# BPA-Benutzerhandbuch Konfiguration, Compliance und Problembehebung v5.1

# Einleitung

Die Anwendung Configuration Compliance and Remediation (CnR) stattet Netzwerkbetreiber mit der Durchführung von Compliance-Prüfungen der Gerätekonfiguration für benutzerdefinierte Richtlinien aus, die aus Konfigurationsblöcken erstellt werden. Operatoren erstellen manuell oder automatisch Konfigurationsblöcke mithilfe des Systems aus ausgewählten Gerätekonfigurationen. Benutzer können auch Regeln erstellen, die für diese Blöcke gelten, wobei Regelbedingungen möglicherweise von Werten abgeleitet werden, die aus der RefD-Anwendung abgerufen werden. Bediener können Compliance-Prüfungen bequem nach einem Zeitplan durchführen oder die Prüfungen sofort einleiten.

Die Anwendung verfügt über ein intuitives Dashboard, das einen umfassenden Überblick über Compliance-Verletzungen bietet und sowohl Zusammenfassungen als auch detaillierte Ansichten auf Geräte- und Konfigurationsblockebene bietet.

Die Anwendung enthält ein robustes Framework zur Behebung von Compliance-Verstößen. Dieses Framework nutzt Workflows und Vorlagen (sowohl Konfigurationsvorlagen, die als Golden Configuration Templates (GCTs) bezeichnet werden, als auch Prozessvorlagen), um den Sanierungsprozess zu optimieren. Ähnlich wie bei Compliance-Prüfungen können auch Sanierungsaufgaben so programmiert werden, dass sie nach einem Zeitplan ausgeführt werden, oder unmittelbar ausgelöst werden, um Verstöße umgehend zu beheben.

Das Compliance and Remediation-Dashboard des Next-Generation-Portals (Next-Gen) bietet Funktionen zur Optimierung des Netzwerksicherheitsmanagements, zur Rationalisierung von Compliance-Verfahren und zur Vereinfachung von Sanierungsmaßnahmen. Das Dashboard bietet eine umfassende Zusammenfassung der Ressourcen- und Richtlinienkonformität. Netzwerkbetreiber können so den Zustand ihres Netzwerks auf einfache Weise bewerten und sicherstellen, dass Geräte strenge Sicherheitsprotokolle erfüllen.

Konfigurationsblöcke können automatisch erstellt, bearbeitet oder manuell hinzugefügt werden, um ein Gleichgewicht zwischen Automatisierung und Anpassung zu schaffen. Die genaue Identifizierung der Konfigurationsbausteine und die detaillierten Zugriffskontrollmechanismen, einschließlich detaillierter Benutzer-, Gruppen- und Berechtigungseinstellungen über klassische und moderne Schnittstellen, stellen sicher, dass die Netzwerkkonfigurationen sowohl sicher als auch in den Händen vertrauenswürdiger Mitarbeiter bleiben. Diese Funktionen bieten ein leistungsstarkes Toolset für Unternehmen, die hohe Netzwerk-Compliance- und Sicherheitsstandards aufrechterhalten möchten.

# Neuerungen

Die folgenden wichtigen Funktionen und Verbesserungen wurden eingeführt:

- Umfassendes Reporting-Dashboard zum Erstellen, Anzeigen und Herunterladen von Compliance-Berichten
- Möglichkeit zur Durchführung von Offline-Konformitätsprüfungen durch Hochladen von Gerätekonfigurationen ohne Geräteintegration mit Asset Manager
- Möglichkeit zur Konfiguration von Mustern in der Blockkonfiguration zum Maskieren vertraulicher Gerätekonfigurationsdaten
- Möglichkeit zum Exportieren von zusammengefassten Daten zu Richtlinien und Ressourcen als CSV-Dateien
- Generierte Wiederherstellungskonfigurationen anzeigen und mit laufenden Gerätekonfigurationen vergleichen
- Verbesserungen in Blöcken zur Unterstützung der Auslösung von Verletzungen, wenn die Konfiguration vorhanden ist
- Vernetzte Benutzerumgebung auf Seiten zum Erstellen und Bearbeiten von Richtlinien aktivieren, um sie übergreifend in untergeordnete Komponenten wie die Seite zum Erstellen von Blöcken zu starten
- Verbesserungen bei Compliance-Aufträgen - Erstellung und Bearbeitung von Seiten für den Querstart zur Bearbeitungsseite für Richtlinien

## Komponenten

Compliance und Fehlerbehebung unterstützen die folgenden Controller und Gerätetypen:

| Controller | Betriebssystemtypen |
|---|---|
| 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 X, IOS X Nur validierte Compliance |
| FMC (7.2.5) | FX-OS (FTD) Nur validierte Compliance |
| Direct To Device (D2D) | IOS XE, IOS XR, JunOS |

Anmerkung: Nokia SR-OS-Unterstützung über den NSO-Controller gilt nur für die Funktion zur Einhaltung von Konfigurationsvorgaben. Die Behebung wird für Nokia-Geräte nicht unterstützt.

Anmerkung: Die Kompatibilitätsfunktion funktioniert mit der Gerätekonfiguration im CLI-

Format (Cisco Command Line Interface) und im YAML-ähnlichen Format für Juniper- und Nokia-Geräte. Derzeit unterstützt das Framework keine anderen Formate wie Netconf, JSON, XML usw.

Als Teil der Version 5.0 wurde die klassische Compliance- und Behebungsanwendung (CnR) verworfen. Alle CnR-Funktionen sind jetzt vollständig integriert und im Portal der nächsten Generation verfügbar.

## Voraussetzungen und Voraussetzungen

Die folgenden Voraussetzungen sind für eine effektive Nutzung des CnR-Anwendungsfalls erforderlich.

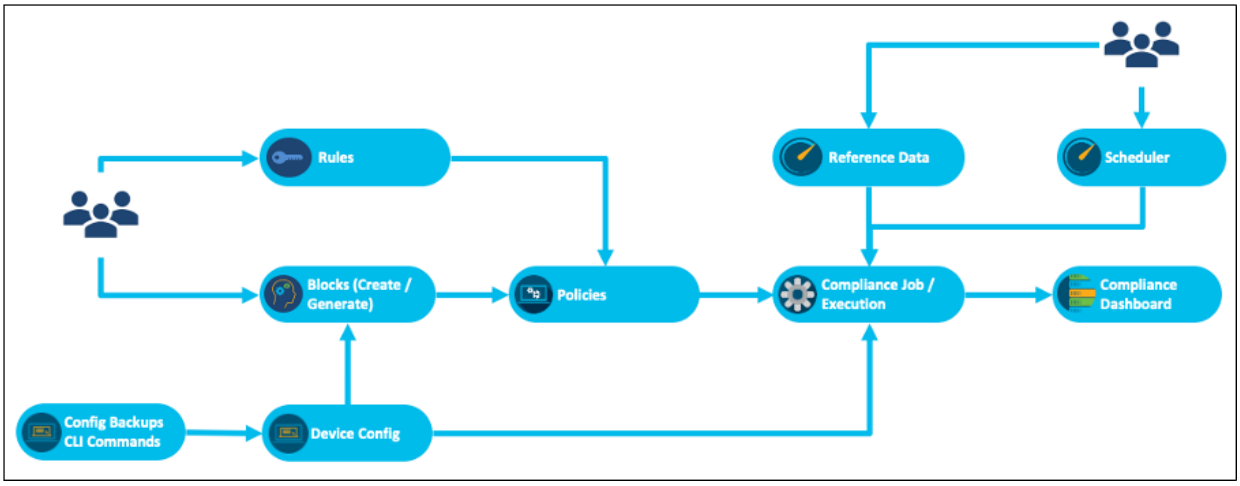
- Der Berechtigungsschlüssel für das Abonnement für einen CnR-Anwendungsfall muss hochgeladen werden.
- Der entsprechende Controller und die entsprechenden Geräte sollten im Rahmen des BPA Asset Managers integriert und verfügbar sein. Weitere Informationen finden Sie im Abschnitt "Asset Manager" im BPA-Benutzerhandbuch.
- Die integrierten Ressourcen müssen den Kundenanforderungen entsprechend im Next-Gen-Portal in Ressourcengruppen gruppiert werden.

## Compliance-Dashboard

Das Compliance-Dashboard bietet eine zusammengefasste Ansicht der Verstöße auf allen Geräten für die ausgewählte Zeit. Die Daten für den aktuellen Monat werden standardmäßig angezeigt. Benutzer können das Zeitfenster ändern, um historische Daten zu Compliance-Verletzungen anzuzeigen. Der aktuelle Monat ist die standardmäßig ausgewählte Ansicht.

Anmerkung: Das veraltete Compliance-Dashboard in der klassischen Benutzeroberfläche wurde entfernt und ist nicht mehr verfügbar. Es sollte das im Next-Gen Portal verfügbare Dashboard verwendet werden.

### Flussdiagramm zur Konfigurationskonformität



Übersicht über die Compliance-Komponente

Die im Dashboard angezeigten Compliance-Verletzungen werden eingetragen, wenn ein Compliance-Auftrag für eine Richtlinie mit einer Liste von Ressourcen ausgeführt wird. Die Compliance-Richtlinie wird erstellt, indem eine Liste der Blockkonfigurationen und die erforderlichen Compliance-Regeln hinzugefügt werden. Die Compliance-Regel kann Prüfungen mit statischen Werten oder dynamischen Variablen enthalten, für die Daten aus der RefD-Anwendung abgerufen werden. Ein Compliance-Job kann bei Bedarf oder als einmaliger oder wiederkehrender Zeitplan ausgeführt werden.

Die Einhaltung der Konfigurationsrichtlinien umfasst die folgenden wichtigen Funktionen:

- Blockerstellung: Blöcke werden manuell erstellt oder automatisch mithilfe der Vorlage Template Text Parser (TTP) generiert. Sie können statisch oder dynamisch (mit Variablen) sein.
- Regelerstellung: Regeln validieren die Variablen in den Blöcken. Regelwerte können während der Laufzeit statisch festgelegt oder dynamisch aus dem Referenzdatensystem (RefD) abgerufen werden.
- Richtlinienerstellung: Richtlinien werden erstellt, indem Sie die Liste der Blöcke und die entsprechenden Regeln auswählen. Die Daten für die Regeln können entweder statisch oder dynamisch zur Laufzeit aus dem RefD-Framework abgerufen werden.
- Schaffung von Compliance-Arbeitsplätzen: Compliance-Jobs werden durch Auswahl einer Richtlinie und einer Asset-Gruppe (die eine Liste der Ressourcen enthält) erstellt, um die Compliance-Prüfung durchzuführen. Benutzer können die Gerätekonfiguration aus dem Backup-Framework abrufen oder während der Ausführung Live-Befehle über Prozessvorlagen auf den Geräten ausführen. Das Abrufen der Konfiguration aus dem Backup hilft bei der Offline-Überprüfung von Geräten, ohne dass eine Verbindung zu einem Live-Gerät hergestellt werden muss. Die Jobs können geplant oder bei Bedarf ausgeführt werden.
- Verstöße gegen die Compliance: Compliance-Verletzungen können im Dashboard angezeigt werden.

# Übersicht über die Ressourceneinhaltung

Die Registerkarte "Übersicht über die Ressourcenkonformität" ist eine wichtige Funktion, die einen umfassenden Überblick über die Verstöße gegen die Richtlinien über alle Geräte im Netzwerk bietet. Auf dieser Registerkarte können Benutzer Compliance-Probleme schnell identifizieren und sicherstellen, dass alle Geräte die festgelegten Richtlinien und Standards einhalten. Die Schnittstelle verfügt über leistungsstarke Filter- und Suchfunktionen, die die Navigation und Analyse von Compliance-Daten vereinfachen.

## Wichtigste Funktionen

- Verletzungszusammenfassung pro Gerät: Die Registerkarte zeigt eine zusammengefasste Ansicht der Compliance-Verletzungen für jedes Gerät an. So erhalten Benutzer einen schnellen Überblick über den Compliance-Status insgesamt, der nach Schweregraden wie "Kritisch", "Hoch", "Mittel" und "Gering" kategorisiert ist.
- Detaillierte Informationen zu Verletzungen: Für jedes Gerät enthält das Popup-Fenster detaillierte Informationen zu den verletzten Richtlinien, und der Benutzer kann einen weiteren Drilldown in den Block und die Konfigurationszeile durchführen, die die Verletzung verursacht haben.

Übersicht über die Ressourceneinhaltung anzeigen

- Erweiterte Filteroptionen: Mit den Filtern oben und links auf der Registerkarte können Benutzer die im Raster angezeigten Daten eingrenzen. Benutzer können nach Datumsbereich, Asset-Gruppe, Produktfamilie und mehr filtern und so eine fokussierte Analyse von Compliance-Daten ermöglichen.
- Suchfunktion: Es steht ein Suchfeld zur Verfügung, um die Daten im Raster weiter zu verfeinern. Benutzer können durch Eingabe relevanter Schlüsselwörter oder Ausdrücke schnell nach bestimmten Geräten suchen oder diese über den Controller verwalten.
- Anpassbarer Datumsbereich: Standardmäßig wird der aktuelle Monat im Datumsbereichsfilter ausgewählt, und es werden die aktuellsten Konformitätsdaten bereitgestellt. Benutzer können den Datumsbereich jedoch anpassen, um Daten

anzuzeigen.

- Filter: Es stehen mehrere Filter zur Verfügung, z. B. Produktfamilie, Asset-Gruppe und Audit-Typ. Wenden Sie den Filter an, um das Raster zu aktualisieren.


Übersicht über die Ressourceneinhaltung

- Als CSV exportieren: Eine Funktion, mit der Benutzer eine lokale Kopie der Ressourcenkonfigurations-Compliance für Offline-Analysen, Berichte und Archivierungszwecke erhalten. Um Daten als CSV-Datei zu exportieren, wählen Sie Als CSV exportieren aus dem Symbol Weitere Optionen. Die heruntergeladene CSV-Datei enthält die Daten, die derzeit im Raster angezeigt werden, wobei alle angewendeten Filter berücksichtigt werden.


Zusammenfassung der Ressourcen-Compliance: Als CSV exportieren

## CSV-Dateidetails für Asset Compliance

Die CSV-Datei enthält alle Spalten, die im Raster "Übersicht über die Asset-Compliance" sichtbar sind, wie Gerätename, Controller-Instanz (verwaltet von), Produktfamilie des Geräts, Geräte-Compliance-Status, Anzahl der Verstöße nach Schweregrad (z. B. Kritisch, Schwer, Gering, Warnung, Info, Unbekannt) und Datum, an dem die Konformität zuletzt für das Gerät überprüft wurde.

Wenn das Raster eine Seitenumrandung aufweist, umfasst der Export alle Datensätze auf den Seiten, nicht nur die sichtbare Seite.

## Öffnen und Verwenden der CSV-Datei für die Asset-Compliance

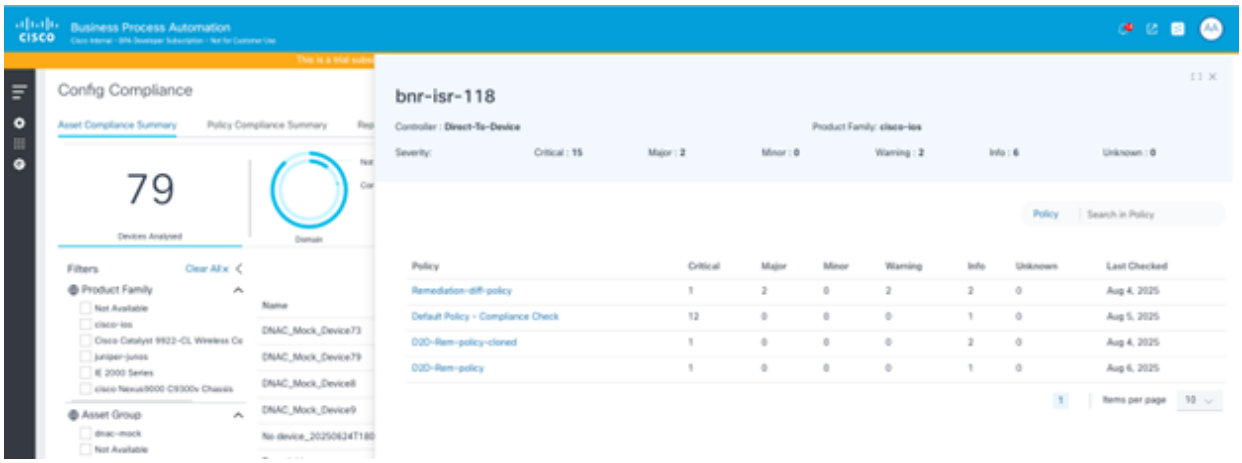
1. Öffnen Sie die heruntergeladene CSV-Datei in Excel oder einer anderen kompatiblen Tabellenkalkulationsanwendung.
2. Stellen Sie sicher, dass der Inhalt mit dem übereinstimmt, was im Raster Übersicht über die Asset-Compliance angezeigt wird, einschließlich gefilterter Ergebnisse.

| | 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 | | | | | | | | | | | |

Zusammenfassung der Ressourcen-Compliance: CSV-Datei in Excel-Anwendung geöffnet

Übersicht über die Ressourcenkonformität nach Richtlinie anzeigen

Wenn Sie auf eine Zeile im Raster "Übersicht über die Einhaltung der Geräte" klicken, werden die Details der Verletzungen der Geräte angezeigt, die nach den verschiedenen Richtlinien kategorisiert sind, für die das Gerät validiert wurde. Dies dient als Detailansicht, in der Benutzer die Anzahl der Verletzungen nach Schweregrad in jeder Richtlinie anzeigen können.



Zusammenfassung der Ressourcen-Compliance: Compliance-Zusammenfassung nach Richtlinie

---

Anmerkung: Folgendes sollte beachtet werden.
- Über den Hyperlink in der Spalte "Policy" werden die Benutzer zur Seite mit den Richtliniendetails geleitet.
- Wenn Sie auf eine Zeile klicken, wird die Seite mit den Details zur Verletzung der ausgewählten Richtlinie angezeigt.

---

## Anzeigen von Verletzungsdetails

Auf der Seite Verletzungsdetails werden Verstöße auf Block- und Regelebene angezeigt, die der Gerätekonfiguration überlagert sind. Darüber hinaus können Benutzer die Blockkonfiguration und die empfohlenen Wiederherstellungskonfigurationen anzeigen.

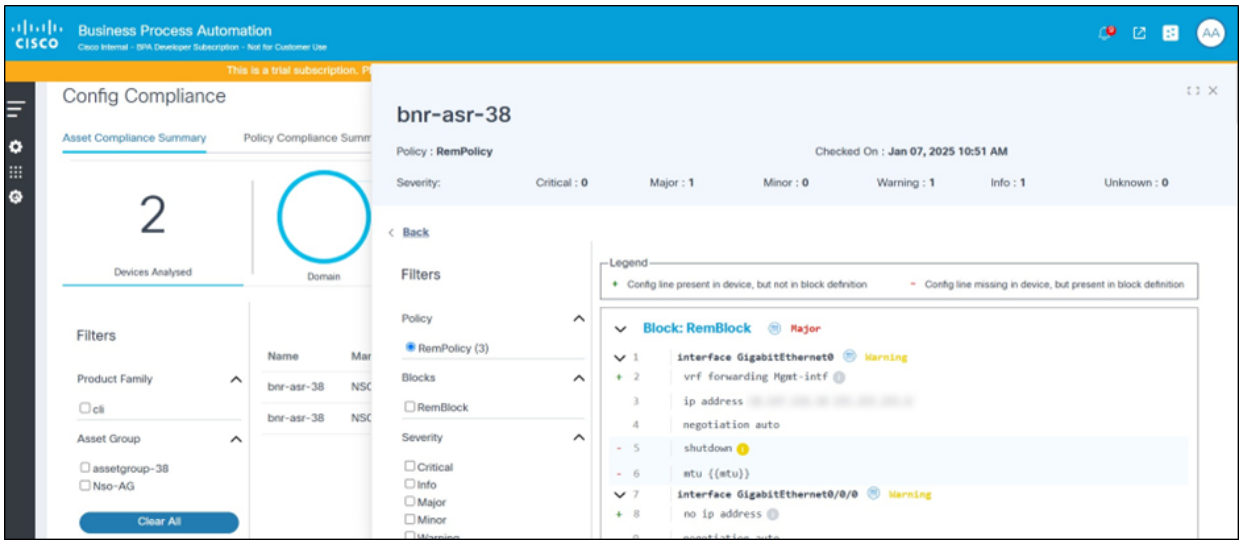
So zeigen Sie die Seite "Verletzungsdetails" auf der Seite "Übersicht Anlagenkonformität" zusammen mit der Aufteilung auf Richtlinienebene an:

1. Wählen Sie eine Zeile im Raster Asset Compliance. Ein Popup-Fenster wird angezeigt. Das Raster zeigt eine Aufteilung der Compliance-Details nach Richtlinie an.
2. Wählen Sie eine Zeile im Raster aus. Die Seite "Details zur Verletzung" wird angezeigt.

So zeigen Sie die Seite "Details zu Verletzungen" im Raster Zusammenfassung Richtlinienkonformität an:

1. Wählen Sie das Raster für Richtlinienkonformität aus.
2. Wählen Sie eine Zeile > Raster für betroffene Ressourcen.
3. Wählen Sie eine Zeile aus. Die Seite "Details zu Verletzungen" wird angezeigt.

Auf der rechten Seite der Seite "Violations Details" (Verletzungsdetails) werden die Gerätekonfigurationsblöcke angezeigt, und die Verletzungen werden darüber gelegt. Verstöße werden in Bezug auf die entsprechenden Konfigurationszeilen aufgeführt. Im Fall eines Fehlers enthält das Menüband für die Verletzung Details zum Regelnamen, zur Bedingung und zur erwarteten Konfiguration (wie in der Regel definiert) im Vergleich zur aus der Gerätekonfiguration abgerufenen Konfiguration.



Verstöße gegen die Ressourcen-Compliance

Blocksymbole

- Ein "+"-Zeichen für eine Leitung bedeutet, dass die Konfiguration nicht gemäß der Blockkonfiguration erwartet wird, sondern zusätzlich in der Gerätekonfiguration vorhanden ist.
- Ein "-"-Zeichen für eine Leitung impliziert, dass die Konfiguration gemäß der Blockkonfiguration erwartet wird, in der Gerätekonfiguration jedoch fehlt.

Filter

Der Filterabschnitt auf der linken Seite ermöglicht es Benutzern, die folgenden Aktionen auszuführen:

- Ändern Sie die Richtlinie. Dadurch wird die Seite aktualisiert und die Verletzungen für die neu ausgewählte Richtlinie geladen.
- Aktivieren Sie die Kontrollkästchen Blöcke, um die für die ausgewählten Blöcke relevanten Verletzungen anzuzeigen.
- Aktivieren Sie die Kontrollkästchen Severity (Schweregrad), um Verletzungen mit bestimmten Schweregraden anzuzeigen.
- Aktivieren Sie die Kontrollkästchen Verletzungstyp, um Verletzungen des ausgewählten Typs anzuzeigen:
  - Nicht übereinstimmende Bestellung: Die Reihenfolge der Gerätekonfigurationsposten stimmt nicht mit der in der Blockkonfiguration definierten Reihenfolge überein.
  - Fehlende Konfiguration: Konfigurationszeilen anzeigen, die gemäß der Blockkonfiguration erwartet werden, in der Gerätekonfiguration jedoch fehlen
  - Zusätzliche Konfiguration: Konfigurationszeilen anzeigen, die nicht gemäß der Blockkonfiguration erwartet werden, aber zusätzlich in der Gerätekonfiguration vorhanden sind
  - Regelfehler: Fehler einer oder mehrerer Bedingungen in Regeln.

- Fehlende Blöcke: Der gesamte Gerätekonfigurationsblock fehlt oder stimmt nicht mit der definierten Blockkonfiguration überein.
- Übersprungene Blöcke: Dieser Konfigurationsblock wird übersprungen, da die Filterbedingungen des Blocks nicht erfüllt sind.

## Anzeigen und Vergleichen von Korrekturkonfigurationen

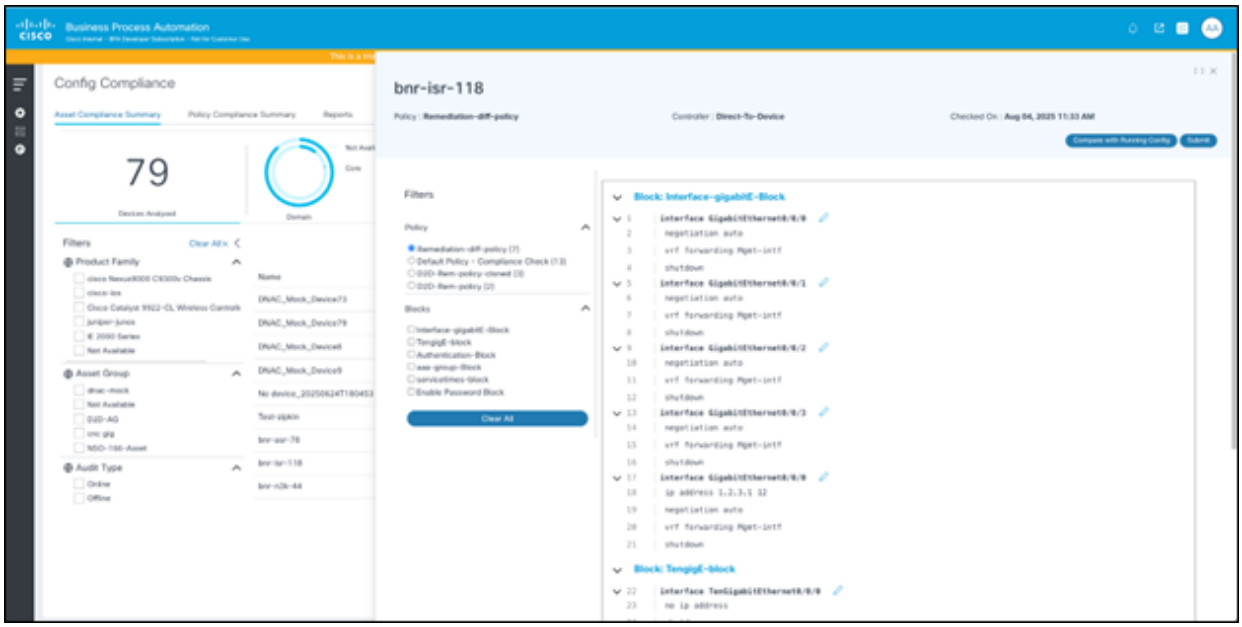
Auf der Seite Remediation Config (Bereinigungskonfiguration) wird die generierte Konfiguration für das ausgewählte Gerät für jeden Block in einer bestimmten Richtlinie angezeigt. Die Konfiguration wird generiert und berücksichtigt die Block- und Regeldetails in der Richtlinie sowie die Gerätekonfiguration, die während der Compliance-Ausführung abgerufen wurde. Benutzer haben auf derselben Seite die Möglichkeit, die Konfiguration zu aktualisieren. Diese generierte Konfiguration kann mithilfe der Funktion zur Problembehebung per Push an das Gerät gesendet werden. Darüber hinaus bietet diese Seite Benutzern die Möglichkeit, die generierte Konfiguration mit der aktuellen Gerätekonfiguration zu vergleichen. Der Benutzer kann einen oder mehrere Befehle angeben, um die aktuelle Gerätekonfiguration abzurufen.

So zeigen Sie die Seite "Remediation Config" (Wiederherstellungskonfiguration) im Raster "Asset Compliance" an:

1. Klicken Sie auf die Registerkarte Übersicht über die Asset-Konformität.
2. Wählen Sie im Raster "Ressourcenkonformität" in der Spalte "Aktion" das Symbol "Weitere Optionen" > "Korrekturkonfiguration anzeigen". Die Seite "Problembehebungskonfiguration" wird angezeigt.

So zeigen Sie die Seite "Remediation Config" im Raster "Policy Compliance" an:

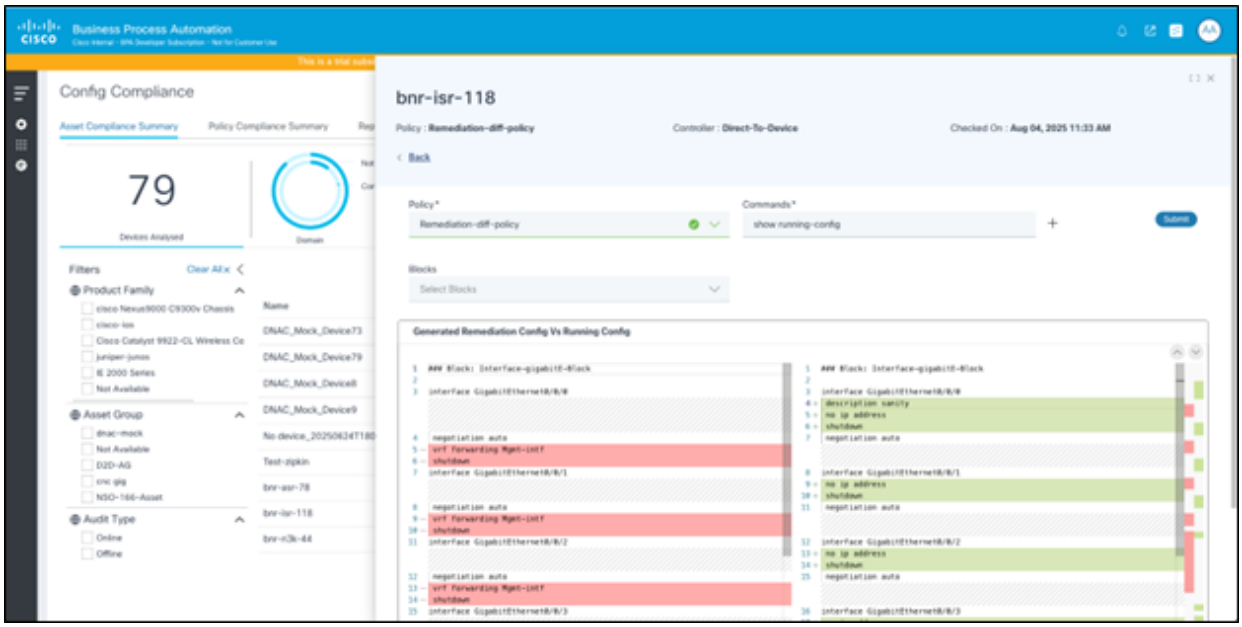
1. Klicken Sie auf die Registerkarte "Übersicht Richtlinienkonformität".
2. Wählen Sie im Raster für die Richtlinienkonformität die gewünschte Zeile aus. Das Raster "Betroffene Ressourcen" wird angezeigt.
3. Wählen Sie in der Spalte "Aktion" das Symbol Weitere Optionen > Wählen Sie Korrekturkonfiguration anzeigen aus. Die Seite "Problembehebungskonfiguration" wird angezeigt.




Seite "Problembehebungskonfiguration"

Auf der Seite Remediation Config (Bereinigungskonfiguration) wird Folgendes angezeigt:

- Generierte Behebungskonfiguration: Die generierte Konfiguration wird rechts auf der Seite angezeigt. Außerdem haben Benutzer die Möglichkeit, die Konfigurationsblöcke zu bearbeiten und die zu speichernden Änderungen zu übermitteln.
- Filter: Die Filter können verwendet werden, um eine Richtlinie auszuwählen und anschließend optional einen oder mehrere Blöcke auszuwählen, um die entsprechende generierte Konfiguration anzuzeigen.
- Vergleich mit laufender Konfiguration: Klicken Sie auf Mit laufender Konfiguration vergleichen, um eine detaillierte Seite anzuzeigen, auf der Benutzer die generierte Konfiguration mit der aktuellen Gerätekonfiguration vergleichen können.




Seite "Mit laufender Konfiguration vergleichen"

Auf der Seite "Mit laufender Konfiguration vergleichen" wird Folgendes angezeigt:

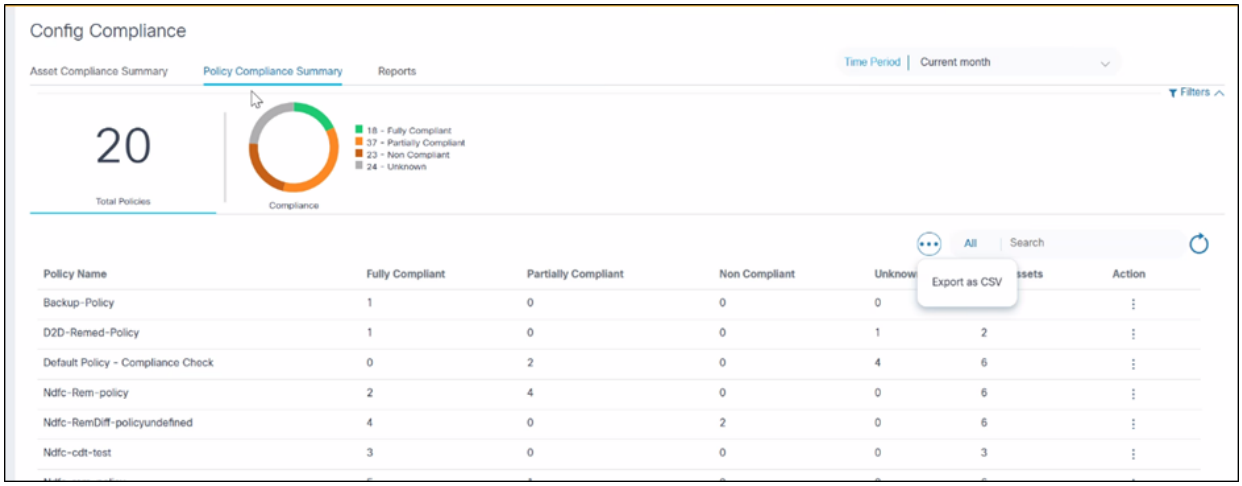
- Option zur Auswahl einer Richtlinie: Die auf der vorherigen Seite ausgewählte Richtlinie ist vorausgewählt.
- Ein Textfeld zur Eingabe eines oder mehrerer auf dem Gerät auszuführender Befehle
- Eine Schaltfläche "Senden", um die Befehle auf dem Gerät auszuführen und die Konfiguration abzurufen.
- Option zum Anzeigen und Filtern von Blöcken: Standardmäßig werden alle Blöcke in der Richtlinie angezeigt. Benutzer können bei Bedarf einzelne Blöcke auswählen.
- Config Diff Viewer zur parallelen Anzeige der generierten Konfiguration und Gerätekonfiguration mit Highlights zu den Unterschieden

## Zusammenfassung der Richtlinienkonformität

Die Registerkarte "Übersicht zur Richtlinienkonformität" bietet einen klaren und präzisen Überblick über den Compliance-Status von Geräten mit definierten Richtlinien. Auf dieser Registerkarte können Benutzer schnell die Compliance-Landschaft bewerten und Problembereiche identifizieren. Die Registerkarte kategorisiert Geräte nach ihrem Compliance-Status, sodass die Compliance für kurze Zeit verständlich und einfach zu verwalten ist.

Compliance-Status:

- Vollständig konform: Alle Geräte erfüllen alle Compliance-Regeln für die jeweilige Richtlinie.
- Teilweise konform: Einige Geräte erfüllen die Regeln, andere nicht.
- Nicht konform: Keine Geräte erfüllen die Richtlinien.
- Unbekannt: Die Richtlinie kann aufgrund von Problemen mit der Netzwerkverbindung oder fehlender Backups nicht auf Konformität überprüft werden.



Zusammenfassung der Richtlinienkonformität mit CSV-Export

## Als CSV exportieren für Richtlinienkonformität

Mit der Funktion Als CSV exportieren können Benutzer eine lokale Kopie der Richtlinien-Compliance für Offline-Analysen, Berichte und Archivierungszwecke erhalten. Um Daten als CSV-Datei zu exportieren, wählen Sie Als CSV exportieren aus dem Symbol Weitere Optionen. Die heruntergeladene CSV-Datei enthält die Daten, die derzeit im Raster angezeigt werden, wobei alle angewendeten Filter berücksichtigt werden.

## CSV-Dateidetails für Richtlinienkonformität

Die CSV-Datei enthält den Richtliniennamen, die Gesamtzahl der validierten Ressourcen und die Aufschlüsselung der Anzahl nach Compliance-Status (d. h. vollständig konform, teilweise konform, nicht konform und unbekannt). Wenn das Raster eine Seitenumrandung aufweist, umfasst der Export alle Datensätze auf allen Seiten, nicht nur die auf der aktuellen Seite angezeigten.

## Öffnen und Verwenden der CSV-Datei zur Einhaltung von Richtlinien

1. Öffnen Sie die heruntergeladene CSV-Datei in Excel oder einer anderen kompatiblen Tabellenkalkulationsanwendung.
2. Stellen Sie sicher, dass der Inhalt mit dem übereinstimmt, was im Raster Zusammenfassung der Richtlinienkonformität angezeigt wird, einschließlich gefilterter Ergebnisse.

| | 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 | | | | | | |

Richtlinienkonformität: Richtliniendetails

Anzeigen von Richtliniendetails

Richtliniendetails anzeigen:

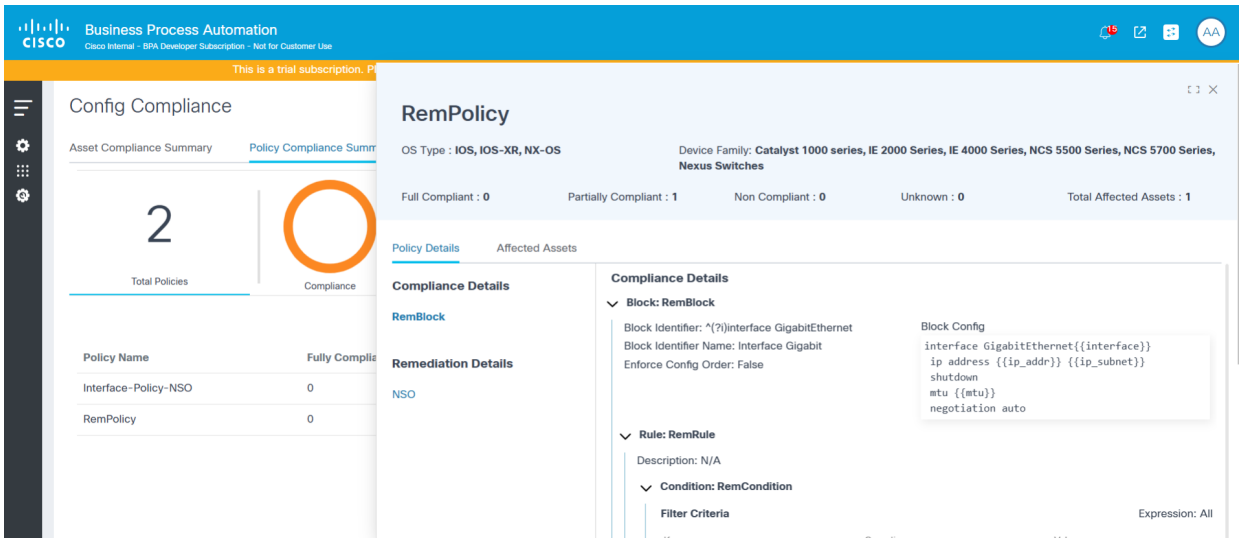
1. Wählen Sie eine Richtlinie aus dem Symbol Weitere Optionen in der Spalte Aktion aus.

2. Wählen Sie Richtliniendetails anzeigen aus. Die Seite "Policy Details" wird angezeigt.

---

Anmerkung: Die Seite "Policy Details" ist eine schreibgeschützte Ansicht aller Richtlinieninformationen, einschließlich Blöcken, Regeln und Bedingungen. Benutzer können auf Hyperlinks innerhalb der Seite klicken, die direkt zum entsprechenden Block navigieren.

---



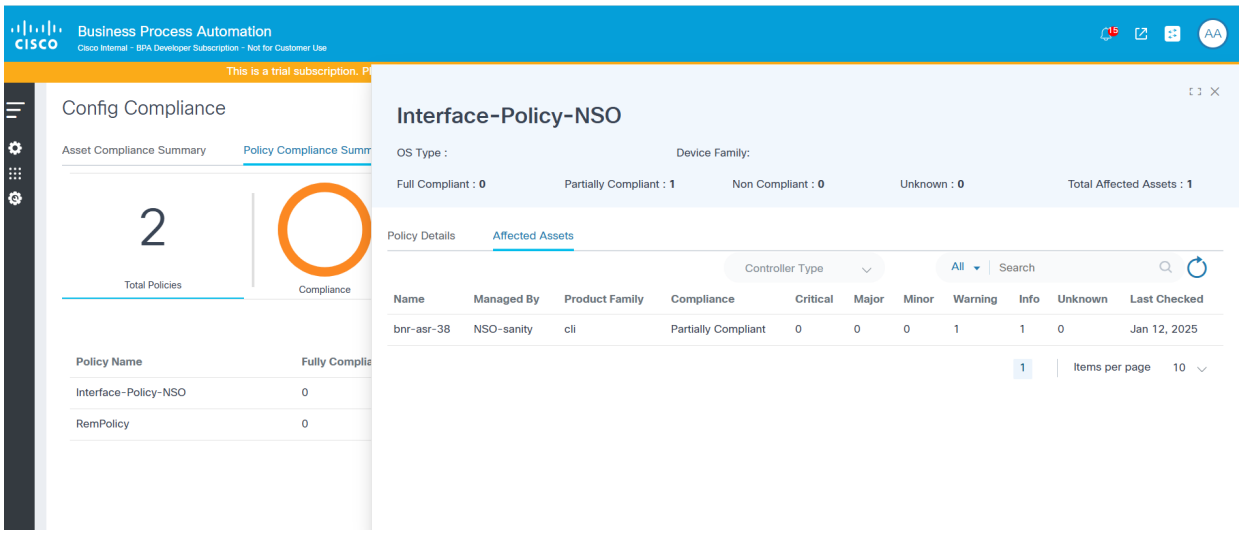
Richtlinienkonformität: Richtliniendetails

Betroffene Ressourcen anzeigen

Auf der Registerkarte "Betroffene Ressourcen" werden die Liste der gemäß jeder Richtlinie analysierten Ressourcen und die Anzahl der Verstöße nach Schweregrad aufgeteilt angezeigt. Geräte können über die Dropdown-Liste Controller Type (Controller-Typ) und das Suchfeld gefiltert werden.

