Conformità e risoluzione della configurazione della Guida per l'utente BPA versione 5.1

- Monitoraggio dei log di conformità

Introduzione

L'applicazione CnR (Configuration Compliance and Remediation) consente agli operatori di rete di eseguire controlli di conformità della configurazione dei dispositivi per i criteri personalizzati costruiti dai blocchi di configurazione. Gli operatori creano manualmente o automaticamente blocchi di configurazione utilizzando il sistema da configurazioni di dispositivi selezionate. Gli utenti possono inoltre stabilire regole da applicare a questi blocchi, con condizioni delle regole potenzialmente derivate dai valori ottenuti dall'applicazione RefD. Gli operatori possono eseguire i controlli di conformità in base a un programma oppure avviare i controlli immediatamente.

L'applicazione è dotata di un dashboard intuitivo che offre una panoramica completa delle violazioni della conformità, offrendo sia riepiloghi che viste dettagliate a livello di dispositivo e blocco di configurazione.

L'applicazione include un solido framework di correzione per la gestione delle violazioni di conformità. Questa struttura utilizza workflow e modelli, sia modelli di configurazione, noti come GCT (Golden Configuration Templates) che modelli di processo, per semplificare il processo di correzione. Analogamente ai controlli di conformità, è possibile programmare le attività di correzione da eseguire in base a un calendario oppure attivarle immediatamente per affrontare le violazioni tempestivamente.

Il dashboard per la conformità e la risoluzione dei problemi del portale di nuova generazione (Next-Gen) include funzionalità progettate per migliorare la gestione della sicurezza di rete, semplificare le procedure di conformità e le attività di risoluzione dei problemi. Il dashboard fornisce un riepilogo completo della conformità delle risorse e delle policy, semplificando la valutazione dello stato della rete da parte degli operatori e garantendo la conformità dei dispositivi ai rigidi protocolli di sicurezza.

I blocchi di configurazione possono essere generati automaticamente e quindi modificati o aggiunti manualmente, offrendo un equilibrio tra automazione e personalizzazione. L'identificazione precisa da parte del sistema dei blocchi di configurazione e dei meccanismi granulari di controllo dell'accesso, incluse le impostazioni dettagliate di utenti, gruppi e autorizzazioni su interfacce classiche e moderne, garantiscono che le configurazioni di rete rimangano sicure e nelle mani di personale affidabile. Queste funzionalità forniscono un potente set di strumenti per le organizzazioni che desiderano mantenere elevati standard di sicurezza e conformità di rete.

Novità

Sono stati introdotti i seguenti miglioramenti e caratteristiche principali:

- Un dashboard di reporting completo per generare, visualizzare e scaricare i report di conformità
- Possibilità di eseguire controlli di conformità offline caricando le configurazioni dei dispositivi senza caricare il dispositivo tramite Asset Manager
- Possibilità di configurare i modelli nella configurazione a blocchi per mascherare i dati di configurazione dei dispositivi sensibili
- Possibilità di esportare i dati della griglia di riepilogo di conformità alle regole e agli asset come file CSV
- Visualizza e confronta le configurazioni di monitoraggio e aggiornamento generate con le configurazioni in esecuzione sui dispositivi
- Miglioramenti nei blocchi per supportare l'aumento delle violazioni se la configurazione esiste
- Abilitare un'esperienza utente connessa nelle pagine di creazione e modifica dei criteri per l'avvio incrociato nei componenti figlio, ad esempio la pagina di creazione del blocco
- Miglioramento dei processi di conformità per la creazione e la modifica di pagine da utilizzare per il lancio incrociato nella pagina di modifica dei criteri

Componenti

Conformità e monitoraggio e aggiornamento supportano i seguenti controller e tipi di dispositivi:

Controller	Tipi di sistema operativo
NSO (6.5)	IOS XE, IOS XR, NX-OS, JunOS, Nokia SR-OS
CNC (6.0)	IOS XE, IOS XR, NX-OS
NDFC (3.2.0 / Fabric v12.2.2)	NX-OS
Cisco Catalyst Center (2.3.5)	IOS XE, IOS XR. Solo conformità convalidata
CCP (7.2.5)	FX-OS (FTD). Solo conformità convalidata
D2D (Direct To Device)	IOS XE, IOS XR, JunOS

Nota: Il supporto di Nokia SR-OS tramite controller NSO è applicabile solo alla funzionalità di conformità alla configurazione. Monitoraggio e aggiornamento non supportati per i dispositivi Nokia.

Nota: La funzionalità di conformità funziona con la configurazione dei dispositivi nel formato Cisco Command Line Interface (CLI) e nel formato YAML per i dispositivi Juniper e Nokia.

Attualmente, il framework non supporta altri formati come Netconf, JSON, XML, ecc.

Come parte della versione 5.0, l'applicazione classica CnR (Compliance and Remediation) è stata deprecata. Tutte le funzionalità CnR sono ora completamente integrate e disponibili nel portale di nuova generazione.

Presupposti e prerequisiti

Per utilizzare in modo efficace lo Use Case CnR, è necessario soddisfare i seguenti prerequisiti.

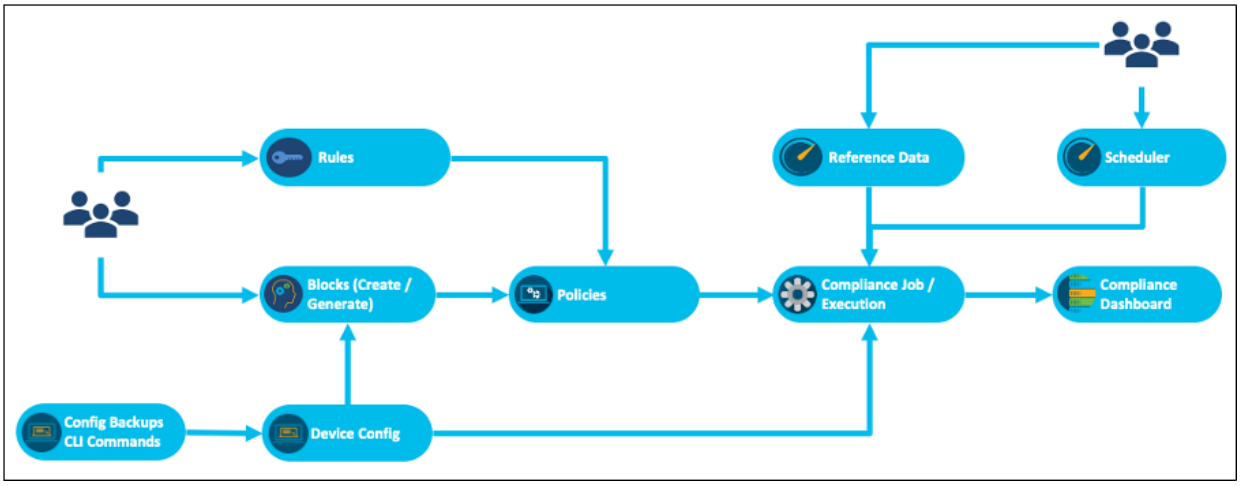
- È necessario caricare la chiave di sottoscrizione per lo Use Case CnR.
- Il controller e i dispositivi pertinenti devono essere integrati e disponibili come parte di BPA Asset Manager. Per ulteriori informazioni, consultare la sezione Asset Manager della Guida dell'utente di BPA.
- Gli asset integrati devono essere raggruppati, in base ai requisiti del cliente, in gruppi nel portale di nuova generazione.

Dashboard di conformità

Il dashboard di conformità fornisce una visualizzazione riepilogativa delle violazioni su tutti i dispositivi per il tempo selezionato. Per impostazione predefinita, vengono visualizzati i dati relativi al mese corrente. Gli utenti possono modificare la finestra temporale per visualizzare i dati cronologici sulle violazioni di conformità. Il mese corrente è la visualizzazione selezionata predefinita.

Nota: Il dashboard di conformità deprecato nell'interfaccia utente classica è stato rimosso e non è più disponibile. Utilizzare il dashboard disponibile nel portale di nuova generazione.

Diagramma di flusso della conformità della configurazione



Panoramica del componente di conformità alla configurazione

Le violazioni di conformità visualizzate nel dashboard vengono popolate quando viene eseguito un processo di conformità per un criterio in base a un elenco di asset. Il criterio di conformità viene creato aggiungendo un elenco di configurazioni di blocchi con le regole di conformità necessarie. La regola di conformità può disporre di controlli con valori statici o variabili dinamiche per le quali vengono recuperati dati dall'applicazione RefD. Un processo di conformità può essere eseguito su richiesta oppure come programma occasionale o ricorrente.

La conformità della configurazione include le seguenti importanti funzionalità:

- Creazione blocchi: I blocchi vengono creati manualmente o automaticamente utilizzando il modello TTP (Template Text Parser). Possono essere statici o dinamici (con variabili).
- Creazione regole: Le regole convalidano le variabili nei blocchi. I valori delle regole possono essere impostati in modo statico o recuperati dinamicamente dal sistema dei dati di riferimento (RefD) durante il tempo di esecuzione.
- Creazione criteri: I criteri vengono creati selezionando l'elenco dei blocchi e le regole corrispondenti. I dati per le regole possono essere statici o recuperati dinamicamente dal framework RefD in fase di esecuzione.
- Creazione di processi per la conformità: I processi di conformità vengono creati selezionando un criterio e un gruppo di asset (contenente un elenco di asset) per eseguire il controllo di conformità. Gli utenti possono scegliere di recuperare la configurazione del dispositivo dal framework di backup o eseguire comandi dinamici tramite modelli di processo sui dispositivi durante l'esecuzione. Il recupero della configurazione dal backup consente di eseguire il controllo offline dei dispositivi senza la necessità di connettersi a un dispositivo attivo. I processi possono essere programmati o eseguiti su richiesta.
- Violazioni di conformità: Visualizzare le violazioni di conformità nel dashboard.

Riepilogo sulla conformità degli asset

La scheda Riepilogo sulla conformità degli asset è una funzione essenziale progettata per fornire una panoramica completa delle violazioni della conformità su tutti i dispositivi all'interno di una

rete. Questa scheda consente agli utenti di identificare rapidamente i problemi di conformità, garantendo che tutti i dispositivi siano conformi alle policy e agli standard stabiliti. L'interfaccia è dotata di potenti funzionalità di filtraggio e ricerca che semplificano la navigazione e l'analisi dei dati di conformità.

Caratteristiche principali

- Riepilogo violazioni per dispositivo: La scheda mostra un riepilogo delle violazioni di conformità per ciascun dispositivo, fornendo agli utenti una rapida istantanea dello stato di conformità complessivo classificato in base ai livelli di gravità, ad esempio critico, alto, medio e basso.
- Informazioni dettagliate sulle violazioni: Per ciascun dispositivo, la finestra popup fornisce informazioni dettagliate sui criteri violati e l'utente può eseguire un'ulteriore analisi del blocco e della linea di configurazione che ha causato la violazione.

Visualizza riepilogo conformità cespiti

- Opzioni di filtro avanzate: I filtri posizionati nella parte superiore e sinistra della scheda consentono agli utenti di restringere la visualizzazione dei dati nella griglia. Gli utenti possono filtrare per intervallo di date, Asset Group, famiglia di prodotti e altro ancora, consentendo un'analisi mirata dei dati di conformità.
- Funzionalità di ricerca: È disponibile un campo di ricerca per perfezionare ulteriormente i dati nella griglia. Gli utenti possono individuare rapidamente dispositivi specifici o gestirli tramite il controller immettendo parole chiave o frasi rilevanti.
- Intervallo di date personalizzabile: Per impostazione predefinita, il mese corrente viene selezionato nel filtro dell'intervallo di date e fornisce i dati di conformità più recenti. Gli utenti possono tuttavia personalizzare l'intervallo di date per visualizzare i dati.
- Filtri: Sono disponibili più filtri, ad esempio Famiglia di prodotti, Gruppo asset e Tipo di audit. Applicare il filtro per aggiornare la griglia.

Riepilogo sulla conformità degli asset

- Esporta come CSV: Funzionalità disponibile per consentire agli utenti di ottenere una copia locale della conformità della configurazione delle risorse per scopi di analisi, creazione di report e archiviazione offline. Per esportare i dati come file CSV, selezionare Esporta come CSV dall'icona Altre opzioni. Il file CSV scaricato contiene i dati attualmente visualizzati nella griglia, rispettando i filtri applicati.

Riepilogo conformità asset: Esporta come CSV

Dettagli del file CSV per la conformità degli asset

Il file CSV include tutte le colonne visibili nella griglia Riepilogo conformità asset, ad esempio il nome del dispositivo, l'istanza del controller (gestita da), la famiglia di prodotti del dispositivo, lo stato di conformità del dispositivo, il numero di violazioni per gravità (ad esempio, Critico, Principale, Secondario, Avviso, Informazioni, Sconosciuto) e la data dell'ultimo controllo di conformità del dispositivo.

Se la griglia contiene l'impaginazione, l'esportazione include tutti i record nelle pagine, non solo la pagina visibile.

Apertura e utilizzo del file CSV per la conformità degli asset

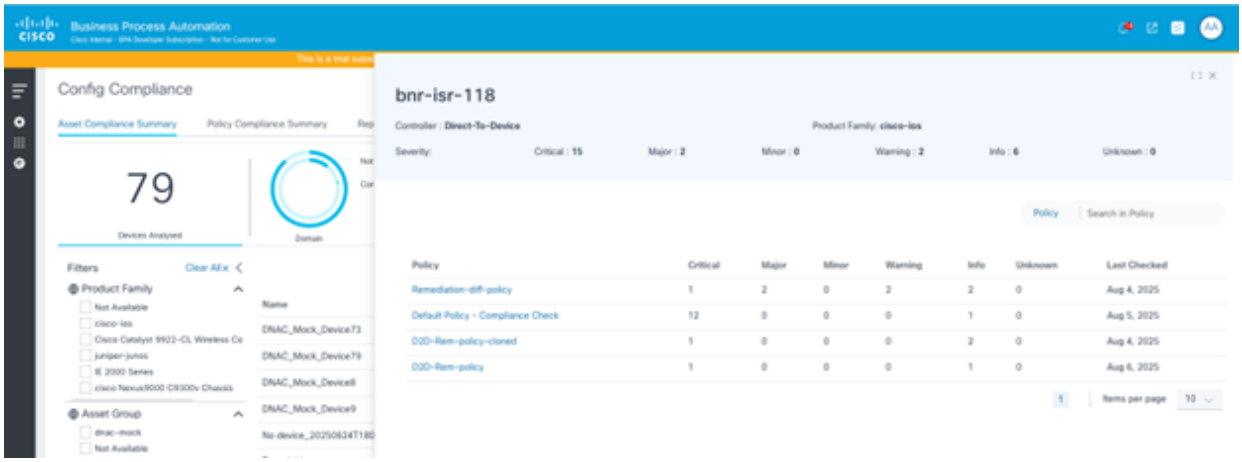
1. Aprire il file CSV scaricato in Excel o in qualsiasi applicazione per fogli di calcolo compatibile.
2. Verificare che il contenuto corrisponda a quanto visualizzato nella griglia Riepilogo conformità asset, inclusi i risultati filtrati.

	A	B	C	D	E	F	G	H	I	J	K
1	Device Name	Managed By	Product Family	Compliance	Critical	Major	Minor	Warning	Info	Unknown	Last Checked
2	CNC-bnr-asr-78	Direct-To-Device	IE 2000 Series	Non Compliant	1	0	0	0	0	0	04-Aug-25
3	D2d-118	Direct-To-Device	IE 2000 Series	Partially Compliant	0	1	0	1	1	0	04-Aug-25
4	D2d-juniper	Direct-To-Device	juniper-junos	Partially Compliant	0	0	0	2	2	1	06-Aug-25
5	DNAC_Mock_Device0	DNAC-Mock	Cisco Catalyst 9922-CL Wireless Controller for Cloud	Unknown	0	0	0	0	0	1	05-Aug-25
6	bnr-asr-78	cnc6		Partially Compliant	0	0	1	0	0	0	05-Aug-25
7	bnr-isr-118	Direct-To-Device	cisco-ios	Partially Compliant	15	2	0	2	6	0	06-Aug-25
8	bnr-n3k-44	NSO-166	cisco Nexus9000 C9300v Chassis	Partially Compliant	12	0	0	0	3	0	05-Aug-25
9											

Riepilogo conformità asset: File CSV aperto nell'applicazione Excel

Visualizzazione del sintetico di conformità degli asset per criterio

Facendo clic su una riga della griglia Riepilogo conformità asset vengono visualizzati i dettagli delle violazioni degli asset, suddivisi in categorie in base ai diversi criteri in base ai quali il dispositivo viene convalidato. In questa vista dettagliata gli utenti possono visualizzare il conteggio delle violazioni in base alla gravità in ogni criterio.



Riepilogo conformità asset: Riepilogo conformità per criterio

---

Nota: Si noti quanto segue.
- Il collegamento ipertestuale nella colonna Criterio indirizza gli utenti alla pagina dei dettagli del criterio
- Se si fa clic su una riga, viene visualizzata la pagina Dettagli violazione relativa al criterio

---

selezionato

Visualizzazione dei dettagli delle violazioni

La pagina Dettagli violazioni visualizza le violazioni a livello di blocco e di regola sovrapposte nella configurazione del dispositivo. Gli utenti possono inoltre visualizzare la configurazione del blocco e le configurazioni di correzione consigliate.

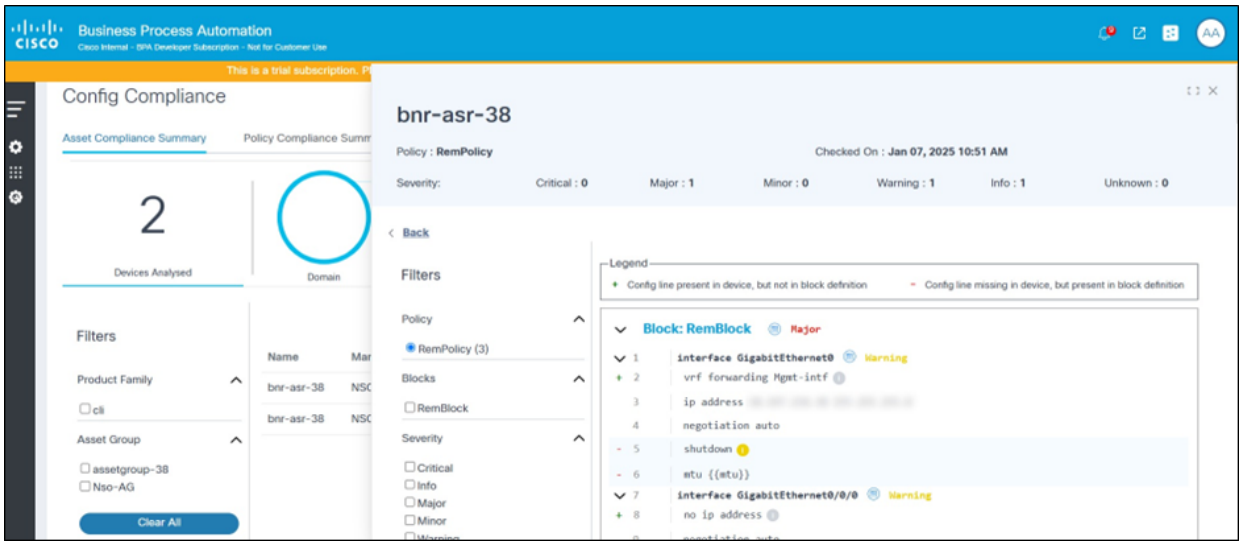
Per visualizzare la pagina Dettagli violazioni dalla pagina Riepilogo conformità asset insieme alla suddivisione dei livelli dei criteri:

1. Selezionare una riga nella griglia Conformità asset. Viene visualizzato un popup. Nella griglia viene visualizzata una suddivisione dei dettagli di conformità per criterio.
2. Selezionate una riga nella griglia. Verrà visualizzata la pagina Dettagli violazione.

Per visualizzare la pagina Dettagli violazioni dalla griglia Riepilogo conformità criteri:

1. Selezionare la griglia di conformità ai criteri.
2. Selezionare una riga > Griglia cespite interessato.
3. Selezionare una riga. Verrà visualizzata la pagina Dettagli violazioni.

La parte destra della pagina Dettagli violazioni mostra i blocchi di configurazione del dispositivo e sovrappone le violazioni sopra di esso. Le violazioni vengono elencate rispetto alle righe di configurazione corrispondenti. In caso di errore di una condizione, la barra multifunzione delle violazioni fornisce i dettagli relativi al nome della regola, alla condizione e alla configurazione prevista (definita nella regola) rispetto alla configurazione recuperata dalla configurazione del dispositivo.



Violazioni di conformità degli asset

Simboli di blocco

- Un segno "+" su una riga indica che la configurazione non è prevista in base alla configurazione del blocco, ma che è presente anche nella configurazione del dispositivo.
- Un segno "-" su una riga indica che la configurazione è prevista in base alla configurazione del blocco ma non è presente nella configurazione del dispositivo.

Filtri

La sezione dei filtri sul lato sinistro della pagina consente agli utenti di eseguire le operazioni riportate di seguito.

- Cambiare la politica; la pagina verrà aggiornata e verranno caricate le violazioni per il nuovo criterio selezionato
- Selezionare le caselle di controllo Blocchi per visualizzare le violazioni relative ai blocchi selezionati
- Selezionare le caselle di controllo Gravità per visualizzare le violazioni con il livello o i livelli di gravità specificati
- Selezionare le caselle di controllo Tipo di violazione per visualizzare le violazioni del tipo selezionato:
    - Mancata corrispondenza ordine: L'ordine delle righe di configurazione del dispositivo non corrisponde all'ordine definito nella configurazione del blocco
    - Configurazione mancante: Visualizza le righe di configurazione previste in base alla configurazione del blocco ma mancanti nella configurazione del dispositivo
    - Configurazione aggiuntiva: Visualizzare le righe di configurazione non previste in base alla configurazione del blocco, ma presenti anche nella configurazione del dispositivo.
    - Errori regola: Errori di una o più condizioni nelle regole.
    - Blocchi mancanti: L'intero blocco di configurazione del dispositivo è mancante o non corrisponde alla configurazione del blocco definita.
    - Blocchi ignorati: Questo blocco di configurazione viene ignorato perché le condizioni del filtro del blocco non sono soddisfatte.

Visualizzazione e confronto della configurazione di monitoraggio e aggiornamento

La pagina Configurazione di monitoraggio e aggiornamento visualizza la configurazione generata per il dispositivo selezionato per ciascuno dei blocchi in un determinato criterio. La configurazione viene generata e considera i dettagli relativi al blocco e alla regola presenti nel criterio, nonché la configurazione del dispositivo recuperata durante l'esecuzione della conformità. Gli utenti hanno la possibilità di aggiornare la configurazione nella stessa pagina. È possibile eseguire il push della configurazione generata nel dispositivo utilizzando la funzionalità dei processi di monitoraggio e

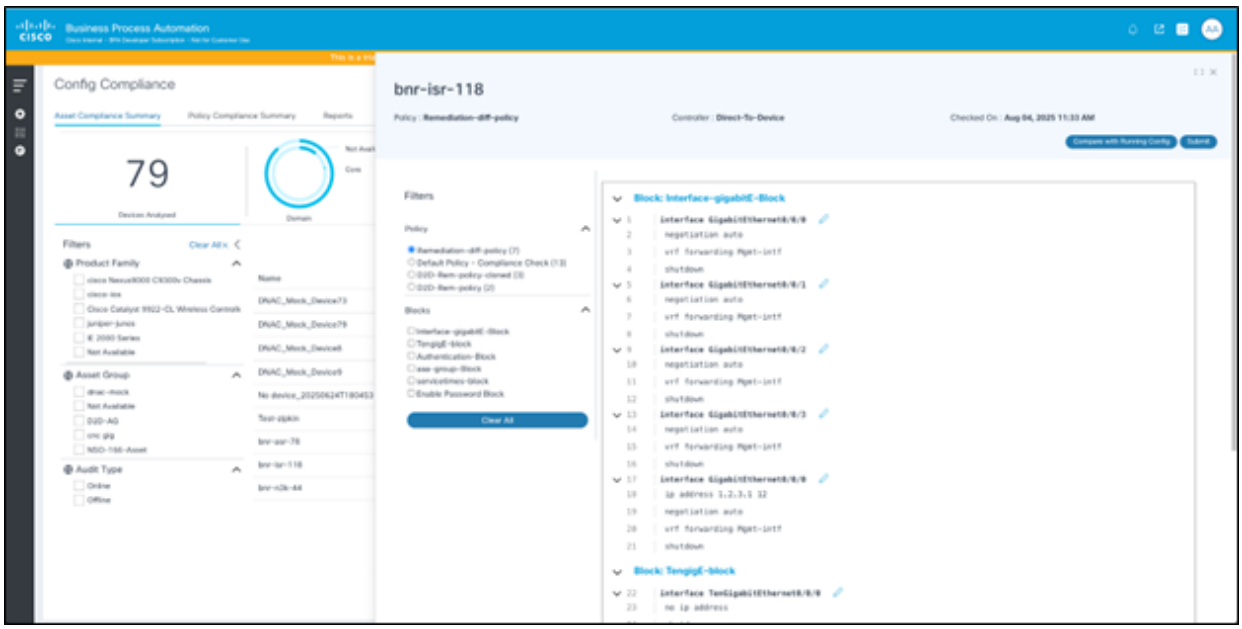
aggiornamento. Inoltre, questa pagina fornisce agli utenti un'opzione per confrontare la configurazione generata con la periferica che esegue la configurazione corrente. L'utente può specificare uno o più comandi per recuperare la configurazione del dispositivo corrente.

Per visualizzare la pagina Configurazione correzione dalla griglia Conformità asset:

1. Fare clic sulla scheda Riepilogo conformità asset.
2. Nella griglia di conformità degli asset nella colonna Azione, selezionare l'icona Altre opzioni > Visualizza configurazione di monitoraggio e aggiornamento. Verrà visualizzata la pagina Configurazione di monitoraggio e aggiornamento.

Per visualizzare la pagina Configurazione di correzione dalla griglia Conformità ai criteri:

1. Fare clic sulla scheda Riepilogo conformità ai criteri.
2. Nella griglia di conformità ai criteri, selezionare la riga desiderata. Viene visualizzata la griglia Asset interessati.
3. Nella colonna Azione, selezionare l'icona Altre opzioni > Seleziona Visualizza configurazione di monitoraggio e aggiornamento. Verrà visualizzata la pagina Configurazione di monitoraggio e aggiornamento.

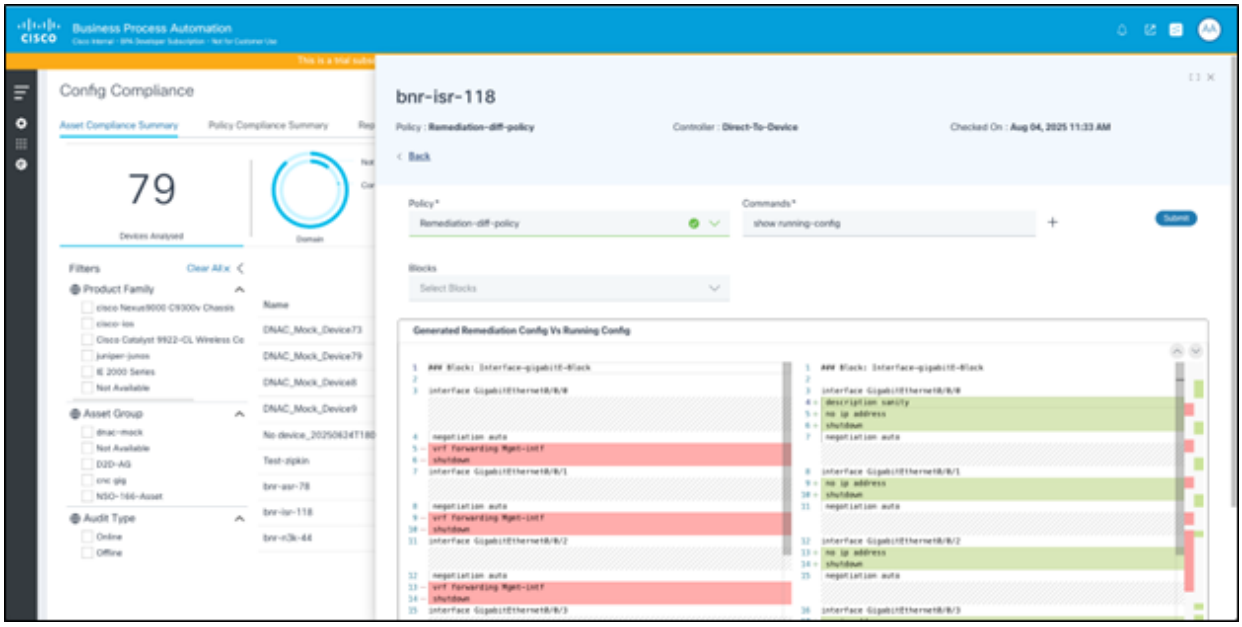


Pagina Configurazione di monitoraggio e aggiornamento

La pagina Configurazione di correzione visualizza quanto segue:

- Configurazione di monitoraggio e aggiornamento generata: La configurazione generata viene visualizzata sul lato destro della pagina, insieme all'opzione che consente agli utenti di modificare i blocchi di configurazione e inviare le modifiche da salvare
- Filtri: I filtri possono essere utilizzati per selezionare un criterio e quindi facoltativamente uno

o più blocchi per visualizzare la configurazione generata corrispondente
- Confronta con configurazione in esecuzione: Fare clic su Confronta con configurazione corrente per visualizzare una pagina dettagliata che consente agli utenti di confrontare la configurazione generata con il dispositivo che esegue la configurazione



Pagina Confronta con configurazione in esecuzione

La pagina Confronta con configurazione in esecuzione visualizza quanto segue:

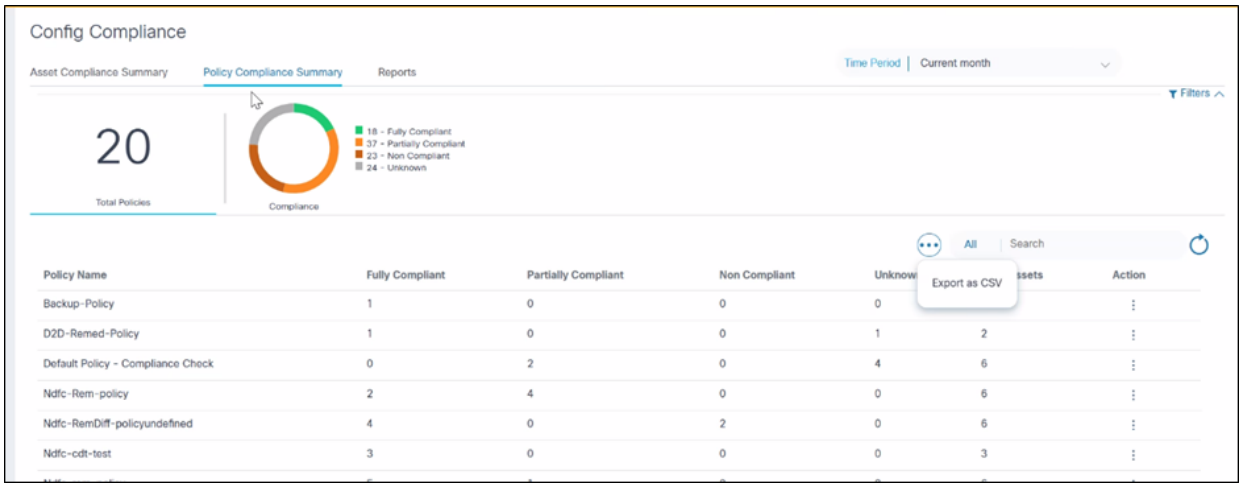
- Opzione per la selezione di un criterio: Il criterio selezionato nella pagina precedente è preselezionato.
- Casella di testo in cui immettere uno o più comandi da eseguire sul dispositivo
- Un pulsante Submit (Invia) per eseguire i comandi sul dispositivo e recuperare la configurazione
- Opzione per visualizzare e filtrare i blocchi: Per impostazione predefinita, vengono visualizzati tutti i blocchi all'interno del criterio. gli utenti possono selezionare singoli blocchi in base alle esigenze
- Un visualizzatore delle differenze di configurazione che mostra la configurazione generata e la configurazione del dispositivo affiancate, evidenziando le differenze

Riepilogo sulla conformità ai criteri

La scheda Riepilogo conformità alle policy è progettata per fornire una panoramica chiara e concisa dello stato di conformità dei dispositivi rispetto alle policy definite. Questa scheda consente agli utenti di valutare rapidamente lo scenario relativo alla conformità e di identificare le aree problematiche. La scheda classifica i dispositivi in base allo stato di conformità, semplificando la comprensione e la gestione della conformità.

Stati di conformità:

- Pienamente conforme: Tutti i dispositivi soddisfano tutte le regole di conformità per la rispettiva policy.
- Parzialmente conforme: Alcuni dispositivi sono conformi alle norme, mentre altri non lo sono.
- Non conforme: Nessun dispositivo è conforme ai criteri.
- Sconosciuto: Impossibile verificare la conformità del criterio a causa di problemi con la connessione di rete o l'indisponibilità dei backup.



Riepilogo sulla conformità ai criteri con esportazione CSV

Esporta come CSV per la conformità alle policy

La funzione Esporta come file CSV consente agli utenti di ottenere una copia locale della conformità ai criteri per l'analisi, la creazione di report e l'archiviazione offline. Per esportare i dati come file CSV, selezionare Esporta come CSV dall'icona Altre opzioni. Il file CSV scaricato contiene i dati attualmente visualizzati nella griglia, rispettando i filtri applicati.

Dettagli del file CSV per la conformità ai criteri

Il file CSV include il nome del criterio, il conteggio totale delle risorse convalidate e l'analisi del conteggio per stato di conformità (ad esempio, Completamente conforme, Parzialmente conforme, Non conforme e Sconosciuto). Se la griglia contiene l'impaginazione, l'esportazione include tutti i record di tutte le pagine, non solo quelli visualizzati nella pagina corrente.

Apertura e utilizzo del file CSV per la conformità alle policy

1. Aprire il file CSV scaricato in Excel o in qualsiasi applicazione per fogli di calcolo compatibile.

2. Verificare che il contenuto corrisponda a quanto visualizzato nella griglia Riepilogo conformità criteri, inclusi i risultati filtrati.

	A	B	C	D	E	F
1	Policy Name	Fully Compliant	Partially Compliant	Non Compliant	Unknown	Total Assets
2	D2D-Juniper-policy	0	1	0	0	1
3	D2D-Raiseviolation-policy	0	1	0	0	1
4	D2D-Rem-policy	0	1	0	2	3
5	D2D-Rem-policy-cloned	0	1	0	0	1
6	Default Policy - Compliance Check	0	2	0	70	72
7	Policy Delete Issue	1	0	0	0	1
8	Policy Test	1	0	0	0	1
9	Remediation-diff-policy	0	1	0	0	1
10	cnc gig policy	0	1	0	0	1
11	cnc gigabit	0	2	1	1	4
12						

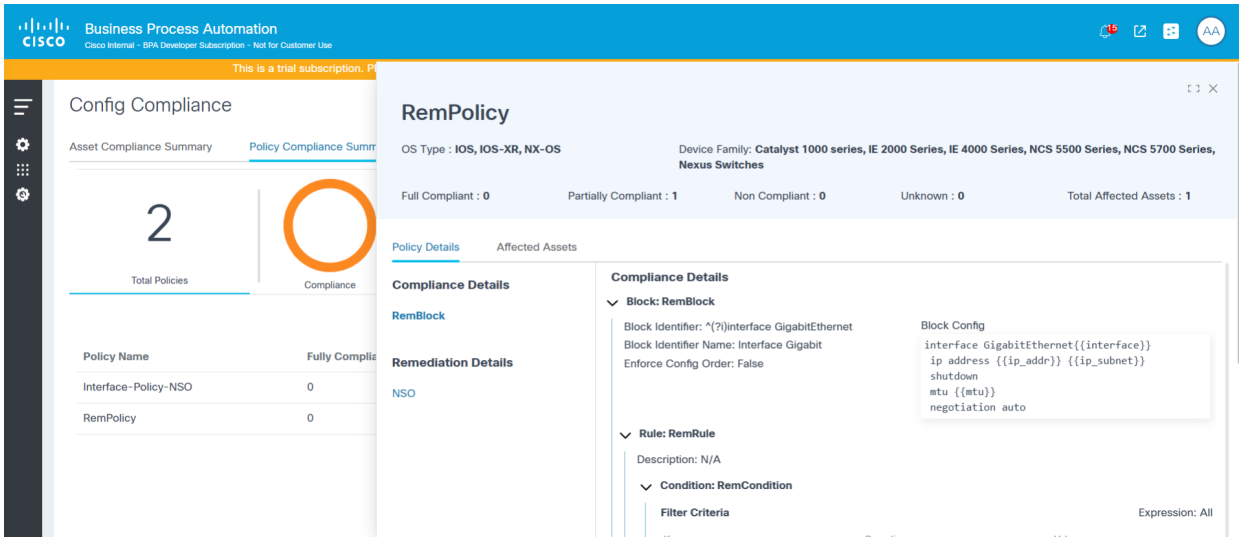
Conformità alle regole: Dettagli criteri

Visualizzazione dei dettagli dei criteri

Per visualizzare i dettagli dei criteri:

1. Selezionare un criterio dall'icona Altre opzioni nella colonna Azione.
2. Selezionare Visualizza dettagli criteri. Viene visualizzata la pagina Dettagli criterio.

Nota: La pagina Dettagli criterio è una visualizzazione di sola lettura di tutte le informazioni sui criteri, inclusi blocchi, regole e condizioni.Gli utenti possono fare clic sui collegamenti ipertestuali all'interno della pagina che consente di passare direttamente al blocco pertinente.



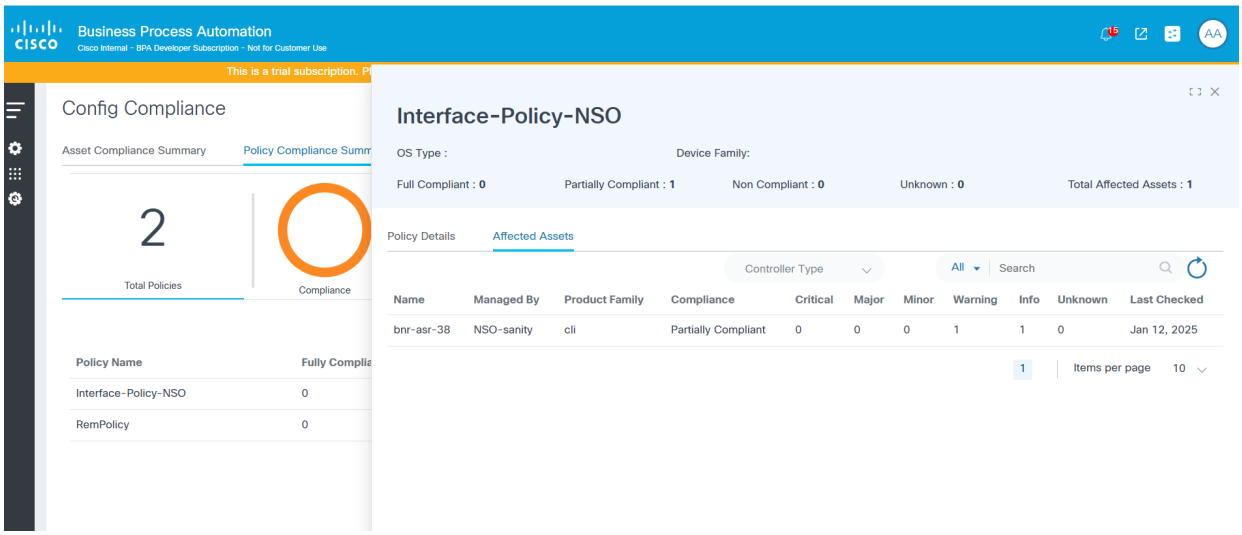
Conformità alle regole: Dettagli criteri

Visualizzazione dei cespiti interessati

La scheda Asset interessati visualizza l'elenco degli asset analizzati in ciascun criterio e il conteggio delle violazioni diviso per severità. I dispositivi possono essere filtrati utilizzando l'elenco a discesa Controller Type (Tipo di controller) e la casella di ricerca.

Per visualizzare i cespiti interessati dalla scheda Riepilogo conformità criteri:

1. Selezionare una riga. Viene visualizzata la finestra Criteri di conformità.
2. Fare clic sulla scheda Asset interessati.



