

# BPA使用手冊配置合規性和補救v5.1

- [簡介](#)
- [快訊](#)
  - [元件](#)
- [假設和前提條件](#)
- [合規性控制面板](#)
  - [配置合規性流程圖](#)
  - [資產合規性摘要](#)
  - [資產合規性的CSV檔案詳細資訊](#)
- [開啟和使用CSV檔案以實現資產合規性](#)
  - [檢視違規詳細資訊](#)
  - [檢視和比較補救配置](#)
  - [策略符合性摘要](#)
  - [匯出為CSV以實現策略合規性](#)
  - [策略合規性的CSV檔案詳細資訊](#)
  - [開啟和使用CSV檔案以遵守策略](#)
- [報告](#)
  - [報告控制面板](#)
  - [報告配置](#)
  - [生成報告](#)
  - [下載和檢視報告](#)
    - [瞭解配置合規性摘要報告](#)
  - [刪除報告](#)
- [合規性作業](#)
  - [主要功能](#)
  - [建立合規性作業](#)
- [建立離線稽核作業](#)
  - [編輯符合性作業](#)
- [立即運行或重新運行合規性作業](#)
  - [刪除符合性作業](#)
  - [終止合規性作業](#)
  - [合規性作業歷史記錄](#)
- [補救作業](#)
  - [配置補救流程圖](#)
  - [補救作業清單](#)
  - [建立和編輯補救作業](#)
  - [補救執行：裝置清單](#)
- [組態：塊和規則](#)
  - [塊的功能](#)
  - [規則的功能](#)
    - [與Block生命週期整合](#)
  - [清單塊](#)
    - [功能塊的詳細資訊](#)

- [新增或編輯塊和規則](#)
- [使用忽略行語法](#)
- [引發違規](#)
- [規則管理](#)
  - [新增或編輯規則詳細資訊](#)
  - [新增或編輯規則違規](#)
- [動態使用者定義的塊 — 最佳實踐](#)
- [瞭解規則層次和規則與非RefD規則中的RefD整合](#)
- [RefD整合](#)
  - [符合性規則值的語法](#)
  - [變數型別](#)
  - [非RefD規則](#)
  - [變數使用](#)
  - [執行](#)
- [檢視塊詳細資訊](#)
- [刪除塊](#)
- [組態:自動生成塊](#)
  - [自動生成塊](#)
- [塊識別符號](#)
  - [清單塊識別符號](#)
  - [建立或編輯塊識別符號](#)
- [組態:政策](#)
  - [列出策略](#)
  - [新增和編輯策略](#)
  - [策略詳細資訊](#)
  - [「選擇塊」對話方塊](#)
  - [條件式篩選條件](#)
  - [Remediation部分](#)
  - [自動生成GCT功能](#)
- [角色和訪問控制](#)
  - [靜態許可權清單](#)
  - [預定義角色](#)
  - [訪問策略](#)
- [離線符合性](#)
  - [使用裝置備份配置](#)
  - [在符合性作業中使用建立離線稽核功能](#)
- [通過Ingestor部署配置](#)
- [參考資料](#)
- [API 說明文件](#)
- [疑難排解](#)
  - [控制面板](#)
  - [合規性作業](#)
  - [合規性規則](#)
  - [監控合規性日誌](#)

# 簡介

配置合規性和補救(CnR)應用程式允許網路操作員對從配置塊構建的自定義策略執行裝置配置合規性檢查。操作員使用系統從選定的裝置配置手動定製或自動生成配置塊。使用者還可以建立應用於這些塊的規則，規則條件可能源自從RefD應用程式獲得的值。操作員可以方便地按照時間表執行合規性檢查或立即啟動檢查。

該應用程式擁有直觀的儀表板，呈現合規性違規的全面概述，提供裝置和配置塊級別的摘要和詳細檢視。

該應用包括用於處理合規性違規的強健補救框架。此框架利用工作流和模板(稱為黃金配置模板(GCT)的配置模板和流程模板)來簡化補救流程。與合規性檢查類似，補救任務也可以按照時間表運行或立即觸發，以迅速解決違規問題。

新一代(下一代)門戶的Compliance and Remediation控制面板具有多項功能，旨在增強網路安全管理、簡化合規性程式和簡化補救活動。控制面板提供資產和策略合規性的全面摘要，使網路運營商可以輕鬆評估其網路的運行狀況，並確保裝置符合嚴格的安全協定。

配置塊可以自動生成並手動編輯或新增，從而在自動化和自定義之間實現平衡。系統精確識別配置塊和精細訪問控制機制(包括傳統和現代介面上的詳細使用者、組和許可權設定)，確保網路配置保持安全，並掌握在受信任人員手中。這些功能為希望保持高網路合規性和安全標準的組織提供了強大的工具集。

## 快訊

引入了以下主要功能和增強功能：

- 用於生成、檢視和下載合規性報告的全面報告控制面板
- 能夠使用Asset Manager通過上傳裝置配置執行離線合規性稽核，而無需登入裝置
- 能夠在塊配置中配置模式以遮蔽敏感裝置配置資料
- 能夠將策略和資產合規性摘要網格資料匯出為CSV檔案
- 檢視生成的補救配置並將其與裝置運行配置進行比較
- 塊中的增強功能，可在配置存在時支援引發違規
- 在策略建立和編輯頁面中啟用連線的使用者體驗，以交叉啟動子元件，如塊建立頁面
- 合規性作業中的增強功能建立和編輯頁面以交叉啟動到策略編輯頁面

## 元件

合規性和補救支援以下控制器和裝置型別：

| 控制器                        | 作業系統型別                             |
|----------------------------|------------------------------------|
| NSO(6.5)                   | IOS XE、IOS XR、NX-OS、JunOS、諾基亞SR-OS |
| CNC(6.0)                   | IOS XE、IOS XR、NX-OS                |
| NDFC ( 3.2.0/交換矩陣v12.2.2 ) | NX-OS                              |
| Cisco Catalyst中心(2.3.5)    | IOS XE、IOS XR。僅限經驗證的合規性            |
| FMC(7.2.5)                 | FX-OS(FTD)。僅限經驗證的合規性               |
| 直接到裝置(D2D)                 | IOS XE、IOS XR、JunOS                |

---

 附註：通過NSO控制器提供諾基亞SR-OS支援僅適用於配置合規性功能。Nokia裝置不支援補救。

---

 附註：合規性功能適用於思科命令列介面(CLI)格式的裝置配置以及Juniper和Nokia裝置的類似YAML格式。目前，框架不支援其他格式，如Netconf、JSON、XML等。

---

作為v5.0版本的一部分，已棄用合規性和補救(CnR)傳統應用程式。所有CnR功能現已完全整合，可在下一代門戶中使用。

## 假設和前提條件

要有效地使用CnR使用案例，需要滿足以下先決條件。

- 應上傳CnR使用案例的訂閱權利金鑰。
- 相關控制器和裝置應已入網並作為BPA Asset Manager的一部分提供。有關詳細資訊，請參閱[BPA使用手冊](#)中的Asset Manager部分。
- 在下一代門戶中，需要根據客戶需求將入網資產分組為資產組。

## 合規性控制面板

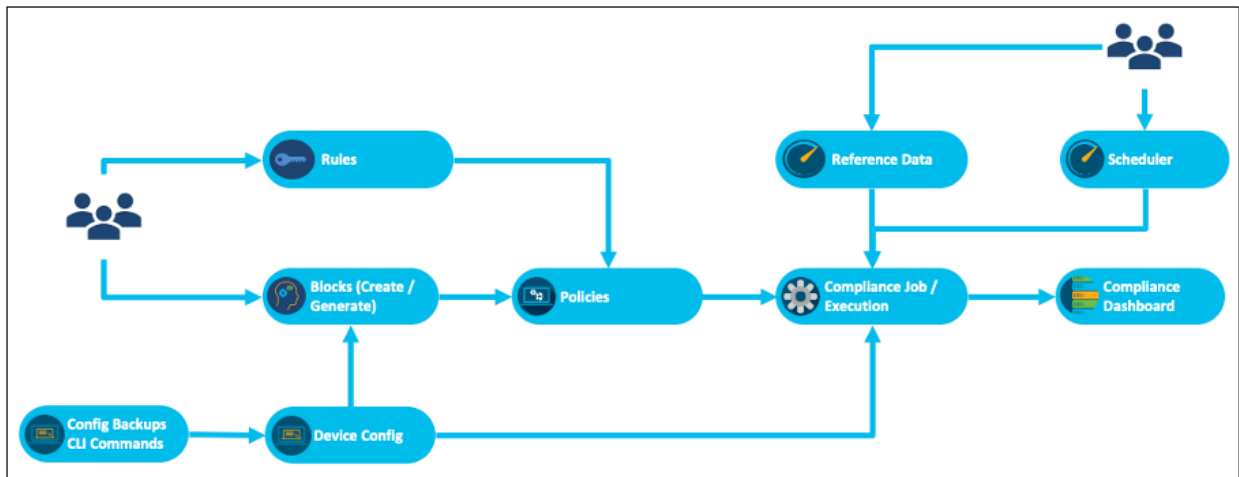
合規性控制面板提供所選時間所有裝置上的違規的彙總檢視。預設顯示當前月份的資料。使用者可以更改時間視窗以檢視有關遵循性違規的歷史資料。當前月份是預設選定的檢視。

---

 附註：傳統UI中已棄用的合規性儀表板已被刪除，並且不再可用。應使用下一代門戶中可用的控制面板。

---

## 配置合規性流程圖



配置合規性元件概述

針對資產清單為策略運行合規性作業時，會填充儀表板中顯示的合規性違規。通過新增塊配置清單以及必要的遵循性規則來建立遵循性策略。相容性規則可以檢查靜態值或動態變數，這些變數從 RefD 應用程式獲取資料。合規性作業可以按需運行，也可以作為一次性或定期計畫運行。

配置合規性包括以下重要功能：

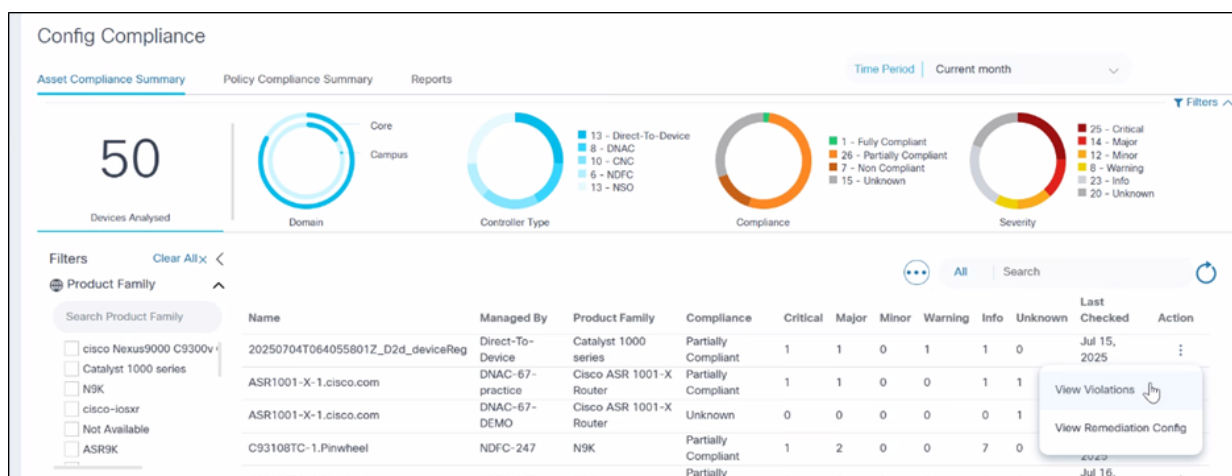
- 阻止建立:使用模板文本解析器(TTP)模板手動建立或自動生成塊。它們可以是靜態的，也可以是動態的（帶有變數）。
- 規則建立:規則驗證塊中的變數。在執行期間，可以靜態設定規則值，也可以從參考資料(RefD)系統動態檢索規則值。
- 策略建立:通過選擇塊清單和相應的規則來建立策略。規則的資料可以是靜態的，在運行時從 RefD 框架動態獲取。
- 合規性作業建立:通過選擇策略和資產組（包含資產清單）來運行合規性檢查，可以建立合規性作業。使用者可以選擇從備份框架中檢索裝置配置，或者在執行期間通過裝置上的流程模板運行即時命令。從備份獲取配置有助於離線稽核裝置，而無需連線到活動裝置。可以計畫作業或按需運行作業。
- 遵循性違規：檢視儀表板上的遵循性違規。

## 資產合規性摘要

Asset Compliance Summary 頁籤是一項基本功能，旨在全面概述網路中所有裝置的違規情況。此頁籤允許使用者快速確定合規性問題，確保所有裝置都遵守既定的策略和標準。該介面具備強大的過濾和搜尋功能，便於導航和分析合規性資料。

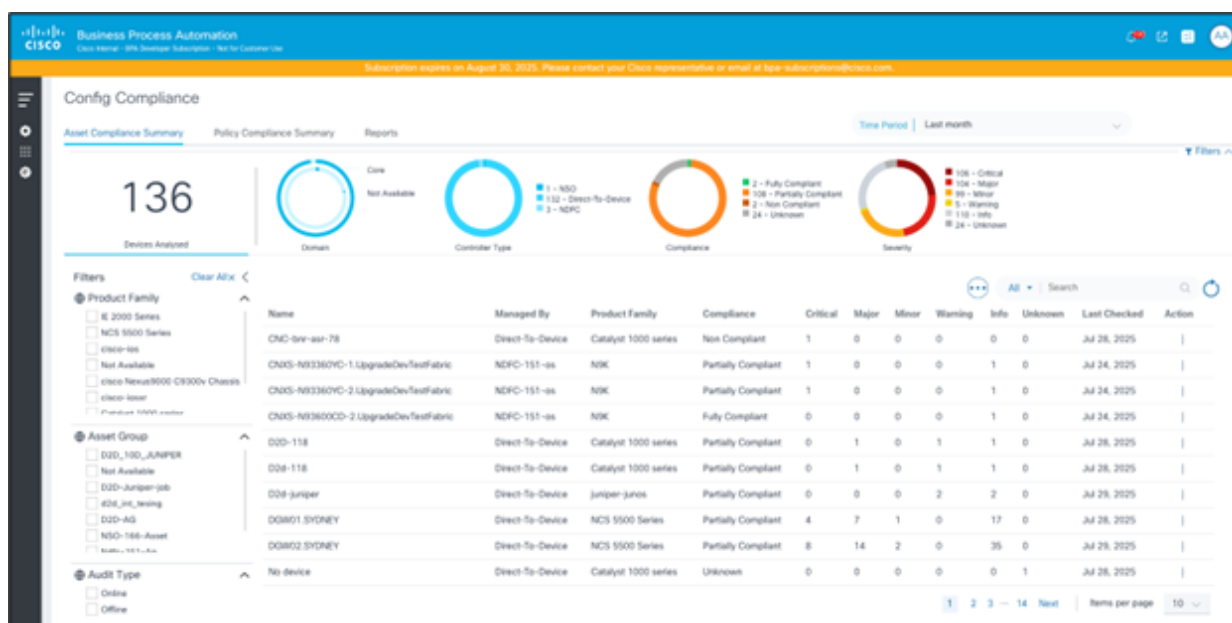
主要功能

- 每個裝置的違規摘要:該頁籤顯示每個裝置的合規性違規的彙總檢視，使使用者可以快速瞭解按嚴重性級別（如嚴重、高、中和低）分類的整個合規性狀態。
- 詳細的違規資訊:對於每個裝置，彈出視窗提供關於違規策略的詳細資訊，使用者可以進一步深入檢視導致違規的塊和配置行。



## 檢視資產符合性摘要

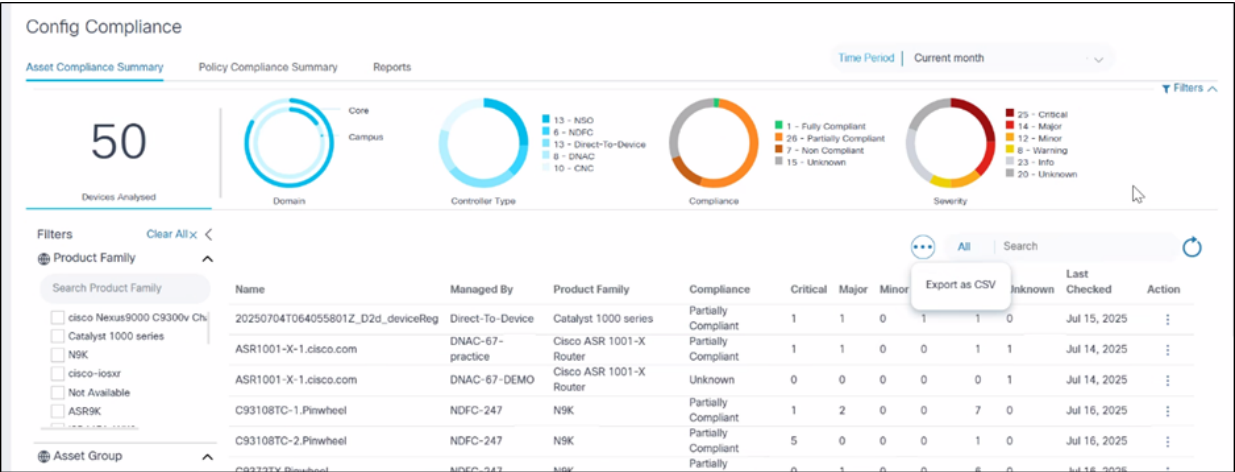
- 高級篩選選項:位於頁籤頂部和左部的篩選器允許使用者縮小顯示在網格中的資料。使用者可以按日期範圍、資產組、產品系列等進行篩選，從而實現對合規性資料的重點分析。
- 搜尋功能:可使用搜尋欄位來進一步縮小網格中的資料。使用者可以通過輸入相關關鍵字或短語來快速找到特定裝置或按控制器進行管理。
- 可自定義的日期範圍：預設情況下，在日期範圍篩選器中選擇當前月份，從而提供最新的符合性資料。但是，使用者可以自定義日期範圍以檢視資料。
- 篩選條件：可以使用多個篩選器，如產品系列、資產組和稽核型別。應用篩選器以刷新網格。



