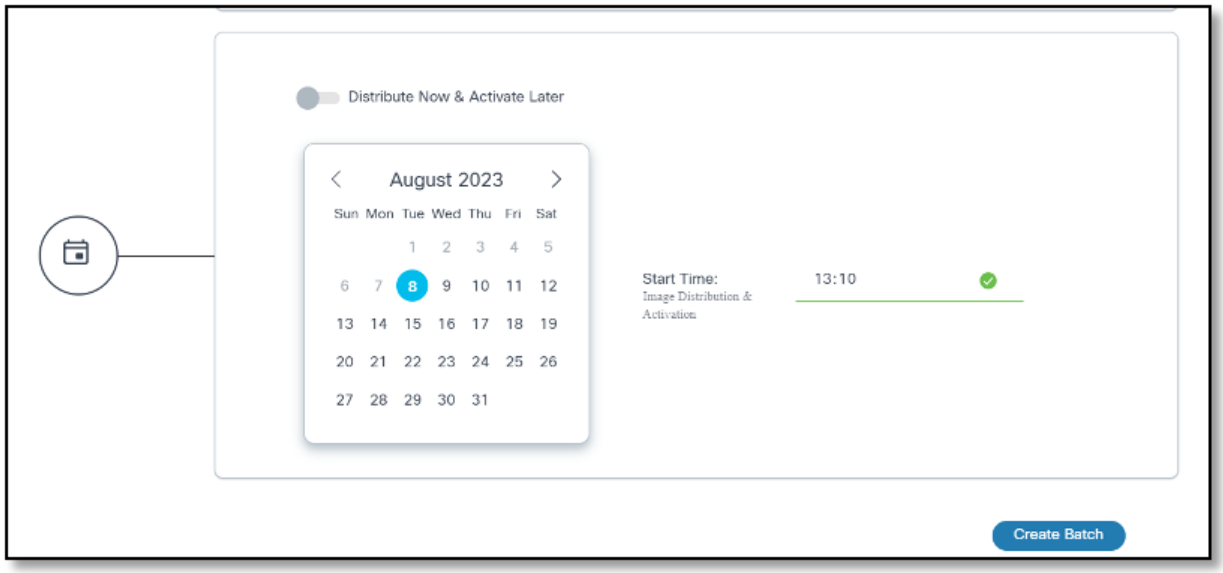
Tipo di processo	Attiva/disattiva distribuzione	Data e ora programmazione	Dettagli distribuzione
Distribuzione	Disattivato per impostazione predefinita	Active	La distribuzione viene eseguita nella data e ora pianificate specificate
Distribuzione	Attivato	Disabled	Distribuzione eseguita dopo il commit del processo
Attivazione	N/D	Active	L'attivazione viene eseguita alla data e all'ora specificate
Distribuzione e attivazione	Disattivato per impostazione predefinita	Active	La distribuzione e l'attivazione avvengono nella data e ora specificate
Distribuzione e attivazione	Attivato	Active	La distribuzione viene eseguita dopo il commit del processo e i trigger di attivazione alla data e all'ora pianificate specificate



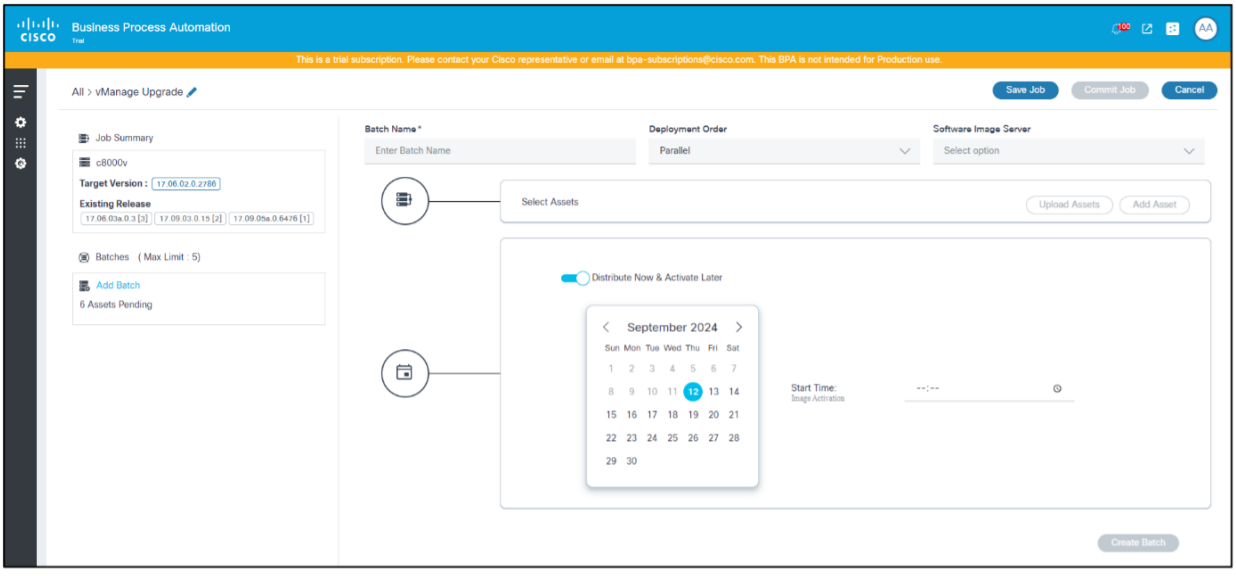
Opzioni di pianificazione per il tipo di job di distribuzione



Opzioni di pianificazione per il tipo di processo di attivazione



Opzioni di pianificazione per il tipo di processo di distribuzione e attivazione

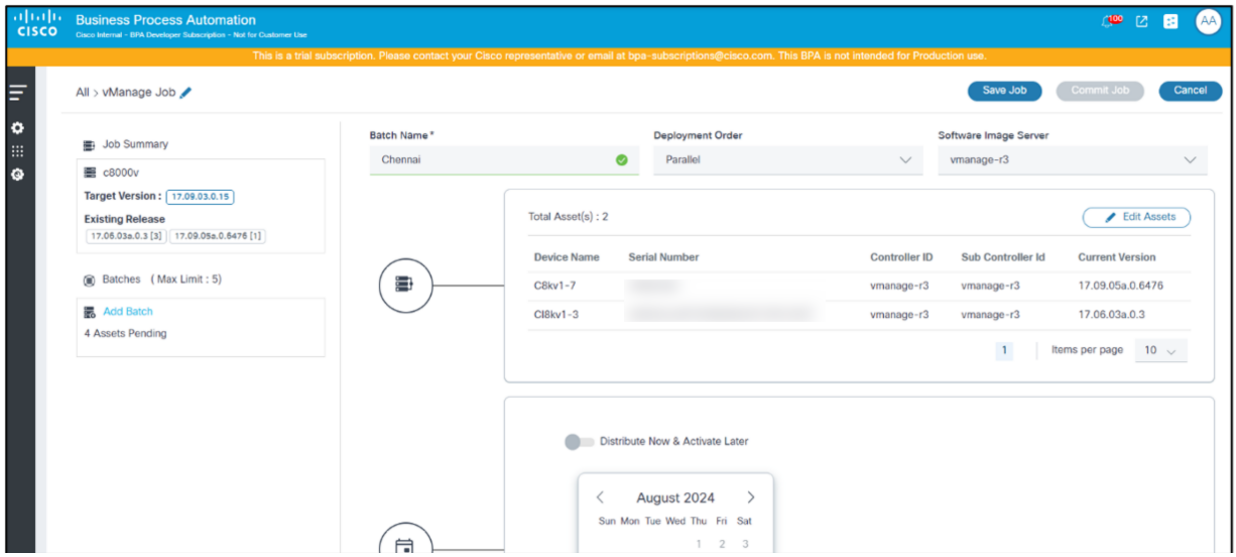


Opzioni di pianificazione per il tipo di processo di distribuzione e attivazione con l'opzione Distribuisci ora e attiva in seguito abilitata

Nota: Occorre prendere nota del seguente elenco.

- Quando si programmano più batch, prevedere un intervallo di tempo tra i due batch per evitare il sovraccarico del sistema. Se i batch multipli si sovrappongono, è consigliabile aggiungerli a un singolo batch.
- Quando l'opzione Distribuisci ora e attiva in seguito è abilitata, specificare un intervallo di tempo tra l'ora di commit del job e la pianificazione dell'attivazione. In caso contrario, i flussi di lavoro di attivazione potrebbero creare attività utente che richiedono un intervento manuale, ovvero gli utenti devono attendere il completamento della distribuzione e riprovare.

16. Fare clic su Crea batch. Il batch può essere visualizzato sul lato sinistro della pagina.



Crea processo - Commit processo

Creare tutti i batch necessari. Un processo può essere in stato Bozza finché non sono disponibili tutte le informazioni necessarie.

Nota: Per evitare la perdita dei dati del processo, fare clic su Salva processo per salvare la bozza.

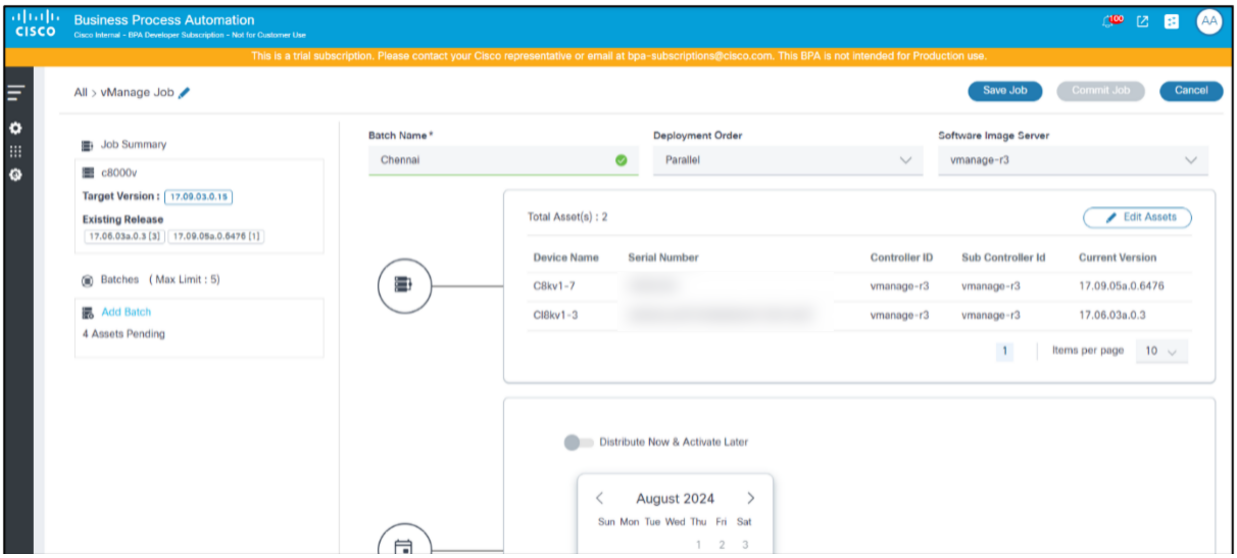
17. Fare clic su Conferma processo per completare la creazione del processo. Il job passa allo stato Distribuisci quando la programmazione viene attivata per uno qualsiasi dei batch.

Nota: La soglia per il numero massimo di batch può essere estesa o aggiornata nella pagina Criteri di aggiornamento.

Modifica di un batch in un processo

Nota: I batch possono essere aggiornati solo quando il job è in fase Bozza.

1. Selezionate il batch desiderato dal pannello sinistro.

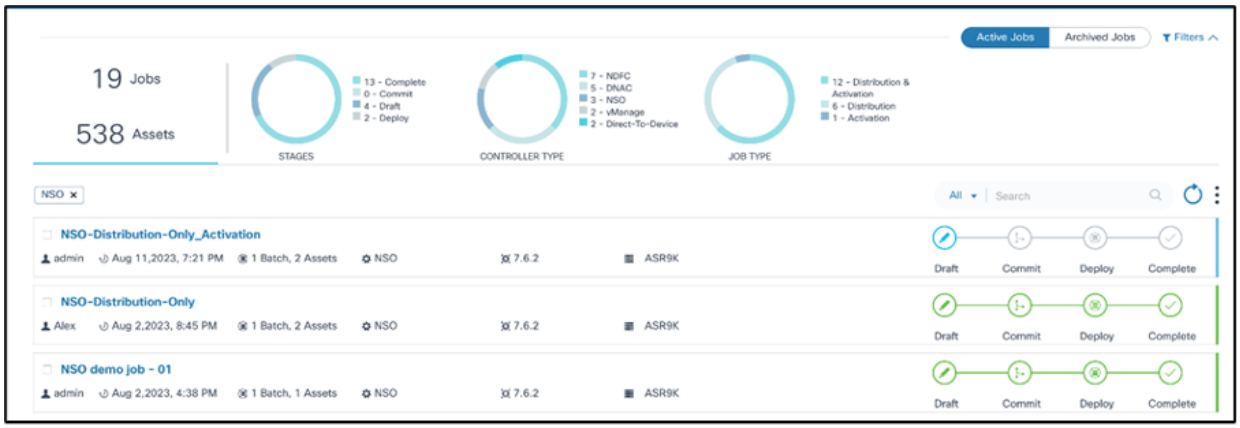


Modifica risorse

2. Fare clic su Modifica risorse.
3. Apportare le modifiche necessarie selezionando o deselezionando i cespiti in Aggiungi cespiti o Carica cespiti oppure modificando il programma batch apportando modifiche alla data o all'ora di inizio.
4. Fare clic su Aggiorna batch.