Conformità alle regole: Asset interessati

Nota: La scheda Cespiti interessati fornisce le azioni necessarie per aprire le pagine Visualizza dettagli violazione e Visualizza configurazione di correzione. Per ulteriori informazioni, fare riferimento a Riepilogo conformità cespiti.

Report

La sezione Report è progettata per fornire informazioni complete sulla conformità dei dispositivi, identificare le violazioni e semplificare le attività di correzione. L'applicazione offre un'interfaccia intuitiva per la generazione, la visualizzazione, il download e la gestione di vari tipi di report di conformità.

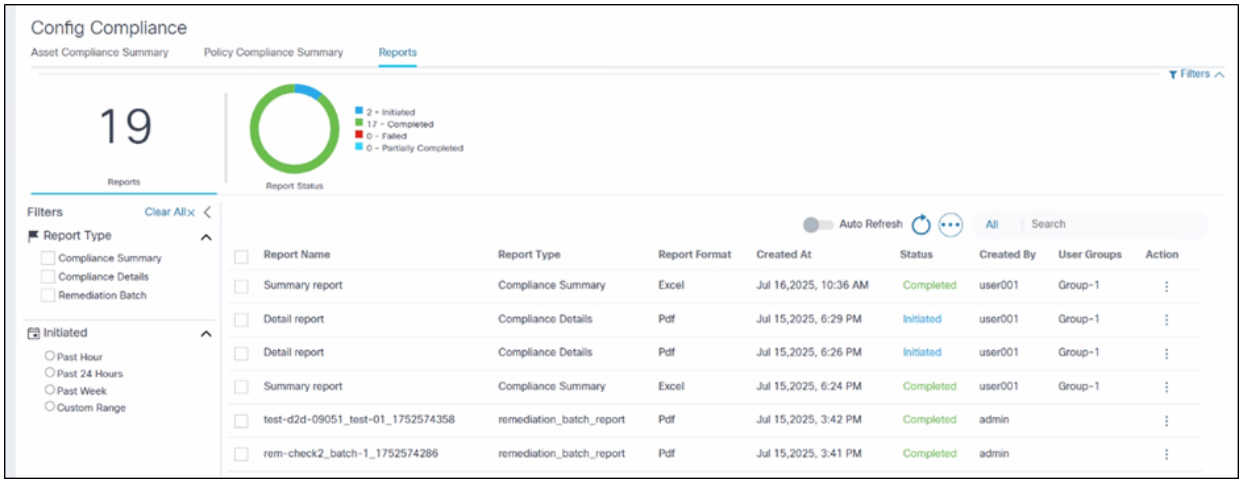
Dashboard report

Il dashboard di report funge da hub centrale per tutte le attività di reporting di conformità. Gli utenti

possono gestire in modo efficiente i report da un'unica interfaccia. Le funzionalità chiave disponibili nel pannello di controllo dei rapporti includono:

- Visualizzazione dei report: Gli utenti possono visualizzare una lista di tutti i report generati, inclusi il nome, il tipo, il criterio associato, il formato, la data di creazione e lo stato corrente (ad esempio Iniziato, Completato, Non riuscito, Completato parzialmente)
- Download dei report: I report, una volta generati, possono essere scaricati a scopo di analisi o archiviazione offline; la colonna Azione fornisce le opzioni per il download
- Eliminazione dei report: Gli utenti hanno la possibilità di rimuovere dal dashboard i report vecchi o non necessari, contribuendo a mantenere un ambiente di reporting pulito e organizzato
- Filtro e ricerca: Il dashboard offre opzioni di filtro complete, consentendo agli utenti di individuare rapidamente report specifici in base a criteri quali il tipo di report (ad esempio, dettagli di conformità, riepilogo di conformità, batch di risoluzione), la policy e lo stato di avvio (ad esempio, Ultima ora, Ultime 24 ore, Ultima settimana, Intervallo personalizzato); è disponibile anche una barra di ricerca
- Monitoraggio stato report: Un riepilogo visivo, ad esempio un grafico a torta, indica lo stato dei report, visualizzando il numero di report avviati, completati, non riusciti o parzialmente completati.

Il pannello di controllo Report è la pagina iniziale della scheda Report nel pannello di controllo Conformità e monitoraggio e aggiornamento.



Dashboard report

- I tipi di report disponibili includono:
  - Rapporto Riepilogo conformità
  - Rapporto dettagliato sulla conformità
  - Rapporto batch di monitoraggio e aggiornamento
- Utilizzare i filtri per selezionare quanto segue:
  - Tipo di report
  - Policy
  - Periodo di tempo avviato (l'elenco dei report viene filtrato in base all'intervallo di tempo

selezionato)
- Opzione per l'aggiornamento automatico dell'elenco di report

Configurazioni report

Le configurazioni di reporting consentono a un amministratore di configurare i parametri chiave relativi ai report, in base ai requisiti di distribuzione e business. Per la configurazione sono disponibili i seguenti parametri:

- Elimina automaticamente rapporti anteriori a (giorni): Tutti i report precedenti a questa durata vengono eliminati dal sistema
- Numero massimo di blocchi da selezionare per criterio in un report Riepilogo conformità: Consente di mantenere il numero di schede nel file di Excel a un limite leggibile
- Numero massimo di cespiti da selezionare in un rapporto dettagliato sulla conformità: Consente di limitare il numero di file PDF generati per un determinato report dettagliato

Elenco processi di conformità

Generazione di report

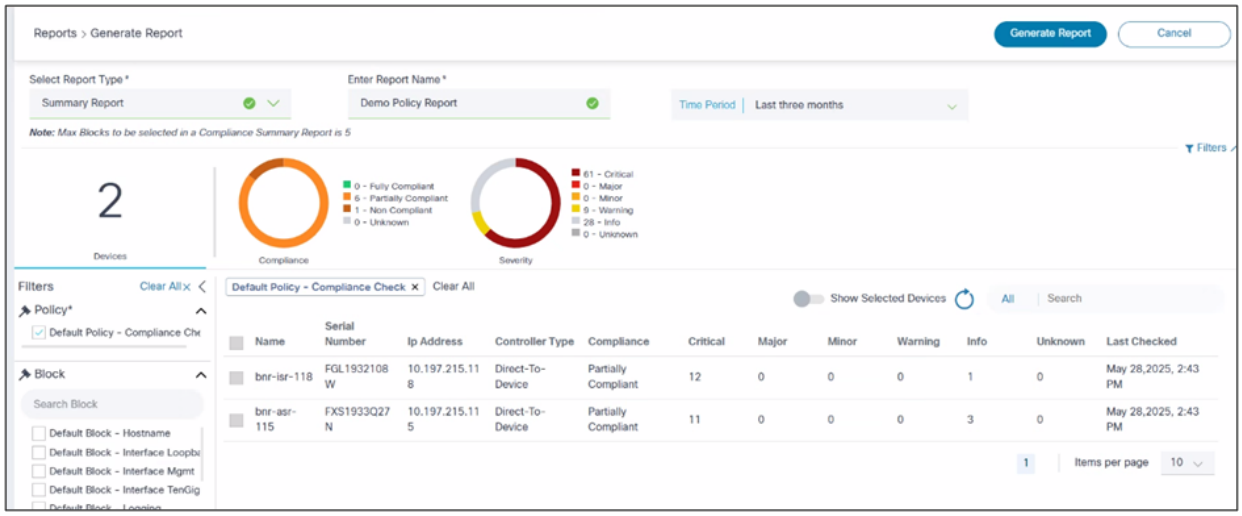
L'applicazione fornisce un'interfaccia dedicata per la generazione di nuovi report di conformità, consentendo agli utenti di selezionare il tipo di report, definire l'ambito e applicare filtri specifici. Il processo di generazione del report viene avviato dall'azione "Genera report" nella pagina del dashboard di report.

Gli aspetti chiave della generazione di report includono:

- Selezione del tipo di report: Gli utenti possono scegliere tra i seguenti tipi di report
  - Report di riepilogo: Fornisce una panoramica della conformità in tutti i dispositivi per i criteri selezionati
  - Rapporto dettagliato: Offre una visualizzazione dettagliata più granulare, che fornisce informazioni dettagliate sulle violazioni specifiche per ciascun dispositivo
- Denominazione del report: Agli utenti viene richiesto di fornire un nome appropriato per il report generato
- Selezione periodo di tempo: I report possono essere generati per intervalli di tempo specifici, ad esempio "Mese corrente" o intervalli personalizzati, per concentrarsi sui dati recenti relativi alla conformità
- Applicazione dei filtri: Opzioni di filtro complete che consentono agli utenti di restringere l'ambito del report
  - Policy: Selezionare uno o più criteri di conformità da includere nel report. Selezione criterio obbligatoria

    - Blocco: All'interno dei criteri selezionati, scegliere blocchi di configurazione specifici da includere nel report. La selezione del blocco è facoltativa
    - Gruppo di asset: Gli utenti possono filtrare gli asset nell'ambito selezionando uno o più gruppi di asset
- Selezione asset: Questa opzione è applicabile solo ai report dettagliati
    - Gli utenti possono selezionare dispositivi specifici per cui generare il report
    - Nella tabella degli asset vengono visualizzati dettagli quali Nome, Numero di serie, Indirizzo IP, Gestito da e stato di conformità corrente con conteggi per livelli di gravità diversi

Per generare un rapporto Sintetico conformità:

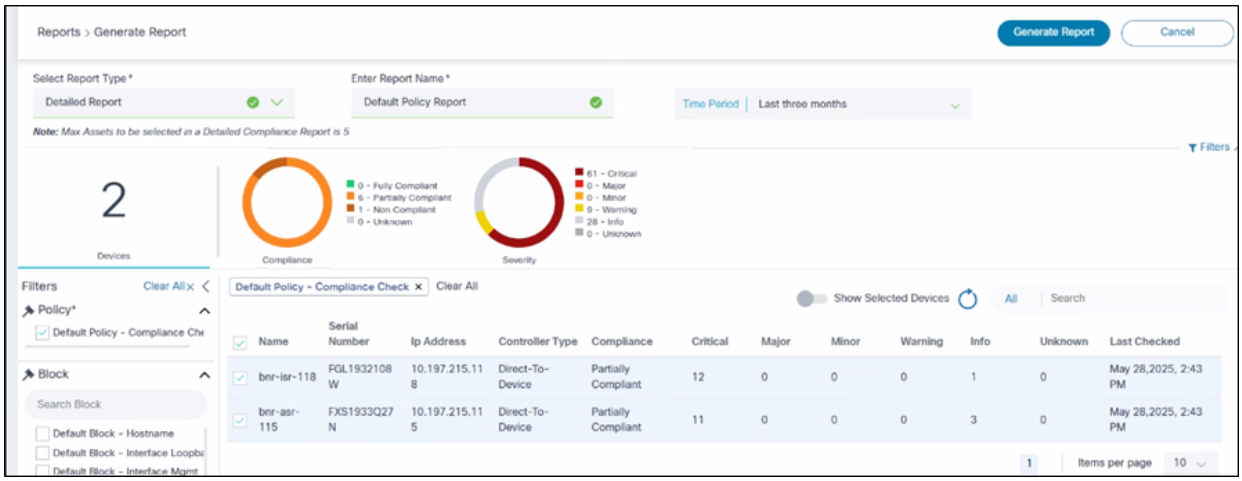


Genera report di riepilogo

1. Selezionare Report di riepilogo nell'elenco a discesa Seleziona tipo di report.
2. Inserire il nome di un report.
3. Selezionare un intervallo di tempo. I criteri e i blocchi verranno elencati in base a questa selezione.
4. Selezionare un criterio. È inoltre possibile selezionare criteri aggiuntivi.
5. Se lo si desidera, selezionare Blocchi. Se non viene selezionato alcun blocco, verranno inclusi tutti i blocchi.
6. Selezionare i gruppi di asset, lo stato di conformità e i livelli di gravità richiesti.
7. Fare clic su Genera report.

- Nella pagina di elenco dei report lo stato del report è impostato su Avviato
- Al completamento, lo stato diventa Completato. Se alcuni sottoreport hanno esito negativo, lo stato diventa Completato parzialmente
- Se l'intera generazione del report ha esito negativo, viene visualizzata una notifica e lo stato viene modificato in Non riuscito
- Al termine, l'opzione di download è disponibile. Gli utenti possono scaricare un file zip contenente i report di Excel

Per generare un report dettagliato sulla conformità:



Genera report dettagliato

1. Selezionare Rapporto dettagliato nell'elenco a discesa Seleziona tipo di rapporto.
2. Inserire il nome di un report.
3. Selezionare un intervallo di tempo. I criteri e i blocchi verranno elencati in base a questa selezione.
4. Selezionare un criterio. È inoltre possibile selezionare criteri aggiuntivi.
5. Se lo si desidera, selezionare Blocchi. Se non viene selezionato alcun blocco, verranno inclusi tutti i blocchi.
6. Selezionare i gruppi di asset, lo stato di conformità e i livelli di gravità richiesti.
7. Selezionare le risorse necessarie dalla griglia. Gli utenti possono selezionare "Select all" (Seleziona tutti) e "Show selected devices" (Mostra dispositivi selezionati).
8. Fare clic su Genera report.

- Nella pagina di elenco dei report lo stato del report è impostato su Avviato
- Al completamento, lo stato diventa Completato. Se alcuni sottoreport hanno esito negativo, lo stato diventa Completato parzialmente
- Se l'intera generazione del report ha esito negativo, viene visualizzata una notifica e lo stato viene modificato in Non riuscito

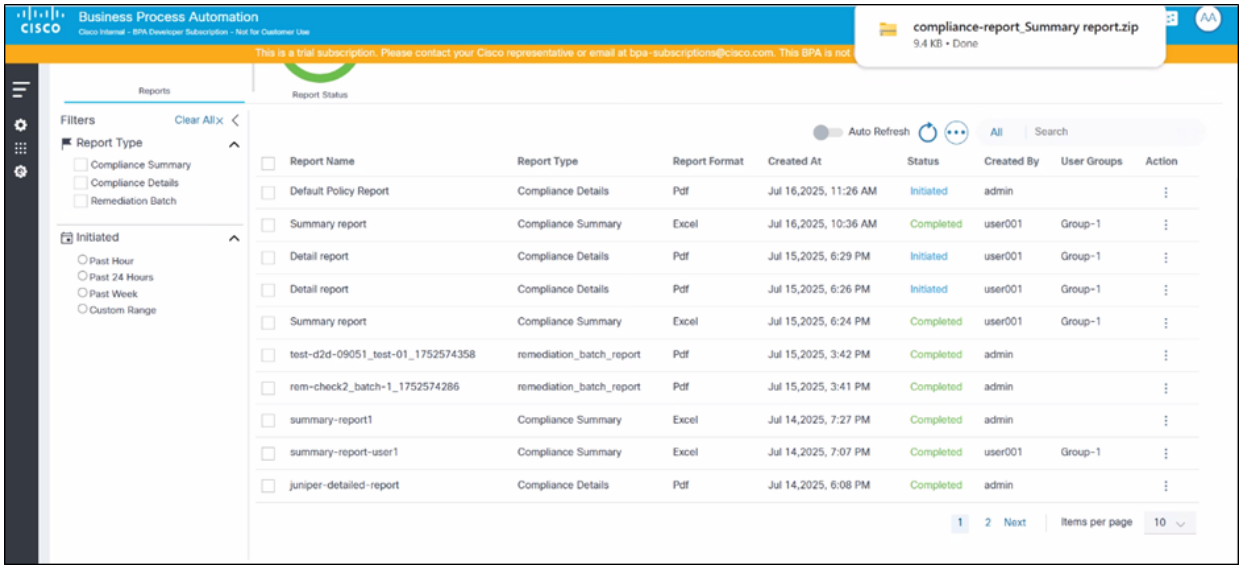
Download e visualizzazione dei report

I report completati possono essere scaricati utilizzando l'icona Scarica nella riga desiderata della griglia del dashboard di report.

Informazioni sul report di riepilogo della conformità alla configurazione

Il report Riepilogo conformità è un file zip che contiene singoli report PDF, con un PDF generato

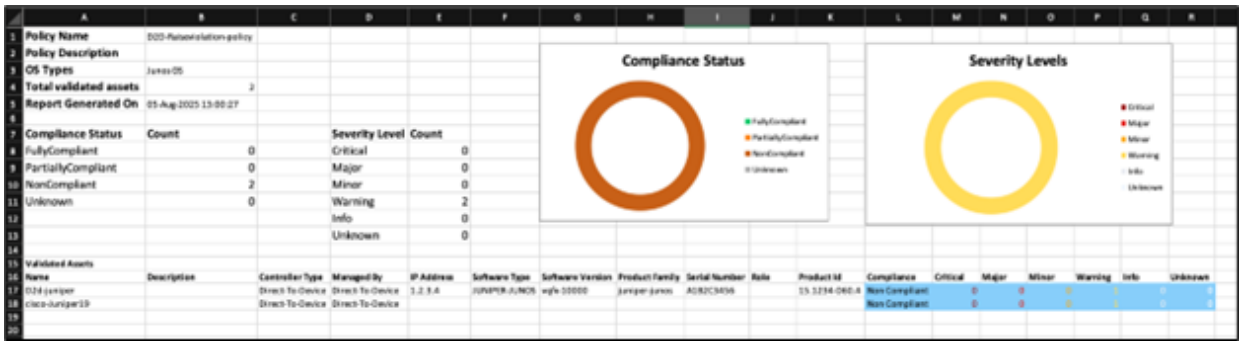
per dispositivo. Questo tipo di report offre una panoramica delle violazioni di conformità per criterio, insieme ai dettagli delle violazioni del mapping di espansione a livello di blocco per i dispositivi.



Rapporto Riepilogo conformità

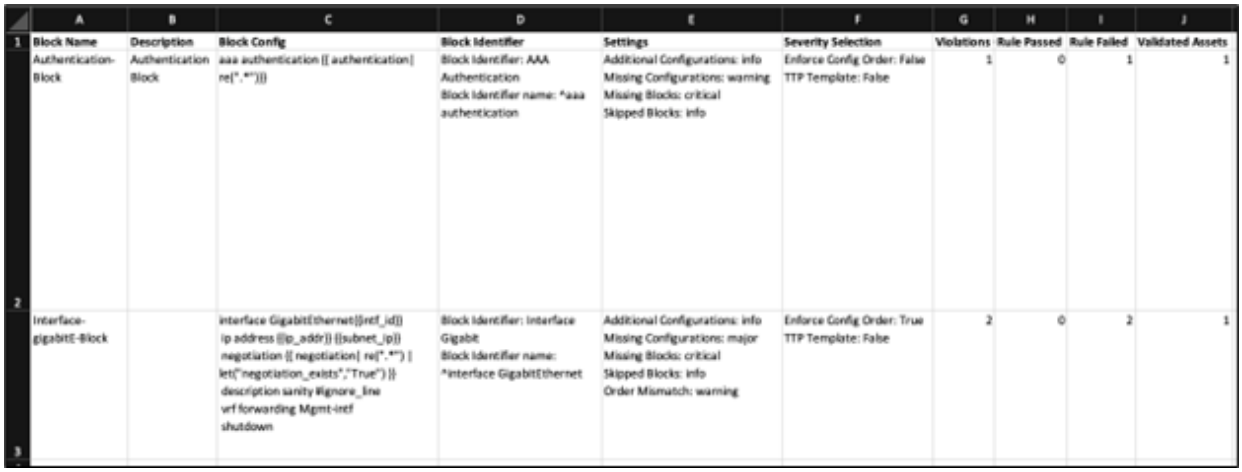
Ogni rapporto di Excel include i seguenti fogli e fornisce le seguenti informazioni:

- Riepilogo criteri:
  - Dettagli generali, quali il nome del criterio, la descrizione, il tipo o i tipi di sistema operativo e il totale delle risorse convalidate
  - Vista in griglia e in grafico del conteggio degli asset convalidati suddiviso per stato di conformità (ad esempio, Completamente conforme, Parzialmente conforme, Non conforme e Sconosciuto)
  - Visualizzazione griglia e grafico del conteggio totale delle violazioni diviso per livello di gravità (ad esempio, Critico, Principale, Secondario, Informazioni avviso e Sconosciuto)
  - Una griglia delle risorse con i dettagli dei dispositivi, lo stato di conformità e il conteggio delle violazioni per ogni livello di gravità



Foglio di riepilogo criteri

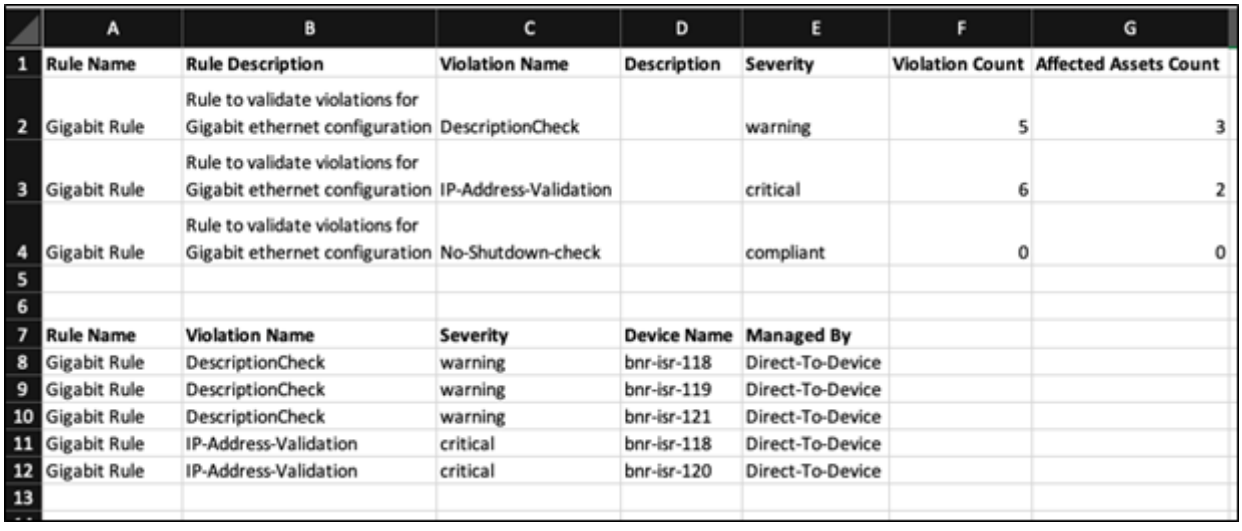
- Riepilogo blocchi:
  - Dettagli dei blocchi, ad esempio il nome, la descrizione, la configurazione, i dettagli dell'identificatore e le impostazioni di severità della violazione di blocco
  - Numero di violazioni, regole passate, regole non riuscite e asset convalidati per il blocco specificato



Block Name	Description	Block Config	Block Identifier	Settings	Severity Selection	Violations	Rule Passed	Rule Failed	Validated Assets
Authentication-Block	Authentication Block	aaa authentication {{ authentication| re(".*")}}	Block Identifier: AAA Authentication Block Identifier name: ^aaa authentication	Additional Configurations: info Missing Configurations: warning Missing Blocks: critical Skipped Blocks: info	Enforce Config Order: False TTP Template: False	1	0	1	1
Interface-gigabitE-Block		interface GigabitEthernet{{intf_id}} ip address {{ip_addr}} {{subnet_ip}} negotiation {{ negotiation| re(".*") | let("negotiation_exists","True") }} description sanity #ignore_line vrf forwarding Mgmt-intf shutdown	Block Identifier: Interface Gigabit Block Identifier name: ^interface GigabitEthernet	Additional Configurations: info Missing Configurations: major Missing Blocks: critical Skipped Blocks: info Order Mismatch: warning	Enforce Config Order: True TTP Template: False	2	0	2	1

Foglio riepilogativo

- Dettagli regola e violazione per blocco:
- Nella griglia del livello di violazione viene visualizzato un elenco di nomi di regole, descrizioni, nomi di violazioni, livello di gravità della descrizione, conteggio delle violazioni rilevate tra le risorse e conteggio delle risorse interessate
- Nella griglia a livello di dispositivo viene visualizzato il mapping tra regola, violazione, gravità, nome del dispositivo e nome del controller (gestito da)



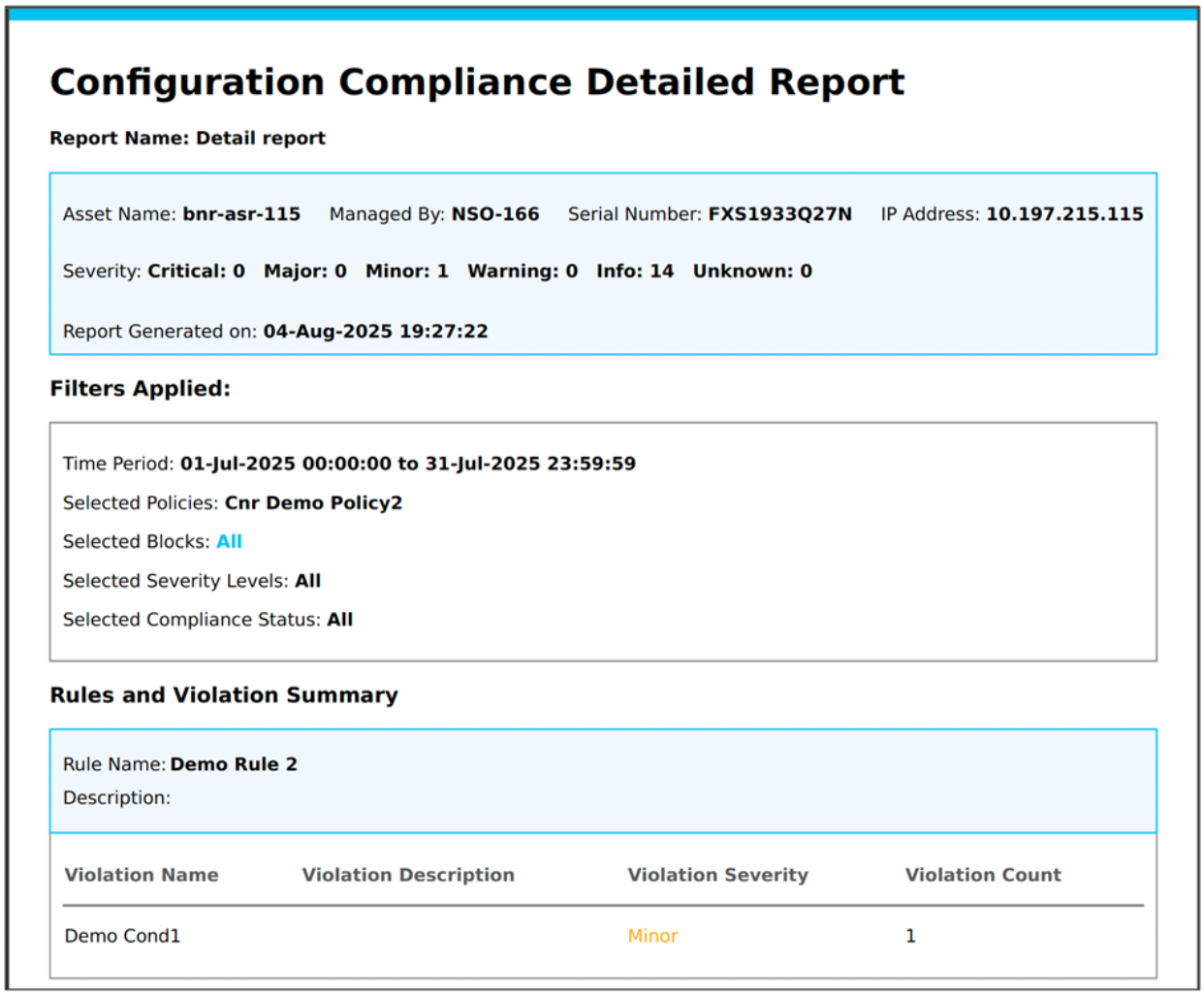
Rule Name	Rule Description	Violation Name	Description	Severity	Violation Count	Affected Assets Count
Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	DescriptionCheck		warning	5	3
Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	IP-Address-Validation		critical	6	2
Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	No-Shutdown-check		compliant	0	0
Rule Name	**Violation Name**	**Severity**	**Device Name**	**Managed By**		
Gigabit Rule	DescriptionCheck	warning	bnr-isr-118	Direct-To-Device		
Gigabit Rule	DescriptionCheck	warning	bnr-isr-119	Direct-To-Device		
Gigabit Rule	DescriptionCheck	warning	bnr-isr-121	Direct-To-Device		
Gigabit Rule	IP-Address-Validation	critical	bnr-isr-118	Direct-To-Device		
Gigabit Rule	IP-Address-Validation	critical	bnr-isr-120	Direct-To-Device		

Rapporto Dettagli conformità

Il rapporto Dettagli conformità contiene le seguenti informazioni:

- Nome report: Identifica il nome del report

    - Nome asset: Specifica il dispositivo per il quale è stato eseguito il controllo di conformità
    - Altri dettagli asset: Include dettagli quali l'indirizzo IP e il numero di serie, se presenti
    - Gravità: Fornisce un riepilogo delle violazioni per livello di gravità
    - Report generato il: Indica l'indicatore orario di creazione del report
- Filtri applicati: Descrive i dettagli dei criteri di filtro specifici utilizzati per generare un rapporto specifico, garantendo trasparenza e riproducibilità. Ciò include il periodo di tempo, le regole, i blocchi, i livelli di gravità e gli stati di conformità selezionati
- Riepilogo regole e violazioni: Elenca ogni regola valutata e fornisce un riepilogo delle violazioni rilevate per tale regola. Nella griglia di riepilogo vengono visualizzati il nome, la descrizione, la gravità della violazione e il numero di volte in cui si è verificata la violazione
- Dettagli violazione: Offre dettagli espliciti su ciascuna linea di configurazione dei dispositivi per i blocchi selezionati, insieme ai dettagli delle violazioni per ciascuna linea



Configuration Compliance Detailed Report

Report Name: Detail report

Asset Name: **bnr-asr-115** Managed By: **NSO-166** Serial Number: **FXS1933Q27N** IP Address: **10.197.215.115**

Severity: **Critical: 0** **Major: 0** **Minor: 1** **Warning: 0** **Info: 14** **Unknown: 0**

Report Generated on: **04-Aug-2025 19:27:22**

Filters Applied:

Time Period: **01-Jul-2025 00:00:00 to 31-Jul-2025 23:59:59**

Selected Policies: **Cnr Demo Policy2**

Selected Blocks: **All**

Selected Severity Levels: **All**

Selected Compliance Status: **All**

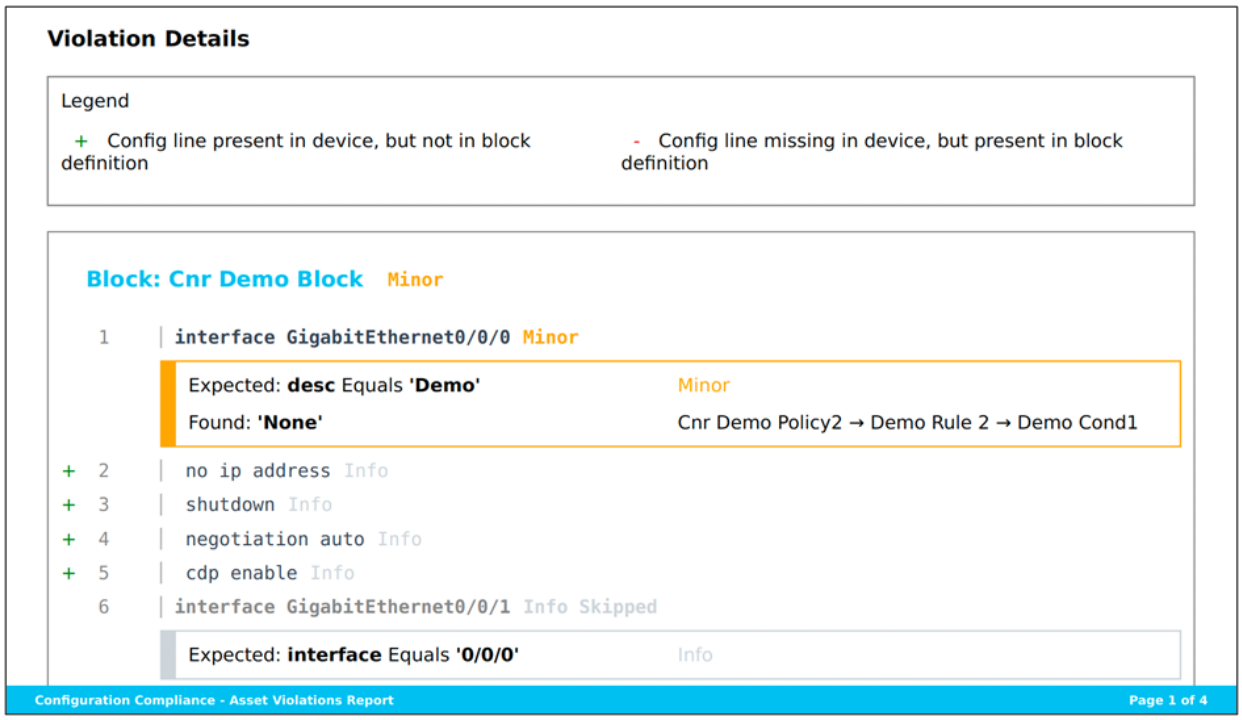
Rules and Violation Summary

Rule Name: **Demo Rule 2**

Description:

Violation Name	Violation Description	Violation Severity	Violation Count
Demo Cond1		Minor	1

Rapporto dettagliato sulla conformità - PDF di esempio Pagina 1

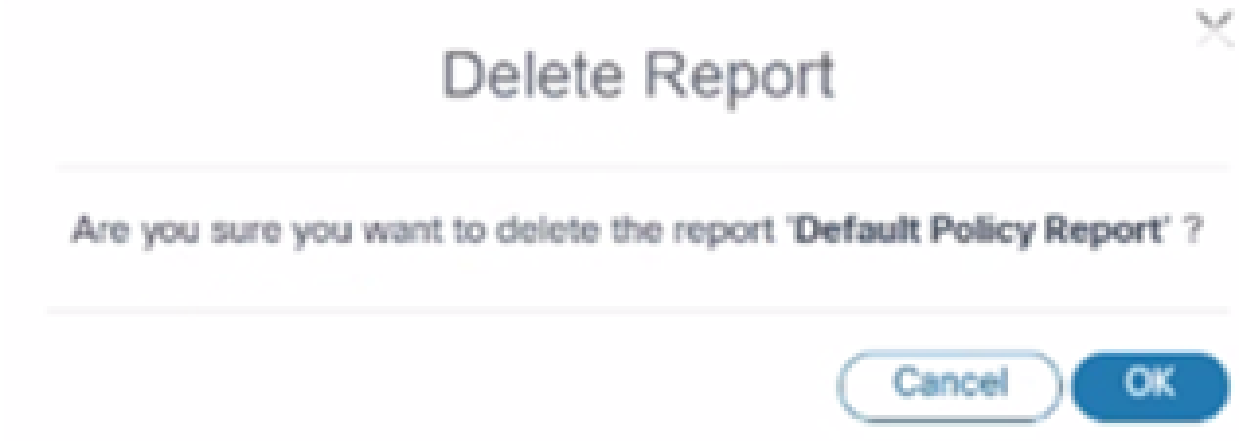


Rapporto dettagliato sulla conformità - PDF di esempio Pagina 2

Nota: Il report PDF del batch di monitoraggio e aggiornamento creato dalla pagina del batch di monitoraggio e aggiornamento può inoltre essere scaricato e visualizzato dall'elenco dei report.

Elimina report

I report possono essere eliminati singolarmente selezionando l'icona Elimina o in blocco selezionando le caselle di controllo per i report e selezionando l'icona Altre opzioni > Elimina.



Elenco processi di conformità

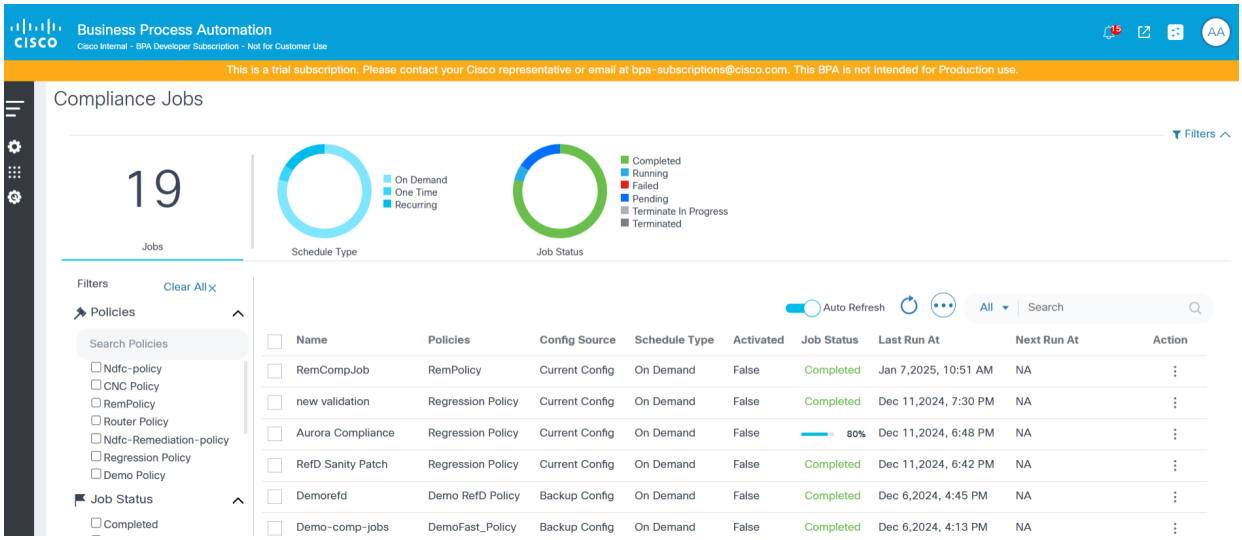
Nota: L'eliminazione di un report comporta solo la rimozione dei file e delle voci del report dal pannello di controllo dei report. i dettagli dell'esecuzione della conformità sottostante vengono mantenuti.

Processi di conformità

La funzione Compliance Job (Processi di conformità) del portale di nuova generazione è progettata per aiutare gli utenti a creare, gestire ed eseguire i Processi di conformità su criteri e gruppi di risorse selezionati. Questi processi possono essere pianificati per l'esecuzione a intervalli regolari o su richiesta, in modo da garantire che tutte le risorse siano sottoposte a controlli coerenti per verificarne la conformità.

Caratteristiche principali

- Elenca processi di conformità: Visualizzare tutti i job di conformità definiti, con opzioni che consentono di controllare, filtrare, creare, modificare, eliminare ed eseguire i job non in linea.
- OdL programmati e su richiesta: Impostare i processi per l'esecuzione a intervalli pianificati o per l'esecuzione immediata, in base alle esigenze.
- Controllo granulare degli accessi: L'accesso ai processi di conformità è controllato in base alle autorizzazioni utente, garantendo che gli utenti vedano solo i processi correlati ai criteri per i quali dispongono dell'accesso.
- Opzioni filtro: Filtrare i job in base ai criteri, allo stato dei job, al tipo di pianificazione e all'intervallo di date per semplificare la navigazione e la gestione.



Elenco processi di conformità

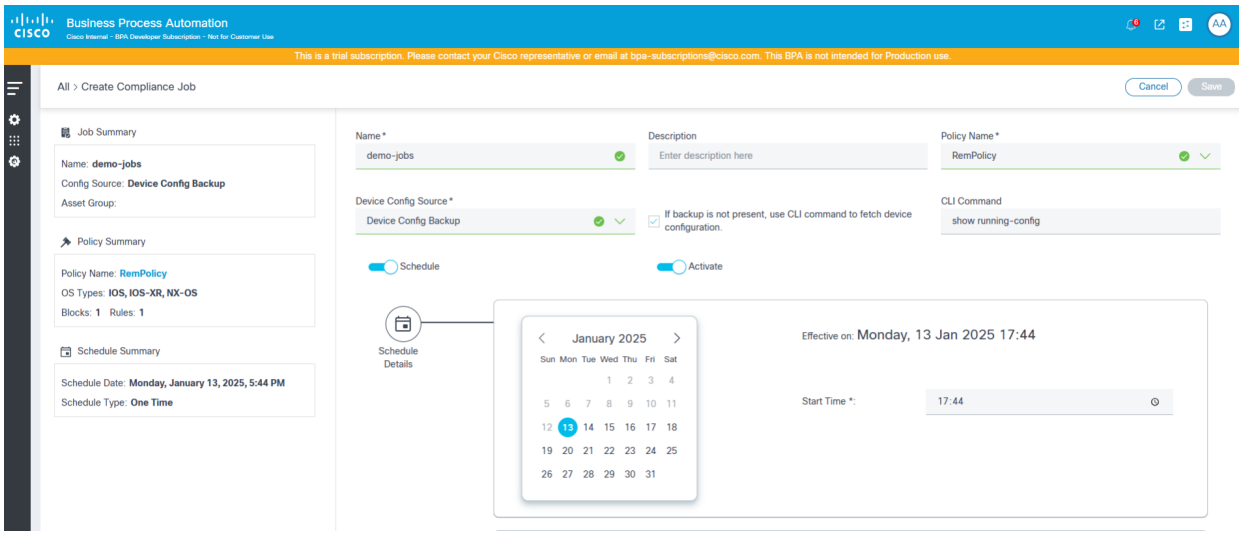
Creazione di job di conformità

La pagina Creazione job di conformità include gli attributi riportati di seguito.