## 資產合規性摘要

- 匯出為CSV:一項功能，可幫助使用者獲取資產配置合規性的本地副本，以用於離線分析、報

告和存檔目的。要將資料匯出為CSV檔案，請從「更多選項」圖標中選擇「匯出為CSV」。下載的CSV檔案包含當前顯示在網格中的資料，並遵循任何應用的篩選器。



資產合規性摘要：匯出為CSV

資產合規性的CSV檔案詳細資訊

CSV檔案包括Asset Compliance Summary網格中可見的所有列，例如裝置名稱、控制器例項（管理者）、裝置的產品系列、裝置合規性狀態、按嚴重性列出的違規計數（例如，嚴重、主要、次要、警告、資訊、未知）以及上次檢查裝置合規性的日期。

如果網格具有分頁，則匯出將包含跨頁的所有記錄，而不只是可見的頁。

開啟和使用CSV檔案以實現資產合規性

- 1. 在Excel或任何相容的電子表格應用程式中開啟下載的CSV檔案。
- 2. 確保內容與「資產合規性摘要」網格中顯示的內容相匹配，包括篩選的結果。

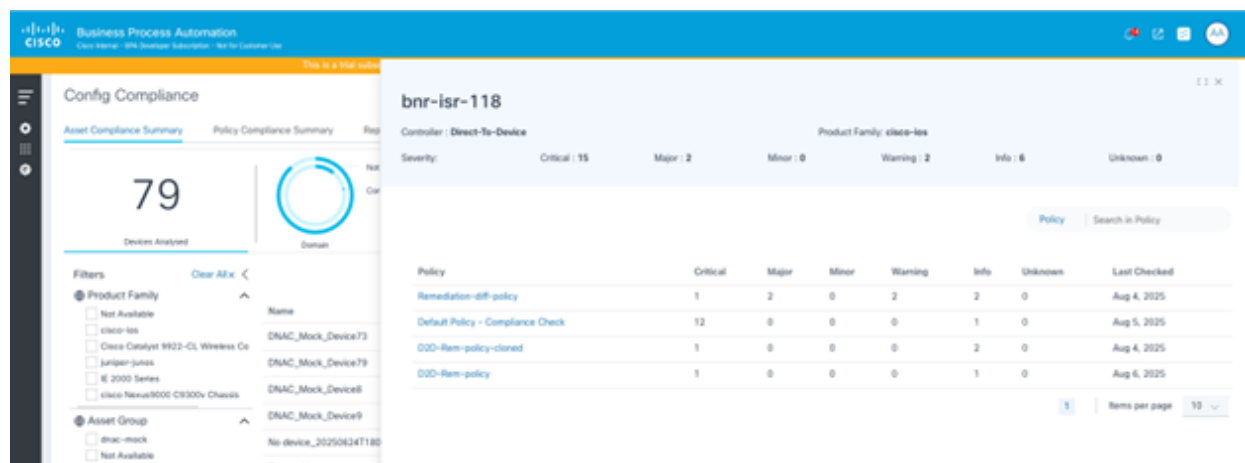
|   | A                 | B                | C                                                    | D                   | E        | F     | G     | H       | I    | J       | K            |
|---|-------------------|------------------|------------------------------------------------------|---------------------|----------|-------|-------|---------|------|---------|--------------|
| 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 |                   |                  |                                                      |                     |          |       |       |         |      |         |              |

資產合規性摘要：在Excel應用程式中開啟的CSV檔案

按策略檢視資產符合性摘要

按一下「資產合規性摘要」網格中的某一行，將顯示資產違規的詳細資訊，按照驗證裝置所依據的不同策略進行分類。此檢視為使用者提供了一個詳細的檢視，用於按嚴重性檢視每個策略中的違規

計數。



資產合規性摘要：按策略列出的合規性摘要



附註：應該注意以下幾點。

- Policy列中的超連結將使用者定向到Policy details頁面
- 按一下某一行將顯示所選策略的「違規詳細資訊」頁面

## 檢視違規詳細資訊

Violation Details頁面顯示裝置配置上覆蓋的塊和規則級違規。此外，使用者還可以檢視塊配置和建議的補救配置。

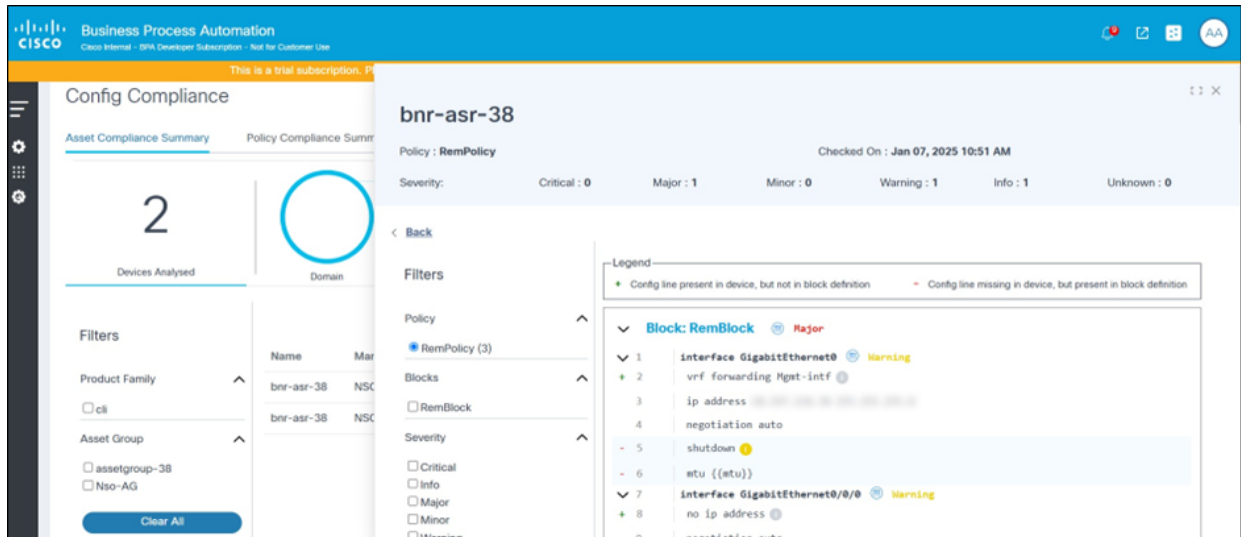
要從「資產合規性彙總」頁檢視「違例詳細資訊」頁以及策略級別分解，請執行以下操作：

1. 在資產合規性網格中選擇行。系統會顯示一個彈出視窗。網格按策略顯示合規性詳細資訊的細分。
2. 在網格中選擇一行。系統隨即會顯示Violation Details頁面。

要從Policy Compliance Summary網格中檢視「違規詳細資料」頁，請執行以下操作：

1. 選擇Policy Compliance Grid。
2. 選擇行>受影響的資產網格。
3. 選擇行。將顯示Violations Details頁。

Violations Details頁面的右側顯示裝置配置塊，並將違規疊加在裝置配置塊上。系統會根據相應的配置行列出違規。在條件失敗的情況下，違規功能區會提供規則名稱、條件以及預期配置（如規則中所定義）與從裝置配置中檢索到的配置的詳細資訊。



## 違反資產合規性

### 塊符號

- 針對某行的「+」符號表示根據塊配置不需要該配置，但額外存在於裝置配置中。
- 針對某行的「—」符號表示該配置按塊配置進行配置，但在裝置配置中缺失。

### 篩選條件

頁面左側的過濾器部分允許使用者執行下列操作：

- 改變政策；這將刷新頁面並載入新選定策略的違規
- 選中Blocks釐取方塊以檢視與所選塊相關的違規
- 選中Severity釐取方塊以檢視具有給定嚴重性級別的違規
- 選中Violation Type釐取方塊以檢視所選型別的違規：
  - 順序不相符:裝置配置行的順序與塊配置中定義的順序不匹配
  - 缺少配置:檢視根據塊配置預期但在裝置配置中缺少的配置行
  - Additional Config:檢視根據塊配置不應出現但額外存在於裝置配置中的配置行
  - 規則失敗:規則中的一個或多個條件的失敗。
  - 缺少塊：整個裝置配置塊丟失或與定義的塊配置不匹配。
  - 跳過的塊:已跳過此配置塊，因為不符合塊過濾器條件。

## 檢視和比較補救配置

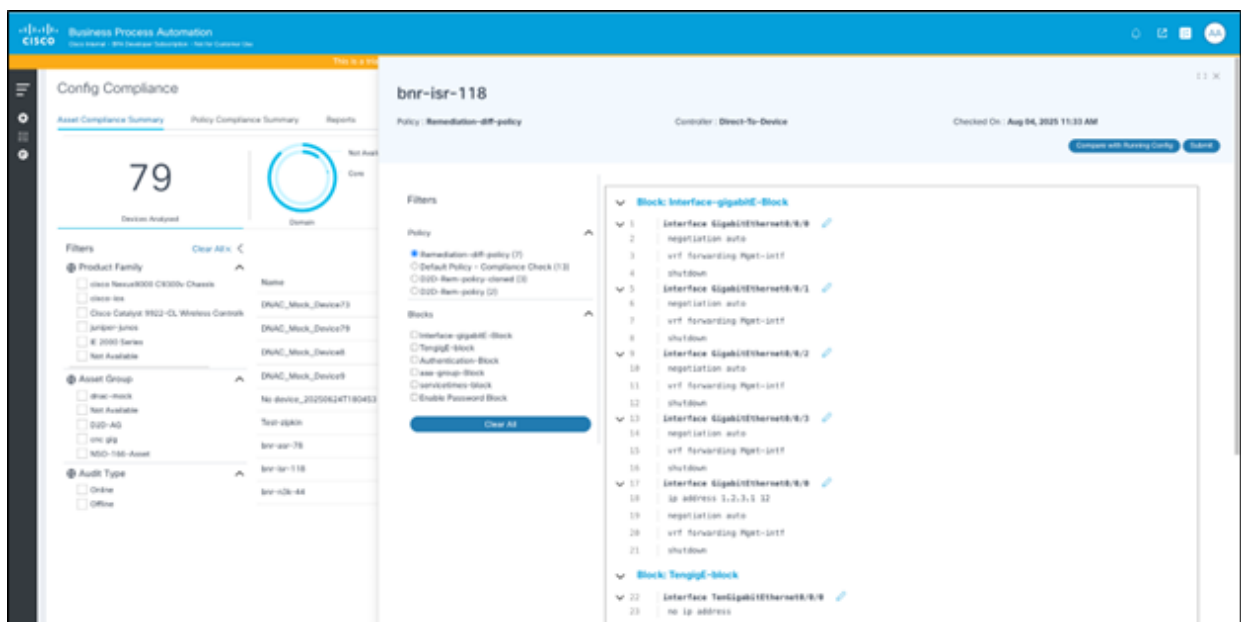
Remediation Config頁顯示給定策略中每個塊的選定裝置生成的配置。生成配置時，會考慮策略中存在的塊和規則詳細資訊，以及在合規性執行期間檢索的裝置配置。使用者可以選擇在同一頁中更新配置。可以使用補救作業功能將此生成的配置推送到裝置。此外，此頁還為使用者提供將生成的配置與當前裝置運行配置進行比較的選項。使用者可以指定一個或多個命令來檢索當前裝置配置。

要從資產合規性網格中查看「修正配置」頁面：

1. 按一下Asset Compliance Summary選項卡。
2. 在「操作」列的資產符合性網格中，選擇更多選項圖示 > 檢視修正配置。系統隨即會顯示 Remediation Config頁面。

要從策略符合性網格中檢視Remediation Config頁：

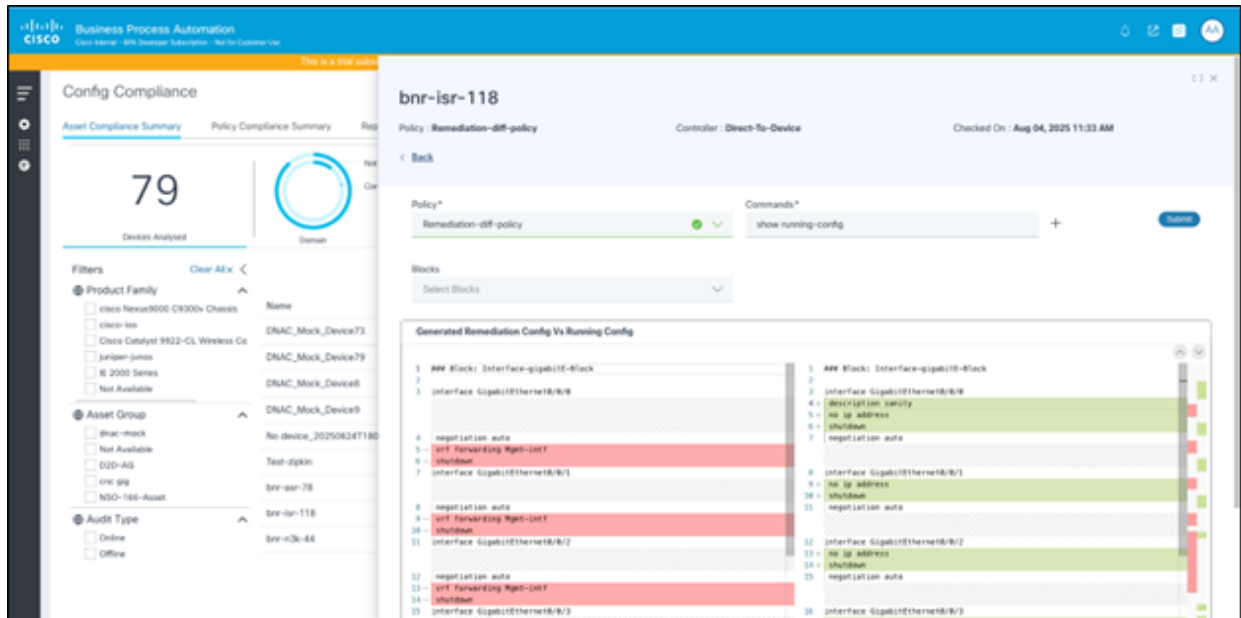
1. 按一下Policy Compliance Summary頁籤。
2. 在策略符合性網格中，選擇所需的行。系統隨即會顯示「受影響的資產」網格。
3. 在Action列中，選擇More Options圖示>選擇View Remediation Config。系統隨即會顯示 Remediation Config頁面。



「補救配置」頁

Remediation Config頁顯示以下內容：

- 生成的補救配置:生成的配置將顯示在頁面的右側，使用者還可以選擇編輯配置塊並提交要儲存的更改
- 篩選條件：過濾器可用於選擇策略，然後可選地選擇一個或多個塊以檢視相應的生成配置
- 與運行配置比較:按一下Compare with Running Config以顯示詳細頁面，該頁面允許使用者將生成的配置與裝置的運行配置進行比較



「與運行配置比較」頁

Compare with Running Config頁顯示以下內容：

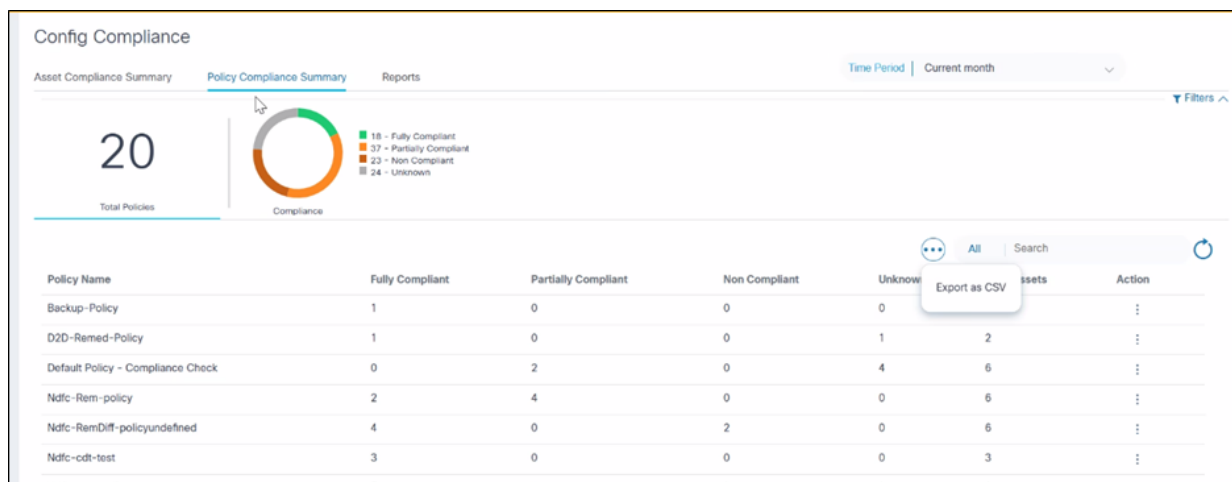
- 用於選擇策略的選項:上一頁中選定的策略已預先選定。
- 一個文本框，用於輸入要在裝置上執行的一個或多個命令
- 一個Submit按鈕，用於在裝置上運行命令並檢索配置
- 用於檢視和篩選塊的選項:預設情況下，會顯示策略中的所有塊；使用者可以根據需要選擇單個塊
- 配置比較查看器並行顯示生成的配置和裝置配置，並突出顯示差異