So zeigen Sie Betroffene Ressourcen über die Registerkarte Zusammenfassung Richtlinienkonformität an:

1. Wählen Sie eine Zeile aus. Das Fenster Compliance Policy (Compliance-Richtlinie) wird geöffnet.
2. Klicken Sie auf die Registerkarte Betroffene Ressourcen.




Richtlinienkonformität: Betroffene Ressourcen

Anmerkung: Die Registerkarte Betroffene Ressourcen enthält Aktionen zum Öffnen der Seiten Verletzungsdetails anzeigen und Problembehebungskonfiguration anzeigen. Weitere Informationen finden Sie unter Übersicht über die Asset-Konformität.

# Berichte

Der Abschnitt "Berichte" soll umfassende Einblicke in die Geräte-Compliance bieten, Verletzungen identifizieren und die Problembehebung erleichtern. Die Anwendung bietet eine benutzerfreundliche Oberfläche zum Generieren, Anzeigen, Herunterladen und Verwalten verschiedener Arten von Compliance-Berichten.

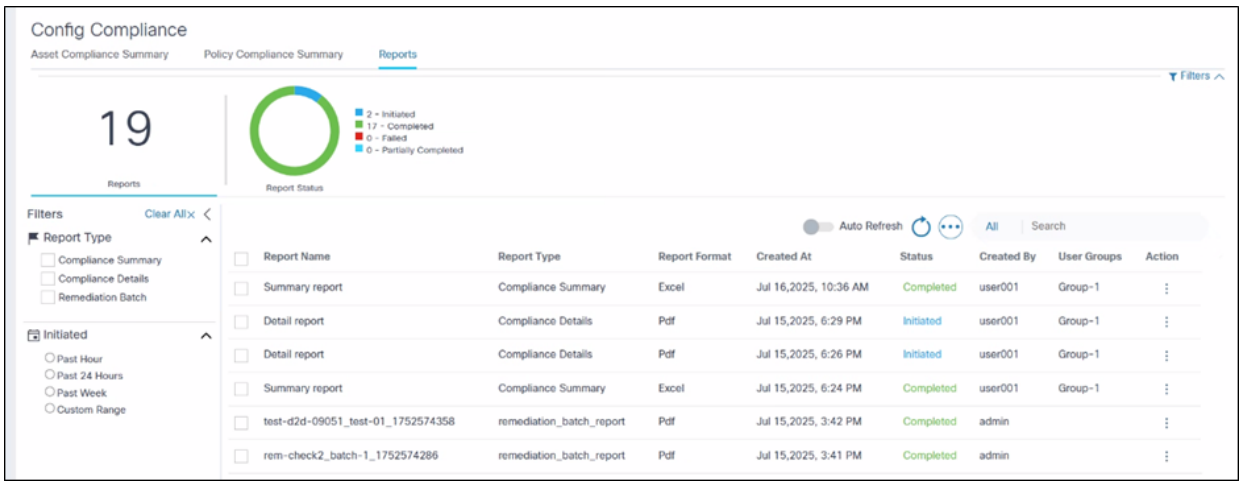
## Reporting-Dashboard

Das Reporting Dashboard dient als zentrale Anlaufstelle für alle Compliance-Reporting-Aktivitäten. Über diese zentrale Benutzeroberfläche können die Benutzer ihre Berichte effizient verwalten. Zu den wichtigsten Funktionen des Berichts-Dashboards gehören:

- Anzeigen von Berichten: Benutzer können eine Liste aller erstellten Berichte anzeigen, einschließlich Name, Typ, zugehöriger Richtlinie, Format, Erstellungsdatum und aktuellem Status (z. B. Initiiert, Abgeschlossen, Fehlgeschlagen, Teilweise Abgeschlossen)
- Herunterladen von Berichten: Nach der Erstellung können Berichte für Offline-Analysen oder zur Archivierung heruntergeladen werden. Die Spalte Aktion enthält Optionen zum Herunterladen.
- Berichte löschen: Benutzer haben die Möglichkeit, alte oder unnötige Berichte aus dem Dashboard zu entfernen, um eine saubere und organisierte Berichtsumgebung zu erhalten.
- Filterung und Suche: Das Dashboard bietet umfangreiche Filteroptionen, mit denen Benutzer bestimmte Berichte anhand von Kriterien wie Berichtstyp (z. B. Compliance-Details,

Compliance-Zusammenfassung, Behebungsstapel), Richtlinie und Initiierungsstatus (z. B. Letzte Stunde, Letzte 24 Stunden, Letzte Woche, Benutzerdefinierter Bereich) schnell finden können. Eine Suchleiste ist ebenfalls verfügbar.
- Statusüberwachung des Berichts: Eine visuelle Zusammenfassung (d. h. ein Tortendiagramm) gibt den Status von Berichten an und zeigt an, wie viele Berichte initiiert, abgeschlossen, fehlgeschlagen oder teilweise abgeschlossen wurden.

Das Reporting-Dashboard ist die Landing Page auf der Registerkarte "Reports" (Berichte) im Dashboard für Compliance und Problembehebung.



Berichte-Dashboard

- Zu den verfügbaren Berichtstypen gehören:
  - Zusammenfassender Bericht zur Compliance
  - Detaillierter Compliance-Bericht
  - Behebungs-Batch-Bericht
- Verwenden Sie Filter, um Folgendes auszuwählen:
  - Berichtstyp
  - Richtlinie
  - Initiated Time period (die Berichtsliste wird basierend auf dem ausgewählten Zeitrahmen gefiltert)
- Option zum automatischen Aktualisieren der Berichtsliste

## Reporting-Konfigurationen

Mithilfe von Berichtskonfigurationen können Administratoren wichtige Parameter für die Berichterstellung konfigurieren, die auf der Bereitstellung und den geschäftlichen Anforderungen basieren. Die folgenden Parameter stehen für die Konfiguration zur Verfügung:

- Berichte automatisch löschen nach (Tage): Alle Berichte, die älter als diese Dauer sind, werden aus dem System gelöscht.

- Max. Anzahl von Blöcken, die pro Richtlinie in einem zusammenfassenden Konformitätsbericht ausgewählt werden: Hilft, die Anzahl der Registerkarten in der Excel-Datei auf ein lesbares Limit zu begrenzen
- Max. Anzahl der in einem detaillierten Bericht zur Compliance auszuwählenden Ressourcen: Hilft, die Anzahl der für einen bestimmten detaillierten Bericht generierten PDF-Dateien zu begrenzen

Liste der Compliance-Aufträge

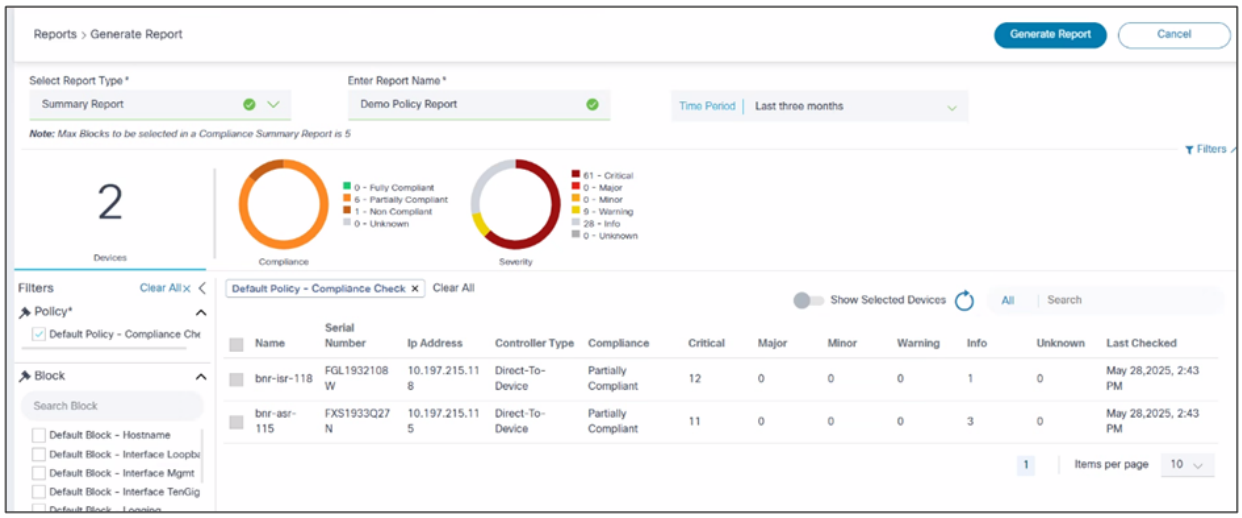
## Berichte erstellen

Die Anwendung stellt eine dedizierte Schnittstelle zum Generieren neuer Compliance-Berichte bereit, über die Benutzer den Berichtstyp auswählen, den Umfang definieren und bestimmte Filter anwenden können. Der Prozess zur Berichterstellung wird über die Aktion "Bericht erstellen" auf der Seite "Reporting Dashboard" gestartet.

Wichtigste Aspekte der Berichterstellung:

- Berichtstyp auswählen: Benutzer können zwischen den folgenden Berichtstypen wählen:
  - Zusammenfassender Bericht: Bietet einen Überblick über die Compliance auf allen Geräten für die ausgewählten Richtlinien
  - Detaillierter Bericht: Bietet eine detaillliertere Ansicht mit detaillierten Informationen zu spezifischen Verletzungen für jedes Gerät
- Benennen des Berichts: Der Benutzer muss einen relevanten Namen für den generierten Bericht angeben.
- Zeitperiodenauswahl: Berichte können für bestimmte Zeitrahmen erstellt werden, z. B. "Aktueller Monat" oder benutzerdefinierte Bereiche, um sich auf die neuesten Compliance-Daten zu konzentrieren.
- Anwenden von Filtern: Umfassende Filteroptionen ermöglichen es Benutzern, den Umfang des Berichts einzugrenzen.
  - Richtlinie: Wählen Sie mindestens eine Konformitätsrichtlinie aus, die in den Bericht aufgenommen werden soll. Die Richtlinienauswahl ist obligatorisch.
  - Blockieren: Wählen Sie innerhalb der ausgewählten Richtlinien bestimmte Konfigurationsblöcke aus, die in den Bericht aufgenommen werden sollen. Die Blockauswahl ist optional.
  - Asset-Gruppe: Benutzer können den Umfang der Ressourcen filtern, indem sie eine oder mehrere Asset-Gruppen auswählen.
- Ressourcenauswahl: Dies gilt nur für detaillierte Berichte.
  - Benutzer können bestimmte Geräte auswählen, für die der Bericht erstellt werden soll.
  - In der Anlagentabelle werden Details wie Name, Seriennummer, IP-Adresse, Verwaltet von und aktueller Konformitätsstatus mit Zählungen für unterschiedliche Schweregrade angezeigt

So erstellen Sie einen Konformitätsübersichtsbericht:

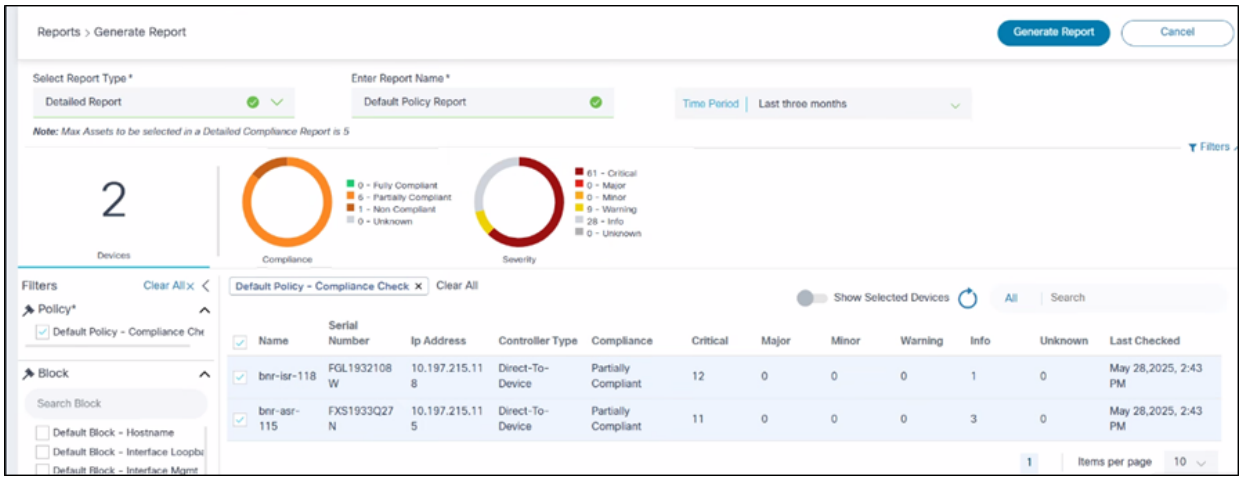


Zusammenfassungsbericht erstellen

1. Wählen Sie in der Dropdown-Liste "Berichtstyp auswählen" die Option Zusammenfassender Bericht aus.
2. Geben Sie einen Berichtsnamen ein.
3. Wählen Sie einen Zeitbereich aus. Die Richtlinien und Bausteine werden basierend auf dieser Auswahl aufgelistet.
4. Wählen Sie eine Richtlinie aus. Es können auch zusätzliche Richtlinien ausgewählt werden.
5. Wählen Sie optional Blöcke aus. Wenn keine Option ausgewählt ist, werden alle Blöcke eingeschlossen.
6. Wählen Sie erforderliche Ressourcengruppen, Compliance-Status und Schweregrade aus.
7. Klicken Sie auf Bericht erstellen.

- Auf der Seite mit der Berichtsliste wird der Berichtsstatus auf Initiiert gesetzt
- Nach Abschluss des Vorgangs ändert sich der Status in Abgeschlossen. Wenn einige Unterberichte fehlschlagen, wird der Status in "Teilweise abgeschlossen" geändert.
- Wenn die gesamte Berichterstellung fehlschlägt, wird eine Benachrichtigung angezeigt, und der Status ändert sich in Failed (Fehlgeschlagen).
- Nach Abschluss dieses Vorgangs ist die Download-Option verfügbar. Benutzer können eine ZIP-Datei herunterladen, die die Excel-Berichte enthält

So erstellen Sie einen detaillierten Compliance-Bericht:



Detaillierten Bericht erstellen

1. Wählen Sie in der Dropdown-Liste Berichtstyp auswählen die Option Detaillierter Bericht aus.
2. Geben Sie einen Berichtsnamen ein.
3. Wählen Sie einen Zeitbereich aus. Die Richtlinien und Bausteine werden basierend auf dieser Auswahl aufgelistet.
4. Wählen Sie eine Richtlinie aus. Es können auch zusätzliche Richtlinien ausgewählt werden.
5. Wählen Sie optional Blöcke aus. Wenn keine Option ausgewählt ist, werden alle Blöcke eingeschlossen.
6. Wählen Sie erforderliche Ressourcengruppen, Compliance-Status und Schweregrade aus.
7. Wählen Sie die erforderlichen Ressourcen aus dem Raster aus. Benutzer haben die Möglichkeit, alle Geräte auszuwählen und die ausgewählten Geräte anzuzeigen.
8. Klicken Sie auf Bericht erstellen.

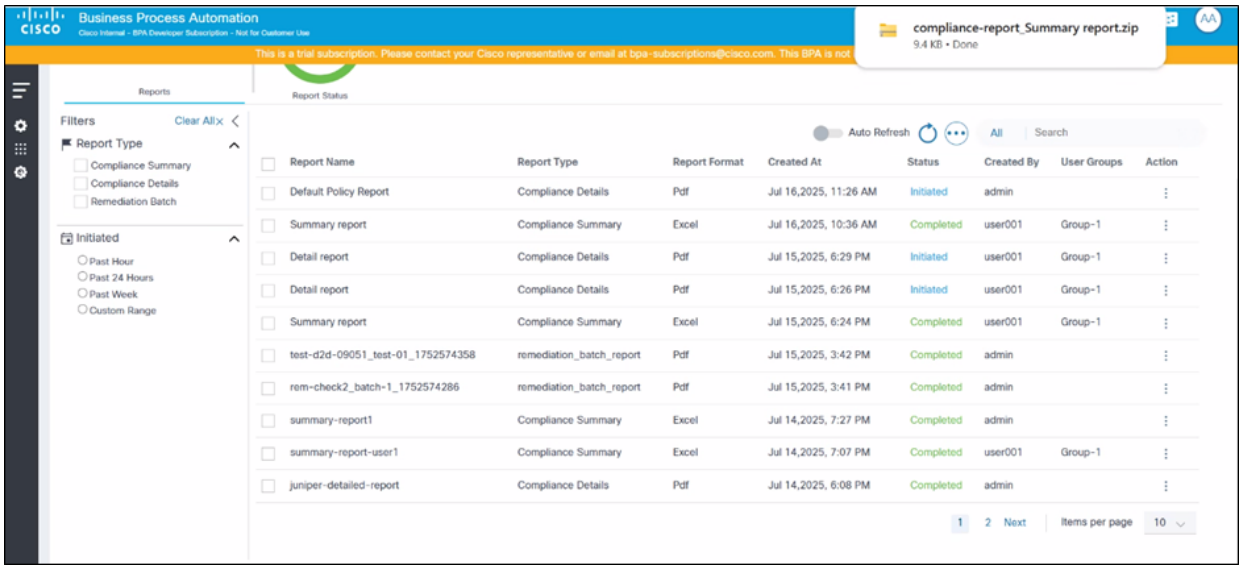
- Auf der Seite mit der Berichtsliste wird der Berichtsstatus auf Initiiert gesetzt
- Nach Abschluss des Vorgangs ändert sich der Status in Abgeschlossen. Wenn einige Unterberichte fehlschlagen, wird der Status in "Teilweise abgeschlossen" geändert.
- Wenn die gesamte Berichterstellung fehlschlägt, wird eine Benachrichtigung angezeigt, und der Status ändert sich in Failed (Fehlgeschlagen).

## Herunterladen und Anzeigen von Berichten

Abgeschlossene Berichte können über das Download-Symbol in der gewünschten Zeile des Reporting Dashboard-Rasters heruntergeladen werden.

Informationen zum zusammenfassenden Bericht zur Konfigurationskompatibilität

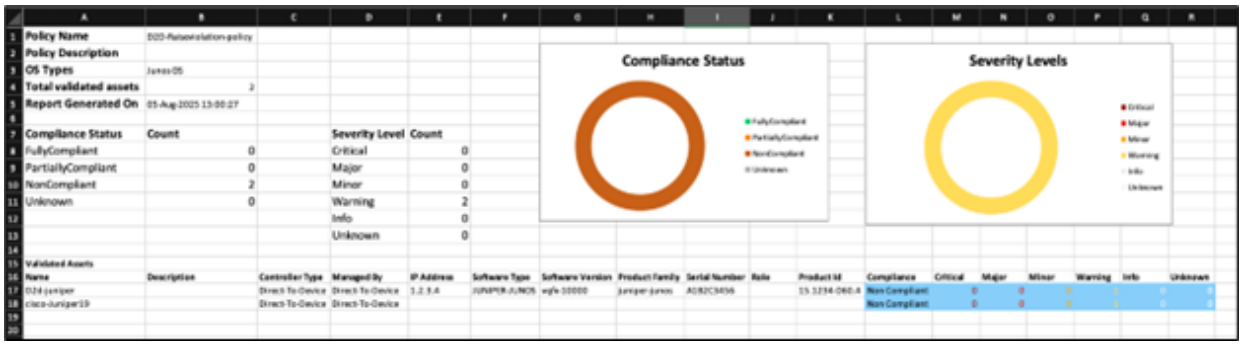
Der Compliance Summary-Bericht ist eine ZIP-Datei mit individuellen PDF-Berichten, wobei pro Gerät eine PDF generiert wird. Dieser Berichtstyp bietet einen Überblick über Richtlinienverstöße sowie Details zur Zuordnung von Verstößen auf Blockebene zu den Geräten.



Zusammenfassender Bericht zur Compliance

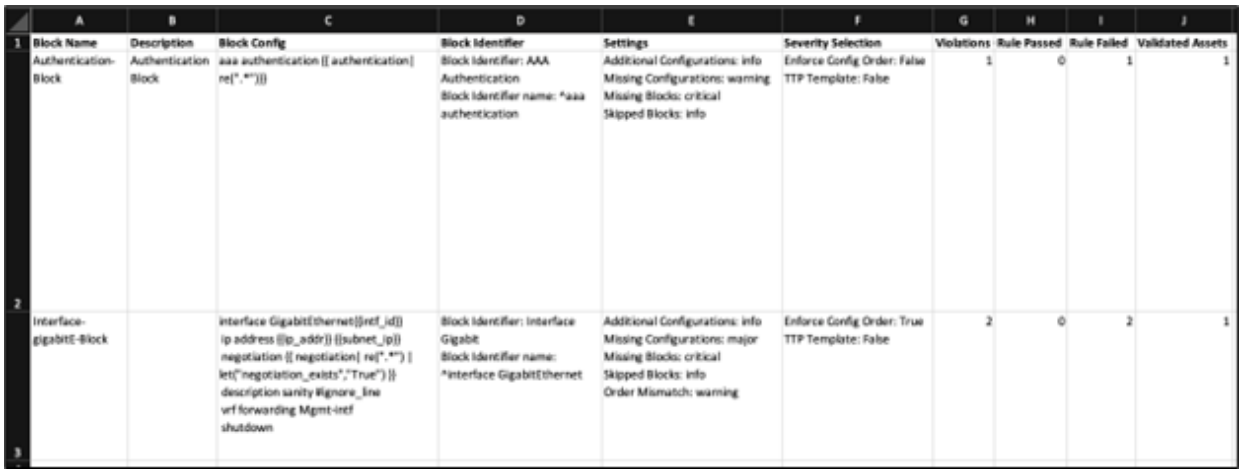
Jeder Excel-Bericht enthält die folgenden Tabellen und enthält die folgenden Informationen:

- Richtlinienübersicht:
  - Übersichtsdetails, z. B. Richtlinienname, Beschreibung, Betriebssystemtyp(en) und insgesamt validierte Ressourcen
  - Raster- und Diagrammansicht der Anzahl der validierten Ressourcen, aufgeteilt nach Konformitätsstatus (z. B. vollständig, teilweise, nicht konform und unbekannt)
  - Eine Raster- und Diagrammansicht der Gesamtanzahl der Verletzungen, aufgeteilt nach Schweregrad (z. B. Kritisch, schwerwiegend, untergeordnet, Warnungsinformationen und Unbekannt)
  - Ein Ressourcen-Grid mit Gerätedetails, Compliance-Status und Anzahl der Verstöße für jeden Schweregrad



Richtlinienübersicht

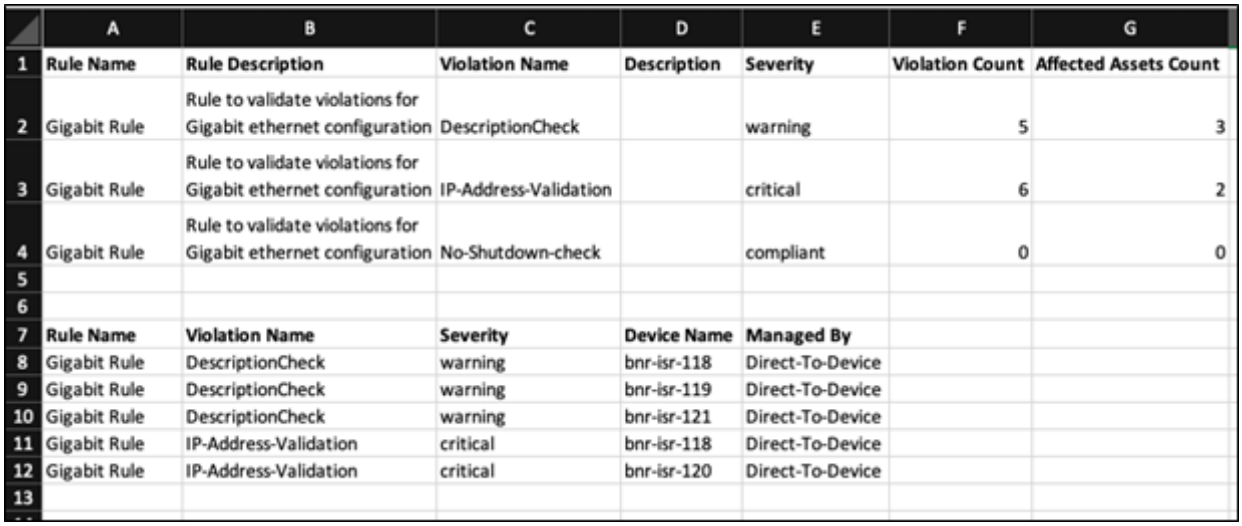
- Zusammenfassung sperren:
  - Blockdetails wie Blockname, Beschreibung, Blockkonfiguration, Blockbezeichner-Details und Einstellungen für den Schweregrad der Blockverletzung
  - Anzahl der Verletzungen, Regeln, Regeln, Fehler und validierte Ressourcen für den jeweiligen Block



| | 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<br>Block Identifier name: ^aaa authentication | Additional Configurations: info<br>Missing Configurations: warning<br>Missing Blocks: critical<br>Skipped Blocks: info | Enforce Config Order: False<br>TTP Template: False | 1 | 0 | 1 | 1 |
| 3 | Interface-gigabitE-Block | | interface GigabitEthernet{{intf_id}}<br>ip address {{ip_addr}} {{subnet_ip}}<br>negotiation {{ negotiation\| re(".*") \| let("negotiation_exists","True") }}<br>description sanity #ignore_line<br>vrf forwarding Mgmt-intf<br>shutdown | Block Identifier: Interface Gigabit<br>Block Identifier name: ^interface GigabitEthernet | Additional Configurations: info<br>Missing Configurations: major<br>Missing Blocks: critical<br>Skipped Blocks: info<br>Order Mismatch: warning | Enforce Config Order: True<br>TTP Template: False | 2 | 0 | 2 | 1 |

Zusammenfassende Blockansicht

- Details zu Regeln und Verstößen pro Block:
- Im Raster für die Verletzungsstufe werden Regelnamen, Beschreibung, Verletzungsname, Beschreibung, Schweregrad, Anzahl der Verletzungen, die in den Ressourcen festgestellt wurden, und die Anzahl der betroffenen Ressourcen angezeigt.
- Das Raster auf Geräteebene zeigt die Zuordnung zwischen Regel, Verletzung, Schweregrad, Gerätename und Controller-Name (verwaltet von) an.



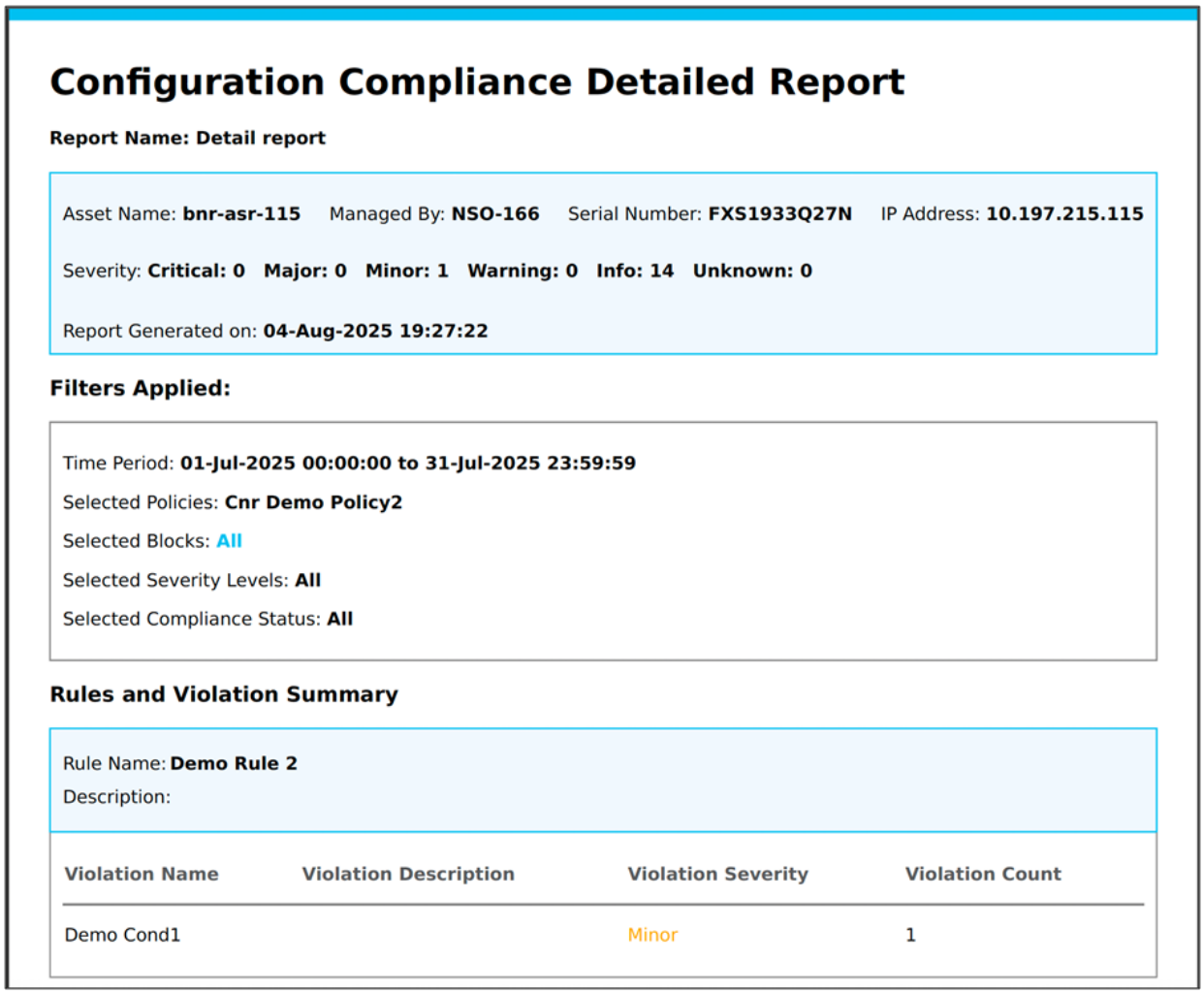
| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | Rule Name | Rule Description | Violation Name | Description | Severity | Violation Count | Affected Assets Count |
| 2 | Gigabit Rule | Rule to validate violations for Gigabit ethernet configuration | DescriptionCheck | | warning | 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 | | | | | | | |

Compliance-Detailbericht

Der Compliance-Detailbericht enthält folgende Informationen:

- Berichtsname: Identifiziert den Namen des Berichts.
  - Name der Ressource: Gibt das Gerät an, für das die Konformitätsprüfung durchgeführt wurde
  - Weitere Asset-Details: Beinhaltet Details wie die IP-Adresse und Seriennummer, falls vorhanden
  - Schweregrad: Bietet eine Übersicht über die Anzahl der Verletzungen nach Schweregrad
  - Bericht erstellt am: Gibt den Zeitstempel der Berichtserstellung an

- Filter angewendet: Beschreibt die Details spezifischer Filterkriterien, die zur Erstellung eines bestimmten Berichts verwendet werden, um Transparenz und Reproduzierbarkeit zu gewährleisten. Dies umfasst den Zeitraum, ausgewählte Richtlinien, Blöcke, Schweregrade und Compliance-Status.
- Zusammenfassung der Regeln und Verstöße: Führt alle ausgewerteten Regeln auf und liefert eine Zusammenfassung der für diese Regel gefundenen Verletzungen. Das Übersichtsraster zeigt den Verletzungsnamen, die Beschreibung, den Schweregrad und die Anzahl der Vorfälle dieser Verletzung.
- Details zur Verletzung: Bietet explizite Details zu jeder Gerätekonfigurationszeile für die ausgewählten Blöcke sowie Details zu Verstößen für jede Zeile



## 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**

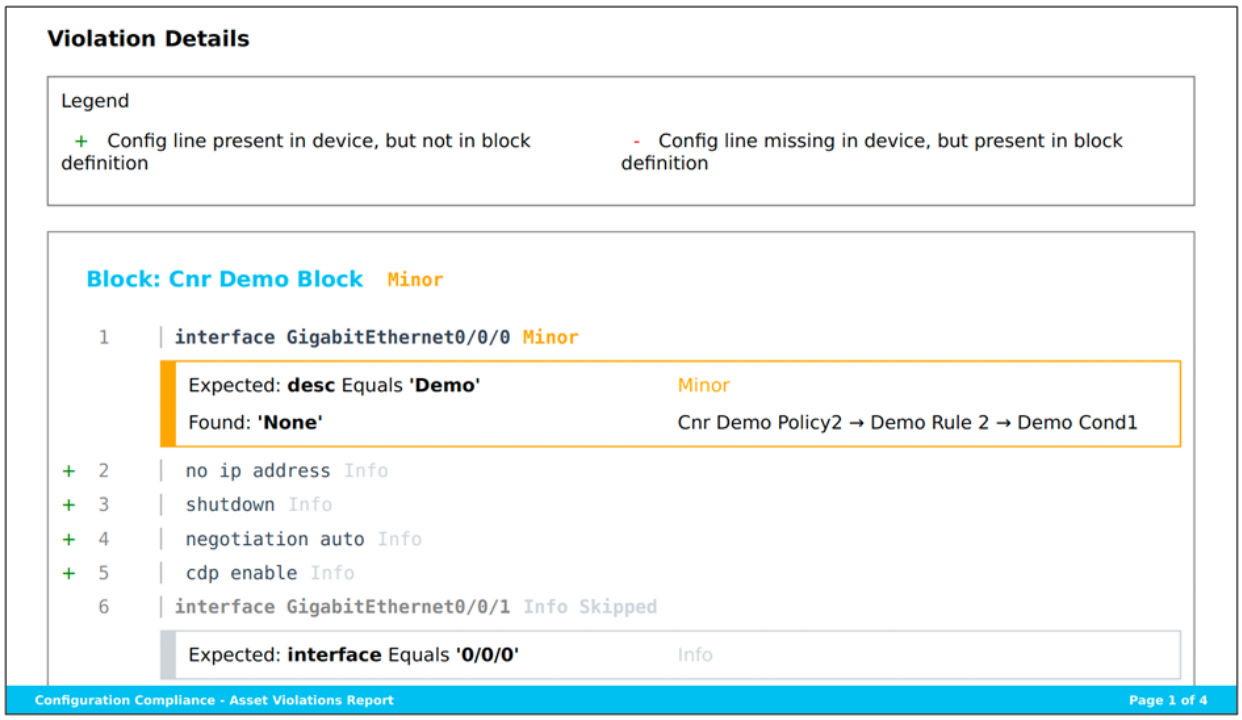
**Rules and Violation Summary**

Rule Name: **Demo Rule 2**

Description:

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

Detaillierter Compliance-Bericht - Beispiel für PDF Seite 1




Detaillierter Compliance-Bericht - Beispiel für PDF, Seite 2

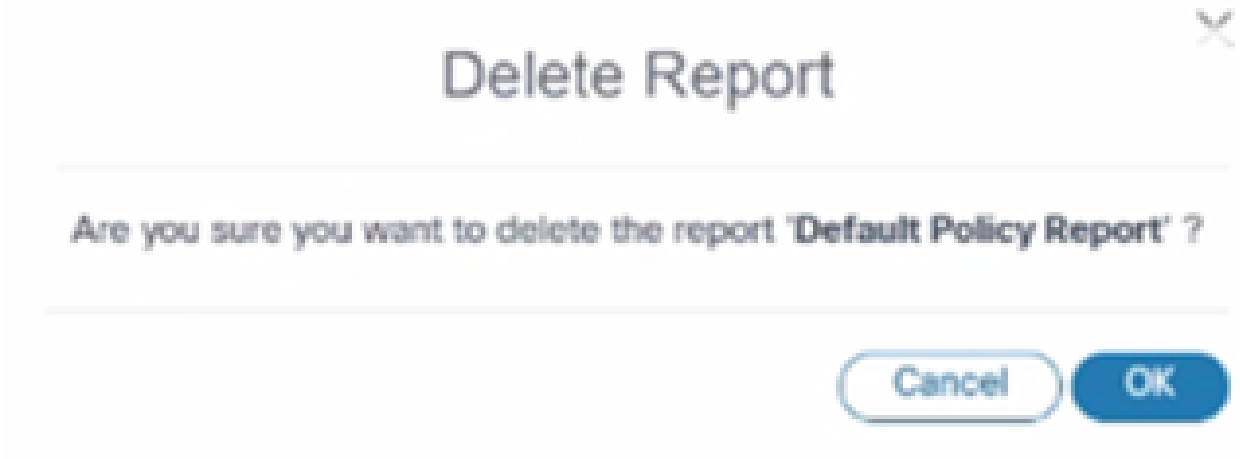
---

Anmerkung: Der PDF-Bericht für den Korrekturstapel, der auf der Seite "Korrekturstapel" erstellt wurde, kann ebenfalls heruntergeladen und in der Berichtsliste angezeigt werden.

---

## Berichte löschen

Berichte können einzeln gelöscht werden, indem Sie das Symbol Löschen auswählen oder indem Sie im großen Stil die Kontrollkästchen für die Berichte aktivieren und dann auf das Symbol Weitere Optionen klicken > Löschen.




Liste der Compliance-Aufträge

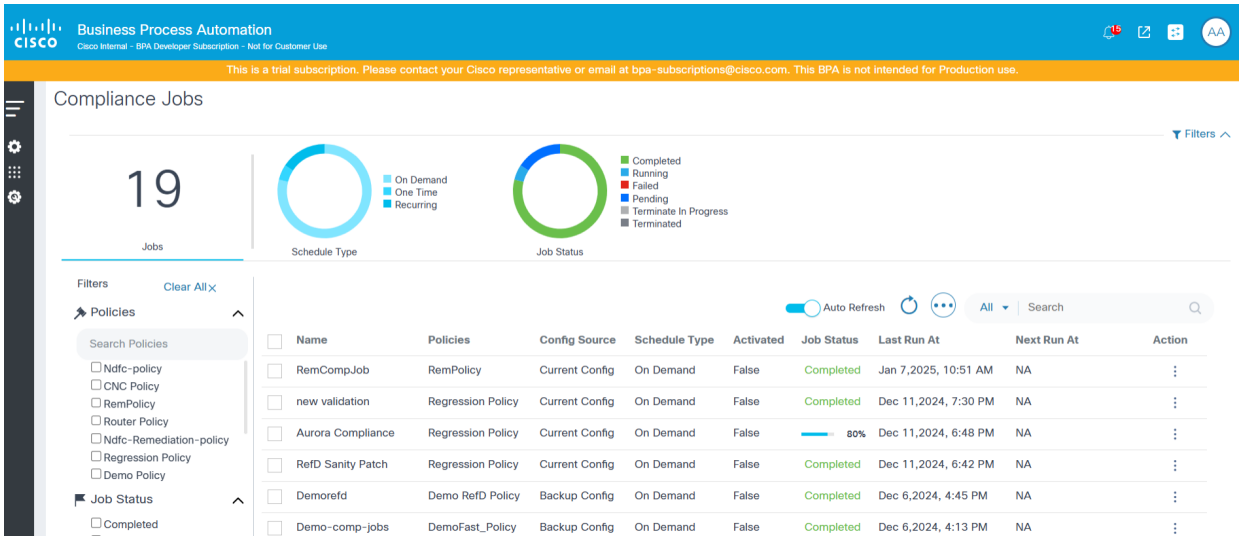
Anmerkung: Beim Löschen eines Berichts werden nur die Berichtsdateien und der Eintrag aus dem Berichts-Dashboard entfernt. die zugrunde liegenden Compliance-Ausführungsdetails werden beibehalten.

# Compliance-Jobs

Die Compliance Jobs-Funktion im Next-Gen-Portal soll Benutzern helfen, Compliance Jobs für ausgewählte Richtlinien und Ressourcengruppen zu erstellen, zu verwalten und auszuführen. Die Ausführung dieser Jobs kann in regelmäßigen Abständen geplant oder bedarfsgesteuert erfolgen, sodass alle Ressourcen konsistent auf ihre Konformität überprüft werden.

## Wichtigste Funktionen

- Compliance-Aufträge auflisten: Zeigen Sie alle definierten Compliance-Aufträge an, mit Optionen zum Offline-Audit, zum Filtern, Erstellen, Bearbeiten, Löschen und Ausführen von Aufträgen.
- Geplante Jobs und On-Demand-Jobs: Richten Sie Jobs so ein, dass sie in geplanten Intervallen ausgeführt werden, oder führen Sie sie bei Bedarf sofort aus.
- Detaillierte Zugriffskontrolle: Der Zugriff auf Compliance-Aufträge wird auf der Grundlage von Benutzerberechtigungen gesteuert. Dadurch wird sichergestellt, dass Benutzer nur Aufträge anzeigen, die mit Richtlinien verknüpft sind, auf die sie Zugriff haben.
- Filteroptionen: Zur einfacheren Navigation und Verwaltung können Jobs nach Richtlinien, Jobstatus, Zeitplantyp und Datumsbereich gefiltert werden.