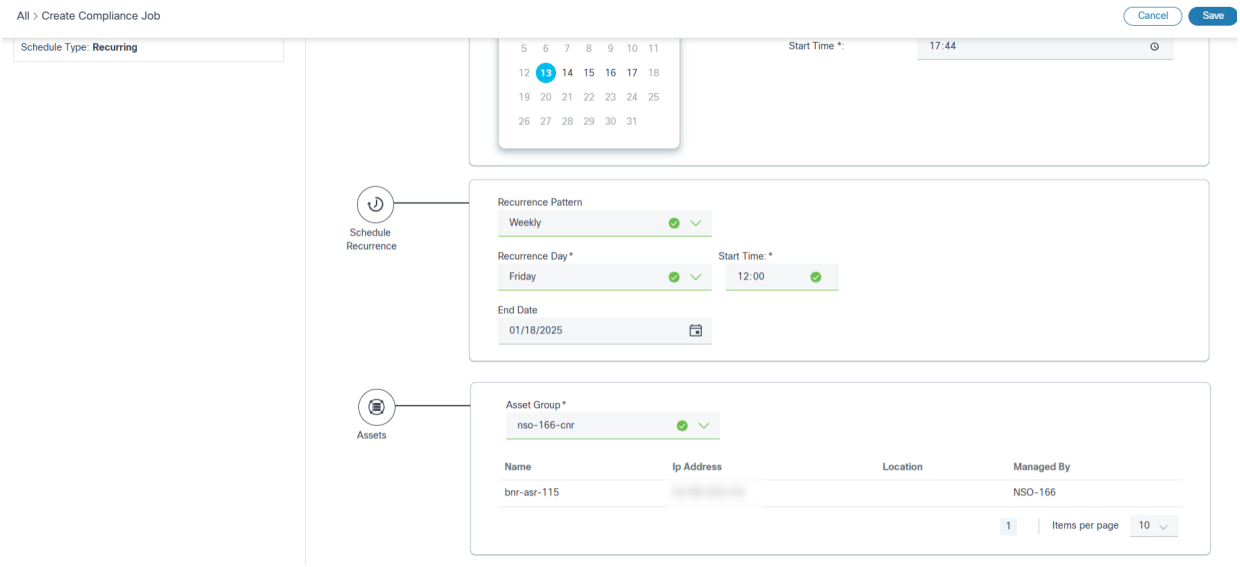
- Nome: Nome del processo
- Descrizione: Descrizione facoltativa
- Nome criterio: Elenco a discesa per selezionare un criterio da eseguire, potenzialmente filtrato in base ai criteri di accesso configurati per l'utente connesso
- Origine configurazione dispositivo: Un elenco a discesa per selezionare l'origine per il recupero della configurazione del dispositivo (Configurazione corrente o Backup configurazione dispositivo) per l'esecuzione del job di conformità e una casella di controllo per indicare se eseguire il fallback a un comando CLI se il backup non è presente.

Nota: L'opzione Backup configurazione dispositivo funziona solo se il controller sottostante supporta la funzionalità di backup.

- Variabili definite dall'utente: Casella di testo modificabile per lo spazio dei nomi disponibile quando il criterio selezionato contiene variabili definite dall'utente
- Dettagli pianificazione: Sezione per selezionare vari parametri di pianificazione, ad esempio data/ora di inizio e di fine, criteri di ricorrenza e così via.
- Risorse: Sezione per selezionare un gruppo di risorse per identificare l'elenco di dispositivi per eseguire la conformità
- Pianificazione: Attivare o disattivare l'esecuzione del job nei tempi previsti (una tantum o ricorrente). Se disabilitato, il job viene eseguito immediatamente
- È attivo: Indica se la pianificazione selezionata è attiva o meno



Creazione di job di conformità



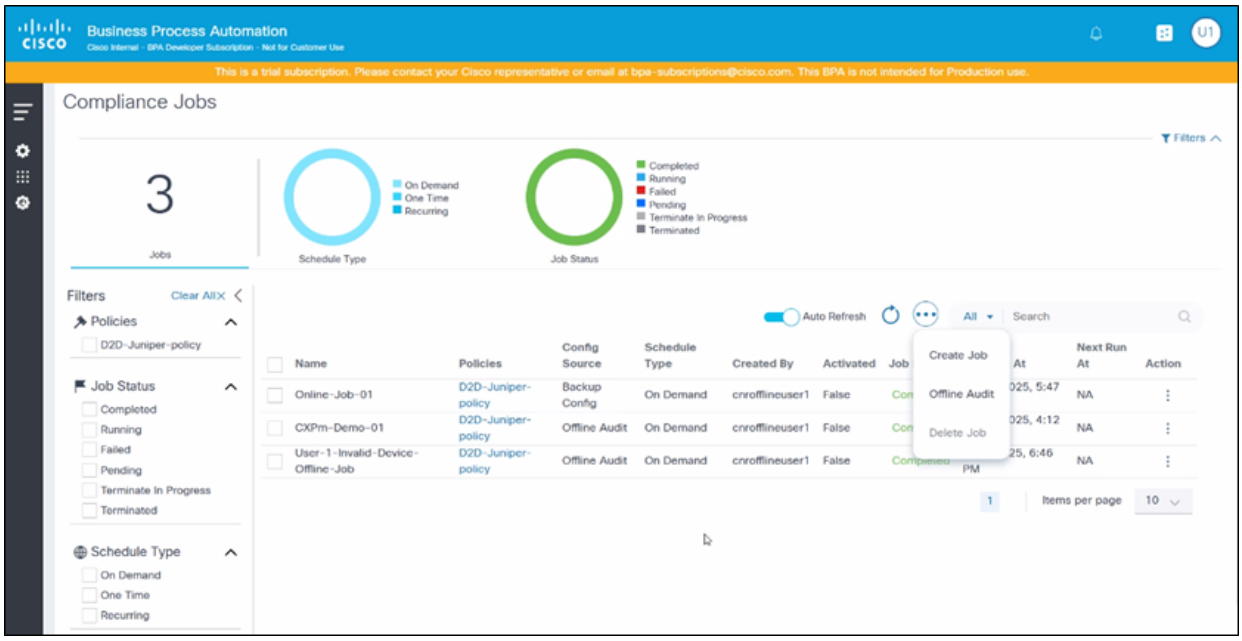
Creazione dei job di conformità 2

Creazione di job di audit offline

La funzione Controllo non in linea dei processi di conformità consente agli utenti di eseguire controlli di conformità sulle configurazioni dei dispositivi senza che sia necessario caricare i dispositivi in BPA. Gli utenti possono caricare manualmente la configurazione del dispositivo come file. È possibile comprimere e caricare diverse configurazioni di dispositivi come file zip. Una volta caricati, questi file di configurazione vengono analizzati e i job di conformità possono essere creati utilizzando il contenuto di tali file come origine. I risultati degli audit offline vengono quindi visualizzati sul dashboard conformità insieme ai risultati degli audit online.

La pagina Controllo non in linea include gli attributi riportati di seguito.

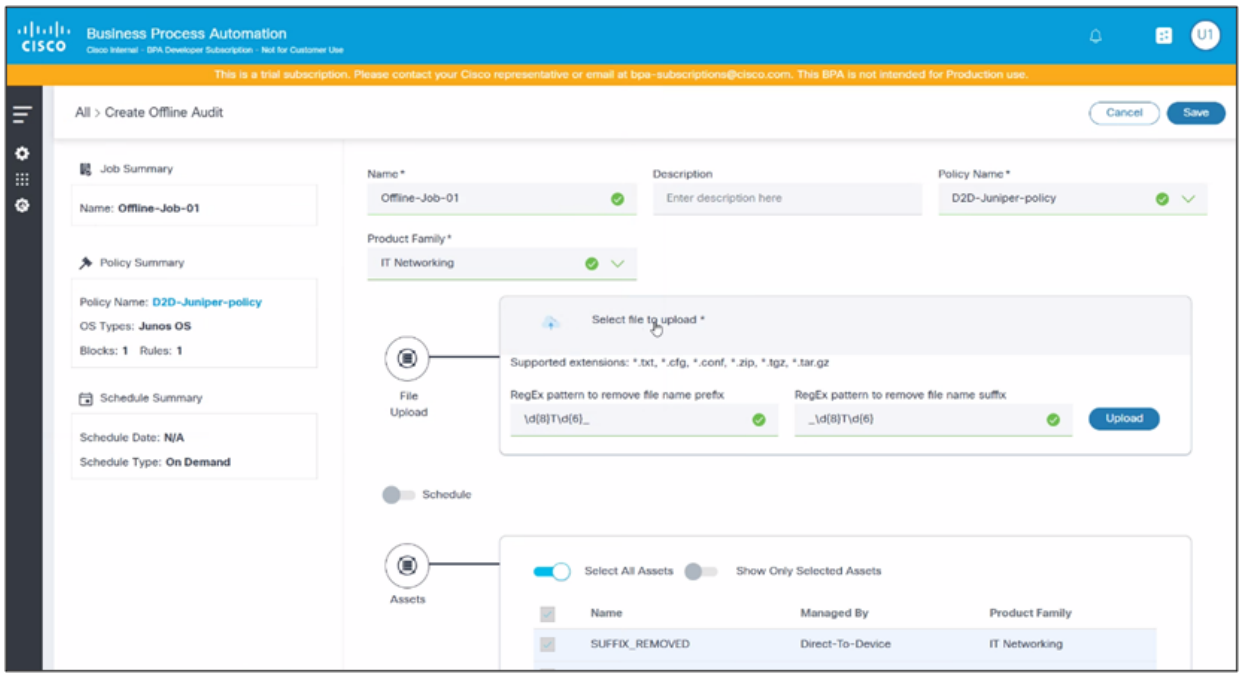
- Nome: Nome del processo
- Descrizione: Descrizione facoltativa
- Nome criterio: Elenco a discesa per selezionare un criterio da eseguire, potenzialmente filtrato in base ai criteri di accesso configurati per l'utente connesso
- Famiglia di prodotti: Un elenco a discesa per selezionare la famiglia di prodotti
- Caricamento file: Utilizzare la funzione di controllo non in linea per caricare manualmente i file di configurazione; Questa operazione viene eseguita tramite un'interfaccia di caricamento in cui è possibile selezionare i file dal sistema locale
- Pianificazione: Attiva/disattiva per attivare la pianificazione
- Risorse: Mostra l'elenco dei dispositivi per il contenuto del file caricato



Seleziona controllo offline

Per creare processi di controllo non in linea:

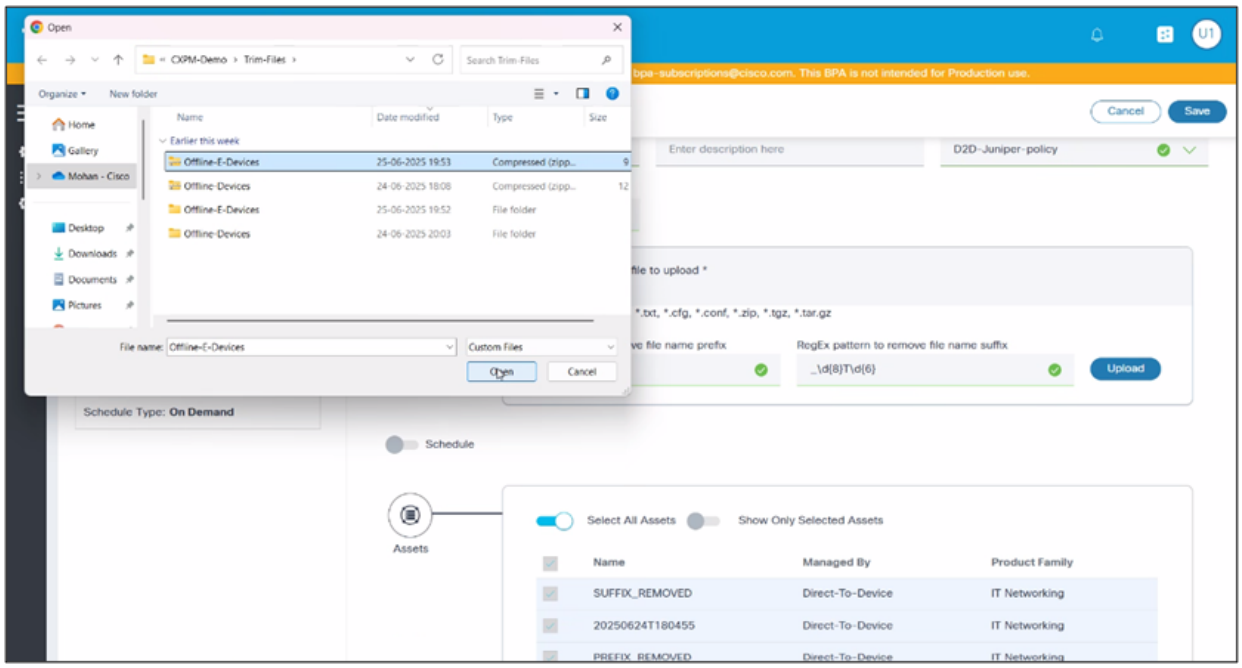
1. Selezionare Controllo non in linea dall'icona Altre opzioni.



Carica file

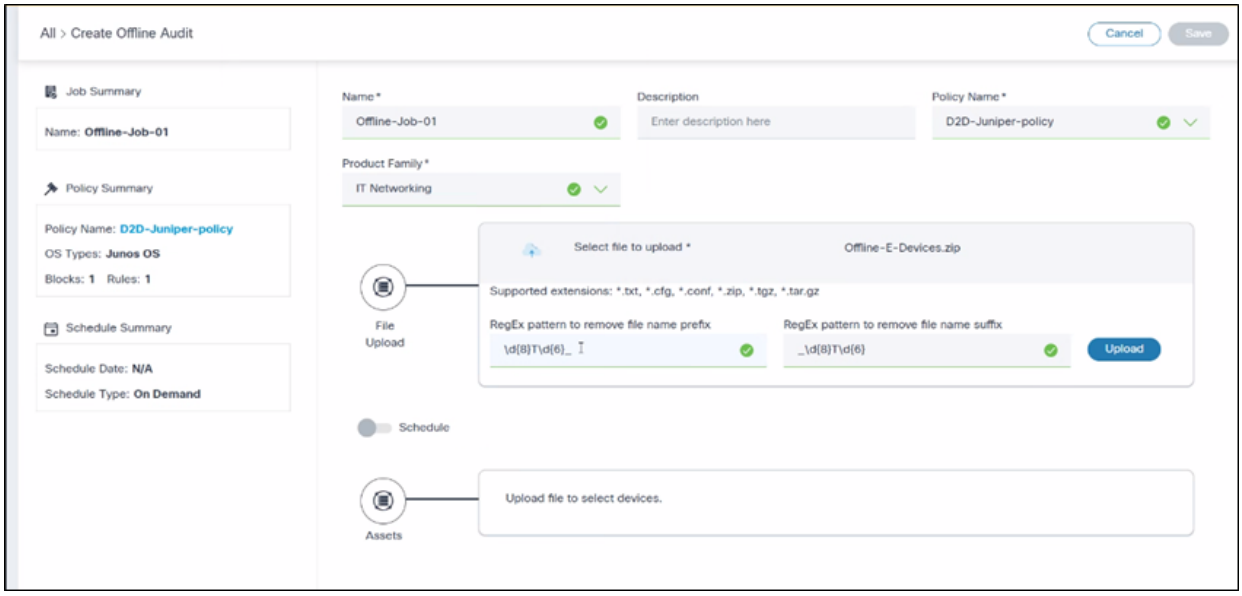
2. Fare clic su Select file to upload per caricare i file di configurazione.

Nota: I tipi di file supportati includono (.txt,.cfg,.conf,.zip,.tgz,.tar.gz).



File del desktop

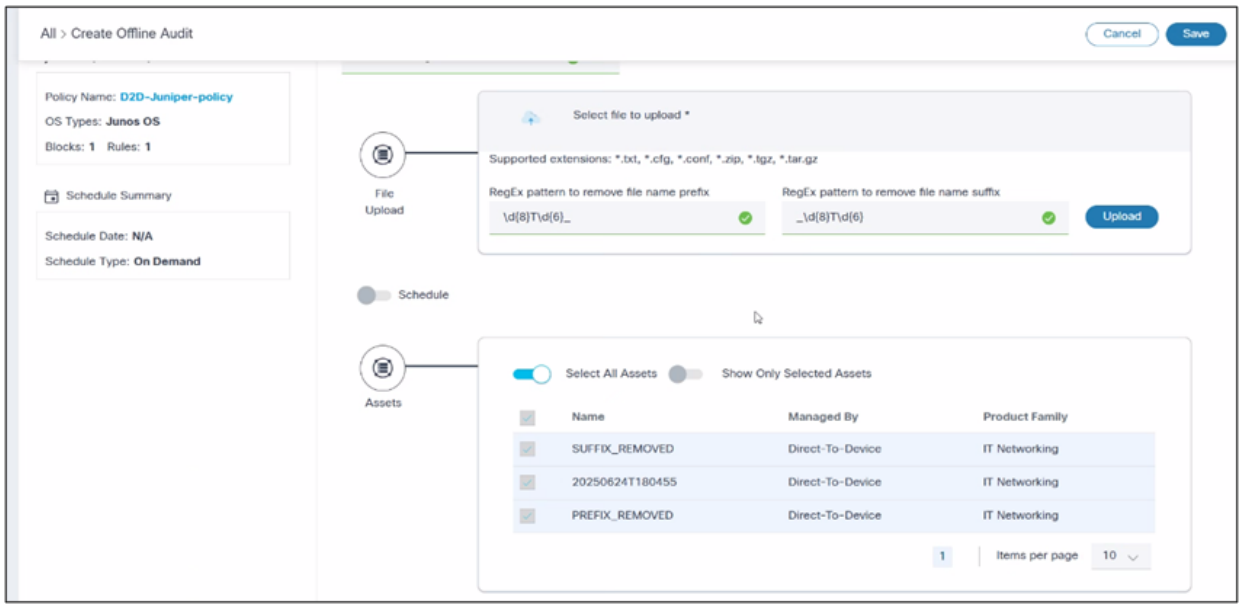
3. Se i file di configurazione sono compressi in una cartella o in un archivio, estrarli prima di caricarli.



Motivo Regex

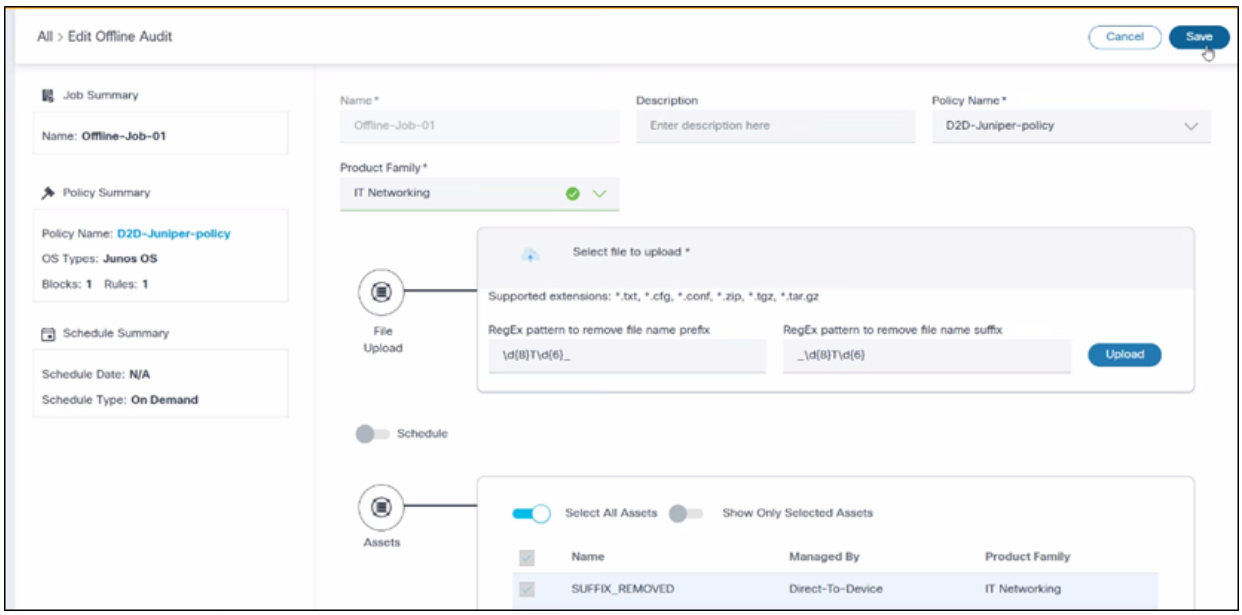
4. Applicare il modello Regex per la rifilatura dei nomi di file (facoltativo).

Nota: Usa i pattern di trimming dei prefissi o dei suffissi (regex) per standardizzare o semplificare i nomi di file caricati per semplificare l'elaborazione.



Carica i file

5. Fare clic su Upload. Viene visualizzato un messaggio di conferma che indica che i file sono stati salvati nel database e caricati correttamente.



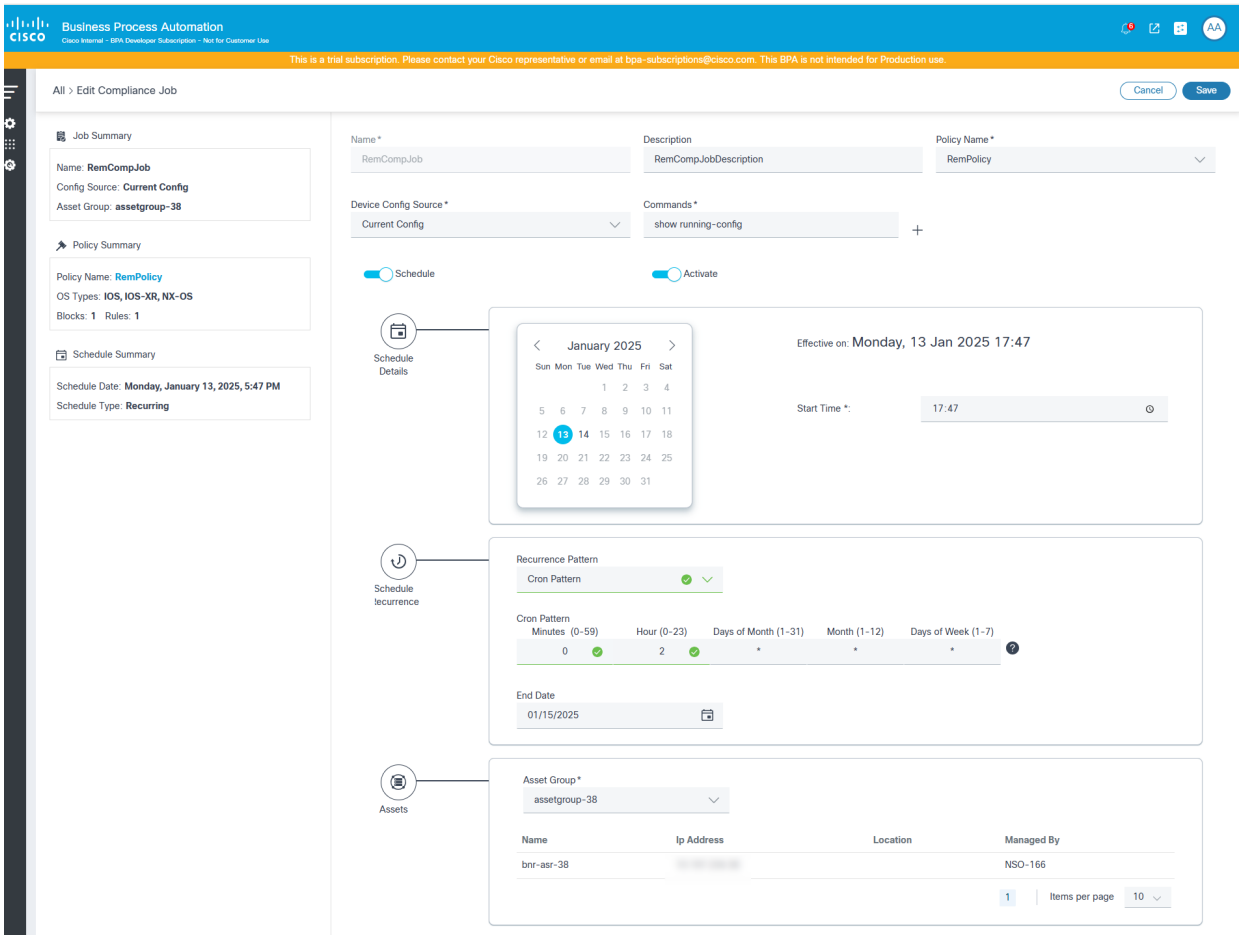
Salva controllo offline

6. Fare clic su Salva per creare il processo di controllo offline.

Modifica dei job di conformità

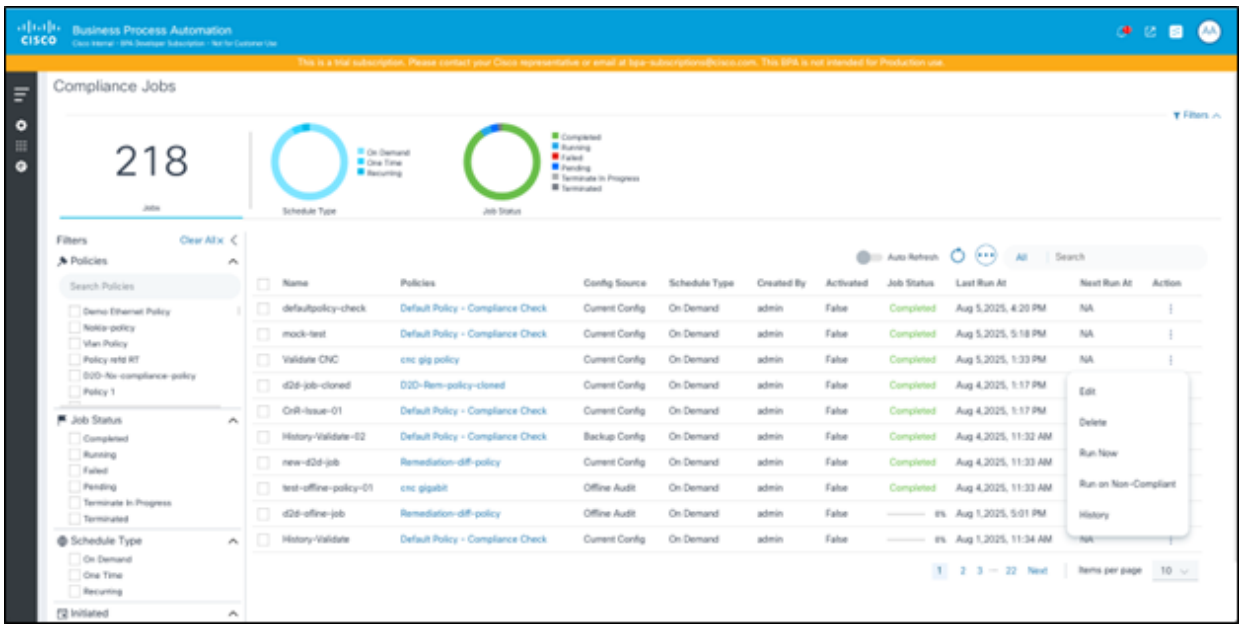
Per modificare i job di conformità, seguire i passi descritti in Creazione dei job di conformità.

Nota: Il valore nName del processo non è modificabile.



Modifica del processo di conformità

Esegui ora o riesegui processi di conformità



Processo di conformità - Esegui ora ed esegui su non conforme

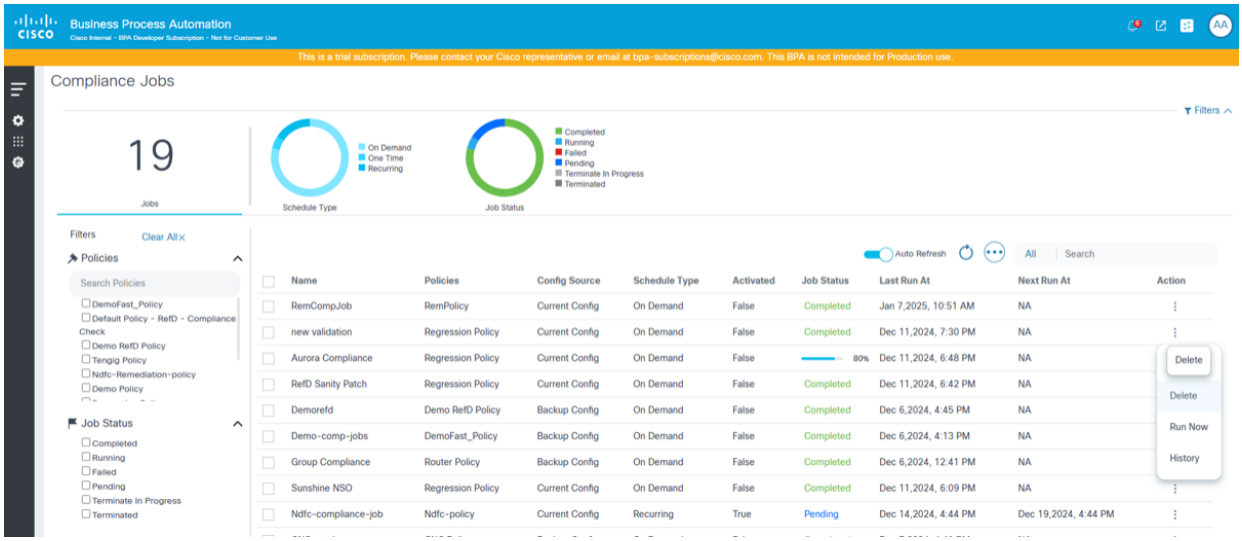
La griglia Processi conformità consente di eseguire un processo su richiesta selezionando Esegui

adesso dall'icona Altre opzioni. Se per un job esiste già un'esecuzione, gli utenti possono selezionare Esegui su non conforme dall'icona Altre opzioni. Questa azione esegue il processo di conformità solo nell'elenco di asset non contrassegnati come completamente conformi nell'esecuzione precedente.

Eliminazione dei job di conformità

Il portale consente di eliminare uno o più processi di conformità se l'utente dispone del ruolo RBAC (Role Based Access Control) corretto. Impossibile eliminare i processi quando è in corso un'esecuzione. Gli utenti possono scegliere di eliminare uno o più processi di conformità.

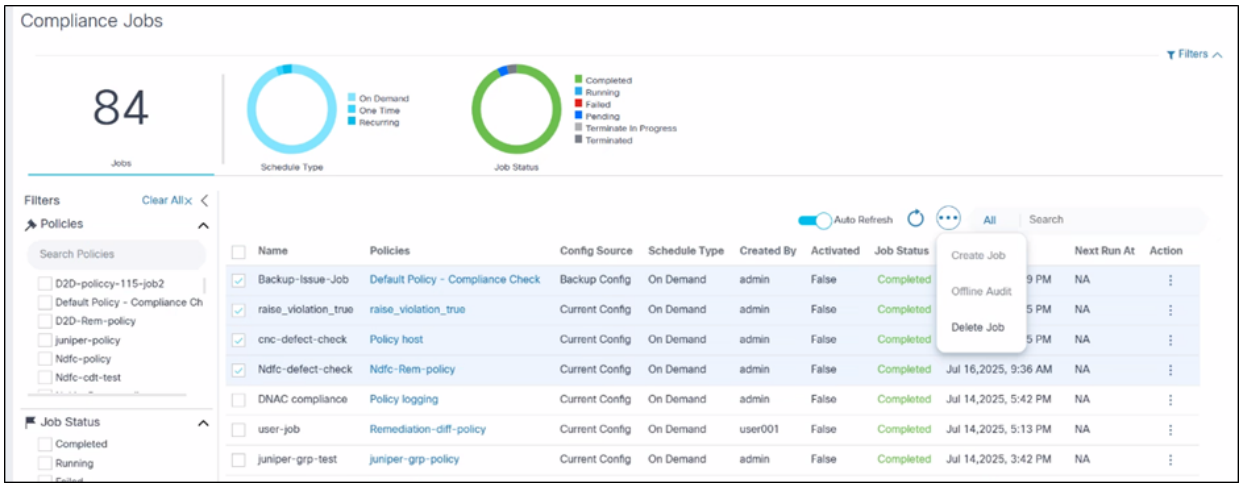
Per eliminare un processo di conformità:



Eliminazione di un singolo processo di conformità

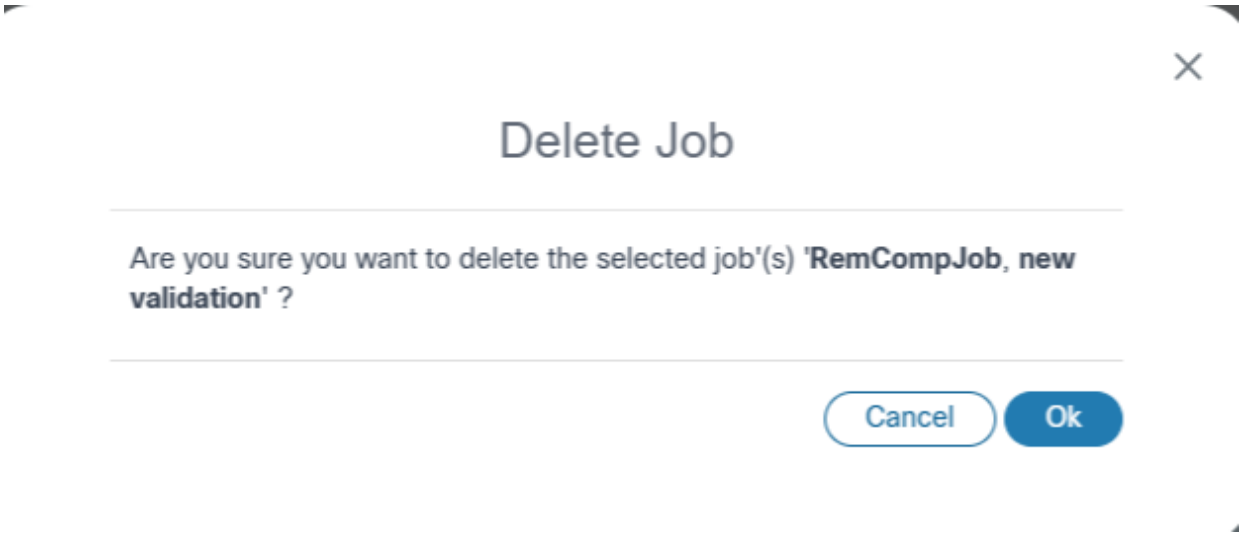
1. Dalla pagina Job di conformità, selezionare l'icona Altre opzioni > Elimina sul job da eliminare.

O



Eliminazione di più job di conformità

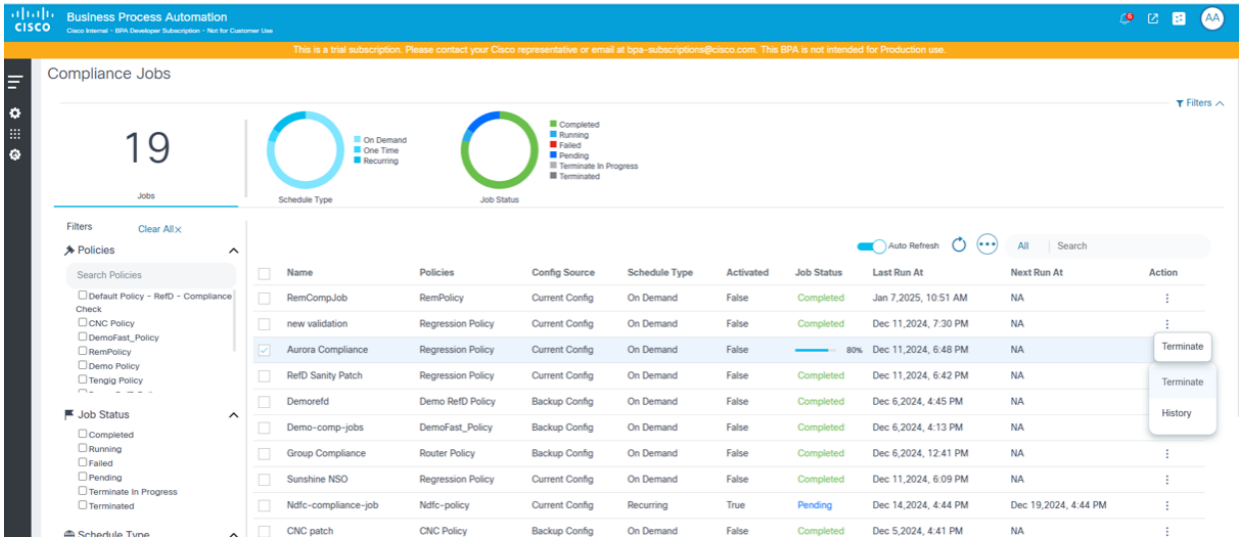
Per eliminare più job di conformità, selezionare le caselle di controllo relative ai job da eliminare e selezionare Altre opzioni > Elimina job. Viene visualizzata una conferma.



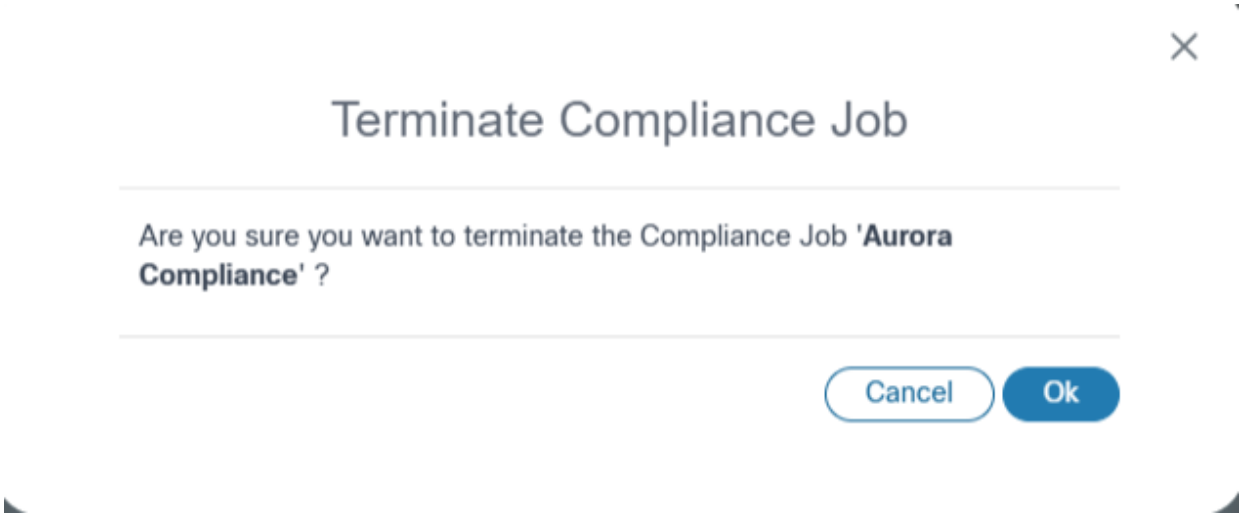
Conferma processo eliminazione conformità

Interruzione dei job di conformità

Il portale offre agli utenti la possibilità di interrompere l'esecuzione di un determinato processo. Quando un processo viene terminato, i dispositivi in esecuzione completano l'esecuzione e annullano tutte le esecuzioni dei dispositivi in coda.