## 策略符合性摘要

Policy Compliance Summary頁籤旨在根據定義的策略提供裝置的合規性狀態的清晰而簡明的概述。此頁籤可幫助使用者快速評估合規性狀況並確定需要關注的方面。該頁籤根據裝置的合規性狀態對裝置進行分類，便於您輕鬆瞭解並簡要管理合規性。

符合性狀態：

- 完全符合:所有裝置均符合各自策略的所有合規性規則。
- 部分符合:有些裝置符合規則，但有些裝置不符合規則。
- 不符合:沒有裝置符合策略。
- 未知:由於網路連線問題或備份不可用，無法檢查策略是否一致。



## CSV匯出的策略合規性摘要

## 匯出為CSV以實現策略合規性

匯出為CSV功能可幫助使用者獲取策略合規性的本地副本，以用於離線分析、報告和存檔目的。要將資料匯出為CSV檔案，請從More Options圖示中選擇Export as CSV。下載的CSV檔案包含當前顯示在網格中的資料，並遵循任何應用的篩選器。

## 策略合規性的CSV檔案詳細資訊

CSV檔案包括策略名稱、已驗證資產的總數以及按照合規狀態（即「完全合規」、「部分合規」、「不合規」和「未知」）細分的計數。如果網格具有分頁，則匯出包括所有頁面中的所有記錄，而不僅僅是當前頁面上顯示的記錄。

## 開啟和使用CSV檔案以遵守策略

1. 在Excel或任何相容的電子表格應用程式中開啟下載的CSV檔案。
2. 確保內容與「策略符合性摘要」網格中顯示的內容相匹配，包括篩選的結果。

|    | 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 |                                   |                 |                     |               |         |              |

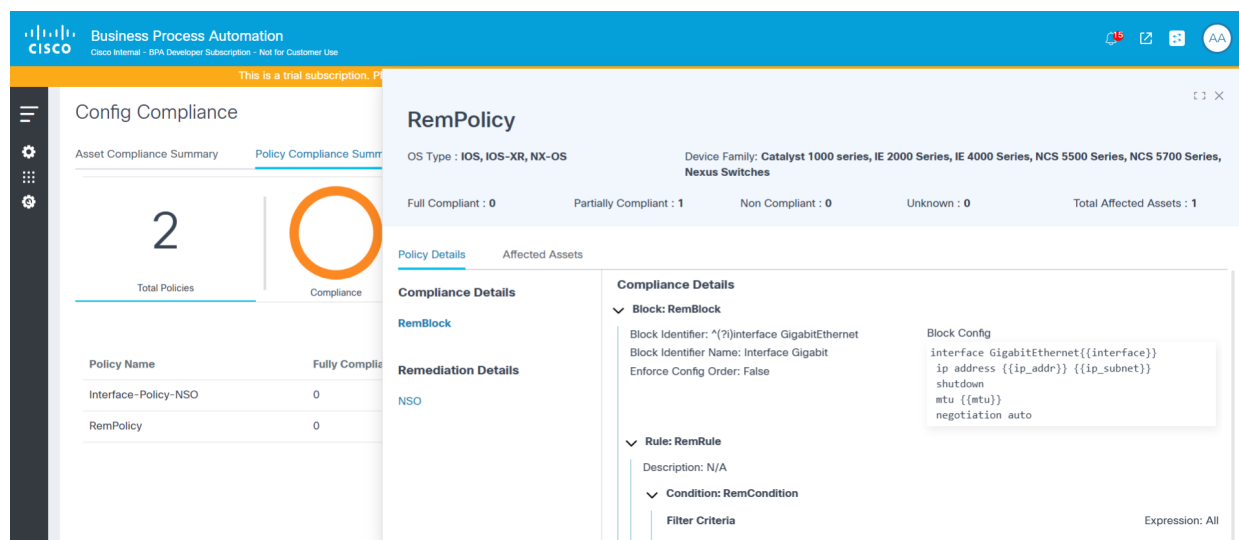
## 策略合規性：策略詳細資訊

### 檢視策略詳細資訊

要檢視策略詳細資訊，請執行以下操作：

1. 從操作(Action)列下的更多選項(More Options)圖示中選擇策略。
2. 選擇檢視策略詳細資訊。系統隨即會顯示Policy Details頁面。

 附註：Policy Details頁為所有策略資訊（包括塊、規則和條件）的只讀檢視。使用者可以按一下直接導航到相關塊的頁面中的超連結。



| Policy Name          | Fully Compliant |
|----------------------|-----------------|
| Interface-Policy-NSO | 0               |
| RemPolicy            | 0               |

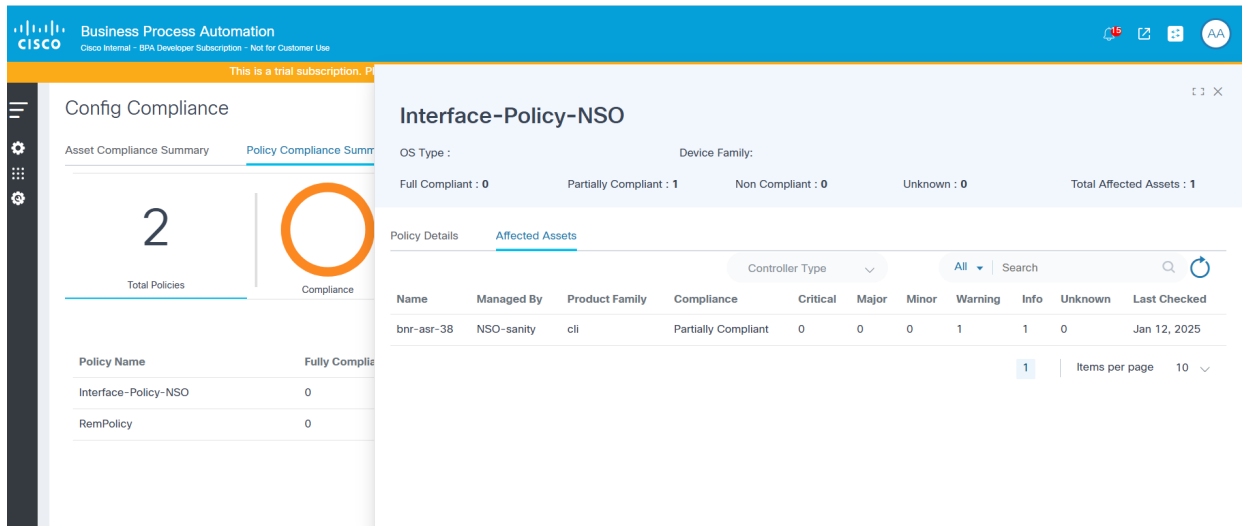
## 策略合規性：策略詳細資訊

### 檢視受影響的資產

Affected Assets頁籤顯示每個策略下分析的資產清單以及按嚴重性分割的違規計數。可使用 Controller Type 下拉選單和搜尋框過濾裝置。

要從Policy Compliance Summary選項卡查看受影響的資產，請執行以下操作：

1. 選擇行。將開啟遵循性策略視窗。
2. 按一下Affected Assets頁籤。



策略合規性：受影響的資產



附註：Affected Assets頁籤提供用於開啟View Violation Details頁和View Remediation Config頁的操作。有關詳細資訊，請參閱資產合規性摘要。

## 報告

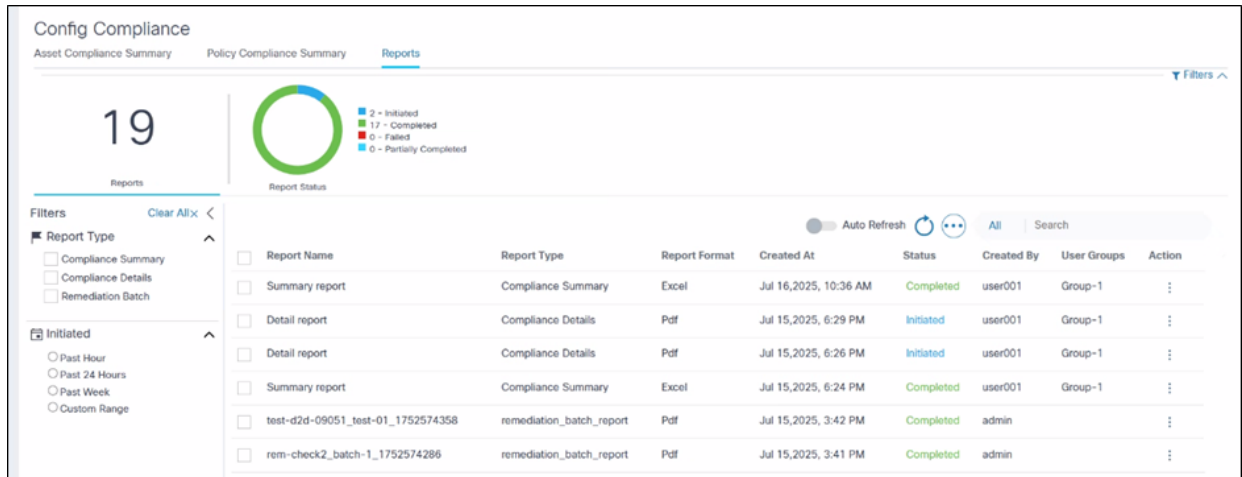
報告部分旨在提供裝置合規性的全面見解、識別違規行為和促進補救工作。該應用程式提供了一個使用者友好的介面，用於生成、檢視、下載和管理各種型別的合規性報告。

### 報告控制面板

Reporting Dashboard是所有合規性報告活動的中心中心。使用者可以通過此單一介面高效地管理其報告。Reports Dashboard上的主要功能包括：

- 檢視報告:使用者可以檢視所有生成的報告的清單，包括其名稱、型別、關聯策略、格式、建立日期和當前狀態（例如，已啟動、已完成、失敗、部分完成）
- 下載報告:報告一旦生成，就可以下載用於離線分析或存檔目的；「操作」(Action)列提供下載選項
- 刪除報告:使用者可以從控制面板中刪除舊的或不必要的報告，從而幫助維護一個乾淨和有組織的報告環境
- 篩選和搜尋:控制面板提供了廣泛的篩選選項，允許使用者根據報告型別（如Compliance Details、Compliance Summary、Remediation Batch）、策略和啟動狀態（如Past Hour、Past 24 Hours、Past Week、Custom Range）等標準快速查詢特定報告；酒店還設有搜尋欄
- 報告狀態監控:視覺化摘要（如餅圖）表示報告的狀態，顯示有多少報告已啟動、已完成、失敗或部分完成。

Reporting控制面板是Compliance and Remediation控制面板上Reports頁籤下的登入頁。



## 報告控制面板

- 可用的報告型別包括：
  - 符合性摘要報告
  - 合規性詳細報告
  - 補救批處理報告
- 使用過濾器選擇以下內容：
  - 報告型別
  - 政策
  - 啟動時間段（根據所選時間範圍過濾報告清單）
- 用於自動刷新報告清單的選項

## 報告配置

報告配置使管理員能夠根據部署和業務需求配置與報告相關的關鍵引數。以下引數可用於配置：

- 自動刪除早於（天）的報告：任何早於此持續時間的報告都將從系統中刪除
- 合規性摘要報告中每個策略要選擇的最大塊數：幫助將Excel檔案中的頁籤數量限制為可讀限制
- 要在合規性詳細報告中選擇的最大資產：幫助限制為給定詳細報告生成的PDF檔案的數量

## 符合性作業清單

## 生成報告

該應用程式提供了用於生成新符合性報告的專用介面，允許使用者選擇報告型別、定義範圍並應用特定的篩選器。報告生成過程從「報告」控制面板頁面下的「生成報告」操作啟動。

生成報告的主要方面包括：

- 選擇報告型別:使用者可以選擇以下不同的報告型別
  - 摘要報告:提供所選策略的所有裝置的合規性概述
  - 詳細報告:提供更詳細的檢視，提供關於每個裝置特定違規的深入資訊
- 命名報告:使用者必須為生成的報告提供相關名稱
- 時間段選擇:可以為特定時間範圍（如「當前月份」或自定義範圍）生成報告，以重點分析最近的符合性資料
- 套用篩選條件:綜合過濾選項使使用者能夠縮小報告的範圍
  - 原則：選擇一個或多個要包括在報告中的符合性策略。策略選擇是必需的
  - 封鎖:在選定的策略中，選擇要包括在報告中的特定配置塊。塊選擇是可選的
  - 資產組:使用者可以通過選擇一個或多個資產組來篩選範圍內的資產
- 資產選擇:這僅適用於詳細報告
  - 使用者可以選擇應為其生成報告的特定裝置
  - 資產表顯示了詳細資訊，如名稱、序列號、IP地址、管理者和當前符合性狀態，以及不同嚴重性級別的計數

要生成符合性摘要報告，請執行以下操作：

## 生成摘要報告

1. 在選擇報告型別下拉選單中選擇摘要報告。
2. 輸入報表名稱。
3. 選擇時間範圍。將基於此選擇列出策略和塊。
4. 選擇策略。還可以選擇其他策略。
5. 或者，選擇塊。如果未選擇任何選項，則包含所有塊。
6. 選擇所需的資產組、合規性狀態和嚴重性級別。
7. 按一下Generate Report。

- 在報告清單頁面中，報告狀態設定為Initiated
- 完成後，狀態更改為Completed。如果某些子報告失敗，狀態將更改為Partially Completed
- 如果整個報告生成失敗，將顯示通知並將狀態更改為「失敗」
- 下載完成後，即可使用下載選項。使用者可以下載包含excel報告的zip檔案

要生成符合性詳細報告，請執行以下操作：

Reports > Generate Report

Select Report Type \*  
Detailed Report

Enter Report Name \*  
Default Policy Report

Time Period | Last three months

Note: Max Assets to be selected in a Detailed Compliance Report is 5

2 Devices

Compliance

Severity

Filters

Policy\*

Default Policy - Compliance Chk

Block

Search Block

Default Block - Hostname

Default Block - Interface Loopba

Default Block - Interface Myme

Default Policy - Compliance Check X Clear All

Show Selected Devices All Search

| Name        | Serial Number | Ip Address      | Controller Type  | Compliance         | Critical | Major | Minor | Warning | Info | Unknown | Last Checked          |
|-------------|---------------|-----------------|------------------|--------------------|----------|-------|-------|---------|------|---------|-----------------------|
| bnr-isr-118 | FGL1932108 W  | 10.197.215.11 8 | Direct-To-Device | Partial Compliance | 12       | 0     | 0     | 0       | 1    | 0       | May 28, 2025, 2:43 PM |
| bnr-asr-115 | FXS1933Q27 N  | 10.197.215.11 5 | Direct-To-Device | Partial Compliance | 11       | 0     | 0     | 0       | 3    | 0       | May 28, 2025, 2:43 PM |

1 Items per page 10

## 生成詳細報告

1. 在選擇報告型別下拉選單中選擇詳細報告。
2. 輸入報表名稱。
3. 選擇時間範圍。將基於此選擇列出策略和塊。
4. 選擇策略。還可以選擇其他策略。
5. 或者，選擇塊。如果未選擇任何選項，則包含所有塊。
6. 選擇所需的資產組、合規性狀態和嚴重性級別。
7. 從網格中選擇所需的資源。使用者可以選擇「全選」裝置和「顯示所選裝置」。
8. 按一下Generate Report。

- 在報告清單頁面中，報告狀態設定為Initiated
- 完成後，狀態更改為Completed。如果某些子報告失敗，狀態將更改為Partially Completed
- 如果整個報告生成失敗，將顯示通知並將狀態更改為「失敗」

## 下載和檢視報告

可以使用報告儀表板網格中所需行中的「下載」圖示下載已完成的報告。

## 瞭解配置合規性摘要報告

「合規性摘要」報告是包含單個PDF報告的zip檔案，每個裝置生成一個PDF。此報告型別提供每個策略的合規性違規概述，以及針對裝置的塊級向下鑽取對映違規詳細資訊。



|   | 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 |
|   | Authentication-Block     | Authentication-Block | aaa authentication ([ authentication] re["*"])                                                                                                                                                                                          | Block Identifier: AAA<br>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                |
| 2 | Interface-gigabitE-Block |                      | interface GigabitEthernet{{ref_id}}<br>ip address {{ip_addr}} {{subnet_ip}}<br>negotiation {{ negotiation { re["*"] } }}<br>!{{ negotiation_exists, "True" }}<br>description sanity ignore_line<br>vrf forwarding Mgmt-intf<br>shutdown | Block Identifier: Interface<br>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                |
| 3 |                          |                      |                                                                                                                                                                                                                                         |                                                                                             |                                                                                                                                                 |                                                    |            |             |             |                  |