Liste der Compliance-Aufträge

## Erstellen von Compliance-Jobs

Die Seite Compliance-Auftrag erstellen enthält die folgenden Attribute:

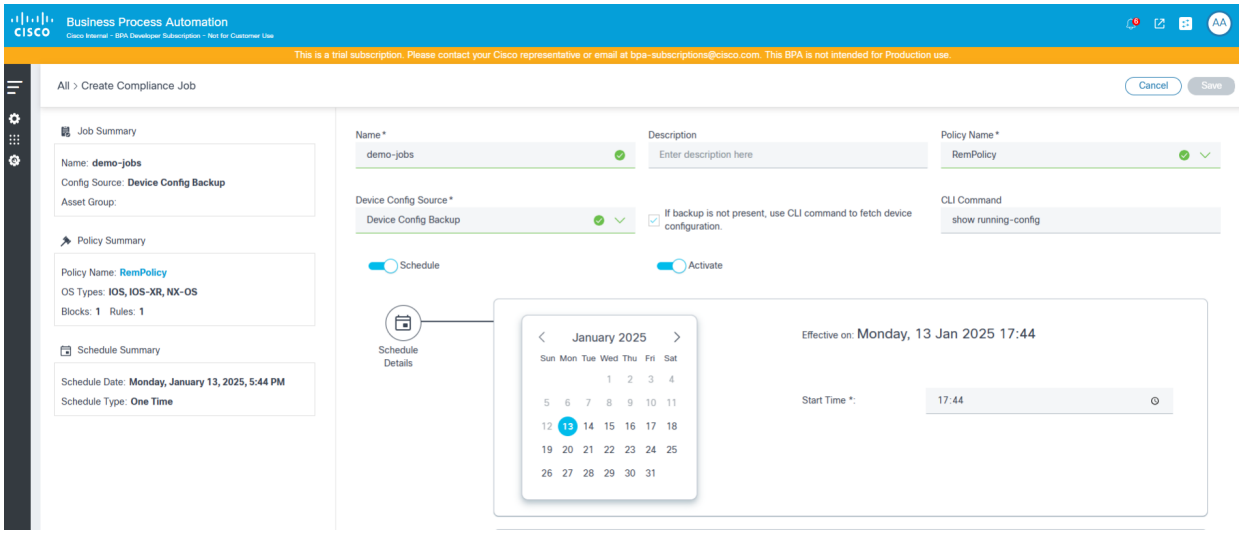
- Name: Name des Auftrags
- Beschreibung: Eine optionale Beschreibung
- Richtlinienname: Eine Dropdown-Liste zur Auswahl einer auszuführenden Richtlinie, die nach Zugriffsrichtlinien gefiltert werden kann, die für den angemeldeten Benutzer konfiguriert wurden.
- Gerätekonfigurationsquelle: Eine Dropdown-Liste, in der die Quelle zum Abrufen der Gerätekonfiguration (aktuelle Konfiguration oder Gerätekonfigurations-Backup) für den Compliance-Job ausgewählt wird, sowie ein Kontrollkästchen zum Angeben, ob auf einen CLI-Befehl zurückgegriffen werden soll, wenn keine Sicherung vorhanden ist.

---

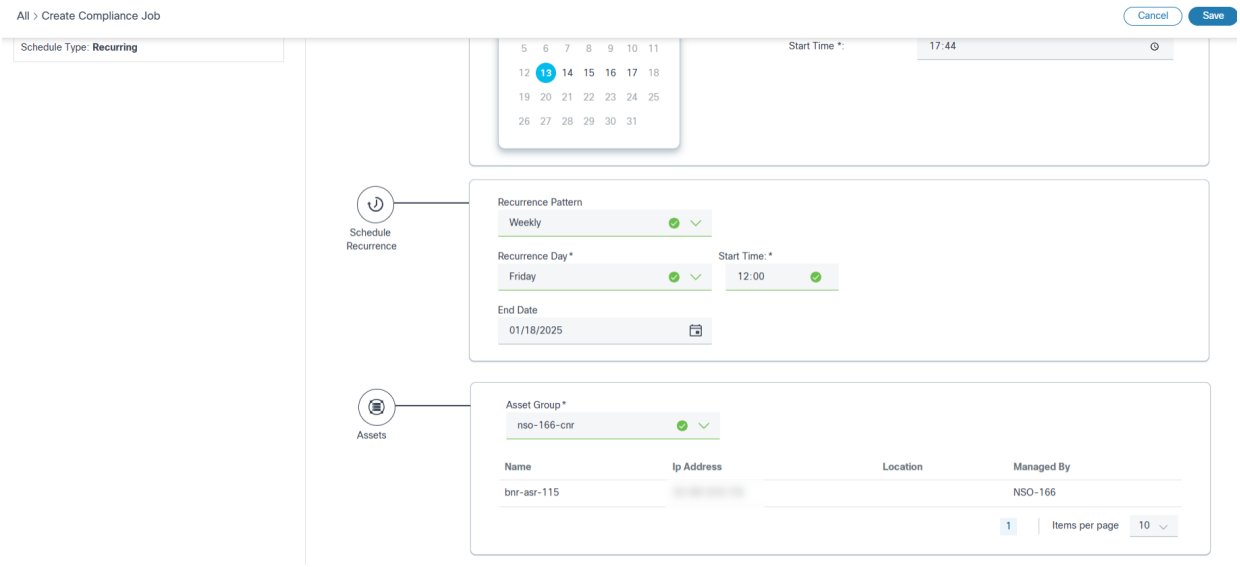
Anmerkung: Die Option Device Config Backup (Sicherung der Gerätekonfiguration) funktioniert nur, wenn der zugrunde liegende Controller die Backup-Funktion unterstützt.

---

- Benutzerdefinierte Variablen: Bearbeitbares Textfeld für verfügbaren Namespace, wenn die ausgewählte Richtlinie benutzerdefinierte Variablen enthält
- Details zum Zeitplan: Abschnitt zur Auswahl verschiedener Zeitplanparameter wie Start- und Enddatum/-uhrzeit, Wiederholungsmuster usw.
- Ressourcen: Abschnitt zur Auswahl einer Anlagengruppe, um die Liste der Geräte zu identifizieren, für die die Compliance ausgeführt werden soll
- Zeitplan: Zum Ein-/Ausschalten der geplanten Ausführung des Auftrags (einmalig oder wiederholt) Wenn deaktiviert, wird der Job sofort ausgeführt
- Ist aktiv: Gibt an, ob der ausgewählte Zeitplan aktiv ist oder nicht.




Erstellen von Compliance-Jobs



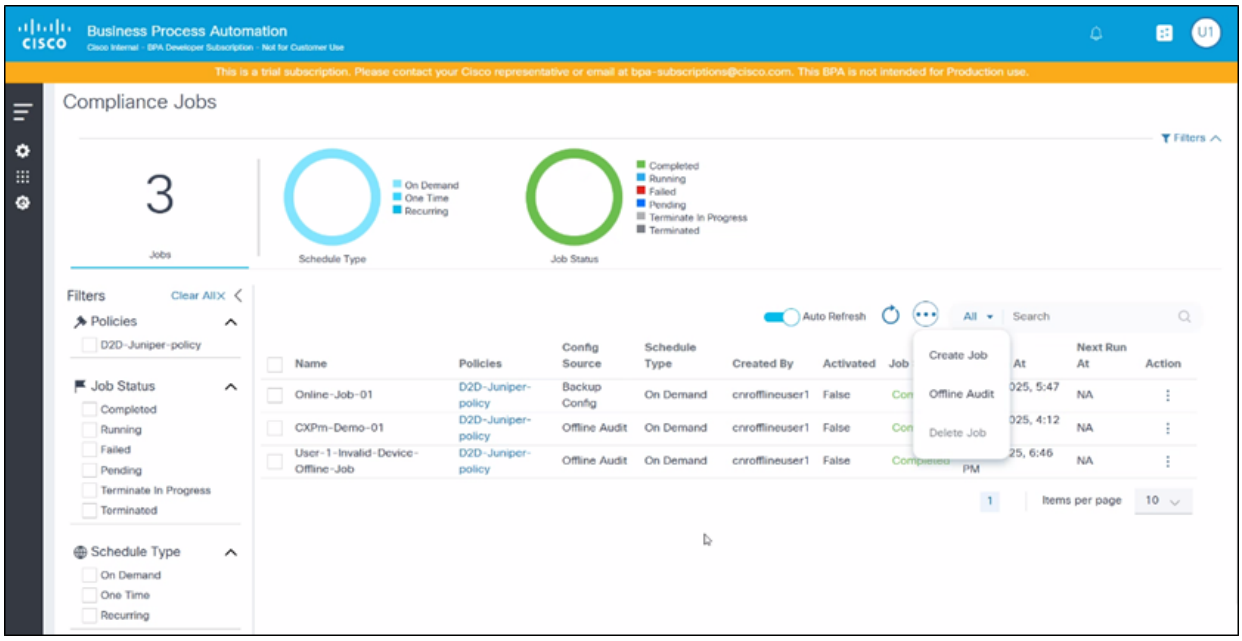

Compliance-Aufträge erstellen 2

# Offline-Überwachungsaufträge erstellen

Die Funktion "Offline Audit" in Compliance-Aufträgen ermöglicht es Benutzern, Compliance-Prüfungen für Gerätekonfigurationen durchzuführen, ohne dass die Geräte in BPA integriert werden müssen. Benutzer können die Gerätekonfiguration manuell als Datei hochladen. Mehrere Gerätekonfigurationen können komprimiert und zusammen als ZIP-Datei hochgeladen werden. Nach dem Hochladen werden diese Konfigurationsdateien analysiert, und Compliance-Jobs können mit diesem Dateiinhalt als Quelle erstellt werden. Die Ergebnisse der Offline-Prüfungen werden dann zusammen mit den Ergebnissen der Online-Prüfung im Compliance-Dashboard angezeigt.

Die Seite Offline-Audit enthält die folgenden Attribute:

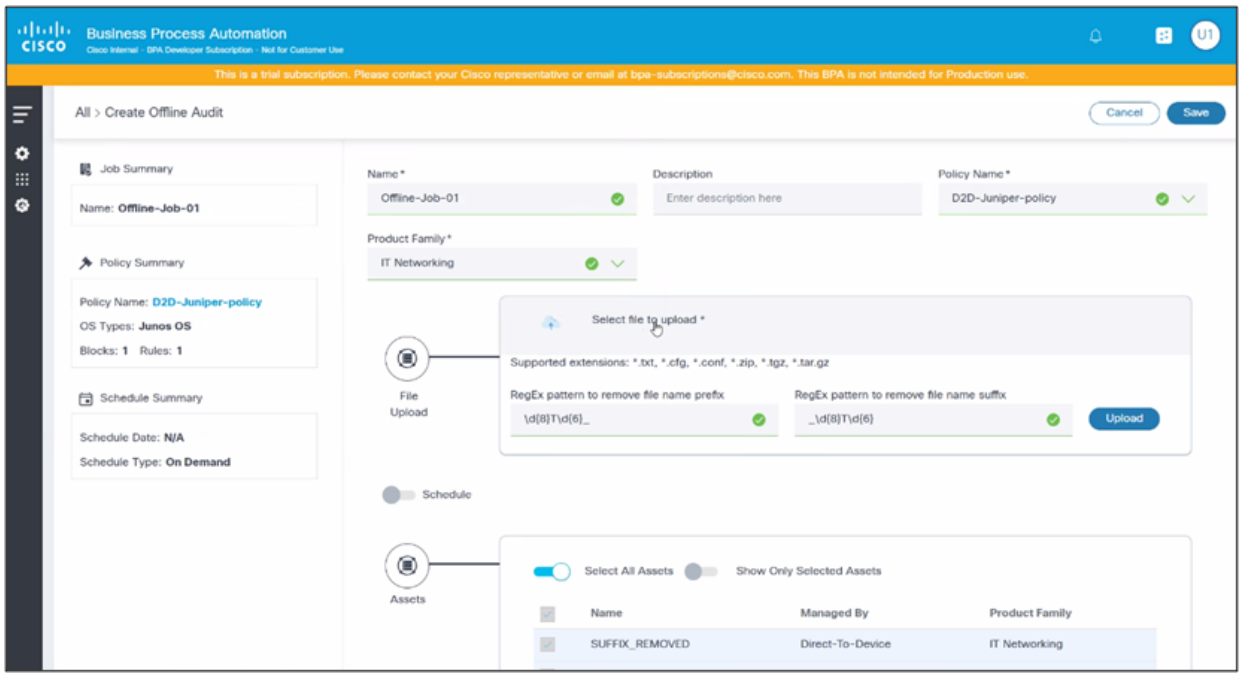
- Name: Name des Auftrags
- Beschreibung: Eine optionale Beschreibung
- Richtlinienname: Eine Dropdown-Liste zur Auswahl einer auszuführenden Richtlinie, die nach Zugriffsrichtlinien gefiltert werden kann, die für den angemeldeten Benutzer konfiguriert wurden.
- Produktfamilie: Eine Dropdown-Liste zur Auswahl der Produktfamilie
- Datei hochladen: Verwenden Sie die Offline-Audit-Funktion, um die Konfigurationsdateien manuell hochzuladen. Dies erfolgt über eine Upload-Schnittstelle, in der Sie die Dateien vom lokalen System auswählen.
- Zeitplan: Zum Einschalten des Zeitplans umschalten
- Ressourcen: Zeigt eine Liste der Geräte nach hochgeladenem Dateiinhalt an.




Offline-Audit auswählen

So erstellen Sie Offline-Überwachungsaufträge:

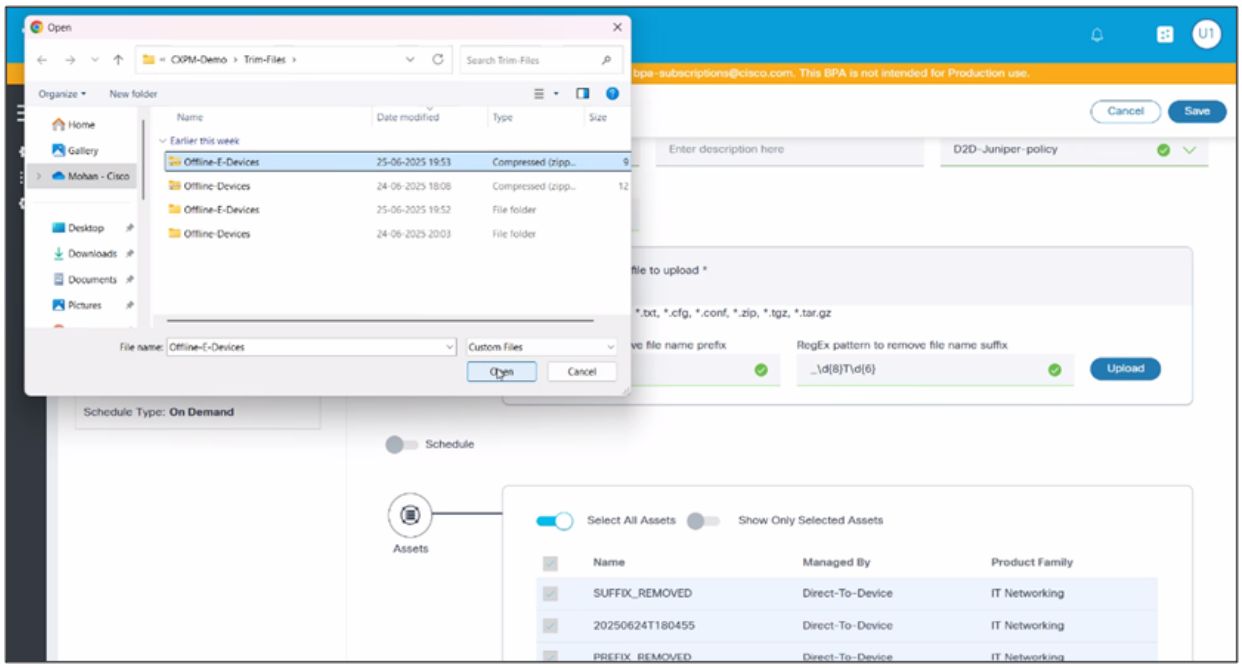
1. Wählen Sie Offline-Audit aus dem Symbol Weitere Optionen aus.




Datei hochladen

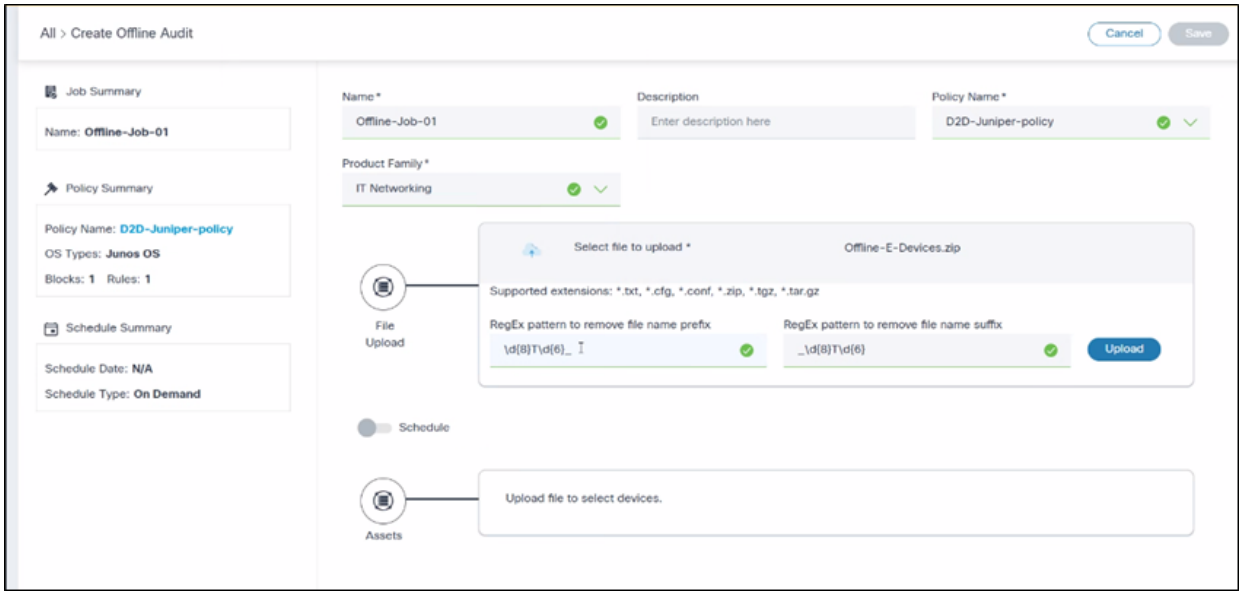
2. Klicken Sie auf Datei auswählen, die hochgeladen werden soll, um Konfigurationsdateien hochzuladen.

Anmerkung: Zu den unterstützten Dateitypen gehören (.txt,.cfg,.conf,.zip,.tgz,.tar.gz).




Desktop-Dateien

3. Wenn die Konfigurationsdateien in einem Ordner oder Archiv komprimiert sind, extrahieren Sie die Dateien vor dem Hochladen.



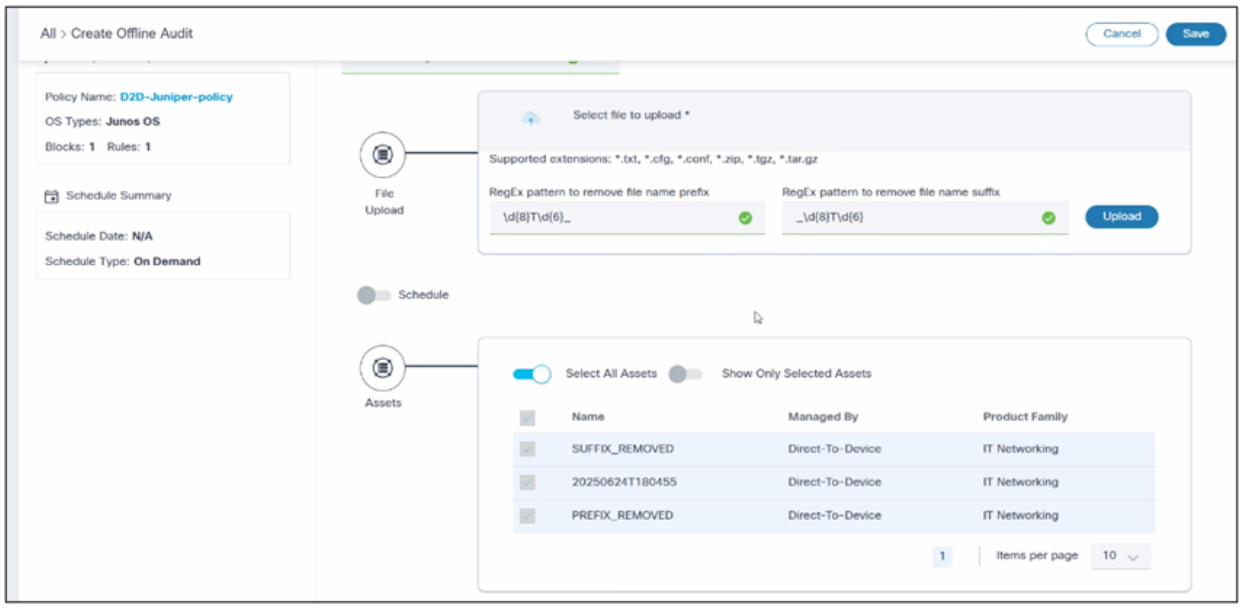

Regex-Muster

4. Wenden Sie das Regex-Muster für das Trimmen von Dateinamen an (optional).

---

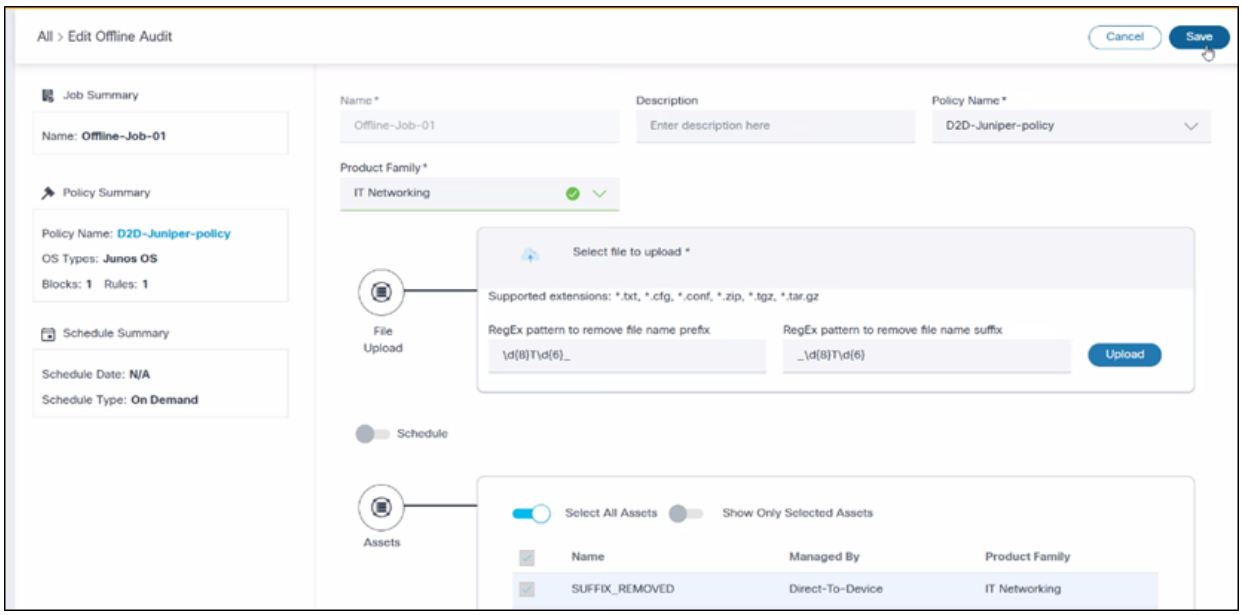
Anmerkung: Verwenden Sie Präfix- oder Suffix-Trimmmuster (Regex), um hochgeladene Dateinamen zu standardisieren oder zu vereinfachen und so die Verarbeitung zu vereinfachen.

---




Dateien hochladen

5. Klicken Sie auf Hochladen. Es wird eine Bestätigungsmeldung angezeigt, die bestätigt, dass die Dateien in der Datenbank gespeichert und erfolgreich hochgeladen wurden.



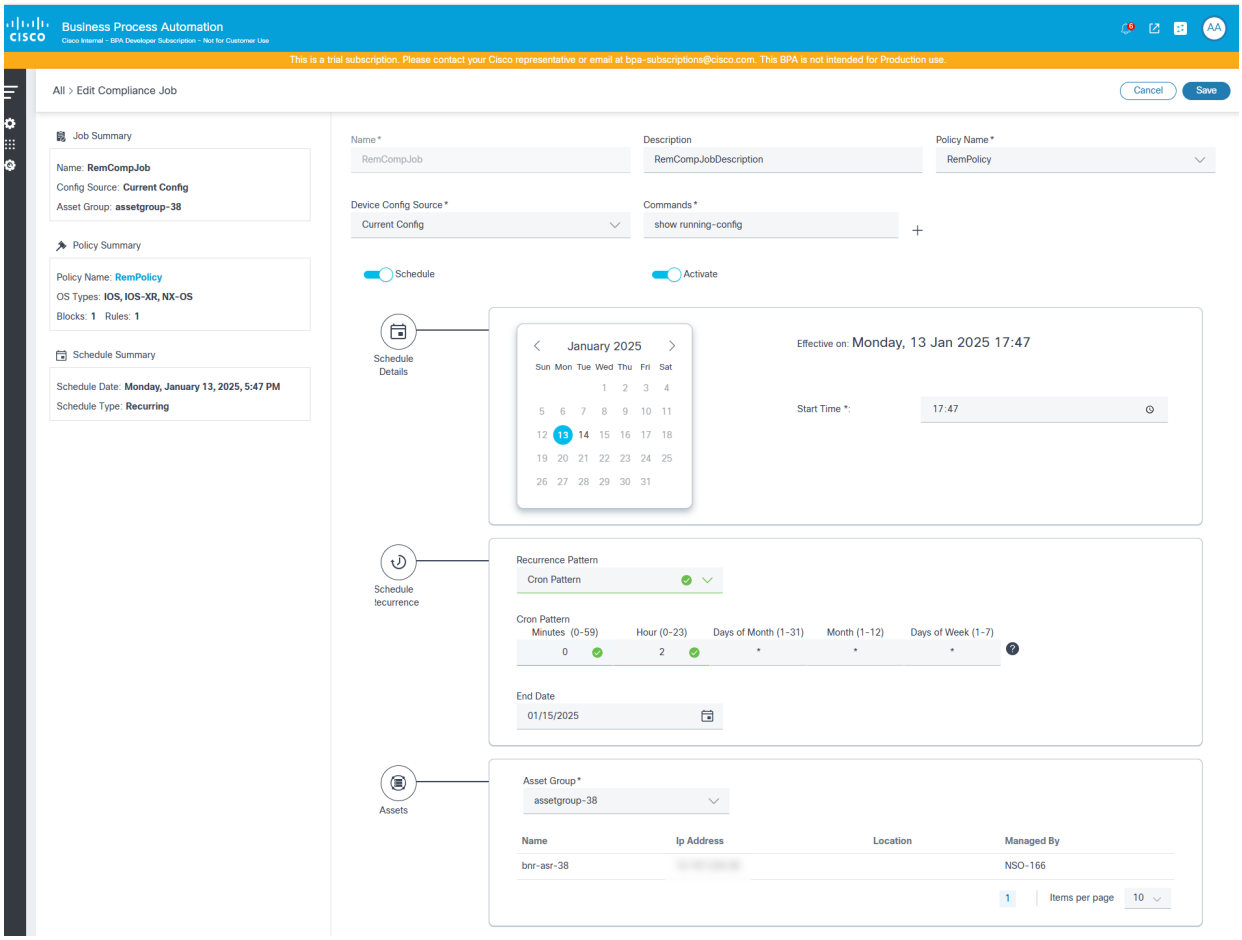

Offline-Audit speichern

6. Klicken Sie auf Speichern, um den Offline-Überwachungsauftrag zu erstellen.

## Compliance-Jobs bearbeiten

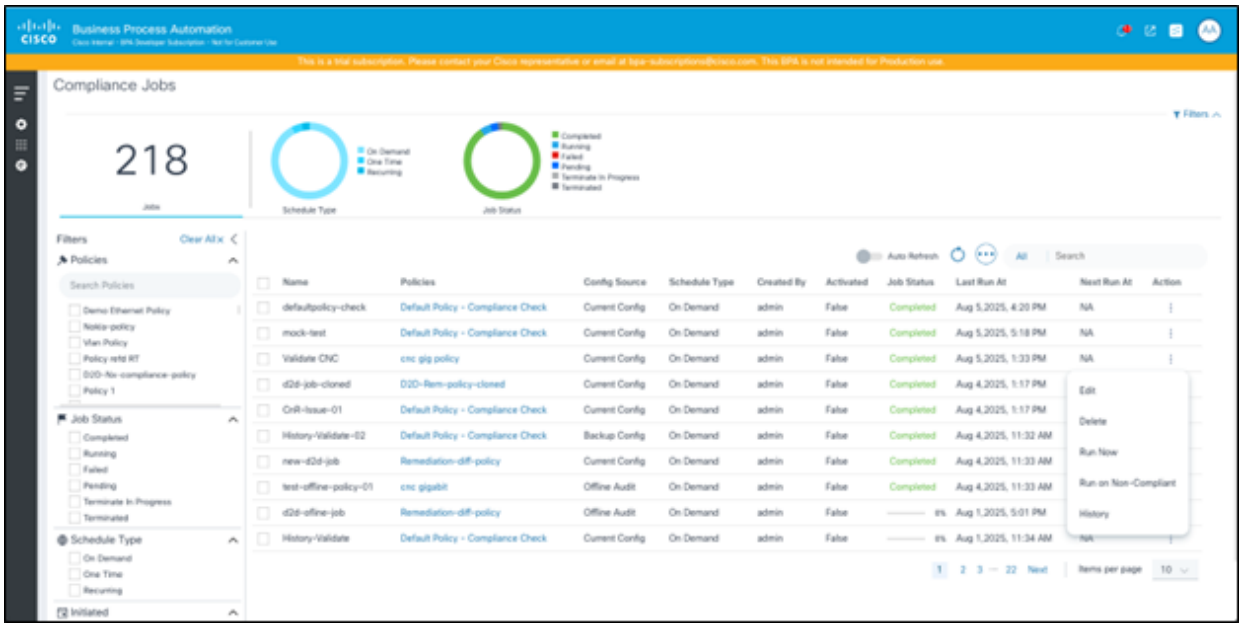
Um Compliance-Jobs zu bearbeiten, befolgen Sie die Schritte unter Erstellen von Compliance-Jobs.

Anmerkung: Der Jobname kann nicht bearbeitet werden.




Compliance-Auftrag bearbeiten

# Jetzt ausführen oder Compliance-Aufträge erneut ausführen



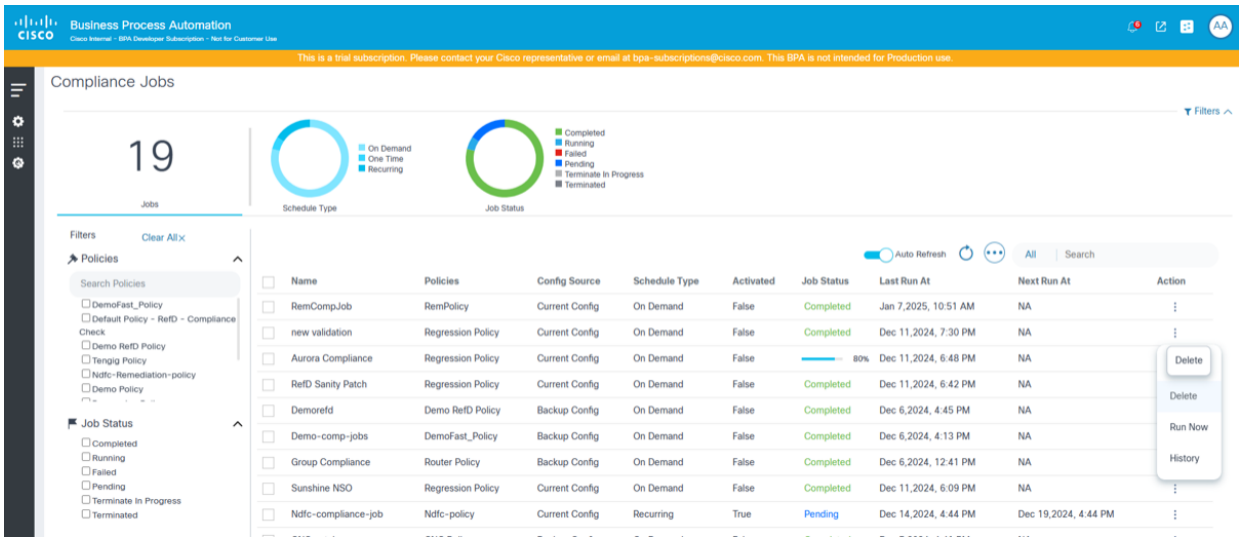

Compliance-Auftrag - Jetzt ausführen und Nicht-konform ausführen

Im Raster für Compliance-Aufträge steht eine Option zum Ausführen eines Auftrags nach Bedarf zur Verfügung. Wählen Sie dazu Jetzt ausführen aus dem Symbol Weitere Optionen. Wenn ein Job bereits ausgeführt wird, können Benutzer über das Symbol Weitere Optionen die Option Bei nicht konformer Ausführung ausführen auswählen. Mit dieser Aktion wird der Compliance-Job nur auf der Liste der Ressourcen ausgeführt, die bei der vorherigen Ausführung nicht als vollständig konform markiert wurden.

## Compliance-Jobs löschen

Das Portal bietet eine Option zum Löschen eines oder mehrerer Compliance-Jobs, wenn der Benutzer über die richtige rollenbasierte Zugriffskontrolle (RBAC) verfügt. Jobs können nicht gelöscht werden, wenn eine Ausführung ausgeführt wird. Benutzer können wählen, ob einzelne oder mehrere Compliance-Jobs gelöscht werden sollen.

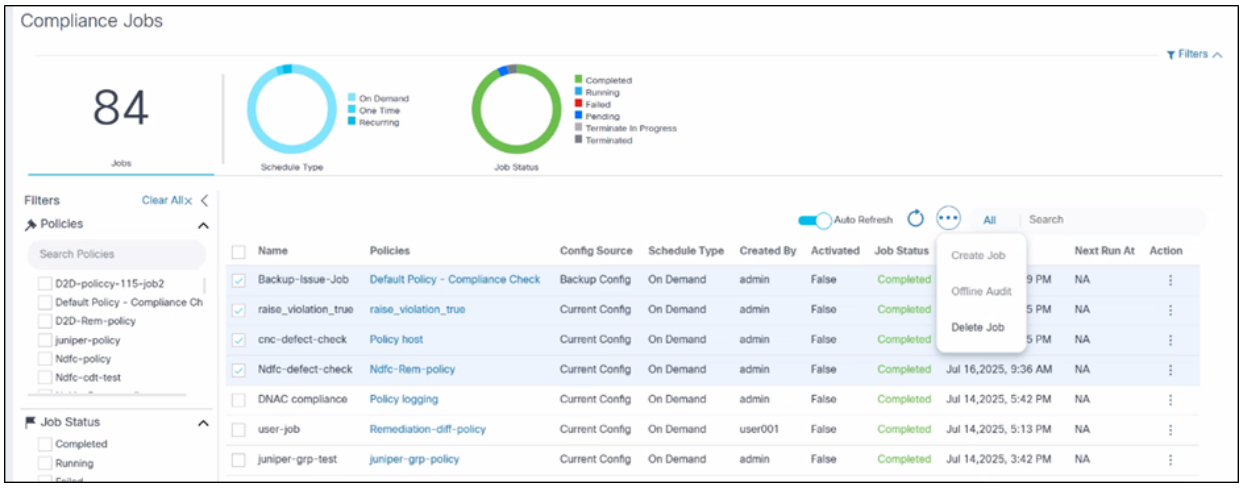
So löschen Sie einen Compliance-Auftrag:



Löschen eines einzelnen Compliance-Auftrags

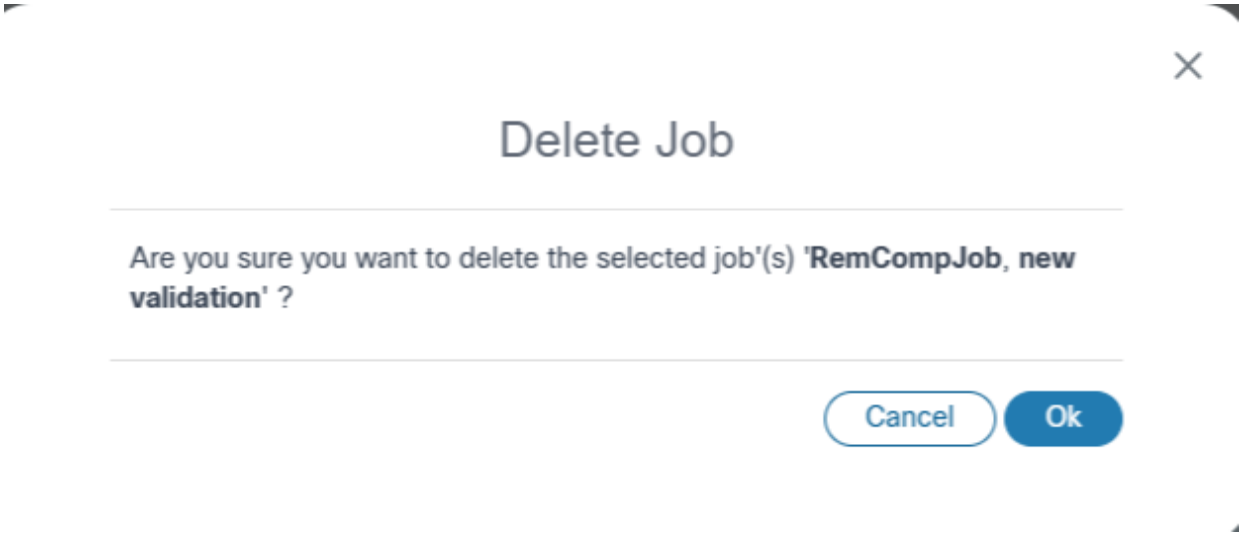
1. Wählen Sie auf der Seite Compliance-Aufträge das Symbol Weitere Optionen > Löschen für den zu löschenden Auftrag aus.

ODER




Mehrere Compliance-Aufträge löschen

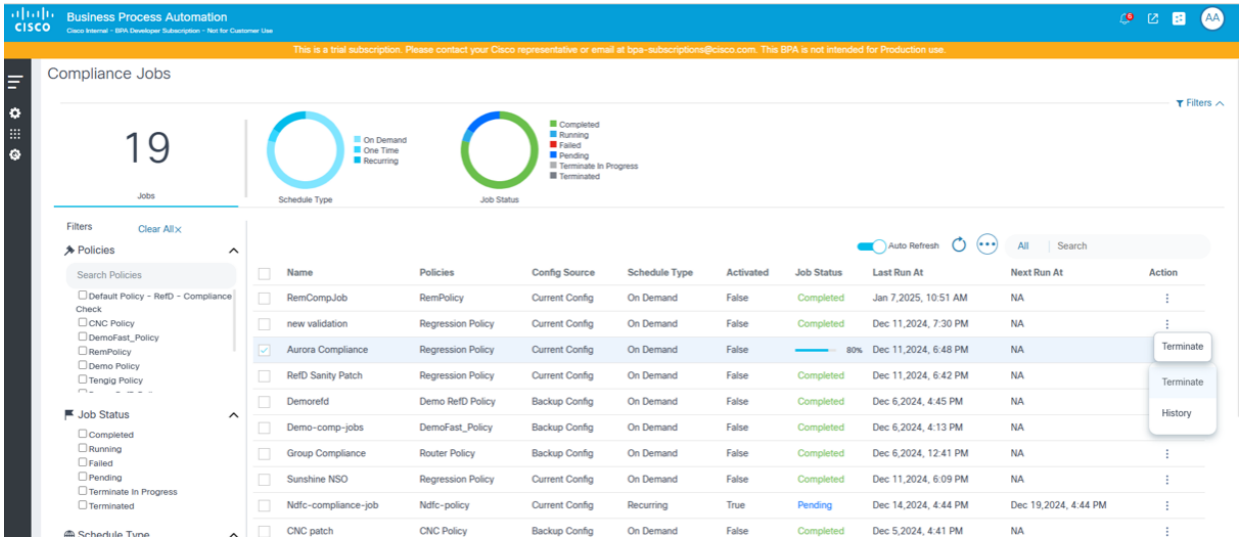
Um mehrere Compliance-Jobs zu löschen, aktivieren Sie die Kontrollkästchen für die zu löschenden Jobs, und wählen Sie Weitere Optionen > Job löschen aus. Es wird eine Bestätigung angezeigt.



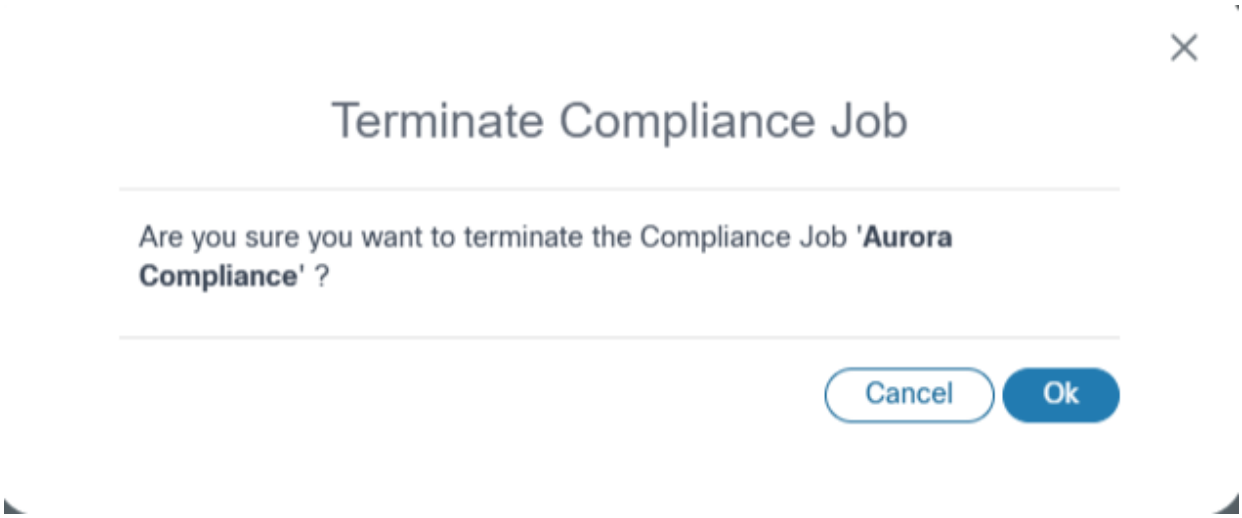

Bestätigung des Compliance-Auftrags löschen

## Compliance-Jobs beenden

Das Portal bietet den Benutzern die Möglichkeit, die Ausführung eines bestimmten Auftrags zu beenden. Wenn ein Job beendet wird, schließen die aktuell ausgeführten Geräte ihre Ausführung ab und brechen alle weiteren in der Warteschlange befindlichen Geräteausführungen ab.