Interruzione dei job di conformità

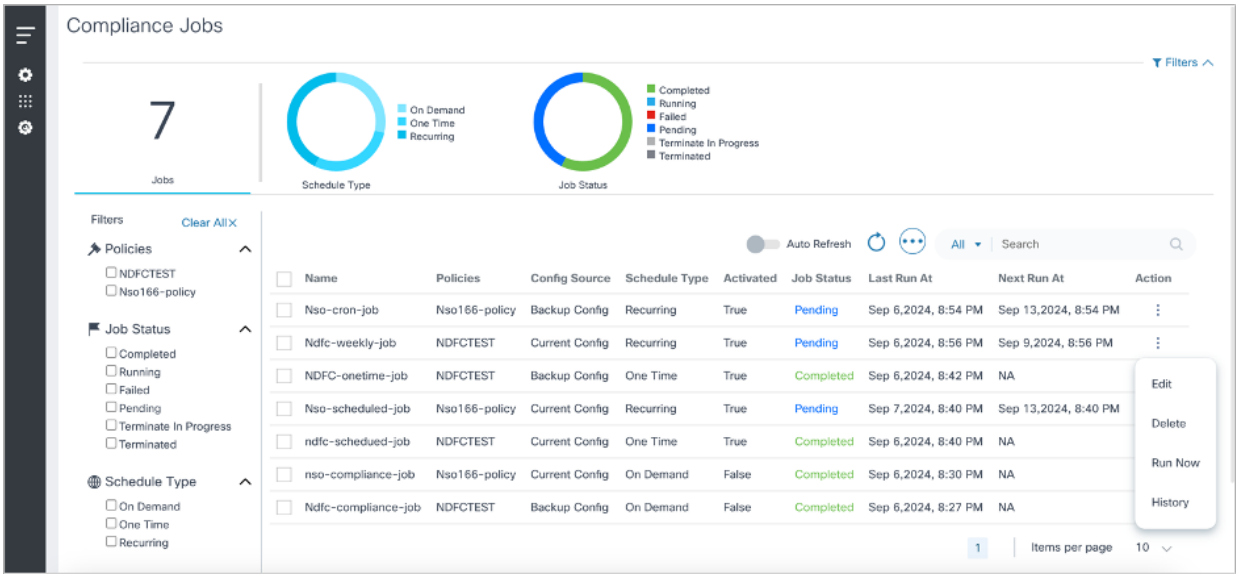


Conferma interruzione processo di conformità

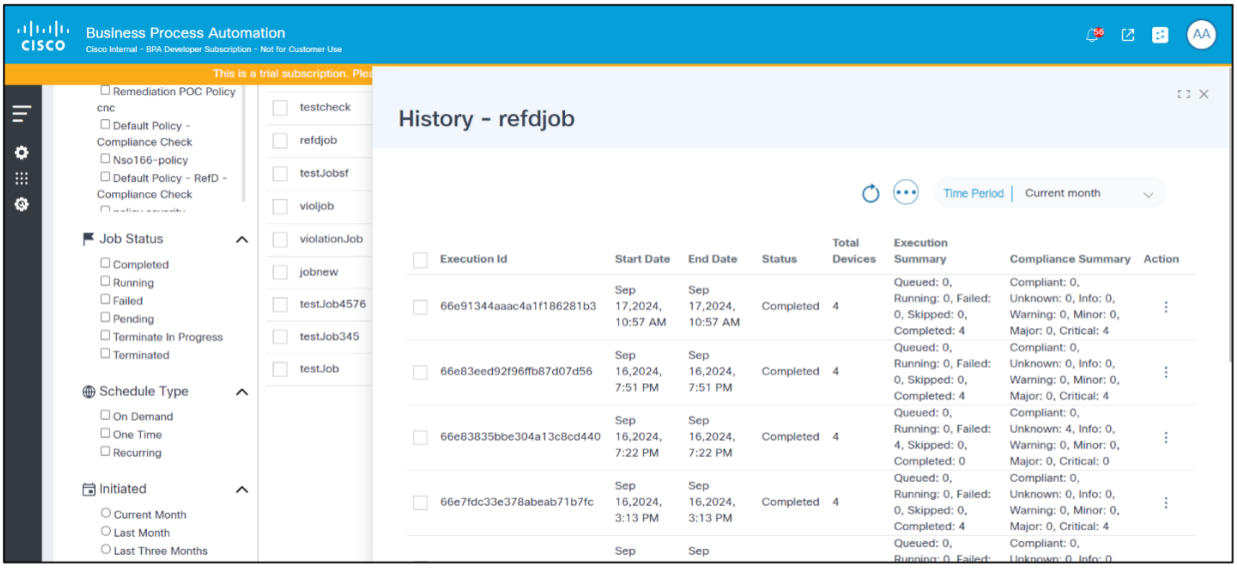
Cronologia processi conformità

L'opzione Cronologia nel job di conformità mostra la lista delle esecuzioni per il job selezionato, filtrate in base all'intervallo di date della pianificazione.

Per visualizzare la cronologia di un job di conformità, nella pagina Job di conformità, selezionare l'icona Altre opzioni > Cronologia. Viene visualizzata la pagina Cronologia.



Cronologia processi di conformità

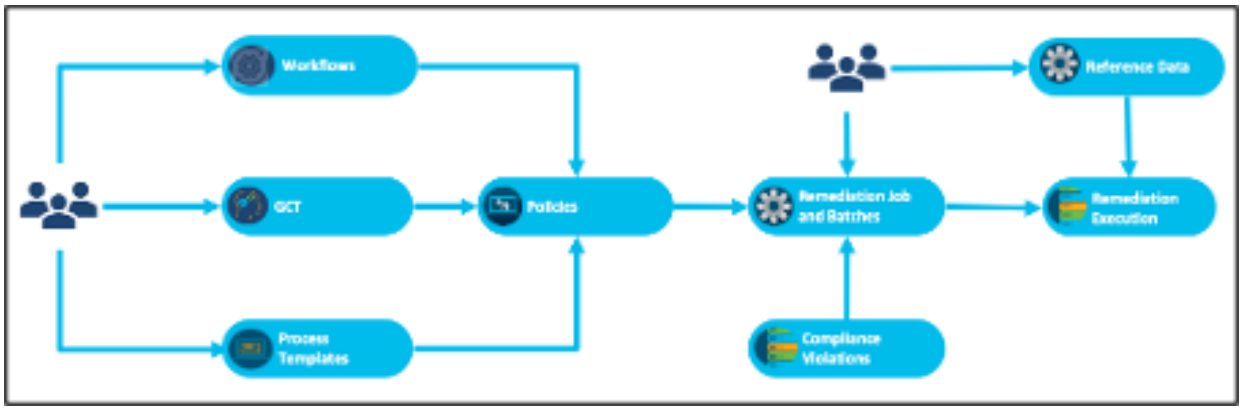


Pagina Cronologia

Processi di monitoraggio e aggiornamento

Il framework di monitoraggio e aggiornamento consente agli operatori di correggere le violazioni di conformità elencate nel dashboard di conformità. Questa struttura utilizza workflow, GCT e modelli di processo.

Diagramma di flusso di risoluzione della configurazione



Panoramica di Monitoraggio e aggiornamento configurazione

Lo Use Case di monitoraggio e aggiornamento della configurazione consente agli operatori di correggere le violazioni della configurazione nei dispositivi che utilizzano i processi di monitoraggio e aggiornamento. I criteri di conformità vengono innanzitutto configurati con il flusso di lavoro, i modelli GCT e i modelli di processo appropriati per ogni tipo di controller. Viene eseguito un processo di monitoraggio e aggiornamento per un criterio in base a un elenco di asset interessati. Durante il monitoraggio e l'aggiornamento, i valori da applicare a un dispositivo possono essere recuperati da varie origini di dati, tra cui il risultato dell'esecuzione della conformità, l'applicazione RefD e la configurazione del dispositivo esistente. Il flusso di lavoro può essere personalizzato in base alle specifiche esigenze del cliente, in modo da supportare fasi aggiuntive durante il risanamento.

Di seguito sono illustrati i passaggi più importanti della funzionalità di monitoraggio e aggiornamento.

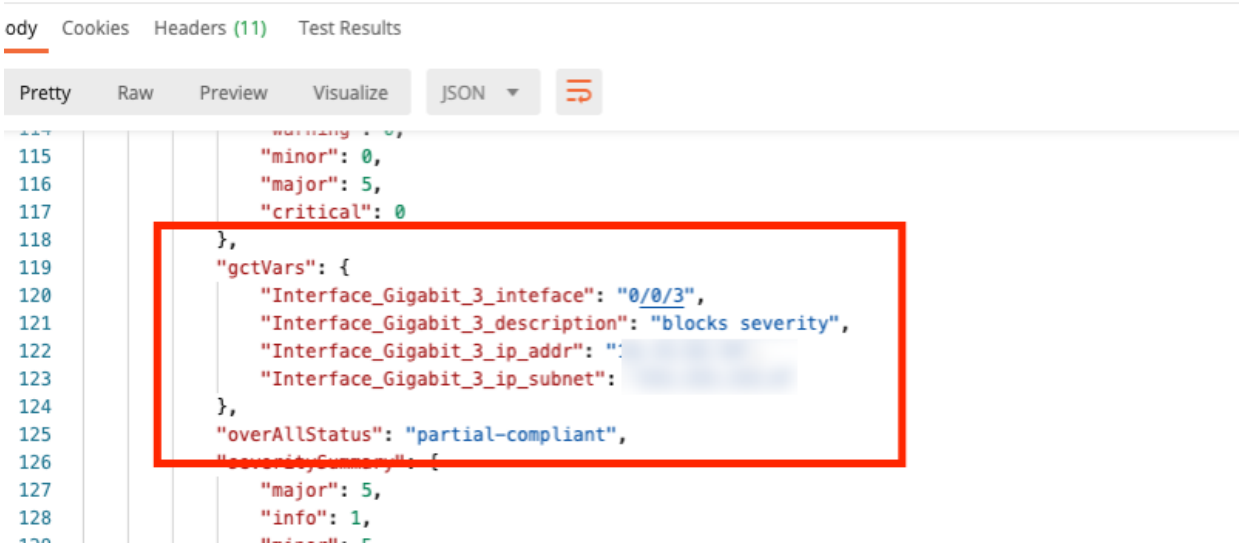
Modello GCT

I GCT sono una funzionalità di base BPA utilizzata per applicare le modifiche alla configurazione sui dispositivi che utilizzano modelli specifici per i controller.

- Creazione di un modello GCT per l'aggiornamento delle configurazioni dei dispositivi e la risoluzione delle violazioni di conformità
- La struttura supporta il mapping automatico delle variabili se le variabili all'interno del modello GCT sono conformi alla sintassi seguente:
  - Per i blocchi di configurazione a dispositivo singolo: <>_<> Esempio: management_interface_ipv4_addr, interfaccia di gestione_ipv4_subnet
  - Per una release futura sono previsti più blocchi di configurazione dei dispositivi
- Se "Block Identifier Name" e "Variable Name from block" contengono spazi, questi spazi devono essere sostituiti da caratteri di sottolineatura ("_") (ad esempio, se "Block Identifier Name" è "Management Interface" e "Variable Name" è "IPV4_ADDR", il nome della variabile nella GCT deve essere "Management_Interface_IPV4_ADDR")
- Gli utenti possono controllare l'output "gctVars" dall'esecuzione del dispositivo di conformità per verificare se la sintassi e le mappature delle variabili GCT sono corrette; Per ottenere

l'esecuzione del dispositivo di conformità, utilizzare le seguenti API REST:

- Ottenere le esecuzioni per trovare l'ID esecuzione
  - URL: /api/v1.0/compliance-remediation/compliance-executions
  - Metodo: OTTIENI
- Ottieni esecuzioni dispositivo tramite ID esecuzione
  - URL: https://<>/bpa/api/v1.0/compliance-remediation/compliance-device-execute?executionId=<>
  - Metodo: OTTIENI



Variabili GCT - gctVars

- Per recuperare le variabili dal blocco, utilizzare la seguente API REST:
  - URL: https://<>/bpa/api/v1.0/compliance-remediation/utils/schema
  - Metodo: POST
  - Corpo: {"blockName": "<< nome blocco >>" }
- Convalidare i modelli GCT applicando i modelli ai dispositivi sia per l'esecuzione a secco che

per l'esecuzione
- Configurare i modelli GCT sopra riportati nei criteri di conformità

Flussi di lavoro

Il framework di correzione fornisce i seguenti flussi di lavoro di riferimento predefiniti:

- PROCESSO DI CORREZIONE: Il flusso di lavoro include il set comune di passaggi necessari per l'esecuzione della correzione.
- SOTTOPROCESSO DI CORREZIONE: Questo flusso di lavoro contiene l'assegnazione di variabili, l'esecuzione a secco di GCT e le attività di commit di GCT che possono essere personalizzate da altri team in base ai requisiti.

Entrambi i flussi di lavoro possono essere utilizzati così come sono, aggiornati o sostituiti in base alle esigenze del cliente.

Modelli di processo

I modelli di processo e i modelli di analisi possono essere configurati in base ai criteri per eseguire controlli preliminari e successivi e confrontare l'output.

Politiche

Il criterio CnR unisce i flussi di lavoro, i modelli GCT e i modelli di processo per tipo di dispositivo, che possono essere utilizzati per correggere la configurazione utilizzando i processi.

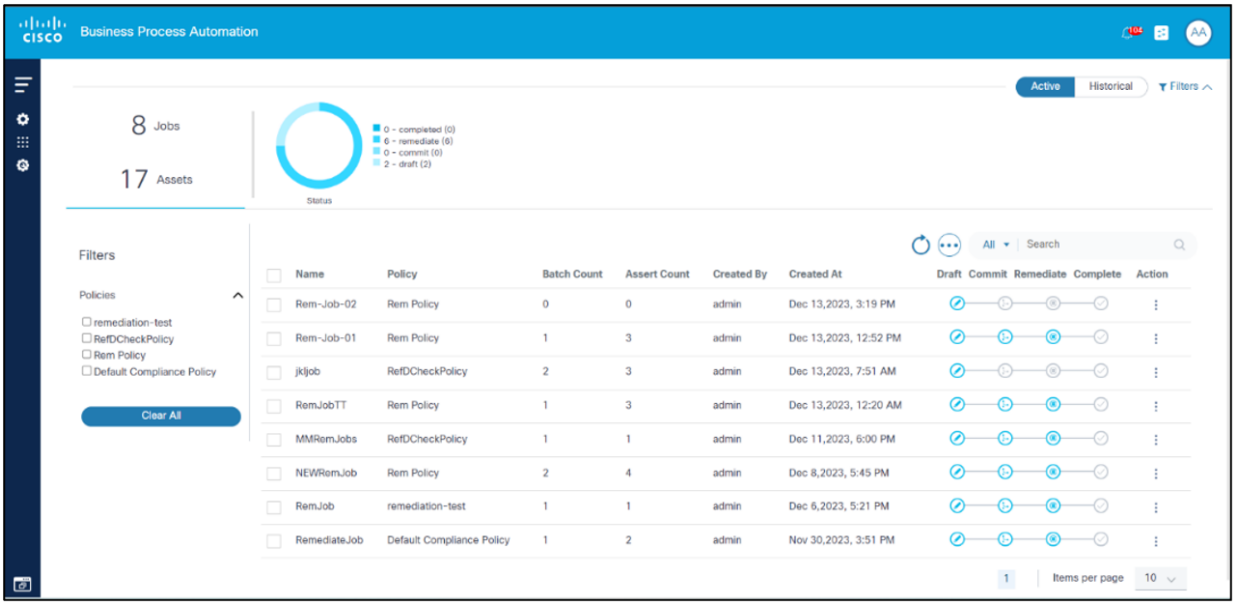
Processi di monitoraggio e aggiornamento

I processi di monitoraggio e aggiornamento consentono agli operatori di applicare criteri di monitoraggio e aggiornamento a un elenco selezionato di asset interessati. Il processo di monitoraggio e aggiornamento può essere eseguito su richiesta o nei tempi previsti. In fase di esecuzione, il flusso di lavoro di monitoraggio e aggiornamento può estrarre dati da diverse origini, inclusi i dettagli dei dispositivi, i dettagli di esecuzione della conformità e il framework RefD.

Elenco processi di monitoraggio e aggiornamento

Gli utenti possono filtrare, ordinare e visualizzare i processi di monitoraggio e aggiornamento creati nel dashboard come indicato di seguito:

- Processi: Visualizza il totale dei processi creati
- Risorse: Visualizza il totale dei cespiti creati
- Stato: Visualizza i processi per stato
- Attivo e storico: Visualizza i job attivi o cronologici (inattivi), in base alla selezione
- Criteri: Filtra i processi di monitoraggio e aggiornamento in base ai criteri
- Griglia principale: Visualizza l'elenco predefinito di job che è possibile ordinare facendo clic sull'intestazione e include una ricerca per nome e criterio con le paginazioni
- Azioni: I processi possono essere archiviati o eliminati quando sono in stato di bozza o completati. impossibile archiviare o eliminare un processo in esecuzione

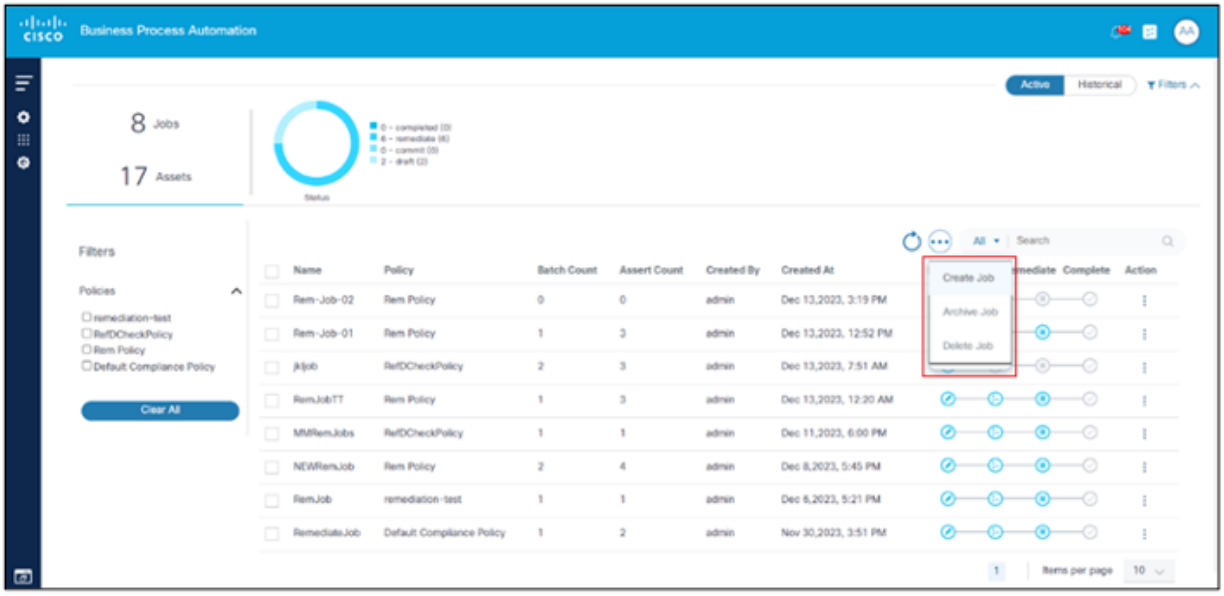


Elenco processi di monitoraggio e aggiornamento

Creazione e modifica di job di risoluzione

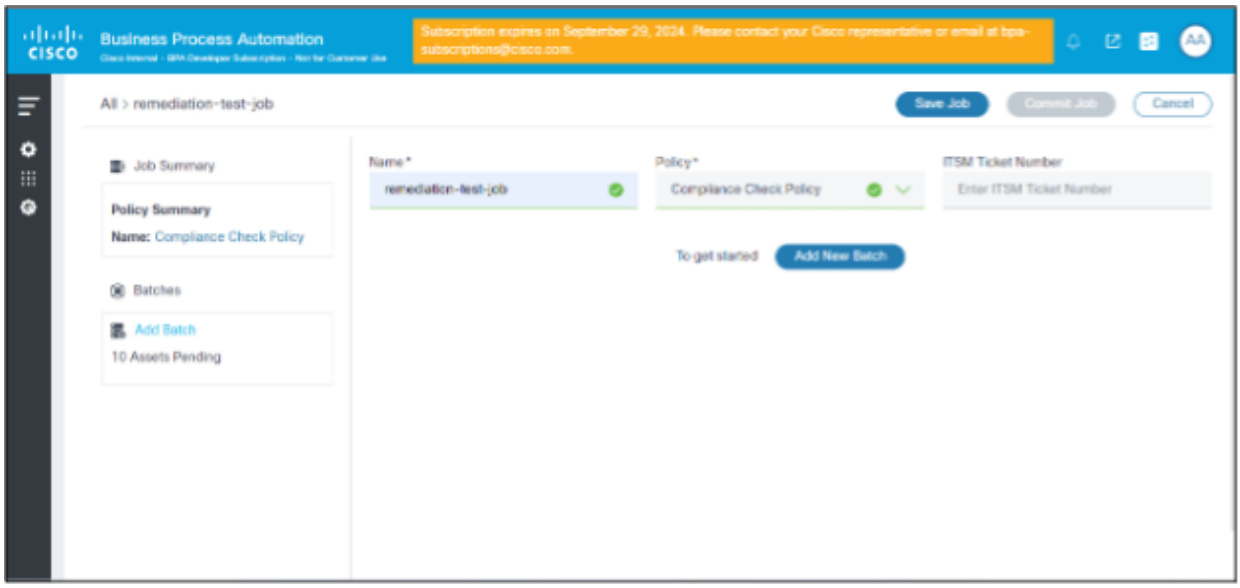
I job di risoluzione vengono creati dalla pagina Elenco job e possono essere creati eseguendo le operazioni riportate di seguito.

1. Selezionare l'icona Altre opzioni > Crea job. Viene visualizzata la pagina Crea job.



Opzioni processi di monitoraggio e aggiornamento

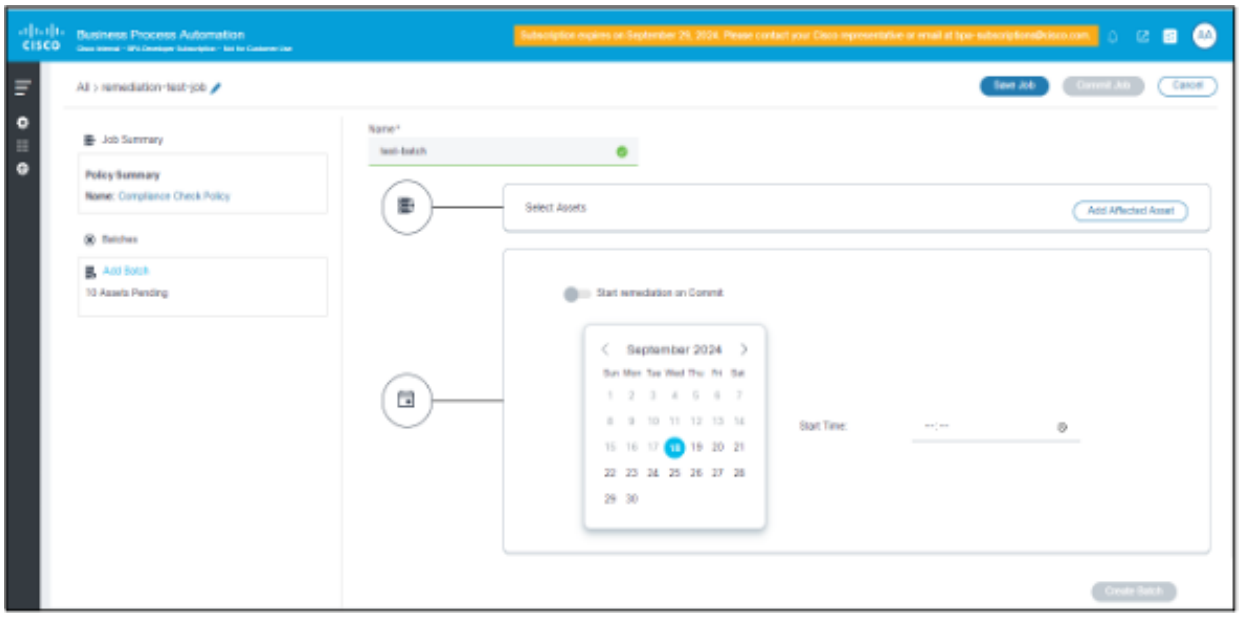
2. Completare o modificare i dettagli.



Processi di risoluzione: Dettagli

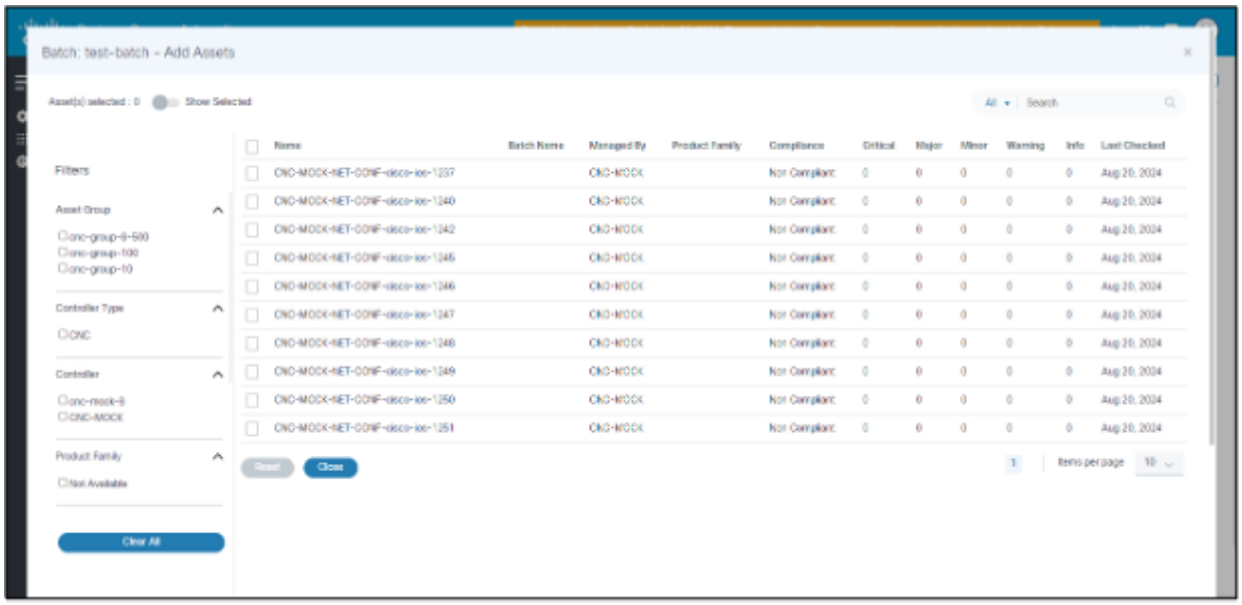
3. Fare clic su Salva job.

Per aggiungere batch ai job dalla pagina Crea job:



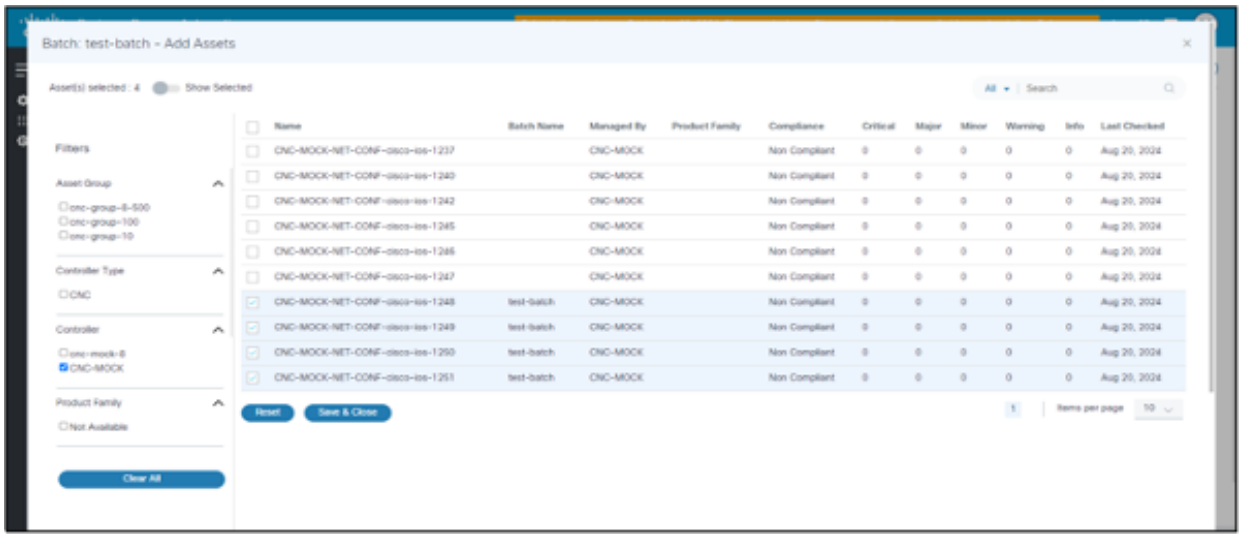
Processi di risoluzione: Aggiungi batch

1. Fare clic su Aggiungi nuovo batch.
2. Inserire il Nome, i Dettagli cespite interessato e i Dettagli programma.
3. Fare clic su Aggiungi asset interessati.
4. Nella pagina Dettagli asset, selezionare l'elenco degli asset interessati e fare clic su Salva job.
5. Filtrare le risorse in base al tipo di controller, al controller, al gruppo di asset e alla famiglia di prodotti.
6. Una volta selezionate le risorse, fare clic su Salva e chiudi per tornare alla pagina precedente.



Processi di risoluzione: Aggiungi asset interessati

Nota: Gli utenti possono applicare i filtri nella pagina Asset interessati



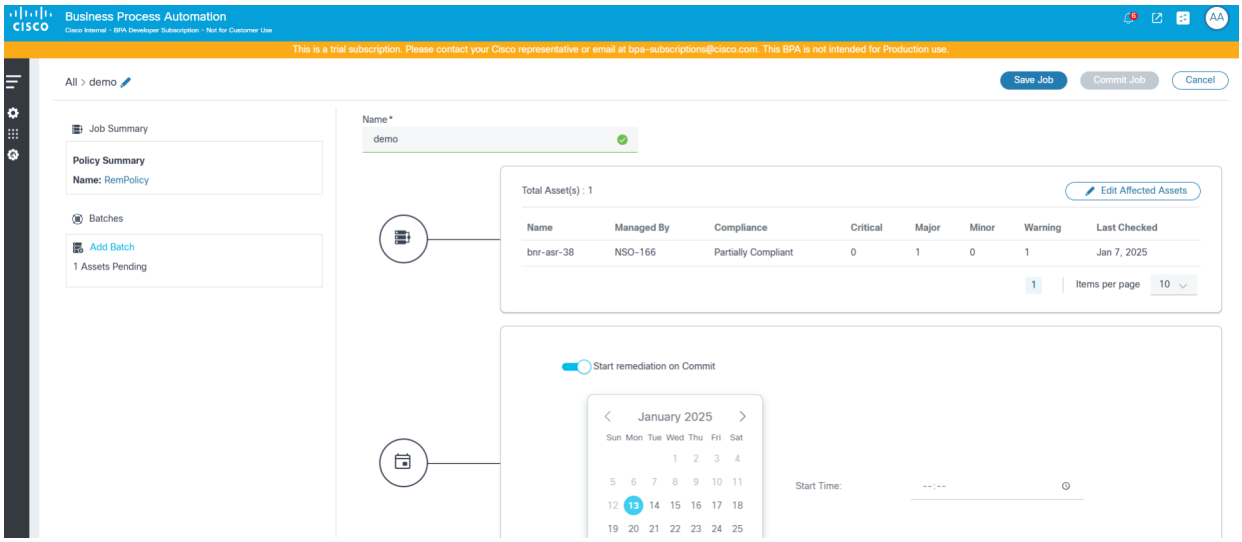
Processi di risoluzione: Aggiungi filtri interessati

Una volta aggiunti i cespiti interessati, il batch può essere eseguito una sola volta, al momento del salvataggio o a un'ora futura programmata.

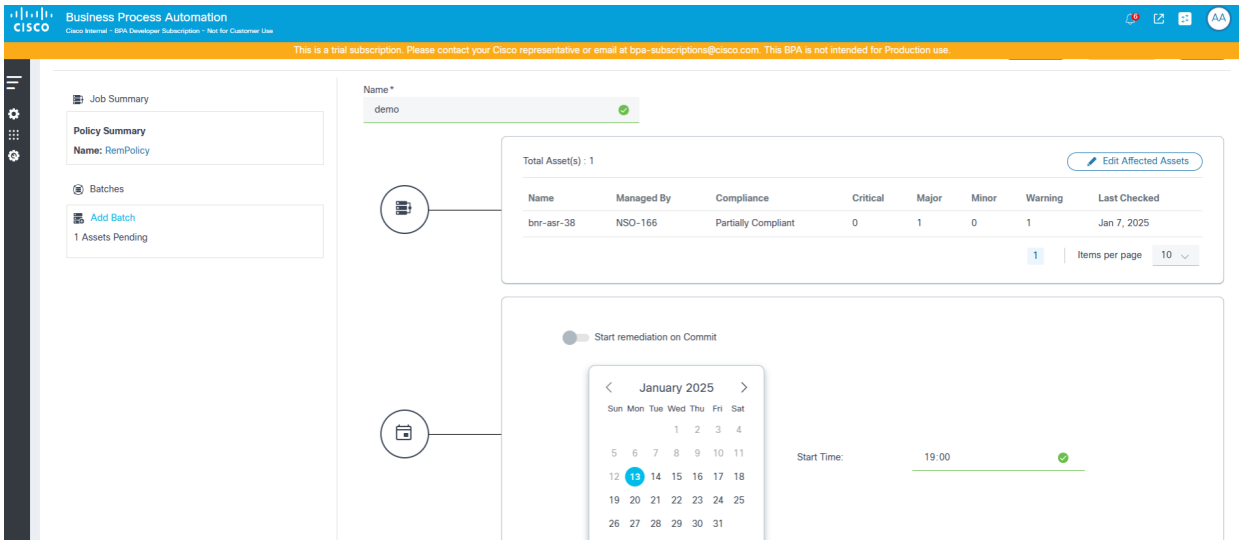
Nota: Per eseguire il job come On Demand, abilitare l'interruttore Avvia monitoraggio e aggiornamento su commit. Se un utente seleziona questa opzione, la data e l'ora non sono necessarie. Se l'utente seleziona l'opzione Occasionale, è necessario specificare la data e l'ora per eseguire il job.

Un singolo processo di monitoraggio e aggiornamento dispone di più batch. Ogni batch può essere avviato al momento del commit o in una data e ora pianificate.

Un batch di monitoraggio e aggiornamento in-commit può essere eseguito su richiesta o programmato.



Processi di risoluzione: Su richiesta

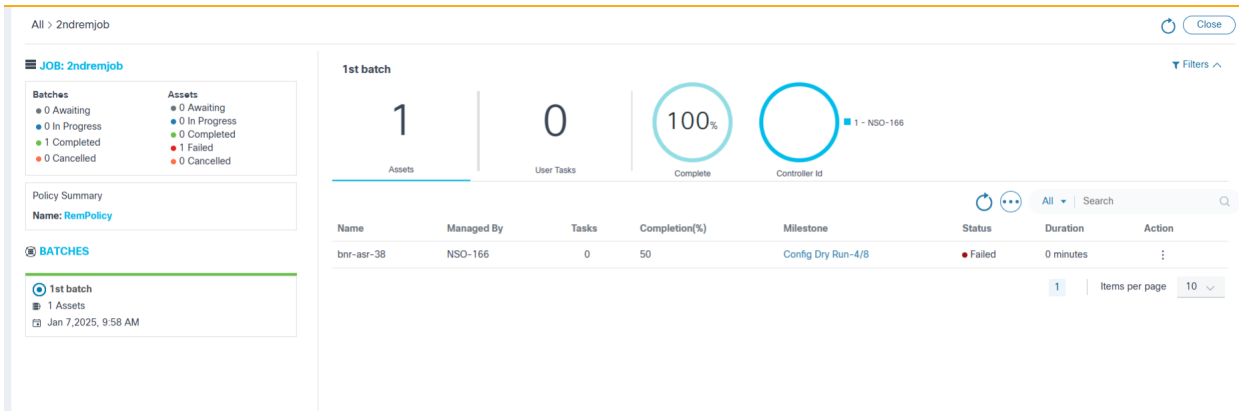


Processi di risoluzione: Una tantum/pianificato

Esecuzione correzione: Elenco dispositivi

Una volta eseguito il commit del job di monitoraggio e aggiornamento, l'esecuzione viene attivata e lo stato del job viene visualizzato nella pagina Elenca dispositivi in Job di monitoraggio e aggiornamento. Gli utenti possono applicare i filtri in base a ID controller, Nome, Gestito da, Famiglia di prodotti.

- PROCESSO: visualizza i dettagli sullo stato di batch e asset e il nome del criterio selezionato per eseguire il processo di monitoraggio e aggiornamento
- BATCH: visualizza l'elenco dei batch come parte del processo di monitoraggio e aggiornamento corrente
- Aggiornamento automatico: visualizza le opzioni per aggiornare automaticamente la pagina ogni 30 secondi se il job è in esecuzione, aggiornare la pagina o annullare per tornare alla pagina precedente.
- Dettagli livello batch: visualizza i dettagli di riepilogo a livello di batch, tra cui il conteggio totale degli asset, il conteggio delle attività utente, la percentuale di completamento e i dettagli del controller
- Griglia cespiti: visualizza la visualizzazione della griglia dei cespiti, che include il task utente, la percentuale di completamento e la fase cardine corrente per ciascun cespite.



Esecuzione correzione: Elenco dispositivi

Esecuzione correzione: Dettagli attività utente in linea

Nell'elenco dei dispositivi, la colonna Attività indica se un utente ha delle attività da eseguire.

Per visualizzare i dettagli dei task utente in linea:

1. Selezionare il conteggio delle attività. Viene visualizzata la finestra dell'elenco Attività utente.
2. Selezionare un'attività. Viene visualizzata la finestra Dettagli task utente.

È possibile eseguire le azioni seguenti da inline:

- Completa
- Riprova
- Annulla

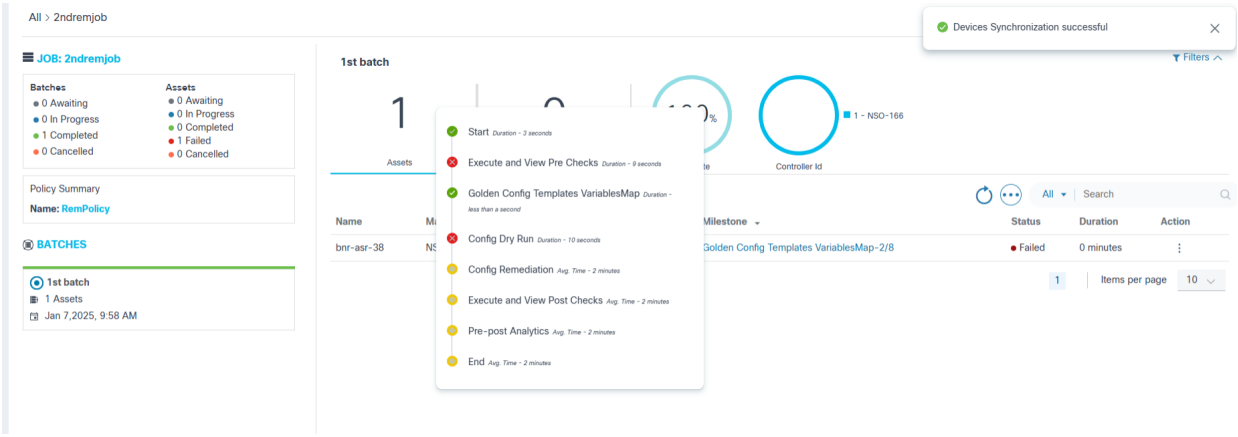
Esecuzione correzione: Dettagli attività cardine in linea

Nell'elenco dei dispositivi, la colonna Cardine indica l'attività cardine corrente relativa al ripristino del dispositivo specificato.

Per visualizzare i dettagli delle attività cardine in linea, selezionare la colonna. Viene visualizzata la finestra Dettagli attività cardine.

Per le fasi cardine sono disponibili gli stati riportati di seguito.