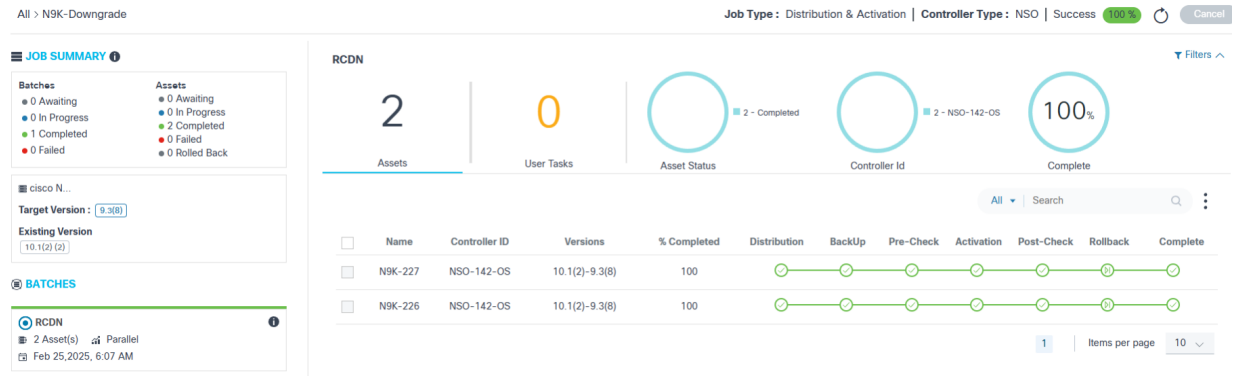
Esecuzione processo di aggiornamento e monitoraggio avanzamento

1. Accedere a BPA con le credenziali che hanno accesso ai processi di aggiornamento.
2. Selezionare Aggiornamento sistema operativo > Processi di aggiornamento. Viene visualizzata la pagina Job di aggiornamento.

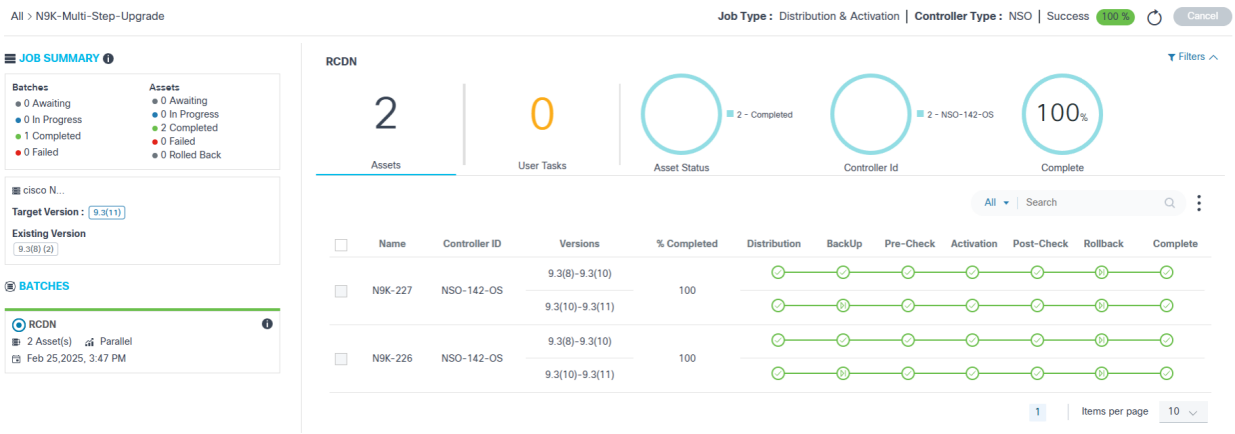


Processo di aggiornamento

3. Utilizzare il filtro Cerca in combinazione con i filtri grafici disponibili per filtrare rapidamente il processo.
4. Fare clic sul job desiderato. Viene visualizzata la pagina Riepilogo job.

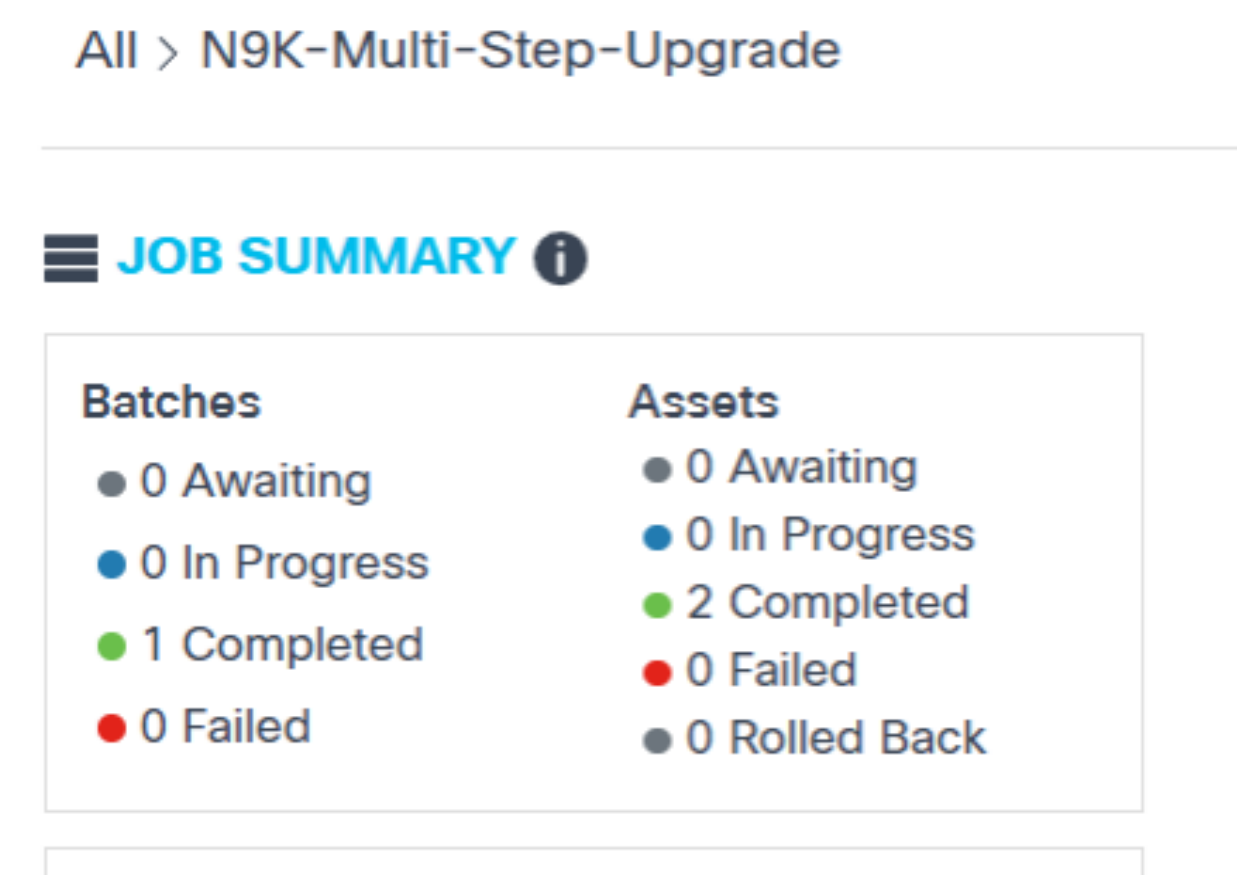


Aggiornamento in un unico passaggio



Aggiornamento in più passaggi

Il pannello sinistro fornisce le seguenti informazioni:



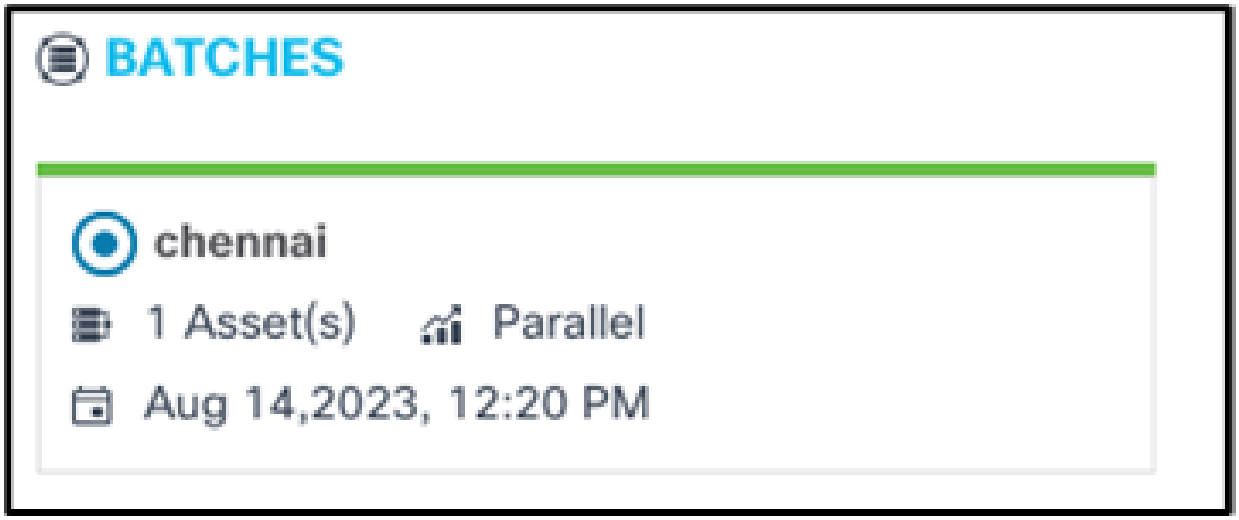
Riepilogo processi

- Breve riepilogo dei batch e dei rispettivi asset

Dettagli criteri di conformità (se i criteri dispongono di un modello)

Dettagli criteri di conformità (se i criteri dispongono di più modelli)

- Il modello di dispositivo interessato dal processo, la versione del software di destinazione e la versione di rilascio esistente
- Elenco di batch che fanno parte di questo processo



Dettagli batch

- Dettagli batch:
  - Il bordo superiore grigio indica che il batch è in attesa della programmazione
  - Il bordo superiore blu indica che la distribuzione batch è in corso
  - Il bordo superiore verde indica che la distribuzione batch è stata completata

Nella parte superiore della pagina Riepilogo job vengono visualizzate le informazioni riportate di seguito.

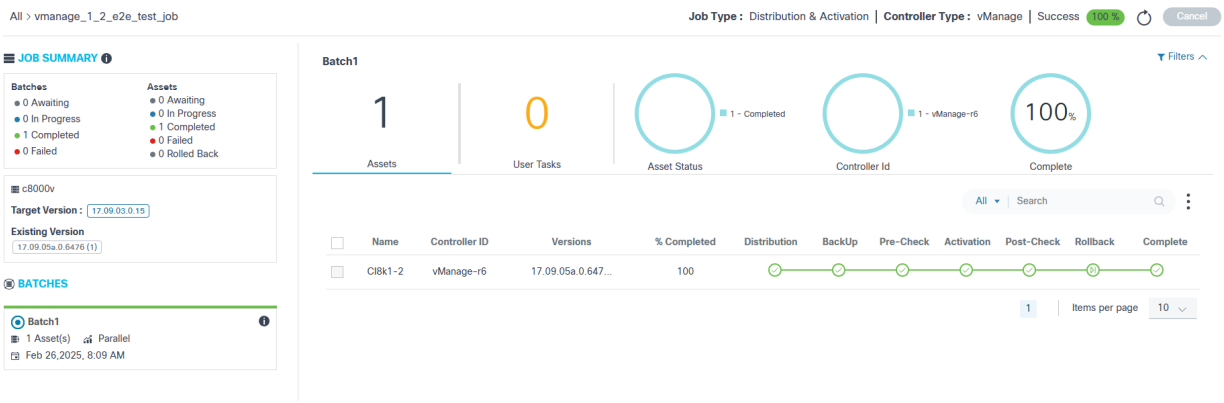
Inizio riepilogo processi

- Navigazione di navigazione dell'OdL corrente (ad esempio, All > manage_1_2_e2e). L'opzione All passa a Job Dashboard
- Tipo di processo
- Tipo di controller
- Stato processo con percentuale di completamento:
    - Operazione riuscita: Processo di aggiornamento completato
    - Operazione non riuscita: Processo di aggiornamento non riuscito per qualche motivo
    - In corso: Processo di aggiornamento in corso

Nota: Lo stato del processo viene spostato su In corso anche se viene raggiunta la programmazione di un batch

---

- In attesa: Il processo è stato eseguito ma è in attesa del raggiungimento di una o più pianificazioni batch



Riepilogo processi

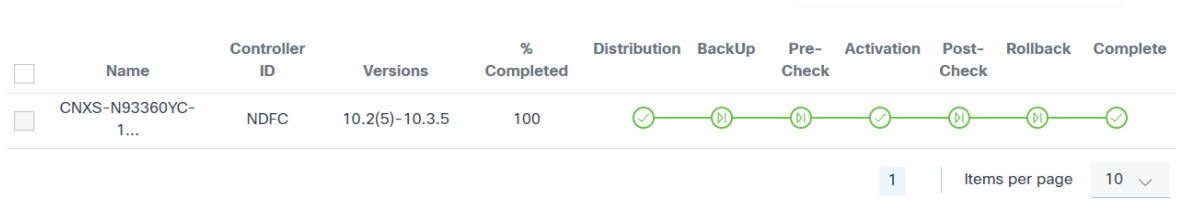
Nella pagina Riepilogo job sono disponibili le opzioni riportate di seguito.