Compliance-Jobs beenden

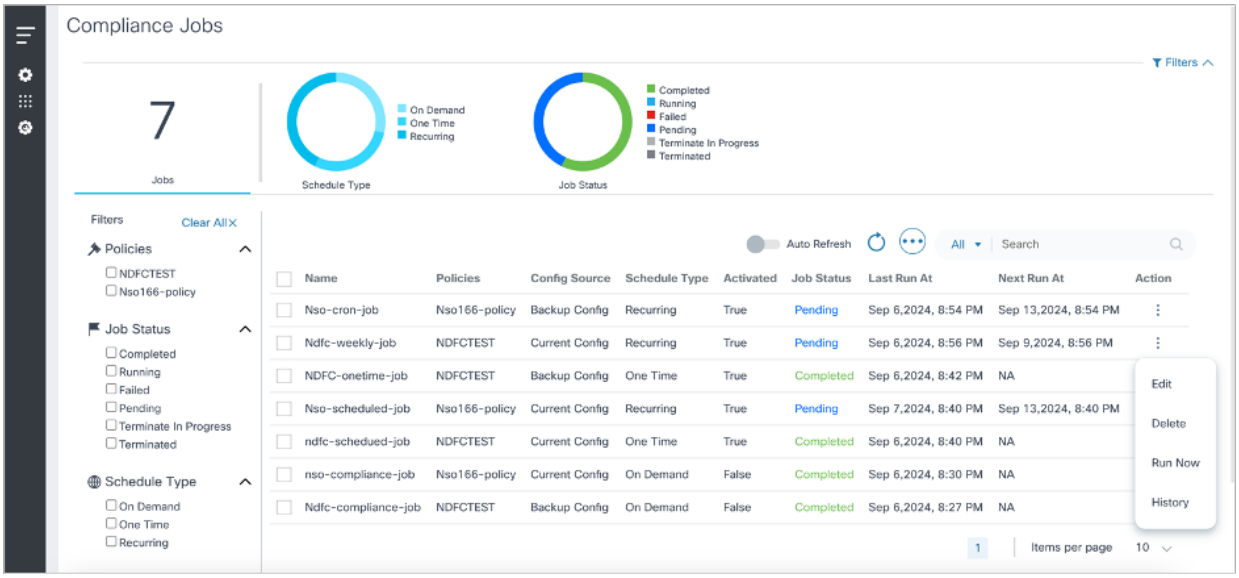


Compliance-Auftragsbestätigung beenden

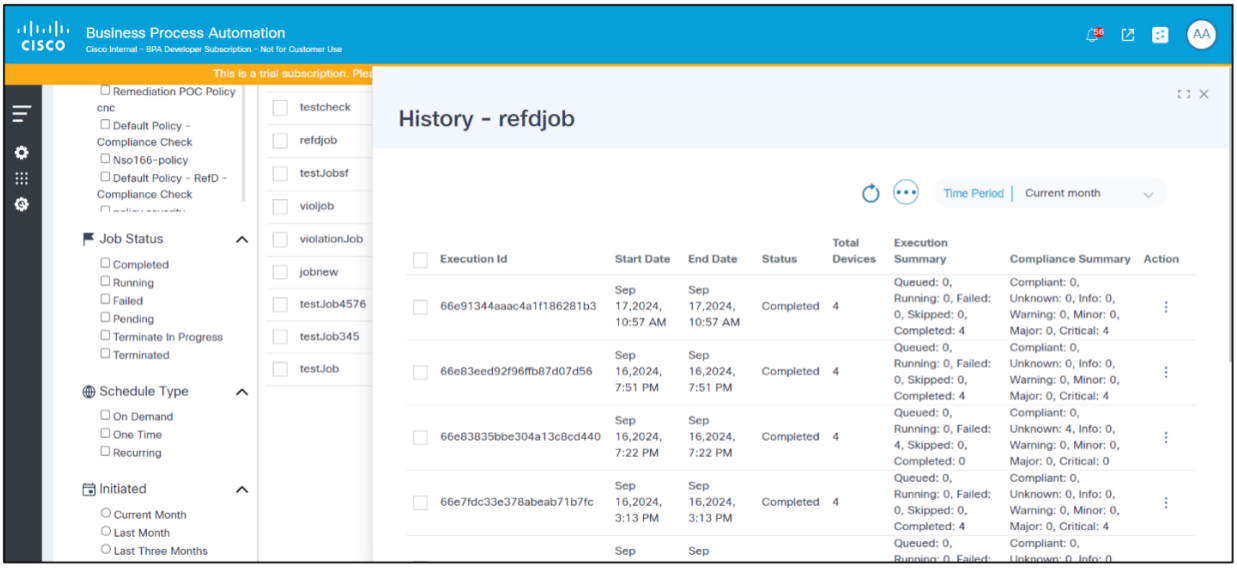
## Verlauf der Compliance-Jobs

Die Option Verlauf im Compliance-Job zeigt die Liste der Ausführungsvorgänge für den ausgewählten Job an, gefiltert nach dem Zeitplandatumsbereich.

Um den Verlauf eines Compliance-Auftrags anzuzeigen, wählen Sie auf der Seite Compliance-Aufträge das Symbol Weitere Optionen > Verlauf aus. Die Seite Verlauf wird angezeigt.




Verlauf des Compliance-Jobs

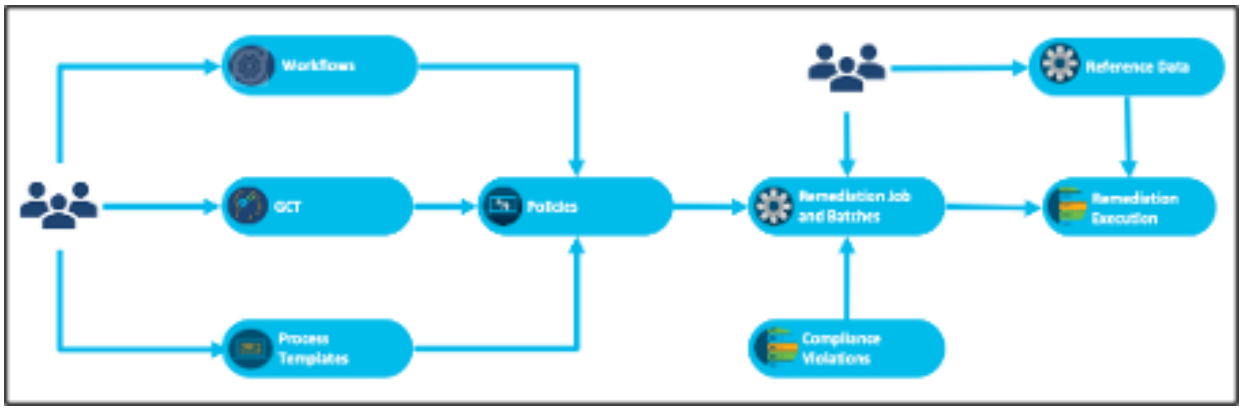



Verlaufsseite

# Bereinigungsaufträge

Das Remediation Framework ermöglicht die Behebung von Compliance-Verletzungen, die im Compliance-Dashboard aufgeführt sind. Dieses Framework verwendet Workflows, GCTs und Prozessvorlagen.

## Flussdiagramm zur Konfigurationsbereinigung



Konfigurationsbereinigung - Übersicht

Der Anwendungsfall "Konfigurationskorrektur" ermöglicht es Betreibern, Konfigurationsverletzungen auf Geräten mithilfe von Korrekturaufträgen zu beheben. Die Compliance-Richtlinie wird zunächst mit dem entsprechenden Workflow, GCT-Vorlagen und Prozessvorlagen je Controller-Typ konfiguriert. Ein Wiederherstellungsauftrag wird für eine Richtlinie für eine Liste betroffener Ressourcen ausgeführt. Bei der Sanierung können die auf ein Gerät anzuwendenden Werte aus verschiedenen Datenquellen abgerufen werden, darunter das Ergebnis der Compliance-Ausführung, die RefD-Anwendung und die Konfiguration des vorhandenen Geräts. Der Workflow kann je nach Kundenanforderung angepasst werden, um zusätzliche Schritte bei der Problembehebung zu ermöglichen.

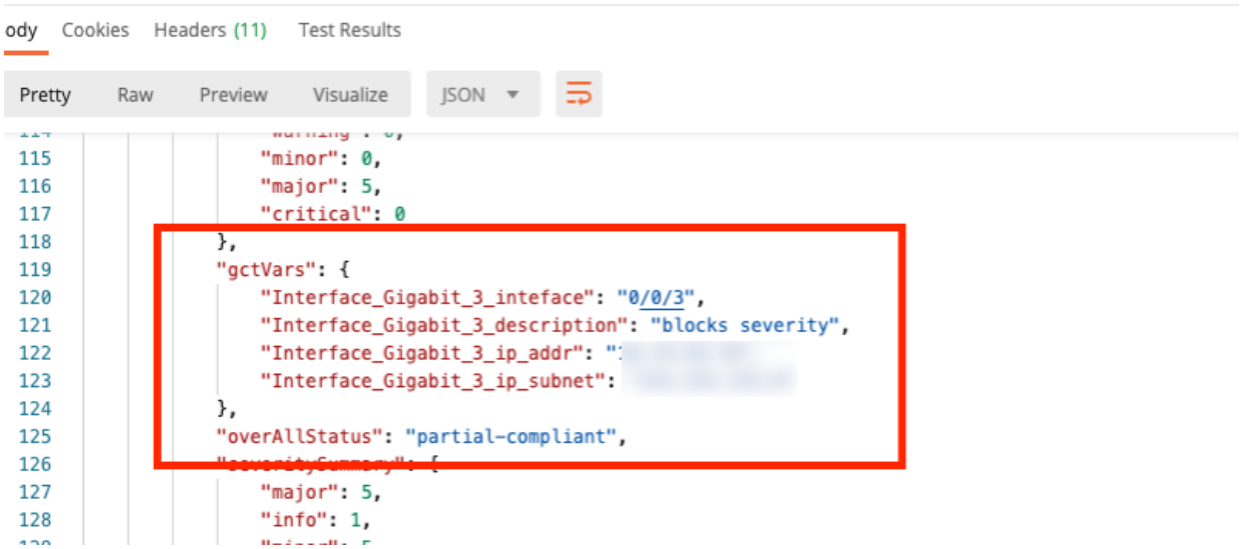
Die wichtigsten Schritte der Sanierungsfunktion werden im Folgenden erläutert:

GCT-Vorlage

GCTs sind eine BPA-Kernfunktion, die verwendet wird, um Konfigurationsänderungen auf Geräte anzuwenden, die Controller-spezifische Vorlagen verwenden.

- Erstellung einer GCT-Vorlage zur Aktualisierung der Gerätekonfigurationen, um Compliance-Verletzungen zu beheben
- Das Framework unterstützt die automatische Variablenzuordnung, wenn die Variablen innerhalb der GCT-Vorlage der folgenden Syntax entsprechen:
  - Für Konfigurationsbausteine mit einem Gerät: <>_<>. Beispiel: management_interface_ipv4_addr, management_interface_ipv4_subnet
  - Mehrere Bausteine der Gerätekonfiguration sind für eine zukünftige Version geplant
- Wenn "Blockkennungsname" und "Variablenname aus Block" Leerzeichen enthalten, sollten diese Leerzeichen durch Unterstriche ("_") ersetzt werden (z. B. wenn "Blockkennungsname" "Verwaltungsschnittstelle" ist und "Variablenname" "IPV4_ADDR" ist, sollte der Variablenname im GCT "Management_Interface_IPV4_ADDR" sein).
- Benutzer können die Ausgabe von "gctVars" aus der Ausführung des Compliance-Geräts überprüfen, um festzustellen, ob die Syntax und die Zuordnungen der GCT-Variablen korrekt sind. Verwenden Sie die folgenden REST-APIs, um die Ausführung des Compliance-Geräts zu erhalten:

- Ausführungs-ID abrufen
  - URL: /api/v1.0/compliance-remediation/compliance-executions
  - Methode: HOLEN
- Geräteausführungen mit Ausführungs-ID abrufen
  - URL: https://<>/bpa/api/v1.0/compliance-sanierung/compliance-device-executions?executeId=<>
  - Methode: HOLEN

GCT Variablen - gctVars

- Verwenden Sie die folgende REST-API, um die Variablen aus dem Block abzurufen:
  - URL: https://<>/bpa/api/v1.0/compliance-sanierung/utils/schema
  - Methode: POST
  - Nachrichtentext: {"blockName": "<< Blockname >>" }
- Validieren Sie die GCT-Vorlagen, indem Sie die Vorlagen sowohl für den Probelauf als auch für den Commit auf die Geräte anwenden

- Konfigurieren der oben genannten GCT-Vorlagen in der Compliance-Richtlinie

Workflows

Das Framework für die Problembehebung bietet die folgenden einsatzbereiten Referenz-Workflows:

- SANIERUNGSPROZESS: Dieser Workflow umfasst die allgemeinen Schritte zur Durchführung der Problembehebung.
- BESEITIGUNGS-UNTERPROZESS: Dieser Workflow enthält variable Zuweisungen, GCT-Trockenlauf und GCT-Commit-Aufgaben, die von anderen Teams entsprechend den Anforderungen angepasst werden können.

Beide Workflows können je nach Kundenanforderungen unverändert verwendet, aktualisiert oder ersetzt werden.

Prozessvorlagen

Prozessvorlagen und Analysevorlagen können anhand der Richtlinie konfiguriert werden, um Vor- und Nachprüfungen durchzuführen und die Ergebnisse zu vergleichen.

Richtlinien

Die CnR-Richtlinie verknüpft Workflows, GCT-Vorlagen und Prozessvorlagen nach Gerätetyp, mit denen Konfigurationen mithilfe von Jobs bereinigt werden können.

Bereinigungsaufträge

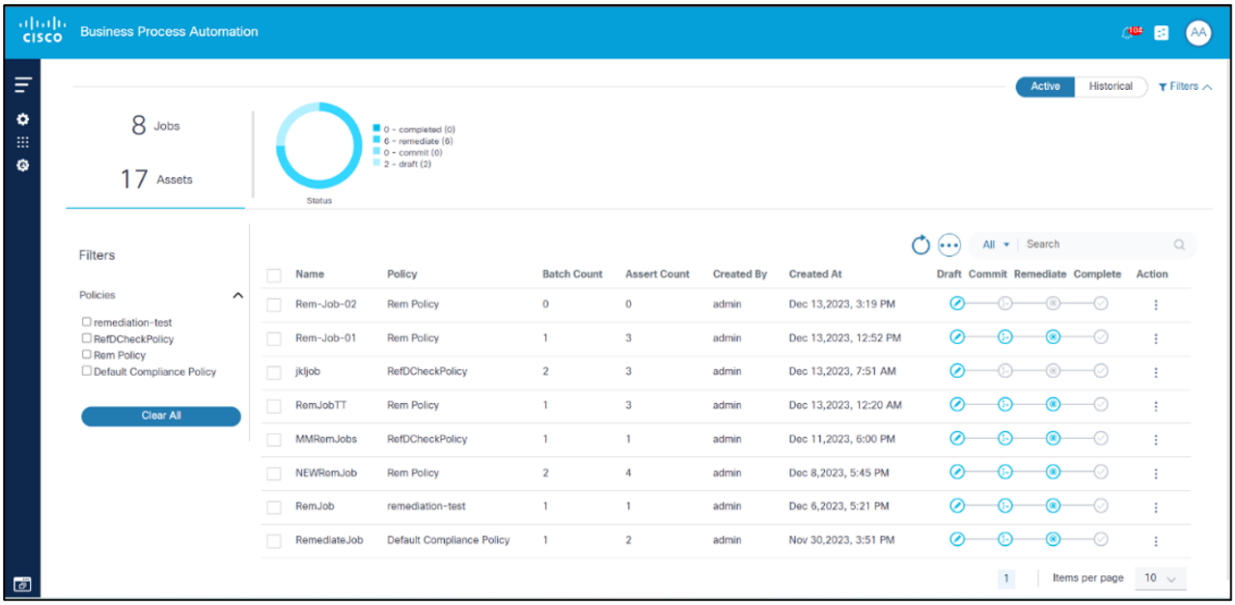
Reparaturaufträge unterstützen Betreiber bei der Anwendung von Korrekturrichtlinien auf eine ausgewählte Liste betroffener Ressourcen. Der Bereinigungsauftrag kann bei Bedarf oder nach Zeitplan ausgeführt werden. Zur Laufzeit kann der Korrekturworkflow Daten aus einer Vielzahl von Quellen abrufen, darunter die Gerätedetails, Details zur Compliance-Ausführung und das RefD-Framework.

## Liste von Bereinigungsaufträgen

Benutzer können im Dashboard erstellte Korrekturaufträge wie folgt filtern, sortieren und anzeigen:

- Jobs: Zeigt alle erstellten Jobs an

- Ressourcen: Erstellte Gesamtrechnungen anzeigen
- Status: Zeigt Jobs nach Status an.
- Aktiv und historisch: Zeigt aktive oder historische (inaktive) Aufträge an, abhängig von der Auswahl
- Richtlinien: Filtert Bereinigungsaufträge nach Richtlinien
- Hauptraster: Zeigt die Standardliste der Jobs an, die durch Klicken auf die Überschrift sortiert werden können, und enthält eine Suche nach Name und Richtlinie mit Paginierungen.
- Aktionen: Jobs können archiviert oder gelöscht werden, wenn sie den Status Entwurf oder Abgeschlossen haben. Ein laufender Job kann nicht archiviert oder gelöscht werden.

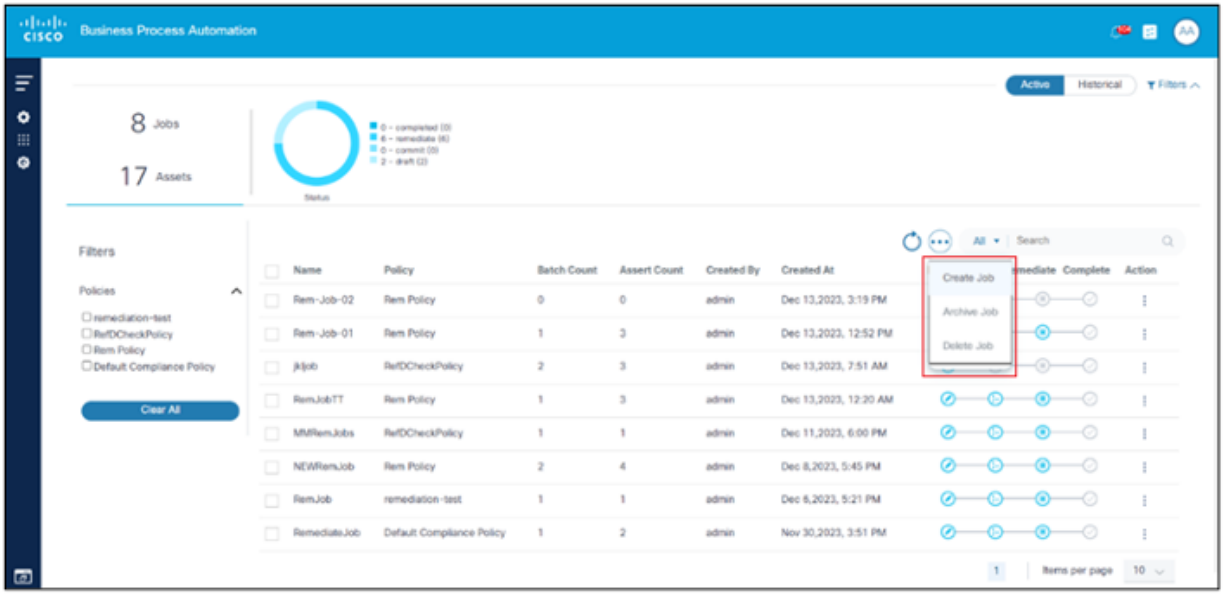



Liste von Bereinigungsaufträgen

## Erstellen und Bearbeiten von Bereinigungsaufträgen

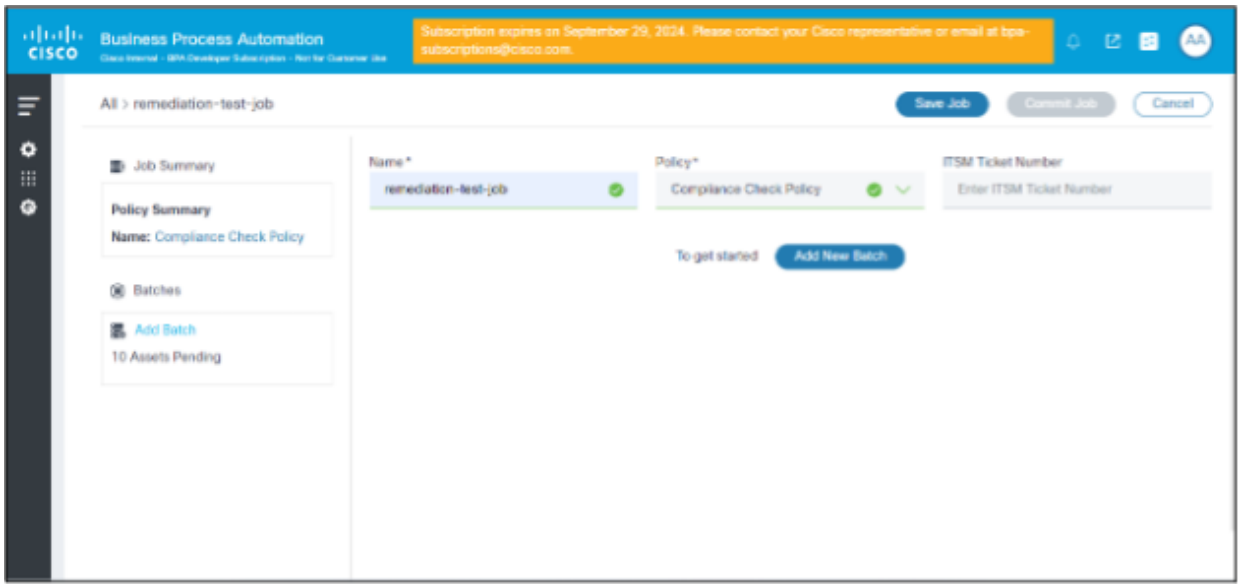
Korrekturaufträge werden auf der Seite Jobliste erstellt und können wie folgt erstellt werden:

1. Wählen Sie das Symbol Weitere Optionen > Job erstellen aus. Die Seite "Job erstellen" wird angezeigt.




Optionen für Bereinigungsaufträge

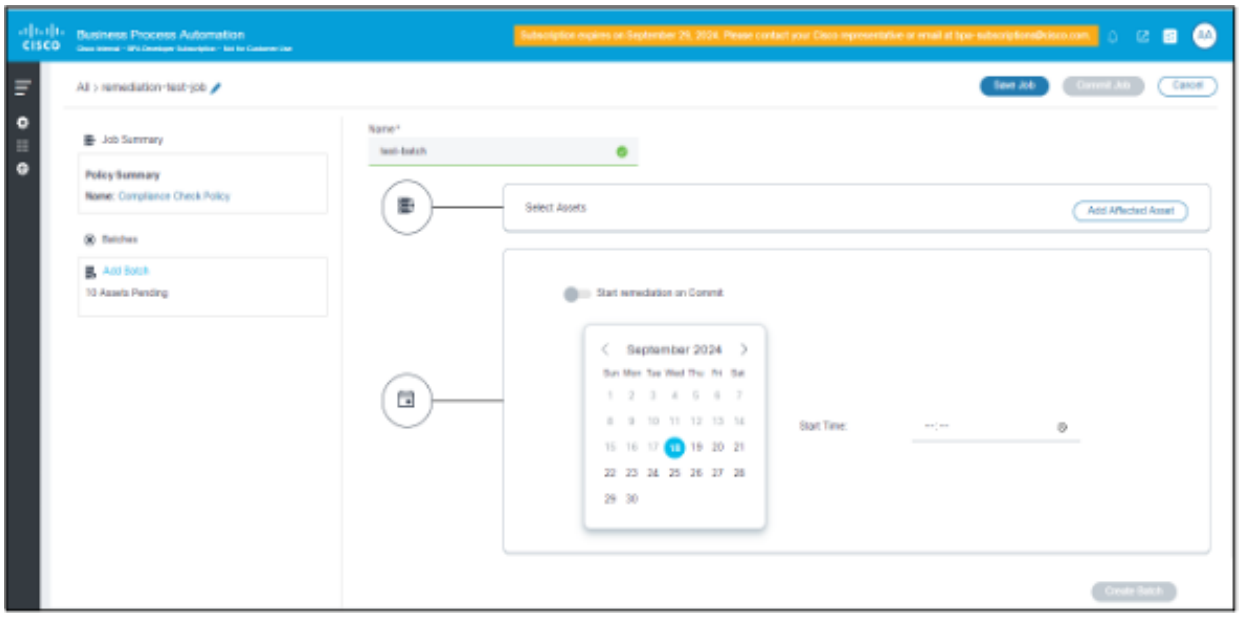
2. Details vervollständigen oder bearbeiten.




Bereinigungsaufträge: Details

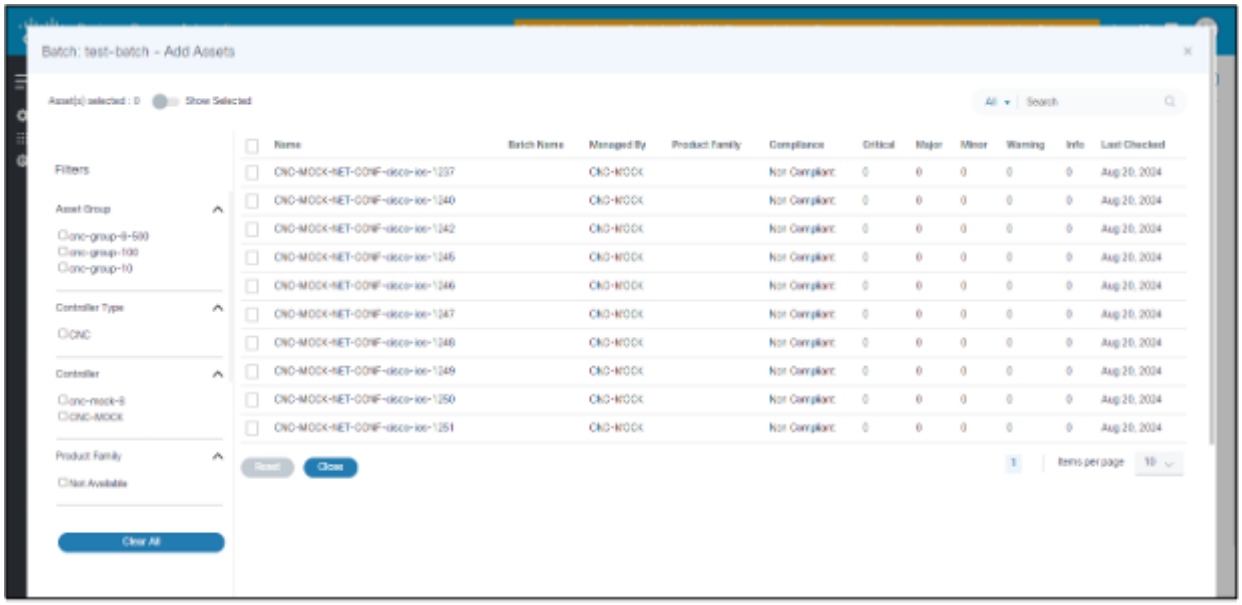
3. Klicken Sie auf Auftrag speichern.

So fügen Sie Stapeln auf der Seite "Auftrag erstellen" zu Aufträgen hinzu:



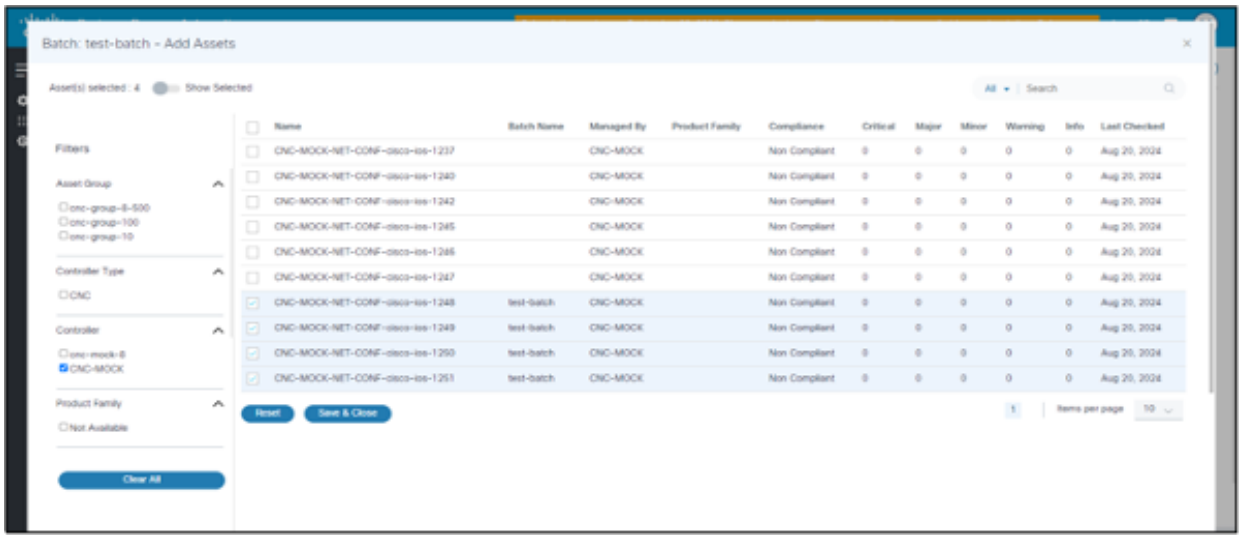

Bereinigungsaufträge: Stapel hinzufügen

1. Klicken Sie auf Neuen Stapel hinzufügen.
2. Geben Sie den Namen, die Details zu den betroffenen Ressourcen und die Details zum Zeitplan ein.
3. Klicken Sie auf Betroffene Ressourcen hinzufügen.
4. Wählen Sie auf der Seite Asset Details (Ressourcendetails) die Liste der betroffenen Ressourcen aus, und klicken Sie auf Save Job (Job speichern).
5. Filtern Sie die Ressourcen nach Controller-Typ, Controller, Asset-Gruppe und Produktfamilie.
6. Klicken Sie nach der Auswahl der Ressourcen auf Speichern und schließen, um zur vorherigen Seite zurückzukehren.




Bereinigungsaufträge: Betroffene Ressourcen hinzufügen

Anmerkung: Benutzer können auf der Seite Betroffene Ressourcen Filter anwenden



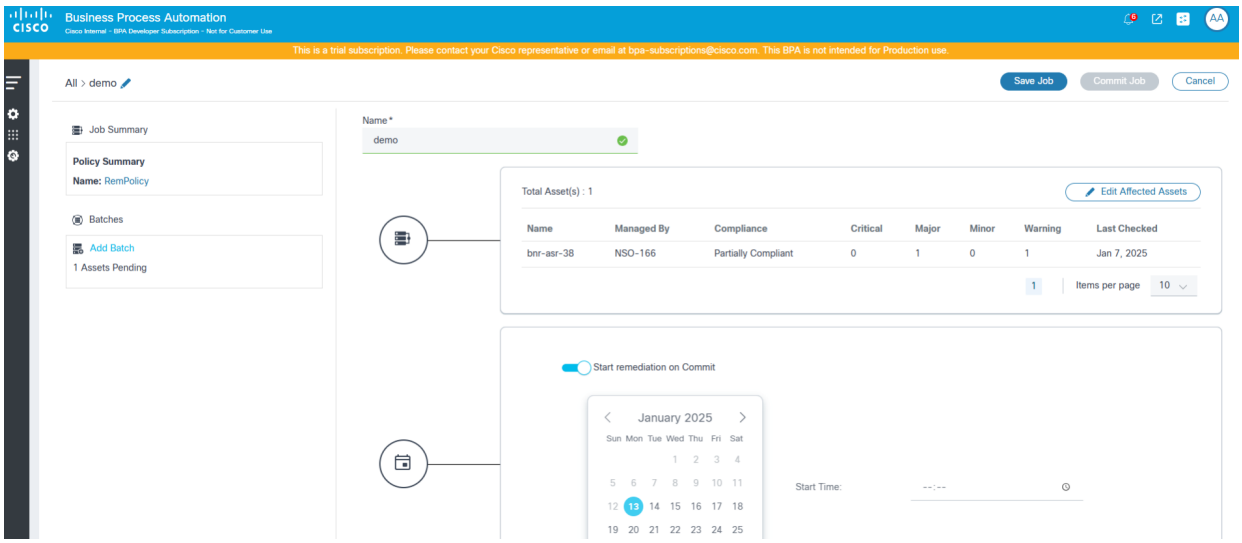

Bereinigungsaufträge: Betroffene Filter hinzufügen

Nach dem Hinzufügen der betroffenen Ressourcen kann der Stapel beim Speichern oder zu einem geplanten späteren Zeitpunkt einmalig ausgeführt werden.

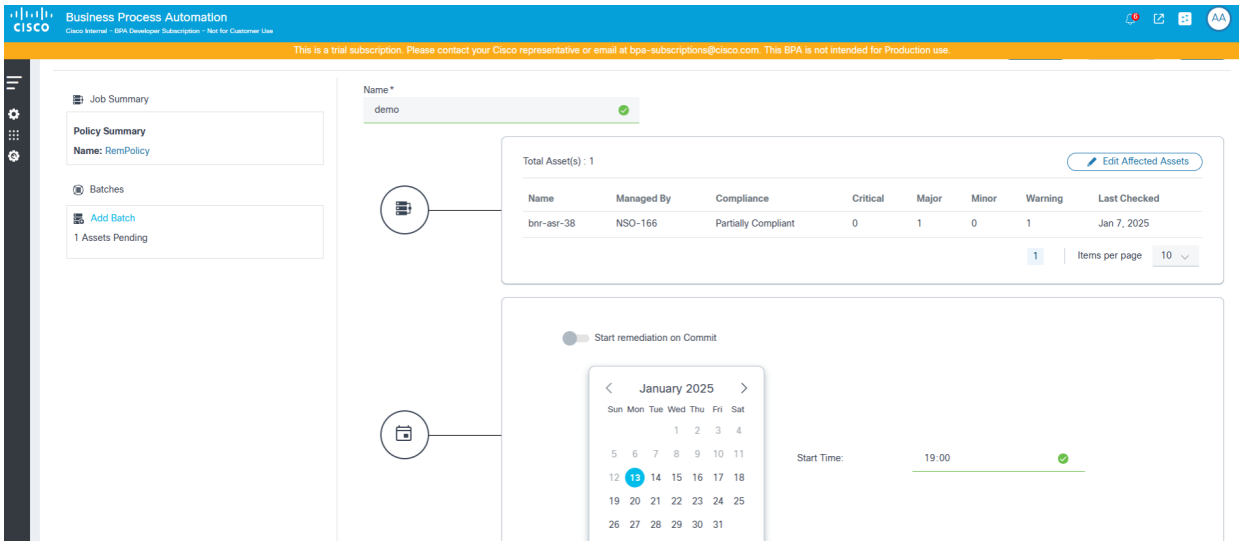
Anmerkung: Um den Job als On Demand auszuführen, aktivieren Sie den Umschalter Wiederherstellung bei Bestätigung starten. Wenn ein Benutzer diese Option auswählt, werden Datum und Uhrzeit nicht benötigt. Wenn der Benutzer die einmalige Option auswählt, müssen Datum und Uhrzeit angegeben werden, um den Job auszuführen.

Ein einzelner Korrekturauftrag hat mehr als einen Stapel. Jeder Stapel kann mit einem Commit oder zu einem festgelegten Datum und einer festgelegten Uhrzeit gestartet werden.

Ein Commit-Behebungs-Batch kann bei Bedarf oder geplant ausgeführt werden.



Bereinigungsaufträge: On-Demand

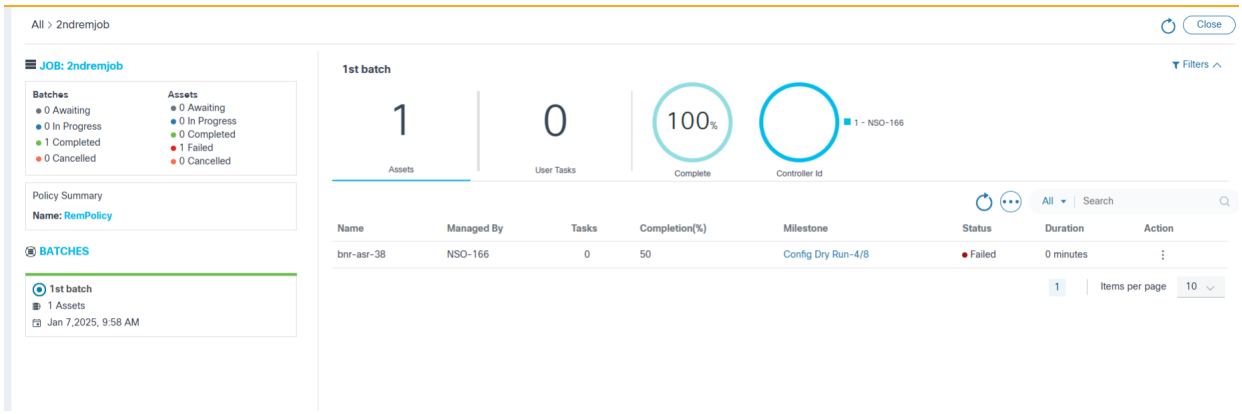



Bereinigungsaufträge: Einmal/Geplant

## Problembehebung: Liste der Geräte

Sobald der Wiederherstellungsauftrag bestätigt wurde, wird die Ausführung ausgelöst, und der Status des Auftrags wird auf der Seite Geräte auflisten unter Wiederherstellungsaufträge angezeigt. Benutzer können Filter nach Controller-ID, Name, Verwaltet von, Produktfamilie anwenden.

- AUFGABE: zeigt die Statusdetails der Stapel und Ressourcen sowie den Namen der Richtlinie an, die für die Ausführung des Korrekturauftrags ausgewählt wurde.
- STAPEL: zeigt die Liste der Stapel als Teil des aktuellen Korrekturauftrags an.
- Automatische Aktualisierung: zeigt die Optionen an, die Seite automatisch alle 30 Sekunden zu aktualisieren, wenn der Job ausgeführt wird, die Seite zu aktualisieren oder abzubrechen, um zur vorherigen Seite zurückzukehren.
- Details auf Stapelebene: zeigt die Details der Zusammenfassung auf Stapelebene an, einschließlich der Gesamtanzahl der Ressourcen, der Anzahl der Benutzeraufgaben, des Prozentsatz der Fertigstellung und der Controller-Details.
- Asset-Raster: zeigt die Anlagenrasteransicht mit Benutzeraufgabe, Fertigstellungsprozentsatz und aktuellem Meilenstein für jede Anlage an




Problembehebung: Geräteliste

Problembehebung: Details der Inline-Benutzeraufgabe

In der Geräteliste gibt die Spalte Tasks an, ob ein Benutzer Aufgaben auszuführen hat.

So zeigen Sie Details zu Inline-Benutzeraufgaben an:

1. Wählen Sie die Taskanzahl aus. Das Listenfenster Benutzeraufgaben wird geöffnet.
2. Wählen Sie eine Aufgabe aus. Das Fenster Details der Benutzeraufgabe wird geöffnet.

Die folgenden Aktionen können vom Inline-Modus ausgeführt werden:

- Abschließen
- Wiederholen
- Abbrechen

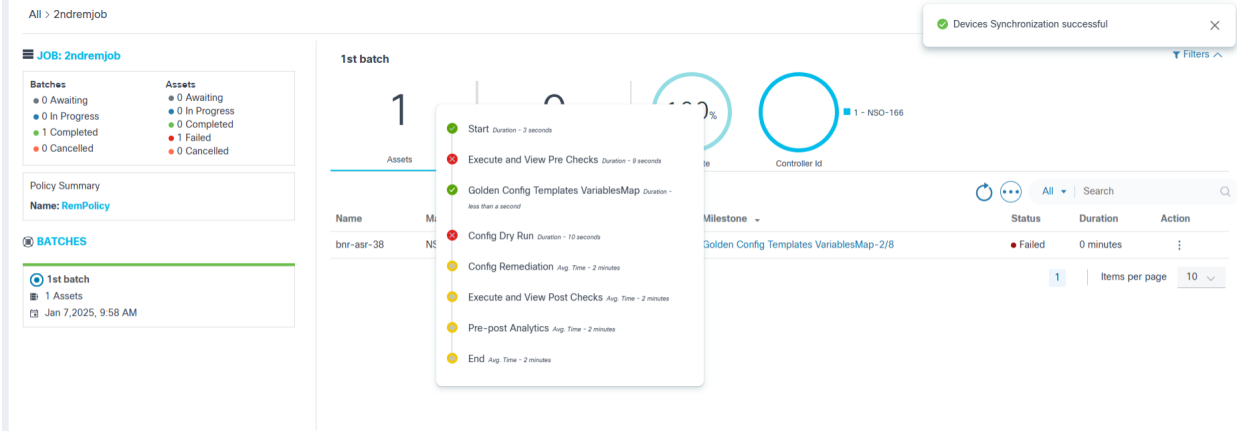
Problembehebung: Details zum Inline-Meilenstein

In der Geräteliste gibt die Spalte Meilenstein den aktuellen Meilenstein an, der mit der Sanierung des jeweiligen Geräts zusammenhängt.

Um Details zum Inline-Meilenstein anzuzeigen, wählen Sie die Spalte aus. Das Fenster Meilensteindetails wird geöffnet.