- Non iniziata
- In esecuzione
- Completato
- Non riuscito



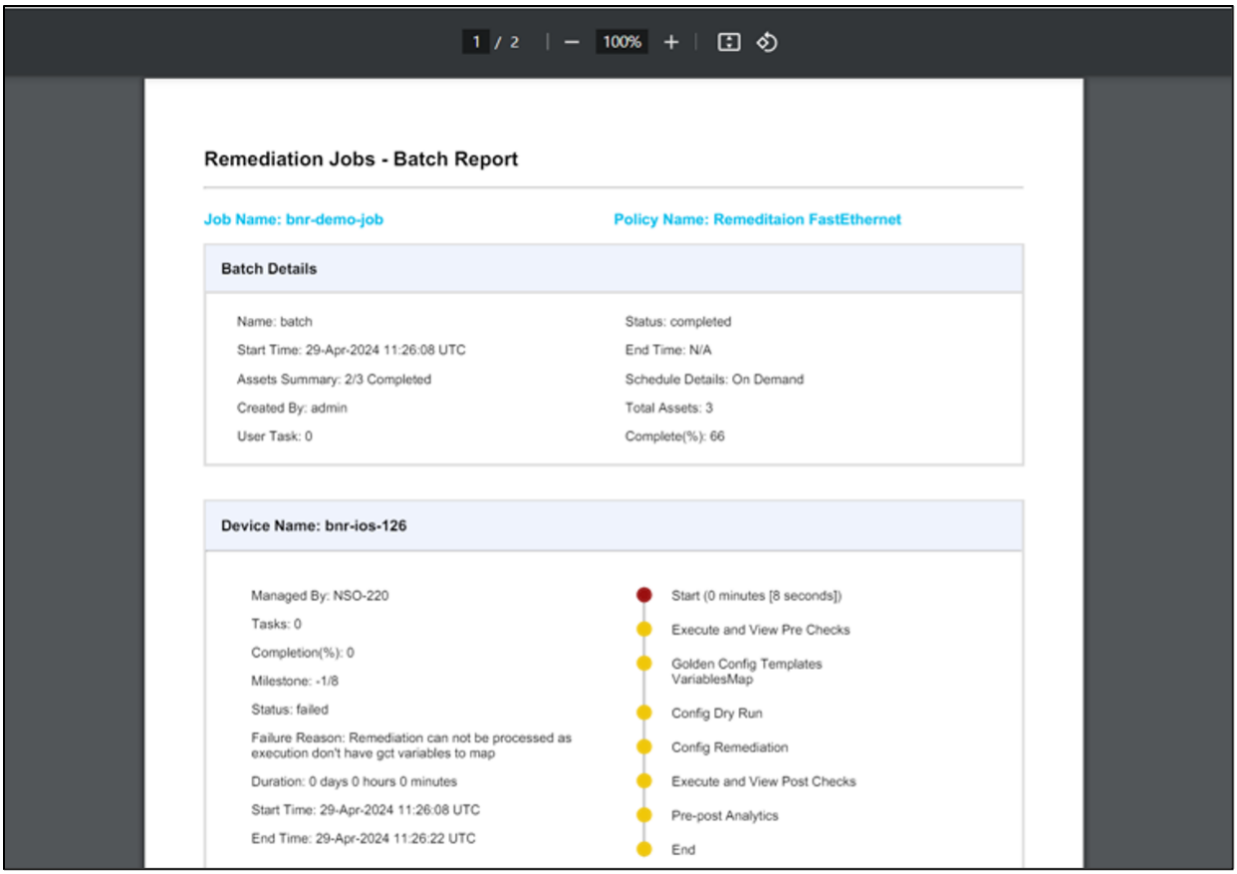
Esecuzione correzione: Dettagli attività cardine in linea

Esecuzione correzione: Generazione e download di report PDF di riepilogo batch

È possibile generare e scaricare riepiloghi batch.

Per scaricare il report riepilogativo in formato PDF per batch:

1. Selezionare l'icona Altre opzioni > Genera report. Il sistema verifica internamente che il report sia pronto. Quando il report è pronto, l'opzione Scarica report è abilitata.
2. Selezionare l'icona Altre opzioni > Scarica report. Il PDF viene scaricato.



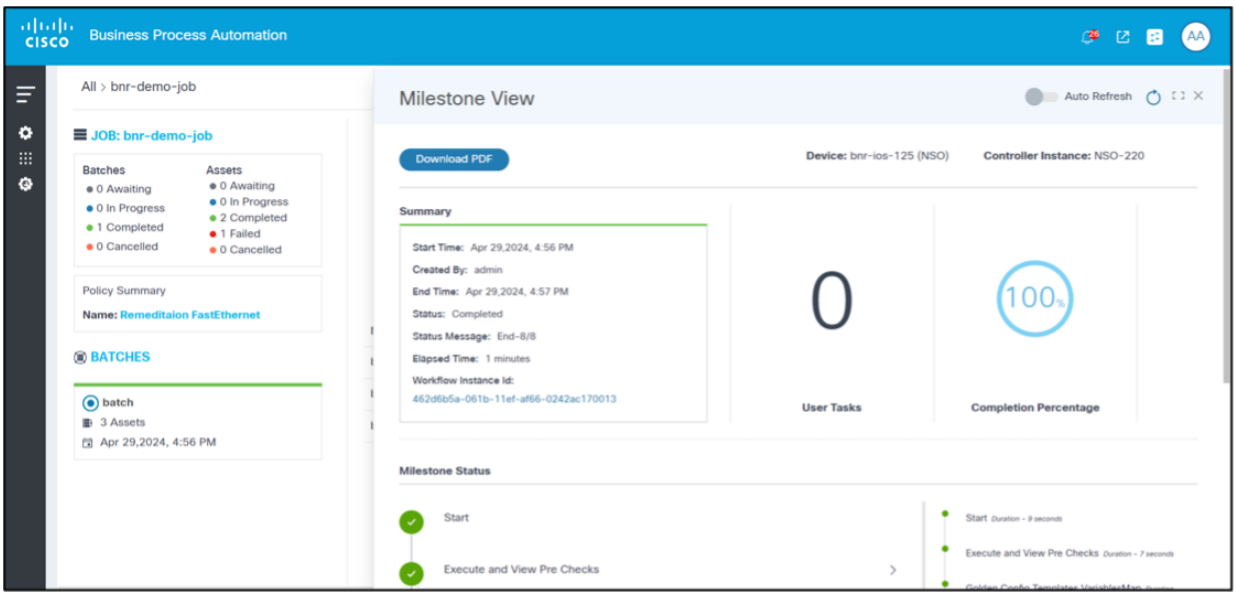
PDF report riepilogo batch

Il rapporto Batch processi di risoluzione contiene una sezione Dettagli batch che fornisce un riepilogo del batch di correzione, ad esempio il nome del processo, il nome del batch, l'ora di inizio e di fine, i cespiti totali e lo stato generale. È seguita da una sezione Device Detail (una sezione per dispositivo) che include il nome del dispositivo, lo stato di ripristino specifico del dispositivo, la cronologia, la durata, l'elenco delle fasi cardine e lo stato.

Esecuzione correzione: Dettagli dispositivo

Per visualizzare i dettagli dei dispositivi per le attività cardine, selezionare la pagina Dettagli dispositivo. Verrà visualizzata la pagina Visualizzazione attività cardine.

Viene visualizzato un riepilogo del monitoraggio e dell'aggiornamento per il dispositivo specificato con uno stato dettagliato delle fasi cardine, incluso l'output dei comandi relativi alle fasi cardine completate. Ad esempio, è possibile visualizzare gli output del comando process template, l'output del comando GCT dry run e il contenuto dell'output delle differenze di analisi.



Esecuzione correzione: Visualizzazione attività cardine

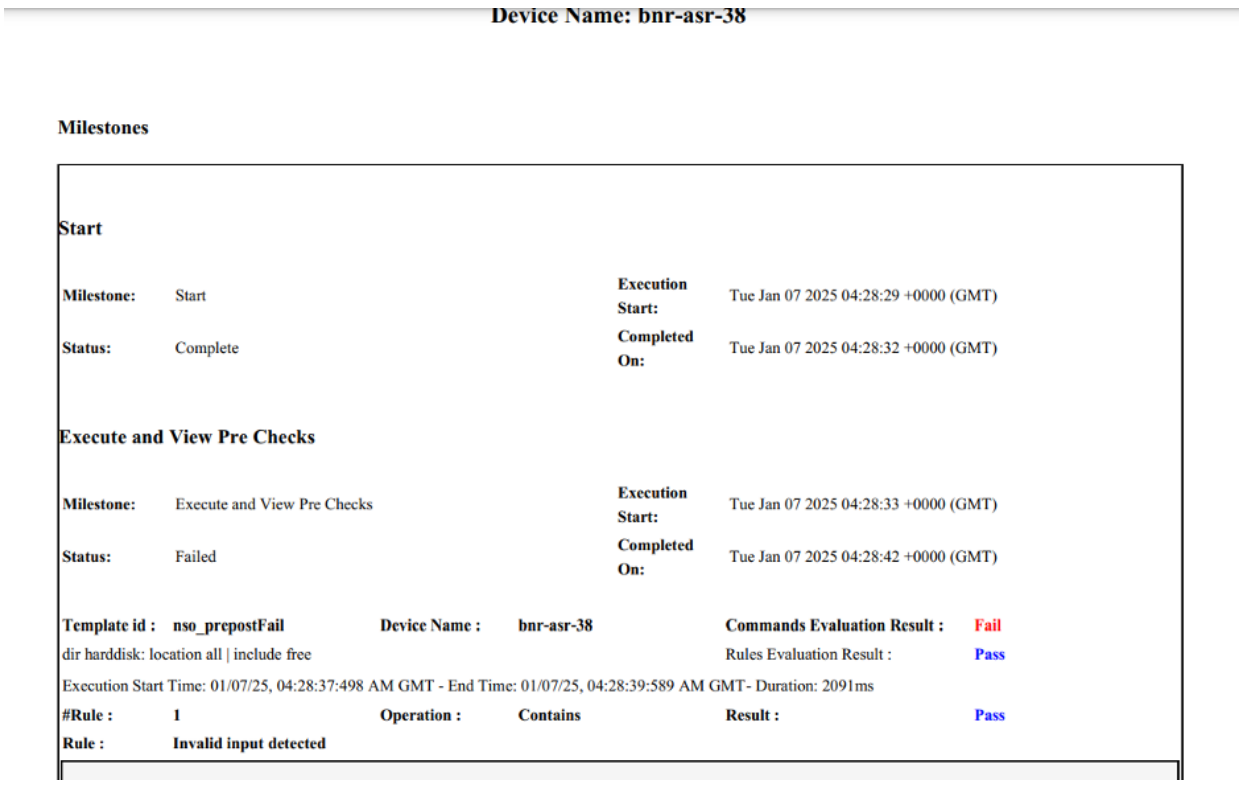
Esecuzione correzione: Dettagli dispositivo - Report attività cardine

Per visualizzare il rapporto attività cardine:

1. Selezionare la pagina Dettagli dispositivo. Verrà visualizzata la pagina Visualizzazione attività cardine.
2. Fare clic su Download PDF. Il report visualizzazione cardine viene generato e scaricato come illustrato di seguito.

Questo report fornisce dettagli più elaborati sulle fasi cardine e il contenuto corrispondente per il

monitoraggio e l'aggiornamento del dispositivo selezionato.



Device Name: bnr-asr-38

Milestones

Start

Milestone:	Start	**Execution Start:**	Tue Jan 07 2025 04:28:29 +0000 (GMT)
Status:	Complete	**Completed On:**	Tue Jan 07 2025 04:28:32 +0000 (GMT)

Execute and View Pre Checks

Milestone:	Execute and View Pre Checks	**Execution Start:**	Tue Jan 07 2025 04:28:33 +0000 (GMT)
Status:	Failed	**Completed On:**	Tue Jan 07 2025 04:28:42 +0000 (GMT)

Template id :	**nso_prepostFail**	**Device Name :**	**bnr-asr-38**	**Commands Evaluation Result :**	**Fail**
dir harddisk: location all | include free				Rules Evaluation Result :	**Pass**
Execution Start Time: 01/07/25, 04:28:37:498 AM GMT - End Time: 01/07/25, 04:28:39:589 AM GMT- Duration: 2091ms					
#Rule :	**1**	**Operation :**	**Contains**	**Result :**	**Pass**
Rule :	**Invalid input detected**				

Esecuzione correzione: Dettagli dispositivo - Cardine Visualizza rapporto PDF

Configurazione: Blocchi e regole

Funzionalità dei blocchi

I blocchi di configurazione sono elementi essenziali per la creazione e l'applicazione di policy di conformità nei sistemi di gestione della rete. Rappresentano configurazioni CLI dei dispositivi, ad esempio quelle per interfacce, BGP (Router Border Gateway Protocol) e altro ancora. Di seguito sono riportate le caratteristiche principali dei blocchi di configurazione:

- Modularità: I blocchi di configurazione consentono la creazione di regole modulari, consentendo agli amministratori di definire e gestire in modo indipendente sezioni discrete delle configurazioni dei dispositivi. Questa modularità semplifica il processo di aggiornamento e gestione delle policy di conformità.
- Granularità: Suddividendo le configurazioni dei dispositivi in parti più piccole e gestibili, gli amministratori possono eseguire controlli di conformità accurati e applicare standard specifici. In questo modo, ogni parte della configurazione del dispositivo rispetta le regole richieste.
- Riutilizzabilità: Una volta definiti, i blocchi di configurazione possono essere riutilizzati su più dispositivi e policy di conformità. Questa riutilizzabilità riduce la ridondanza e garantisce coerenza nella gestione della configurazione.

- Blocco di configurazione statica: Un blocco di configurazione statico rappresenta la configurazione del dispositivo raw senza variabili.

  Esempio: Il blocco seguente può essere utilizzato per eseguire un controllo di conformità sull'interfaccia TwentyFiveGigE0/0/0/31

```
interface TwentyFiveGigE0/0/0/31
  description au01-inv-5g-08 enp94s0f0
  no shutdown
  load-interval 30
  l2transport
```

- Blocco configurazione dinamica: Un blocco di configurazione dinamico rappresenta la configurazione del dispositivo che include variabili che consentono una maggiore adattabilità e riutilizzabilità. Questi blocchi funzionano come un modello TTP, si applicano alle configurazioni dei dispositivi e recuperano i valori per le variabili. È possibile aggiungere condizioni alle regole per la convalida di queste variabili. Fare riferimento a https://ttp.readthedocs.io/en/latest/Overview.html per ulteriori dettagli su TTP.

  Esempio: Il blocco seguente può essere utilizzato per eseguire un controllo di conformità su tutte le interfacce TwentyFiveGigE

```
interface TwentyFiveGigE{{INTERFACE_ID}}
  description {{DESCRIPTION}}
  no shutdown
  load-interval {{LOAD_INTERVAL}}
  l2transport
```

Blocco di configurazione dinamico con sottogerarchie: Questo blocco funziona come un blocco di configurazione dinamico ed è utilizzato per recuperare i valori dalle configurazioni dei dispositivi che hanno più gerarchie.

Esempio: Nell'esempio seguente viene illustrata la configurazione di un dispositivo e il blocco dinamico corrispondente utilizzato per recuperare i valori da una struttura gerarchica.

Configurazione dispositivo con struttura gerarchica:

```
router bgp 12.34
address-family ipv4 unicast
  router-id 1.1.1.X
!
vrf CT2S2
  rd 102:103
  !
```

```
  neighbor 10.1.102.XXX
  remote-as 102.XXX
  address-family ipv4 unicast
    send-community-ebgp
    route-policy vCE102-link1.102 in
    route-policy vCE102-link1.102 out
  !
  !
  neighbor 10.2.102.XXX
  remote-as 102.XXX
  address-family ipv4 unicast
    route-policy vCE102-link2.102 in
    route-policy vCE102-link2.102 out
  !
  !
vrf AS65000
  rd 102:XXX
  !
  neighbor 10.1.37.X
  remote-as 65000
  address-family ipv4 labeled-unicast
    route-policy PASS-ALL in
    route-policy PASS-ALL out
```

Dynamic Block Configuration per analizzare la configurazione precedente.

```
router bgp {{ ASN }}
```

```
address-family ipv4 unicast {{ _start_ }}
  router-id {{ bgp_rid }}
```

```
vrf {{ vrf }}
  rd {{ rd }}
```

```
  neighbor {{ neighbor }}
  remote-as {{ neighbor_asn }}
```

```
address-family ipv4 unicast {{ _start_ }}
  send-community-ebgp {{ send_community_ebgp }}
  route-policy {{ RPL_IN }} in
  route-policy {{ RPL_OUT }} out
```

Funzionalità delle regole

Le regole consentono agli utenti di definire le condizioni da convalidare in base alle variabili presenti in un blocco di configurazione. Come parte di un'esecuzione, il modulo di gestione della conformità analizza la configurazione del dispositivo, trova le istanze corrispondenti delle istanze dei blocchi di dispositivo, legge i valori dalle righe ed esegue le condizioni definite nelle regole in base ai valori. Il risultato, indipendentemente dalla violazione o meno delle linee di configurazione, viene memorizzato per la visualizzazione nel quadro comandi.

Le regole di configurazione fanno ora parte del ciclo di vita di creazione dei blocchi. Non esiste quindi una pagina separata per visualizzare le regole. Le regole possono essere elencate, create e aggiornate nella pagina di creazione o aggiornamento dei blocchi corrispondente.

Nel quadro del CnR, le regole svolgono un ruolo cruciale nella convalida delle configurazioni in base a condizioni specifiche. In questa sezione viene fornita una panoramica di come le regole vengono integrate e gestite nel sistema.

- Scopo: Le regole consentono agli utenti di definire le condizioni utilizzate per convalidare le variabili presenti in un blocco di configurazione
- Processo di esecuzione:
    - Il modulo di gestione della conformità analizza la configurazione del dispositivo
    - Identifica le istanze corrispondenti delle istanze dei blocchi di dispositivo
    - Estrae i valori dalle righe di configurazione
    - Applica a questi valori le condizioni definite nelle regole.
    - I risultati che indicano le violazioni vengono memorizzati e visualizzati nel dashboard

Integrazione con il ciclo di vita dei blocchi

- Integrazione del ciclo di vita: Le regole di configurazione sono ora parte integrante del ciclo di vita di creazione dei blocchi
- Gestione:
    - Le regole vengono elencate, create e aggiornate direttamente all'interno delle pagine utilizzate per la creazione di blocchi o gli aggiornamenti
    - Non esiste una pagina separata dedicata alla visualizzazione delle regole, che ne semplifica la gestione all'interno del ciclo di vita del blocco

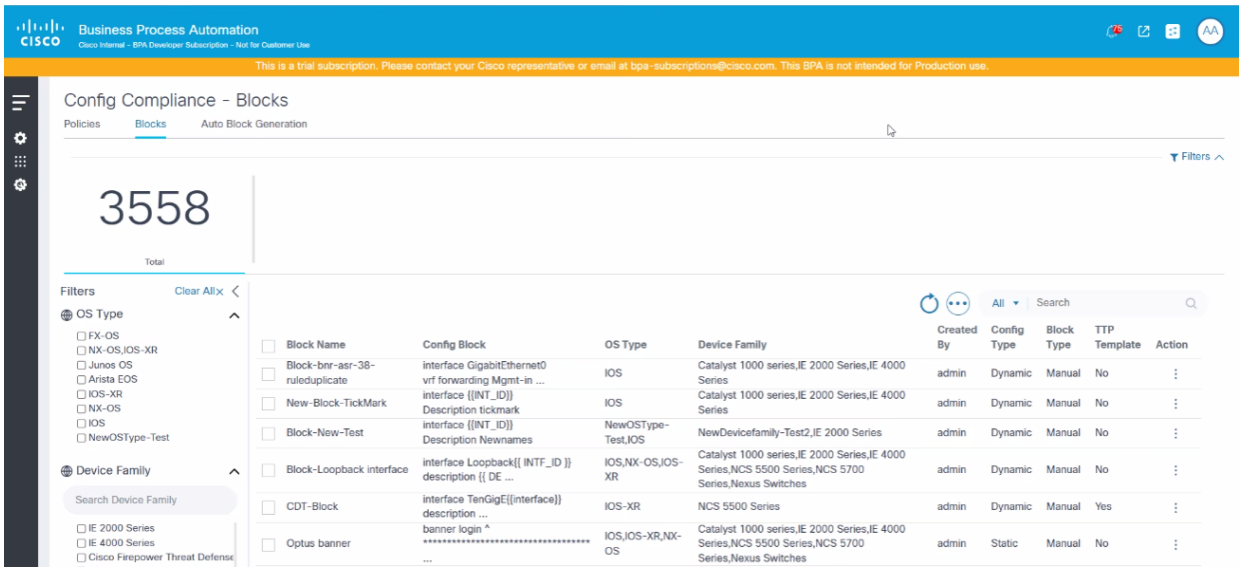
Questa integrazione garantisce l'integrazione dei controlli di conformità nel processo di gestione della configurazione, consentendo il monitoraggio e la gestione efficiente delle configurazioni dei dispositivi in base a regole predefinite.

Elenca blocchi

La pagina Blocchi elenca tutti i blocchi di configurazione e fornisce le azioni per generare, aggiungere, modificare, eliminare, importare ed esportare i blocchi. Gli utenti possono filtrare, ordinare e visualizzare i dettagli dei blocchi.

Blocco Dettagli funzionalità

- Conteggio totale: Visualizza il numero totale di blocchi creati
- Opzioni filtro:
    - Tipi di sistema operativo e famiglia di dispositivi: Consente agli utenti di filtrare i blocchi in base ai criteri selezionati
- Griglia principale:
    - Visualizza un elenco predefinito di blocchi
    - Gli utenti possono ordinare l'elenco facendo clic sulle intestazioni di colonna
    - Include una funzione di ricerca che consente agli utenti di eseguire ricerche in base a tutti gli attributi o in modo specifico in base al nome del blocco
    - Supporta l'impaginazione per una facile navigazione nell'elenco
- Azioni:
    - Modifica: Gli utenti possono modificare i blocchi esistenti
    - Elimina: Gli utenti possono rimuovere i blocchi dall'elenco



Elenco blocchi di configurazione

Aggiunta o modifica di blocchi e regole

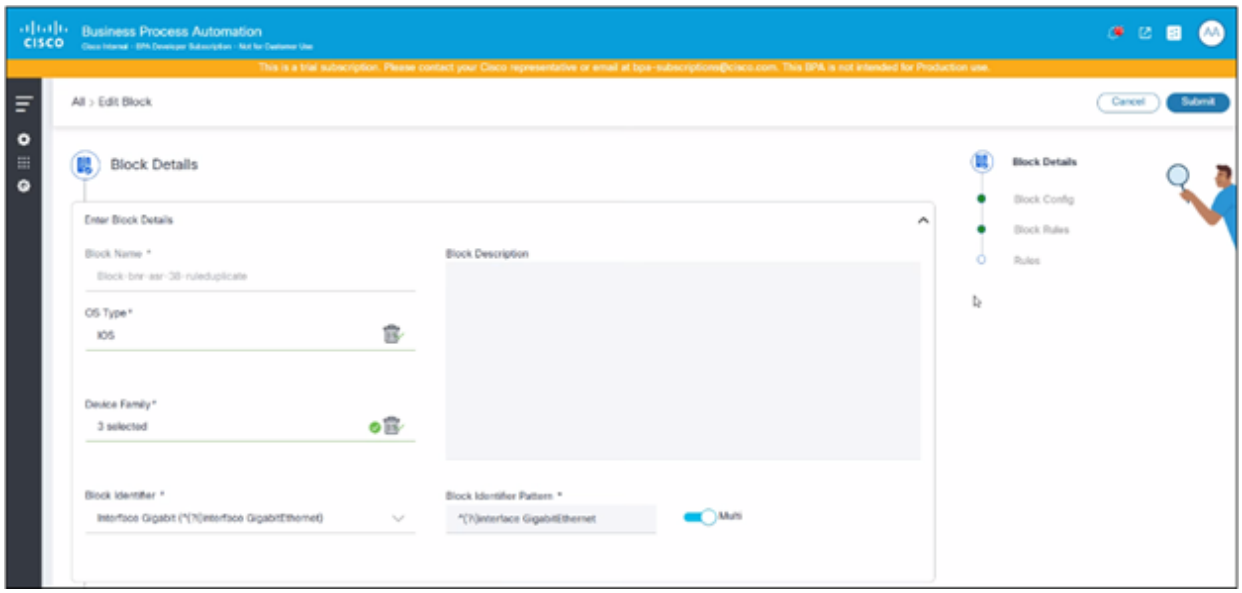
La pagina Aggiungi o Modifica blocco è stata progettata per acquisire e gestire le informazioni essenziali relative ai blocchi. In questa pagina sono disponibili le sezioni riportate di seguito.

- Dettagli blocco di base:

  La sezione Dettagli di base include:

  - Nome blocco: Nome designato per il blocco
  - Descrizione: Breve panoramica o spiegazione dello scopo o della funzionalità del blocco
  - Tipo di sistema operativo: Tipo di sistema operativo associato al blocco
  - Famiglia di dispositivi: Categoria o gruppo di dispositivi compatibili con il blocco
  - Selezione identificatore blocco: Opzioni per selezionare un identificatore univoco per il blocco
  - Aggiungere o modificare i dettagli dell'identificatore di blocco: Se non è presente un identificatore di blocco appropriato, gli utenti possono utilizzare gli stessi campi per aggiungere o modificare i seguenti dettagli:

    - Nome identificatore blocco: Nome specifico assegnato all'identificatore di blocco
    - Motivo: Modello o formato seguito dall'identificatore di blocco
    - Multiplo: Attiva/disattiva per indicare se considerare il blocco di configurazione come una configurazione multilinea

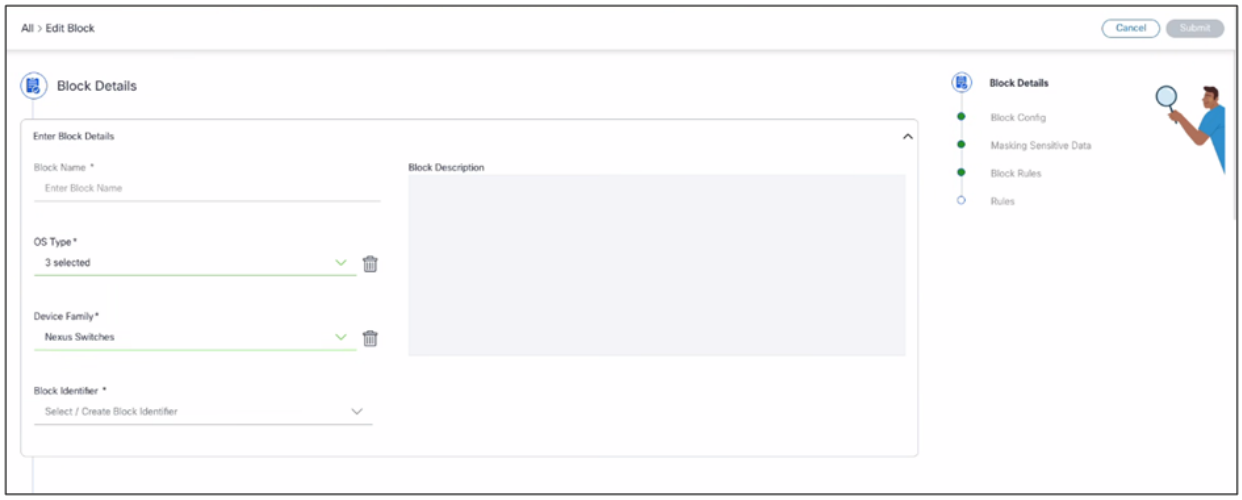


Aggiungi o modifica blocchi - Dettagli blocco

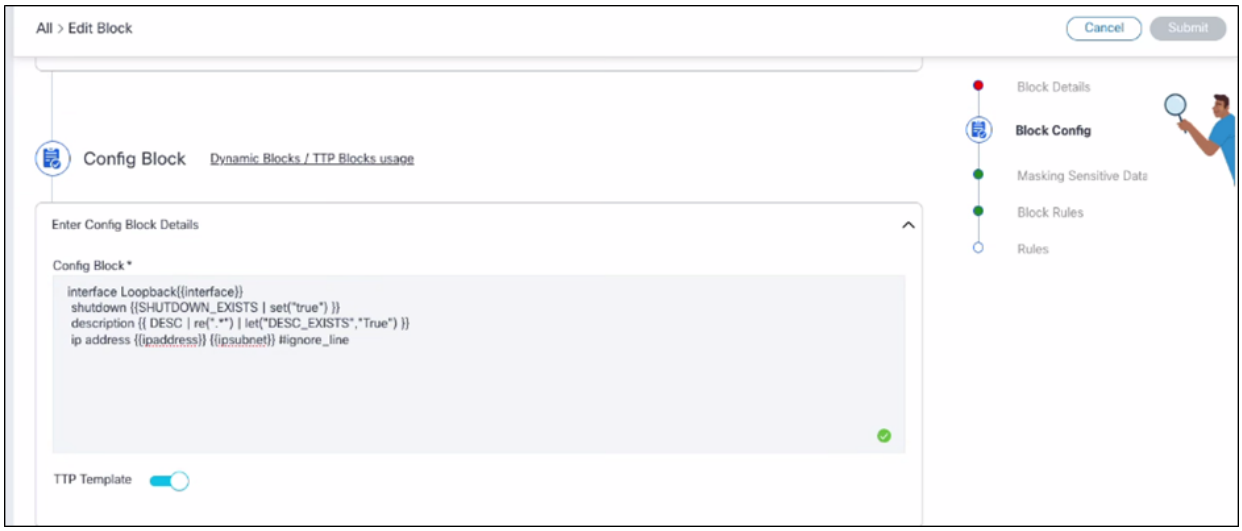
- Configurazione blocco:

La sezione Configurazione blocco include quanto riportato di seguito.

- Blocco di configurazione: Rappresenta la configurazione di un dispositivo, che incorpora variabili diverse. In questa configurazione viene descritto come configurare e gestire il dispositivo nel sistema.
- Modello TTP: Indica se il blocco è designato come modello TTP (Template Transformation Protocol), consentendo di identificare i blocchi utilizzati come modelli per la trasformazione o la standardizzazione delle configurazioni tra i dispositivi.



Dettagli blocco



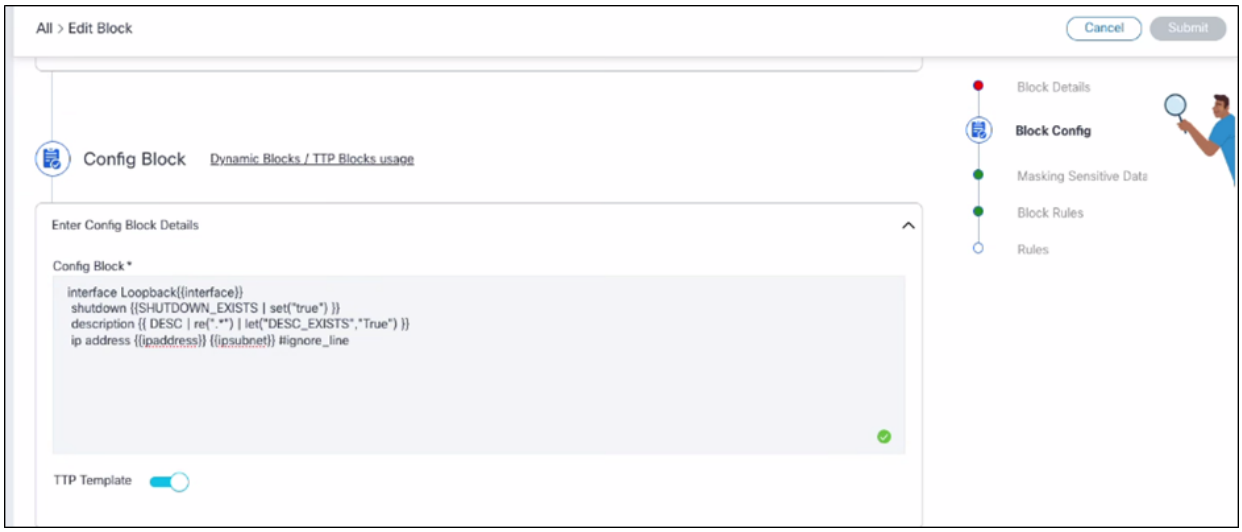
Configurazione blocco

Utilizzo della sintassi Ignora riga

La sintassi Ignora riga consente agli utenti di aggiungere un commento alla fine di una riga di configurazione specifica in un blocco per indicare al sistema di ignorare eventuali controlli di conformità o violazioni su tale riga. In questo modo la linea non verrà visualizzata come violazione nei report o nel dashboard.

Per utilizzare la sintassi Ignora linea, completare la procedura seguente:

1. Individuare la riga di configurazione da escludere dai controlli di conformità (ad esempio, indirizzo IP).



Ignora sintassi delle righe

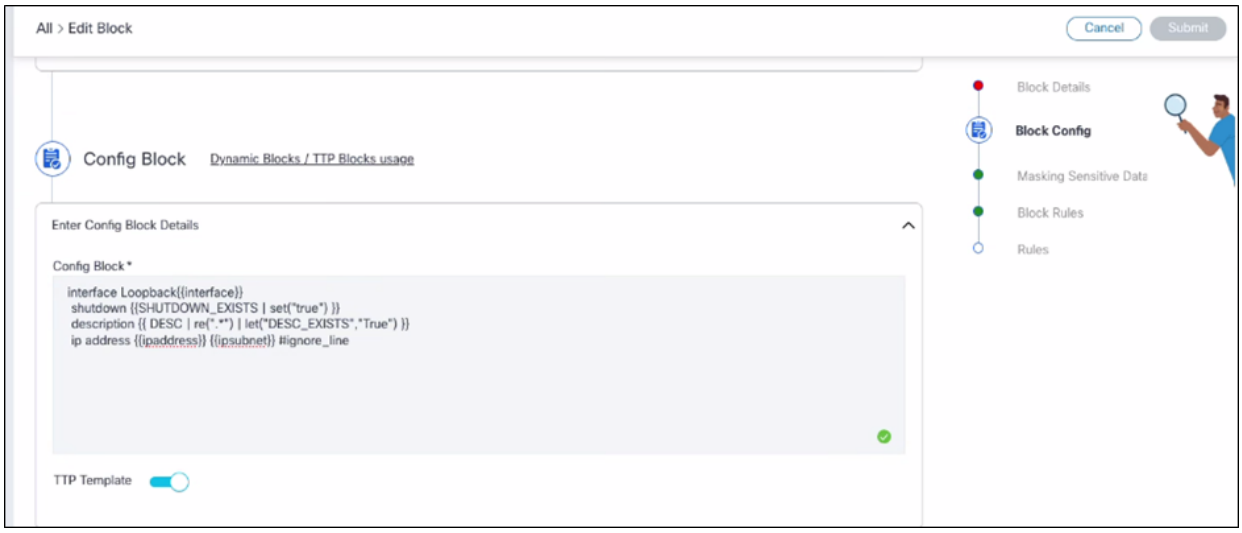
2. Aggiungere la riga utilizzando la sintassi di commento "#ignore_line" alla fine della riga. Esempio: indirizzo ip {{ipAddress}} {{ipSubnet}} #ignore_line

Generazione di violazioni

Questa funzionalità TTP (Template Text Parser) nella configurazione a blocchi può essere utilizzata per indicare se deve essere generata una violazione in presenza di una determinata riga.

Per utilizzare la funzionalità TTP, completare le seguenti operazioni:

1. Nella sezione Configurazione blocco della pagina di creazione o modifica del blocco, individuare la riga di configurazione da controllare.
2. Definite una variabile TTP utilizzando il comando set o let come indicato di seguito:
   - Se la riga di configurazione è stata chiusa, utilizzare il comando set per definire una variabile nel modo seguente:
     shutdown | {{FLAG_ARRESTO | set("true")}}"
   - Se gli utenti hanno una variabile esistente nella riga di configurazione come la descrizione {{DESC}}, utilizzare il comando let come segue:
     descrizione {{ DESC | re(".*") | let("DESC_EXISTS", "True") }}
3. Utilizzare queste variabili (SHUTDOWN_FLAG o DESC_EXISTS nell'esempio precedente) in una regola per aumentare le violazioni.



Genera violazioni

Effetto:

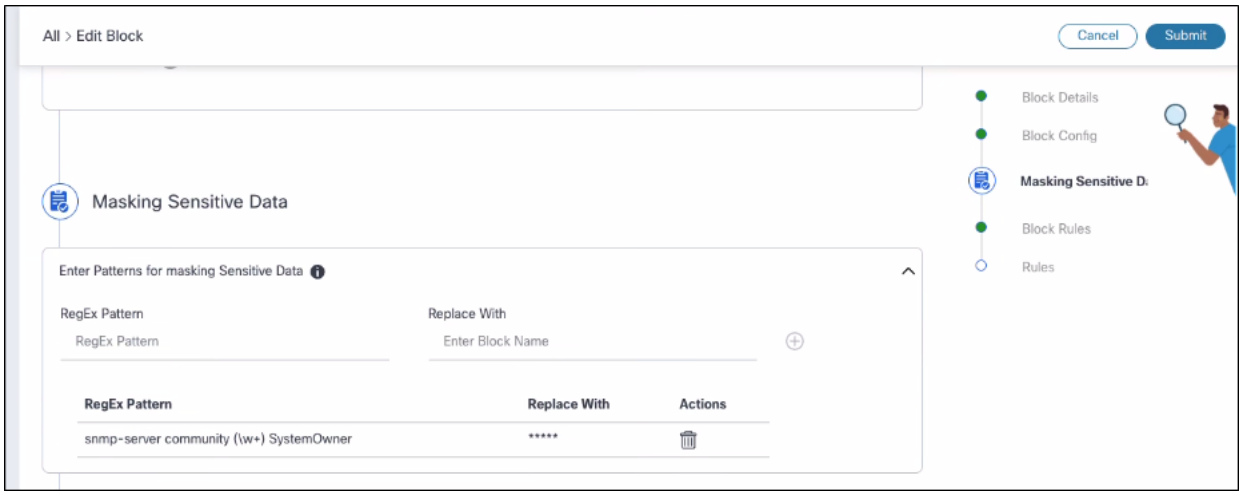
Se le righe "shutdown" (arresto) o "description config" (configurazione descrizione) sono disponibili nella configurazione del dispositivo, nella pagina del dashboard viene visualizzata una violazione. La gravità della violazione dipende dalla selezione effettuata durante la creazione della regola.

- Maschera dati sensibili:

I dati sensibili maschera sono una funzione che consente agli utenti di definire modelli utilizzando espressioni regolari per identificare e mascherare informazioni riservate (come password o chiavi) nelle configurazioni dei dispositivi. In questo modo si evita che i dati sensibili vengano visualizzati in viste delle violazioni o che la configurazione di correzione differisca sostituendo i dati corrispondenti con una maschera specifica (ad esempio, "***").