- L'icona Aggiorna consente agli utenti di recuperare gli aggiornamenti su richiesta
- Annulla viene utilizzato per annullare gli OdL nelle fasi Bozza e Commit a meno che non venga raggiunta la programmazione per uno qualsiasi dei batch
- L'opzione Attiva (Activate) consente di creare un nuovo processo di attivazione in stato Bozza con gli stessi batch e gli stessi asset che facevano parte del processo precedentemente completato
    - L'opzione Attiva è disponibile solo se il tipo di processo è Distribuzione e viene completato correttamente
    - Se il job di attivazione è già stato creato e si fa clic su Attiva, viene visualizzato un messaggio con lo stato del job creato in precedenza e viene fornita un'opzione per reindirizzare il job già creato; nel nuovo job creato, gli utenti hanno la possibilità di modificare o eliminare i batch o gli asset, ma il tipo di job, il tipo di controller e i criteri di conformità non sono modificabili.

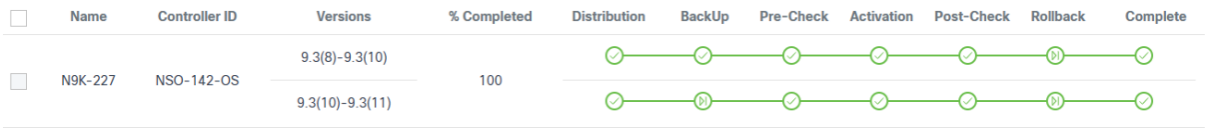
- Sotto la sezione Analisi viene visualizzato un elenco impaginato di risorse
- Il campo Cerca consente di eseguire ricerche generali e specifiche per le colonne, ad esempio:
    - Nome dispositivo
    - ID controller
    - Numero di serie

Scarica report batch

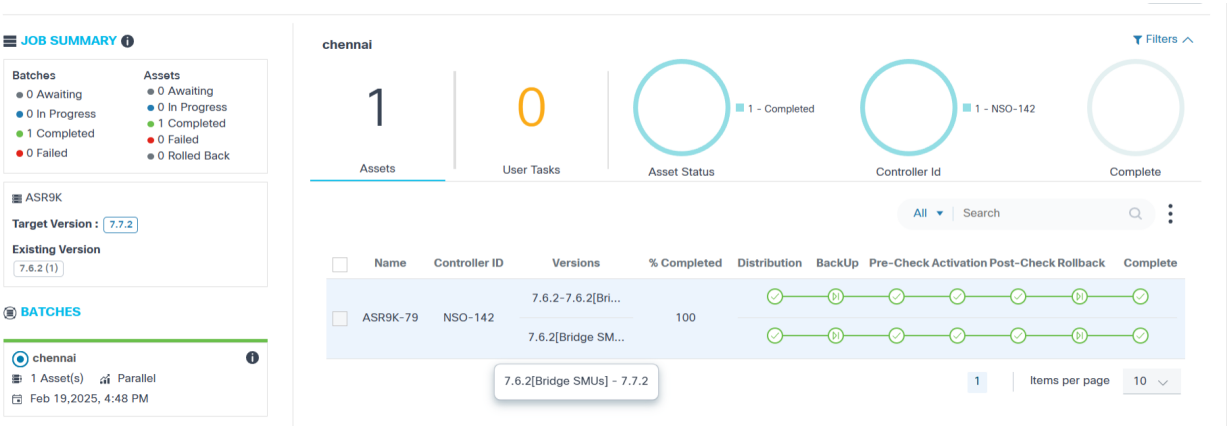
- L'opzione per scaricare il report a livello di batch selezionando l'icona Altre opzioni > Scarica; il report è costituito dai dettagli a livello di batch con i dettagli del dispositivo



Ordinamento - Aggiornamento in un unico passaggio



Ordinamento - Aggiornamento in più passaggi

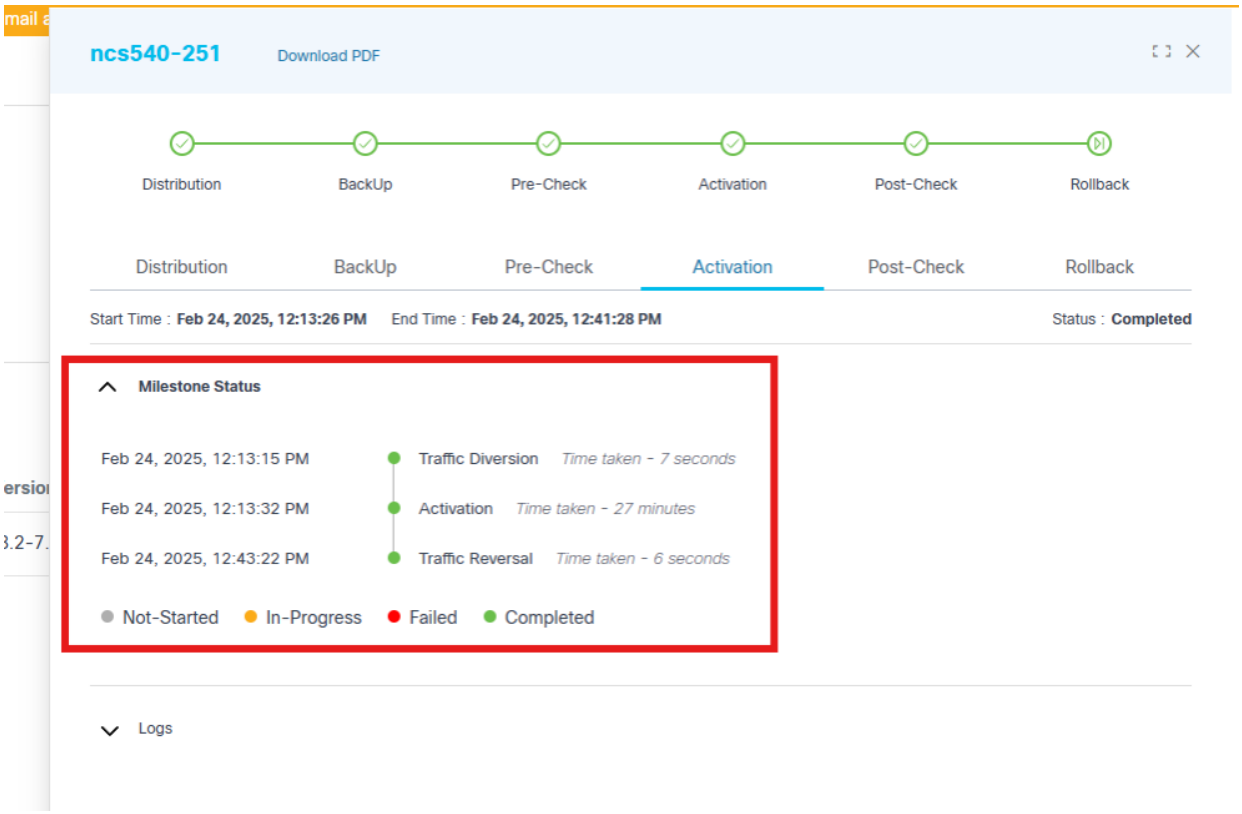


Ordinamento - Aggiornamento Bridge SMU

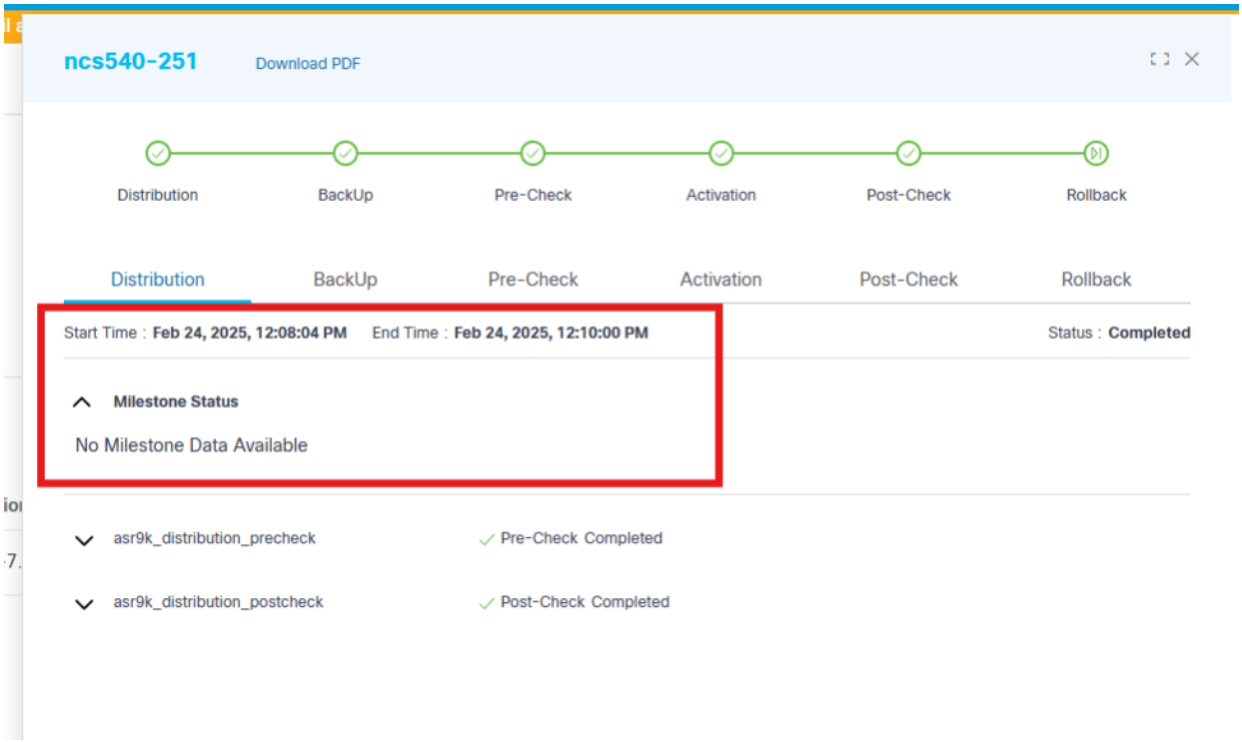
- È possibile eseguire l'ordinamento facendo clic sui nomi delle colonne
- Per ogni dispositivo vengono visualizzate le fasi cardine di aggiornamento seguenti insieme a Nome, ID controller, Versioni e % completato:
    - Distribuzione
    - Backup
    - Verifica preliminare
    - Traffic-Diversion
    - Attivazione
    - Post-controllo
    - Traffic-Reverse
    - Rollback
    - Completa

Nota: % completato visualizza lo stato in base al numero di fasi cardine completate per un dispositivo. Tutte le percentuali di completamento a livello di dispositivo di un batch vengono aggregate per calcolare la percentuale di completamento del batch. A sua volta, tutte le percentuali di completamento batch vengono aggregate per calcolare la percentuale di completamento a livello di processo.

Le fasi cardine secondarie, note anche come fasi cardine personalizzate, sono le fasi significative intermedie eseguite e visualizzate sotto la fase cardine standard quando vengono aggiunte. Per ulteriori informazioni sull'aggiunta di attività cardine personalizzate, consultare la Guida per gli sviluppatori BPA.



Visualizzazione attività cardine secondarie (se le attività cardine secondarie vengono aggiunte con il nome di attività cardine standard)

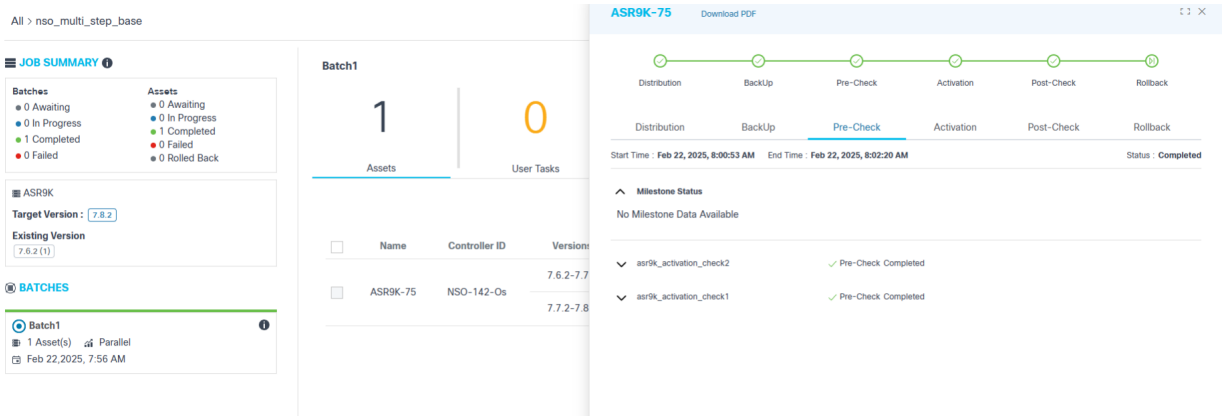


Visualizzazione attività cardine secondarie (se le attività cardine secondarie non vengono aggiunte con il nome di attività cardine standard)

Nota: Le fasi cardine variano in base al tipo di processo selezionato. L'attività cardine TrafficReversal non è disponibile per i processi di distribuzione.