## 阻止摘要工作表

- 每塊的規則和違規詳細資訊：
- 違規級別網格顯示規則名稱、說明、違規名稱、說明嚴重性級別、跨資產可見的違規計數以及受影響的資產計數的清單
- 裝置級網格顯示規則、違規、嚴重性、裝置名稱和控制器名稱（由管理）之間的對映

|    | 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 |              |                                                                |                       |             |                  |                 |                       |

## 合規性詳細資訊報告

合規性詳細資訊報告包含以下資訊：

- 報告名稱:標識報告的名稱
  - 資產名稱:指定為其執行符合性檢查的裝置
  - 其他資產詳情:包括IP地址和序列號等詳細資訊（如果存在）
  - 嚴重性:按嚴重性級別提供違規的摘要計數
  - 報告生成時間:指示建立報表的時間戳
- 應用的篩選器：概述用於生成特定報告的特定過濾標準的詳細資訊，以確保透明度和可複製性。其中包括時間段、選定的策略、塊、嚴重性級別和遵從性狀態
- 規則和違規摘要:列出已評估的每個規則，並提供為該規則找到的違規的摘要。摘要網格顯示違規名稱、說明、嚴重性和發生此違規的次數
- 違規詳細資訊:提供有關選定資料塊的每個裝置配置行的明確詳細資訊以及每行的違規詳細資

# 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               |

合規性詳細報告 — 示例PDF第1頁

Violation Details

Legend

+ Config line present in device, but not in block definition

- Config line missing in device, but present in block definition

Block: Cnr Demo Block    Minor

1    interface GigabitEthernet0/0/0    Minor

Expected: desc Equals 'Demo'    Minor

Found: 'None'    Cnr Demo Policy2 → Demo Rule 2 → Demo Cond1

+ 2    no ip address    Info

+ 3    shutdown    Info

+ 4    negotiation auto    Info

+ 5    cdp enable    Info

6    interface GigabitEthernet0/0/1    Info Skipped

Expected: interface Equals '0/0/0'    Info

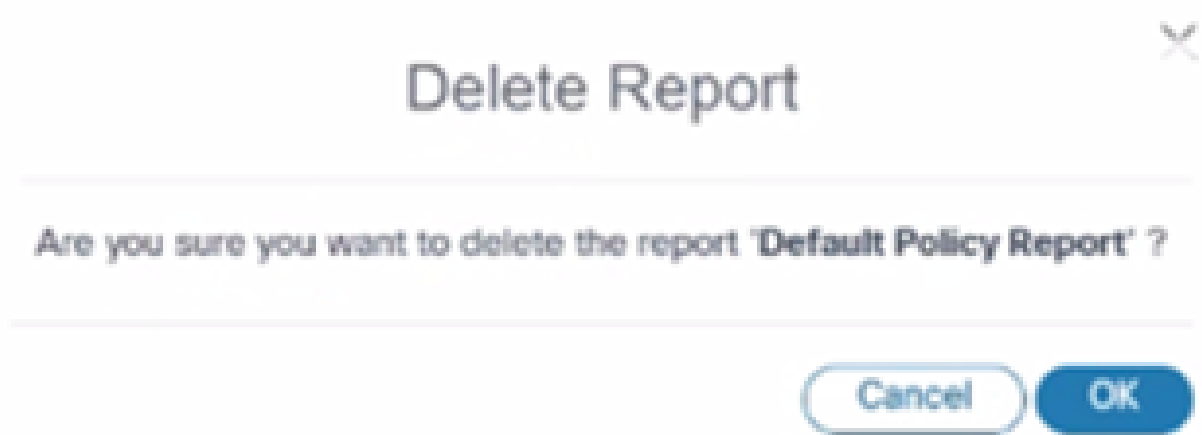
---

 附註：從Remediation batch頁面建立的Remediation batch PDF報告也可從報告清單中下載和檢視。

---

## 刪除報告

通過選擇刪除圖示可以單獨刪除報告，也可以通過選中報告的覈取方塊並選擇更多選項圖示> 刪除來批次刪除報告。



## 符合性作業清單

---

 附註：刪除報告只會從報告控制面板中刪除報告檔案和條目；基礎合規執行詳細資訊將保留。

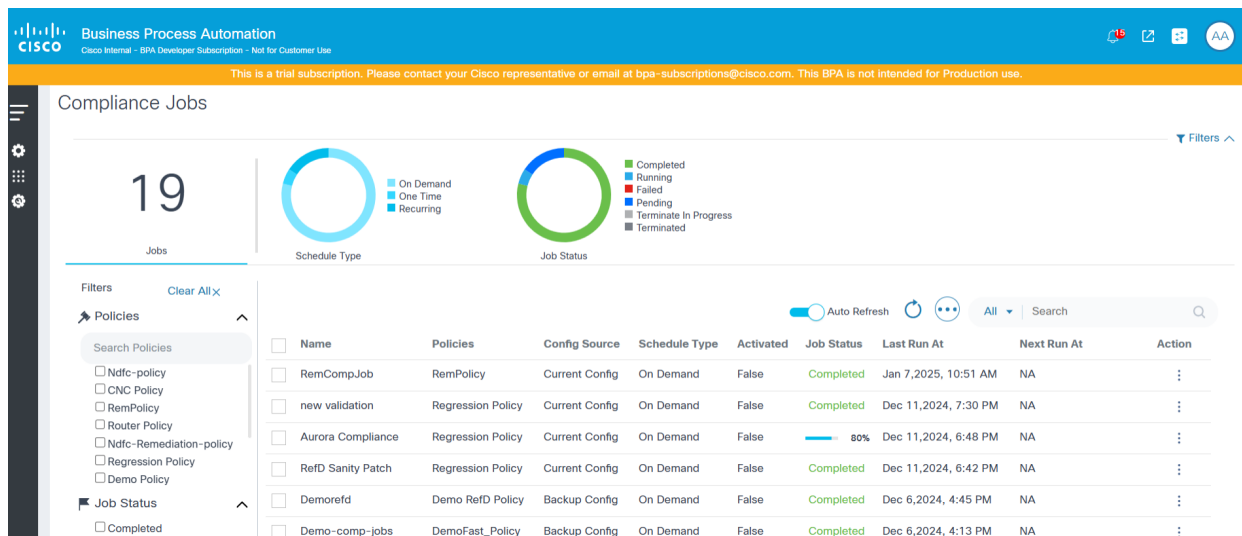
---

## 合規性作業

下一代門戶中的「合規性作業」功能旨在幫助使用者建立、管理並執行選定策略和資產組的合規性作業。可以計畫定期運行這些作業或按需執行這些作業，以確保所有資產都一致地檢查其符合性。

### 主要功能

- 列出符合性作業:檢視所有已定義的符合性作業，以及離線稽核、篩選、建立、編輯、刪除和執行作業的選項。
- 計畫作業和按需作業:將作業設定為按計畫的間隔運行，或根據需要立即執行。
- 細粒度訪問控制：根據使用者許可權控制對合規性作業的訪問，確保使用者只能檢視與其有權訪問的策略相關的作業。
- 篩選選項:按策略、作業狀態、計畫型別和日期範圍過濾作業，便於導航和管理。



## 符合性作業清單

## 建立合規性作業

Compliance Job Create頁包含以下屬性：

- 名稱:作業的名稱
- 說明:可選說明
- 策略名稱:用於選擇要運行的策略的下拉選單，可能按為登入使用者配置的訪問策略進行過濾
- 裝置配置源:一個下拉選單，用於選擇要獲取裝置配置（當前配置或裝置配置備份）以運行符合性作業的源，以及一個覈取方塊，用於指示在沒有備份時是否回退到CLI命令。



附註：僅當底層控制器支援備份功能時，Device Config Backup選項才起作用。

- 使用者定義變數:所選策略具有使用者定義的變數時可用名稱空間的可編輯文本框
- 計畫詳細信息：此部分用於選擇各種計畫引數，如開始和結束日期/時間、定期模式等。
- 資產:用於選擇資產組以標識要運行合規性的裝置清單的部分
- 計畫:切換為啟用或禁用按計畫運行作業（一次性或重複）；如果禁用，作業將立即執行
- 處於活動狀態:指示所選計畫是否處於活動狀態

## 建立合規性作業

## 建立合規性作業2

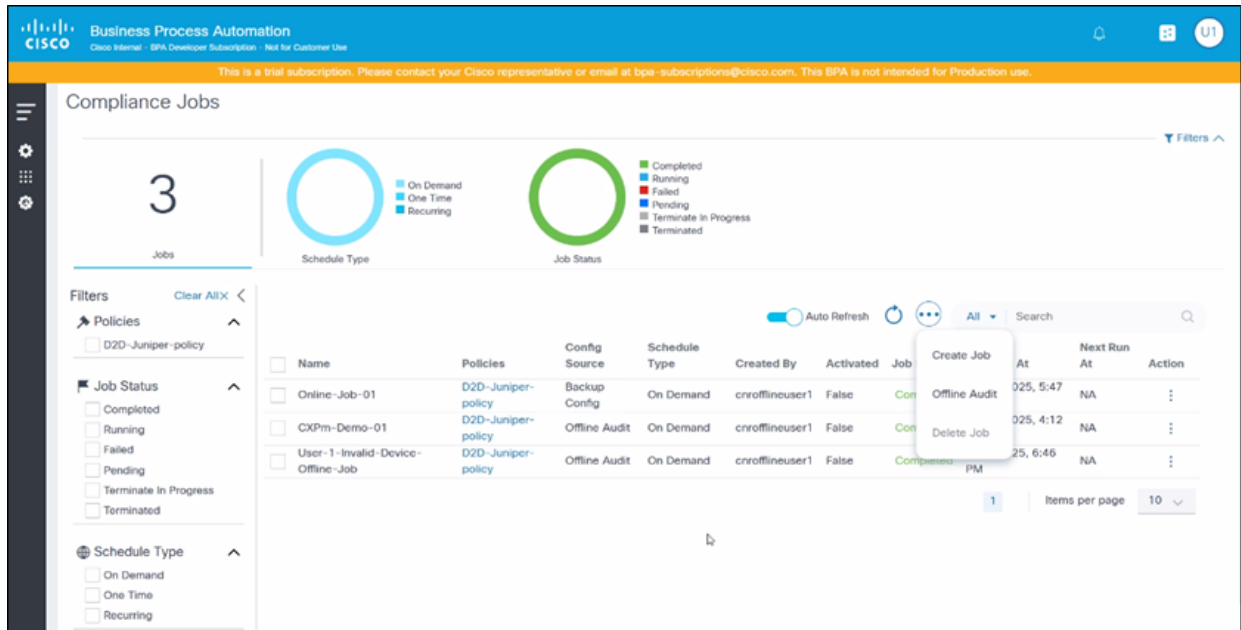
## 建立離線稽核作業

Compliance Jobs中的Offline Audit功能允許使用者對裝置配置執行合規性檢查，而無需將裝置安裝到BPA中。使用者可以手動將裝置配置上傳為檔案。可以將多個裝置配置壓縮並以zip檔案的形式上傳在一起。上載後，將解析這些配置檔案，並且可以使用這些檔案內容作為源建立合規性作業。然後，離線稽核的結果會與聯機稽核結果一起顯示在遵循性控制面板中。

Offline Audit頁包括以下屬性：

- 名稱:作業的名稱
- 說明:可選說明
- 策略名稱:用於選擇要運行的策略的下拉選單，可能按為登入使用者配置的訪問策略進行過濾
- 產品系列:用於選擇產品系列的下拉選單

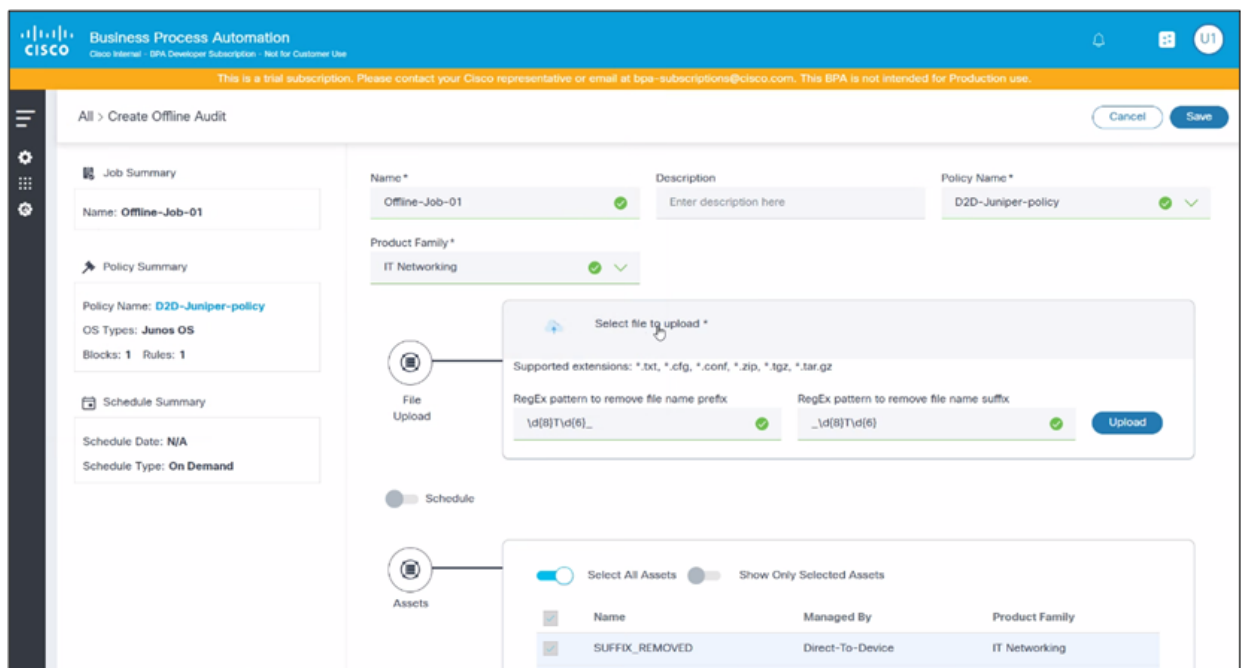
- 檔案上傳:使用離線稽核功能手動上傳組態檔；這是通過上傳介面完成的，您可以在該介面中選擇本地系統中的檔案
- 計畫:切換以啟用計畫
- 資產:按上載的檔案內容顯示裝置清單