Folgende Status sind für Meilensteine verfügbar:

- Nicht gestartet
- Ausgeführt
- Completed
- Fehler



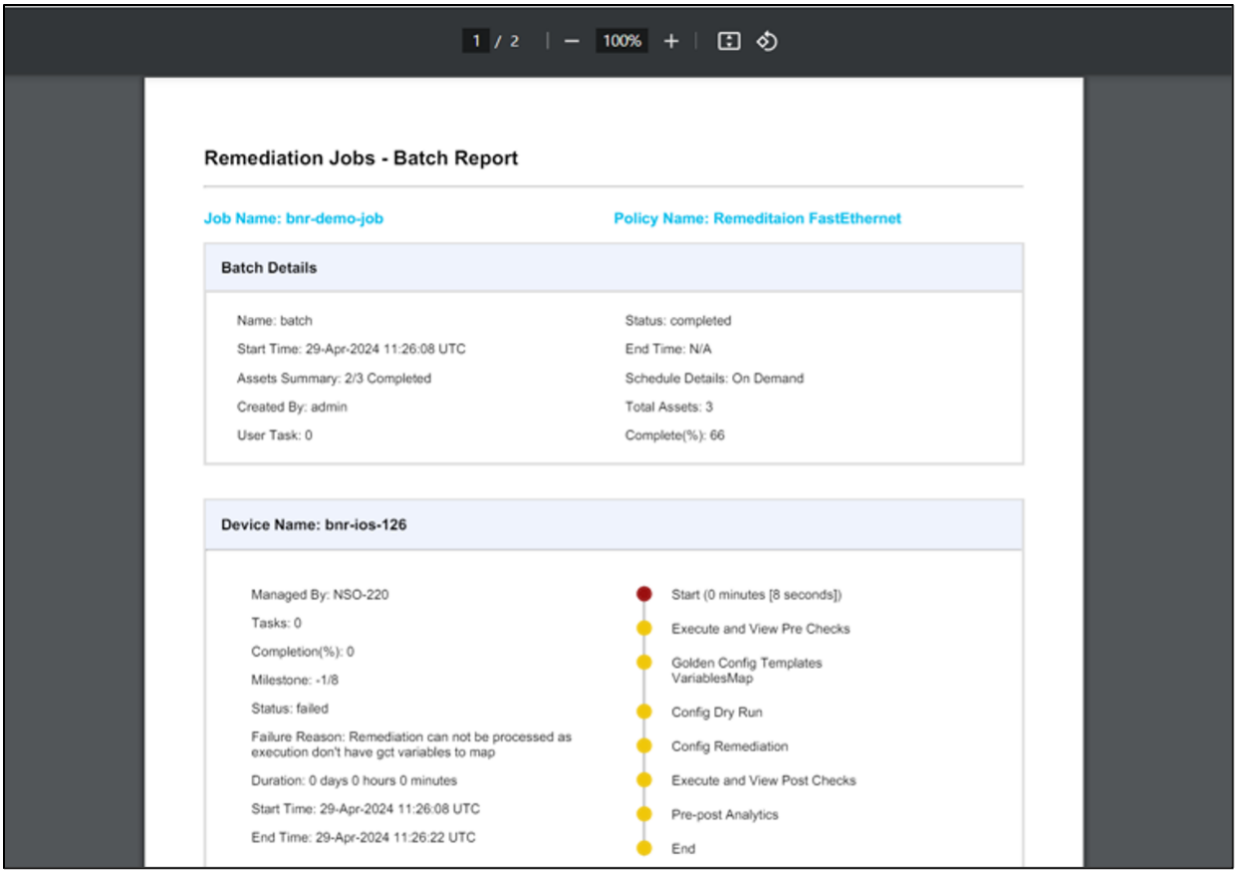

Problembehebung: Details zum Inline-Meilenstein

## Problembehebung: Generieren und Herunterladen von PDF-Berichten mit Stapelübersicht

Batch-Übersichten können erstellt und heruntergeladen werden.

So laden Sie den zusammenfassenden Bericht als PDF pro Stapel herunter:

1. Klicken Sie auf das Symbol Weitere Optionen > Bericht erstellen. Das System überprüft intern, ob der Bericht bereit ist. Wenn der Bericht fertig ist, ist die Option Bericht herunterladen aktiviert.
2. Wählen Sie das Symbol Weitere Optionen > Bericht herunterladen aus. Die PDF wird heruntergeladen.



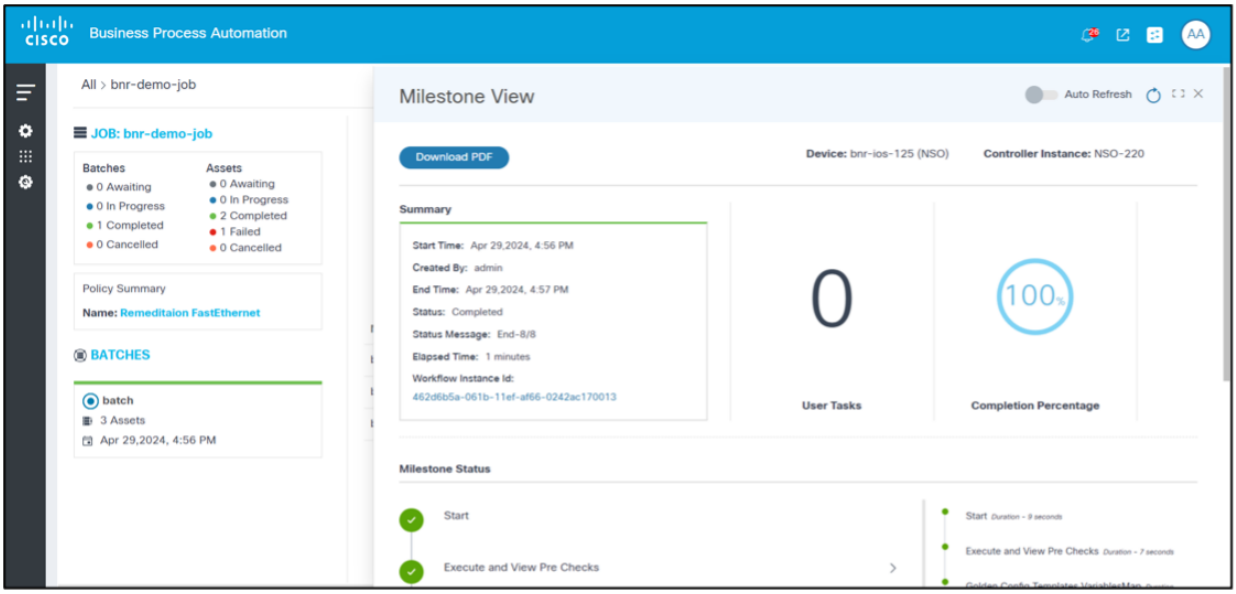
Batch-Zusammenfassungsbericht - PDF

Die Auswertung "Reparaturaufträge - Stapel" enthält einen Abschnitt "Stapeldetails", der eine Zusammenfassung des Korrekturstapels enthält, z. B. Name des Auftrags, Stapelname, Start- und Endzeit, Summe der Ressourcen und Gesamtstatus. Anschließend folgt ein Abschnitt mit Gerätedetails (ein Abschnitt pro Gerät), der den Gerätenamen, den gerätespezifischen Sanierungsstatus, den Zeitplan, die Dauer, die Liste der Meilensteine und den Status enthält.

Problembehebung: Gerätedetails

Um Gerätedetails für Meilensteine anzuzeigen, wählen Sie die Seite Device Details (Gerätedetails) aus. Die Seite Meilensteinansicht wird angezeigt.

Es wird eine Zusammenfassung der Fehlerbehebung für das jeweilige Gerät mit einem detaillierten Meilensteinstatus angezeigt, einschließlich der Befehlsausgabe aller abgeschlossenen Meilensteine. Beispielsweise können die Befehlsausgaben der Prozessvorlage, die GCT-Trockenausgabe und der Inhalt der Analysedifferenzausgabe angezeigt werden.



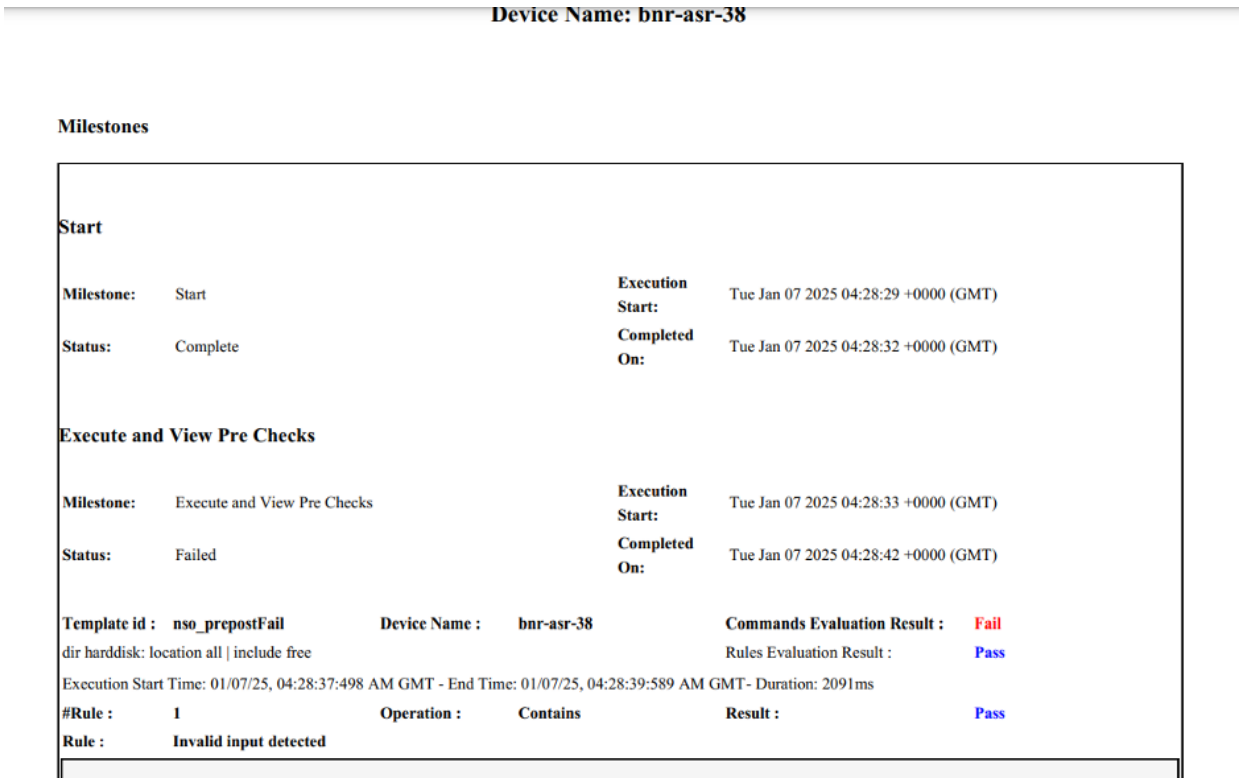

Problembehebung: Meilensteinansicht

Problembehebung: Gerätedetails - Meilensteinbericht

So zeigen Sie den Meilensteinbericht an:

1. Wählen Sie die Seite Device Details (Gerätedetails) aus. Die Seite Meilensteinansicht wird angezeigt.
2. Klicken Sie auf PDF herunterladen. Der Meilenstein-Ansichtsbericht wird wie unten gezeigt generiert und heruntergeladen.

Dieser Bericht enthält detailliertere Informationen zu Meilensteinen und den entsprechenden Inhalten für die Behebung des ausgewählten Geräts.



**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**

Problembehebung: Gerätedetails - Meilenstein PDF-Bericht anzeigen

# Konfiguration: Blöcke und Regeln

## Funktionalität der Blöcke

Konfigurationsblöcke sind wichtige Elemente für die Erstellung und Durchsetzung von Compliance-Richtlinien in Netzwerkmanagementsystemen. Sie stellen CLI-Gerätekonfigurationen dar, z. B. für Schnittstellen, das Router Border Gateway Protocol (BGP) usw. Nachfolgend sind die wichtigsten Funktionen von Konfigurationsblöcken aufgeführt:

- Modularität: Konfigurationsblöcke ermöglichen die Erstellung modularer Richtlinien, sodass Administratoren separate Abschnitte von Gerätekonfigurationen unabhängig definieren und verwalten können. Diese Modularität vereinfacht die Aktualisierung und Einhaltung von Compliance-Richtlinien.
- Granularität: Durch die Aufteilung von Gerätekonfigurationen in kleinere, verwaltbare Teile können Administratoren präzise Konformitätsprüfungen durchführen und bestimmte Standards durchsetzen. So wird sichergestellt, dass jeder Teil der Gerätekonfiguration den erforderlichen Richtlinien entspricht.
- Wiederverwendbarkeit: Nach der Definition können Konfigurationsblöcke über mehrere Compliance-Richtlinien und Geräte hinweg wiederverwendet werden. Diese Wiederverwendbarkeit reduziert die Redundanz und gewährleistet Konsistenz im Konfigurationsmanagement.
- Statischer Konfigurationsblock: Ein statischer Konfigurationsblock stellt die Raw-

Gerätekonfiguration ohne Variablen dar.

Beispiel: Der folgende Block kann verwendet werden, um eine Konformitätsprüfung für die TwentyFiveGigE0/0/0/31Schnittstelle durchzuführen.

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

- Dynamischer Konfigurationsblock: Ein dynamischer Konfigurationsblock stellt die Gerätekonfiguration dar, die Variablen enthält, die eine bessere Anpassbarkeit und Wiederverwendbarkeit ermöglichen. Diese Blöcke funktionieren wie eine TTP-Vorlage, werden auf die Gerätekonfigurationen angewendet und rufen die Werte für die Variablen ab. Regeln können Bedingungen hinzugefügt werden, um diese Variablen zu validieren. Weitere Informationen zu TTP finden Sie unter https://ttp.readthedocs.io/en/latest/Overview.html.

  Beispiel: Der folgende Block kann verwendet werden, um eine Konformitätsprüfung für alle TwentyFiveGigE-Schnittstellen durchzuführen

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

Dynamischer Konfigurationsblock mit Unterhierarchien: Dieser Block funktioniert wie ein dynamischer Konfigurationsblock und wird verwendet, um Werte aus Gerätekonfigurationen mit mehreren Hierarchien abzurufen.

Beispiel: Im folgenden Beispiel werden eine Gerätekonfiguration und der entsprechende dynamische Block veranschaulicht, mit dem Werte aus einer hierarchischen Struktur abgerufen werden.

Hierarchische Gerätekonfiguration:

```
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
```

Dynamische Blockkonfiguration zum Analysieren der Konfiguration oben.

```
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
```

## Funktionalität von Regeln

Mithilfe von Regeln können Benutzer Bedingungen definieren, die anhand von Variablen in einem Konfigurationsblock validiert werden. Im Rahmen einer Ausführung analysiert das Compliance-Modul die Gerätekonfiguration, findet übereinstimmende Instanzen von Geräteblockinstanzen, liest Werte aus den Zeilen und führt die in den Regeln definierten Bedingungen für die Werte aus. Das Ergebnis wird zur Anzeige im Dashboard gespeichert, unabhängig davon, ob in den Konfigurationspositionen eine Verletzung aufgetreten ist.

Konfigurationsregeln sind jetzt Teil des Lebenszyklus für die Blockerstellung. Daher gibt es keine separate Seite zum Anzeigen von Regeln. Regeln können auf der entsprechenden Seite zum Erstellen oder Aktualisieren von Blöcken aufgelistet, erstellt und aktualisiert werden.

Im CnR-Framework spielen Regeln eine entscheidende Rolle bei der Validierung von Konfigurationen anhand festgelegter Bedingungen. Dieser Abschnitt bietet einen Überblick über die Integration und Verwaltung von Regeln im System.

- Zweck: Mithilfe von Regeln können Benutzer Bedingungen definieren, mit denen Variablen in einem Konfigurationsblock validiert werden.
- Ausführungsprozess:
    - Die Compliance-Engine analysiert die Gerätekonfiguration.
    - Identifiziert übereinstimmende Instanzen von Geräteblockinstanzen
    - Extraktion von Werten aus den Konfigurationspositionen
    - Wendet die in den Regeln definierten Bedingungen auf diese Werte an
    - Ergebnisse, die Verstöße anzeigen, werden gespeichert und im Dashboard angezeigt.

Integration in Blockierungslebenszyklus

- Lebenszyklus-Integration: Konfigurationsregeln sind jetzt ein integraler Bestandteil des Lebenszyklus für die Erstellung von Blöcken
- Verwaltung:
  - Regeln werden direkt auf den Seiten aufgelistet, erstellt und aktualisiert, die zur Erstellung oder Aktualisierung von Blöcken verwendet werden.
  - Es gibt keine separate Seite zum Anzeigen von Regeln, um deren Verwaltung innerhalb des Blocklebenszyklus zu optimieren.

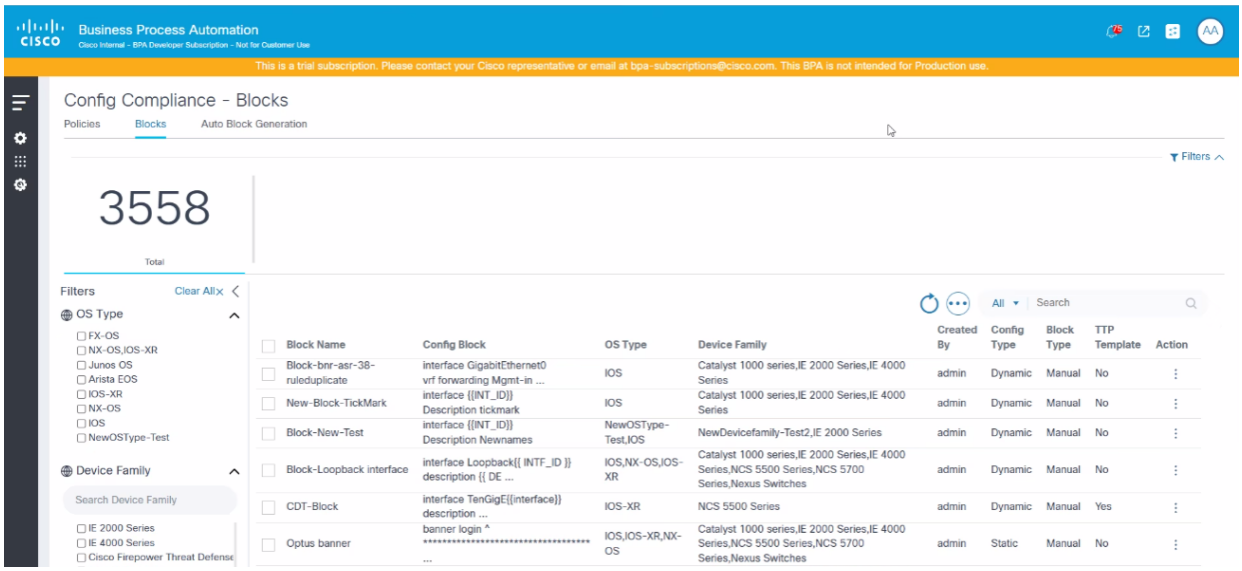
Durch diese Integration werden Compliance-Prüfungen nahtlos in den Konfigurationsmanagementprozess integriert, sodass Gerätekonfigurationen anhand vordefinierter Regeln effizient überwacht und verwaltet werden können.

## Listenblöcke

Auf der Seite Blöcke werden alle Konfigurationsblöcke aufgelistet und Aktionen zum Generieren, Hinzufügen, Bearbeiten, Löschen, Importieren und Exportieren von Blöcken beschrieben. Benutzer können Blockdetails filtern, sortieren und anzeigen.

Details zum Funktionsblock

- Gesamtzahl: Zeigt die Gesamtzahl der erstellten Blöcke an
- Filteroptionen:
  - Betriebssystemtypen und Gerätefamilie: Ermöglicht Benutzern das Filtern von Blöcken anhand ausgewählter Kriterien
- Hauptraster:
  - Zeigt eine Standardliste von Blöcken an.
  - Benutzer können die Liste sortieren, indem sie auf die Spaltenüberschriften klicken
  - Enthält eine Suchfunktion, mit der Benutzer nach allen Attributen oder speziell nach Blocknamen suchen können.
  - Unterstützt Paginierung für einfaches Navigieren durch die Liste
- Aktionen:
  - Bearbeiten: Benutzer können vorhandene Blöcke ändern
  - Löschen: Benutzer können Blöcke aus der Liste entfernen



Liste der Konfigurationsblöcke

## Hinzufügen oder Bearbeiten von Blöcken und Regeln

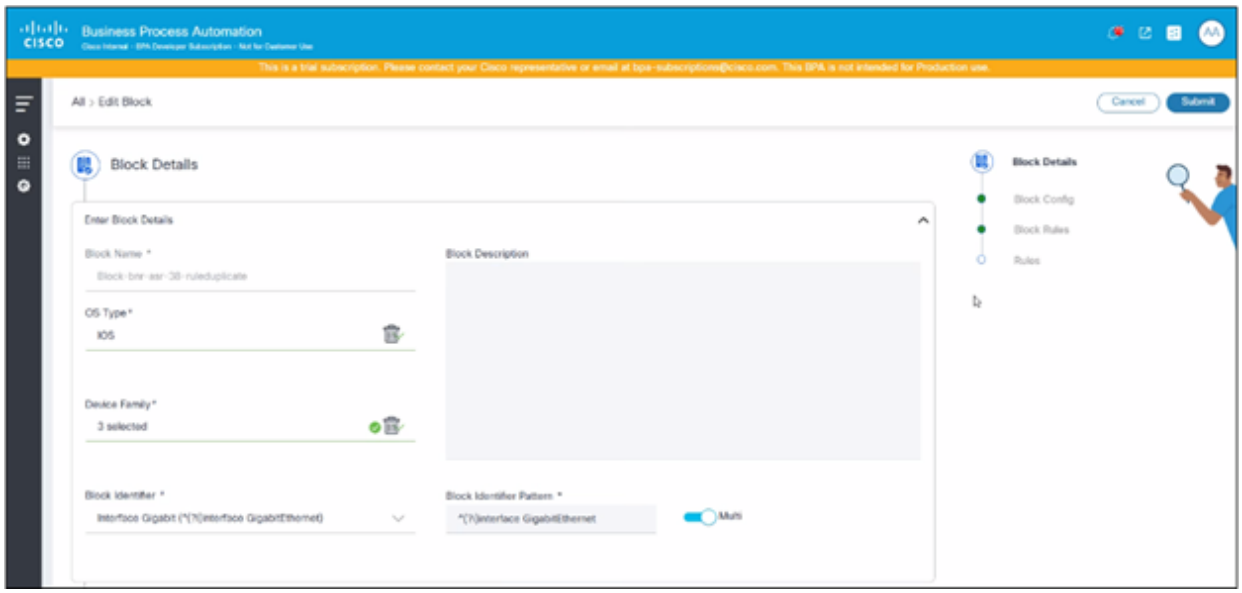
Auf der Seite Hinzufügen oder Bearbeiten von Blöcken können Sie wichtige Informationen zu Blöcken erfassen und verwalten. Diese Seite enthält die folgenden Abschnitte:

- Allgemeine Blockdetails:

  Der Abschnitt Grundlegende Details umfasst Folgendes:

  - Blockname: Zugewiesener Name für den Block
  - Beschreibung: Eine kurze Übersicht oder Erläuterung des Zwecks oder der Funktionalität des Blocks
  - BS-Typ: Dem Block zugeordneter Betriebssystemtyp
  - Gerätefamilie: Kategorie oder Gruppe von Geräten, die mit dem Block kompatibel sind
  - Auswahl der Blockkennung: Optionen zur Auswahl einer eindeutigen Kennung für den Block
  - Blockbezeichnerdetails hinzufügen oder bearbeiten: Wenn kein geeigneter Blockbezeichner vorhanden ist, können die folgenden Blockbezeichnerdetails mithilfe derselben Felder hinzugefügt oder bearbeitet werden:

    - Name der Blockkennung: Der spezifische Name für die Blockkennung
    - Muster: Das Muster oder Format, dem die Blockkennung folgt
    - Mehrere: Umschalten, um anzugeben, ob der Konfigurationsblock als mehrzeilige Konfiguration behandelt werden soll

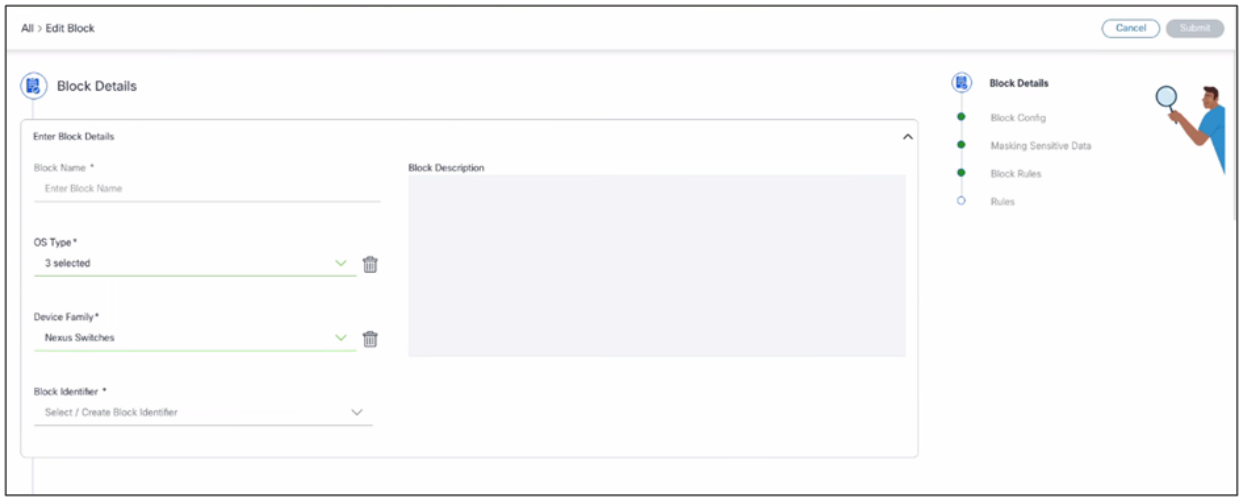



Blöcke hinzufügen oder bearbeiten - Blockdetails

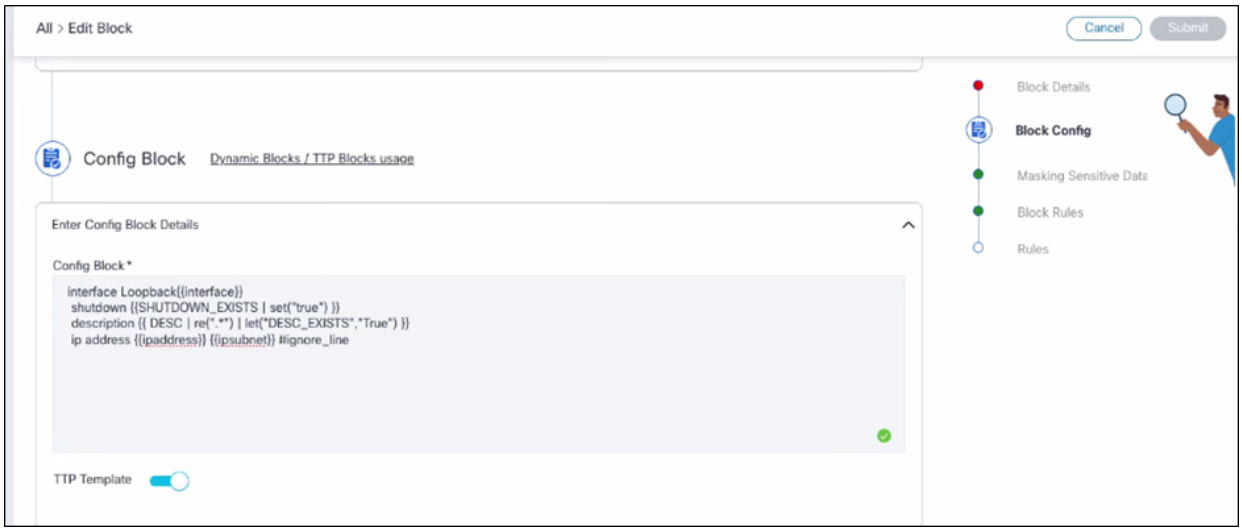
- Konfiguration sperren:

Der Abschnitt Blockkonfiguration umfasst:

- Konfigurationsblock: Stellt die Konfiguration eines Geräts mit verschiedenen Variablen dar. In dieser Konfiguration wird erläutert, wie das Gerät innerhalb des Systems eingerichtet und verwaltet werden soll.
- TTP-Vorlage: Gibt an, ob der Block als TTP-Vorlage (Template Transformation Protocol) festgelegt wurde, um die Blöcke zu identifizieren, die als Vorlagen für die geräteübergreifende Transformation oder Standardisierung von Konfigurationen verwendet werden.




Details sperren



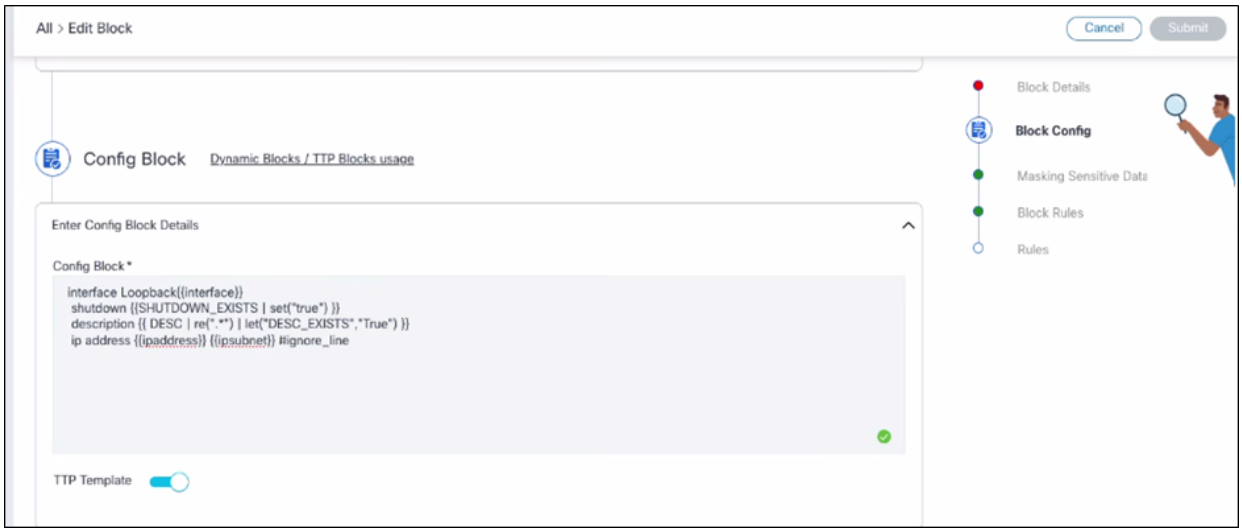

Konfiguration sperren

## Verwenden der Zeilensyntax ignorieren

Mit der Syntax "Zeilen ignorieren" können Benutzer einen Kommentar am Ende einer bestimmten Konfigurationszeile in einem Block hinzufügen, um das System anzuweisen, Compliance-Prüfungen oder Verstöße in dieser Zeile zu überspringen. Dadurch wird verhindert, dass der Posten in Berichten oder Dashboards als Verletzung angezeigt wird.

Führen Sie die folgenden Schritte aus, um die Syntax zum Ignore Line (Leitung ignorieren) zu verwenden:

1. Suchen Sie die Konfigurationszeile, die von den Konformitätsprüfungen ausgeschlossen werden soll (z. B. die IP-Adresse).




Zeilensyntax ignorieren

2. Hängen Sie die Zeile an, indem Sie die Kommentarsyntax "#ignore_line" am Ende der Zeile

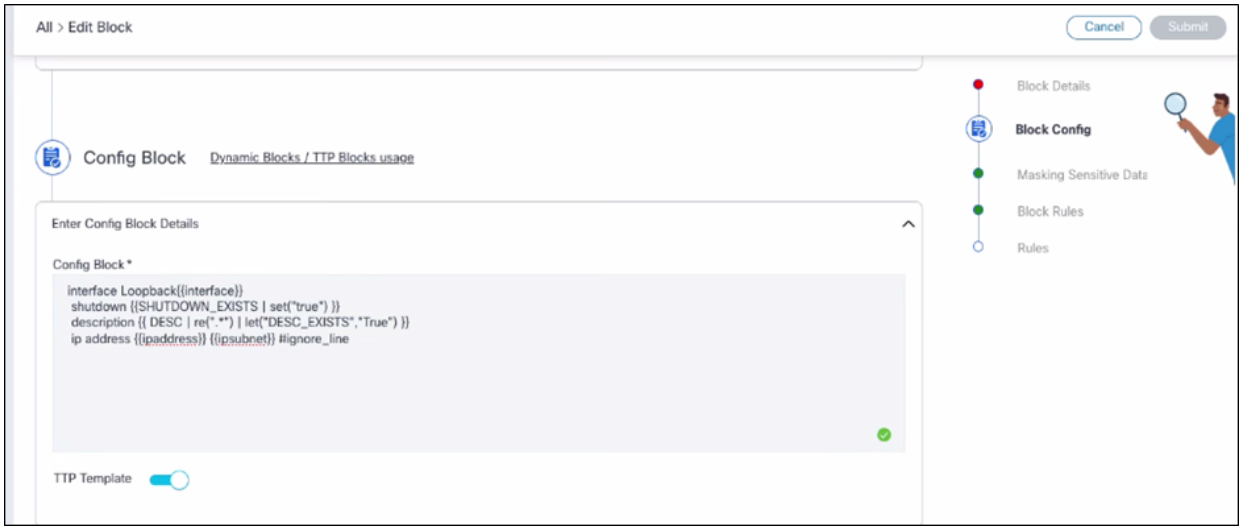
verwenden. Beispiel: ip address {{ipAddress}} {{ipSubnet}} #ignore_line

## Anstiftung zu Verstößen

Mit dieser Funktion zum Analysieren von Vorlagentext (TTP) in der Blockkonfiguration kann angegeben werden, ob eine Verletzung ausgelöst werden soll, wenn eine bestimmte Zeile vorhanden ist.

Gehen Sie wie folgt vor, um die TTP-Funktion zu verwenden:

1. Suchen Sie auf der Seite zum Erstellen oder Bearbeiten des Blocks im Abschnitt Blockkonfiguration nach der zu steuernden Konfigurationszeile.
2. Definieren Sie eine TTP-Variable mithilfe des Befehls set oder let wie folgt:
   - Wenn die Konfigurationszeile heruntergefahren ist, definieren Sie mit dem Befehl set eine Variable wie folgt:
     herunterfahren | {{SHUTDOWN_FLAG} | set("true")}"
   - Wenn Benutzer eine vorhandene Variable in der Konfigurationszeile wie die Beschreibung {{DESC}} haben, verwenden Sie den Befehl let wie folgt:
     description {{ DESC | re(".*") | let("DESC_EXISTS", "True") }}
3. Verwenden Sie diese Variablen (SHUTDOWN_FLAG oder DESC_EXISTS im obigen Beispiel) in einer Regel, um Verletzungen auszulösen.




Verstöße hervorrufen

Wirkung:

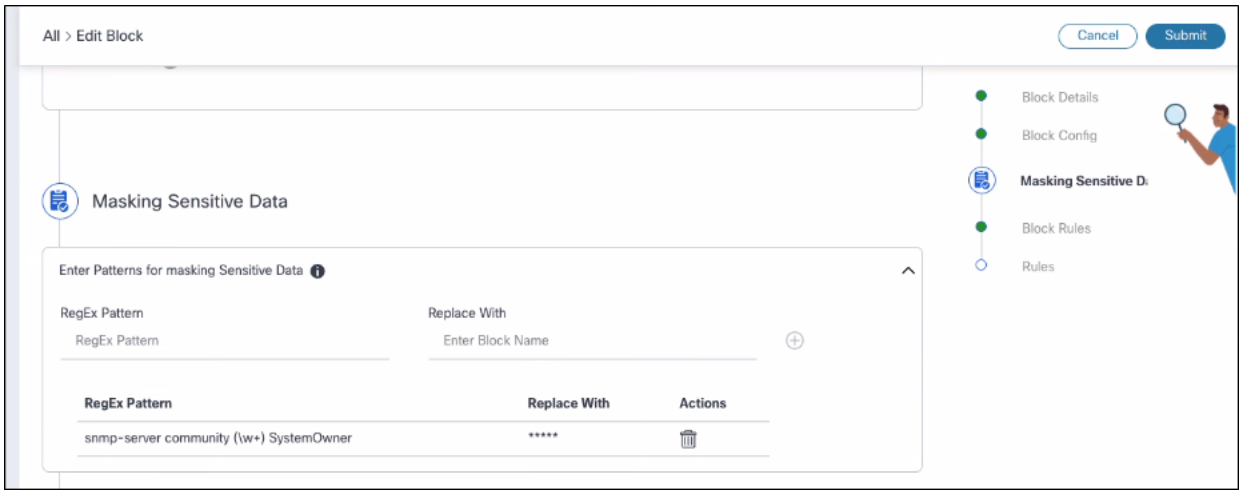
Eine Verletzung wird auf der Dashboard-Seite angezeigt, wenn die Zeilen "shutdown" oder "description config" in der Gerätekonfiguration verfügbar sind. Der Schweregrad der Verletzung hängt von der Auswahl bei der Regelerstellung ab.

- Sensible Daten maskieren:

Maskenvertrauliche Daten ist eine Funktion, mit der Benutzer Muster mithilfe von regulären Ausdrücken definieren können, um vertrauliche Informationen (wie Kennwörter oder Schlüssel) in Gerätekonfigurationen zu identifizieren und zu maskieren. Dadurch wird verhindert, dass vertrauliche Daten in Verletzungsansichten oder bei Konfigurationsabweichungen angezeigt werden, indem übereinstimmende Daten durch eine bestimmte Maske (z. B. "***") ersetzt werden.

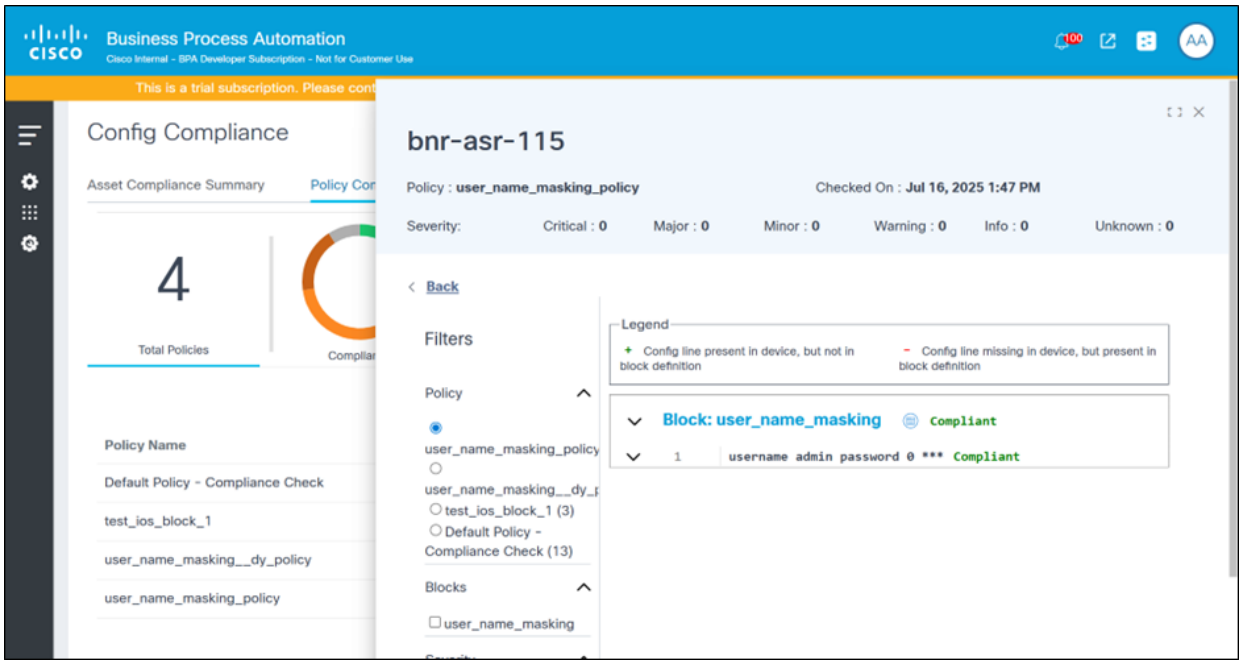
Gehen Sie wie folgt vor, um vertrauliche Daten zu maskieren:

1. Im Abschnitt "Maskenvertrauliche Daten":
    - Hinzufügen mehrerer regulärer Ausdrucksmuster (Regex) zum Identifizieren vertraulicher Daten
    - Geben Sie die Ersetzungszeichenfolge an, um die übereinstimmenden Daten zu maskieren (z. B. ""). Beispielsweise kann das Regex-Muster mit einem Kennwort gefüllt werden (um mit einem beliebigen Text zu beginnen, der mit "Kennwort" gefolgt von einem Wort beginnt), und die Ersetzung sollte erfolgen.
2. Fügen Sie so viele Regex-Muster wie nötig hinzu. sie werden im Rasterformat angezeigt



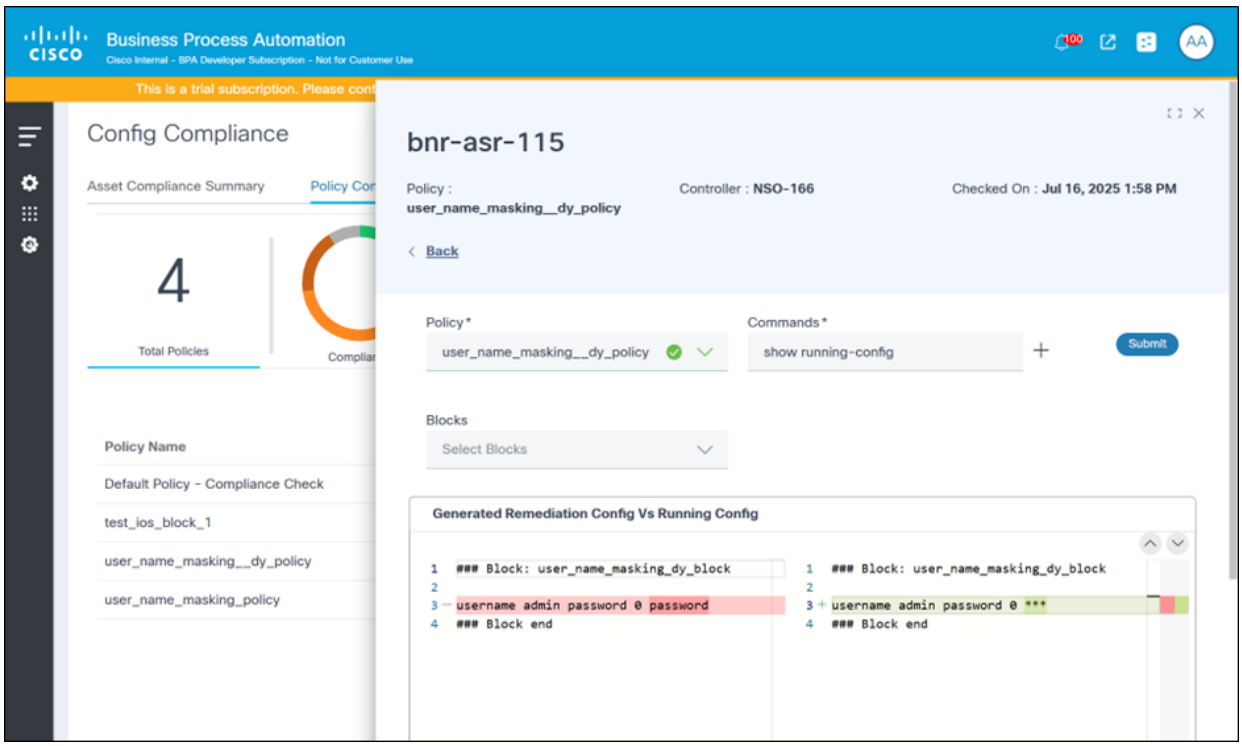

Sensible Daten maskieren

3. Löschen Sie alle Muster aus der Liste, wenn sie nicht mehr benötigt werden.
4. Das System verwendet die regulären Ausdrücke, um passende sensible Gerätekonfigurationsdaten zu finden und durch die angegebene Maske (z. B. "***") zu ersetzen. Diese Maskierung wird auf den folgenden Seiten verwendet:
    - Compliance-Dashboard > Betroffene Ressourcen > Seite "Verstöße anzeigen": Die in der Benutzeroberfläche angezeigten Konfigurationsdaten sowie ein Bericht zur Ressourcenkonformität, der auf der Grundlage dieser Verletzungsdetails generiert wurde




Vertrauliche Daten auf der Seite "Verletzungen anzeigen" maskieren

- Compliance-Dashboard > Korrekturkonfiguration anzeigen > Seite "Korrekturunterschied anzeigen": Die Gerätekonfigurationsdaten zeigen maskierte vertrauliche Daten entsprechend den Maskeneinstellungen des Blocks an.