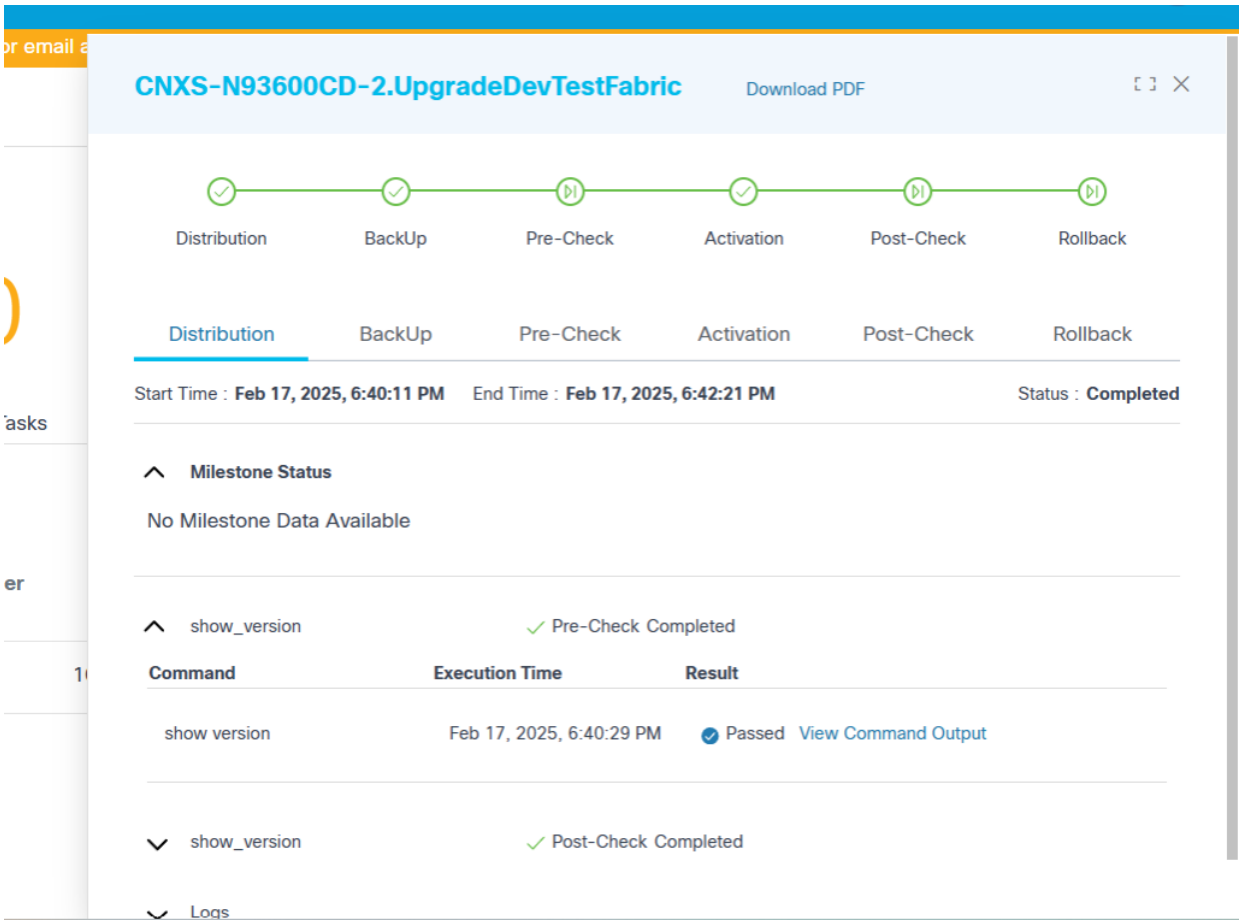
La deviazione e l'inversione del traffico vengono spostate sotto la fase cardine di attivazione.

- Legenda a colori di un'attività cardine composta da:
  - Controllo grigio: In sospeso
  - Blue Check: In corso
  - Contrassegno verde: Ignorato
  - Assegno verde: Completato
  - Controllo arancione: Attività utente
  - Controllo rosso: Non riuscito



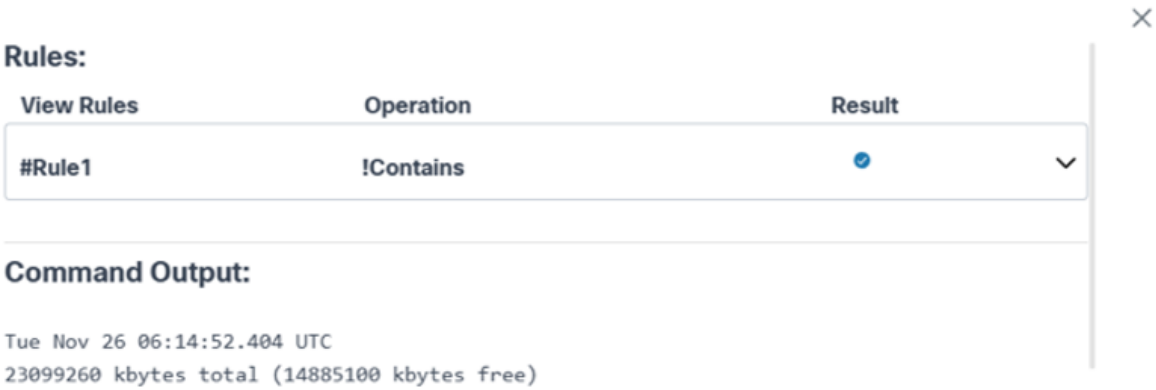
Visualizzazione attività cardine pre- e post-controllo

Per le fasi cardine con esecuzione precedente o successiva al controllo, gli utenti possono visualizzare l'output completo dei comandi insieme alle regole di convalida e ai relativi stati per tutti i comandi configurati nel rispettivo modello di processo.



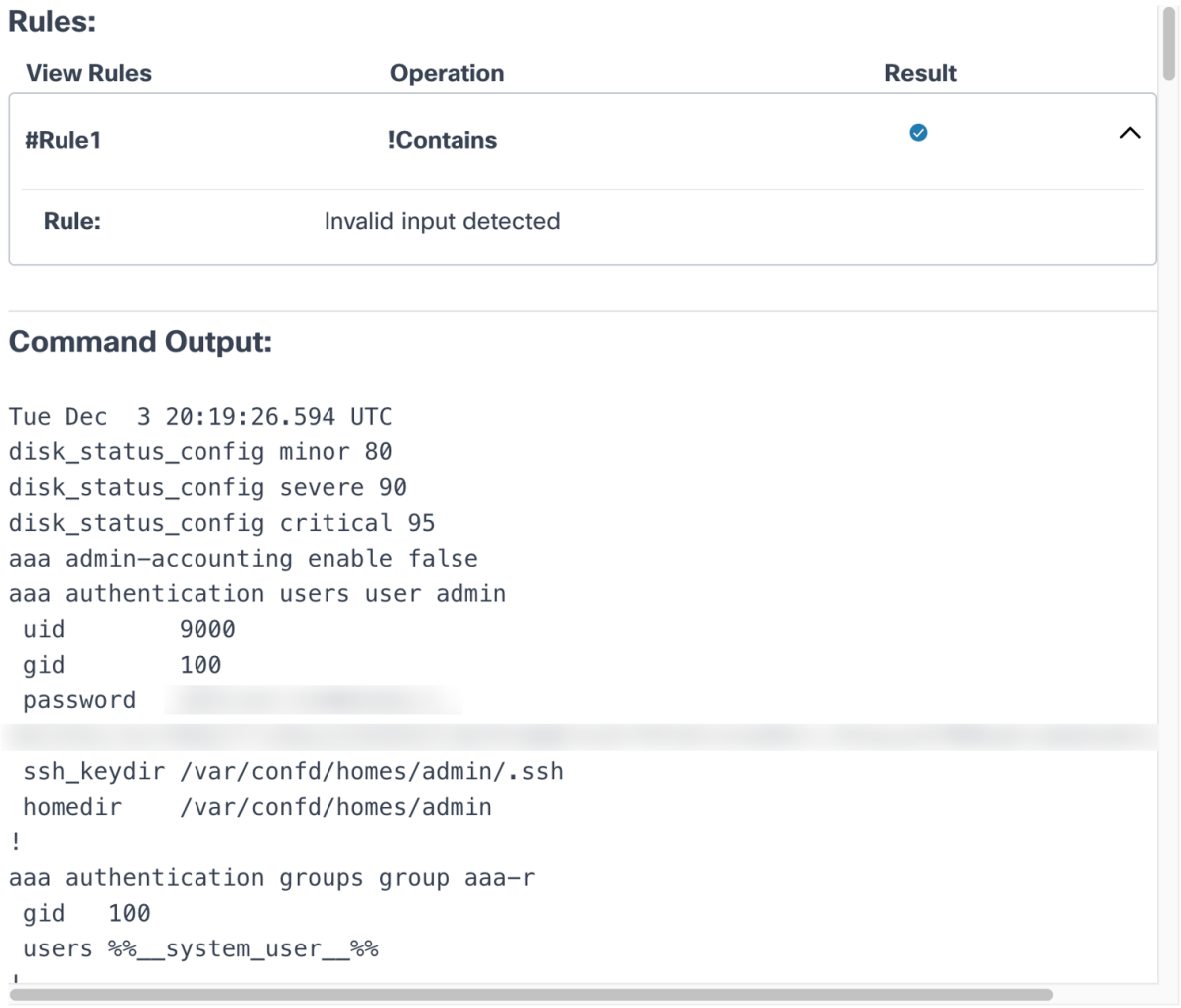
Visualizzazione delle fasi cardine di distribuzione con output del comando di pre-controllo

1. Per visualizzare l'output del comando e le regole associate ai comandi di pre e post-controllo, fare clic sul collegamento Visualizza output comando.

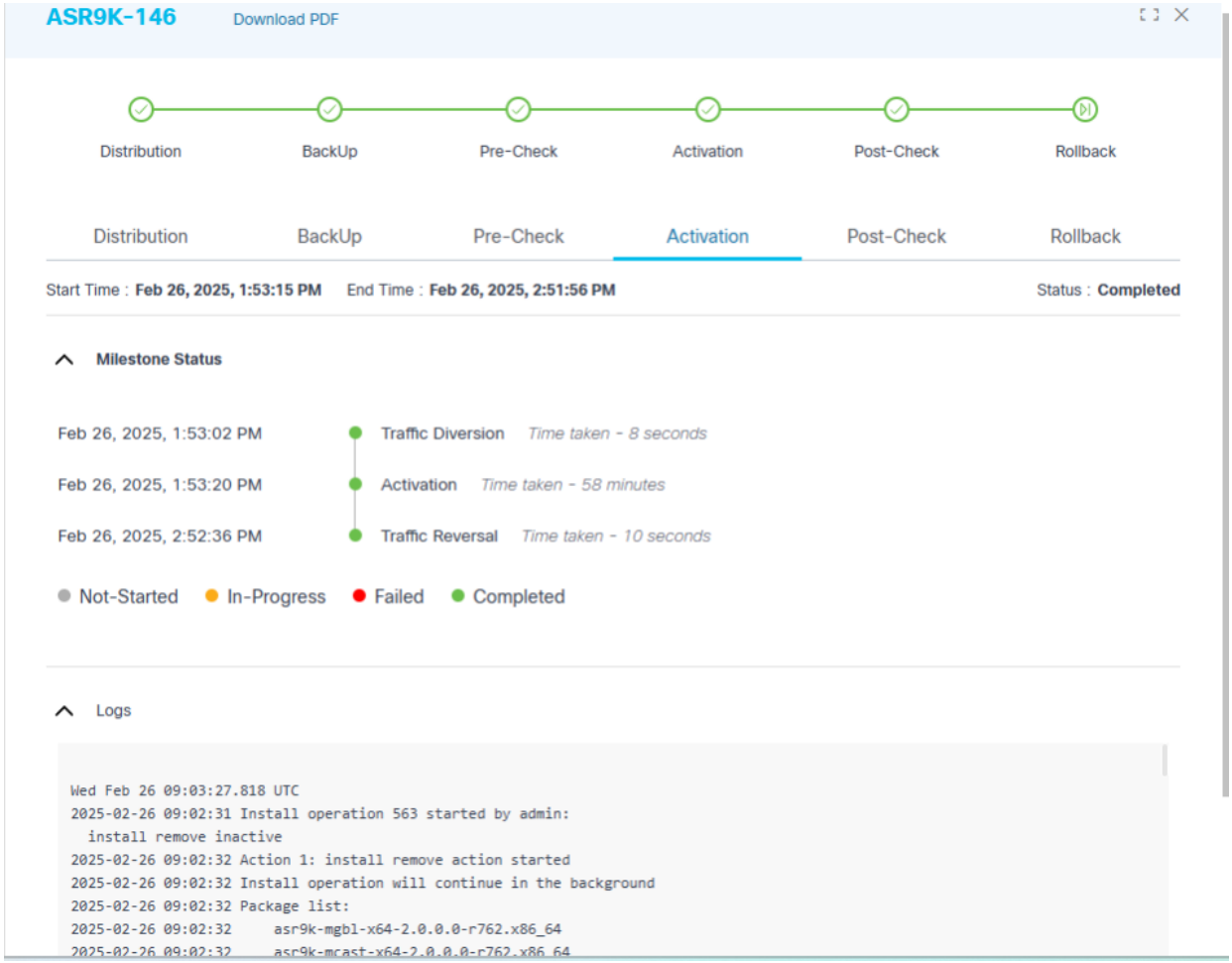


Output dei comandi di pre-controllo e post-controllo e regole associate

2. Selezionare l'icona Espandi per visualizzare i dettagli completi di ogni regola.



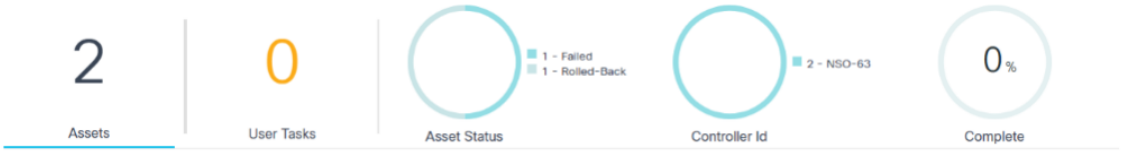
Output dei comandi di pre e post-controllo con regole di convalida



Visualizzazione attività cardine di attivazione con Live Log

La figura precedente fornisce i dettagli della fase cardine di attivazione, che include i registri attivi per monitorare lo stato dell'attivazione software di un determinato dispositivo.