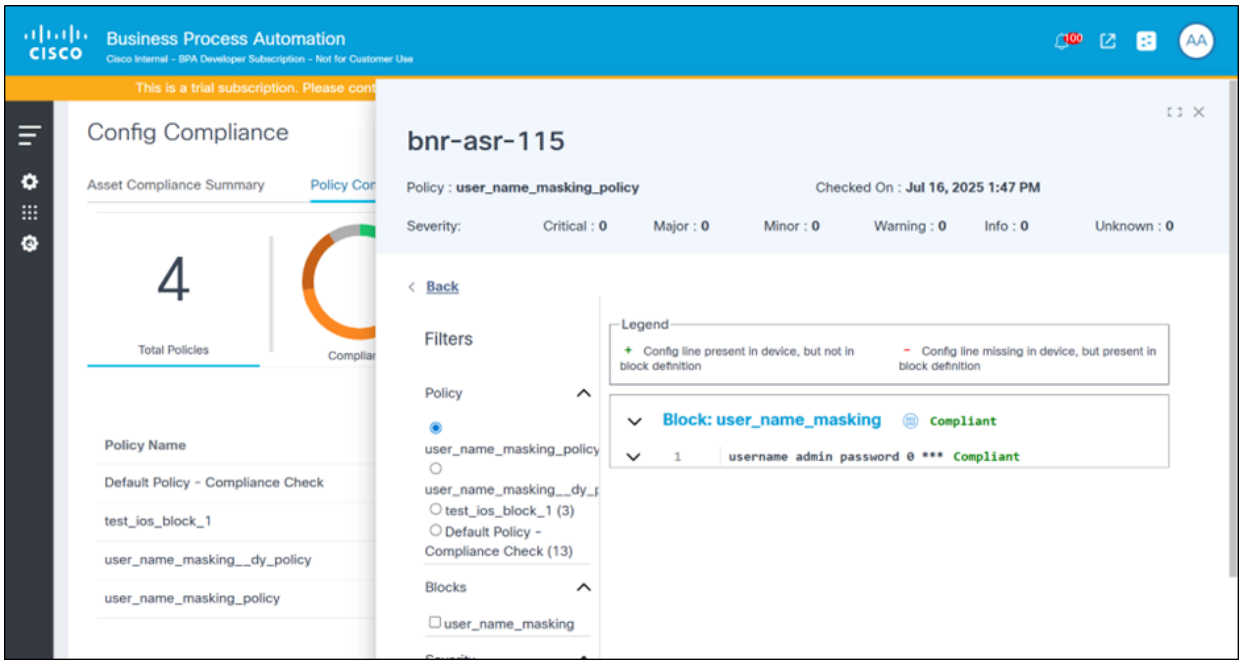
La procedura seguente illustra come mascherare i dati riservati:

1. Nella sezione Dati sensibili maschera:
    - Aggiungere più modelli di espressione regolare (regex) per identificare i dati sensibili
    - Specificare la stringa di sostituzione per mascherare i dati corrispondenti (ad esempio, "") Ad esempio, il modello Regex può essere compilato con una password (per far corrispondere qualsiasi testo che inizia con "password" seguito da una parola) e la sostituzione deve essere .
2. Aggiungere tutti i modelli regex necessari; sono visualizzati in formato griglia



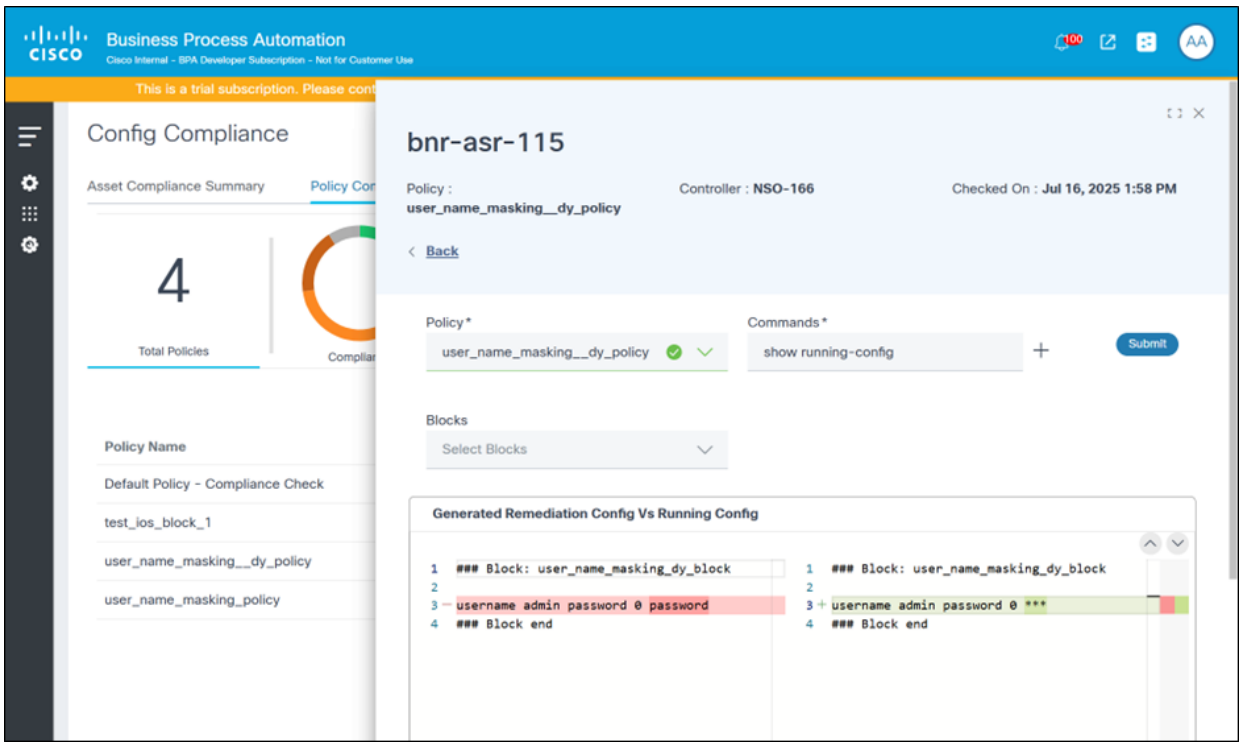
Maschera dati sensibili

3. Se non è più necessario, eliminate un pattern dall'elenco.
4. Il sistema utilizza le espressioni regolari per trovare i dati di configurazione sensibili corrispondenti e sostituirli con la maschera specificata (ad esempio, "***"). Questo mascheramento viene utilizzato nelle pagine seguenti:
    - Dashboard conformità > Asset interessati > Pagina Visualizza violazioni: I dati di configurazione visualizzati nell'interfaccia utente e il report sulla conformità degli asset generato in base ai dettagli della violazione



Maschera dati sensibili nella pagina Visualizza violazioni

- Dashboard di conformità > Visualizza configurazione di correzione > Pagina Visualizza differenze di correzione: I dati di configurazione del dispositivo visualizzano i dati sensibili mascherati in base alle impostazioni della maschera del blocco

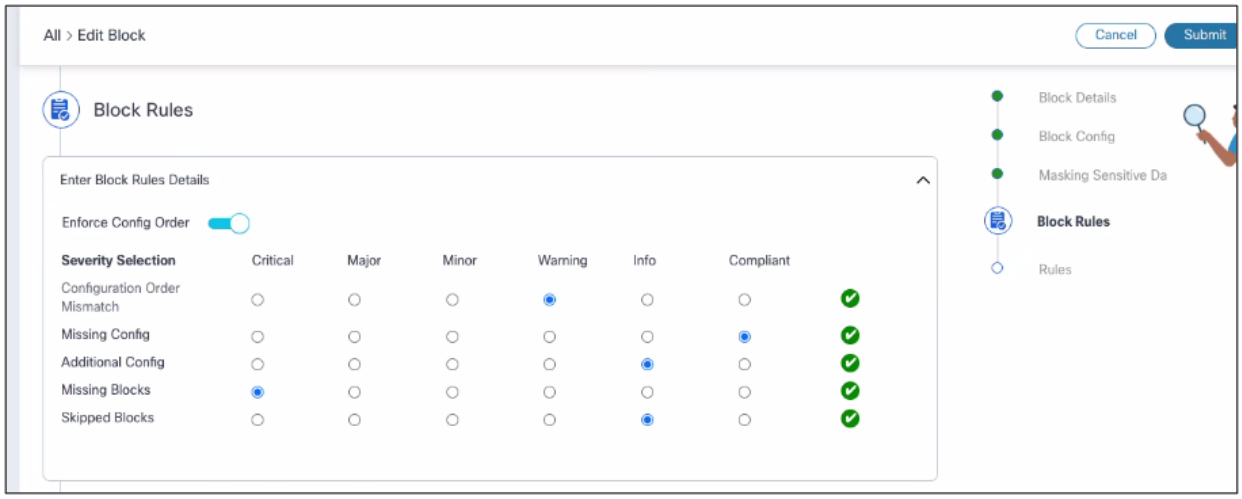


Maschera dati sensibili nella pagina diff di correzione

- Regole di blocco (selezione gravità):

  La sezione Regole di blocco include le informazioni riportate di seguito.

- Applica ordine di configurazione: Assicura che le linee di configurazione vengano visualizzate nell'ordine corretto durante i controlli di conformità. Il modulo di gestione della conformità controlla la sequenza delle linee di configurazione rispetto all'ordine previsto.
- Selezione gravità: Consente agli utenti di assegnare un livello di gravità alle violazioni all'interno di un blocco. I livelli di gravità consentono di assegnare priorità e gestire in modo efficace i problemi di conformità.
- Ordine di configurazione non corrispondente: Identifica le discrepanze nell'ordine delle linee di configurazione e avvisa quando la sequenza delle linee di configurazione del dispositivo non corrisponde all'ordine previsto.
- Configurazione mancante:
  - Rileva righe di configurazione mancanti
  - Evidenzia le righe di configurazione previste assenti nella configurazione del dispositivo
  - Controlla se l'intero blocco di configurazione del dispositivo è mancante o non corrisponde alla configurazione del blocco definita
- Configurazione aggiuntiva:
  - Identifica le righe di configurazione impreviste
  - Visualizza le righe di configurazione presenti nella configurazione del dispositivo ma non previste in base alla configurazione del blocco
- Blocchi ignorati:
  - Indica i blocchi di configurazione non controllati
  - Il blocco viene ignorato se non soddisfa le condizioni di filtro specificate



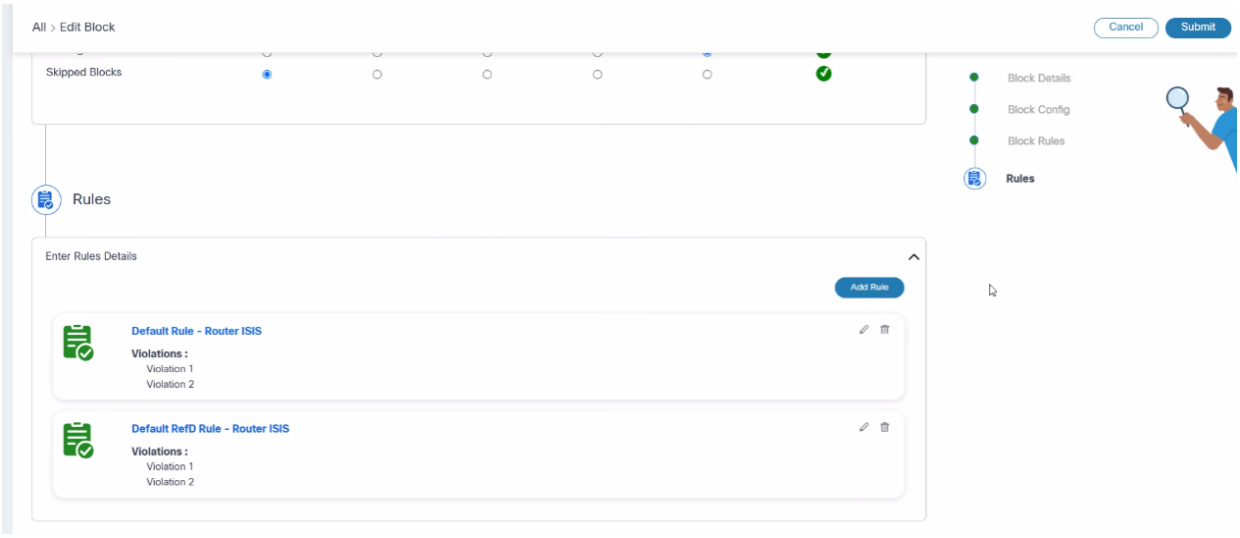
Aggiungi o modifica regole blocchi-blocchi

Gestione delle regole

Nel framework CnR, gli utenti possono gestire le regole di blocco tramite l'interfaccia "Add or Edit Blocks". Questa funzionalità è strutturata come illustrato nella sezione seguente:

Nota: Se un utente non desidera aumentare una particolare violazione a livello di blocco, è possibile selezionare il livello di gravità "Conforme".

- Configurazione regole:
  - Gli utenti possono impostare e gestire le regole utilizzate dal motore di conformità per convalidare le configurazioni
  - Gli utenti possono creare, modificare o eliminare le regole in base alle esigenze
- Elenco regole:
  - Fornisce un elenco completo di tutte le regole create, offrendo visibilità nei relativi dettagli
  - Gli utenti possono modificare le regole esistenti o eliminare quelle non più necessarie



Aggiunta e modifica dei blocchi di configurazione

Aggiunta o modifica dei dettagli delle regole

- Nome regola:
  - Assegnare un nome univoco alla regola per l'identificazione
  - Questo campo è obbligatorio per garantire il riconoscimento di ogni regola
- Regola predefinita:
  - Specificare se la regola deve essere impostata come predefinita
  - Gli utenti possono abilitare questa impostazione per impostare la regola come predefinita all'interno del framework di conformità
- Descrizione:
  - Fornisce informazioni o contesto aggiuntivi sulla regola
  - Questo campo è facoltativo, ma può essere utile per la documentazione e la chiarezza
- Violazioni:
  - Gestire l'elenco di violazioni associate alla regola
  - Gli utenti possono aggiungere, modificare o eliminare le violazioni in base alle esigenze

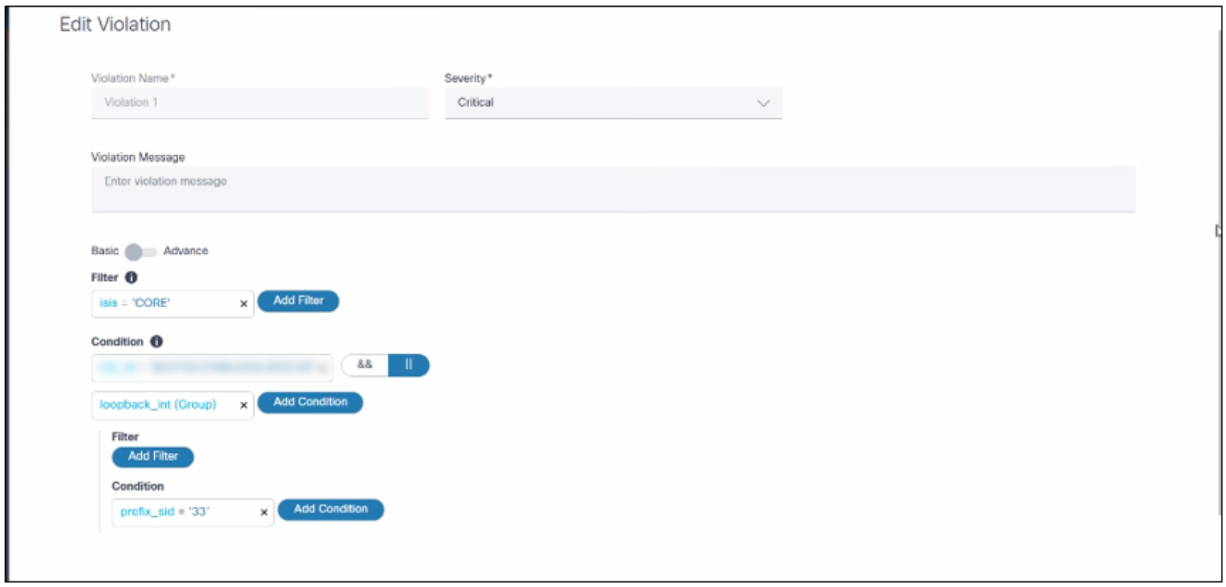
	A	B	C	D	E	F	G	H	I	J	K
1	Device Name	Managed By	Product Family	Compliance	Critical	Major	Minor	Warning	Info	Unknown	Last Checked
2	CNC-bnr-asr-78	Direct-To-Device	IE 2000 Series	Non Compliant	1	0	0	0	0	0	04-Aug-25
3	D2d-118	Direct-To-Device	IE 2000 Series	Partially Compliant	0	1	0	1	1	0	04-Aug-25
4	D2d-juniper	Direct-To-Device	juniper-junos	Partially Compliant	0	0	0	2	2	1	06-Aug-25
5	DNAC_Mock_Device0	DNAC-Mock	Cisco Catalyst 9922-CL Wireless Controller for Cloud	Unknown	0	0	0	0	0	1	05-Aug-25
6	bnr-asr-78	cnc6		Partially Compliant	0	0	1	0	0	0	05-Aug-25
7	bnr-isr-118	Direct-To-Device	cisco-ios	Partially Compliant	15	2	0	2	6	0	06-Aug-25
8	bnr-n3k-44	NSO-166	cisco Nexus9000 C9300v Chassis	Partially Compliant	12	0	0	0	3	0	05-Aug-25
9											

Aggiungi o modifica blocchi-regole: Aggiungi o modifica regola

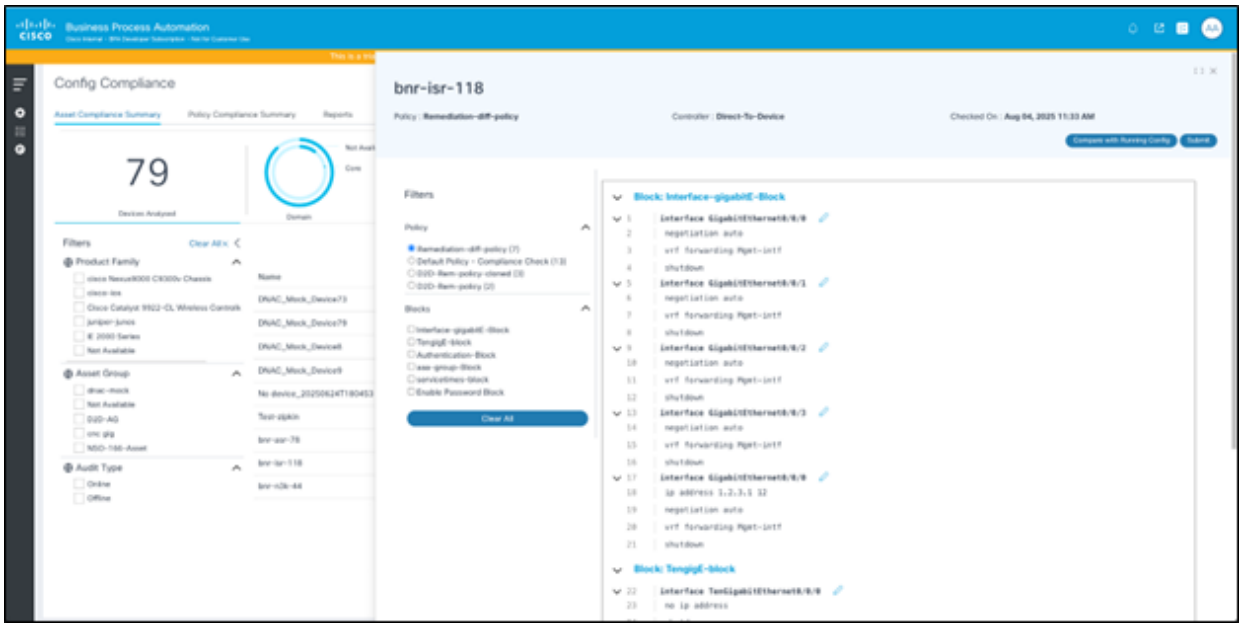
Aggiunta o modifica di violazioni di regole

Le violazioni delle regole sono un componente critico nell'esecuzione della conformità, in cui vengono descritti in dettaglio i controlli specifici da eseguire. Di seguito viene fornita una panoramica della modalità di creazione e gestione delle violazioni delle regole:

- Modalità di base:
  - Elementi interfaccia utente: Questa modalità consente agli utenti di creare violazioni delle regole utilizzando un'interfaccia grafica (GUI). Questo approccio è in genere più semplice da utilizzare e accessibile per coloro che preferiscono non utilizzare la codifica.
  - Guida dettagliata: Gli utenti vengono guidati nel processo di definizione dei controlli utilizzando elementi dell'interfaccia utente predefiniti.
- Modalità avanzata:
  - Formato di codice simile a JSON: Per gli utenti che hanno familiarità con la codifica, questa modalità consente la creazione di violazioni delle regole digitandole in un formato strutturato simile a JSON.
  - Flessibilità e precisione: Questo metodo offre maggiore flessibilità e precisione per la definizione di controlli di regole complesse.



Crea o modifica violazioni regole - Modalità di base



Crea o modifica violazioni regole - Modalità avanzata

Le violazioni delle regole sono suddivise nelle sezioni seguenti:

- Nome violazione: Nome della violazione
- Gravità: Definisce la gravità della conformità se la violazione non riesce durante un'esecuzione
- Messaggio di violazione: Il messaggio viene visualizzato quando un controllo delle violazioni ha esito negativo
- Criteri filtro violazioni: Applica le condizioni di violazione in cui è possibile utilizzare variabili dello schema non di gruppo
  - Utilizzato nei criteri di filtro per impostare condizioni basate su singoli elementi dati che non fanno parte di un gruppo
  - Consente agli utenti di selezionare i criteri in base alla gerarchia e alla struttura dei dati, garantendo un filtraggio preciso e pertinente
- Condizioni delle regole: Condizioni effettive per il controllo della conformità in cui è possibile utilizzare le variabili di schema di gruppo e non di gruppo
  - Entrambi i tipi di variabili vengono utilizzati nelle regole per creare condizioni complete
  - Variabili gruppo: Consentire l'applicazione di condizioni alle raccolte di dati correlati, garantendo controlli approfonditi all'interno di gruppi strutturati
  - Variabili non di gruppo: Consentire l'applicazione di condizioni agli elementi di dati indipendenti, garantendo flessibilità nell'applicazione delle regole

Blocchi dinamici definiti dall'utente - Procedure ottimali

- Assicurarsi che i nomi delle variabili siano univoci all'interno di ogni blocco.
- Evitare di utilizzare variabili nei nomi dei gruppi.
- Per le configurazioni delle gerarchie secondarie, utilizzare "<group>" nei blocchi.

Esempio:
https://ttp.readthedocs.io/en/latest/Writing%20templates/How%20to%20parse%20hierarchical%20(config
to-parse-hierarchical-configuration-data

- Per acquisire i valori per linee di configurazione simili in una singola variabile, utilizzare la variabile come indicato di seguito: `{{<nome-var>> | riga | joinmatch(',') }}`. Racchiudere la riga di configurazione tra `{{ start }}` e `{{ end }}`, come illustrato nell'esempio seguente:

Configurazione dispositivo	Configurazione blocco
ip domain list vrf Mgmt-intf core.cisco.com	{{_start_}}
elenco dei domini ip cisco.com	ip domain list {{ domini | _linea_ | joinmatch(‘,’) }}
elenco dei domini ip east.cisco.com	{{ _end_ }}
elenco dei domini ip west.cisco.com	ip domain list vrf {{ vrf_name }} {{ vrf_domain }}

- Per acquisire un valore che contiene spazi da una riga di configurazione, utilizzare la variabile nel blocco come illustrato nella tabella riportata di seguito. `{{<nome-var>> | re(".*") }}`

Configurazione dispositivo	Configurazione blocco
interface HcentoGigE0/0/1/31	interface {{ INTF_ID }}
description Interfaccia: 12yala01 Hg0/0/1/31	descrizione {{ INTF_DESC | re(".*") }}
mtu 9216	mtu 9216

Informazioni sull'integrazione di gerarchie di regole e RefD nelle regole e nelle regole non RefD

Nel protocollo TTP a blocchi dinamico sono disponibili due schemi distinti che determinano il modo in cui le configurazioni vengono strutturate e convalidate.

- Schema basato su gruppi:
  - Questo schema organizza le configurazioni in modo gerarchico, stabilendo una relazione padre-figlio tra gli elementi
  - Ideale per configurazioni complesse in cui gli elementi sono nidificati logicamente e interconnessi

    - È possibile definire regole per convalidare le relazioni gerarchiche e le dipendenze tra i diversi elementi di configurazione
- Schema non basato su gruppi:
    - Le configurazioni sono strutturate in un formato piatto, con tutti gli elementi esistenti allo stesso livello senza relazioni gerarchiche
    - Ideale per configurazioni più semplici in cui non è necessaria una gerarchia
    - È possibile impostare regole per garantire che ogni elemento di configurazione soddisfi criteri specifici

Integrazione RefD

- Scopo del riferimento:
    - Ruolo: Funge da strumento per la gestione di variabili locali ed esterne all'interno del framework BPA
    - Funzionalità:
        - Recupero dinamico: Facilita il recupero e la gestione dinamici dei dati variabili, consentendo ai controlli di conformità di adattarsi alle modifiche dei dati in tempo reale
        - Interazione API: Offre API per casi di utilizzo BPA per l'accesso e la gestione di queste variabili e valori dinamici, garantendo una facile integrazione nei workflow di conformità

Sintassi dei valori delle regole di conformità

Lo Use Case CnR si integra con la struttura RefD per utilizzare in modo dinamico i dati all'interno dei controlli di conformità e dei workflow di correzione. Di seguito è riportata una descrizione dettagliata del funzionamento di tale integrazione, con particolare riguardo alla sintassi e ai tipi di variabili utilizzati:

- Parola chiave: La sintassi deve iniziare con "RefD"
- Parametri: Il parametro "key" è obbligatorio nella sintassi
- Esempio:

```
plaintext
Copy Code
RefD:ns={$SITE}&key={{#device.deviceIdentifier}}.interfaces.MgmtEth{{ INT_ID }}.ipv4_addr
```

Tipi di variabili

- Variabili definite dall'utente:

    - Configurato durante la creazione dei processi di conformità.
    - Ambito: Applicabile a tutte le esecuzioni per il job specificato
    - Sintassi: `{$VarName}`
    - Esempio: `{$SITE}`
- Variabili di sistema
    - Predefinito dal framework in base ai dati di contesto disponibili durante l'esecuzione
    - Attualmente, il framework fornisce l'accesso all'oggetto dispositivo
    - Sintassi: `{{#VarName}}`
    - Esempi:
        - `{{#device.deviceIdentifier}}` - Rappresenta l'identificatore del dispositivo
        - `{{#device.additionalAttributes.serialNumber}}` - Rappresenta il numero di serie del dispositivo
- Variabili TTP
    - Presente nella configurazione di blocco
    - Sintassi: `{{ NomeVar }}`
    - Esempio: `{{ INT_ID }}`

Regole non RefD

- Queste regole sono simili alle regole RefD, ma non iniziano con la parola chiave "RefD"
- Esempio:

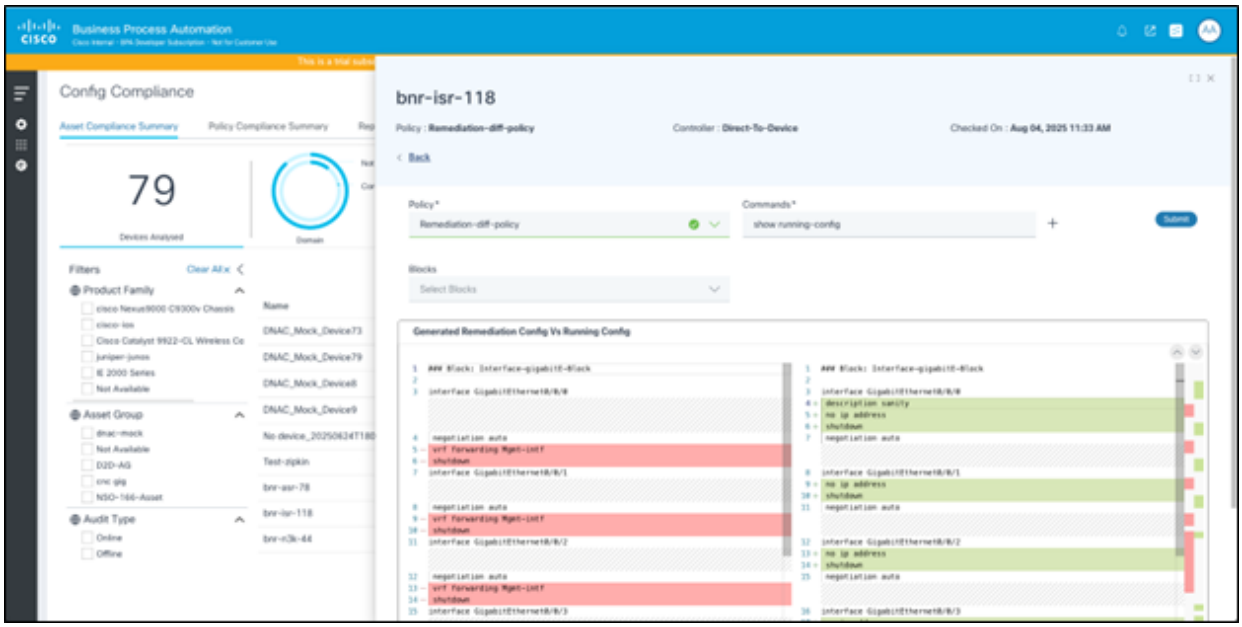
```
plaintext
Copy Code
{$int_id}.{{#device}}.{{ mtu_val }}
```

Utilizzo variabili

- Variabili definite dall'utente: Rappresentato come `{$Var}`
- Variabili di sistema: Rappresentato come `{#Var}}`, espone attributi come deviceIdentifier, controllerId, controllerType, ecc.
- Variabili TTP: Rappresentato tra parentesi graffe doppie come `{{var}}`

Esecuzione

- Durante la creazione del processo, è possibile impostare i relativi valori se vengono specificate variabili $
- I valori combinati delle variabili vengono confrontati con la configurazione del dispositivo recuperato per garantire la conformità



Configurazione dispositivo

	A	B	C	D	E	F
1	Policy Name	Fully Compliant	Partially Compliant	Non Compliant	Unknown	Total Assets
2	D2D-Juniper-policy	0	1	0	0	1
3	D2D-Raiseviolation-policy	0	1	0	0	1
4	D2D-Rem-policy	0	1	0	2	3
5	D2D-Rem-policy-cloned	0	1	0	0	1
6	Default Policy - Compliance Check	0	2	0	70	72
7	Policy Delete Issue	1	0	0	0	1
8	Policy Test	1	0	0	0	1
9	Remediation-diff-policy	0	1	0	0	1
10	cnc gig policy	0	1	0	0	1
11	cnc gigabit	0	2	1	1	4
12						

Regole di configurazione: Rif.

Visualizzazione dei dettagli dei blocchi

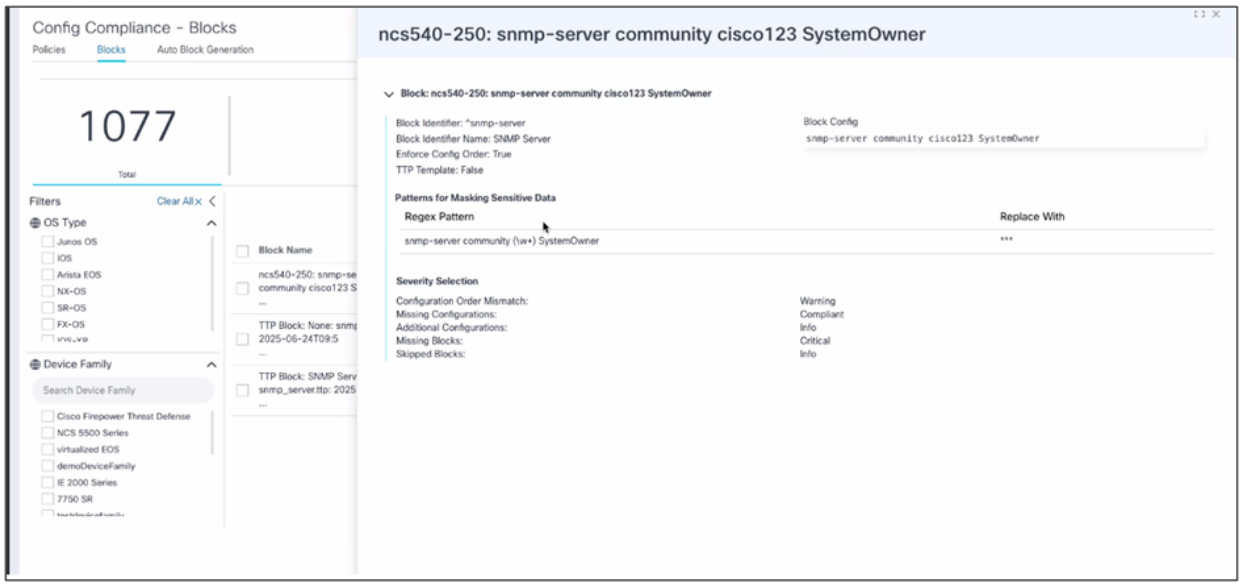
Per accedere ai dettagli dei blocchi:

1. Passare alla pagina Blocchi.
2. Selezionare o fare clic sulla riga nella griglia per visualizzare i dettagli del blocco specifico. Nella parte destra della schermata viene visualizzata la pagina Dettagli blocco.

Nota: Questa pagina fornisce una visualizzazione di sola lettura di tutte le informazioni correlate al blocco, inclusi i blocchi associati, le regole e le eventuali violazioni.

Facendo clic sui collegamenti ipertestuali, se presenti, all'interno dei dettagli gli utenti vengono

reindirizzati al blocco pertinente o alle informazioni correlate.



Visualizzazione dettagli blocco

Eliminazione di blocchi

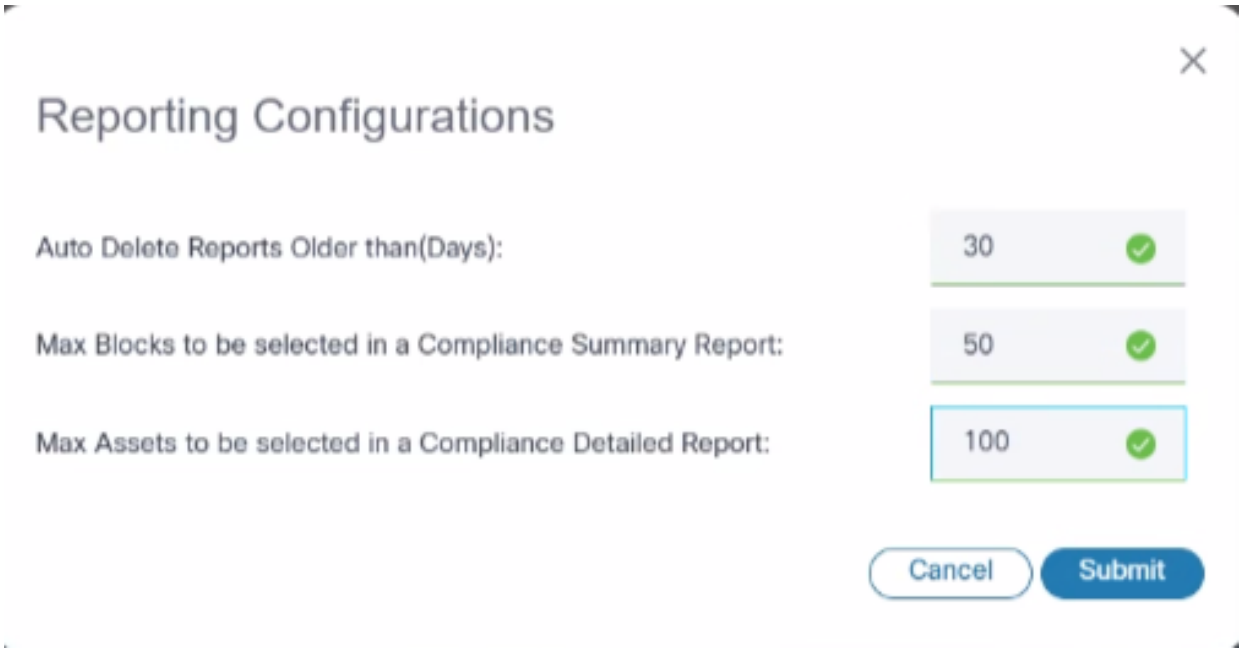
Il portale consente agli utenti di eliminare uno o più blocchi, purché dispongano delle autorizzazioni RBAC appropriate. Gli utenti possono eseguire queste operazioni eseguendo le operazioni riportate di seguito.

Per l'eliminazione di blocchi singoli:

1. Passare alla pagina Blocchi.
2. Fare clic sull'icona Altre opzioni accanto al blocco da eliminare.
3. Selezionare l'opzione Elimina. Viene visualizzato un messaggio di conferma.

Per l'eliminazione di più blocchi:

1. Passare alla pagina Blocchi.
2. Selezionare le caselle di controllo accanto a ogni blocco da eliminare.
3. Fare clic sull'icona Altre opzioni e selezionare Elimina. Un messaggio di conferma.

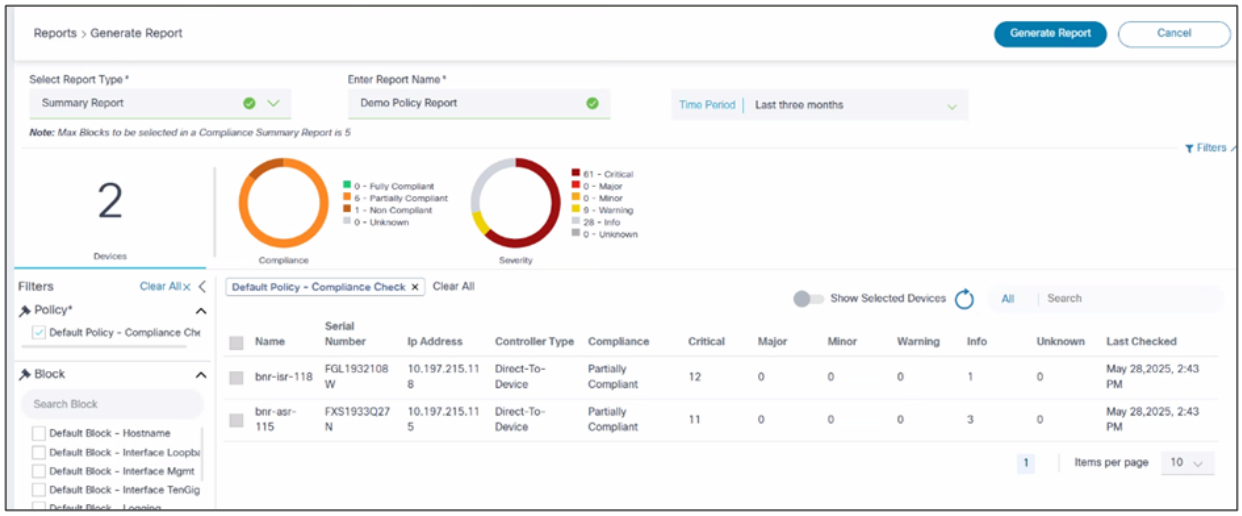


Elimina blocco

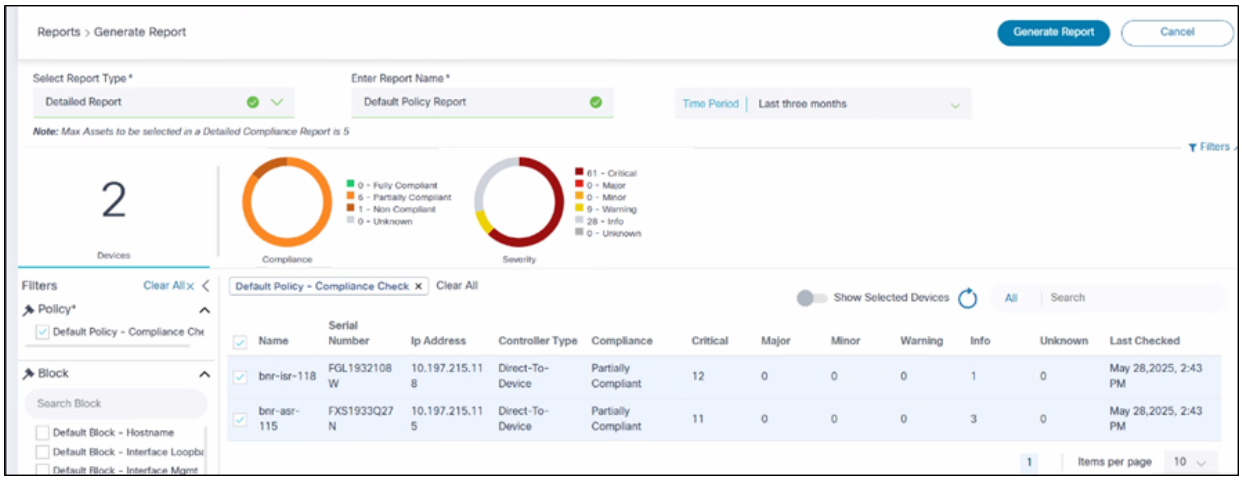
Configurazione: Generazione automatica blocchi

La generazione dei blocchi consente agli utenti di creare automaticamente i blocchi in base alla configurazione di un dispositivo. Questa automazione riduce il tempo e l'impegno necessari per la creazione manuale e semplifica la modifica dei blocchi da parte degli utenti tramite l'aggiunta o la rimozione di variabili anziché partendo da zero.

Fare clic su una riga per visualizzare i dettagli di generazione dei blocchi.