選擇離線稽核

要建立離線稽核作業，請執行以下操作：

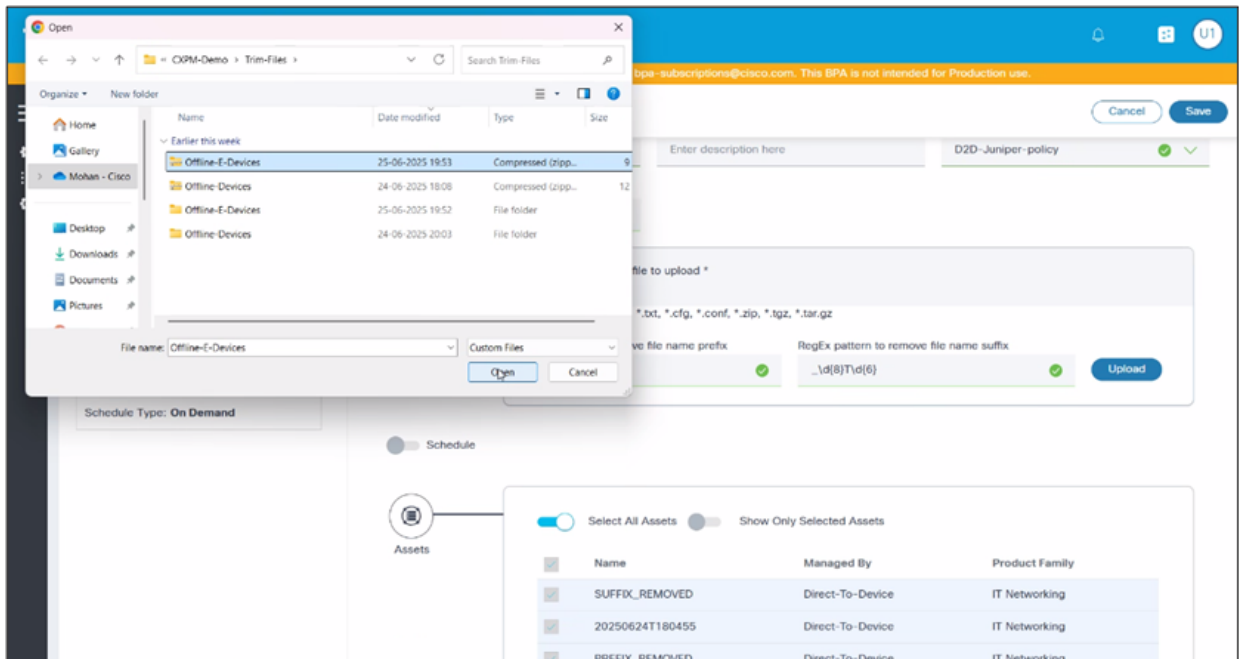
1. 從More Options圖示中選擇Offline Audit。



上傳檔案

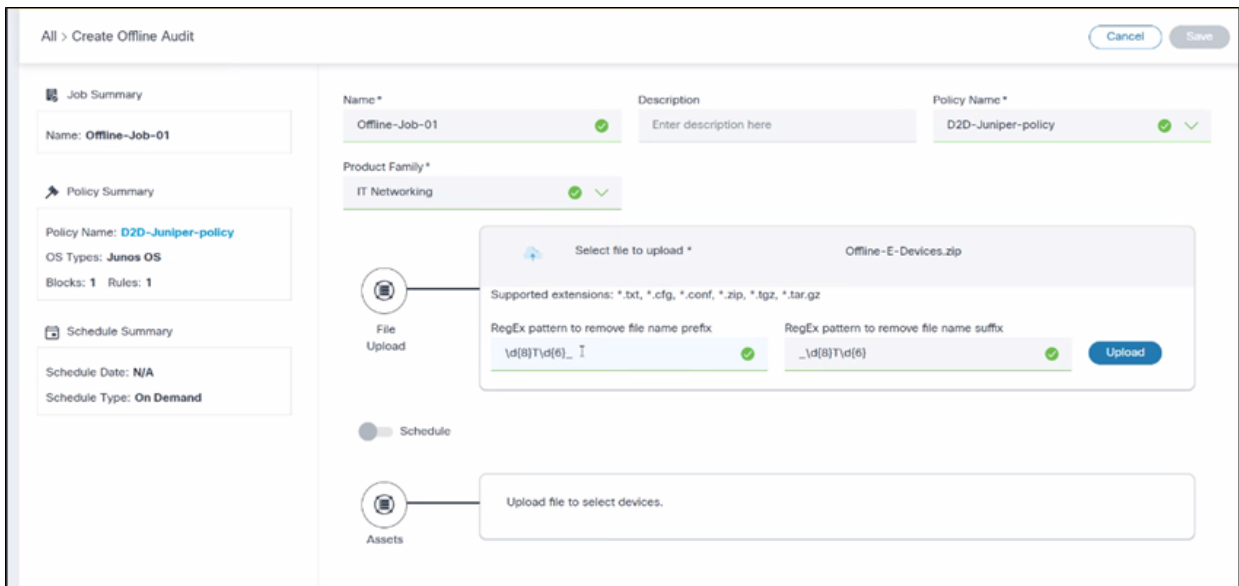
2. 按一下「Select file」以上傳組態檔。

 附註：支援的檔案型別包括(.txt、.cfg、.conf、.zip、.tgz、.tar.gz)。



案頭檔案

3. 如果配置檔案是在資料夾或存檔檔案中壓縮的，請在上傳之前解壓縮這些檔案。



Regex模式

4. 應用Regex模式進行檔名修整（可選）。

 附註：使用字首或字尾修剪模式(regex)來標準化或簡化上傳的檔名，以便更輕鬆地進行處理



All > Create Offline Audit

Policy Name: **D2D-Juniper-policy**  
OS Types: Junos OS  
Blocks: 1 Rules: 1

Schedule Summary  
Schedule Date: N/A  
Schedule Type: On Demand

File Upload

Select file to upload \*

Supported extensions: \*.txt, \*.cfg, \*.conf, \*.zip, \*.tgz, \*.tar.gz

RegEx pattern to remove file name prefix:  ☒  
RegEx pattern to remove file name suffix:  ☒

Upload

Schedule

Assets

Select All Assets ☒ Show Only Selected Assets ☐

| Name            | Managed By       | Product Family |
|-----------------|------------------|----------------|
| SUFFIX_REMOVED  | Direct-To-Device | IT Networking  |
| 20250624T180455 | Direct-To-Device | IT Networking  |
| PREFIX_REMOVED  | Direct-To-Device | IT Networking  |

1 Items per page 10

上傳檔案

5. 按一下「Upload」。系統會顯示確認消息，指示檔案已儲存在資料庫中並且已成功上載。

All > Edit Offline Audit

Job Summary  
Name: **Offline-Job-01**

Policy Summary  
Policy Name: **D2D-Juniper-policy**  
OS Types: Junos OS  
Blocks: 1 Rules: 1

Schedule Summary  
Schedule Date: N/A  
Schedule Type: On Demand

Name \*  Description  Policy Name \* **D2D-Juniper-policy**

Product Family \* **IT Networking**

File Upload

Select file to upload \*

Supported extensions: \*.txt, \*.cfg, \*.conf, \*.zip, \*.tgz, \*.tar.gz

RegEx pattern to remove file name prefix:   
RegEx pattern to remove file name suffix:

Upload

Schedule

Assets

Select All Assets ☒ Show Only Selected Assets ☐

| Name           | Managed By       | Product Family |
|----------------|------------------|----------------|
| SUFFIX_REMOVED | Direct-To-Device | IT Networking  |

儲存離線稽核

6. 按一下儲存以建立離線稽核作業。

## 編輯符合性作業

要編輯合規性作業，請按照[建立合規性作業](#)中提供的步驟操作。

附註：作業名稱不可編輯。

**CISCO Business Process Automation**  
Cisco Internal - BPA Developer Subscription - Not for Customer Use

This is a trial subscription. Please contact your Cisco representative or email at bpa-subscriptions@cisco.com. This BPA is not intended for Production use.

All > Edit Compliance Job

**Job Summary**  
Name: RemCompJob  
Config Source: Current Config  
Asset Group: assetgroup-38

**Policy Summary**  
Policy Name: RemPolicy  
OS Types: IOS, IOS-XR, NX-OS  
Blocks: 1 Rules: 1

**Schedule Summary**  
Schedule Date: Monday, January 13, 2025, 5:47 PM  
Schedule Type: Recurring

Name: RemCompJob Description: RemCompJobDescription Policy Name: RemPolicy

Device Config Source: Current Config Commands: show running-config +

☒ Schedule ☒ Activate

**Schedule Details**  
Effective on: Monday, 13 Jan 2025 17:47  
Start Time: 17:47

**Schedule recurrence**  
Recurrence Pattern: Cron Pattern  
Cron Pattern: Minutes (0-59): 0 Hour (0-23): 2 Days of Month (1-31): \* Month (1-12): \* Days of Week (1-7): \*  
End Date: 01/15/2025

**Assets**  
Asset Group: assetgroup-38

| Name       | Ip Address | Location | Managed By |
|------------|------------|----------|------------|
| bnr-asr-38 |            |          | NSO-166    |

1 Items per page 10

編輯符合性作業

立即運行或重新運行合規性作業

**CISCO Business Process Automation**  
Cisco Internal - BPA Developer Subscription - Not for Customer Use

This is a trial subscription. Please contact your Cisco representative or email at bpa-subscriptions@cisco.com. This BPA is not intended for Production use.

Compliance Jobs

218 Jobs

**Filters**  
Policies: Demo Ethernet Policy, Notice-policy, Vlan Policy, Policy refd RT, D2D-ns-compliance-policy, Policy 1  
Job Status: Completed, Running, Failed, Pending, Remediate In Progress, Terminated  
Schedule Type: On Demand, One Time, Recurring

| Name                   | Policies                          | Config Source  | Schedule Type | Created By | Activated | Job Status | Last Run At           | Next Run At | Action               |
|------------------------|-----------------------------------|----------------|---------------|------------|-----------|------------|-----------------------|-------------|----------------------|
| defaultpolicy-check    | Default Policy - Compliance Check | Current Config | On Demand     | admin      | False     | Completed  | Aug 5, 2025, 4:20 PM  | NA          |                      |
| mock-test              | Default Policy - Compliance Check | Current Config | On Demand     | admin      | False     | Completed  | Aug 5, 2025, 5:18 PM  | NA          |                      |
| Validate CNG           | cnc gigabit                       | Current Config | On Demand     | admin      | False     | Completed  | Aug 5, 2025, 1:33 PM  | NA          |                      |
| d2d-job-cloned         | D2D-Rem-policy-cloned             | Current Config | On Demand     | admin      | False     | Completed  | Aug 4, 2025, 1:17 PM  |             | Edit                 |
| OnR-Issue-01           | Default Policy - Compliance Check | Current Config | On Demand     | admin      | False     | Completed  | Aug 4, 2025, 1:17 PM  |             | Delete               |
| History-Validate-02    | Default Policy - Compliance Check | Backup Config  | On Demand     | admin      | False     | Completed  | Aug 4, 2025, 11:32 AM |             | Run Now              |
| new-d2d-job            | Remediation-df-policy             | Current Config | On Demand     | admin      | False     | Completed  | Aug 4, 2025, 11:33 AM |             | Run on Non-Compliant |
| test-offline-policy-01 | cnc gigabit                       | Offline Audit  | On Demand     | admin      | False     | Completed  | Aug 4, 2025, 11:33 AM |             | History              |
| d2d-offline-job        | Remediation-df-policy             | Offline Audit  | On Demand     | admin      | False     | 8%         | Aug 1, 2025, 5:01 PM  |             |                      |
| History-Validate       | Default Policy - Compliance Check | Current Config | On Demand     | admin      | False     | 0%         | Aug 1, 2025, 11:34 AM |             |                      |

1 2 3 ... 22 Next Items per page 10

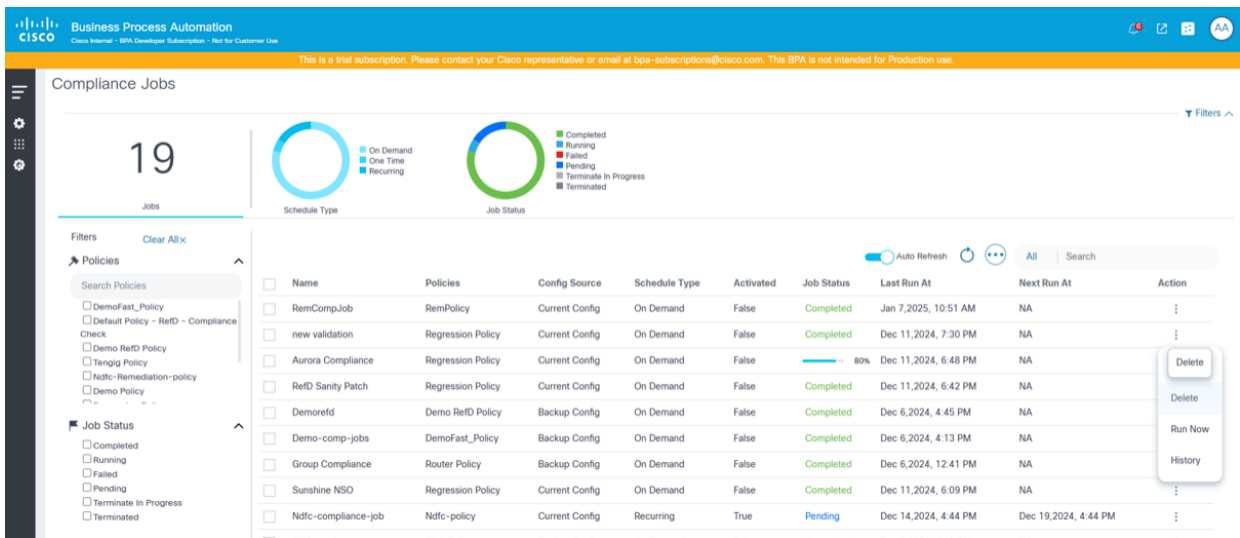
合規性作業 — 立即運行並在不合規時運行

Compliance Jobs網格可通過從「更多選項」圖示中選擇「立即運行」來按需運行作業。如果作業已執行，則使用者可以從更多選項圖示中選擇Run on Non-Compliant。此操作僅在上次執行中未標籤為「完全合規」的資產清單上運行符合性作業。

## 刪除符合性作業

如果使用者具有正確的基於角色的訪問控制(RBAC)角色，則門戶會提供刪除一個或多個合規性作業的選項。在執行過程中無法刪除作業。使用者可以選擇刪除單個或多個符合性作業。

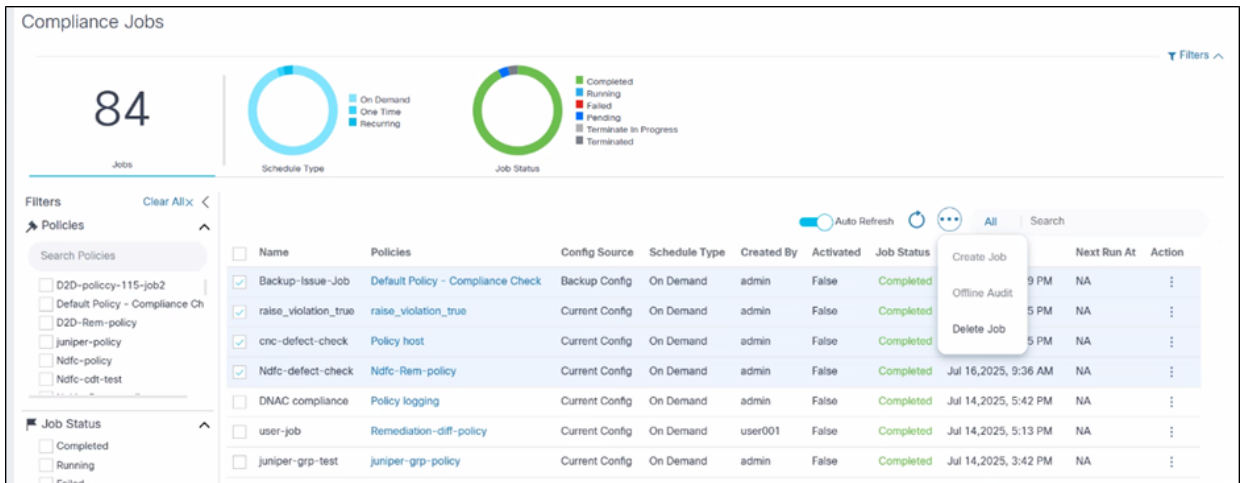
要刪除符合性作業，請執行以下操作：



### 刪除單個符合性作業

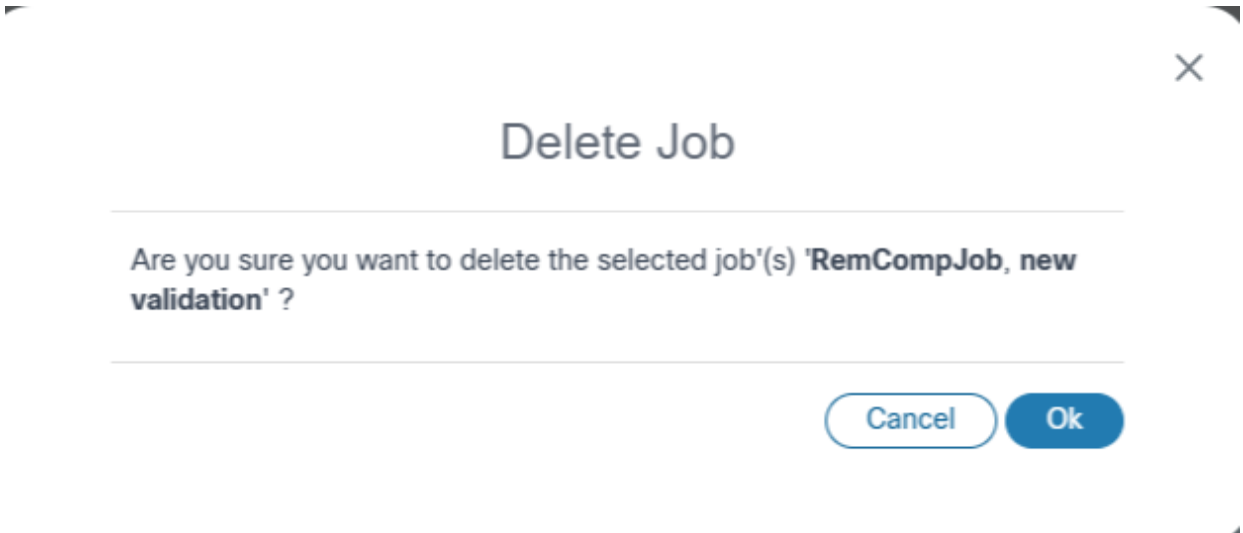
1. 在符合性作業頁中，選擇要刪除的作業上的更多選項圖示> 刪除。

或



### 刪除多個符合性作業

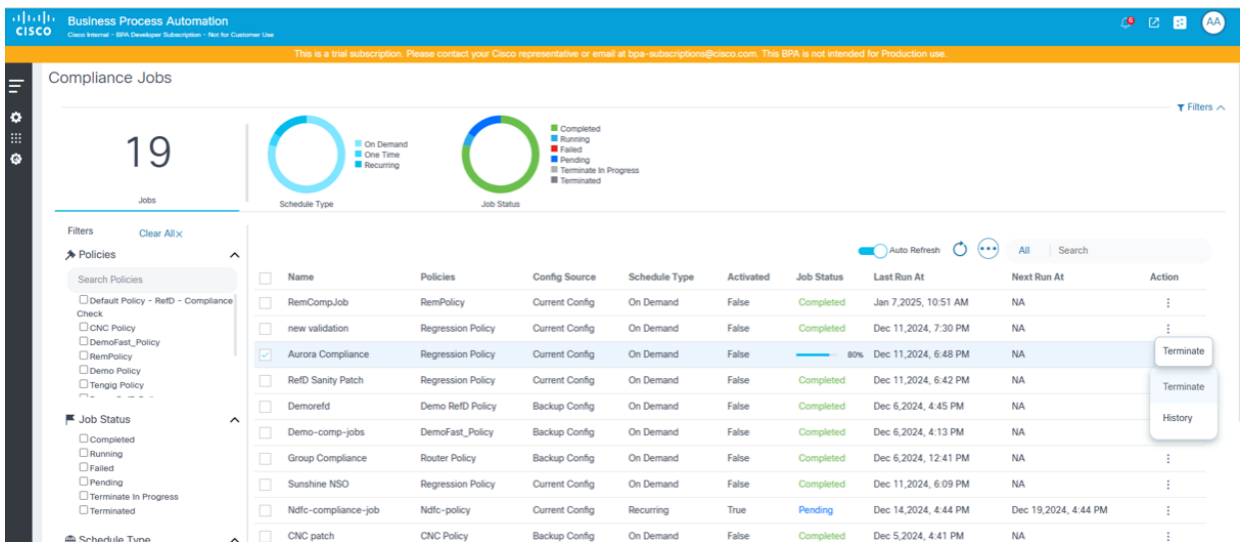
要刪除多個符合性作業，請選中要刪除的作業的覈取方塊，然後選擇更多選項> 刪除作業。系統會顯示確認。