Quando un'attività cardine inizia o termina, facendo clic su di essa vengono visualizzate ulteriori informazioni.



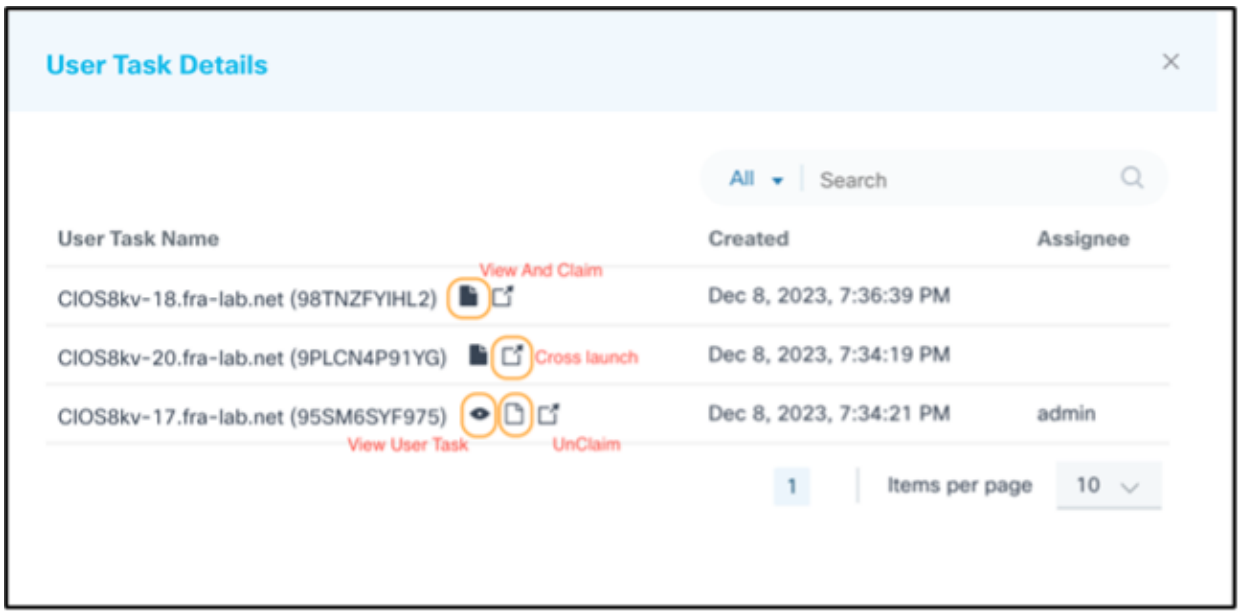
Sezione Analisi

Una sezione Analisi, visualizzata nella parte superiore della pagina Riepilogo job, visualizza le seguenti informazioni relative al job attualmente selezionato:

- Nome del batch (ad esempio Asia)
- Filtri ^ comprime ed espande la sezione Analisi
- I dettagli del batch riportati di seguito sono visualizzati in ordine:

- Risorse: Numero totale di cespiti
- Attività utente: Numero totale di attività utente in attesa dell'input dell'utente o dell'amministratore delle operazioni
- Stato asset: Filtra i dispositivi batch in base allo stato. Il filtro Rollback è stato aggiunto per identificare i dispositivi di cui è stato completato correttamente il rollback.
- ID controller: Filtra i dispositivi batch che appartengono all'ID controller selezionato
- Completa: Percentuale totale di completamento batch

Per eseguire azioni su qualsiasi attività utente, fare clic sul conteggio Attività utente. Viene visualizzata la finestra Dettagli task utente con le informazioni riportate di seguito.



Dettagli attività utente

- Elenco di attività utente che corrispondono ai rispettivi dispositivi che richiedono attenzione
- Le seguenti icone per le opzioni relative alle attività degli utenti:

  - Visualizza e richiede: Visualizzare i dettagli dell'attività dell'utente
  - Cross Launch: Visualizzare le attività del flusso di lavoro BPA nell'interfaccia utente classica
  - Annulla richiesta: Rimuove l'assegnazione di attività utente
  - Visualizza attività utente: Visualizzare i dettagli dell'attività dell'utente

Attività utente

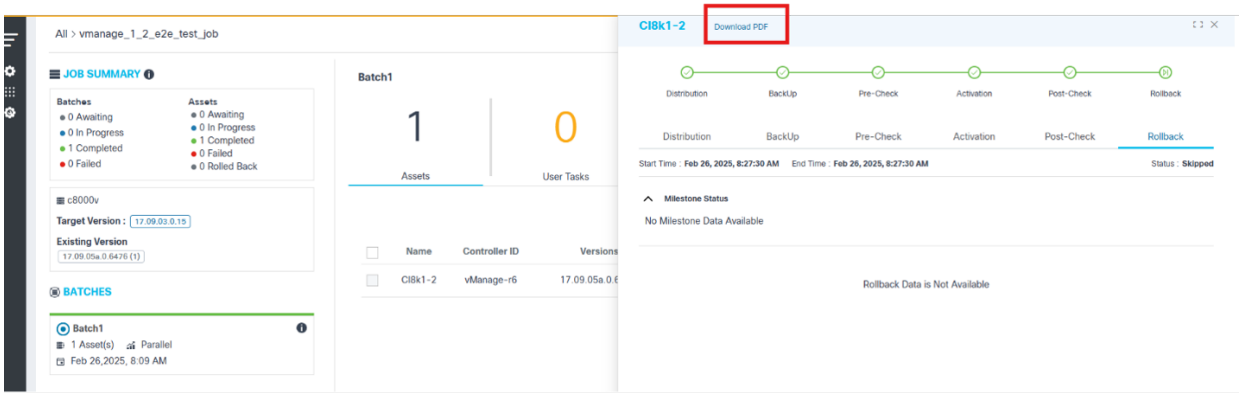
Opzione Visualizza dell'attività utente

- In base al contesto dell'operazione, vengono visualizzate le seguenti opzioni:
  - Riprova: Riesegue l'attività
  - Riprova tutto: Riesegue tutti i controlli precedenti e successivi
  - Continua: Passa all'attività successiva
  - Rollback: Ripristina la versione precedente. Questa opzione è disponibile se l'attivazione o il controllo successivo non è riuscito o se vengono rilevate differenze non valide tra i controlli precedenti o successivi
  - Annulla: Annulla il processo corrente
  - Chiudi: Chiude la finestra Attività utente.
- Eseguire le operazioni utente, se presenti, e selezionare l'icona Aggiorna per aggiornare il conteggio totale delle operazioni utente
- Percentuale di completamento batch totale
- Grafico selezionabile per filtrare in base agli ID controller

---

Nota: Il numero prima dell'ID del controller indica il numero totale di dispositivi gestiti dal rispettivo controller.

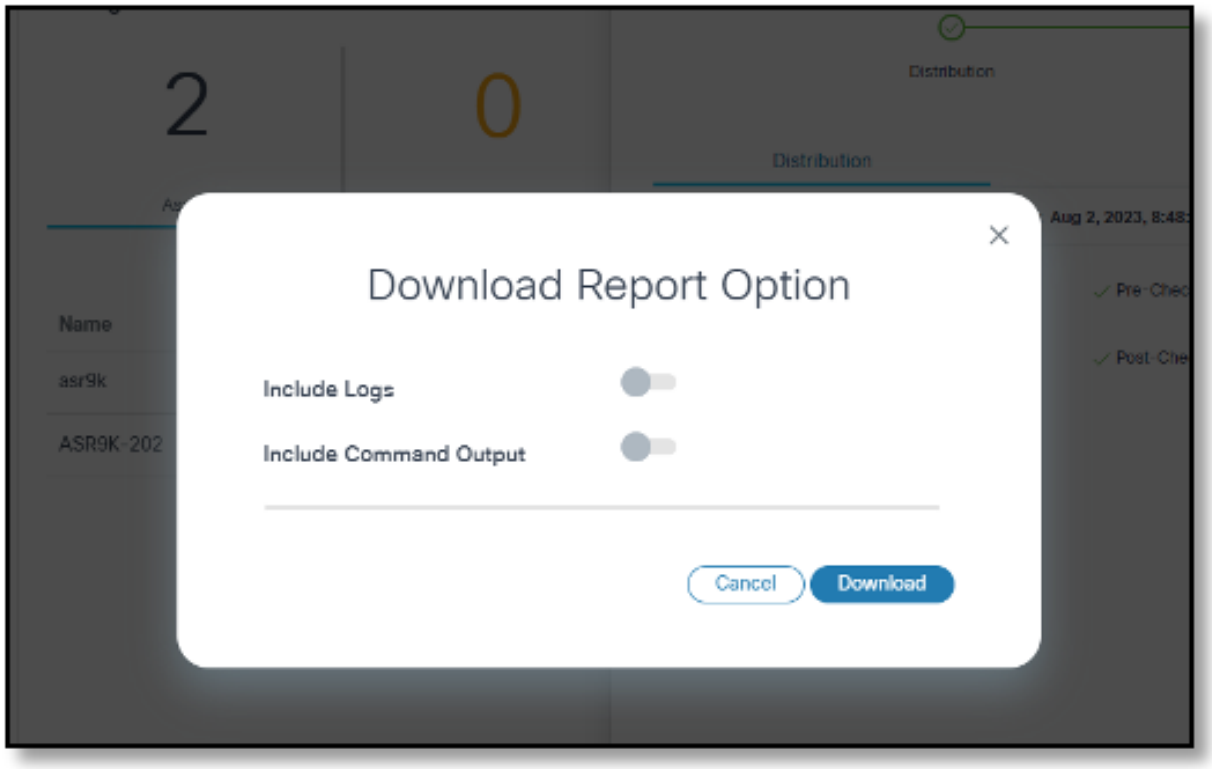
Download del report di aggiornamento software



Scarica PDF

Il nome del dispositivo viene visualizzato seguito da Download PDF nell'intestazione della vista dei dettagli. Gli utenti possono generare e scaricare il report di aggiornamento in formato PDF per il dispositivo attualmente selezionato. Per scaricare il report di aggiornamento in formato PDF:

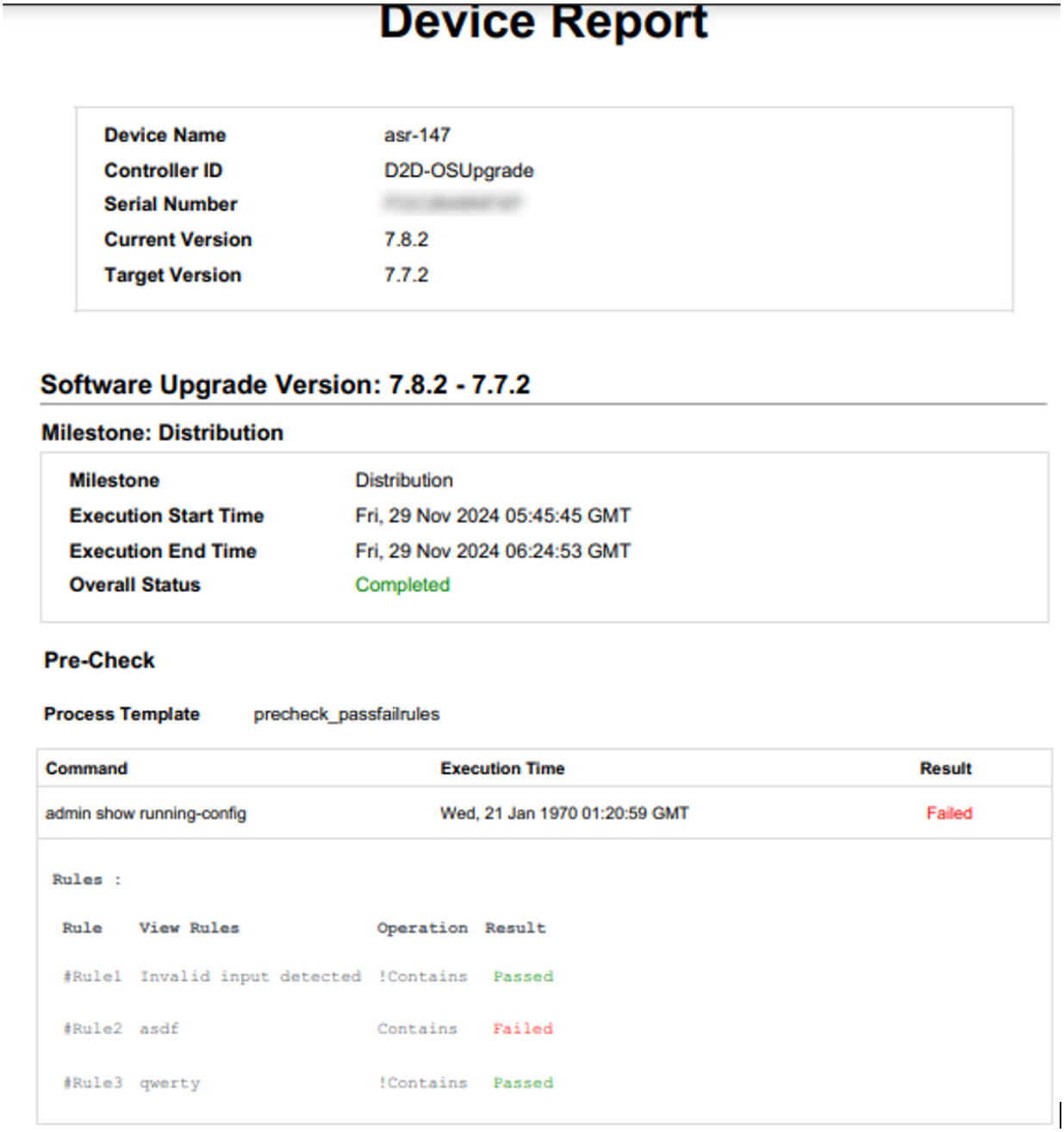
1. Fare clic su Download PDF. Viene visualizzata la finestra Download Report Option (Opzioni report download).