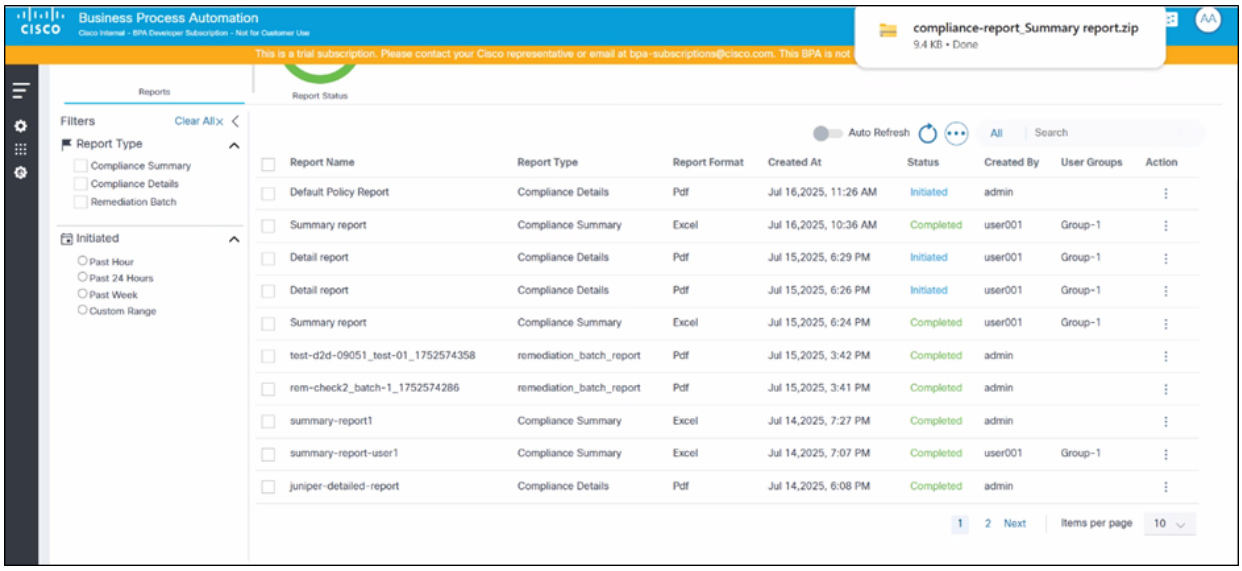


Elenco generazione blocchi automatica - Visualizza



Dettagli generazione blocco automatico

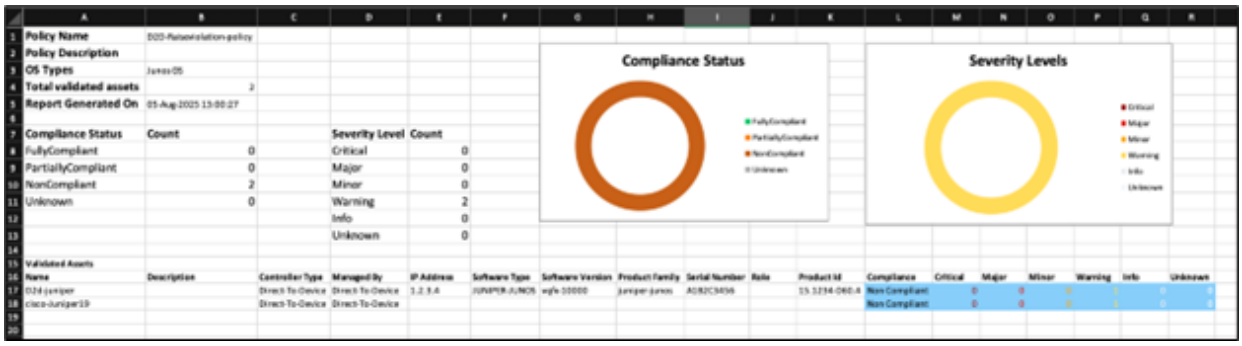
Generazione automatica blocchi



Elenco di generazione blocco automatico

La pagina Generazione automatica blocchi include i campi riportati di seguito.

- Genera da: Origine da cui vengono generati i blocchi. Sono disponibili le tre opzioni seguenti:
  - Backup configurazione dispositivo: Il sistema sceglie una configurazione di dispositivo dal caso di utilizzo del backup



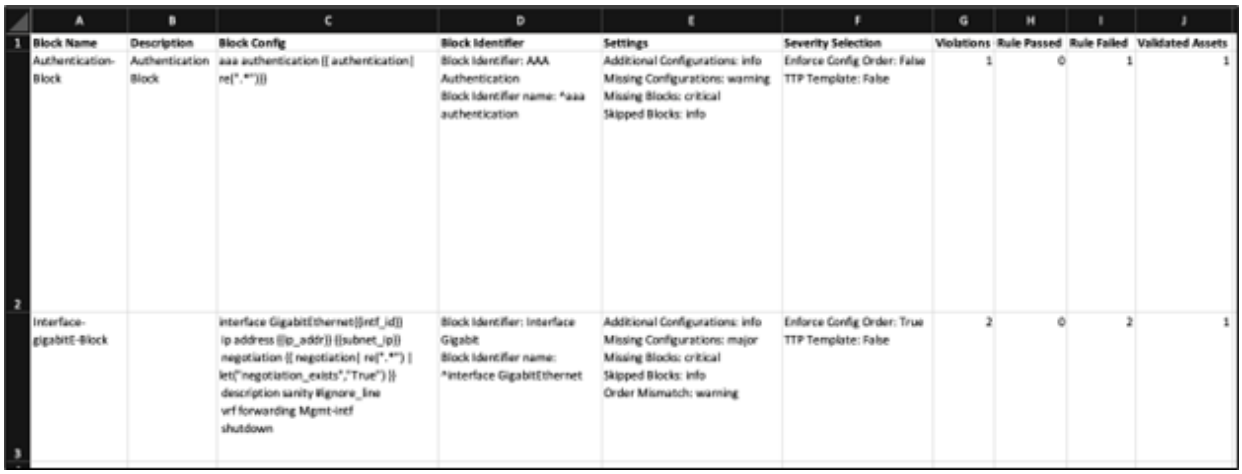
1	Policy Name	D20-Rulevalidation-policy																
2	Policy Description																	
3	OS Types	Junos OS																
4	Total validated assets	2																
5	Report Generated On	05-Aug-2025 13:00:27																
6																		
7	Compliance Status	Count		Severity Level	Count													
8	FullyCompliant	0		Critical	0													
9	PartiallyCompliant	0		Major	0													
10	NonCompliant	2		Minor	0													
11	Unknown	0		Warning	2													
12				Info	0													
13				Unknown	0													
14																		
15	Validated Assets																	
16	Name	Description	Controller Type	Managed By	IP Address	Software Type	Software Version	Product Family	Serial Number	Role	Product Id	Compliance	Critical	Major	Minor	Warning	Info	Unknown
17	D24-juniper		Direct-To-Device	Direct-To-Device	1.2.3.4	JUNIPER-JUNOS	vqfx-10000	juniper-junos	AD82C5456		15-1234-040-4	Non Compliant	0	0	0	1	0	0
18	cisco-juniper19		Direct-To-Device	Direct-To-Device								Non Compliant	0	0	0	1	0	0
19																		
20																		

Compliance Status

Severity Levels

Backup configurazione dispositivo

- Caricamento file: Viene visualizzata una finestra di caricamento file in cui gli utenti possono caricare la configurazione del dispositivo



	A	B	C	D	E	F	G	H	I	J
1	Block Name	Description	Block Config	Block Identifier	Settings	Severity Selection	Violations	Rule Passed	Rule Failed	Validated Assets
2	Authentication-Block	Authentication Block	aaa authentication {{ authentication| re(".*")}}	Block Identifier: AAA Authentication Block Identifier name: ^aaa authentication	Additional Configurations: info Missing Configurations: warning Missing Blocks: critical Skipped Blocks: info	Enforce Config Order: False TTP Template: False	1	0	1	1
3	Interface-gigabitE-Block		interface GigabitEthernet{{intf_id}} ip address {{ip_addr}} {{subnet_ip}} negotiation {{ negotiation| re(".*") | let("negotiation_exists","True") }} description sanity ignore_line vrf forwarding Mgmt-intf shutdown	Block Identifier: Interface Gigabit Block Identifier name: ^interface GigabitEthernet	Additional Configurations: info Missing Configurations: major Missing Blocks: critical Skipped Blocks: info Order Mismatch: warning	Enforce Config Order: True TTP Template: False	2	0	2	1

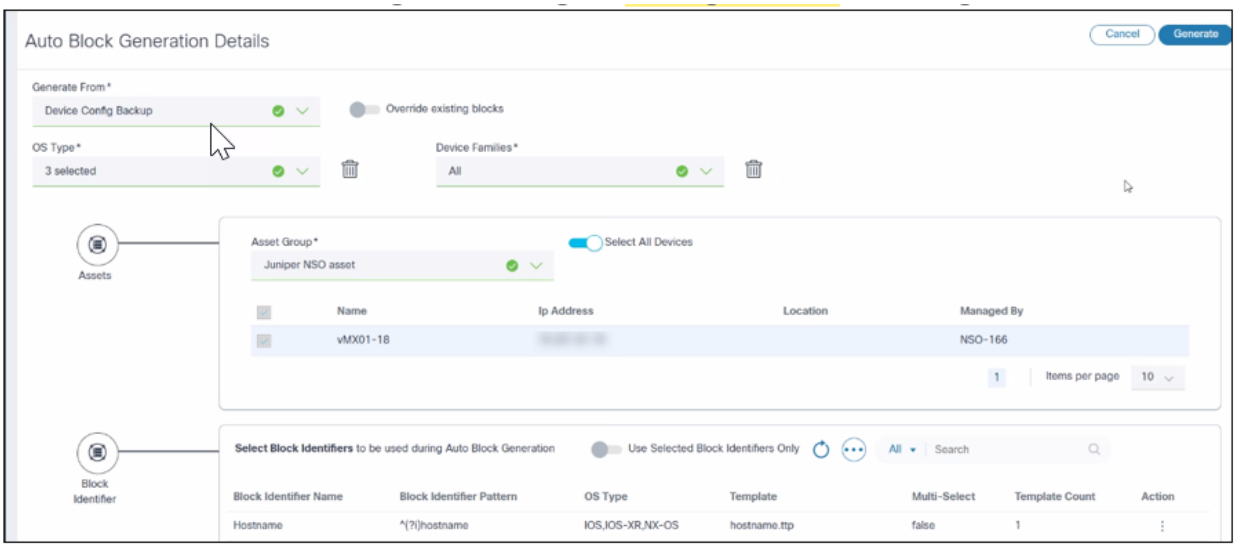
Caricamento file

- Configurazione corrente: Immettere il comando di configurazione CLI usato dal sistema per recuperare la configurazione del dispositivo.

	A	B	C	D	E	F	G
1	Rule Name	Rule Description	Violation Name	Description	Severity	Violation Count	Affected Assets Count
2	Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	DescriptionCheck		warning	5	3
3	Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	IP-Address-Validation		critical	6	2
4	Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	No-Shutdown-check		compliant	0	0
5							
6							
7	Rule Name	Violation Name	Severity	Device Name	Managed By		
8	Gigabit Rule	DescriptionCheck	warning	bnr-isr-118	Direct-To-Device		
9	Gigabit Rule	DescriptionCheck	warning	bnr-isr-119	Direct-To-Device		
10	Gigabit Rule	DescriptionCheck	warning	bnr-isr-121	Direct-To-Device		
11	Gigabit Rule	IP-Address-Validation	critical	bnr-isr-118	Direct-To-Device		
12	Gigabit Rule	IP-Address-Validation	critical	bnr-isr-120	Direct-To-Device		
13							

Configurazione corrente

- Tipo di sistema operativo: Elenco dei tipi di sistemi operativi per i quali il blocco è rilevante.
- Famiglia di dispositivi: Elenco di famiglie di dispositivi per cui il blocco è rilevante.
- Risorse: La funzione Assets fornisce un approccio strutturato per selezionare i dispositivi per la generazione di blocchi dinamici
    - Selezione gruppo cespite:
        - Consente agli utenti di scegliere un gruppo predefinito di dispositivi, noto come gruppo di risorse, utilizzato per generare blocchi dinamici
        - Semplifica la gestione e l'organizzazione dei dispositivi raggruppandoli in base a criteri specifici, ad esempio la posizione, il tipo o la funzione
    - Selezione sottoinsieme di dispositivi:
        - Gli utenti hanno la flessibilità di selezionare un sottoinsieme specifico di dispositivi all'interno del gruppo asset scelto
        - Consente agli utenti di concentrarsi su un particolare segmento di dispositivi, consentendo la generazione e la gestione di blocchi più mirati



Generazione blocco

- Identificatore blocco: Consente agli utenti di selezionare l'elenco di identificatori di blocco utilizzati durante la generazione del blocco. Fornisce inoltre funzionalità di gestione degli identificatori di blocco in linea.

Identificatore blocco

Un identificatore di blocco utilizza CiscoConfParser per estrarre un blocco di configurazione dall'intera configurazione del dispositivo. Ogni identificatore di blocco deve essere associato a un modello regex. Gli utenti possono creare i propri identificativi di blocco o aggiornare gli identificativi di blocco esistenti utilizzando l'interfaccia utente o l'API. Attualmente la piattaforma fornisce circa 55-60 identificatori di blocco predefiniti. Ogni identificatore è univoco per un tipo di sistema operativo e viene caricato durante la distribuzione dell'applicazione BPA tramite il servizio Ingester. È possibile associare un modello TTP a ciascun identificatore di blocco. Il nome e il

modello di un identificatore di blocco devono essere univoci.

Se l'opzione Multi è abilitata per l'identificativo di blocco, il framework di conformità genera più blocchi di configurazione dalle configurazioni corrispondenti. In caso contrario, considera tutte le configurazioni corrispondenti come un unico blocco.

Esempi di identificatori di blocco con l'opzione Multi True: interface, router bgp, vrf, l2vpn, ecc.

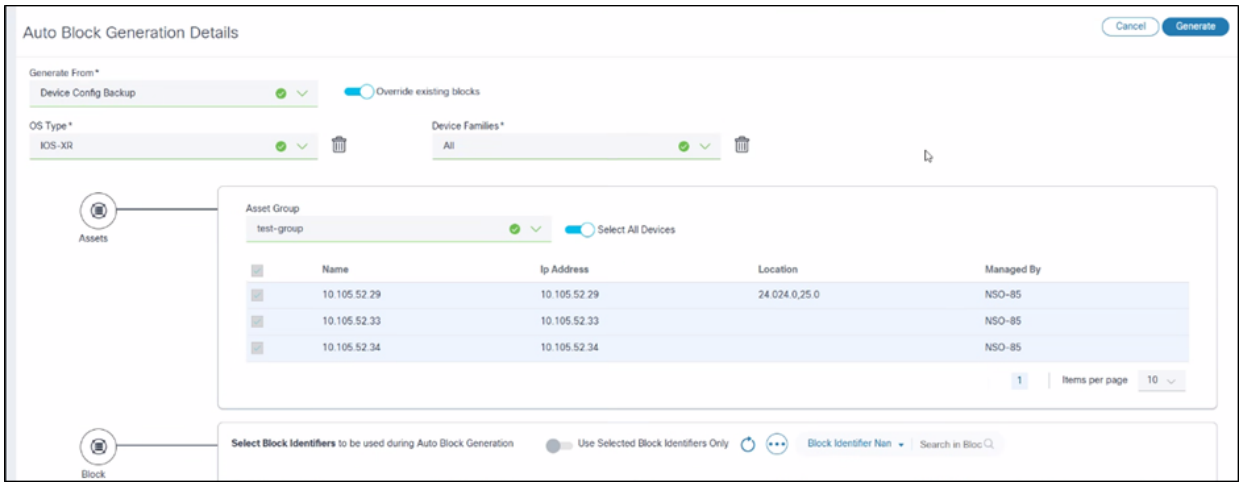
Esempi di identificatori di blocco con l'opzione Multi False: logging, snmp-server, domain, ecc.

Esempi:

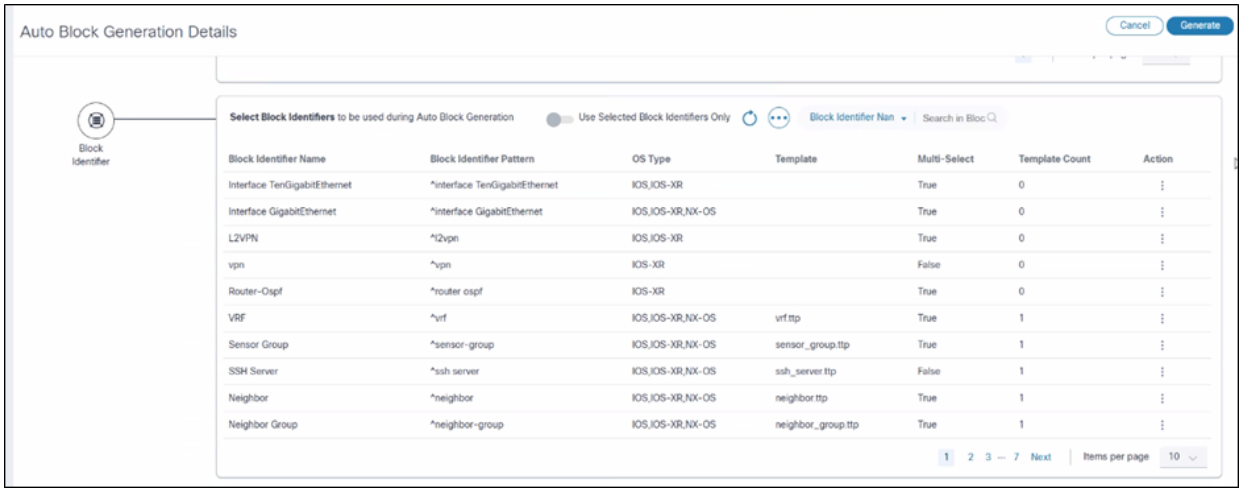
```
{
  “name”: “BundleEthernet Interface”,
  “osType”: [“IOS”, “IOS-XR”, “NX-OS”],
  “multi”: true,
  “blockIdentifier”: “^(?i)interface Bundle-Ether”,
  “templates”: [“parent_interface.ttp”]
}

{
  “name”: “Loopback Interface”,
  “osType”: [“IOS”, “IOS-XR”, “NX-OS”],
  “multi”: true,
  “blockIdentifier”: “^(?i)interface Loopback”,
  “templates”: [“parent_interface.ttp”]
}
```

Identificatore blocco elenco

Elenca identificatore di blocco consente agli utenti di visualizzare l'elenco degli identificatori di blocco insieme alle funzioni di ricerca e ordinamento. Questa funzione è disponibile nella pagina Genera blocchi.

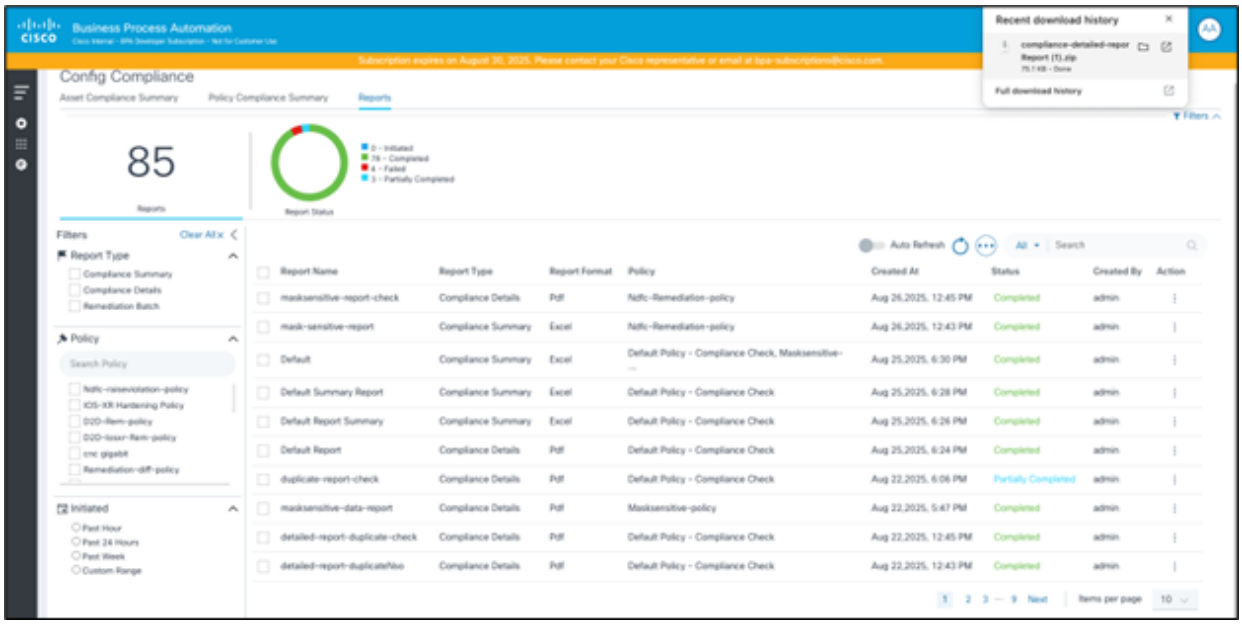


Elenco identificatori di blocco



Identificatore blocco

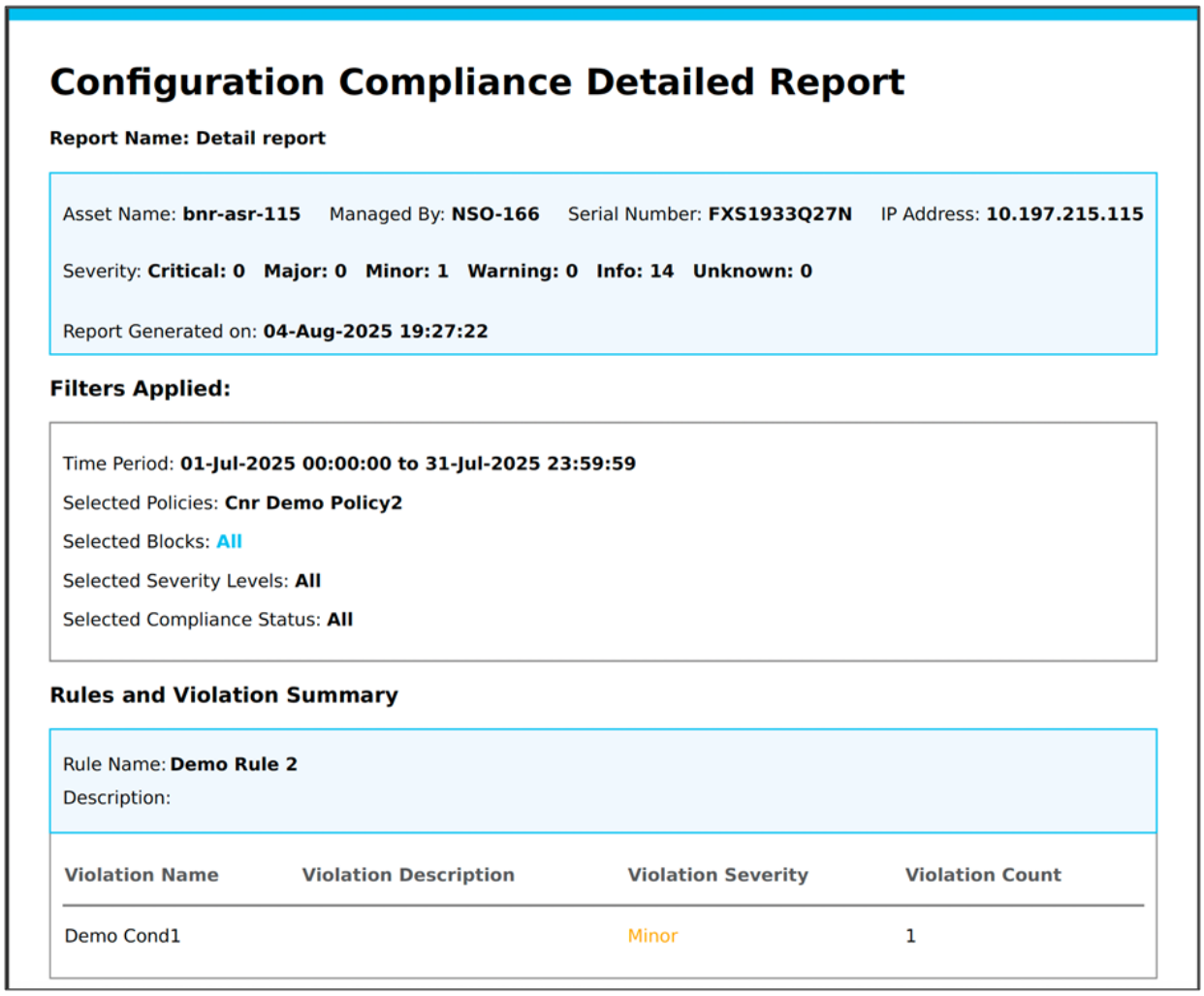
Crea o modifica identificatore di blocco



Modifica identificatore blocco

La sezione Elenco identificatori di blocco della pagina Generazione automatica blocchi fornisce agli utenti gli strumenti per gestire in modo efficace gli identificatori di blocco. Le funzionalità sono elencate di seguito:

- Crea identificatori di blocco
  - Gli utenti possono aggiungere nuovi identificatori di blocco all'elenco
  - Ciò consente l'introduzione di identificatori univoci utilizzabili per organizzare e differenziare i blocchi
- Modifica identificatori di blocco
  - È possibile modificare gli identificatori di blocco esistenti
  - Abilita gli aggiornamenti o le correzioni degli identificatori, garantendo che siano accurati e pertinenti ai blocchi che rappresentano
- Elimina identificatore di blocco
  - Gli utenti hanno la possibilità di rimuovere gli identificatori di blocco dall'elenco
  - Facilita la gestione degli identificatori consentendo la rimozione di quelli non più necessari o applicabili



Configuration Compliance Detailed Report

Report Name: Detail report

Asset Name: **bnr-asr-115** Managed By: **NSO-166** Serial Number: **FXS1933Q27N** IP Address: **10.197.215.115**

Severity: **Critical: 0** **Major: 0** **Minor: 1** **Warning: 0** **Info: 14** **Unknown: 0**

Report Generated on: **04-Aug-2025 19:27:22**

Filters Applied:

Time Period: **01-Jul-2025 00:00:00 to 31-Jul-2025 23:59:59**

Selected Policies: **Cnr Demo Policy2**

Selected Blocks: **All**

Selected Severity Levels: **All**

Selected Compliance Status: **All**

Rules and Violation Summary

Rule Name: **Demo Rule 2**

Description:

Violation Name	Violation Description	Violation Severity	Violation Count
Demo Cond1		Minor	1

Elimina identificatore di blocco

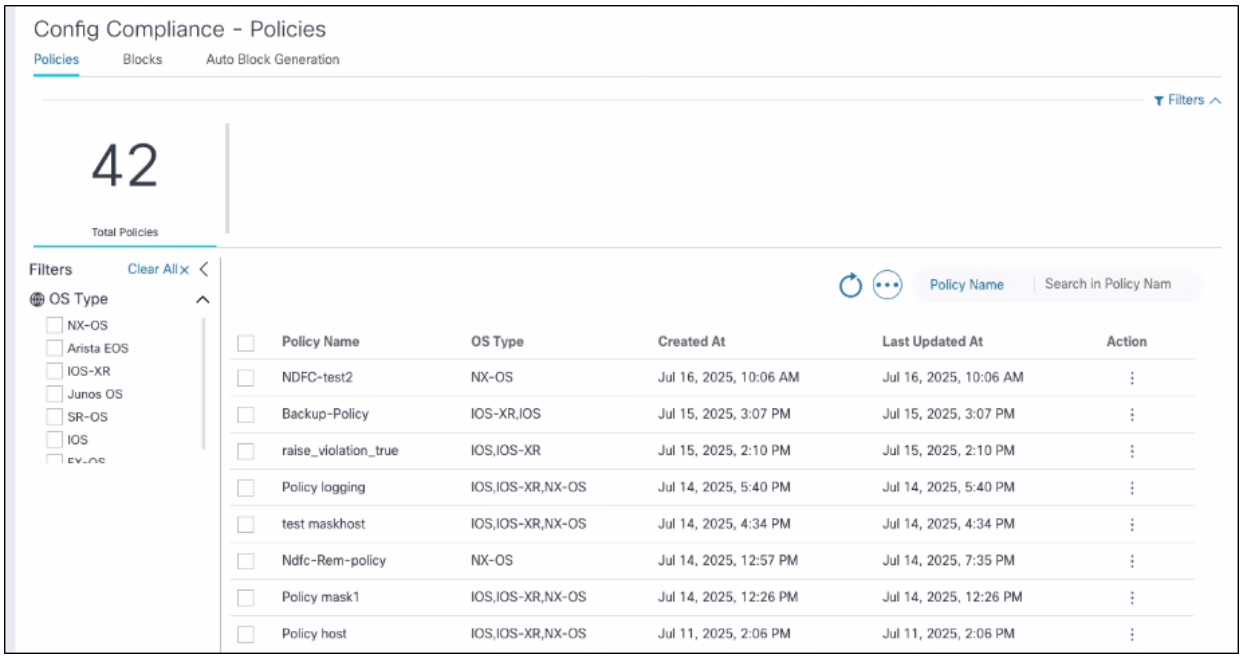
Configurazione: Politiche

Nella scheda Criteri è possibile definire un set di criteri, regole e blocchi per consentire l'esecuzione della conformità. Un criterio è un modello definito dall'utente costituito da blocchi e regole di configurazione. È possibile selezionare un elenco di blocchi di configurazione e un elenco di regole per ogni blocco di configurazione per la creazione di un criterio.

Elenca criteri

Nella scheda Criteri è possibile visualizzare un elenco di criteri che include anche azioni per l'aggiunta, la modifica, l'eliminazione, l'importazione e l'esportazione di criteri.

Nota: I criteri vengono importati o esportati insieme ai blocchi e alle regole correlati.



Elenca criteri

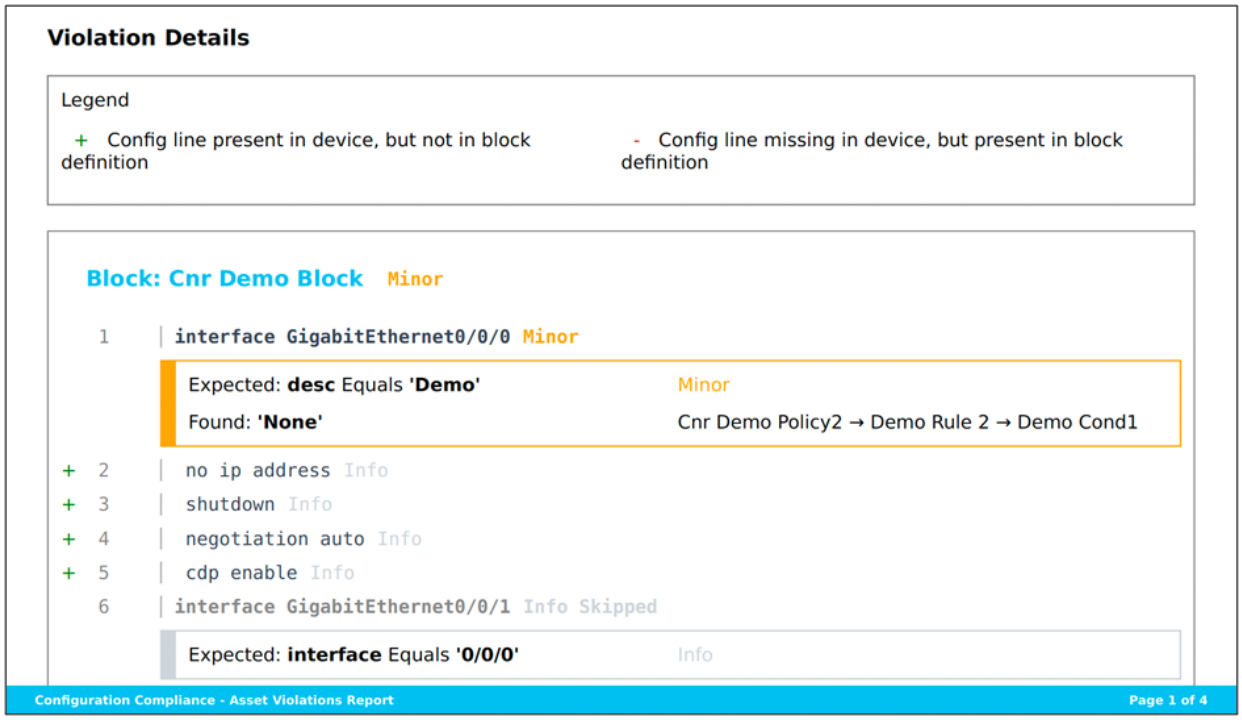
Aggiunta e modifica di criteri

Questa sezione descrive la pagina Aggiungi criterio e Modifica criterio:

Dettagli criteri

- Nome criterio: Nome del criterio
- Tipo di sistema operativo: Elenco dei tipi di sistemi operativi supportati per questo criterio
- Famiglia di dispositivi: Elenco di famiglie di dispositivi supportate per questo criterio
- Descrizione criterio (facoltativa): Descrive il criterio con una breve descrizione

I campi Tipo di sistema operativo e Famiglia di dispositivi vengono popolati automaticamente in base ai blocchi selezionati nella sezione successiva.



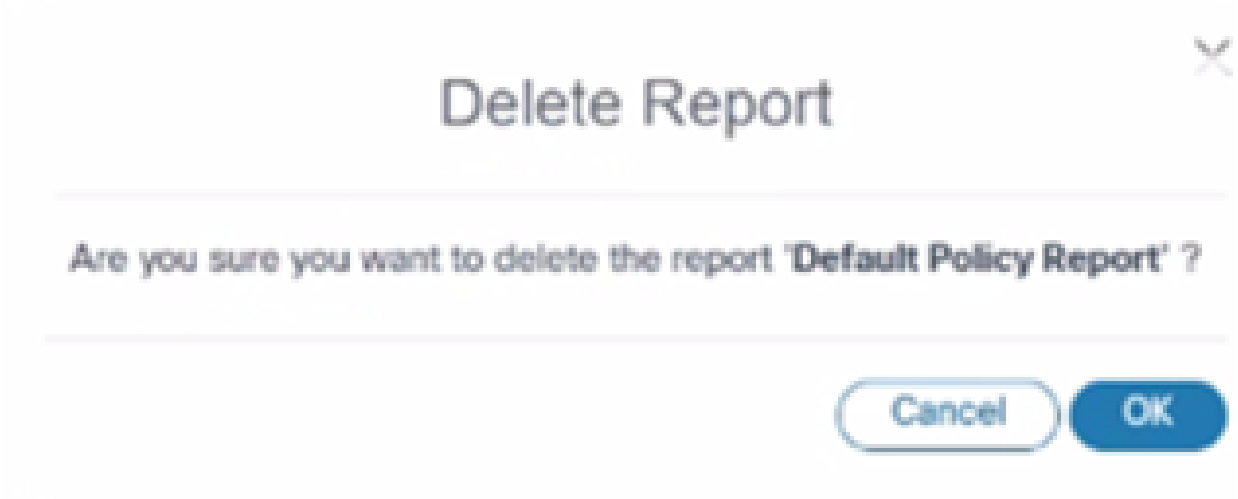
Criteri di configurazione: Dettagli criteri

Finestra di dialogo Seleziona blocchi

La funzione "Select Blocks" (Seleziona blocchi) è un'interfaccia intuitiva progettata per assistere gli utenti nella scelta dei blocchi di configurazione da includere in una regola. Le sue funzionalità sono elencate nella presente sezione:

- Finestra di dialogo popup
  - Scopo: Offre agli utenti uno spazio dedicato per la selezione dei blocchi di configurazione senza uscire dalla pagina corrente
  - Interazione utente: Assicura un processo di selezione intuitivo presentando le opzioni in una finestra di dialogo separata e focalizzata
- Aggiungi e seleziona opzioni
  - Selezioni multiple: Gli utenti possono scegliere uno o più blocchi di configurazione da includere in un criterio
  - Flessibilità: Supporta l'inclusione di diversi blocchi in base ai requisiti specifici dell'utente
- Funzionalità di navigazione
  - Filtri: Consente agli utenti di restringere l'elenco dei blocchi disponibili in base a criteri specifici, facilitando la ricerca dei blocchi rilevanti
  - Impaginazione: Organizza i blocchi in pagine gestibili, migliorando la navigazione attraverso grandi set di dati
  - Funzionalità di ricerca: Consente di individuare rapidamente i blocchi in base al nome

o ad altri identificatori, semplificando il processo di selezione



Selezione blocco

Gli utenti possono creare nuovi blocchi facendo clic su Crea nella sezione Selezione blocco. Una nuova scheda del browser viene avviata in modalità incrociata e gli utenti possono creare un nuovo blocco. Una volta inviato, gli utenti possono tornare alla scheda originale e selezionare il nuovo blocco creato per aggiungerlo al criterio.

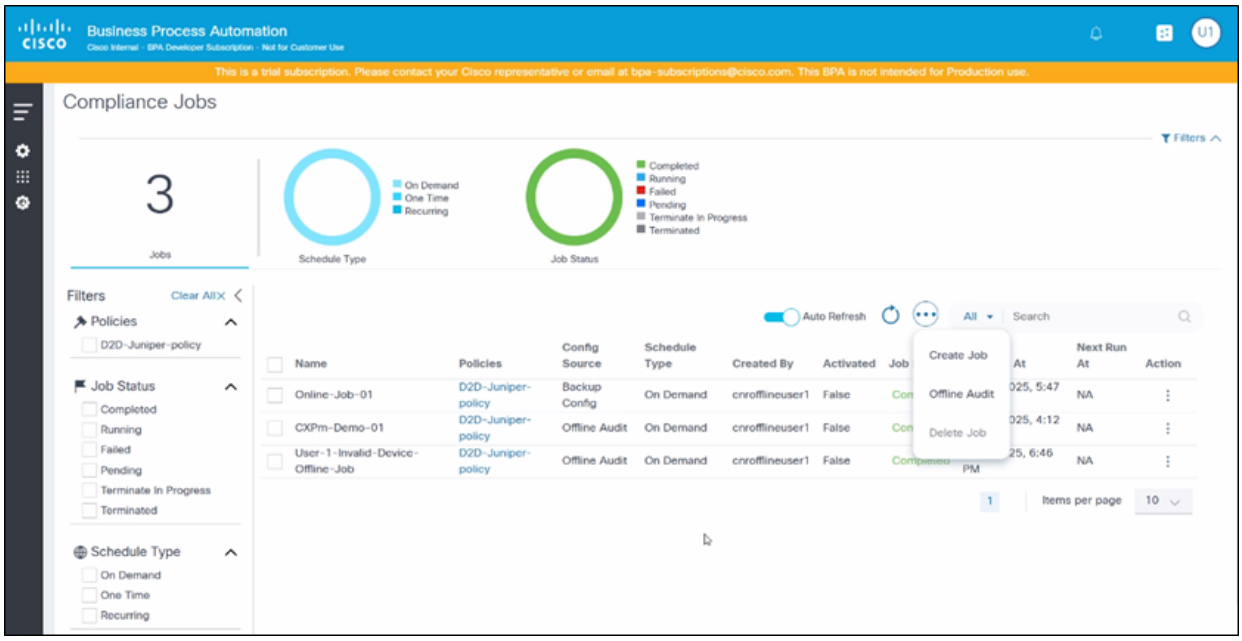
Filtri condizionali

La funzione Filtri condizionali è uno strumento avanzato che consente agli utenti di applicare criteri specifici ai blocchi di configurazione, garantendo controlli di conformità precisi e mirati.