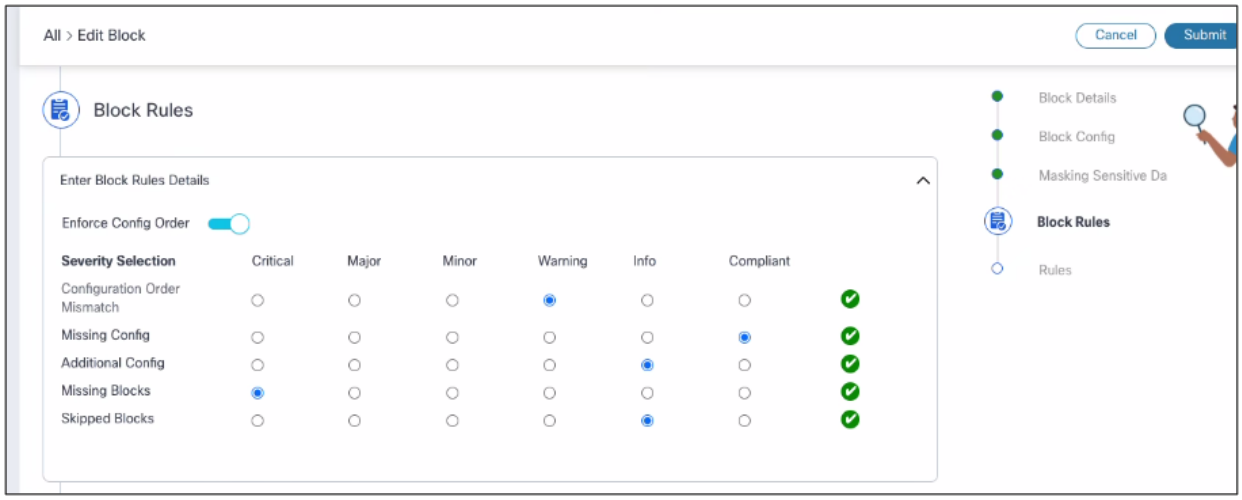



Vertrauliche Daten in Korrekturdiff-Seite maskieren

- Blockierungsregeln (Auswahl des Schweregrads):

  Der Abschnitt Blockierungsregeln umfasst:

- Config-Bestellung durchsetzen: Stellt sicher, dass Konfigurationsposten bei Konformitätsprüfungen in der richtigen Reihenfolge angezeigt werden. Die Compliance-Engine vergleicht die Reihenfolge der Konfigurationsposten mit der erwarteten Bestellung.
- Auswahl des Schweregrads: Ermöglicht es Benutzern, Verletzungen innerhalb eines Blocks einen Schweregrad zuzuweisen. Die Schweregrade helfen dabei, Compliance-Probleme effektiv zu priorisieren und zu verwalten.
- Konfigurationsauftragskonflikt: Identifiziert Abweichungen in der Reihenfolge der Konfigurationsposten und gibt Warnmeldungen aus, wenn die Reihenfolge der Gerätekonfigurationsposten nicht mit der erwarteten Reihenfolge übereinstimmt.
- Fehlende Konfiguration:
  - Erkennt fehlende Konfigurationszeilen
  - Hebt erwartete Konfigurationszeilen hervor, die in der Gerätekonfiguration nicht vorhanden sind.
  - Überprüft, ob der gesamte Gerätekonfigurationsblock fehlt oder nicht der definierten Blockkonfiguration entspricht
- Zusätzliche Konfiguration:
  - Identifizierung unerwarteter Konfigurationszeilen
  - Zeigt die in der Gerätekonfiguration vorhandenen, jedoch nicht erwarteten Konfigurationszeilen gemäß der Blockkonfiguration an.
- Übersprungene Blöcke:
  - Zeigt nicht aktivierte Konfigurationsblöcke an
  - Der Block wird übersprungen, wenn er die angegebenen Filterbedingungen nicht erfüllt



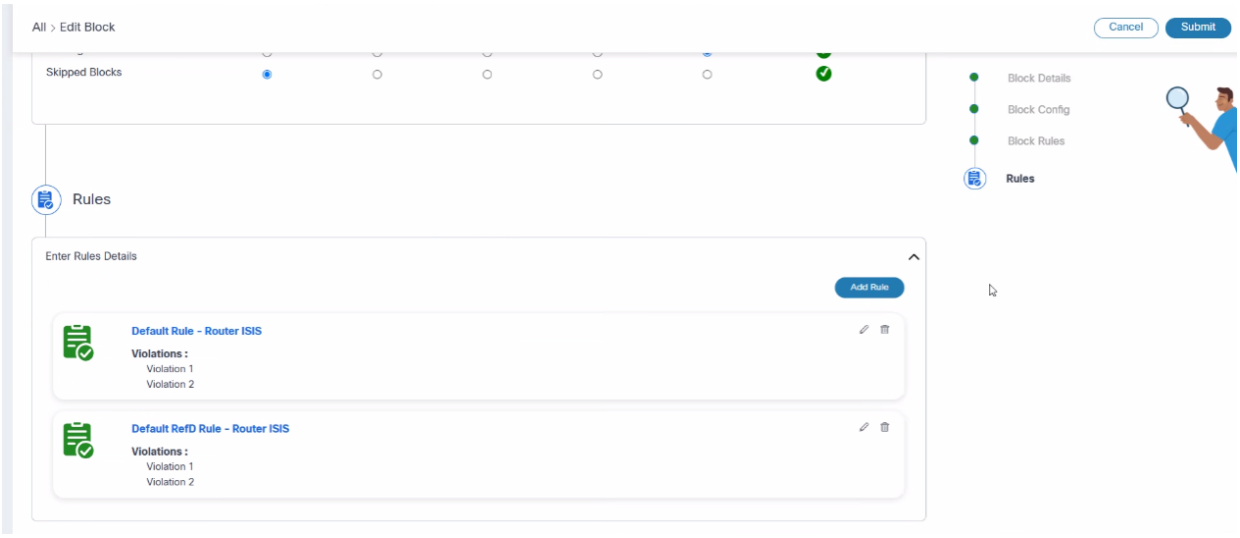
Hinzufügen oder Bearbeiten von Blöcken - Blockregeln

## Regelmanagement

Im CnR-Framework können Benutzer Blockregeln über die Schnittstelle "Blöcke hinzufügen oder bearbeiten" verwalten. Diese Funktion ist wie im folgenden Abschnitt beschrieben aufgebaut:

Anmerkung: Wenn ein Benutzer eine bestimmte Blockebenenverletzung nicht auslösen möchte, kann der Schweregrad "Entspricht" ausgewählt werden.

- Regelkonfiguration:
  - Benutzer können Regeln einrichten und verwalten, die die Compliance Engine zur Validierung von Konfigurationen verwendet
  - Benutzer können Regeln nach Bedarf erstellen, bearbeiten oder löschen
- Regelliste:
  - Bietet eine umfassende Liste aller erstellten Regeln, die Einblick in deren Details bietet
  - Benutzer können vorhandene Regeln bearbeiten oder nicht mehr benötigte Regeln löschen




Hinzufügen und Bearbeiten von Konfigurationsblöcken

Hinzufügen oder Bearbeiten von Regeldetails

- Regelname:
  - Der Regel einen eindeutigen Namen zur Identifizierung zuweisen
  - Dieses Feld ist obligatorisch, damit jede Regel eindeutig erkannt werden kann.
- Standardregel:
  - Festlegen, ob die Regel als Standardregel festgelegt werden soll
  - Benutzer können diese Einstellung aktivieren, um die Regel innerhalb des Compliance-Frameworks als Standard festzulegen.
- Beschreibung:
  - Stellt zusätzlichen Kontext oder Informationen über die Regel bereit
  - Dieses Feld ist optional, kann jedoch für die Dokumentation und Klarheit hilfreich sein.
- Verstöße:
  - Liste der Regelverletzungen verwalten
  - Benutzer können Verstöße nach Bedarf hinzufügen, bearbeiten oder löschen.

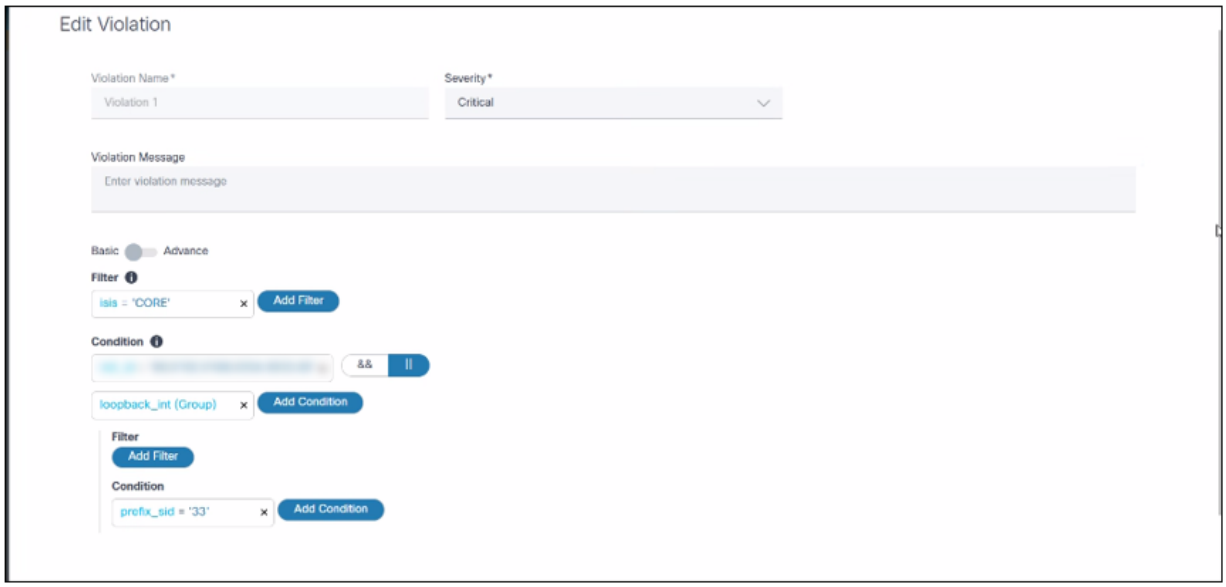
| | A | B | C | D | E | F | G | H | I | J | K |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Device Name | Managed By | Product Family | Compliance | Critical | Major | Minor | Warning | Info | Unknown | Last Checked |
| 2 | CNC-bnr-asr-78 | Direct-To-Device | IE 2000 Series | Non Compliant | 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 | | | | | | | | | | | |

Hinzufügen oder Bearbeiten von Blöcken - Regeln: Regel hinzufügen oder bearbeiten

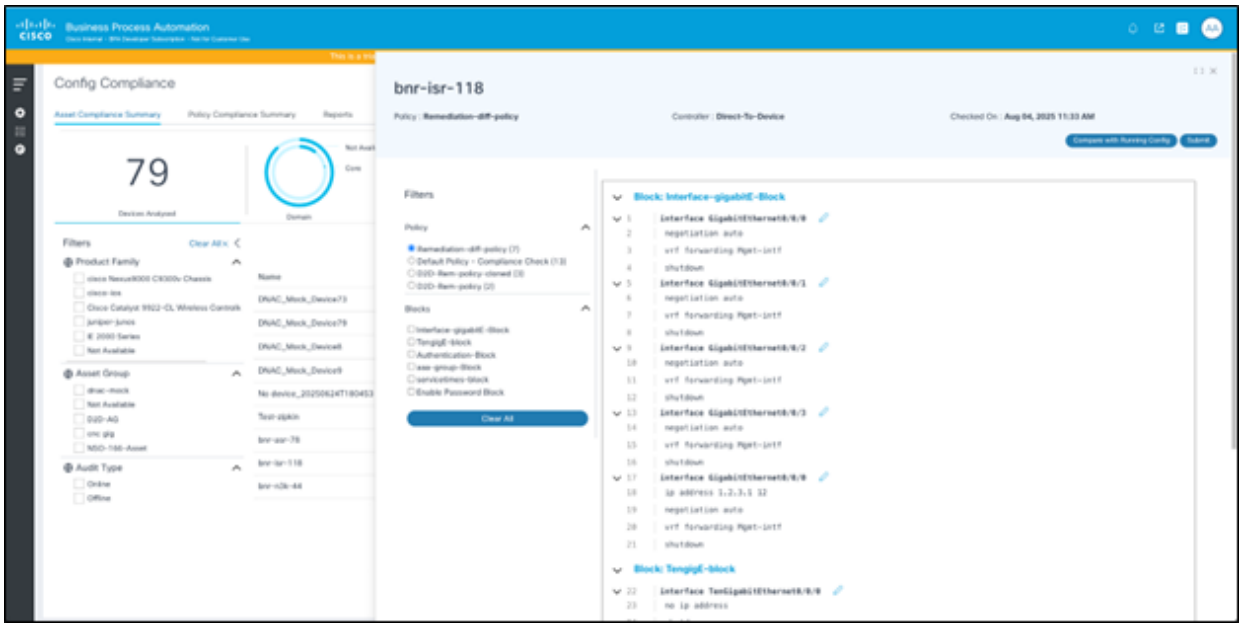
Hinzufügen oder Bearbeiten von Regelverletzungen

Regelverletzungen sind eine wichtige Komponente bei der Compliance-Ausführung und enthalten detaillierte Angaben zu den durchzuführenden Prüfungen. Nachfolgend finden Sie einen Überblick darüber, wie Regelverletzungen erstellt und verwaltet werden können:

- Standardmodus:
  - Elemente der Benutzeroberfläche: In diesem Modus können Benutzer Regelverletzungen über eine grafische Benutzeroberfläche (GUI) erstellen. Dieser Ansatz ist in der Regel benutzerfreundlicher und für diejenigen zugänglich, die es vorziehen, sich nicht mit Programmierung zu beschäftigen.
  - Schrittweise Anleitung: Benutzer werden durch den Prozess des Definierens von Prüfungen mithilfe vordefinierter Benutzeroberflächenelemente geführt.
- Erweiterter Modus:
  - JSON-ähnliches Codeformat: Für Benutzer, die sich mit der Programmierung auskennen, ermöglicht dieser Modus die Erstellung von Regelverletzungen durch Eingabe in einem strukturierten, JSON-ähnlichen Format.
  - Flexibilität und Präzision: Diese Methode bietet mehr Flexibilität und Präzision für das Definieren komplexer Regelprüfungen.




Regelverletzungen erstellen oder bearbeiten - Standardmodus



Regelverletzungen erstellen oder bearbeiten - erweiterter Modus

Regelverletzungen werden in die folgenden Abschnitte unterteilt:

- Name der Verletzung: Name der Verletzung
- Schweregrad: Definiert den Compliance-Schweregrad, wenn diese Verletzung während einer Ausführung fehlschlägt
- Verletzungsmeldung: Die Meldung wird angezeigt, wenn eine Verletzungsprüfung fehlschlägt.
- Filterkriterien für Verstöße: Wendet die Verletzungsbedingungen an, bei denen nicht gruppenspezifische Schemavariablen verwendet werden können.
    - Wird in den Filterkriterien verwendet, um Bedingungen basierend auf einzelnen Datenelementen festzulegen, die nicht Teil einer Gruppe sind.
    - Ermöglicht die Auswahl von Kriterien anhand der Hierarchie und Struktur der Daten und stellt so eine präzise und relevante Filterung sicher
- Bedingungen für Regeln: Tatsächliche Bedingungen zur Überprüfung der Konformität hier können sowohl Gruppen- als auch Nicht-Gruppen-Schemavariablen verwendet werden.
    - Beide Variablentypen werden in Regeln verwendet, um umfassende Bedingungen zu erstellen.
    - Gruppenvariablen: Bedingungen für die Erfassung verwandter Daten zulassen, wodurch gründliche Prüfungen innerhalb strukturierter Gruppen sichergestellt werden
    - Nicht gruppierte Variablen: Zulassen der Anwendung von Bedingungen auf unabhängige Datenelemente für mehr Flexibilität bei der Anwendung von Regeln

## Dynamische benutzerdefinierte Blöcke - Best Practices

- Stellen Sie sicher, dass Variablennamen innerhalb jedes Blocks eindeutig sind.
- Vermeiden Sie die Verwendung von Variablen in Gruppennamen.
- Verwenden Sie für untergeordnete Hierarchiekonfigurationen "<Gruppe>" in Blöcken.

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

- Um Werte für ähnliche Konfigurationszeilen in einer einzelnen Variablen zu erfassen, verwenden Sie die Variable wie folgt: `{{ <<Variablenname>> | Leitung | joinmatch(',') }}`. Schließen Sie die Konfigurationszeile innerhalb von `{{ start }}` und `{{ end }}` ein, wie im folgenden Beispiel gezeigt:

| Gerätekonfiguration | Konfiguration sperren |
|---|---|
| ip domain list vrf Mgmt-intf core.cisco.com<br>ip domain list cisco.com<br>ip domain list east.cisco.com<br>ip domain list west.cisco.com | {{_start_}}<br>ip domain list {{ Domänen \| _line_ \| joinmatch(",") }}<br>{{ _end_ }}<br>ip domain list vrf {{ vrf_name }} {{ vrf_domain }} |

- Um einen Wert zu erfassen, der Leerzeichen aus einer Konfigurationszeile enthält, verwenden Sie die Variable im Block, wie in der folgenden Tabelle dargestellt: `{{ <<Variablenname>> | re(".*") }}`

| Gerätekonfiguration | Konfiguration sperren |
|---|---|
| Schnittstelle HundredGigE0/0/1/31<br>description-Schnittstelle: 12ylaa01 Hg0/0/1/31<br>MTU 9216 | interface {{ INTF_ID }}<br>description {{ INTF_DESC \| re(".*") }}<br>MTU 9216 |

## Verständnis der Regelhierarchie und der RefD-Integration in Regeln und Nicht-RefD-Regeln

Im dynamischen Block TTP gibt es zwei verschiedene Schemas, die bestimmen, wie Konfigurationen strukturiert und validiert werden.

- Gruppenbasiertes Schema:
  - Dieses Schema organisiert Konfigurationen auf hierarchische Weise und stellt eine Beziehung zwischen über- und untergeordneten Elementen her.
  - Ideal für komplexe Konfigurationen, bei denen Elemente logisch verschachtelt und

miteinander verknüpft sind
    - Es können Regeln definiert werden, um die hierarchischen Beziehungen und Abhängigkeiten zwischen verschiedenen Konfigurationselementen zu überprüfen.
- Nicht gruppenbasiertes Schema:
    - Konfigurationen sind in einem flachen Format strukturiert, wobei alle Elemente auf derselben Ebene ohne hierarchische Beziehungen vorhanden sind.
    - Geeignet für einfachere Konfigurationen, bei denen keine Hierarchie erforderlich ist
    - Es können Regeln festgelegt werden, um sicherzustellen, dass jedes Konfigurationselement bestimmte Kriterien erfüllt.

## RefD-Integration

- Zweck des RefD:
    - Rolle: Dient als Tool für das Management lokaler und externer Variablen innerhalb des BPA-Frameworks
    - Funktionalität:
        - Dynamisches Abrufen: Erleichtert den dynamischen Abruf und die Verwaltung variabler Daten und ermöglicht Compliance-Prüfungen zur Anpassung an Datenänderungen in Echtzeit
        - API-Interaktion: Bietet APIs für BPA-Anwendungsfälle für den Zugriff auf diese dynamischen Variablen und Werte und deren Verwaltung, um eine reibungslose Integration in Compliance-Workflows sicherzustellen

Syntax für die Werte der Konformitätsregeln

Der CnR-Anwendungsfall kann in das RefD-Framework integriert werden, um Daten dynamisch im Rahmen von Compliance-Prüfungen und Sanierungs-Workflows zu nutzen. Eine detaillierte Aufschlüsselung, wie diese Integration funktioniert, mit besonderem Schwerpunkt auf der Syntax und den verwendeten Variablentypen, ist unten dargestellt:

- Stichwort: Die Syntax muss mit "RefD" beginnen.
- Parameter: Der Parameter "key" ist in der Syntax obligatorisch
- Beispiel:

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

Variablentypen

- Benutzerdefinierte Variablen:
  - Wird bei der Erstellung von Compliance-Aufträgen konfiguriert.
  - Geltungsbereich: Gilt für alle Ausführungen für den angegebenen Job
  - Syntax: `{$VarName}`
  - Beispiel: `{$SITE}`
- Systemvariablen
  - Durch das Framework vordefiniert, basierend auf Kontextdaten, die während der Ausführung verfügbar sind
  - Das Framework bietet derzeit Zugriff auf das Geräteobjekt.
  - Syntax: `#VarName}`
  - Beispiele:
    - `{{#device.deviceIdentifier}}` - Stellt die Gerätekennung dar
    - `{{#device.additionalAttributes.serialNumber}}` - Stellt die Seriennummer des Geräts dar
- TTP-Variablen
  - In der Blockkonfiguration vorhanden
  - Syntax: `{{ VarName }}`
  - Beispiel: `{{ INT_ID }}`

Non-RefD-Regeln

- Diese Regeln sind wie RefD-Regeln, beginnen jedoch nicht mit dem Schlüsselwort "RefD".
- Beispiel:

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

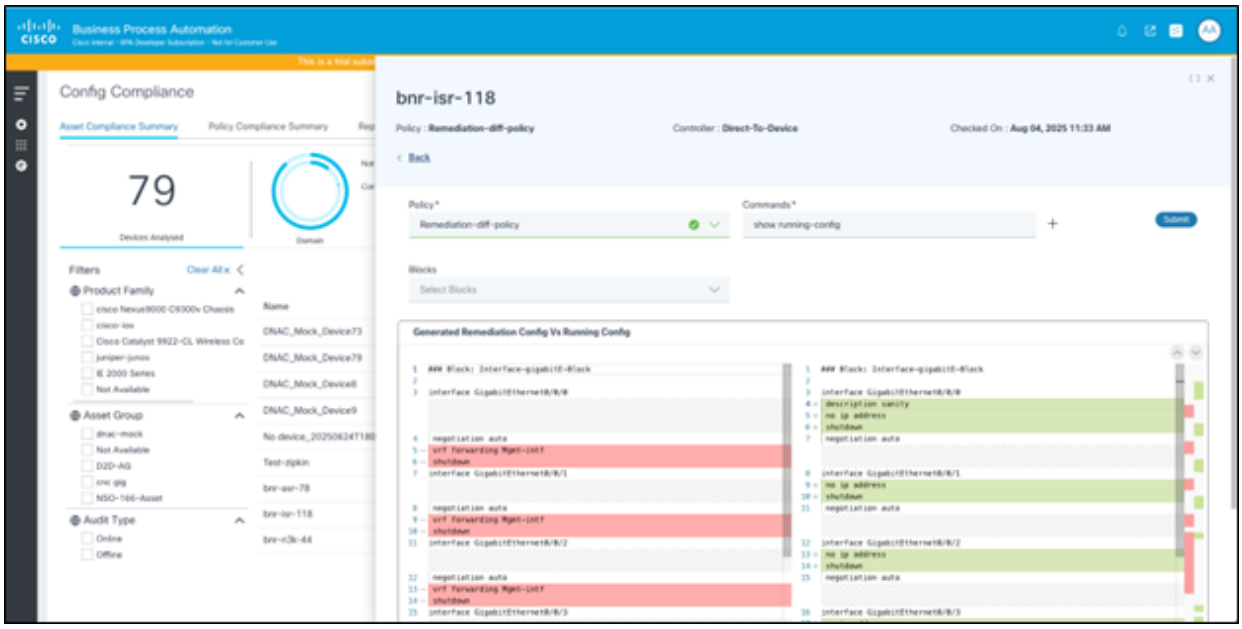
Variablenverwendung

- Benutzerdefinierte Variablen: Dargestellt als `{$Var}`
- Systemvariablen: Wird dargestellt als `{{#Var}}`, wobei Attribute wie deviceIdentifier, controllerId, controllerType usw. verfügbar gemacht werden.
- TTP-Variablen: In doppelten geschweiften Klammern dargestellt als `{{var}}`

Ausführung

- Während der Auftragserstellung können deren Werte festgelegt werden, wenn $-Variablen angegeben werden.
- Die kombinierten Werte der Variablen werden mit der abgerufenen Gerätekonfiguration

verglichen, um die Compliance zu gewährleisten.



Gerätekonfiguration

| | 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 | | | | | | |

Konfigurationsregeln: ReferenzD

## Anzeigen von Blockdetails

So greifen Sie auf Blockdetails zu:

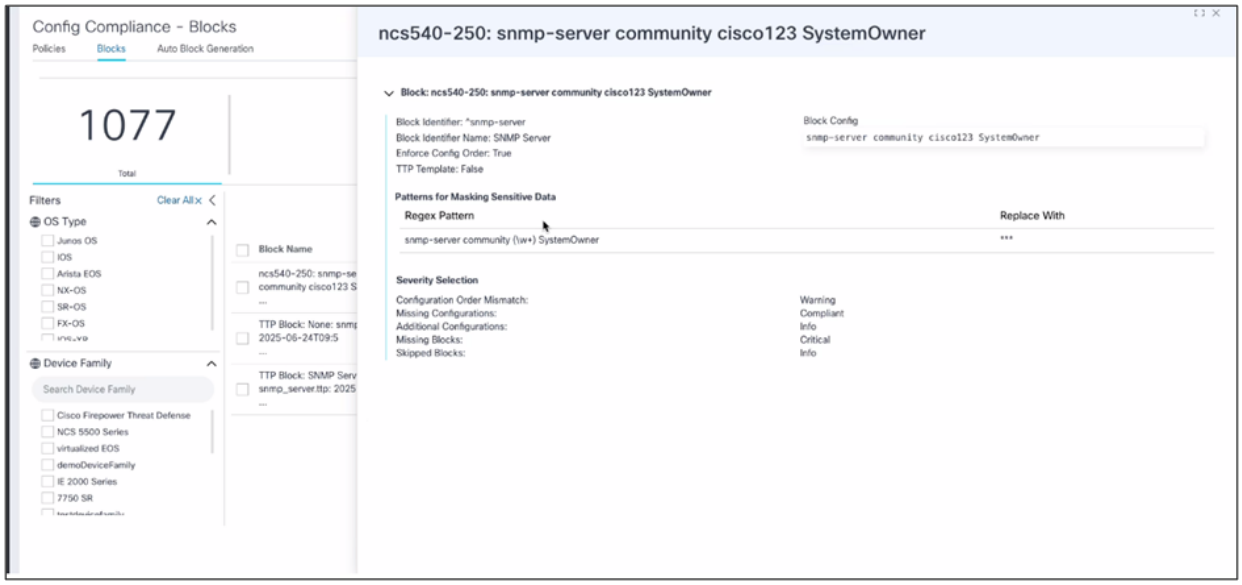
1. Navigieren Sie zur Seite Blöcke.
2. Wählen Sie die Zeile im Raster aus, oder klicken Sie darauf, um die Details des jeweiligen Blocks anzuzeigen.Die Seite Blockdetails wird rechts im Bildschirm angezeigt.

---

Anmerkung: Diese Seite bietet eine schreibgeschützte Ansicht aller Informationen zum Block, einschließlich der zugehörigen Blöcke, Regeln und aller Verletzungen.

---

Durch Klicken auf Hyperlinks innerhalb der Details werden Benutzer zu dem entsprechenden Block oder den zugehörigen Informationen weitergeleitet.




Detailansicht sperren

## Blöcke löschen

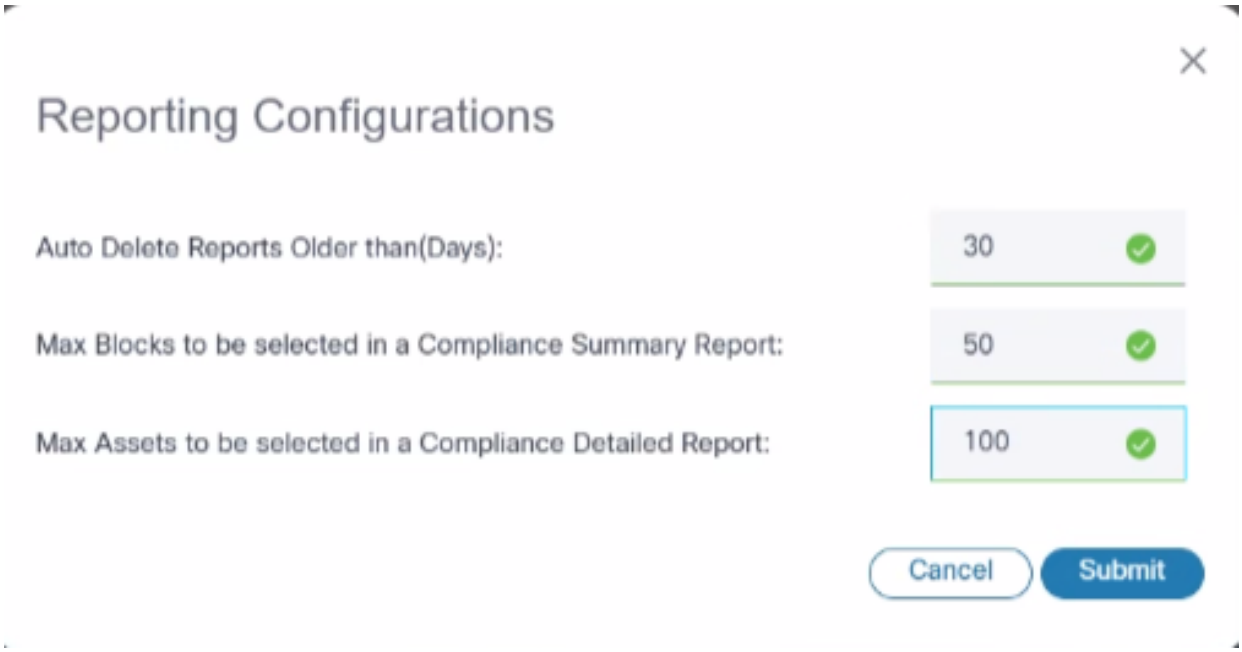
Über das Portal können Benutzer einen oder mehrere Blöcke löschen, sofern sie über die entsprechenden RBAC-Berechtigungen verfügen. Benutzer können diese Aktionen durchführen, indem sie die folgenden Schritte ausführen:

Löschen einzelner Blöcke:

1. Navigieren Sie zur Seite Blöcke.
2. Klicken Sie auf das Symbol Weitere Optionen neben dem zu löschenden Block.
3. Wählen Sie die Option Löschen. Eine Bestätigungsmeldung wird angezeigt.

Löschen mehrerer Blöcke:

1. Navigieren Sie zur Seite Blöcke.
2. Aktivieren Sie die Kontrollkästchen neben jedem zu löschenden Block.
3. Klicken Sie auf das Symbol Weitere Optionen, und wählen Sie Löschen aus. Eine Bestätigungsmeldung.

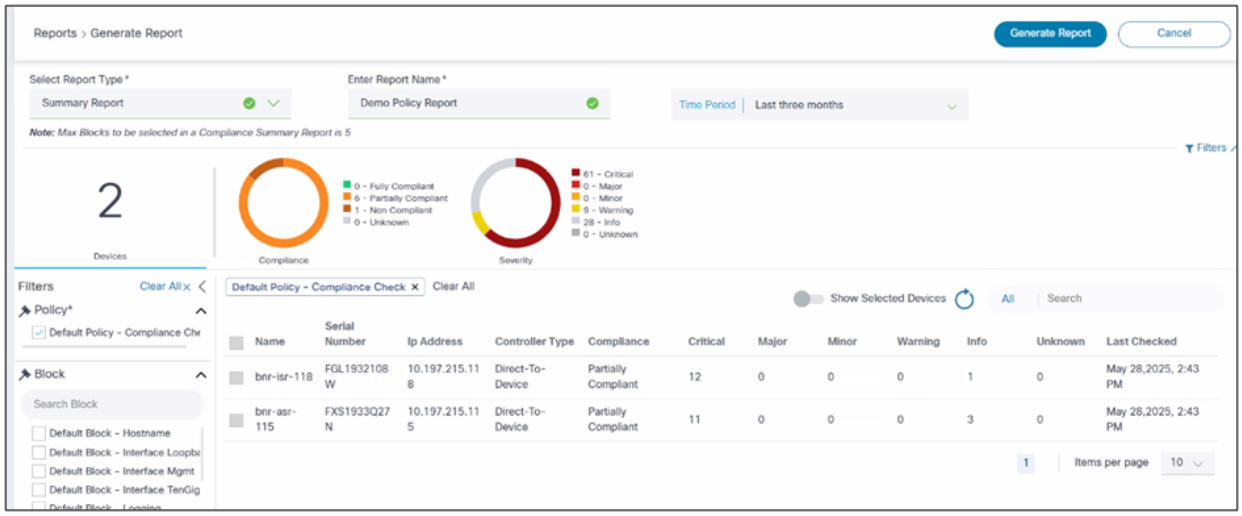



Block löschen

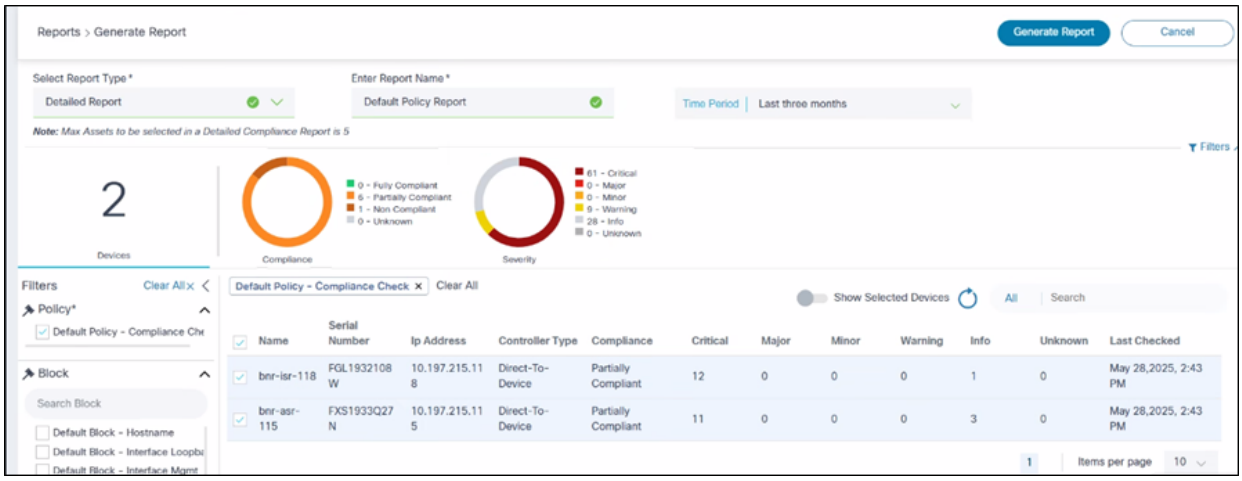
## Konfiguration: Generierung von automatischen Blöcken

Blockgenerierung: Benutzer können Blöcke basierend auf der Konfiguration eines Geräts automatisch erstellen. Diese Automatisierung reduziert den Zeit- und Arbeitsaufwand für die manuelle Erstellung und erleichtert es Benutzern, Blöcke zu bearbeiten, indem Variablen hinzugefügt oder entfernt werden, anstatt von vorne anzufangen.

Klicken Sie auf eine Zeile, um Details zur Blockgenerierung anzuzeigen.