Opzione per il download del report

2. Abilitare gli interruttori Include Logs e Include Command Output.
    - Includi log: Include nel report gli eventuali registri attivi
    - Includi output comando: include nella relazione l'output del comando dei controlli preliminari e successivi; In questo caso, le regole sono seguite dall'output del comando
3. Fare clic su Download (Scarica). Inizio generazione report.

Nota: L'attivazione di Includi log e Includi output comando consente di aumentare il tempo di elaborazione per la generazione del report e le relative dimensioni. Utilizzare queste opzioni solo quando è necessario un report dettagliato. Le regole dei comandi vengono incluse nel report indipendentemente dall'attivazione o disattivazione dell'output del comando.



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

Report dispositivo

Archiviazione dei job

1. Accedere a BPA con credenziali che dispongano di diritti di accesso sufficienti per aggiornare i processi.
2. Selezionare Aggiornamento sistema operativo > Processi di aggiornamento. Viene visualizzata la pagina Job di aggiornamento.
3. Utilizzare il filtro Search in combinazione con i filtri grafici disponibili per filtrare i job.
4. Selezionare uno o più processi.

Processo di archiviazione

5. Selezionare l'icona Altre opzioni > Archivia.

Nota: È possibile archiviare solo i processi completati.

Eliminazione dei job

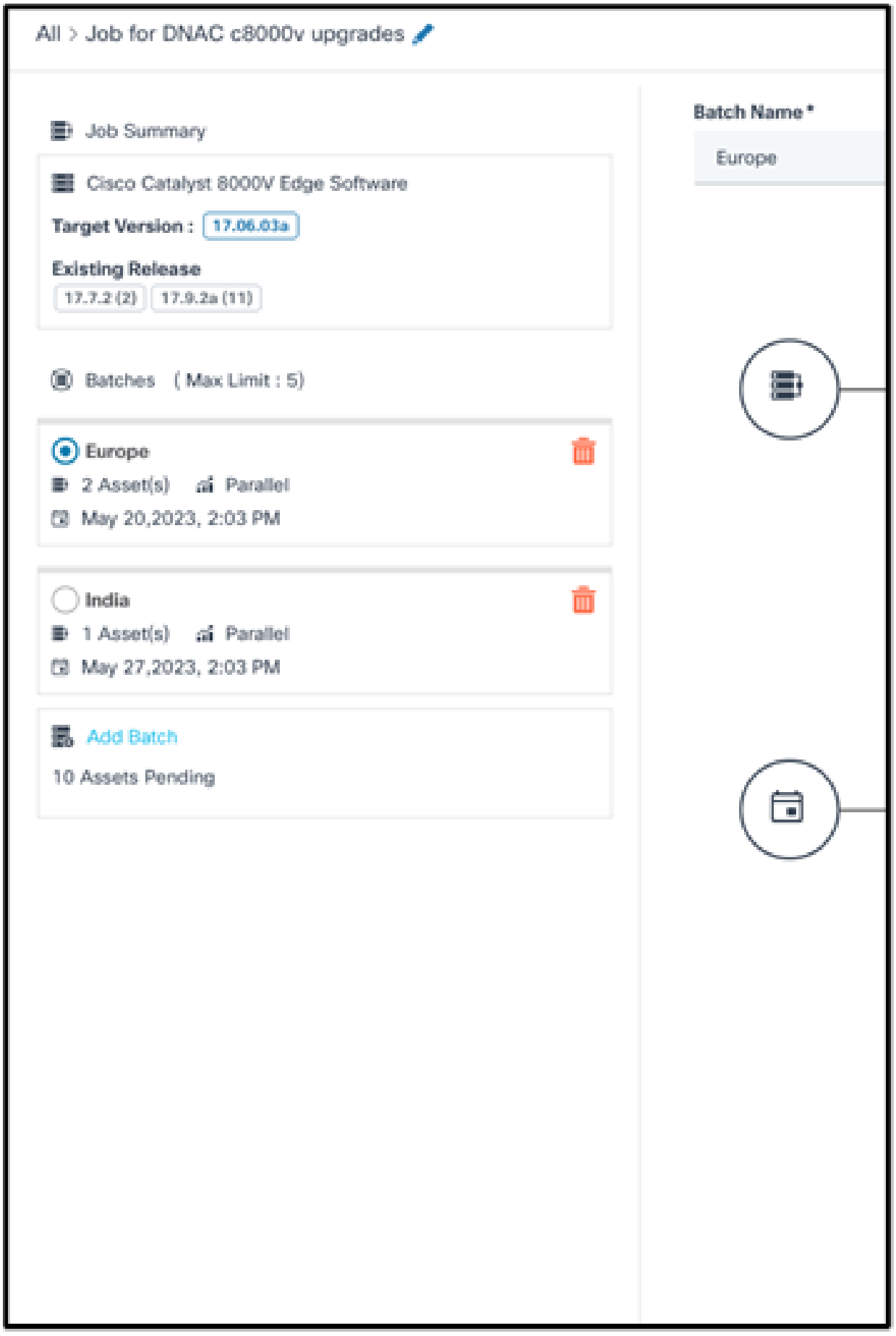
1. Accedere a BPA con credenziali che dispongano di diritti di accesso sufficienti per aggiornare i processi.
2. Selezionare Aggiornamento sistema operativo > Processi di aggiornamento. Viene visualizzata la pagina Job di aggiornamento.
3. Utilizzare il filtro Search in combinazione con i filtri grafici disponibili per filtrare i job.
4. Selezionare uno o più processi.

Elimina processo

5. Selezionare l'icona Altre opzioni > Elimina job.

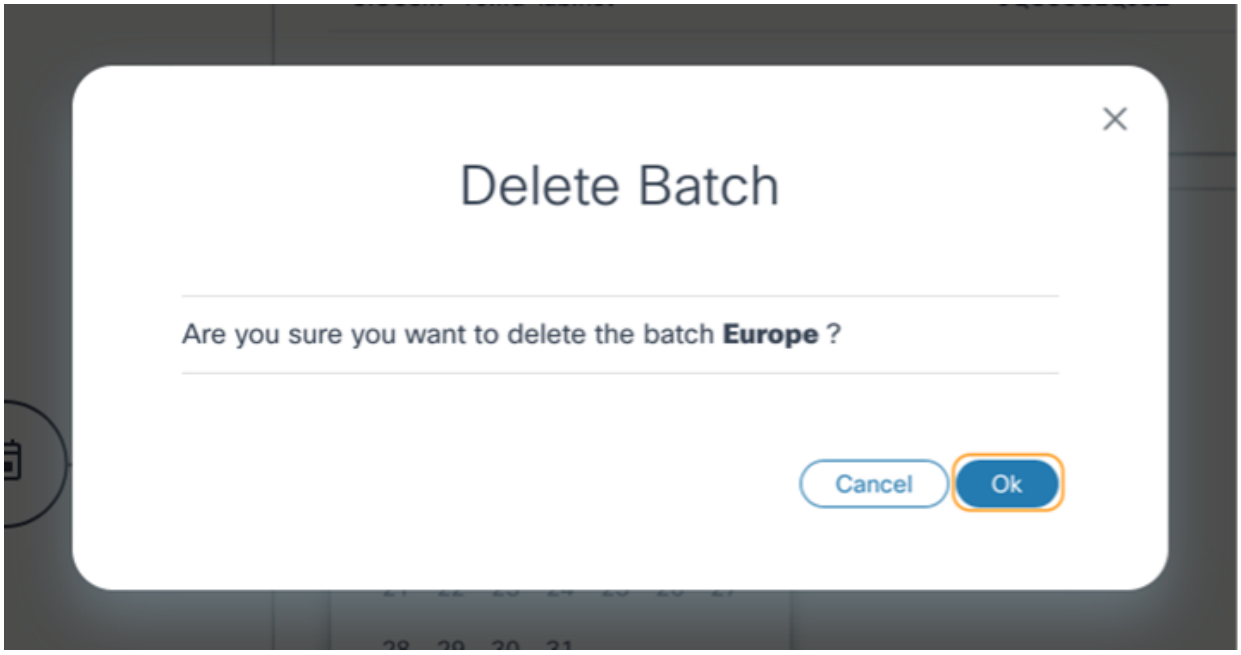
Nota: I processi possono essere eliminati solo quando si trovano nella fase Bozza.

Eliminazione di batch nei job



Eliminare un batch in un processo

1. Selezionare l'icona Elimina del batch desiderato nel pannello laterale. Viene visualizzata una finestra di conferma.



Conferma eliminazione batch

2. Fare clic su OK.

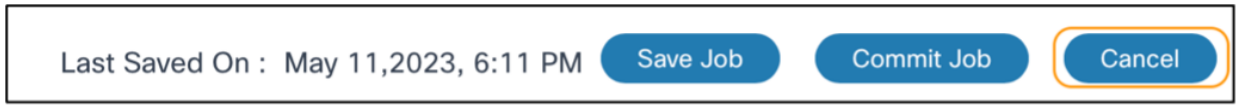
I cespiti associati al batch eliminato vengono restituiti al pool di cespiti in sospeso e possono essere selezionati in batch nuovi o esistenti.

Annullamento dei job

1. Accedere a BPA con credenziali che dispongano di diritti di accesso sufficienti per aggiornare i processi.
2. Selezionare Aggiornamento sistema operativo > Processi di aggiornamento. Viene visualizzata la pagina Job di aggiornamento.

Processo di aggiornamento

3. Utilizzare il filtro Search insieme ai filtri grafici disponibili per filtrare il job desiderato.
4. Fare clic sul job desiderato. Viene visualizzata la pagina Riepilogo job.

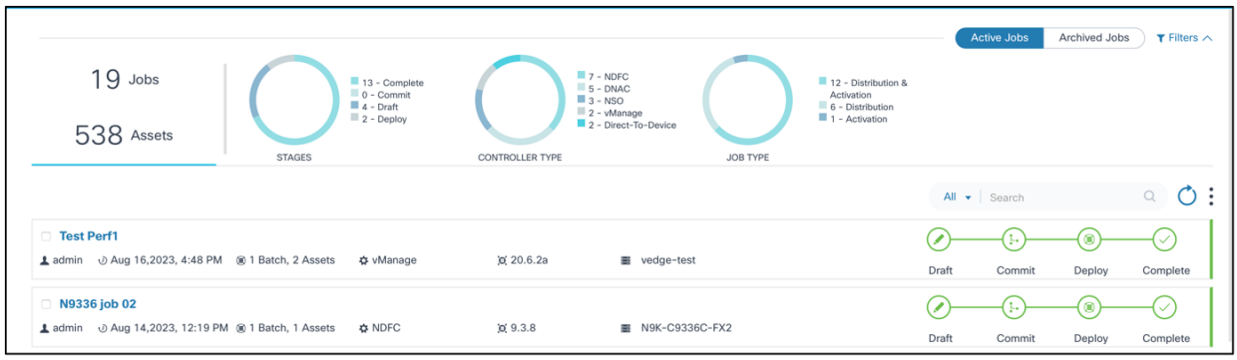


Annulla

5. Fare clic su Annulla.

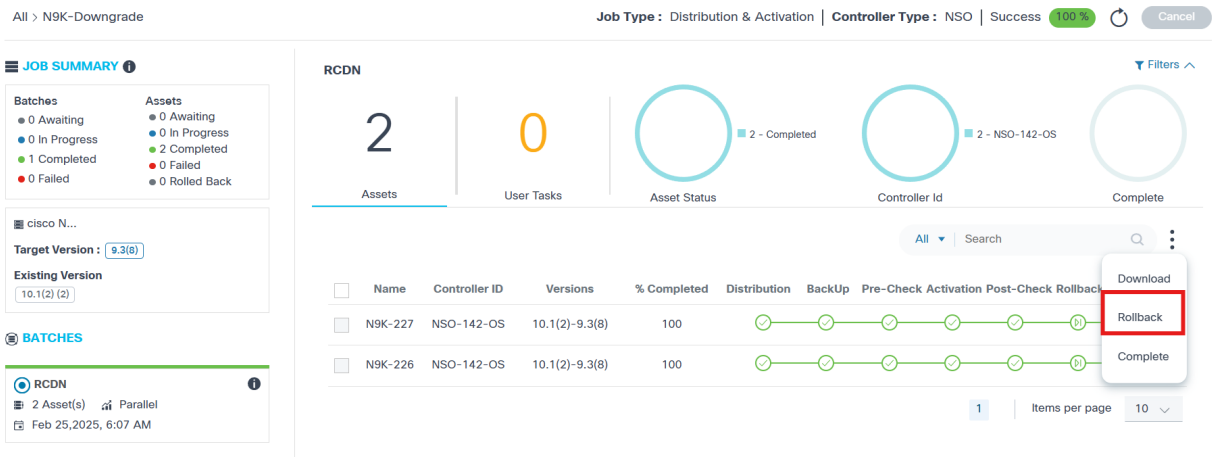
Rollback di processi o aggiornamenti completati

1. Accedere a BPA con credenziali che dispongano di diritti di accesso sufficienti per aggiornare i processi.
2. Selezionare Aggiornamento sistema operativo > Processi di aggiornamento. Viene visualizzata la pagina Job di aggiornamento.