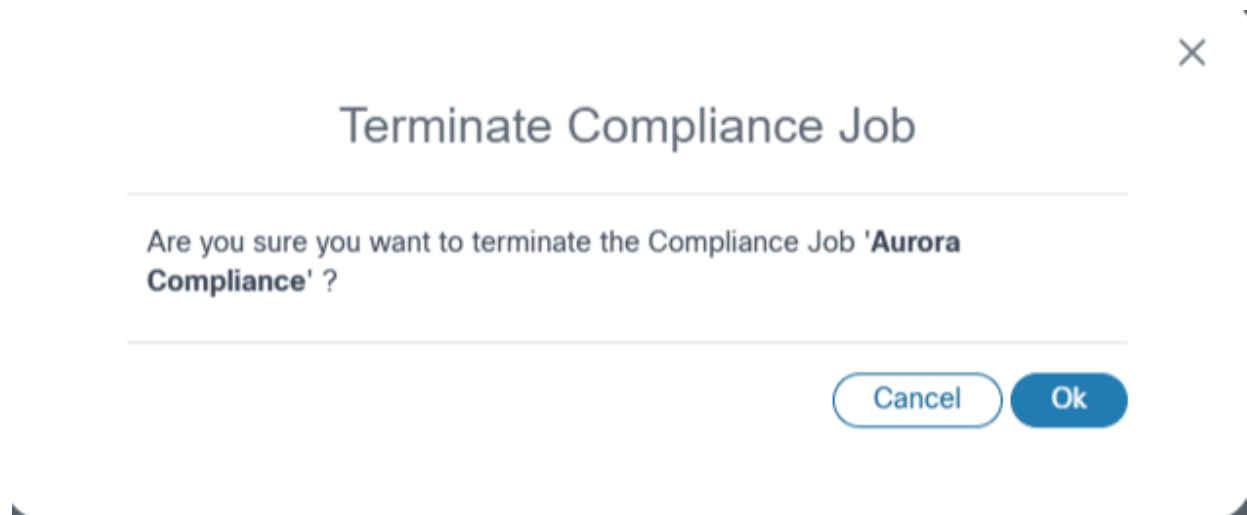
刪除符合性作業確認

終止合規性作業

門戶為使用者提供終止給定作業的運行執行的選項。當作業終止時，當前運行的裝置會完成它們的執行，並取消所有進一步排隊等候的裝置執行。



終止合規性作業



終止合規性作業確認

## 合規性作業歷史記錄

「符合性作業」中的「歷史記錄」選項顯示按排程日期範圍篩選的選定作業的執行清單。

要檢視符合性作業的歷史記錄，請從符合性作業頁中選擇更多選項圖示>歷史記錄。系統隨即會顯示 History 頁面。

Compliance Jobs

7 Jobs

Schedule Type: On Demand, One Time, Recurring

Job Status: Completed, Running, Failed, Pending, Terminate In Progress, Terminated

Filters: Clear All X

- Policies
  - ☐ NDFCTEST
  - ☐ Nso166-policy
- Job Status
  - ☐ Completed
  - ☐ Running
  - ☐ Failed
  - ☐ Pending
  - ☐ Terminate In Progress
  - ☐ Terminated
- Schedule Type
  - ☐ On Demand
  - ☐ One Time
  - ☐ Recurring

| Name                                         | Policies      | Config Source  | Schedule Type | Activated | Job Status | Last Run At          | Next Run At           | Action |
|----------------------------------------------|---------------|----------------|---------------|-----------|------------|----------------------|-----------------------|--------|
| <input type="checkbox"/> Nso-cron-job        | Nso166-policy | Backup Config  | Recurring     | True      | Pending    | Sep 6, 2024, 8:54 PM | Sep 13, 2024, 8:54 PM | ⋮      |
| <input type="checkbox"/> Ndfc-weekly-job     | NDFCTEST      | Current Config | Recurring     | True      | Pending    | Sep 6, 2024, 8:56 PM | Sep 9, 2024, 8:56 PM  | ⋮      |
| <input type="checkbox"/> NDFC-onetime-job    | NDFCTEST      | Backup Config  | One Time      | True      | Completed  | Sep 6, 2024, 8:42 PM | NA                    | ⋮      |
| <input type="checkbox"/> Nso-scheduled-job   | Nso166-policy | Current Config | Recurring     | True      | Pending    | Sep 7, 2024, 8:40 PM | Sep 13, 2024, 8:40 PM | ⋮      |
| <input type="checkbox"/> ndfc-scheduled-job  | NDFCTEST      | Current Config | One Time      | True      | Completed  | Sep 6, 2024, 8:40 PM | NA                    | ⋮      |
| <input type="checkbox"/> nso-compliance-job  | Nso166-policy | Current Config | On Demand     | False     | Completed  | Sep 6, 2024, 8:30 PM | NA                    | ⋮      |
| <input type="checkbox"/> Ndfc-compliance-job | NDFCTEST      | Backup Config  | On Demand     | False     | Completed  | Sep 6, 2024, 8:27 PM | NA                    | ⋮      |

Auto Refresh: ☐ ⌂ ⋮ All Search

1 Items per page 10

Context Menu: Edit, Delete, Run Now, History

合規性作業歷史記錄

History - refdjob

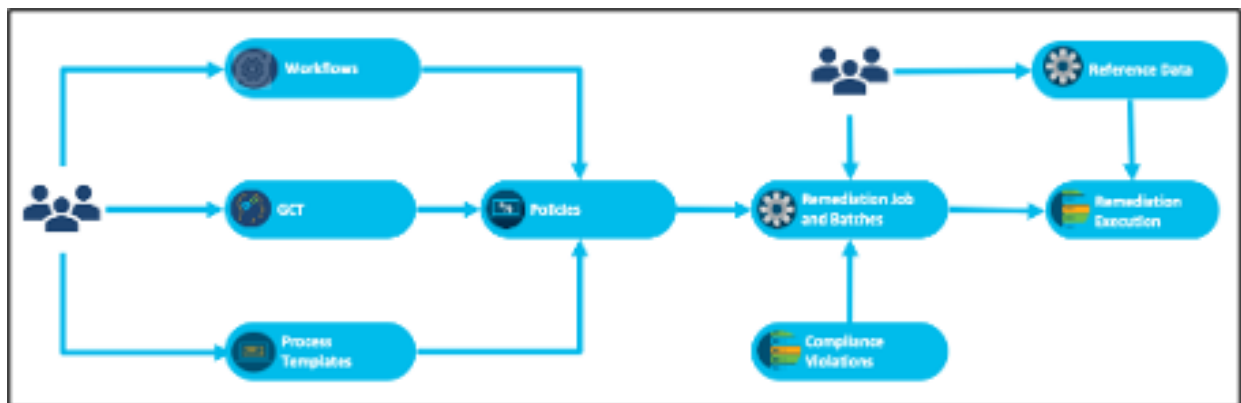
| Execution Id             | Start Date             | End Date               | Status    | Total Devices | Execution Summary                                          | Compliance Summary                                                             | Action |
|--------------------------|------------------------|------------------------|-----------|---------------|------------------------------------------------------------|--------------------------------------------------------------------------------|--------|
| 66e91344aac4a1f186281b3  | Sep 17, 2024, 10:57 AM | Sep 17, 2024, 10:57 AM | Completed | 4             | Queued: 0, Running: 0, Failed: 0, Skipped: 0, Completed: 4 | Compliant: 0, Unknown: 0, Info: 0, Warning: 0, Minor: 0, Major: 0, Critical: 4 | ⋮      |
| 66e83eed92f96fb87d07d56  | Sep 16, 2024, 7:51 PM  | Sep 16, 2024, 7:51 PM  | Completed | 4             | Queued: 0, Running: 0, Failed: 0, Skipped: 0, Completed: 4 | Compliant: 0, Unknown: 0, Info: 0, Warning: 0, Minor: 0, Major: 0, Critical: 4 | ⋮      |
| 66e83835bbe304a13c8cd440 | Sep 16, 2024, 7:22 PM  | Sep 16, 2024, 7:22 PM  | Completed | 4             | Queued: 0, Running: 0, Failed: 4, Skipped: 0, Completed: 0 | Compliant: 0, Unknown: 4, Info: 0, Warning: 0, Minor: 0, Major: 0, Critical: 0 | ⋮      |
| 66e7fdc33e378abeab71b7fc | Sep 16, 2024, 3:13 PM  | Sep 16, 2024, 3:13 PM  | Completed | 4             | Queued: 0, Running: 0, Failed: 0, Skipped: 0, Completed: 4 | Compliant: 0, Unknown: 0, Info: 0, Warning: 0, Minor: 0, Major: 0, Critical: 4 | ⋮      |

「歷史記錄」頁

## 補救作業

通過補救框架，操作員可以補救合規性控制面板上列出的合規性違規。此框架使用工作流、GCT和流程模板。

### 配置補救流程圖



配置補救概述

配置補救使用情形使操作員能夠使用補救作業修復裝置上的配置違規。首先使用相應的工作流程、GCT模板和每個控制器型別的流程模板配置合規性策略。針對受影響的資產清單為策略運行補救作業。在補救期間，可從各種資料來源獲取要應用於裝置的值，包括合規性執行結果、RefD應用程式和現有裝置配置。可以根據客戶的特定要求自定義工作流程，以便在補救過程中執行其他步驟。

補救功能最重要的步驟說明如下：

## GCT模板

GCT是BPA核心功能，用於使用特定於控制器的模板在裝置上應用配置更改。

- 建立更新裝置配置的GCT模板，解決合規性違規
- 如果GCT模板中的變數符合以下語法，則框架支援自動變數對映：
  - 對於單裝置配置塊：`<>_<>`。範例：`management_interface_ipv4_addr`，`management_interface_ipv4_subnet`
  - 為未來的版本規劃了多個裝置配置塊
- 如果「Block Identifier Name」和「Variable Name from block」包含空格，應將這些空格替換為下劃線(「\_」) ( 例如，如果「Block Identifier Name」為「Management Interface」且「Variable Name」為「IPV4\_ADDR」，則GCT中的變數名稱應為「Management\_Interface\_IPV4\_ADDR」。) )
- 使用者可以檢查合規性裝置執行中的「gctVars」輸出，以檢視GCT變數的語法和對映是否正確；要獲取合規性裝置執行，請使用以下REST API:
  - 獲取執行以查詢執行ID
    - URL：`/api/v1.0/compliance-remediation/compliance-executions`
    - 方法：GET
  - 使用執行ID獲取裝置執行
    - URL：`https://<>/bpa/api/v1.0/compliance-remediation/compliance-device-executions?executionId=<>`
    - 方法：GET

Params ● Authorization Headers (8) Body Pre-request Script Tests Settings

#### Query Params

|                                     | KEY         | VALUE                    |
|-------------------------------------|-------------|--------------------------|
| <input checked="" type="checkbox"/> | executionId | 66dfc32a2b855fb425602d4a |
|                                     | Key         | Value                    |

ody Cookies Headers (11) Test Results

Pretty

Raw

Preview

Visualize

JSON

≡

```
115     "minor": 0,  
116     "major": 5,  
117     "critical": 0  
118   },  
119   "gctVars": {  
120     "Interface_Gigabit_3_inteface": "0/0/3",  
121     "Interface_Gigabit_3_description": "blocks severity",  
122     "Interface_Gigabit_3_ip_addr": "10.10.10.1",  
123     "Interface_Gigabit_3_ip_subnet": "10.10.10.0/24"  
124   },  
125   "overAllStatus": "partial-compliant",  
126   "severitySummary": {  
127     "major": 5,  
128     "info": 1,  
129     "critical": 0
```

#### GCT變數 — gctVars

- 要從塊中檢索變數，請使用以下REST API:
  - URL : <https://<>/bpa/api/v1.0/compliance-remediation/utils/schema>
  - 方法 : POST
  - 本文 : {"blockName":"<<塊名>" }
- 通過將模板應用於裝置以進行乾運行和提交，驗證GCT模板
- 在合規性策略中配置上述GCT模板

## 工作流程

Remediation框架提供以下開箱即用的參考工作流：

- 補救流程:此工作流程具有補救執行中涉及的通用步驟集。
- 補救子流程:此工作流程包含變數分配、GCT乾運行和GCT提交任務，其他團隊可根據要求自

定義這些任務。

這兩種工作流程均可根據客戶需求原樣使用、更新或更換。

## 流程模板

可以根據策略配置流程模板和分析模板，以運行預檢查和後檢查並比較輸出。

## 政策

CnR策略將每個裝置型別的工作流、GCT模板和處理模板拼合在一起，這些模板可用於使用作業修復配置。

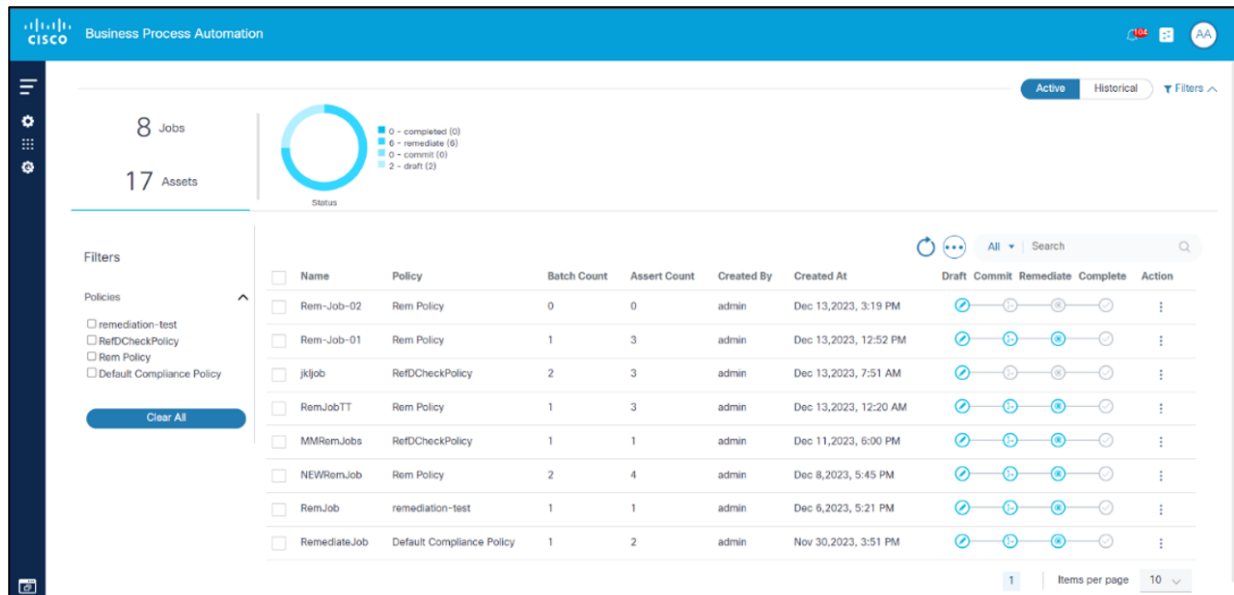
## 補救作業

補救作業幫助操作員對受影響的資產的選定清單應用補救策略。可以按需或按計畫執行補救作業。在運行時，補救工作流程可以從多種來源提取資料，包括裝置詳細資訊、合規性執行詳細資訊和RefD框架。