- Consente agli utenti di applicare le configurazioni o di eseguire controlli di conformità sui blocchi di configurazione selezionati in base a condizioni predefinite
- Concentra le risorse e gli sforzi sui blocchi rilevanti filtrando quelli che non soddisfano i criteri specificati
- Gli utenti possono definire le condizioni che i blocchi di configurazione devono soddisfare per essere inclusi nei controlli di conformità o in altri processi
- Vengono eseguiti solo i blocchi che soddisfano queste condizioni, mentre gli altri vengono ignorati, consentendo un controllo più preciso

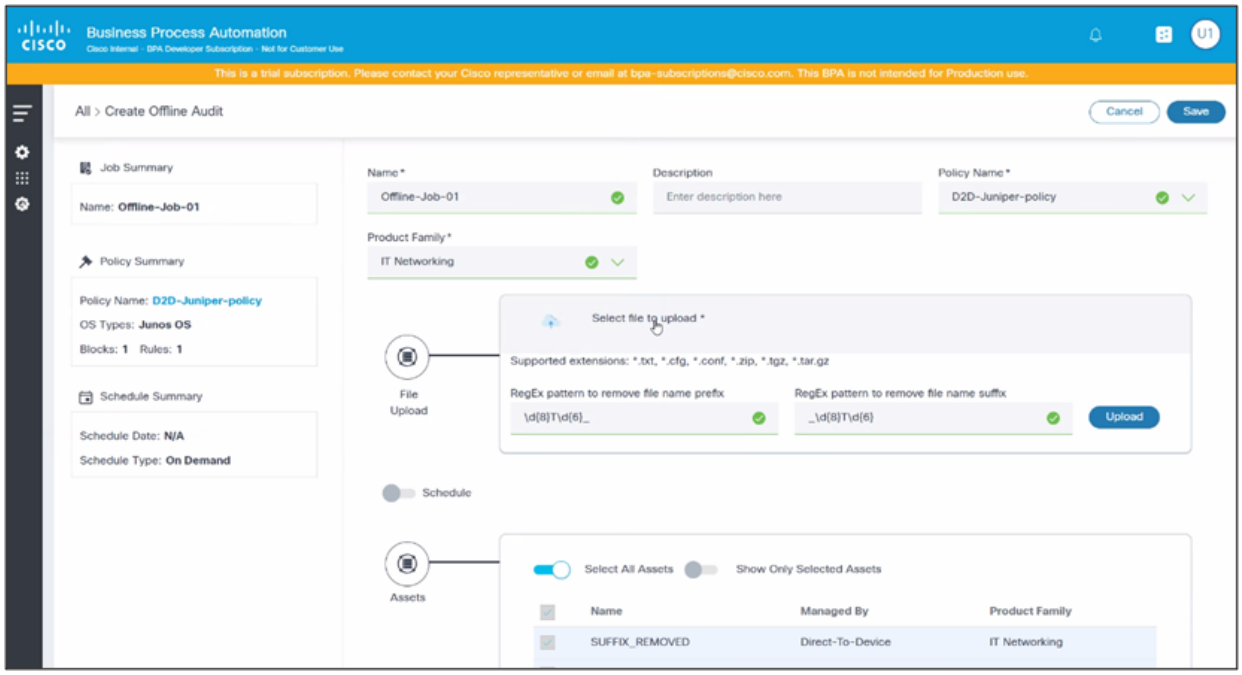
Esempio di caso di utilizzo:

- Controlli di conformità selettivi: Se una regola prevede il controllo delle configurazioni solo su due interfacce specifiche delle 20 disponibili, gli utenti possono impostare condizioni per limitare i controlli di conformità solo a queste due interfacce.



Filtri condizionali

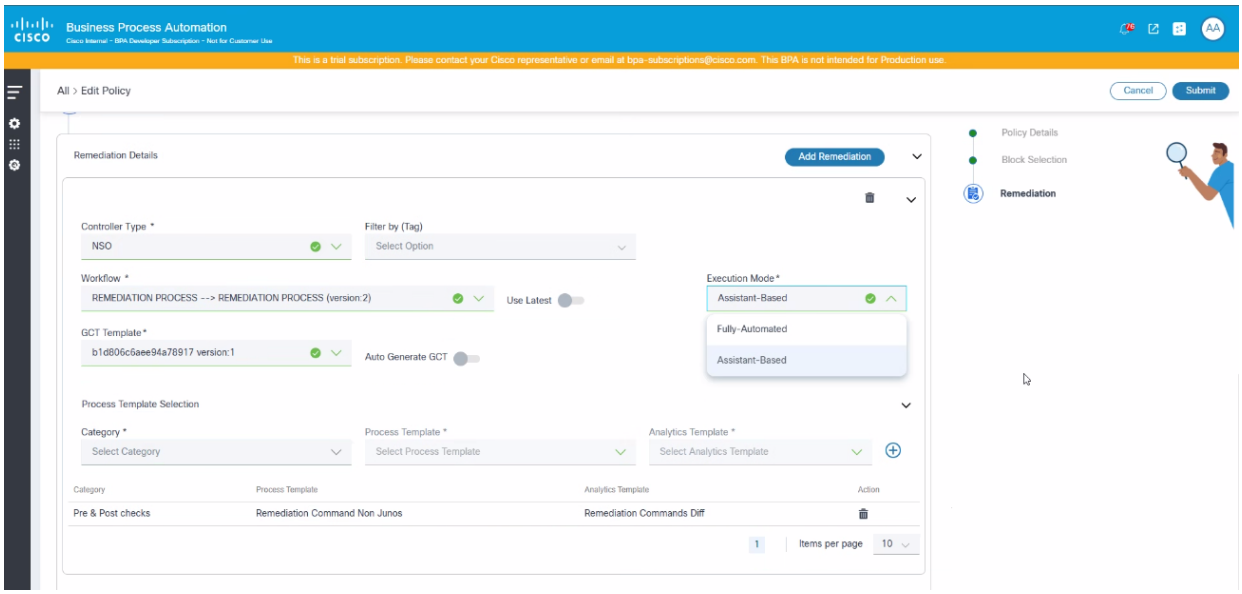
- Seleziona regole: Opzione per selezionare una o più regole per un determinato blocco di configurazione.



Seleziona regole

Sezione Risanamento

La pagina Criteri contiene una sezione facoltativa per la definizione dei dettagli di monitoraggio e aggiornamento per ciascun tipo di controller.



Criteri di configurazione: Dettagli risoluzione

- Tipo di controller: Elenco dei tipi di controller con supporto per la risoluzione dei problemi
- Flusso di lavoro di risoluzione: Flusso di lavoro da eseguire per i dispositivi del tipo di controller selezionato
- Modello GCT: Uno o più modelli GCT da applicare
- Modello di processo: Uno o più modelli di processo da eseguire come parte del pre-controllo e del post-controllo, insieme al modello di analisi corrispondente.
- Modello di pre-controllo: Elenco facoltativo di modelli di processo da eseguire solo per il pre-controllo
- Modello assegno: Elenco facoltativo di modelli di processo da eseguire solo per il controllo post
- Modalità di esecuzione:
    - Completamente automatico: Il processo di monitoraggio e aggiornamento viene eseguito automaticamente senza interventi manuali o attività da parte degli utenti
    - Basato su Assistente: Il sistema crea attività utente che richiedono assistenza manuale durante il processo di risoluzione

Genera automaticamente feature GCT

La funzione di generazione automatica del GCT è stata progettata per semplificare il processo di creazione dei modelli GCT necessari per la correzione. Funziona come descritto di seguito:

- Genera automaticamente modelli GCT in base ai risultati e ai dettagli dell'esecuzione della conformità
- Automatizza il processo di creazione dei modelli
- I modelli generati sono personalizzati per risolvere i problemi identificati durante i controlli di conformità, garantendo l'allineamento delle azioni correttive alle esigenze di conformità

Ruoli e controllo di accesso

Elenco autorizzazioni statiche

Il dashboard Conformità configurazione nel portale di nuova generazione supporta la funzione RBAC di BPA con le autorizzazioni seguenti che rappresentano la modalità di visualizzazione di un blocco di testo dinamico di configurazione in una rappresentazione GUI per la gestione delle regole e delle condizioni:

Group	Azione	Descrizione
ui-app	complianceDashboard.show	Mostra/Nascondi app dashboard conformità
ui-app	dashboard di monitoraggio e aggiornamento.show	Mostra app processi di monitoraggio e aggiornamento
ui-app	processi di conformità.show	Mostra app Processi conformità
ui-app	conformitConfigurazioni.show	Mostra app di configurazione conformità
dashboard di conformità	assetRiepilogoConformità	Visualizza riepilogo conformità cespiti
dashboard di conformità	riepilogoConformitàCriteri	Visualizza riepilogo conformità criteri
dashboard di conformità	visualizzaViolazioni	Visualizza dettagli violazione
dashboard di conformità	RiepilogoConformitàRisorse	Visualizza i cespiti interessati
dashboard di conformità	visualizzaRapporti	Visualizza dashboard di report, impostazioni report e report di download
dashboard di conformità	gestisciReport	Creazione ed eliminazione di report
dashboard di conformità	gestisciImpostazioniReport	Modifica impostazioni report
dashboard di monitoraggio e	visualizzaProcessiRimediativi	Visualizza processi di monitoraggio e aggiornamento

Group	Azione	Descrizione
aggiornamento		
dashboard di monitoraggio e aggiornamento	visualizzaAttivitàCardineMonitoraggio e aggiornamento	Visualizza attività cardine di risoluzione
dashboard di monitoraggio e aggiornamento	gestisciProcessiDiRimedio	Gestire processi di monitoraggio e aggiornamento quali creazione, eliminazione, archiviazione e gestione di attività utente
processi di conformità	visualizzaProcessiConformità	Visualizza processi ed esecuzioni di conformità
processi di conformità	gestisciProcessiConformità	Gestisci processi di conformità
Configurazioni conformità	visualizzaConfigurazioniConformità	Visualizzare configurazioni di conformità quali criteri, blocchi, regole, generazione di blocchi, identificatori di blocchi e modelli TTP
Configurazioni conformità	gestisciCriteriConformità	Gestisci criteri di conformità
Configurazioni conformità	gestisciBlocchiConformità	Gestire blocchi e regole di conformità e identificatori di blocco
Configurazioni conformità	gestisciGenerazioneBlocchiConformità	Gestire la generazione dei blocchi di conformità e i modelli TTP

Ruoli predefiniti

Lo use case Conformità alla configurazione e risoluzione dispone dei ruoli predefiniti elencati nella tabella seguente:

Nota: Gli amministratori possono creare o aggiornare i ruoli in base ai requisiti del cliente.

Ruolo	Descrizione	Autorizzazioni
Amministratore conformità	Ruolo di amministratore con tutte le autorizzazioni relative alla conformità	Applicazioni UI: Mostra Asset Manager - Mostra gruppo asset - Visualizza Dashboard Conformità

Ruolo	Descrizione	Autorizzazioni
		- Mostra processi di conformità - Mostra configurazione conformità Bene: Visualizza elenco risorse - Visualizza la configurazione di backup per gli asset - Configurazione di backup - Esecuzione delle azioni del dispositivo abilitate dal controller Gruppo di asset: - Visualizza gruppi di cespiti - Gestisci gruppi di cespiti - Creazione di gruppi di asset dinamici Configurazione backup: Visualizzazione, confronto e download dei backup della configurazione dei dispositivi Criterio di ripristino backup: Visualizza criteri di ripristino backup Dashboard di conformità: - Visualizzare i riepiloghi di conformità degli asset - Visualizzare i riepiloghi di conformità delle policy - Visualizza violazioni - Visualizzare le risorse interessate Creazione ed eliminazione di report Visualizza dashboard di report, impostazioni report e report di download Modificare le impostazioni del report: Processi di conformità Visualizza processi ed esecuzioni di

Ruolo	Descrizione	Autorizzazioni
		conformità - Gestire i processi di conformità Configurazioni di conformità: - Visualizzare le configurazioni di conformità come regole, blocchi e regole - Gestire le policy di conformità - Gestione di blocchi di conformità, regole e identificatori di blocco - Gestire la generazione di blocchi di conformità e i modelli TTP Applicazioni UI: - Mostra Asset Manager - Mostra gruppo asset - Visualizza Dashboard Conformità - Mostra processi di conformità - Mostra configurazione conformità
Operatore conformità	Ruolo operatore con tutte le autorizzazioni di conformità, ad eccezione della gestione della configurazione	Bene: Visualizza elenco risorse - Visualizza la configurazione di backup per gli asset - Configurazione di backup - Esecuzione delle azioni del dispositivo abilitate dal controller Gruppo di asset: - Visualizza gruppi di cespiti - Gestisci gruppi di cespiti - Creazione di gruppi di asset dinamici Configurazione backup: Visualizzazione, confronto e download dei backup della configurazione dei dispositivi Criterio di ripristino backup: Visualizza

Ruolo	Descrizione	Autorizzazioni
		criteri di ripristino backup Dashboard di conformità: - Visualizza riepilogo conformità cespiti - Visualizzare il riepilogo di conformità alle regole - Visualizza violazioni - Visualizzare le risorse interessate Creazione ed eliminazione di report Visualizza dashboard di report, impostazioni report e report di download Processi di conformità: Visualizza processi ed esecuzioni di conformità - Gestire i processi di conformità Configurazioni di conformità: Visualizzare configurazioni di conformità quali regole, blocchi e regole Applicazioni UI: - Mostra Asset Manager - Mostra gruppo asset - Visualizza Dashboard Conformità - Mostra processi di conformità - Mostra configurazione conformità
Conformità in sola lettura	Fornisce tutte le autorizzazioni di sola lettura relative allo Use Case di conformità	Bene: Visualizza elenco risorse - Visualizza la configurazione di backup per gli asset - Esecuzione delle azioni del dispositivo abilitate dal controller Gruppo di asset:

Ruolo	Descrizione	Autorizzazioni
Amministratore di monitoraggio e aggiornamento/Operatore di monitoraggio e aggiornamento	Ruolo Operatore con tutte le autorizzazioni relative alla risoluzione	- Visualizza gruppi di cespiti Configurazione backup: Visualizzazione, confronto e download dei backup della configurazione dei dispositivi Criterio di ripristino backup: Visualizza criteri di ripristino backup Dashboard di conformità: Visualizza riepilogo conformità cespiti - Visualizzare il riepilogo di conformità alle regole - Visualizza violazioni - Visualizzare le risorse interessate Visualizza dashboard di report, impostazioni report e report di download Processi di conformità: Visualizza processi ed esecuzioni di conformità Configurazioni di conformità: Visualizzare configurazioni di conformità quali regole, blocchi e regole Applicazioni UI: - Mostra Asset Manager - Mostra gruppo asset - Visualizza dashboard di monitoraggio e aggiornamento Bene: - Visualizza elenco risorse Gruppo di asset:

Ruolo	Descrizione	Autorizzazioni
		- Visualizza gruppi di cespiti Gestisci gruppi di cespiti - Creazione di gruppi di asset dinamici Dashboard di monitoraggio e aggiornamento: - Visualizza processi di monitoraggio e aggiornamento - Visualizza attività cardine di risoluzione - Visualizza riepilogo conformità cespiti - Gestire processi di monitoraggio e aggiornamento quali la creazione, l'eliminazione, l'archiviazione e la gestione di attività utente - Visualizzare le risorse interessate Applicazioni UI: - Mostra Asset Manager - Mostra gruppo asset - Visualizza dashboard di monitoraggio e aggiornamento
Correzione - Sola lettura	Fornisce tutte le autorizzazioni di sola lettura relative allo Use Case di monitoraggio e aggiornamento	Bene: - Visualizza elenco risorse Gruppo di asset: - Visualizza gruppi di cespiti Crea gruppi di asset dinamici Dashboard di monitoraggio e aggiornamento: - Visualizza processi di monitoraggio e aggiornamento - Visualizza attività cardine di risoluzione

Ruolo	Descrizione	Autorizzazioni
		- Visualizza riepilogo conformità cespiti - Visualizzare le risorse interessate

Criteri di accesso

La funzionalità Criteri di accesso garantisce agli utenti l'accesso appropriato a specifici criteri di conformità e gruppi di risorse. Questa funzionalità migliora la sicurezza e l'efficienza operativa consentendo agli amministratori di definire e applicare i controlli di accesso in base ai ruoli e alle responsabilità degli utenti. I criteri di accesso vengono gestiti tramite la pagina Criteri di accesso, in cui gli amministratori possono creare, modificare e assegnare criteri a utenti o gruppi. Gli amministratori possono definire autorizzazioni granulari, specificando i criteri di conformità e i gruppi di risorse che ogni utente o gruppo può visualizzare, modificare o gestire. Questo livello di dettaglio contribuisce a mantenere un controllo rigoroso sulle informazioni riservate e sulle operazioni critiche.

Una volta definiti i criteri di accesso, i dati vengono limitati in tutte le pagine di conformità e correzione dell'interfaccia utente di nuova generazione, in base all'elenco di criteri e risorse CnR a cui l'utente corrente ha accesso.

Per fornire l'accesso utente:

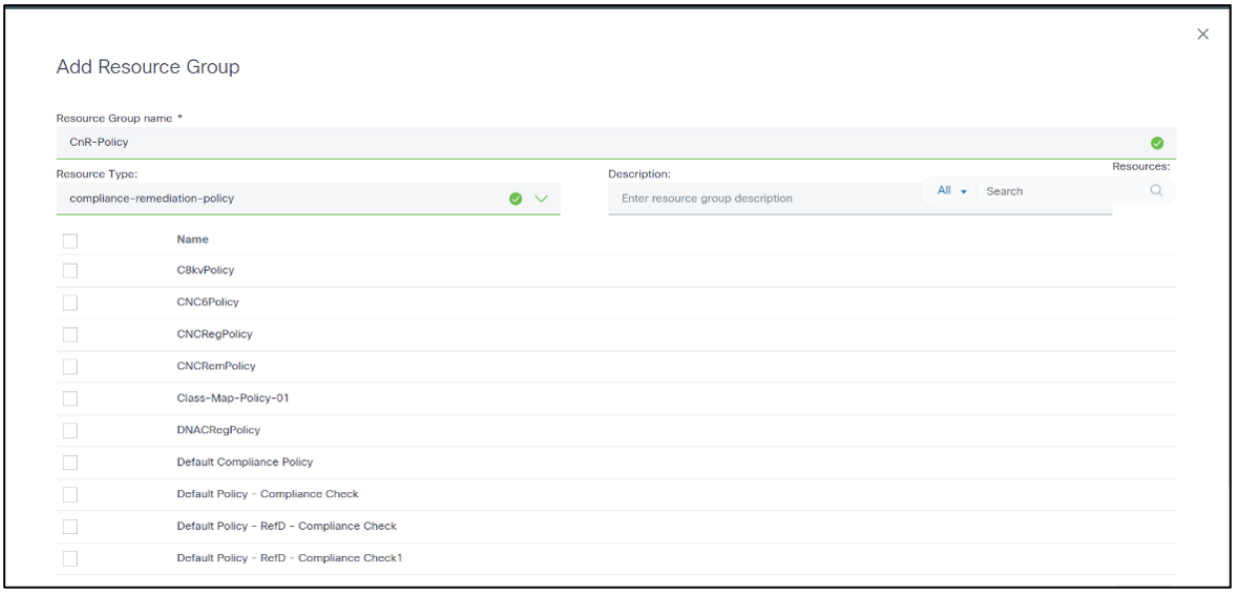
Nota: Le autorizzazioni possono essere fornite solo dagli amministratori.

---

1. Creare uno o più utenti e assegnarne uno a uno o più gruppi di utenti.
2. Creare ruoli utente e assegnarli ai gruppi di utenti creati.
3. Aggiungere cespiti a uno o più gruppi di cespiti.
4. Crea gruppi di risorse per assegnare le risorse dei criteri di conformità.
5. Creare un criterio di accesso e selezionare i gruppi di utenti, i gruppi di risorse e i gruppi di risorse rilevanti.

Creazione del gruppo di risorse

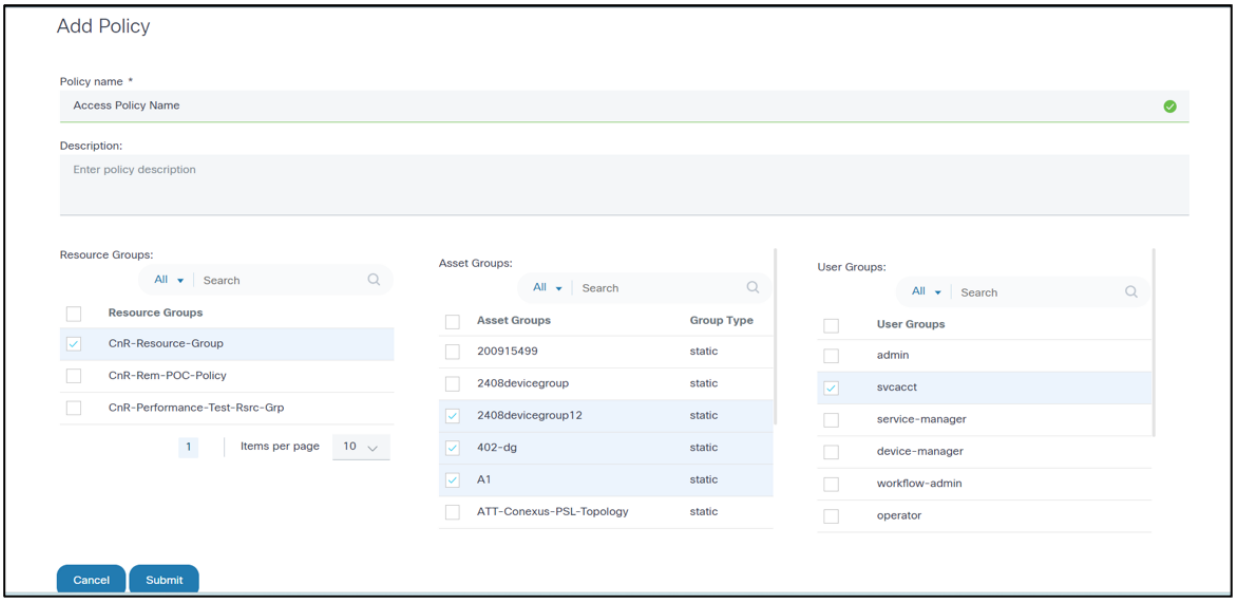
Creare un gruppo di risorse utilizzando il criterio di monitoraggio e aggiornamento della conformità dall'elenco a discesa Tipo di risorsa e selezionare i criteri di conformità a cui è necessario concedere l'accesso al rispettivo gruppo di utenti.



Crea gruppo di risorse

Crea criteri di accesso

Creare un criterio di accesso con gruppi di risorse e gruppi di risorse che devono essere autorizzati dai gruppi di utenti.



Crea criteri di accesso

Conformità offline

La funzione di conformità offline consente agli utenti di eseguire controlli di conformità sulle configurazioni dei dispositivi che non sono disponibili tramite dispositivi attivi nell'inventario degli asset.

Gli utenti possono eseguire la conformità offline utilizzando la configurazione di backup del dispositivo o creando un controllo offline in Processi di conformità. I risultati delle esecuzioni possono essere visualizzati nel dashboard Conformità.

Utilizzo della configurazione di backup del dispositivo

Gli amministratori possono caricare manualmente un file zip contenente la configurazione in esecuzione per un set di dispositivi desiderato. Questa funzione è disponibile nella sezione Configurazione dispositivo - Carica dell'applicazione Backup e ripristino. Una volta caricate le configurazioni dei dispositivi, è possibile creare un processo di conformità per i dispositivi desiderati selezionando Configurazione backup dispositivo come origine della configurazione dei dispositivi. Durante l'esecuzione, la configurazione del dispositivo caricato viene recuperata dall'applicazione di backup e su di essa viene eseguito il controllo di conformità.

Utilizzo della funzione Crea audit non in linea nei job di conformità

Per eseguire la conformità sulla configurazione di un dispositivo in modalità non in linea, gli utenti possono selezionare Controllo non in linea dall'icona Altre opzioni nella pagina Processi di conformità. Ciò consente agli utenti di caricare manualmente un file zip contenente la configurazione in esecuzione direttamente nell'applicazione di conformità. Durante l'esecuzione, viene analizzata la configurazione del dispositivo caricato e viene eseguito il controllo di conformità.

Distribuzione delle configurazioni tramite Ingester

Il caricamento degli artifact di configurazione di conformità può essere automatizzato utilizzando il framework Ingester. Una volta sviluppati, gli artifact possono essere esportati, collocati e distribuiti nell'ambiente di destinazione utilizzando i passi riportati di seguito.

- Creare il pacchetto NPM utilizzando i comandi seguenti:

```
mkdir <

      >
cd  <

        >
npm init (press "enter" for all prompts)
```

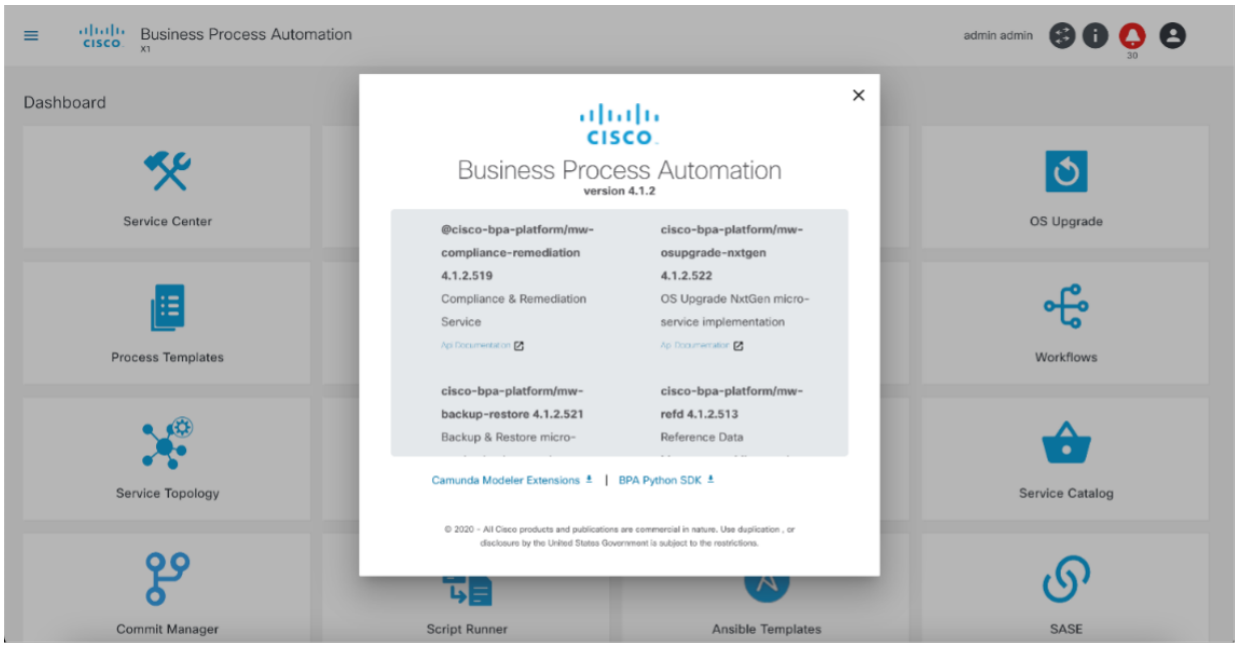
- Esporta configurazioni dal portale BPA (interfaccia utente classica)
    - Passare a BPA Interfaccia classica > Conformità e risoluzione della configurazione > Configurazioni
    - Esporta "Modelli TTP/Identificatori blocchi/Blocchi/Regole/Criteri"
- Rinominare i file esportati nel modo seguente:
    - Modelli TTP: <<nomefile>>.cnrttptemplate.json
    - Identificatori blocco: <<nomefile>>.cnrblockidentifier.json
    - Blocchi: <<nomefile>>.cnrblock.json
    - Regole: <<nomefile>>.cnrrule.json
    - Criteri: <<nomefile>>.cnrpolicy.json
- Dati Package ingester (.tgz)
    - Copiare tutti i file esportati nel pacchetto npm creato nel "passaggio 1"
    - Eseguire il comando `npm pack` nel pacchetto npm per creare il file ".tgz"
- Distribuzione di dati ingester (.tgz) in BPA Single Node env
    - Copiare il file .tgz nella cartella <<BPA core bundle>>/packages/data nel server in cui è stato distribuito il bundle BPA
    - Riavviare il server Ingester (docker restart ingester-service)
- Distribuzione dei dati Ingester (con estensione tgz) nell'ambiente BPA a più nodi
    - Copiare il file .tgz nella cartella /opt/bpa/packages/data del server in cui vengono distribuiti i grafici a elmetto
    - Ridistribuire Ingester pod (`kubectl rollout riavviare la distribuzione ingester-service -n bpa-ns`)

Riferimenti

Nome	Descrizione
TTP	Parser testo modello utilizzato nei blocchi di configurazione
Parser conf	Parser del campo di configurazione utilizzato per analizzare la configurazione del dispositivo CLI

Documentazione sulle API

I dettagli della documentazione API per la conformità e il monitoraggio e l'aggiornamento sono disponibili nel popup Informazioni su dell'interfaccia utente classica:



Informazioni su BPA (interfaccia utente classica)

Risoluzione dei problemi

Dashboard

Risultati recenti del processo di conformità non visualizzati

Osservazione: I risultati recenti del processo di conformità non vengono visualizzati nel dashboard del portale di nuova generazione.

Causa potenziale 1: Il dashboard dispone di una selezione di intervalli di date, che per impostazione predefinita è "Mese corrente". Se di recente è iniziato un nuovo mese (ad esempio, oggi è il primo del mese), le esecuzioni eseguite prima di ieri (ultimo giorno del mese precedente) non verranno visualizzate.

Analisi: Verificare che nel dashboard sia selezionato l'intervallo di date corretto, inclusi i giorni del mese precedente, se necessario, per visualizzare i dati delle violazioni corretti.

Causa potenziale 2: Un utente diverso può aver eseguito un processo di conformità sulla stessa combinazione di criteri e/o risorse. Il dashboard mostra le violazioni rilevate durante l'ultima esecuzione entro l'intervallo di date selezionato.

Analisi: In qualità di amministratore (o utente con accesso a tutti i job di conformità), esaminare l'elenco dei job di conformità e la relativa cronologia per determinare quali combinazioni di criteri o gruppi di asset vengono eseguite.

Processi di conformità

Intero stato di esecuzione impostato su "Ignorato"

Osservazione: Durante l'esecuzione dei job di conformità, un intero stato di esecuzione viene contrassegnato come "Ignorato". Non vengono segnalate violazioni.

Causa potenziale: È ancora in esecuzione un'esecuzione esistente per lo stesso processo.

Analisi: Un processo di conformità può avere una sola esecuzione in stato di esecuzione in un determinato momento. Verificare se è ancora in esecuzione un'esecuzione precedente. Le esecuzioni bloccate o in esecuzione per un periodo di tempo prolungato possono essere terminate/

Stato dispositivo impostato su "Ignorato"

Osservazione: In un'esecuzione di un processo di conformità, lo stato di alcuni dispositivi è contrassegnato come "Ignorato".

Causa potenziale: La funzionalità di conformità non è abilitata per il tipo di controller a cui appartiene il dispositivo.

Analisi: I criteri di conformità si applicano solo ai dispositivi all'interno del gruppo di risorse per i quali la funzionalità è abilitata.

Stato dispositivo impostato su "Non riuscito"

Osservazione: In un'esecuzione del processo di conformità, lo stato di alcuni dispositivi è contrassegnato come "Non riuscito".

Causa potenziale: Errori di runtime che si sono verificati durante il processo di esecuzione della conformità. Tali errori possono essere errori di codice o configurazioni errate in criteri, blocchi, regole, identificatori di blocco e così via.

Analisi:

API per individuare il motivo degli errori di runtime:

1. Recupera le esecuzioni per trovare l'ID esecuzione

API: /api/v1.0/compliance-remediation/

esecuzioni per la conformità

Metodo: OTTIENI

2. Ottieni esecuzioni dispositivo tramite ID esecuzione

   API: /api/v1.0/compliance-remediation/

   conformità-dispositivi-esecuzioni?

   ID esecuzione=<< id esecuzione >>

   Metodo: OTTIENI

Regole di conformità

Valore vuoto visualizzato nelle regole

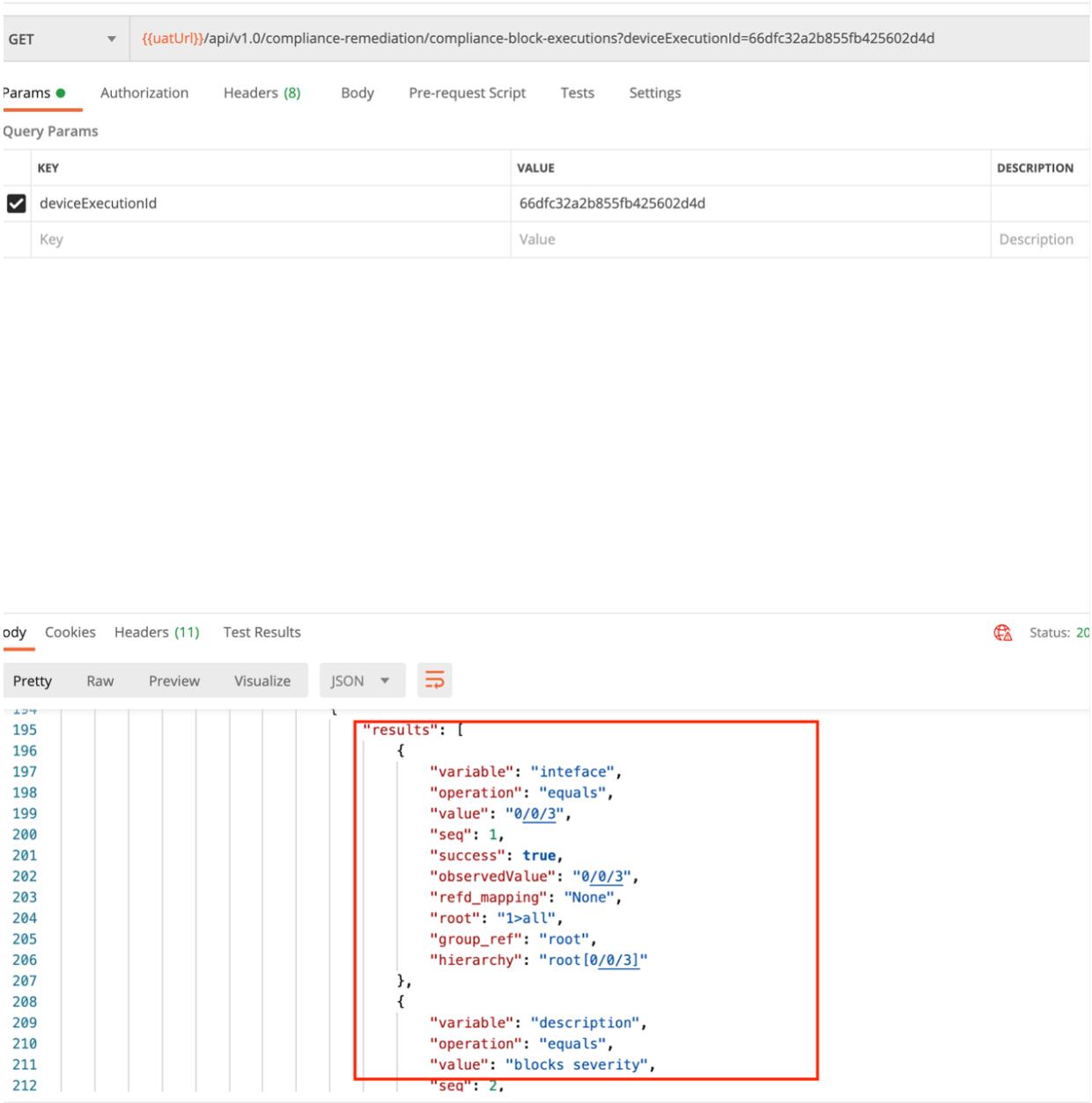
Osservazione: Durante l'esecuzione di un processo di conformità, le variabili della regola visualizzano valori vuoti.

Analisi:

1. Se i dati vengono recuperati dall'applicazione RefD, verificare che il formato delle chiavi RefD sia corretto. In caso affermativo, verificare che l'applicazione RefD disponga di dati per la chiave collegati alla variabile di conformità nelle regole. Verificare inoltre che la chiave RefD corretta venga inviata dall'app di conformità controllando i log del servizio di conformità. Per ulteriori informazioni, fare riferimento al documento sulla descrizione della gerarchia di regole e sull'integrazione dei riferimenti nelle regole e nelle regole non di riferimento.
2. Verificare il risultato dell'esecuzione del blocco di conformità utilizzando l'API seguente:

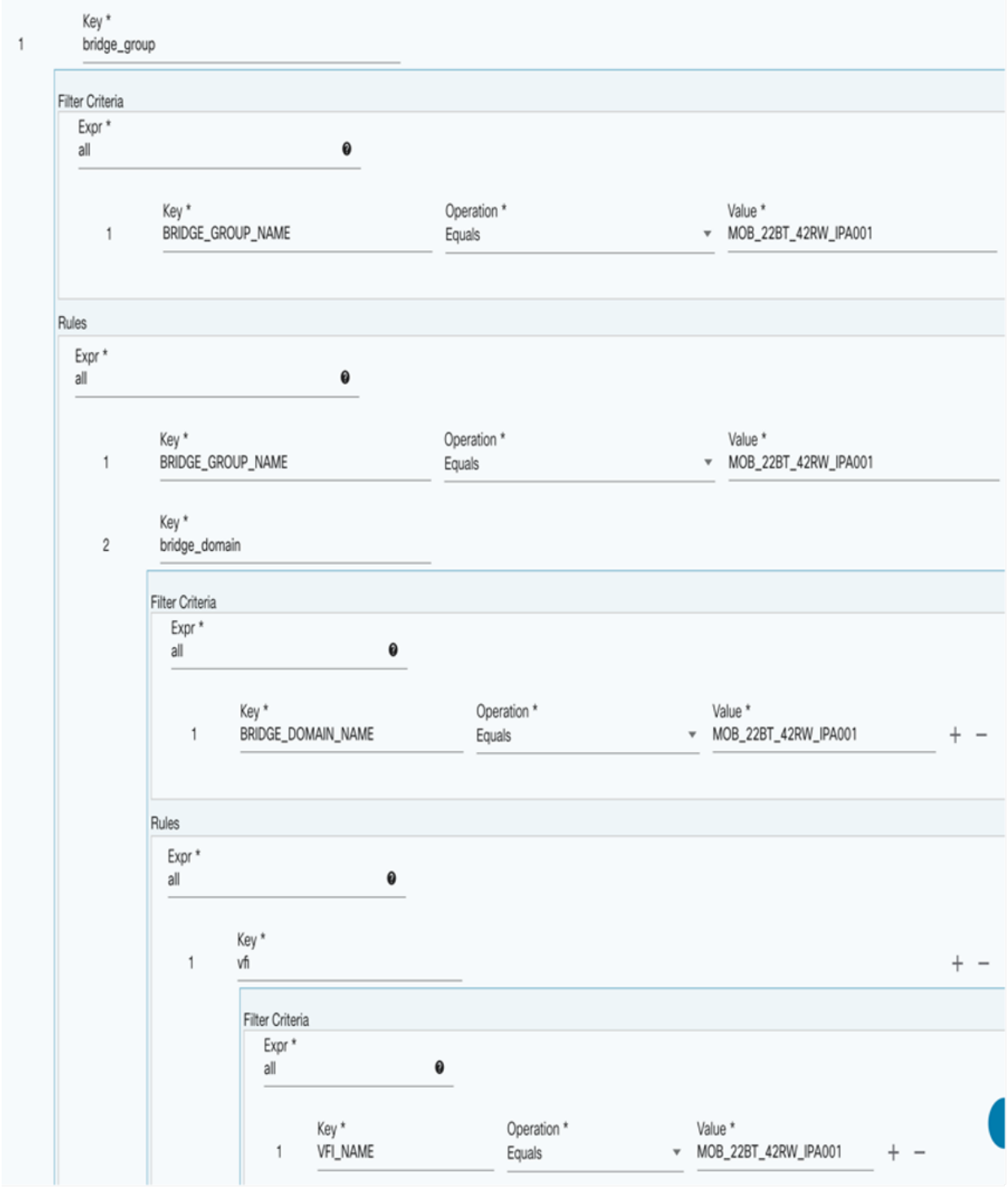
   URL: /api/v1.0/compliance-remediation/compliance-block-execution?deviceExecutionId=<>

   Metodo: OTTIENI



Risultati dall'esecuzione dei blocchi di conformità

3. Verificare se il blocco dispone di sottogerarchie o di un'unica gerarchia e assicurarsi che le regole siano configurate in base alla gerarchia.



Risultati dall'esecuzione dei blocchi di conformità

4. Verificare che il parser TCP estragga il valore dalla configurazione del dispositivo eseguendo il seguente script Python:

```
from ttp import ttp
### Provide device config inside the below variable
data_to_parse = """
"""

### Provide block config inside the below variable
ttp_template = """
```

```
"""

### Create parser object and parse data using template:
parser = ttp(data=data_to_parse, template=ttp_template)
parser.parse()

### Check results and see if TTP parser extracts the value or not
results = parser.result()
print(results)
```

Monitoraggio dei log di conformità

Env. a nodo singolo:

```
docker logs -f compliance-remediation-service
```

Busta Kubernetes a più nodi:

```
kubectl logs -f services/compliance-remediation-service -n bpa-ns
```

Monitoraggio dei log Kibana:

```
https://<< HOST BPA >>:30401
```

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).