Processo di aggiornamento

3. Utilizzare il filtro Search insieme ai filtri grafici disponibili per filtrare il job desiderato.
4. Fare clic sul job desiderato. Viene visualizzata la pagina Riepilogo job. Selezionare il batch richiesto nel riquadro a sinistra e selezionare i dispositivi desiderati che richiedono la conferma Completa / Rollback nel pannello a destra
5. Selezionare l'icona Altre opzioni e fare clic sulle azioni di menu Rollback o Complete in base al requisito.



Rollback

Nota: È possibile selezionare i dispositivi solo quando sono soddisfatti i seguenti prerequisiti:

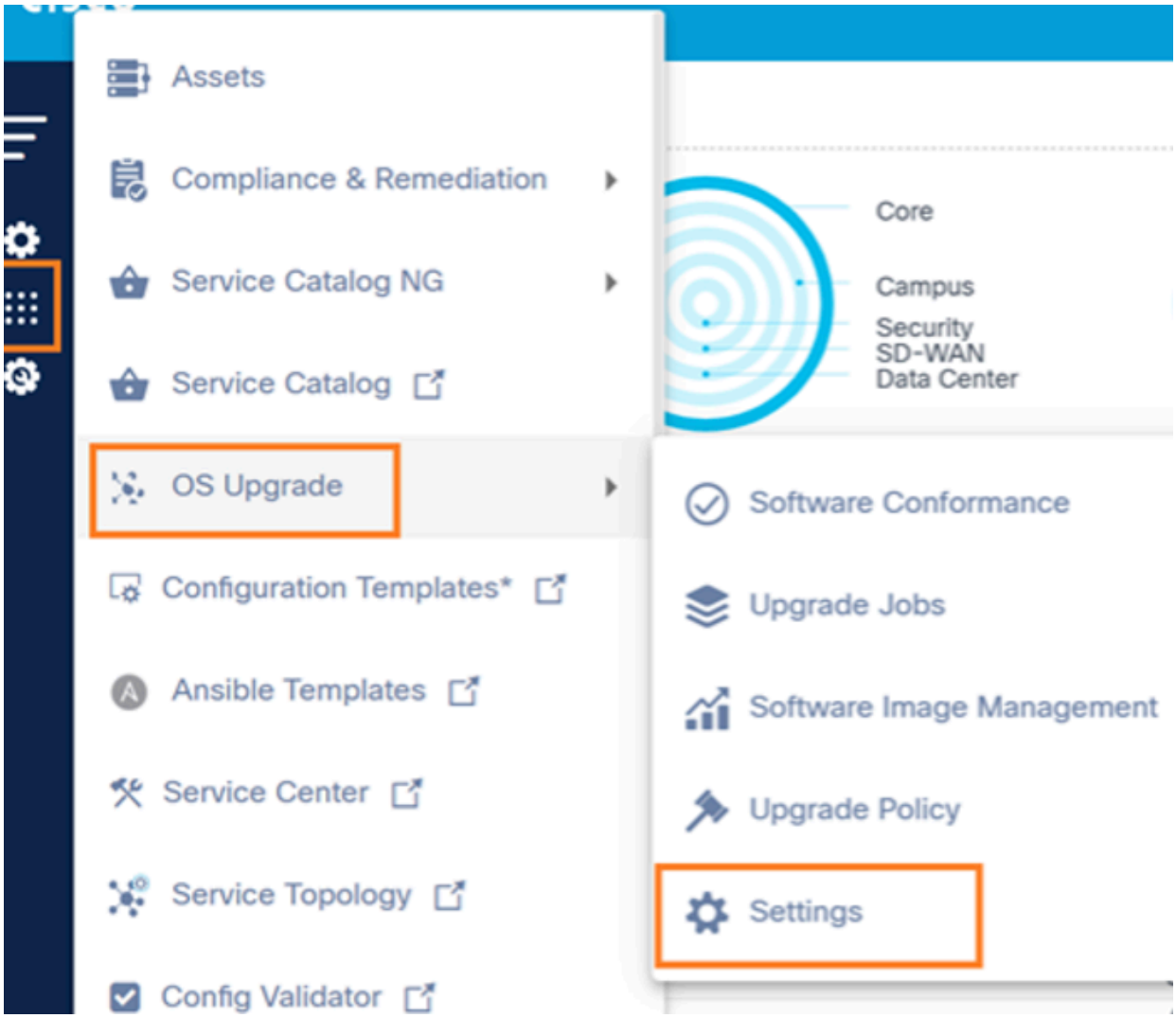
- È necessario configurare le impostazioni per abilitare l'opzione di rollback di un processo aggiornato completato. per ulteriori informazioni, fare riferimento a Impostazioni.
- Se non viene eseguita alcuna operazione entro il tempo specificato, i dispositivi passano automaticamente allo stato Completo
- I dispositivi sono disponibili per l'azione di rollback su richiesta se il rollback è stato precedentemente completato o se l'attività cardine di rollback è nello stato In attesa

Impostazioni

Le impostazioni di aggiornamento del sistema operativo forniscono un segnaposto per contenere le impostazioni comuni utilizzate in altri componenti dell'applicazione.

Per accedere alla pagina Impostazioni:

1. Accedere a BPA con le credenziali che dispongono dell'accesso di gestione alle impostazioni.



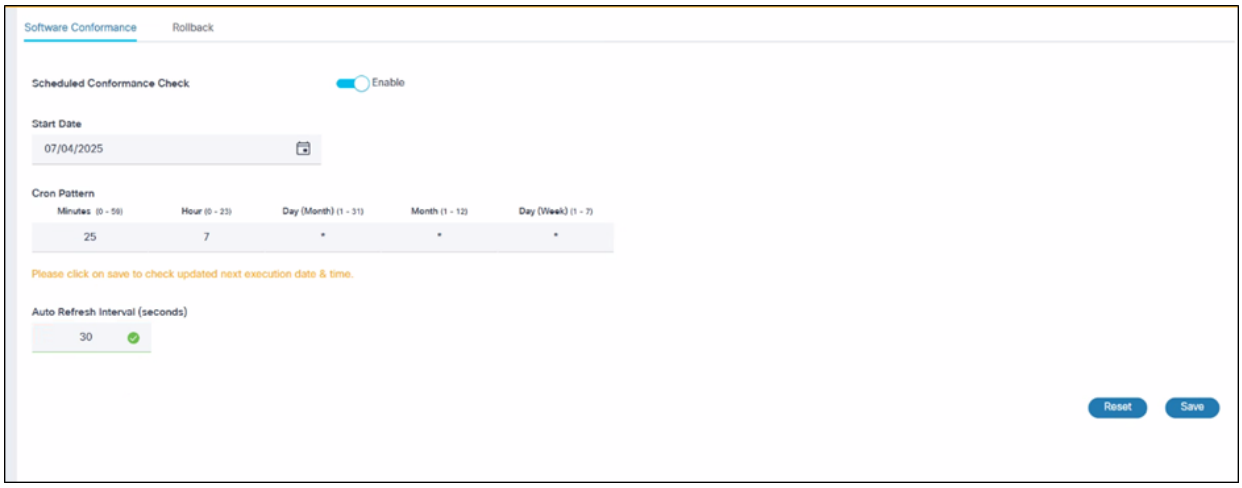
Impostazioni

2. Selezionare Aggiornamento sistema operativo > Impostazioni. Si apre la pagina Impostazioni.

La pagina Impostazioni contiene le due schede riportate di seguito.

- Conformità software: In questa scheda è possibile aggiornare le configurazioni che consentono pianificazioni di esecuzione della conformità automatica
- Rollback: In questa scheda è possibile aggiornare le configurazioni che consentono il rollback di un aggiornamento completo del dispositivo

Conformità software



Scheda Conformità software

La scheda Conformità software fornisce le informazioni riportate di seguito.

- Controllo di conformità programmato: Attivare o disattivare la pianificazione
- Data di inizio: Selezionare il GG/MM/AAAA

Nota: La data di inizio deve essere una data futura.

- Motivo: Fornire i seguenti dettagli:
  - Minuti (0-59)
  - Ora (0-23)
  - Giorno (mese) (1-31)
  - Mese (1-12)
  - Giorno (settimana) (1-7)
- Aggiungi intervallo di aggiornamento automatico: Il valore predefinito è 30 secondi
- Salva: Salva modifiche

Rollback

Scheda Rollback

La scheda Rollback fornisce le informazioni riportate di seguito.

- Attiva/disattiva verifica utente: Abilita o disabilita verifica utente
    - Stato abilitato: I dispositivi nel processo di aggiornamento attendono la conferma dell'utente per il rollback o il completamento dell'aggiornamento finché non viene raggiunto il tempo di soglia configurato in Tempo soglia configurazione (ore); quando raggiunti, i dispositivi passano automaticamente allo stato Completato
    - Stato disabilitato: I dispositivi nel processo di aggiornamento completano automaticamente l'aggiornamento senza attendere la conferma dell'utente
- Ora soglia di conferma: Aggiungere un tempo di attesa di soglia in ore
- Salva: Salva modifiche

Configurazione distribuzione

- Le pianificazioni predefinite per il controllo dei criteri di conformità e per i metadati SWIM vengono configurate ogni giorno alle 7.25 ora locale.
- Per modificare le pianificazioni predefinite della sincronizzazione dei metadati dell'immagine SWIM, passare alla directory di installazione BPA "<directory di installazione BPA>/conf/@cisco-bpa-platform/mw-osupgrade-nxtgen/config.json" e aggiornare la proprietà schedule.swimSchedule con l'espressione Cron. Le pianificazioni possono essere aggiornate dopo la distribuzione. Per ulteriori informazioni, fare riferimento a Conformità software.
- Per aumentare o ridurre il numero massimo di dispositivi elaborati in modalità parallela per i diversi tipi di controller:

1. Aggiornare i seguenti file:
    - File Cisco Catalyst Center: "<DIRECTORY_INSTALLAZIONE_BPA>/conf/@cisco-bpa-platform/mw-dnac-agent/config.json"
    - File vManage: "<DIRECTORY_INSTALLAZIONE_BPA>/conf/@cisco-bpa-platform/mw-vmanage-agent/config.json"
    - File NDFC: "<DIRECTORY_INSTALLAZIONE_BPA>/conf/@cisco-bpa-platform/mw-ndfc-agent/config.json"
    - File FMC: "<DIRECTORY_INSTALLAZIONE_BPA>/conf/@cisco-bpa-platform/mw-fmc-agent/config.json"
2. Passare a Limitazione aggiornamenti > capacità > attivazione immagine, distribuzione immagine per aumentare il limite di attivazione o distribuzione simultanea.

Nota: Prima di aggiornare questi limiti, consultare le piattaforme dei dispositivi e dei controller supportati.

Controllo dell'accesso

Controllo degli accessi basato sui ruoli

BPA supporta il controllo degli accessi basato sui ruoli (RBAC). Nel modello RBAC, un ruolo incapsula un set di autorizzazioni (ad esempio, azioni) che un utente può eseguire. Per il controllo dell'accesso, gli amministratori possono assegnare ruoli predefiniti o nuovi con autorizzazioni ai gruppi di utenti. Un utente può appartenere a uno o più gruppi di utenti e a ogni gruppo di utenti possono essere assegnati uno o più ruoli che attribuiscono agli utenti di quel gruppo determinate autorizzazioni di accesso.

Nella tabella seguente vengono descritti i ruoli di aggiornamento del sistema operativo OOB e le autorizzazioni associate.