## 補救作業清單

使用者可以按如下方式篩選、排序和檢視在控制面板中建立的補救作業：

- 作業:顯示建立的作業總數
- 資產:顯示已建立的總資產
- 狀態:按狀態顯示作業
- 活動和歷史:根據所選內容顯示活動或歷史（非活動）作業
- 策略:按策略過濾補救作業
- 主網格:顯示預設作業清單，可通過按一下標題進行排序，並包括按名稱和策略進行搜尋以及分頁
- 動作:當作業處於草稿狀態或完成狀態時，可以存檔或刪除作業；無法存檔或刪除正在運行的作業

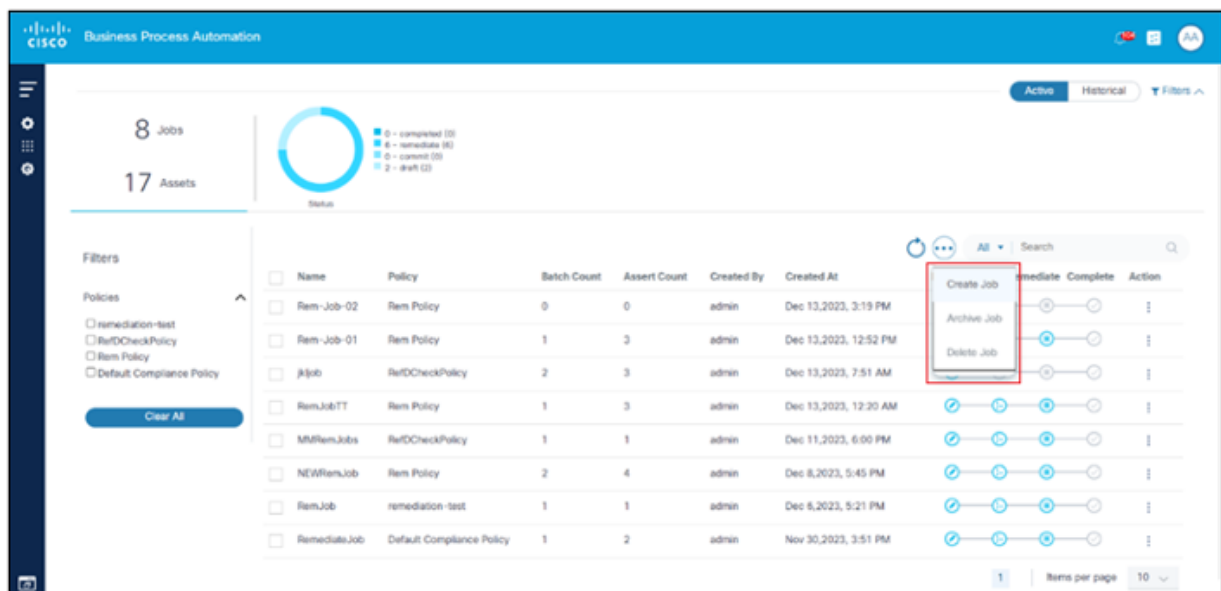


## 補救作業清單

## 建立和編輯補救作業

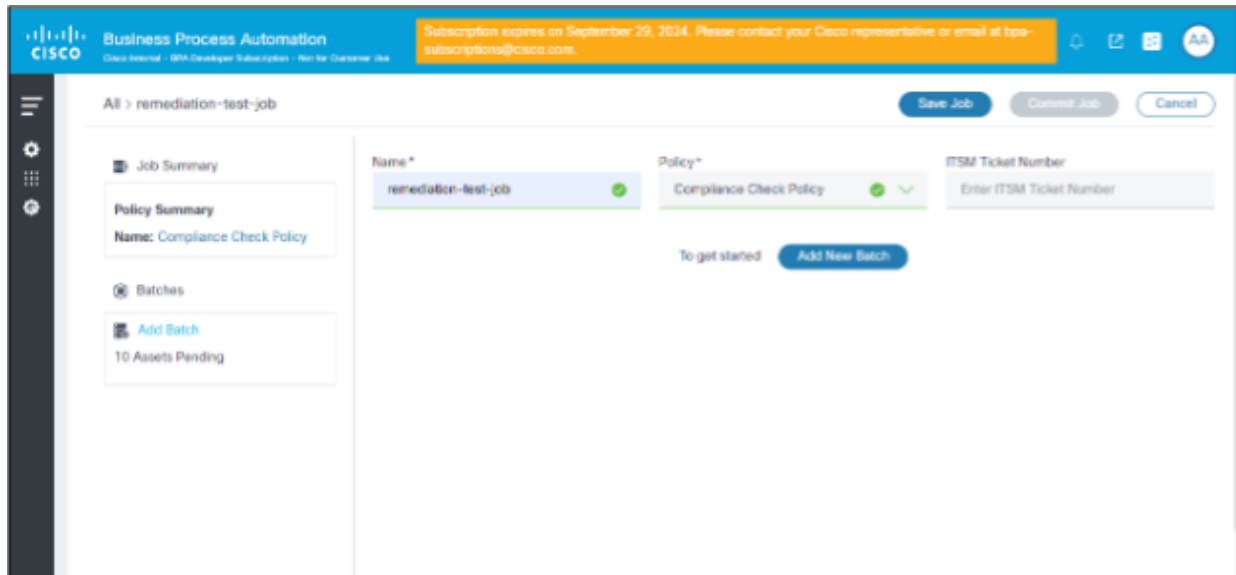
補救作業是從作業清單頁建立的，可以通過執行以下步驟建立：

1. 選擇更多選項圖示> 建立作業。將顯示建立作業頁。



## 補救作業選項

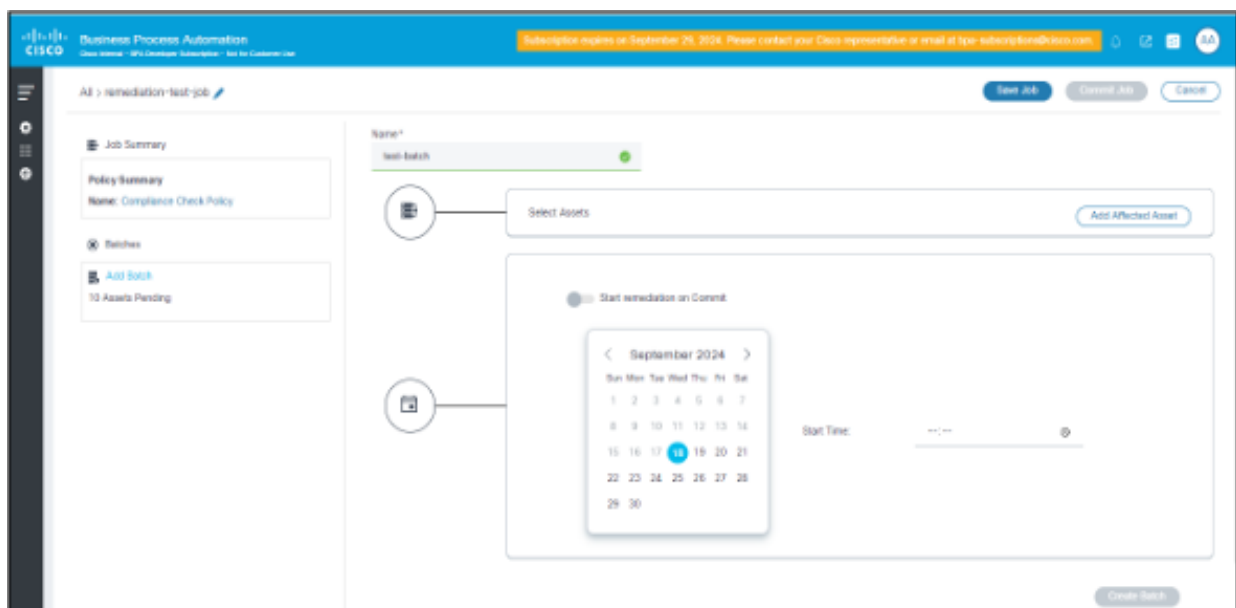
2. 完成或編輯詳細資訊。



補救作業：詳細資料

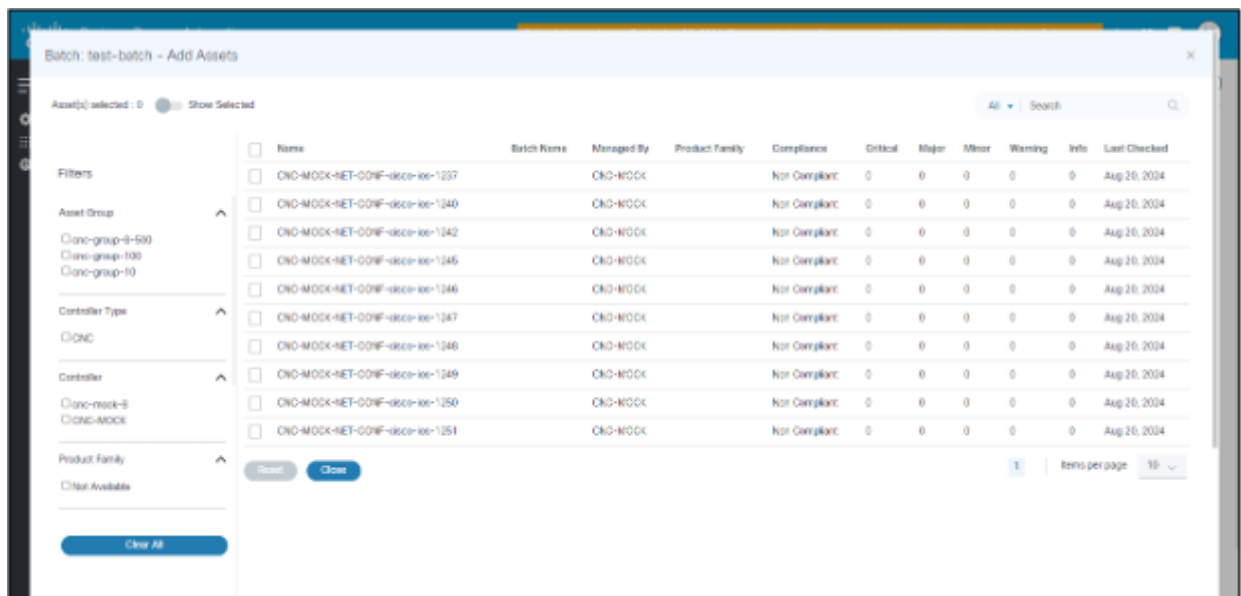
3. 按一下Save Job。

要從「建立作業」頁向作業新增批，請執行以下操作：



補救作業：新增批次

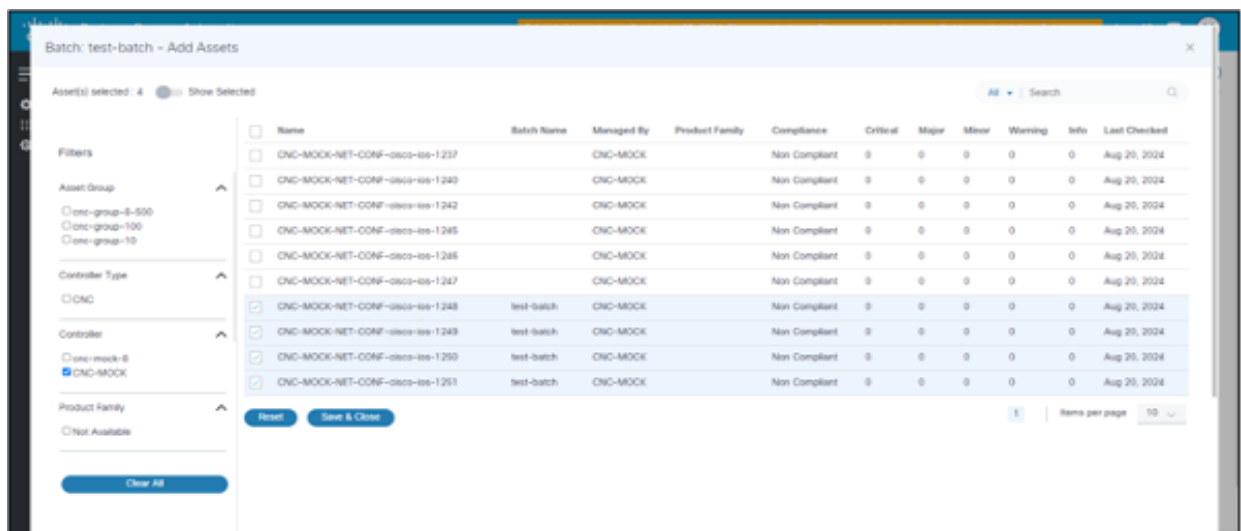
1. 按一下「Add New Batch」。
2. 輸入名稱、受影響的資產詳細資訊和計畫詳細資訊。
3. 按一下Add Affected Assets。
4. 在「Assets Details」頁中，選擇受影響的資產清單，然後按一下Save Job。
5. 根據Controller Type、Controller、Asset Group和Product Family篩選資產。
6. 選擇資產後，按一下儲存並關閉，返回上一頁。



補救作業：新增受影響的資產



附註：使用者可以選擇在「受影響的資產」頁中應用過濾器



補救作業：新增受影響的篩選器

一旦新增了受影響的資產，則可以在儲存時或在計畫的將來時間運行一次批處理。



附註：要以 On Demand 形式運行作業，請啟用 Start remediation on Commit 切換。如果使用者選擇此選項，則不需要日期和時間。如果使用者選擇 One-Time 選項，則必須提供執行作業的日期和時間。

單個修正作業有多個批處理。可以在提交時或在計畫的日期和時間啟動每個批處理。

提交後補救批處理可以按需運行或按計畫運行。

Business Process Automation  
Cisco Internal - BPA Developer Subscription - Not for Customer Use  
This is a trial subscription. Please contact your Cisco representative or email at bpa-subscriptions@cisco.com. This BPA is not intended for Production use.

All > demo

Save Job Commit Job Cancel

Job Summary

Policy Summary  
Name: RemPolicy

Batches  
Add Batch  
1 Assets Pending

Name\*  
demo

Total Asset(s) : 1

| Name       | Managed By | Compliance          | Critical | Major | Minor | Warning | Last Checked |
|------------|------------|---------------------|----------|-------|-------|---------|--------------|
| bnr-asr-38 | NSO-166    | Partially Compliant | 0        | 1     | 0     | 1       | Jan 7, 2025  |

1 Items per page 10

Start remediation on Commit

January 2025

Start Time: --:--

補救作業：按需

Business Process Automation  
Cisco Internal - BPA Developer Subscription - Not for Customer Use  
This is a trial subscription. Please contact your Cisco representative or email at bpa-subscriptions@cisco.com. This BPA is not intended for Production use.

All > demo

Save Job Commit Job Cancel

Job Summary

Policy Summary  
Name: RemPolicy

Batches  
Add Batch  
1 Assets Pending

Name\*  
demo

Total Asset(s) : 1

| Name       | Managed By | Compliance          | Critical | Major | Minor | Warning | Last Checked |
|------------|------------|---------------------|----------|-------|-------|---------|--------------|
| bnr-asr-38 | NSO-166    | Partially Compliant | 0        | 1     | 0     | 1       | Jan 7, 2025  |

1 Items per page 10

Start remediation on Commit

January 2025

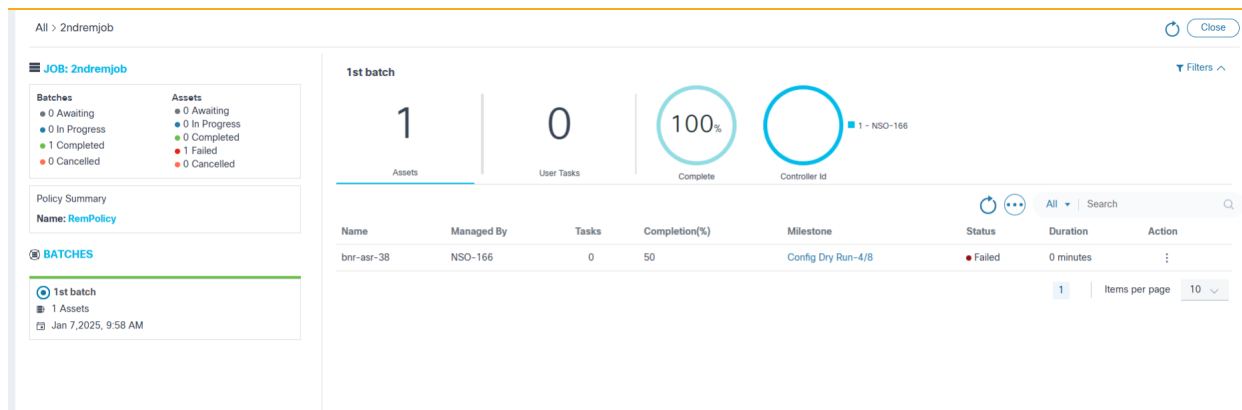
Start Time: 19:00

補救作業：一次/計畫

## 補救執行：裝置清單

提交補救作業後，將觸發執行操作，該作業的狀態將顯示在「補救作業」下的List Devices頁中。使用者可以按控制器ID、名稱、管理者和產品系列套用篩選條件。

- 作業:顯示批和資產的狀態詳細資訊以及選擇運行補救作業的策略的名稱
- 批處理:顯示作為當前補救作業一部分的批處理清單
- 自動刷新:顯示以下選項：如果作業處於運行狀態，則每隔30秒自動刷新頁面；刷新頁面；或顯示取消以返回上一頁
- 批層詳細資訊:顯示批層彙總詳細資訊，包括總資產數量、使用者任務數量、完成百分比和控制器詳細資訊
- 資產網格:顯示資產網格檢視，包括每個資產的使用者任務、完成百分比和當前里程碑