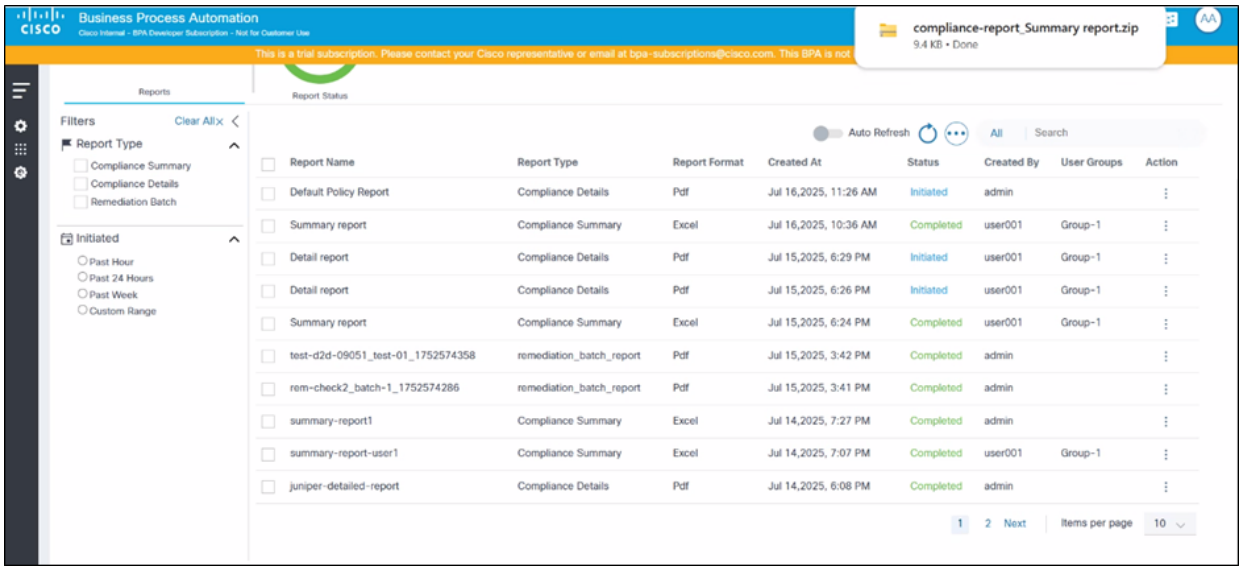



Liste zur automatischen Blockerstellung - Ansicht




Details zur automatischen Blockgenerierung

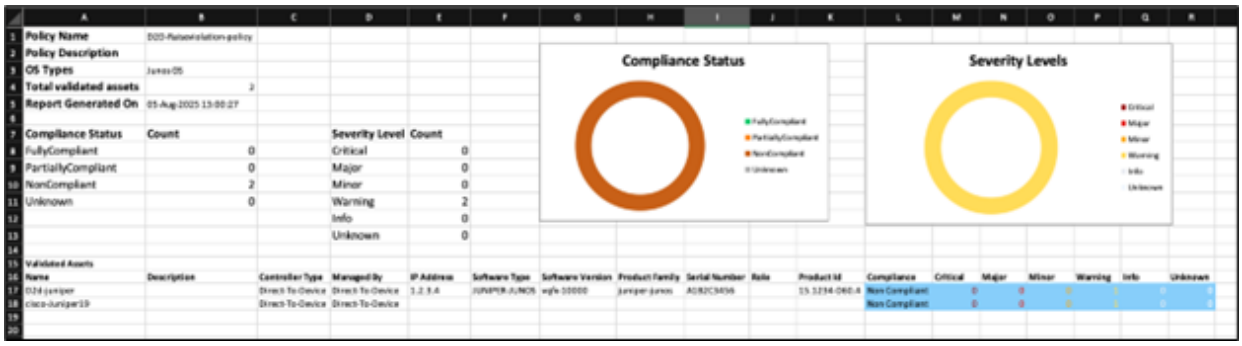
## Generierung von automatischen Blöcken




Liste der automatischen Blockgenerierung

Die Seite "Automatische Blockgenerierung" enthält folgende Felder:

- Generieren aus: Die Quelle, aus der die Blöcke generiert werden. Sie bietet die folgenden drei Optionen:
  - Sicherung der Gerätekonfiguration: Das System wählt eine Gerätekonfiguration aus dem Backup-Anwendungsfall aus

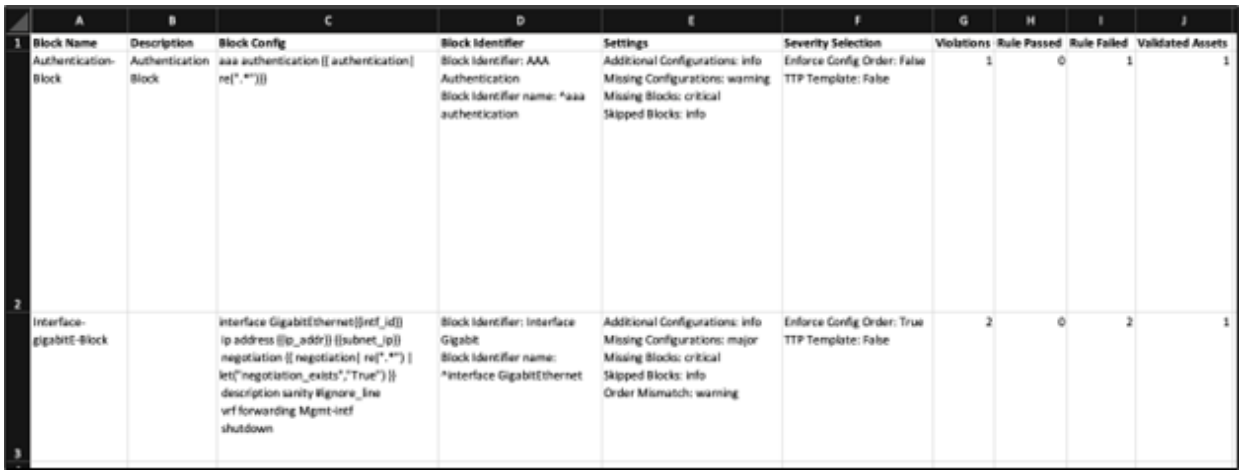


| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Policy Name** | D20-Rulevalidation-policy | | | | | | | | | | | | | | | | | |
| **Policy Description** | | | | | | | | | | | | | | | | | | |
| **OS Types** | Junos OS | | | | | | | | | | | | | | | | | |
| **Total validated assets** | 2 | | | | | | | | | | | | | | | | | |
| **Report Generated On** | 05-Aug-2025 13:00:27 | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| **Compliance Status** | **Count** | | | **Severity Level** | **Count** | | | | | | | | | | | | | |
| FullyCompliant | 0 | | | Critical | 0 | | | | | | | | | | | | | |
| PartiallyCompliant | 0 | | | Major | 0 | | | | | | | | | | | | | |
| NonCompliant | 2 | | | Minor | 0 | | | | | | | | | | | | | |
| Unknown | 0 | | | Warning | 2 | | | | | | | | | | | | | |
| | | | | Info | 0 | | | | | | | | | | | | | |
| | | | | Unknown | 0 | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| Validated Assets | | | | | | | | | | | | | | | | | | |
| **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** |
| D24-juniper | | Direct-To-Device | Direct-To-Device | 1.2.3.4 | JUNIPER-JUNOS | vqfx-10000 | juniper-junos | A0B2C3456 | | 15-1234-040-4 | Non Compliant | 0 | 0 | 0 | 1 | 0 | 0 |
| cisco-juniper19 | | Direct-To-Device | Direct-To-Device | | | | | | | | Non Compliant | 0 | 0 | 0 | 1 | 0 | 0 |



Sicherung der Gerätekonfiguration

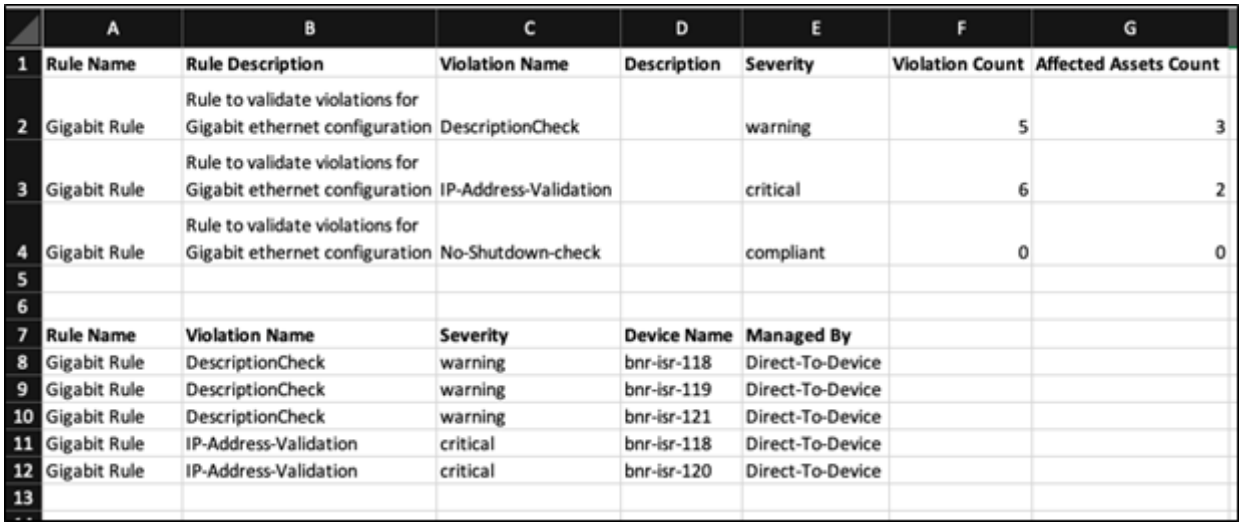
- Datei hochladen: Ein Fenster zum Hochladen von Dateien wird geöffnet, in dem Benutzer die Gerätekonfiguration hochladen können.



| | 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<br>Block Identifier name: ^aaa authentication | Additional Configurations: info<br>Missing Configurations: warning<br>Missing Blocks: critical<br>Skipped Blocks: info | Enforce Config Order: False<br>TTP Template: False | 1 | 0 | 1 | 1 |
| 3 | Interface-gigabitE-Block | | interface GigabitEthernet{{intf_id}}<br>ip address {{ip_addr}} {{subnet_ip}}<br>negotiation {{ negotiation\| re(".*") \| let("negotiation_exists","True") }}<br>description sanity #ignore_line<br>vrf forwarding Mgmt-intf<br>shutdown | Block Identifier: Interface Gigabit<br>Block Identifier name: ^interface GigabitEthernet | Additional Configurations: info<br>Missing Configurations: major<br>Missing Blocks: critical<br>Skipped Blocks: info<br>Order Mismatch: warning | Enforce Config Order: True<br>TTP Template: False | 2 | 0 | 2 | 1 |

Datei hochladen

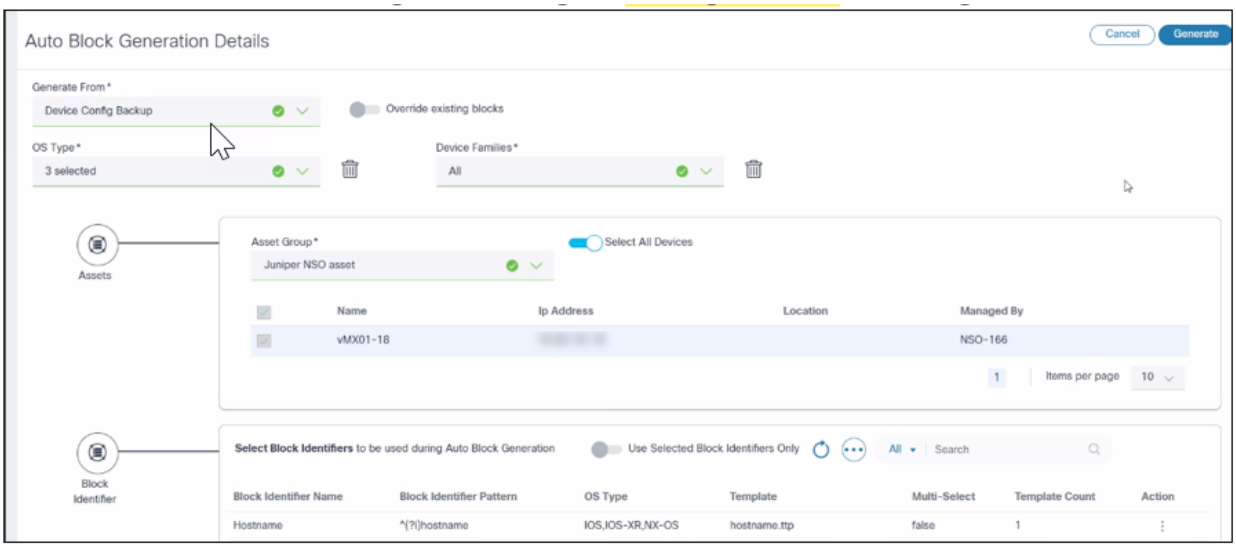
- Aktuelle Konfiguration: Geben Sie den CLI-Konfigurationsbefehl ein, den das System zum Abrufen der Gerätekonfiguration verwendet.



| | 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 | | | | | | | |

Aktuelle Konfiguration

- BS-Typ: Liste der Betriebssystemtypen, für die dieser Block relevant ist.
- Gerätefamilie: Liste der Gerätefamilien, für die dieser Block relevant ist
- Ressourcen: Die Funktion "Ressourcen" bietet einen strukturierten Ansatz zur Auswahl von Geräten zur Erzeugung dynamischer Blöcke.
    - Auswahl der Ressourcengruppe:
        - Ermöglicht es Benutzern, eine vordefinierte Gruppe von Geräten auszuwählen, die als Ressourcengruppe bezeichnet wird und zum Generieren dynamischer Blöcke verwendet wird.
        - Erleichtert die Verwaltung und Organisation von Geräten, indem sie nach bestimmten Kriterien wie Standort, Typ oder Funktion gruppiert werden
    - Auswahl der untergeordneten Geräte:
        - Benutzer können eine bestimmte Untergruppe von Geräten innerhalb der ausgewählten Asset-Gruppe auswählen.
        - Ermöglicht Benutzern, sich auf ein bestimmtes Gerätesegment zu konzentrieren, und ermöglicht so eine gezieltere Blockgenerierung und -verwaltung




Blockgenerierung

- Blockkennung: Bietet Benutzern die Möglichkeit, die Liste der während der Blockgenerierung verwendeten Blockbezeichner auszuwählen. Sie bietet auch inline Funktionen zur Verwaltung von Blockkennungen.

# Blockkennung

Ein Block Identifier verwendet CiscoConfParser, um einen Konfigurationsblock aus der gesamten Gerätekonfiguration zu extrahieren. Jeder Blockbezeichner sollte einem regulären Muster zugeordnet werden. Benutzer können ihre eigenen Blockbezeichner erstellen oder vorhandene Blockbezeichner über die Benutzeroberfläche oder die API aktualisieren. Die Plattform stellt derzeit ca. 55 bis 60 standardmäßige Block-IDs bereit. Jede Kennung ist für einen Betriebssystemtyp eindeutig und wird während der Bereitstellung der BPA-Anwendung über den

Ingester-Dienst geladen. Jedem Blockbezeichner kann eine TTP-Vorlage zugeordnet werden. Sowohl der Name als auch das Muster einer Blockkennung müssen eindeutig sein.

Wenn die Option Multi für die Blockkennung aktiviert ist, generiert das Compliance-Framework aus den zugeordneten Konfigurationen mehrere Konfigurationsblöcke. Andernfalls werden alle übereinstimmenden Konfigurationen als ein Block behandelt.

Beispiele für Blockbezeichner mit der Multi-Option True: Schnittstelle, Router, BGP, VRF, L2VPN usw.

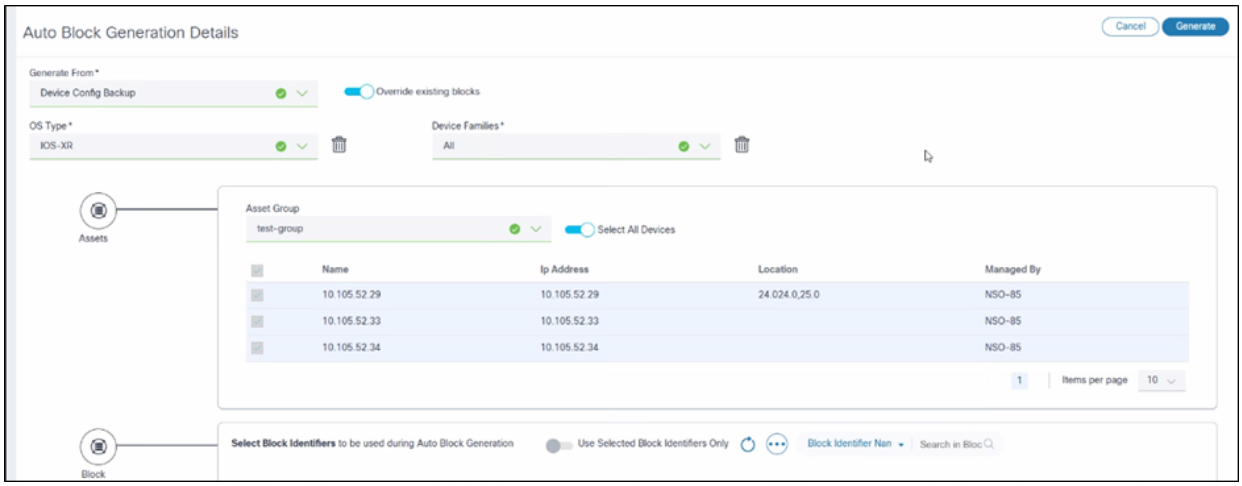
Beispiele für Blockkennungen mit der Multi-Option False: Protokollierung, SNMP-Server, Domäne usw.

Beispiele:

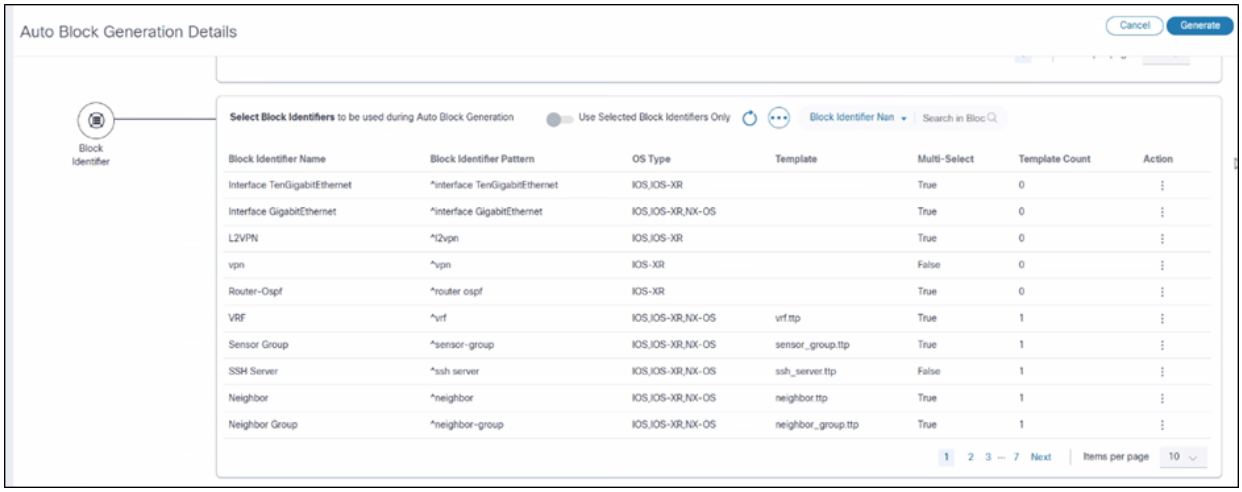
```
{
  “name”: “BundleEthernet Interface”,
  “osType”: [“IOS”, “IOS-XR”, “NX-OS”],
  “multi”: true,
  “blockIdentifier”: “^(?i)interface Bundle-Ether”,
  “templates”: [“parent_interface.ttp”]
}

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

## Blockkennung auflisten

List Block Identifier (Blockkennung auflisten) ermöglicht es Benutzern, die Liste der Blockbezeichner zusammen mit Such- und Sortierfunktionen anzuzeigen. Diese Funktion ist auf der Seite Blöcke generieren verfügbar.

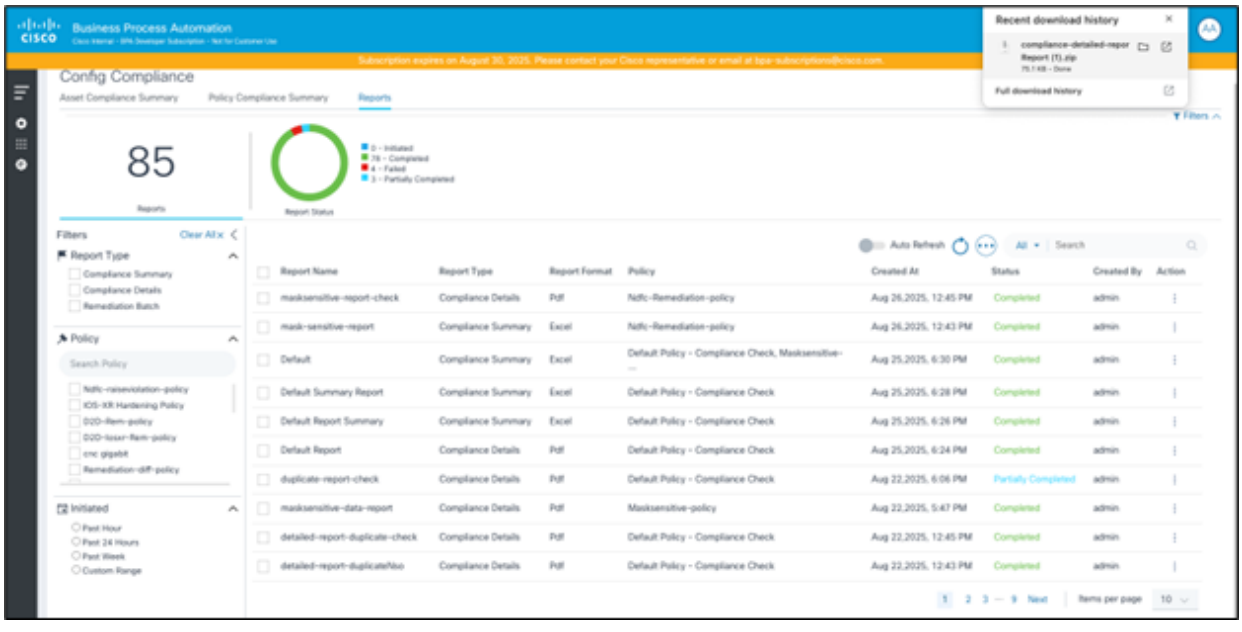



Block-ID-Liste




Blockkennung

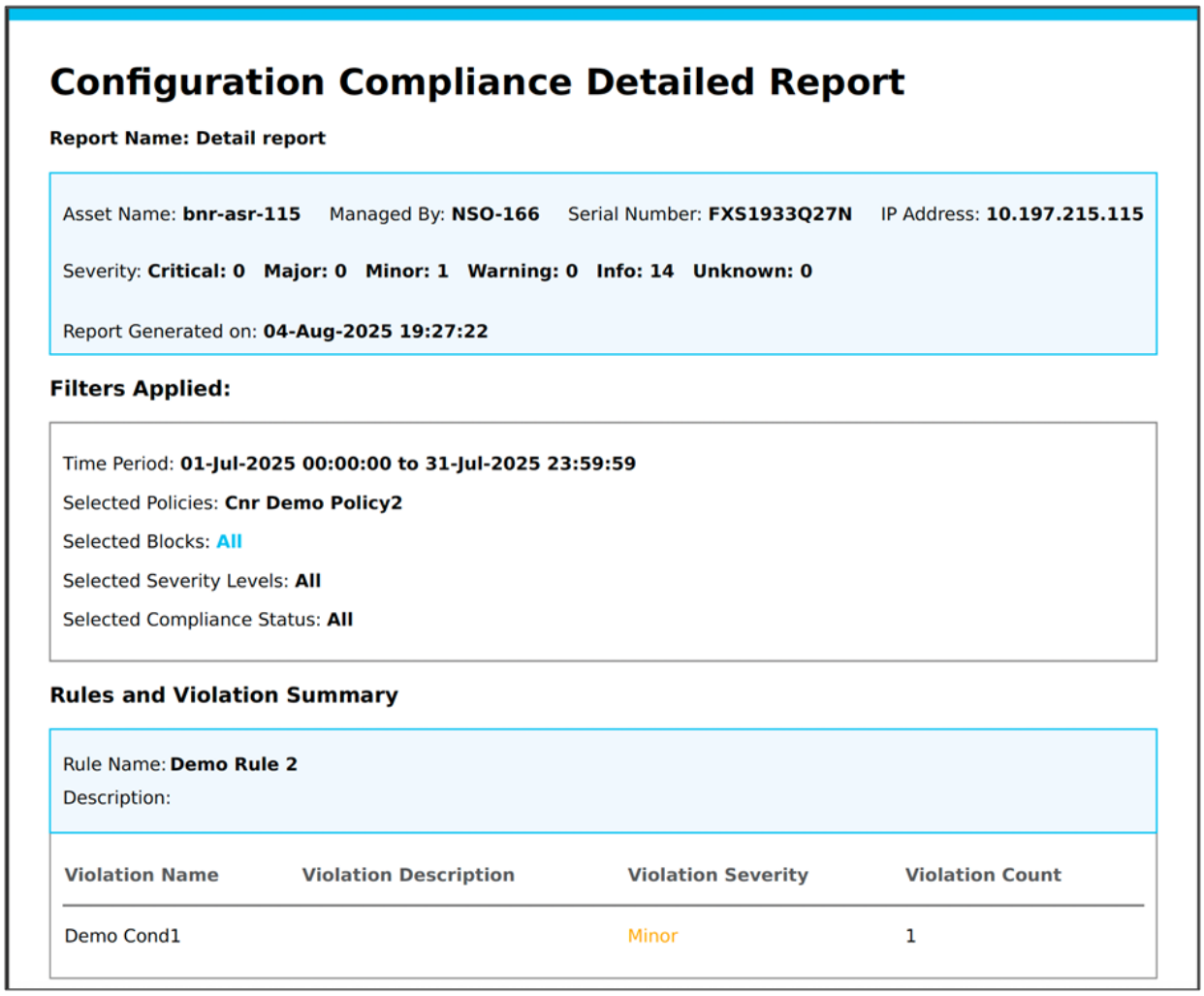
## Block-ID erstellen oder bearbeiten




Block-ID bearbeiten

Der Abschnitt Blockkennungsliste auf der Seite Automatische Blockgenerierung bietet Benutzern die erforderlichen Tools, um Blockkennungen effektiv zu verwalten. Die Funktionen sind im Folgenden aufgeführt:

- Blockbezeichner erstellen
  - Benutzer können neue Blockbezeichner zur Liste hinzufügen
  - Dies ermöglicht die Einführung eindeutiger Bezeichner, die zum Organisieren und Unterscheiden von Blöcken verwendet werden können.
- Blockbezeichner bearbeiten
  - Vorhandene Blockkennungen können geändert werden.
  - Ermöglicht Aktualisierungen oder Korrekturen von Identifikatoren, um sicherzustellen, dass diese korrekt und relevant für die von ihnen repräsentierten Blöcke bleiben
- Blockkennung löschen
  - Benutzer können Blockbezeichner aus der Liste entfernen.
  - Erleichtert die Verwaltung von Identifikatoren, indem das Entfernen von nicht mehr benötigten oder nicht mehr anwendbaren Identifikatoren ermöglicht wird.



**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 |

Blockkennung löschen

# Konfiguration: Richtlinien

Auf der Registerkarte "Policies" (Richtlinien) können Sie einen Satz Richtlinien, Regeln und Blöcke definieren, die die Compliance-Ausführung ermöglichen. Eine Richtlinie ist eine benutzerdefinierte Vorlage, die aus Konfigurationsblöcken und Regeln besteht. Sie können eine Liste mit Konfigurationsblöcken und eine Liste mit Regeln für jeden Konfigurationsblock zum Erstellen einer Richtlinie auswählen.

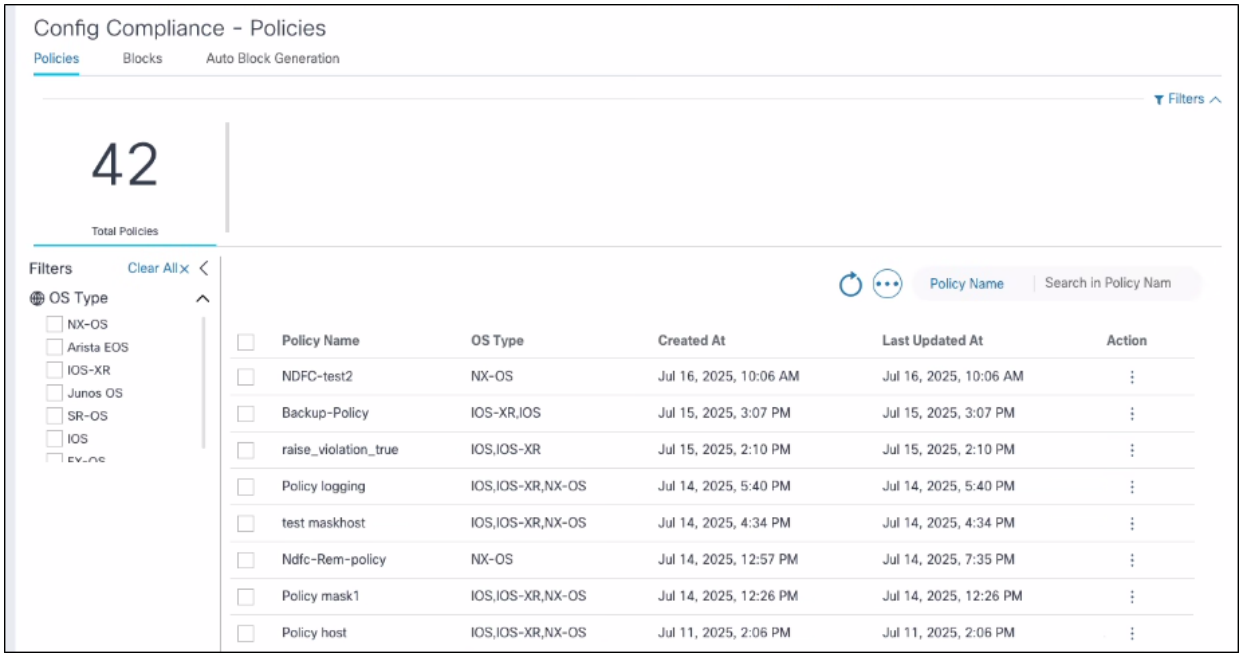
## Richtlinien auflisten

Auf der Registerkarte Policies (Richtlinien) kann eine Liste von Richtlinien angezeigt werden, die auch Aktionen zum Hinzufügen, Bearbeiten, Löschen, Importieren und Exportieren von Richtlinien enthält.

---

Anmerkung: Richtlinien werden zusammen mit zugehörigen Blöcken und Regeln importiert oder exportiert.

---



Richtlinien auflisten

## Hinzufügen und Bearbeiten von Richtlinien

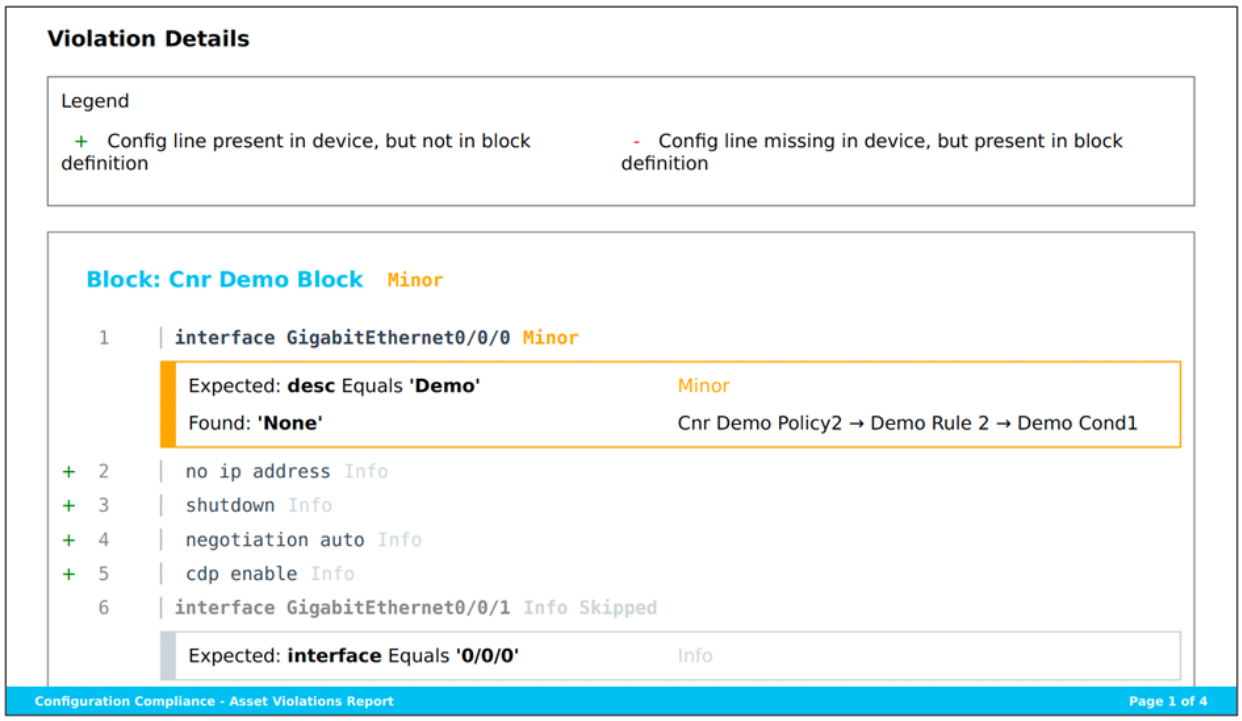
In diesem Abschnitt wird die Seite Richtlinie hinzufügen und Richtlinie bearbeiten beschrieben:

## Richtliniendetails

- Richtlinienname: Name der Richtlinie
- BS-Typ: Liste der unterstützten Betriebssystemtypen für diese Richtlinie

- Gerätefamilie: Liste der unterstützten Gerätefamilien für diese Richtlinie
- Richtlinienbeschreibung (optional): Beschreibt die Richtlinie mit einer kurzen Beschreibung

Die Felder Betriebssystemtyp und Gerätefamilie werden basierend auf den im nächsten Abschnitt ausgewählten Blöcken automatisch ausgefüllt.



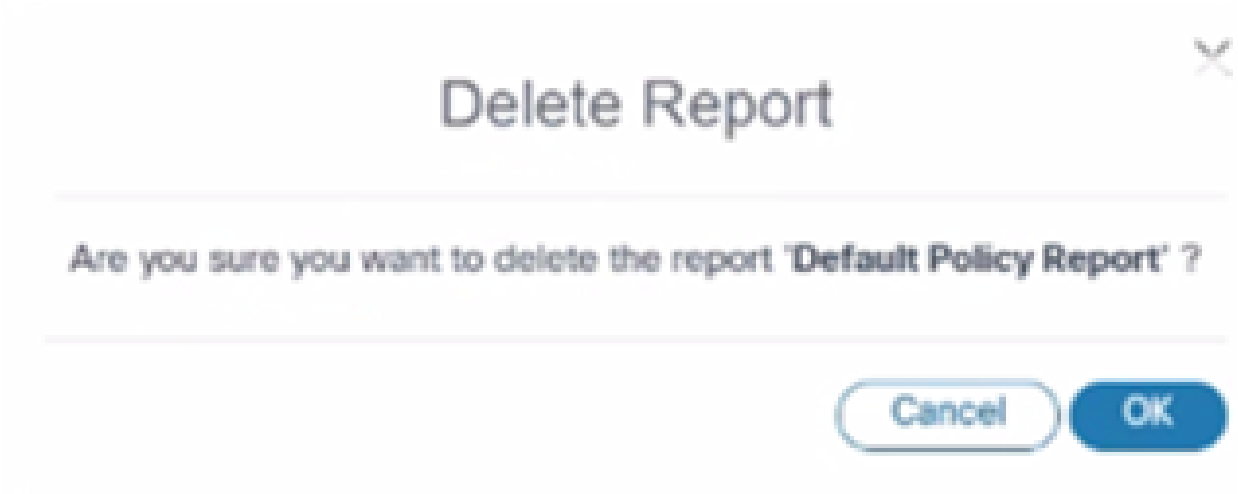
Konfigurationsrichtlinien: Richtliniendetails

## Dialogfeld "Blöcke auswählen"

Die Funktion "Select Blocks" (Blöcke auswählen) ist eine benutzerfreundliche Oberfläche, die Benutzern bei der Auswahl von Konfigurationsblöcken für die Aufnahme in eine Richtlinie helfen soll. Die Funktionen sind in diesem Abschnitt aufgeführt:

- Popup-Dialog
  - Zweck: Bietet Benutzern einen dedizierten Platz zum Auswählen von Konfigurationsblöcken, ohne die aktuelle Seite zu verlassen
  - Benutzerinteraktion: Intuitiver Auswahlprozess durch Anzeige der Optionen in einem separaten, spezifischen Dialogfeld
- Optionen hinzufügen und auswählen
  - Mehrere Optionen: Benutzer können einen oder mehrere Konfigurationsblöcke für die Richtlinie auswählen.
  - Flexibilität: Unterstützt die Einbeziehung verschiedener Bausteine auf Basis der spezifischen Richtlinienanforderungen des Benutzers
- Navigationsfunktionen
  - Filter: Ermöglicht es Benutzern, die Liste der verfügbaren Blöcke anhand bestimmter

Kriterien einzugrenzen, sodass relevante Blöcke leichter gefunden werden können.
    - Paginierung: Strukturierung von Blöcken in überschaubaren Seiten zur Verbesserung der Navigation durch große Datenmengen
    - Suchfunktionen: Ermöglicht die schnelle Lokalisierung von Blöcken nach Namen oder anderen Bezeichnern und optimiert so den Auswahlprozess




Blockauswahl

Benutzer können neue Blöcke erstellen, indem sie im Abschnitt "Blockauswahl" auf Erstellen klicken. Ein neues Browser-Register wird gestartet, und Benutzer können einen neuen Block erstellen. Nach dem Absenden können die Benutzer zur ursprünglichen Registerkarte zurückkehren und den neu erstellten Block auswählen, um ihn der Richtlinie hinzuzufügen.

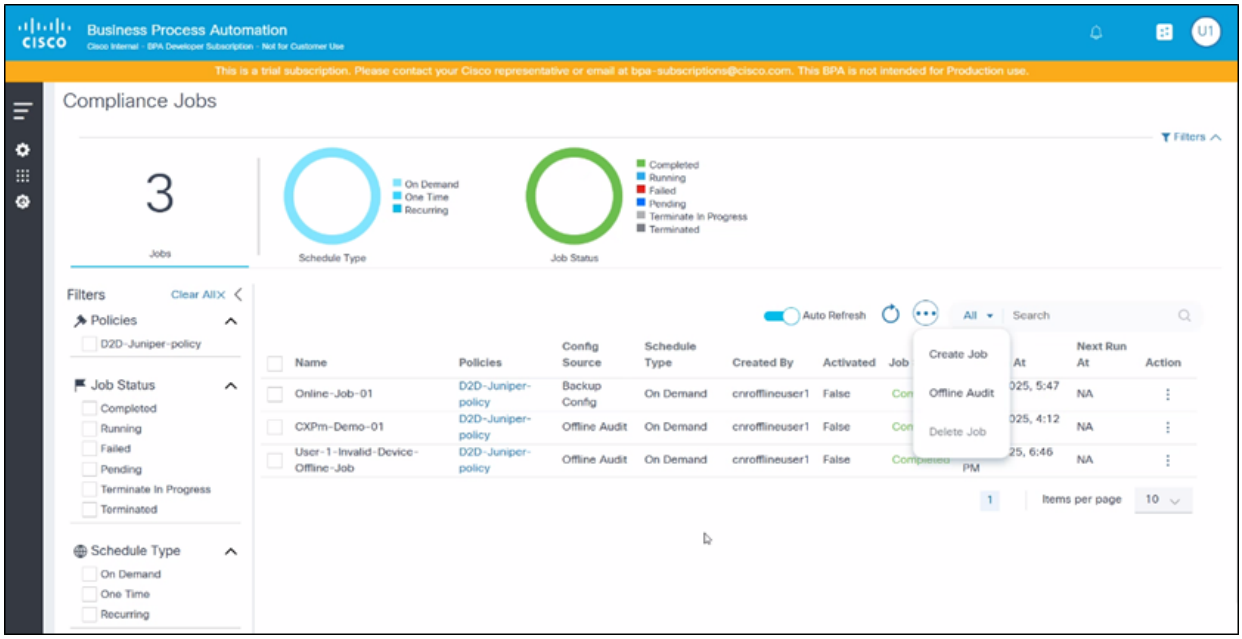
## Bedingte Filter

Die Funktion für bedingte Filter ist ein erweitertes Tool, mit dem Benutzer bestimmte Kriterien auf Konfigurationsblöcke anwenden können, um präzise und gezielte Compliance-Prüfungen sicherzustellen.

- Ermöglicht Benutzern, Konfigurationen anzuwenden oder Compliance-Prüfungen für ausgewählte Konfigurationsblöcke auf der Grundlage vordefinierter Bedingungen durchzuführen
- Konzentration von Ressourcen und Bemühungen auf relevante Blöcke durch Herausfiltern von Blöcken, die die angegebenen Kriterien nicht erfüllen
- Benutzer können Bedingungen definieren, die Konfigurationsblöcke erfüllen müssen, um Compliance-Prüfungen oder anderen Prozessen unterzogen zu werden
- Nur die Blöcke, die diesen Bedingungen entsprechen, werden ausgeführt, während andere ignoriert werden, um eine präzisere Kontrolle zu ermöglichen.

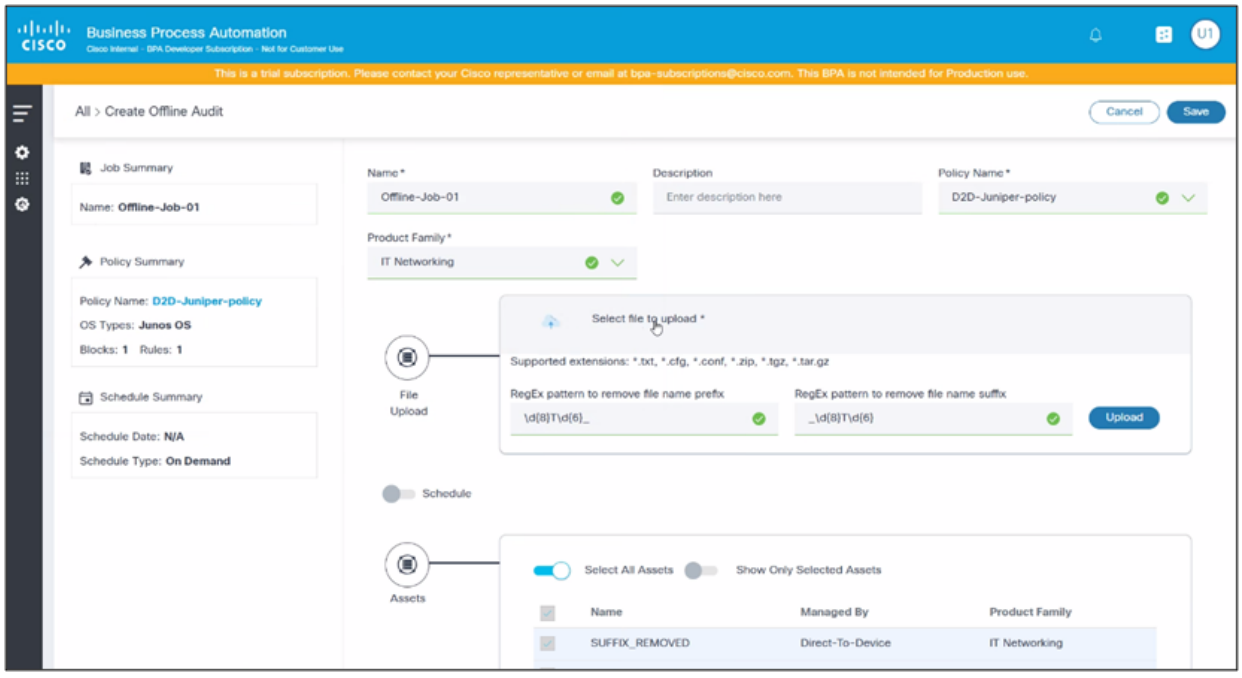
Anwendungsbeispiel:

- Selektive Compliance-Prüfungen: Wenn eine Richtlinie dazu gedacht ist, Konfigurationen nur auf zwei der 20 verfügbaren Schnittstellen zu überprüfen, können Benutzer Bedingungen festlegen, um die Konformitätsprüfungen auf diese beiden Schnittstellen zu beschränken.



Bedingte Filter

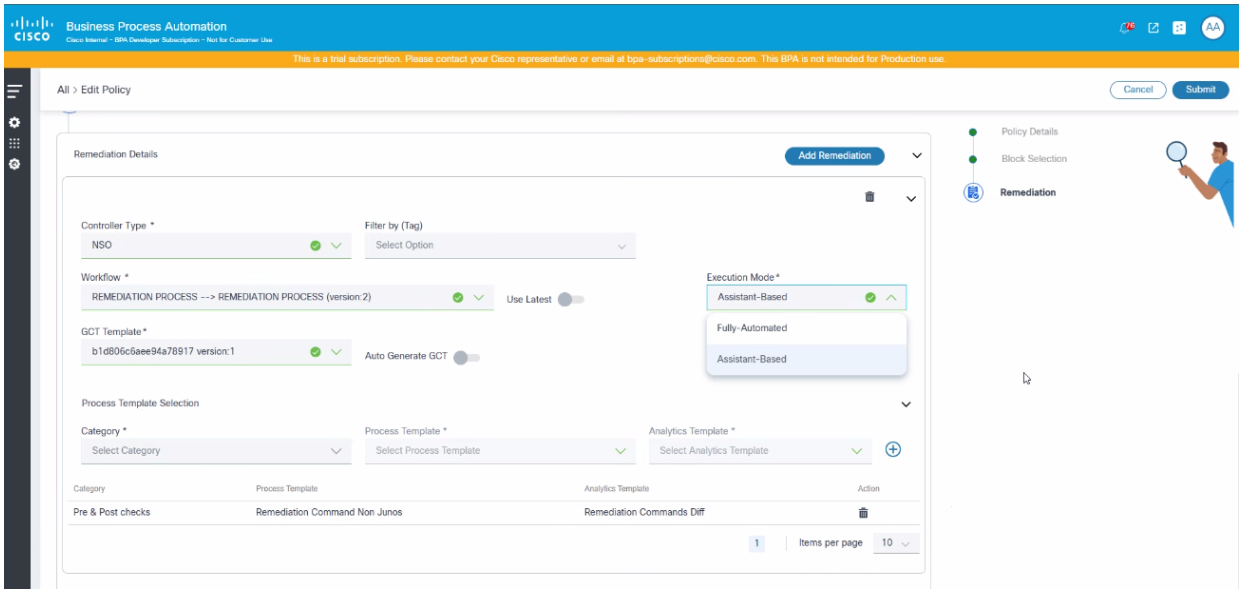
- Regeln auswählen: Möglichkeit zum Auswählen einer oder mehrerer Regeln für einen bestimmten Konfigurationsblock.



Regeln auswählen

## Sanierungsabteilung

Die Seite Policies (Richtlinien) enthält einen optionalen Abschnitt zur Definition von Problembehebungsdetails für jeden Controller-Typ.



Konfigurationsrichtlinien: Sanierungsdetails

- Controller-Typ: Liste der Controller-Typen mit Unterstützung für Fehlerbehebung
- Behebungs-Workflow: Workflow, der für Geräte des ausgewählten Controllertyps ausgeführt werden soll
- GCT-Vorlage: Eine oder mehrere anzuwendende GCT-Vorlagen
- Prozessvorlage: Eine oder mehrere Prozessvorlagen, die im Rahmen der Vor- und Nachprüfung ausgeführt werden, zusammen mit der entsprechenden Analysevorlage.
- Vorlage für Vorabprüfung: Optionale Liste der Prozessvorlagen, die nur zur Vorabprüfung ausgeführt werden
- Vorlage für Nachprüfung: Optionale Liste der Prozessvorlagen, die nur für die Nachprüfung ausgeführt werden
- Ausführungsmodus:
    - Vollständig automatisch: Der Wiederherstellungsprozess wird automatisch ohne manuelle Eingriffe oder Benutzeraufgaben ausgeführt.
    - Assistentenbasiert: Das System erstellt Benutzeraufgaben, für die während des Wiederherstellungsprozesses manuelle Unterstützung erforderlich ist.

## Funktion zur automatischen Generierung von GCT

Die Funktion zum automatischen Generieren von GCT wurde entwickelt, um den Prozess zum Erstellen von GCT-Vorlagen zu optimieren, die für die Sanierung erforderlich sind. Es funktioniert wie folgt:

- Automatische Generierung von GCT-Vorlagen auf Basis der Ergebnisse und Details der Compliance-Ausführung

- Automatisiert die Vorlagenerstellung
- Die generierten Vorlagen sind auf die bei Compliance-Prüfungen identifizierten Probleme zugeschnitten und stellen sicher, dass Abhilfemaßnahmen den Compliance-Anforderungen entsprechen.

# Rollen und Zugriffskontrolle

## Statische Berechtigungsliste

Das Dashboard für die Konfigurationskonformität im Portal der nächsten Generation unterstützt die RBAC-Funktion von BPA mit den folgenden Berechtigungen, die darstellen, wie ein dynamischer Textblock der Konfiguration in einer GUI-Darstellung zur Behandlung der Regeln und Bedingungen angezeigt wird:

| Gruppe | Aktion | Beschreibung |
|---|---|---|
| ui-app | ComplianceDashboard.show | Compliance Dashboard-App anzeigen/ausblenden |
| ui-app | ProblembehebungDashboard.show | Anwendung für Bereinigungsaufträge anzeigen |
| ui-app | complianceJobs.show | Compliance Jobs App anzeigen |
| ui-app | complianceConfigurations.show | Compliance-Konfigurations-App anzeigen |
| ComplianceDashboard | RessourcenComplianceZusammenfassung | Übersicht zur Ressourcenkonformitä anzeigen |
| ComplianceDashboard | RichtlinieComplianceZusammenfassung | Richtlinienkonformität anzeigen |
| ComplianceDashboard | AnsichtVerletzungen | Verletzungsdetails anzeigen |
| ComplianceDashboard | RichtlinieComplianceRessourcenZusammenfassung | Betroffene Ressource anzeigen |
| ComplianceDashboard | AnzeigenBerichte | Anzeigen von Reporting Dashboard, Berichtseinstellungen und Herunterladen vo Berichten |

| Gruppe | Aktion | Beschreibung |
| --- | --- | --- |
| ComplianceDashboard | Berichte verwalten | Erstellen und Löschen von Berichten |
| ComplianceDashboard | VerwaltenBerichtseinstellungen | Berichteinstellungen ändern |
| ProblembehebungDashboard | AnsichtBereinigungsaufträge | Korrekturaufträge anzeigen |
| ProblembehebungDashboard | AnsichtProblembehebungMeilensteine | Wiederherstellungs-Meilensteine anzeigen |
| ProblembehebungDashboard | Behebungsaufträge verwalten | Behebungsaufträge wie Erstellen, Löschen, Archivieren und Verwalten von Benutzeraufgaben verwalten |
| ComplianceJobs | AnsichtComplianceJobs | Compliance-Aufträge und -Ausführungen anzeigen |
| ComplianceJobs | VerwaltenComplianceJobs | Compliance-Aufträge verwalten |
| KonformitätKonfigurationen | AnsichtCompliance-Konfigurationen | Anzeigen von Compliance-Konfigurationen wie Richtlinien, Blöcken, Regeln, Blockgenerierung, Blockkennungen und TTP-Vorlagen |
| KonformitätKonfigurationen | VerwaltenCompliancePolicies | Compliance-Richtlinie verwalten |
| KonformitätKonfigurationen | VerwaltenCompliance-Blöcke | Verwaltung von Compliance-Blöcken und -Regeln und Block-IDs |
| KonformitätKonfigurationen | VerwaltenComplianceBlockgenerierung | Verwaltung von Compliance-Blockgenerierung und TTP-Vorlagen |

## Vordefinierte Rollen

Der Anwendungsfall "Configuration Compliance and Remediation" umfasst die in der nachfolgenden Tabelle aufgeführten vordefinierten Rollen:

Anmerkung: Administratoren können Rollen entsprechend den Kundenanforderungen erstellen oder aktualisieren.

| Rolle | Beschreibung | Berechtigungen |
|---|---|---|
| Compliance-Administrator | Administratorrolle mit allen Berechtigungen in Bezug auf die Compliance | UI-Anwendungen:<br><br>Asset Manager anzeigen<br>- Asset-Gruppe anzeigen<br>- Compliance Dashboard anzeigen<br>- Compliance-Jobs anzeigen<br>- Compliance-Konfiguration anzeigen<br><br>Ressource:<br><br>Anlagenliste anzeigen<br>- Anzeigen der Sicherungskonfiguration für Ressourcen<br>- Sicherungskonfiguration<br>- Ausführen von vom Controller aktivierten Geräteaktionen<br><br>Asset-Gruppe:<br><br>- Asset-Gruppen anzeigen<br>- Ressourcengruppen verwalten<br>- Dynamische Asset-Gruppen erstellen<br><br>Sicherungskonfiguration: Anzeigen, Vergleichen und Herunterladen von Gerätekonfigurations-Backups<br><br>Richtlinie zur Datensicherung und Wiederherstellung: Backup-Wiederherstellungsrichtlinien anzeigen |

| Rolle | Beschreibung | Berechtigungen |
| --- | --- | --- |
| Compliance-Betreiber | Operatorrolle mit allen Compliance-Berechtigungen, außer Konfigurationsverwaltung | Compliance-Dashboard:<br><br>- Anzeigen der Compliance-Übersichten der Ressourcen<br>- Richtlinien-Compliance-Zusammenfassungen anzeigen<br>- Verstöße anzeigen<br>- Betroffene Ressourcen anzeigen<br>Erstellen und Löschen von Berichten<br>Anzeigen von Reporting Dashboard, Berichtseinstellungen und Berichten zum Herunterladen<br>Berichteinstellungen ändern:<br><br>Compliance-Jobs<br><br>Compliance-Aufträge und -Ausführungen anzeigen<br>- Compliance-Jobs verwalten<br><br>Compliance-Konfigurationen:<br><br>- Anzeige von Compliance-Konfigurationen wie Richtlinien, Blöcken und Regeln<br>- Verwaltung von Compliance-Richtlinien<br>- Compliance-Blöcke, Regeln und Blockkennungen verwalten<br>- Verwaltung von Compliance-Blockgenerierung und TTP-Vorlagen<br>UI-Anwendungen:<br><br>- Ressourcenmanager anzeigen<br>- Asset-Gruppe anzeigen<br>- Compliance Dashboard anzeigen<br>- Compliance-Jobs anzeigen<br>- Compliance-Konfiguration anzeigen<br><br>Ressource:<br><br>Anlagenliste anzeigen<br>- Anzeigen der |

| Rolle | Beschreibung | Berechtigungen |
| --- | --- | --- |
| | | Sicherungskonfiguration für Ressourcen<br>- Sicherungskonfiguration<br>- Ausführen von vom Controller aktivierten Geräteaktionen<br><br>Asset-Gruppe:<br><br>- Asset-Gruppen anzeigen<br>- Ressourcengruppen verwalten<br>- Dynamische Asset-Gruppen erstellen<br><br>Sicherungskonfiguration: Anzeigen, Vergleichen und Herunterladen von Gerätekonfigurations-Backups<br><br>Richtlinie zur Datensicherung und Wiederherstellung: Backup-Wiederherstellungsrichtlinien anzeigen<br><br>Compliance-Dashboard:<br><br>- Übersicht über die Ressourcenkonformität anzeigen<br>- Richtlinienkonformitätsübersicht anzeigen<br>- Verstöße anzeigen<br>- Betroffene Ressourcen anzeigen<br>Erstellen und Löschen von Berichten<br>Anzeigen von Reporting Dashboard, Berichtseinstellungen und Berichten zum Herunterladen<br>Compliance-Jobs:<br><br>Compliance-Aufträge und -Ausführungen anzeigen<br>- Compliance-Jobs verwalten<br><br>Compliance-Konfigurationen:<br><br>Compliance-Konfigurationen wie |

| Rolle | Beschreibung | Berechtigungen |
| --- | --- | --- |
| Compliance schreibgeschützt | Bietet alle schreibgeschützten Berechtigungen für Compliance-Anwendungsfälle | Richtlinien, Blöcke und Regeln anzeigen<br>UI-Anwendungen:<br><br>- Ressourcenmanager anzeigen<br>- Asset-Gruppe anzeigen<br>- Compliance Dashboard anzeigen<br>- Compliance-Jobs anzeigen<br>- Compliance-Konfiguration anzeigen<br><br>Ressource:<br><br>Anlagenliste anzeigen<br>- Anzeigen der Sicherungskonfiguration für Ressourcen<br>- Ausführen von vom Controller aktivierten Geräteaktionen<br><br>Asset-Gruppe:<br><br>- Asset-Gruppen anzeigen<br><br>Sicherungskonfiguration: Anzeigen, Vergleichen und Herunterladen von Gerätekonfigurations-Backups<br><br>Richtlinie zur Datensicherung und Wiederherstellung: Backup-Wiederherstellungsrichtlinien anzeigen<br><br>Compliance-Dashboard:<br><br>Übersicht zur Ressourcenkonformität anzeigen<br>- Richtlinienkonformitätsübersicht anzeigen<br>- Verstöße anzeigen<br>- Betroffene Ressourcen anzeigen<br>Anzeigen von Reporting Dashboard, Berichtseinstellungen und Herunterladen von Berichten |

| Rolle | Beschreibung | Berechtigungen |
| --- | --- | --- |
| Behebungsadministrator/-administrator | Operatorrolle mit allen Berechtigungen für die Problembehebung | Compliance-Jobs:<br><br>Compliance-Aufträge und -Ausführungen anzeigen<br><br>Compliance-Konfigurationen:<br><br>Compliance-Konfigurationen wie Richtlinien, Blöcke und Regeln anzeigen<br>UI-Anwendungen:<br><br>- Ressourcenmanager anzeigen<br>- Asset-Gruppe anzeigen<br>- Behebungs-Dashboard anzeigen<br><br>Ressource:<br><br>- Ressourcenliste anzeigen<br><br>Asset-Gruppe:<br><br>- Asset-Gruppen anzeigen<br>Ressourcengruppen verwalten<br>- Dynamische Asset-Gruppen erstellen<br><br>Behebungs-Dashboard:<br><br>- Korrekturaufträge anzeigen<br>- Problembehebungs-Meilensteine anzeigen<br>- Übersicht über die Ressourcenkonformität anzeigen<br>- Verwalten von Wiederherstellungsaufgaben wie Erstellen, Löschen, Archivieren und Verarbeiten von Benutzeraufgaben<br>- Betroffene Ressourcen anzeigen |
| Problembehebung schreibgeschützt | Bietet alle schreibgeschützten Berechtigungen für den | UI-Anwendungen:<br><br>- Ressourcenmanager anzeigen |

| Rolle | Beschreibung | Berechtigungen |
| --- | --- | --- |
| | Problembehebungsfall | - Asset-Gruppe anzeigen<br>- Behebungs-Dashboard anzeigen<br><br>Ressource:<br><br>- Ressourcenliste anzeigen<br><br>Asset-Gruppe:<br><br>- Asset-Gruppen anzeigen<br>Dynamische Asset-Gruppen erstellen<br><br>Behebungs-Dashboard:<br><br>- Korrekturaufträge anzeigen<br>- Problembehebungs-Meilensteine anzeigen<br>- Übersicht über die Ressourcenkonformität anzeigen<br>- Betroffene Ressourcen anzeigen |

## Zugriffsrichtlinien

Die Funktion "Access Policies" (Zugriffsrichtlinien) stellt sicher, dass Benutzer angemessenen Zugriff auf bestimmte Compliance-Richtlinien und Asset-Gruppen haben. Diese Funktion erhöht die Sicherheit und die Betriebseffizienz, da Administratoren Zugriffskontrollen basierend auf Benutzerrollen und -verantwortlichkeiten definieren und durchsetzen können. Die Zugriffsrichtlinien werden über die Seite "Access Policy" (Zugriffsrichtlinie) verwaltet, auf der Administratoren Richtlinien erstellen, bearbeiten und Benutzern oder Gruppen zuweisen können. Administratoren können präzise Berechtigungen definieren und festlegen, welche Compliance-Richtlinien und Asset-Gruppen von den einzelnen Benutzern oder Gruppen angezeigt, bearbeitet oder verwaltet werden können. Diese Detailgenauigkeit trägt dazu bei, eine strenge Kontrolle über vertrauliche Informationen und kritische Vorgänge zu erhalten.

Sobald die Zugriffsrichtlinie definiert ist, werden die Daten auf allen Seiten zur Einhaltung von Richtlinien und zur Problembehebung in der Benutzeroberfläche der nächsten Generation eingeschränkt, basierend auf der Liste der CnR-Richtlinien und -Ressourcen, auf die der aktuelle Benutzer Zugriff hat.

So gewähren Sie Benutzerzugriff:

---

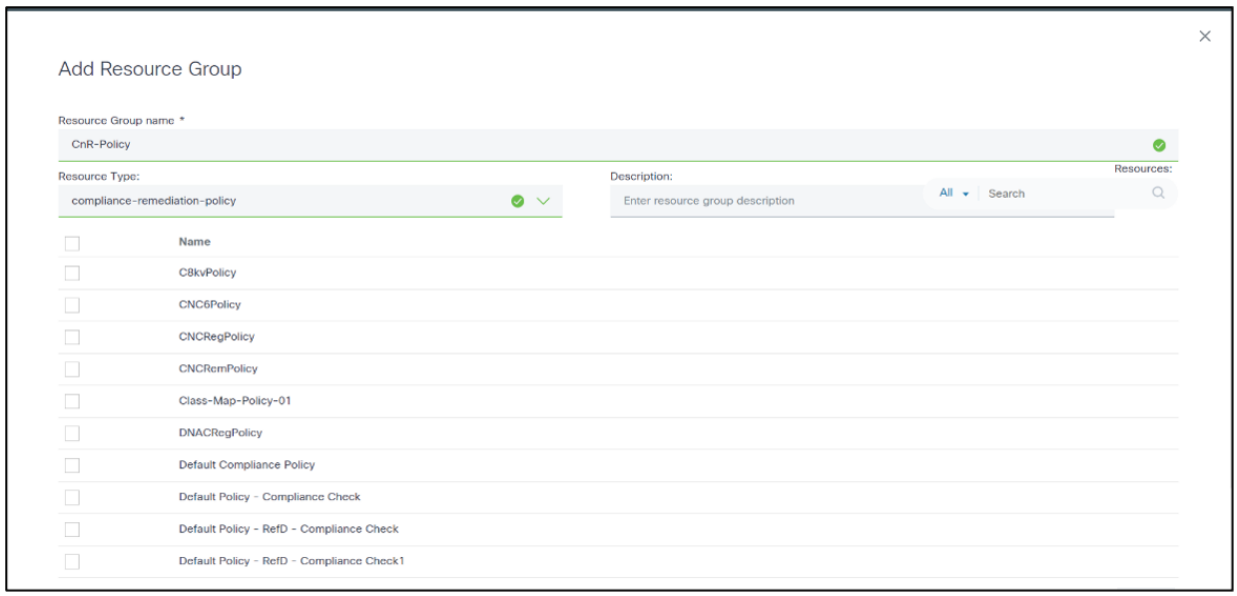
Anmerkung: Berechtigungen können nur von Administratoren bereitgestellt werden.

---

1. Erstellen Sie Benutzer, und weisen Sie sie Benutzergruppen zu.
2. Erstellen Sie eine oder mehrere Benutzerrollen, und weisen Sie sie der bzw. den erstellten Benutzergruppe(n) zu.
3. Anlagen einer Anlagengruppe(n) hinzufügen.
4. Erstellen Sie Ressourcengruppen, um Compliance-Richtlinienressourcen zuzuweisen.
5. Erstellen Sie eine Zugriffsrichtlinie, und wählen Sie die entsprechende(n) Benutzergruppe(n), Anlagengruppe(n) und Ressourcengruppe(n) aus.

Ressourcengruppe wird erstellt

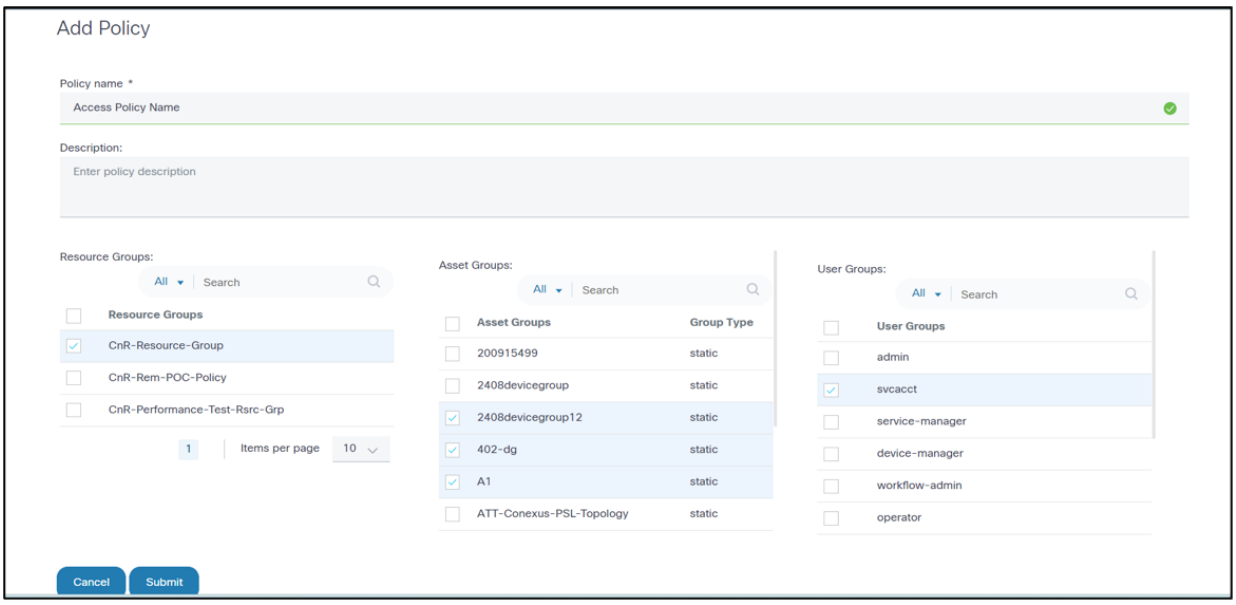
Erstellen Sie eine Ressourcengruppe mithilfe der Compliance-Wiederherstellungsrichtlinie aus der Dropdown-Liste Ressourcentyp, und wählen Sie Compliance-Richtlinien aus, die Zugriff auf die entsprechende Benutzergruppe erhalten sollen.




Ressourcengruppe erstellen

Zugriffsrichtlinie erstellen

Erstellen Sie eine Zugriffsrichtlinie mit Ressourcengruppe(n) und Ressourcengruppe(n), die den Benutzergruppen Berechtigungen erteilen müssen.




Zugriffsrichtlinie erstellen

# Offline-Compliance

Mit der Offline-Compliance-Funktion können Benutzer Konformitätsprüfungen für Gerätekonfigurationen durchführen, die nicht über aktive Geräte im Bestand verfügbar sind.

Benutzer können die Offline-Konformität mithilfe der Gerätesicherungskonfiguration oder durch Erstellen eines Offline-Audits in Compliance Jobs ausführen. Die Ergebnisse der Ausführungen können im Compliance-Dashboard angezeigt werden.

## Verwenden der Geräte-Sicherungskonfiguration

Administratoren können manuell eine ZIP-Datei hochladen, die die aktuelle Konfiguration für die gewünschten Geräte enthält. Diese Funktion steht im Abschnitt Device Config - Upload (Gerätekonfiguration - Hochladen) der Anwendung Backup & Restore (Sicherung und Wiederherstellung) zur Verfügung. Nachdem die Gerätekonfigurationen hochgeladen wurden, kann ein Compliance-Auftrag für die gewünschten Geräte erstellt werden, indem Sie Device Backup Config (Gerätesicherungskonfiguration) als Quelle für die Gerätekonfiguration auswählen. Während der Ausführung wird die hochgeladene Gerätekonfiguration aus der Backup-Anwendung abgerufen, und die Compliance-Prüfung wird auf dieser ausgeführt.

Verwenden der Funktion "Offline-Audit erstellen" in Compliance-Aufträgen

Um die Konformität für eine Gerätekonfiguration offline auszuführen, können Benutzer auf der Seite Compliance-Aufträge über das Symbol Weitere Optionen die Option Offline-Audit auswählen. Dadurch können Benutzer eine ZIP-Datei mit der aktuellen Konfiguration manuell

direkt in die Compliance-Anwendung hochladen. Während der Ausführung wird die hochgeladene Gerätekonfiguration analysiert und die Konformitätsprüfung durchgeführt.

# Bereitstellung von Konfigurationen über Ingester

Das Laden von Compliance-Konfigurationsartefakten kann mithilfe des Ingester-Frameworks automatisiert werden. Sobald Artefakte entwickelt wurden, können sie mithilfe der folgenden Schritte exportiert, in Pakete umgewandelt und in der Zielumgebung bereitgestellt werden.

- Erstellen Sie das NPM-Paket mit den folgenden Befehlen:

```
mkdir <


      >
cd  <


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

- Konfigurationen aus dem BPA-Portal exportieren (klassische Benutzeroberfläche)
    - Navigieren Sie zu BPA Classic UI > Configuration Compliance & Remediation > Configurations
    - "TTP-Vorlagen/Block Identifiers/Blocks/Rules/Policies" exportieren
- Benennen Sie die exportierten Dateien wie folgt um:
    - TTP-Vorlagen: <Dateiname>.cnrttptemplate.json
    - Blockbezeichner: <<Dateiname>>.cnrblockbezeichner.json
    - Blöcke: <Dateiname>.cnrblock.json
    - Regeln: <Dateiname>.cnrrule.json
    - Richtlinien: <Dateiname>.cnrpolicy.json
- Package ingester data (.tgz)
    - Kopieren Sie alle exportierten Dateien in das in "step-1" erstellte npm-Paket.
    - Führen Sie den Befehl `npm pack` im npm-Paket aus, um die Datei ".tgz" zu erstellen.
- Bereitstellung von Ingester-Daten (.tgz) in BPA Single Node env
    - Kopieren Sie die TGZ-Datei in den Ordner <<BPA-Kernpaket>>/Pakete/Daten auf dem Server, auf dem das BPA-Paket bereitgestellt wurde

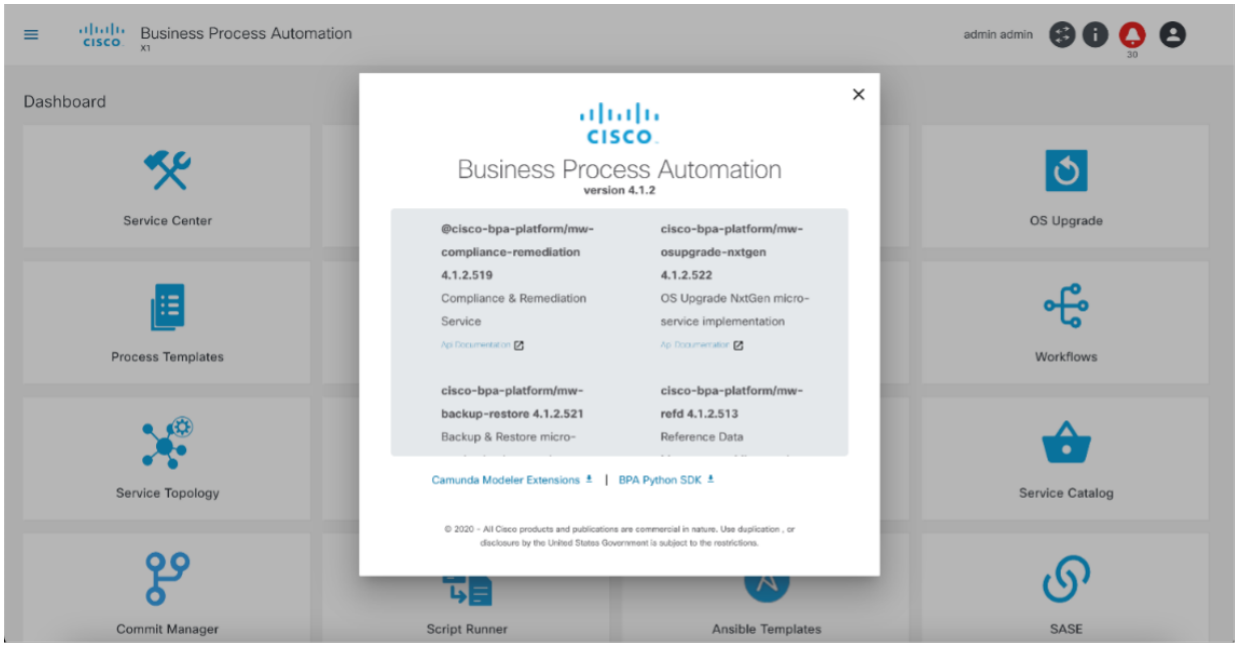
    - Starten Sie den Ingester-Server neu (docker restart ingester-service).
- Bereitstellung von Ingester-Daten (.tgz) in BPA Multi Node env
    - Kopieren Sie die TGZ-Datei in den Ordner /opt/bpa/packages/data auf dem Server, auf dem die Steuerelementdiagramme bereitgestellt werden.
    - Redeploy Ingester Pod (`kubectl rollout restart deployment ingester-service -n bpa-ns`)

## Referenzen

| Name | Beschreibung |
|---|---|
| TTP | Textparser für Vorlagen in Konfigurationsblöcken |
| Konf.-Parser | Konfigurationsfeld-Parser zum Analysieren der CLI-Gerätekonfiguration |

## API-Dokumentation

Die API-Dokumentationsdetails für Compliance und Problembehebung finden Sie im klassischen UI-Popup-Fenster Info:




BPA - Info (klassische Benutzeroberfläche)

## Fehlerbehebung

### Dashboard

Ergebnisse des letzten Compliance-Auftrags werden nicht angezeigt

Beobachtung: Die Ergebnisse der kürzlich durchgeführten Compliance-Jobs werden nicht im Portal-Dashboard der nächsten Generation angezeigt.

Mögliche Ursache 1: Das Dashboard verfügt über einen Datumsbereich, der standardmäßig auf "Aktueller Monat" festgelegt ist. Wenn ein neuer Monat vor kurzem begonnen hat (z.B. heute ist der erste des Monats), werden die Hinrichtungen vor gestern (letzter Tag des Vormonats) nicht angezeigt.

Analyse: Vergewissern Sie sich, dass im Dashboard der richtige Datumsbereich ausgewählt ist, einschließlich der Tage des Vormonats, falls erforderlich, um die korrekten Verletzungsdaten anzuzeigen.

Mögliche Ursache 2: Ein anderer Benutzer hat möglicherweise einen Compliance-Auftrag für dieselbe Richtlinie und/oder Ressourcenkombination ausgeführt. Das Dashboard zeigt Verstöße an, die während der letzten Ausführung innerhalb des ausgewählten Datumsbereichs festgestellt wurden.

Analyse: Als Administrator (oder Benutzer mit Zugriff auf alle Compliance-Aufträge) überprüfen Sie die Liste der Compliance-Aufträge und deren Verlauf, um zu bestimmen, welche Richtlinien- oder Asset-Gruppen-Kombinationen ausgeführt werden.

## Compliance-Jobs

Gesamter Ausführungsstatus als "Übersprungen" festgelegt

Beobachtung: Bei der Ausführung von Compliance-Jobs wird der gesamte Ausführungsstatus als "Übersprungen" markiert. Es werden keine Verstöße gemeldet.

Mögliche Ursache: Eine bestehende Ausführung für denselben Auftrag wird noch ausgeführt.

Analyse: Ein Compliance-Job kann zu einem bestimmten Zeitpunkt nur eine Ausführung im Ausführungszustand aufweisen. Überprüfen, ob eine frühere Ausführung noch ausgeführt wird. Hinrichtungen, die für einen längeren Zeitraum festgehalten oder ausgeführt werden, können beendet/ausgeführt werden.

Gerätestatus als "Übersprungen" festgelegt

Beobachtung: Bei der Ausführung eines Compliance-Auftrags wird der Status einiger Geräte als

"Übersprungen" markiert.

Mögliche Ursache: Die Compliance-Funktion ist für den Controller-Typ, zu dem das Gerät gehört, nicht aktiviert.

Analyse: Die Compliance-Richtlinie gilt nur für Geräte innerhalb der Asset-Gruppe, für die die Funktion aktiviert ist.

Gerätestatus auf "Fehlgeschlagen" gesetzt

Beobachtung: Bei der Ausführung eines Compliance-Auftrags wird der Status für einige Geräte als "Ausgefallen" markiert.

Mögliche Ursache: Laufzeitfehler, die während des Compliance-Ausführungsprozesses aufgetreten sind. Bei diesen Fehlern kann es sich um Codefehler oder falsche Konfigurationen in Richtlinien, Blöcken, Regeln, Blockbezeichnern usw. handeln.

Analyse:

API zur Ermittlung der Ursache von Laufzeitfehlern:

1. Ausführungs-ID abrufen

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

   Compliance-Hinrichtungen

   Methode: HOLEN

2. Geräteausführungen mit Ausführungs-ID abrufen

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

   Compliance-Geräte ausgeführt werden?

   executeId=< Ausführungs-ID >>

   Methode: HOLEN

## Compliance-Regeln

Regeln zeigen leeren Wert an

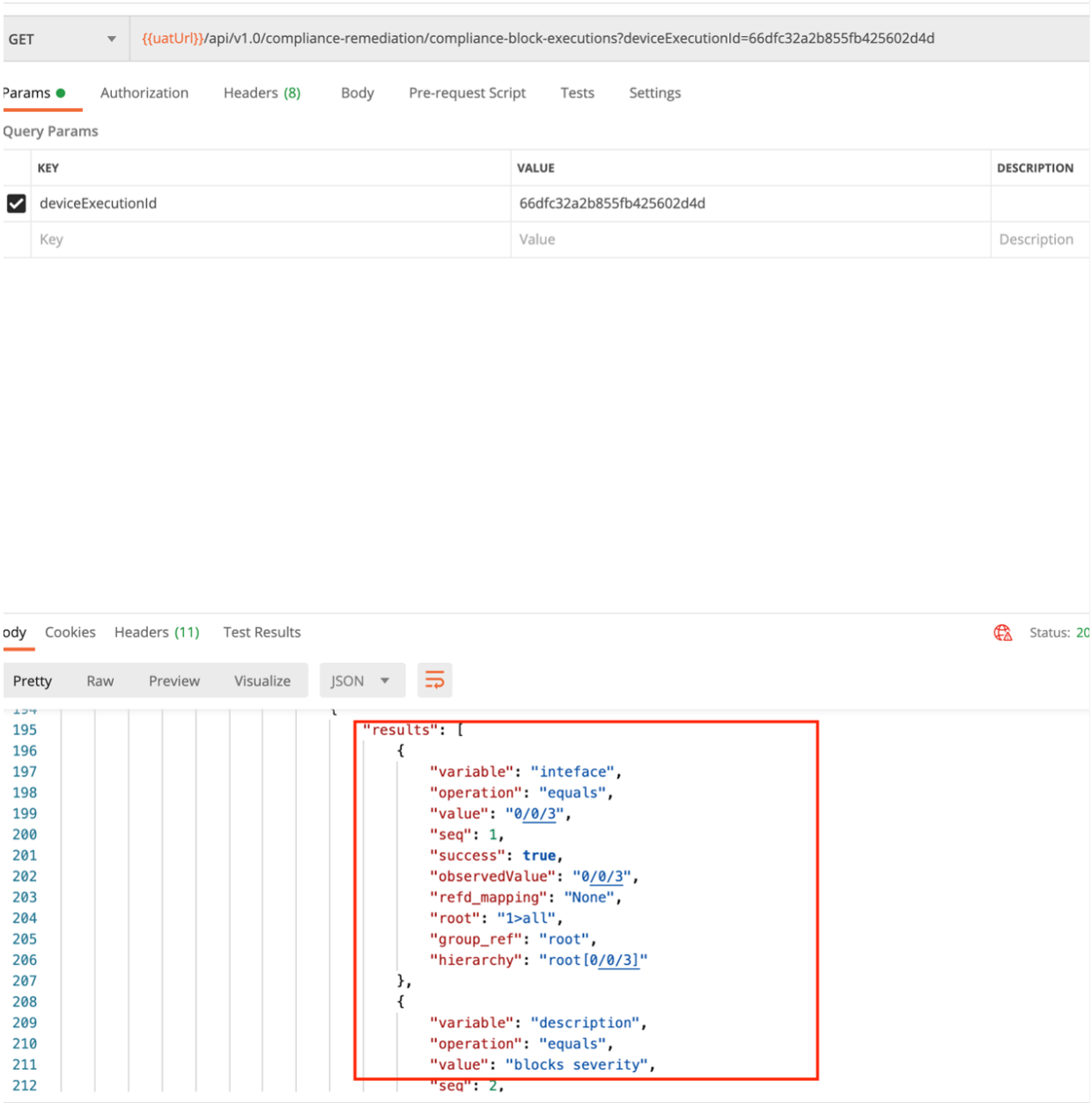
Beobachtung: Während der Ausführung eines Compliance-Auftrags zeigen die Regelvariablen leere Werte an.

Analyse:

1. Wenn Daten aus der RefD-Anwendung abgerufen werden, stellen Sie sicher, dass die RefD-Schlüssel das richtige Format aufweisen. Wenn ja, stellen Sie sicher, dass die RefD-Anwendung über Daten für den Schlüssel verfügt, die mit der Compliance-Variablen in den Regeln verknüpft sind. Überprüfen Sie außerdem, ob der richtige RefD-Schlüssel von der Compliance-App gesendet wird, indem Sie die Compliance-Serviceprotokolle überprüfen. Weitere Informationen finden Sie unter Grundlegendes zur Regelhierarchie und zur RefD-Integration in Regeln und Nicht-RefD-Regeln.
2. Überprüfen Sie das Ergebnis der Compliance-Blockausführung mithilfe der folgenden API:

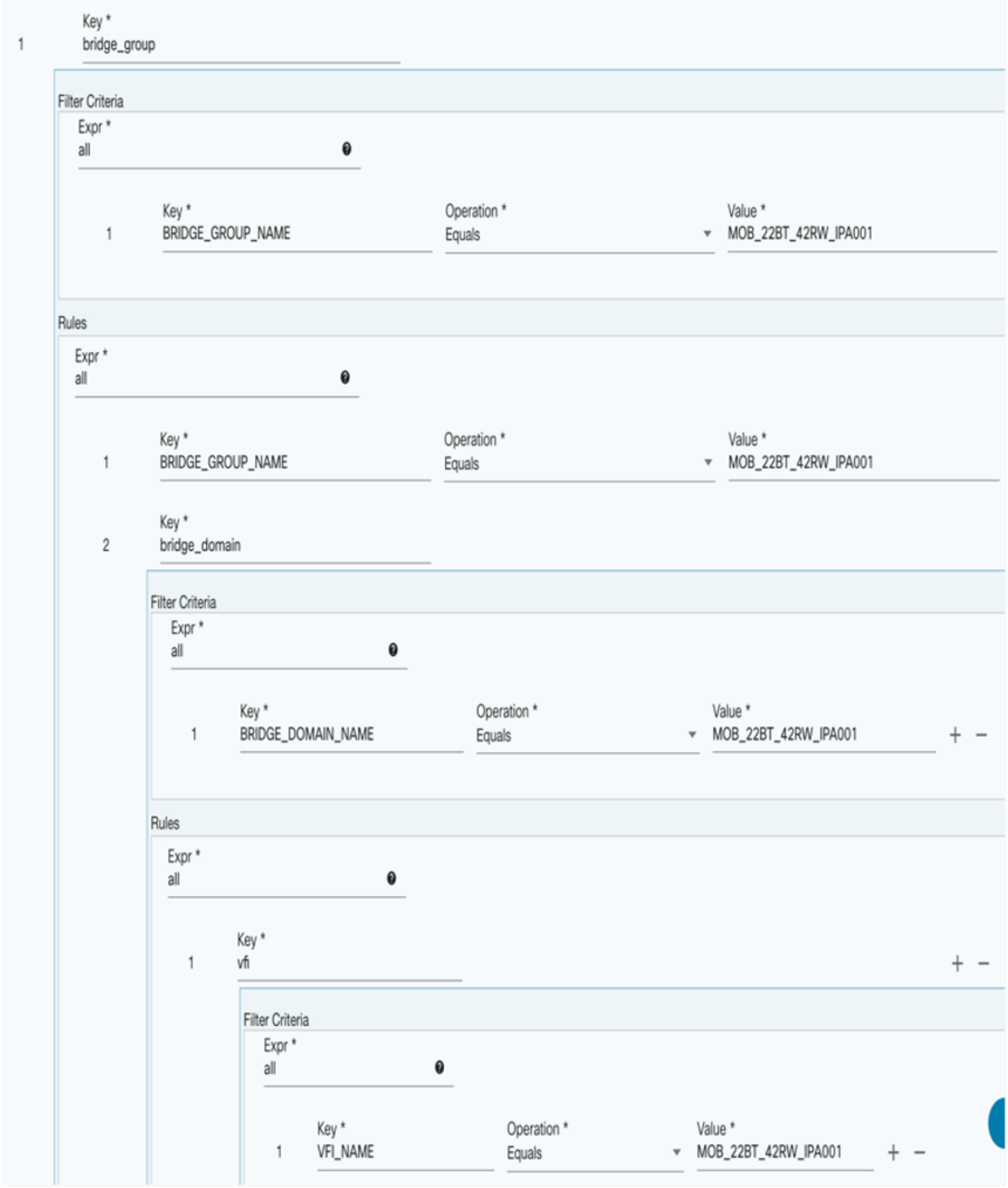
   URL: /api/v1.0/compliance-sanierung/compliance-block-executions?deviceExecutionId=<>

   Methode: HOLEN




Ergebnisse der Compliance-Blockausführung

3. Überprüfen Sie, ob der Block untergeordnete Hierarchien oder eine einzelne Hierarchie aufweist, und stellen Sie sicher, dass die Regeln entsprechend der Hierarchie konfiguriert sind.




Ergebnisse der Compliance-Blockausführung

4. Stellen Sie sicher, dass der TTP Parser den Wert aus der Gerätekonfiguration extrahiert, indem Sie das folgende Python-Skript ausführen:

```
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)
```

## Überwachen von Compliance-Protokollen

### Umschlag mit einem Knoten:

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

### Kubernetes Umschlag mit mehreren Knoten:

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

### Überwachung der Kibana-Protokolle:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.