Servizio	Group	Intento	Amministratore privilegiato	Amministratore Use Case	Utente di sola lettura (utente di sola lettura per l'aggiornamento del sistema operativo)	Ope
OSUpgradeService	app_interfaccia utente	Visualizzare o nascondere l'applicazione Processi di aggiornamento	Sì	Sì	Sì	Sì
OSUpgradeService	app_interfaccia utente	Mostrare o nascondere l'applicazione Software Conformance	Sì	Sì	Sì	Sì
OSUpgradeService	app_interfaccia utente	Mostra o nasconde l'applicazione SWIM	Sì	Sì	Sì	Sì
OSUpgradeService	app_interfaccia utente	Visualizzare o nascondere l'applicazione Criteri di aggiornamento software	Sì	Sì	Sì	Sì
OSUpgradeService	app_interfaccia utente	Visualizzare o nascondere le impostazioni di	Sì	Sì	Sì	Sì

Servizio	Group	Intento	Amministratore privilegiato	Amministratore Use Case	Utente di sola lettura (utente di sola lettura per l'aggiornamento del sistema operativo)	Ope
		Aggiornamento software				
OSUpgradeService	Processi di aggiornamento	Gestire i processi di aggiornamento (ad esempio, creazione, aggiornamento, eliminazione e commit)	Sì	Sì	No	Sì
OSUpgradeService	Processi di aggiornamento	Annulla processi di aggiornamento	Sì	Sì	No	Sì
OSUpgradeService	Processi di aggiornamento	Archiviazione su richiesta dei lavori	Sì	Sì	No	Sì
OSUpgradeService	Processi di aggiornamento	Approvazione manuale	Sì	Sì	No	Sì
OSUpgradeService	Criteri di conformità software	Visualizza i criteri di conformità software e i risultati di esecuzione	Sì	Sì	Sì	Sì
OSUpgradeService	Criteri di conformità software	Crea, aggiorna ed elimina i criteri di conformità software	Sì	Sì	No	No
OSUpgradeService	Criteri di conformità software	Esecuzione su richiesta dei criteri di conformità software	Sì	Sì	No	Sì
OSUpgradeService	Criteri di aggiornamento	Visualizza criteri di aggiornamento del sistema	Sì	Sì	Sì	Sì

Servizio	Group	Intento	Amministratore privilegiato	Amministratore Use Case	Utente di sola lettura (utente di sola lettura per l'aggiornamento del sistema operativo)	Ope
		operativo				
OSUpgradeService	Criteri di aggiornamento	Gestisci criteri di aggiornamento del sistema operativo	Sì	Sì	No	No
OSUpgradeService	Gestione delle immagini in modalità wim	Creazione, aggiornamento ed eliminazione di immagini software	Sì	Sì	No	Sì
OSUpgradeService	Gestione delle immagini in modalità wim	Visualizza NUOTO	Sì	Sì	Sì	Sì
OSUpgradeService	Gestione delle immagini in modalità wim	Sincronizza immagini software	Sì	Sì	No	Sì
OSUpgradeService	Consigli software	Metadati consigli software di sincronizzazione	Sì	Sì	No	No
OSUpgradeService	Consigli software	Visualizza avvisi o informazioni dettagliate	Sì	Sì	Sì	Sì
OSUpgradeService	Consigli software	Gestire i criteri di conformità	Sì	Sì	No	No
OSUpgradeService	Impostazione della conformità software	Visualizza impostazioni di conformità software	Sì	Sì	Sì	Sì
OSUpgradeService	Impostazione della conformità software	Gestisci impostazioni conformità software	Sì	Sì	No	No

Nota: I ruoli personalizzati e il mapping delle autorizzazioni possono essere eseguiti in base

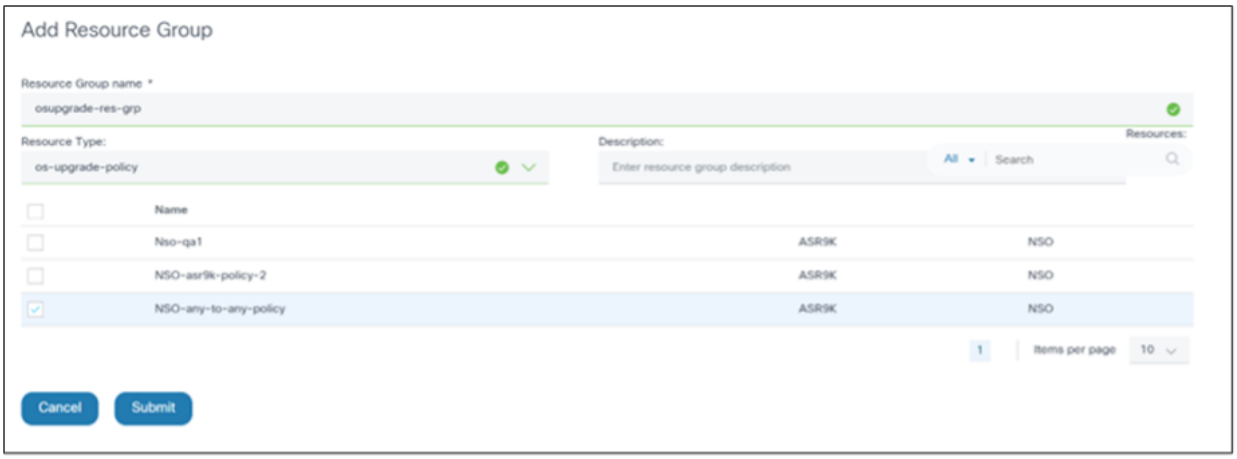
ai requisiti. Fare riferimento a Gruppi di risorse.

Gruppi di risorse

Questa funzionalità fornisce un controllo accurato dell'accesso per le risorse BPA, ad esempio i criteri di aggiornamento, che impediscono agli utenti non autorizzati di aggiornare i criteri definiti nell'applicazione Aggiornamento sistema operativo. Gli amministratori possono limitare l'accesso definendo un gruppo di risorse con criteri accessibili.

Per creare un gruppo di risorse:

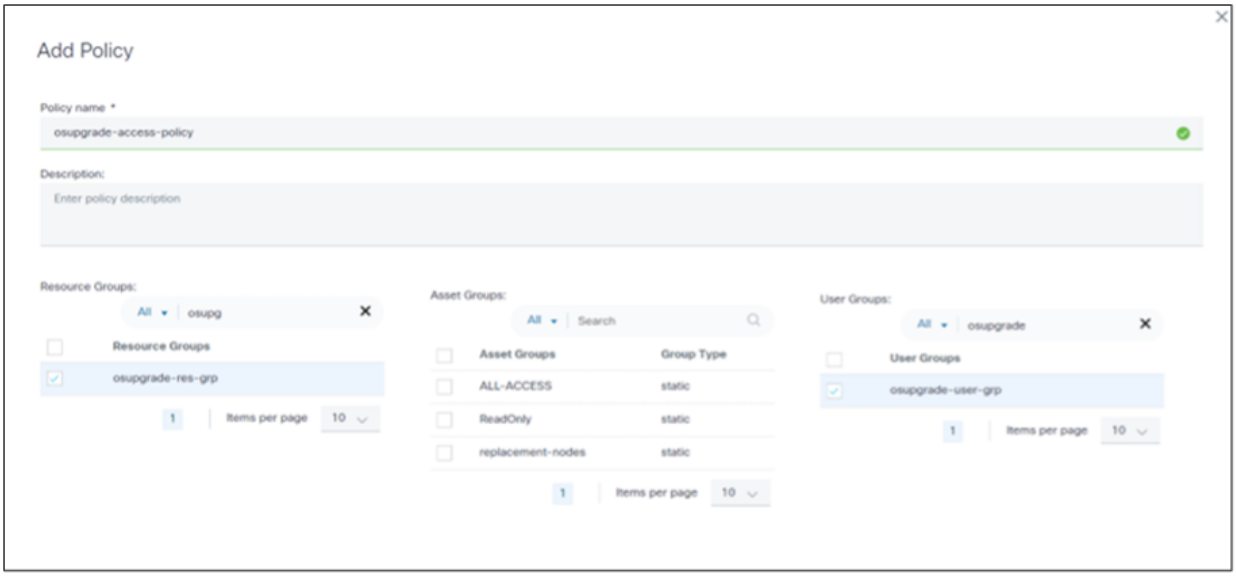
1. Passare a Impostazioni > Gruppi di risorse.



Aggiungi gruppo di risorse

2. Crea un gruppo di risorse con criteri a cui possono accedere utenti non amministratori.
3. Selezionare os-upgrade-policy come tipo di risorsa. Vengono visualizzate le risorse corrispondenti.
4. Selezionare i criteri di aggiornamento richiesti.
5. Fare clic su Invia. Gli utenti non amministratori che appartengono a questo gruppo di utenti possono ora accedere ai criteri disponibili solo nel gruppo di risorse selezionato.

Per associare il gruppo di risorse a un gruppo di utenti, creare un criterio di accesso.

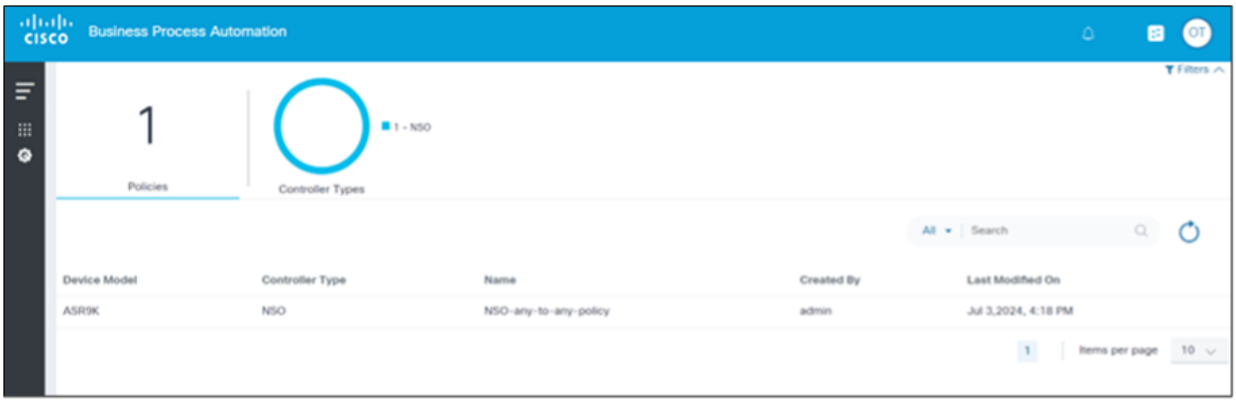


Aggiungi criteri di accesso

Nota: Una volta creato, il gruppo di risorse deve essere associato a un gruppo di utenti tramite i criteri di accesso. Per ulteriori informazioni su quanto segue, fare riferimento a Controllo di accesso:

- Utenti
- Ruoli
- Gruppi di utenti
- Criteri di accesso
- Gruppi di risorse
- Gruppi di asset

Di seguito è riportato un esempio di utente non amministratore che ha accesso a risorse limitate:



Utente non amministratore con limitazioni di risorse

Impostazione del flag di trust zero

Le risorse accessibili da un utente possono variare in base all'impostazione del flag di attendibilità zero. Il flag di attendibilità zero può essere impostato su true o false. Nella tabella seguente vengono riepilogate le possibilità di accesso alle risorse in base all'impostazione del flag di attendibilità zero.

Utente	Gruppo utenti	Criteri di accesso	Gruppo di risorse	Risorse	Attendibilità totale	Attivato
Utente 1	UG1	AP1	RG1	2 risorse	2 risorse	2 risorse
Utente 1	UG1	AP2	RG2	0 risorse	0 risorse	0 risorse
Utente 1	UG1	AP3	Nessuno		0 risorse	Tutte le risorse
Utente 1	UG1	Nessuno	Nessuno		0 risorse	Tutte le risorse

Per attivare o disattivare il flag di attendibilità zero:

1. Passare al seguente percorso di configurazione:

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

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

2. Modificare il valore zeroTrustPolicies.
3. Passare al seguente bundle principale:

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

4. Per eliminare il timone principale, eseguire il comando seguente:

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

5. Eseguire il comando seguente per controllare lo stato dei pod

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

6. Eseguire il seguente comando per installare il timone principale dopo l'interruzione di tutti i pod:

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

7. Eseguire il comando seguente per verificare lo stato dei pod che vengono visualizzati:

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

Risoluzione dei problemi di aggiornamento del sistema operativo

In questa sezione vengono forniti suggerimenti per la risoluzione dei problemi relativi ai problemi osservati con l'applicazione Aggiornamento sistema operativo in BPA.

Impossibile visualizzare il modello del dispositivo di destinazione durante la creazione di un criterio di conformità

Assicurarsi che i metadati dell'immagine corrispondente siano disponibili in Immagini software in SWIM. Se non viene trovato, eseguire una delle opzioni seguenti:

- Sincronizzare le immagini per recuperare i metadati delle immagini da controller quali Cisco Catalyst Center, NDFC, vManage e FMC
- Creare i metadati dell'immagine necessari per controller quali NSO, CNC, Direct-to-Device e ANSIBLE

Conformità software: stato non operativo

Ciò potrebbe essere dovuto ai motivi seguenti:

- Nessuna risorsa trovata con il modello selezionato durante la creazione dei criteri di conformità software
- Il nome del modello in SWIM non corrisponde al modello di dispositivo di conformità nell'inventario dei dispositivi per tutti i dispositivi
- Se l'unità SMU è stata scelta come parte della creazione della conformità software e il rilevamento dell'unità SMU non è riuscito per tutti i dispositivi
- Il modello di processo selezionato per l'esecuzione del modello di controllo di conformità non è riuscito o non è stato trovato
- Il numero di serie o la versione corrente non è disponibile per tutti i dispositivi nel modello selezionato durante la creazione della conformità software

Lo stato dei risultati di conformità software di alcuni dispositivi è sconosciuto

Ciò potrebbe essere dovuto ai motivi seguenti:

- Il nome del modello in SWIM non corrisponde al modello del dispositivo di conformità nell'inventario dei dispositivi
- Se l'unità SMU è stata scelta come parte della creazione della conformità software e il rilevamento dell'unità SMU non è riuscito per un dispositivo
- Il modello di processo selezionato per l'esecuzione del modello di controllo di conformità non è riuscito o non è stato trovato
- Il numero di serie o la versione corrente non è disponibile per i dispositivi

Percentuale avanzamento processo di aggiornamento

Se la percentuale di completamento del processo di aggiornamento è inferiore a 100 anche se l'aggiornamento è stato completato, verificare che le impostazioni Attendi rollback siano abilitate in Aggiornamento sistema operativo > Impostazioni > Rollback e che l'opzione Verifica utente sia attivata. Se la percentuale di completamento complessiva rimane inferiore a 100, selezionare Rollback o Completo.

È stata raggiunta la pianificazione del processo. I dispositivi sono bloccati in stato di attesa

Se dopo l'avvio del processo pianificato i dispositivi sono bloccati in stato di attesa, provare a riavviare i micro servizi Kafka, Camunda, Scheduler e OS Upgrade.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).