補救執行：裝置清單

補救執行：內聯使用者任務詳細資訊

在裝置清單中，Tasks列指示使用者是否有任何要執行的任務。

要檢視內聯使用者任務詳細資訊，請執行以下操作：

1. 選擇任務計數。將開啟使用者任務清單視窗。
2. 選擇一個任務。將開啟使用者任務詳細資訊視窗。

可以從內聯執行以下操作：

- 完成
- 重試
- 取消

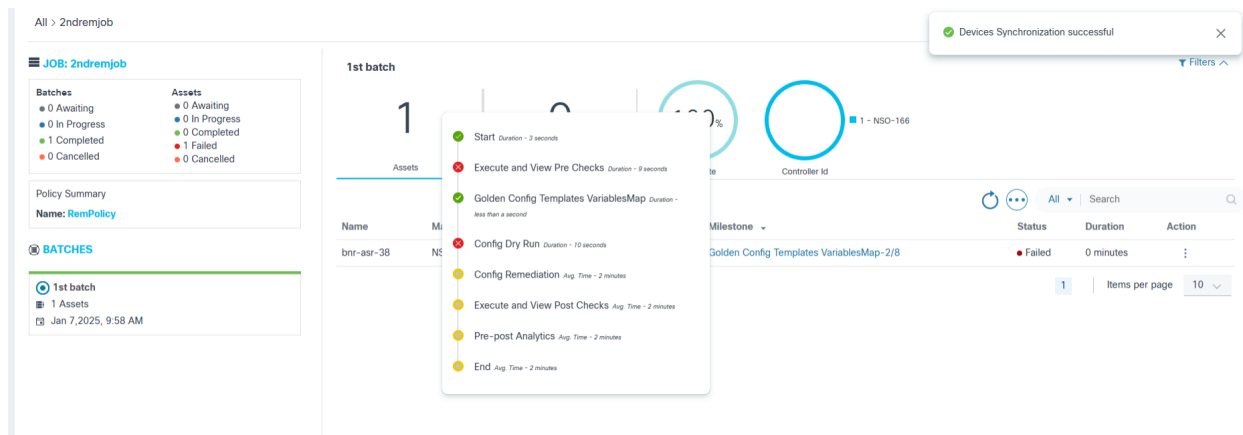
補救執行：內嵌里程碑詳細資訊

在裝置清單中，Milestone列指示與給定裝置的補救相關的當前里程碑。

要檢視內聯里程碑詳細資訊，請選擇該列。將開啟「里程碑詳細資訊」(Milestone Details)視窗。

以下狀態可用於里程碑：

- 未啟動
- running
- Completed
- 失敗



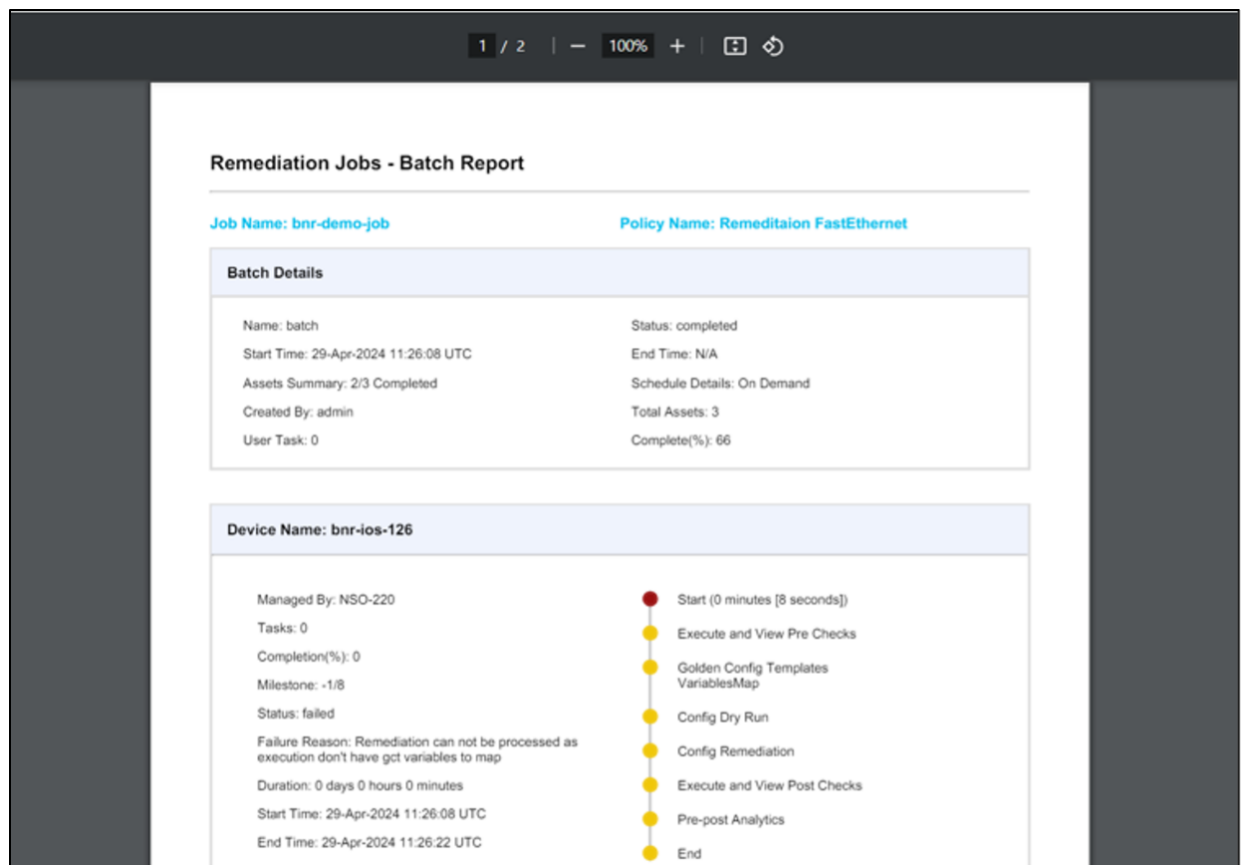
補救執行：內嵌里程碑詳細資訊

補救執行：生成和下載批處理摘要PDF報告

可以生成和下載批次摘要。

要以每批PDF格式下載摘要報告，請執行以下操作：

1. 選擇更多選項圖示> 生成報告。系統在內部檢查報告是否準備就緒。報告就緒後，將啟用 Download Report選項。
2. 選擇More Options圖示> Download Report。PDF下載。



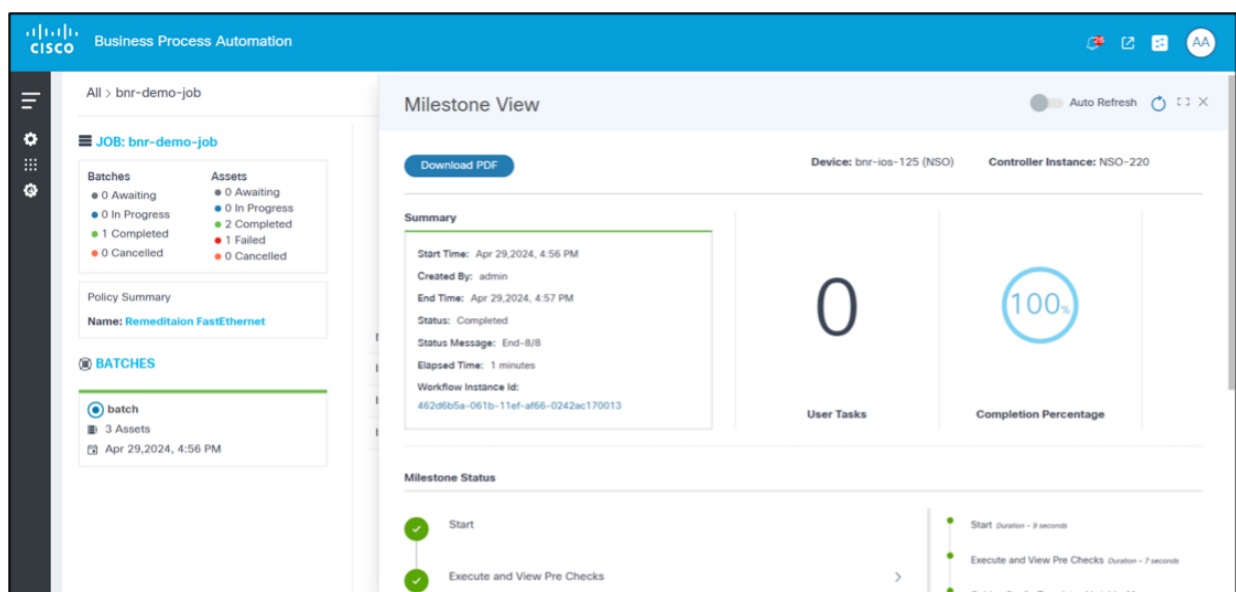
批次摘要報告PDF

「補救作業批處理報表」包含「批處理詳細資訊」部分，該部分提供補救批處理的摘要，例如作業名稱、批處理名稱、開始和結束時間、總資產以及整體狀態。然後是「裝置詳細資訊」部分（每個裝置一個部分），其中包括裝置名稱、裝置特定補救狀態、時間表、持續時間和里程碑清單以及狀態。

## 補救執行：裝置詳細資訊

要檢視里程碑的裝置詳細資訊，請選擇Device Details頁面。系統隨即會顯示「里程碑檢視」頁面。

顯示給定裝置的補救摘要，其中包含詳細的里程碑狀態，包括已完成關鍵里程碑的命令輸出。例如，可以檢視process template命令輸出、GCT乾運行輸出和分析差異輸出內容。



## 補救執行：里程碑檢視

## 補救執行：裝置詳細資訊 — 里程碑報告

要檢視里程碑報表，請執行以下操作：

1. 選擇Device Details頁。系統隨即會顯示「里程碑檢視」頁面。
2. 按一下「Download PDF」。系統將生成並下載里程碑檢視報告，如下所示。

此報告為所選裝置補救提供了更詳細的里程碑詳情和相應內容。

## Milestones

|                                                                                                                  |                             |                              |                                      |
|------------------------------------------------------------------------------------------------------------------|-----------------------------|------------------------------|--------------------------------------|
| <b>Start</b>                                                                                                     |                             |                              |                                      |
| 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) |
| <b>Execute and View Pre Checks</b>                                                                               |                             |                              |                                      |
| 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                           |
| dir harddisk: location all   include free                                                                        |                             | Commands Evaluation Result : | Fail                                 |
| 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 |                             | Rules Evaluation Result :    | Pass                                 |
| #Rule :                                                                                                          | 1                           | Operation :                  | Contains                             |
| Rule :                                                                                                           | Invalid input detected      | Result :                     | Pass                                 |

補救執行：裝置詳細資訊 — 里程碑檢視PDF報告

## 組態:塊和規則

### 塊的功能

配置塊是在網路管理系統中建立和強制執行合規性策略的基本元素。它們代表裝置CLI配置，如介面、路由器邊界網關協定(BGP)等配置。以下是配置塊的主要功能：

- 模組化:配置塊允許模組化策略建立，使管理員能夠獨立定義和管理裝置配置的離散部分。這種模組化簡化了更新和維護合規性策略的過程。
- 粒度:通過將裝置配置拆分為更小、更易於管理的部分，管理員可以執行準確的合規性檢查並強制執行特定標準。這可確保裝置配置的每個部分都遵循所需的策略。
- 可重用性：定義後，配置塊可在多個合規性策略和裝置上重複使用。這種可重用性減少了冗餘並確保了配置管理的一致性。
- 靜態配置塊:靜態配置塊表示不帶任何變數的原始裝置配置。

範例：以下塊可用於對TwentyFigE0/0/0/31介面運行合規性檢查

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

- **動態配置塊:**動態配置塊表示包括變數在內的裝置配置，這些變數允許更靈活且可重複使用。這些塊功能與TTP模板類似，應用於裝置配置並獲取變數的值。可以將條件新增到規則以驗證這些變數。有關TTP的詳細資訊，請參閱<https://ttp.readthedocs.io/en/latest/Overview.html>。

範例：以下塊可用於對所有TwentyFiveGigE介面運行合規性檢查

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

**具有子層次結構的動態配置塊:**此塊功能類似於動態配置塊，用於從具有多個層次的裝置配置中檢索值。

範例：以下示例演示了裝置配置，以及用於從分層結構中檢索值的相應動態塊。

**具有分層結構的裝置配置：**

```
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
```

動態塊配置用於分析上述配置。

```
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
```

## 規則的功能

規則允許使用者定義條件以根據配置塊中存在的變數進行驗證。作為執行的一部分，遵從性引擎會分析裝置配置，查詢裝置塊例項的匹配例項，從行中讀取值，並根據這些值運行規則中定義的條件。結果（無論配置行是否有違規）將儲存以在儀表板中顯示。

現在，配置規則是塊建立生命週期的一部分。因此，沒有單獨的頁面可檢視規則。規則可以在相應的塊建立或更新頁面下列出、建立和更新。

在CnR框架中，規則在根據指定條件驗證配置方面有著關鍵作用。本節概述如何在系統中整合和管理規則。

- 目的:規則允許使用者定義用於驗證配置塊中存在的變數的條件
- 執行流程:
  - 合規引擎解析裝置配置
  - 標識裝置塊例項的匹配例項
  - 從配置行提取值
  - 將規則中定義的條件應用於這些值
  - 指示違規的結果將儲存並顯示在儀表板中

### 與Block生命週期整合

- 生命週期整合：現在，配置規則對於資料塊建立生命週期是不可或缺的
- 管理:
  - 在用於塊建立或更新的頁面中直接列出、建立和更新規則
  - 沒有專用於檢視規則的單獨頁面，從而簡化了它們在資料塊生命週期中的管理

這種整合可確保將合規性檢查無縫地納入配置管理流程，從而能夠根據預定義規則有效地監控和管理裝置配置。

## 清單塊

Blocks頁面列出所有配置塊，並提供用於生成、新增、編輯、刪除、匯入和匯出塊的操作。使用者可以篩選、排序和檢視阻止詳細資訊。

### 功能塊的詳細資訊

- 總計數:顯示已建立的塊總數
- 過濾器選項：

- 作業系統型別和裝置系列:允許使用者根據所選條件篩選塊
- 主網格:
  - 顯示預設塊清單
  - 使用者可以通過按一下列標題對清單進行排序
  - 包括一個搜尋功能，允許使用者按所有屬性或特別按塊名稱進行搜尋
  - 支援分頁，以便瀏覽清單
- 動作:
  - 編輯:使用者可以修改現有塊
  - 刪除:使用者可以從清單中刪除塊

3558

Filters: Clear All x

OS Type

- ☐ FX-OS
- ☐ NX-OS,IOS-XR
- ☐ Junos EOS
- ☐ Arista EOS
- ☐ IOS-XR
- ☐ NX-OS
- ☐ IOS
- ☐ NewOSType-Test

Device Family

Search Device Family

- ☐ IE 2000 Series
- ☐ IE 4000 Series
- ☐ Cisco Firepower Threat Defense

| Block Name                                              | Config Block                                          | OS Type            | Device Family                                                                                     | Created By | Config Type | Block Type | TTP Template | Action |
|---------------------------------------------------------|-------------------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------|------------|-------------|------------|--------------|--------|
| <input type="checkbox"/> Block-bnr-asr-38-ruleduplicate | interface GigabitEthernet0 vrf forwarding Mgmt-in ... | IOS                | Catalyst 1000 series,IE 2000 Series,IE 4000 Series                                                | admin      | Dynamic     | Manual     | No           | :      |
| <input type="checkbox"/> New-Block-TickMark             | interface {[INT_ID]} Description tickmark             | IOS                | Catalyst 1000 series,IE 2000 Series,IE 4000 Series                                                | admin      | Dynamic     | Manual     | No           | :      |
| <input type="checkbox"/> Block-New-Test                 | interface {[INT_ID]} Description Newnames             | NewOSType-Test,IOS | NewDevicefamily-Test2,IE 2000 Series                                                              | admin      | Dynamic     | Manual     | No           | :      |
| <input type="checkbox"/> Block-Loopback interface       | interface Loopback{[ INTF_ID ]} description {[ DE ... | IOS,NX-OS,IOS-XR   | Catalyst 1000 series,IE 2000 Series,IE 4000 Series,NCS 5500 Series,NCS 5700 Series,Nexus Switches | admin      | Dynamic     | Manual     | No           | :      |
| <input type="checkbox"/> CDT-Block                      | interface TenGigE{[interface]} description ...        | IOS-XR             | NCS 5500 Series                                                                                   | admin      | Dynamic     | Manual     | Yes          | :      |
| <input type="checkbox"/> Optus banner                   | banner login ^ *****                                  | IOS,IOS-XR,NX-OS   | Catalyst 1000 series,IE 2000 Series,IE 4000 Series,NCS 5500 Series,NCS 5700 Series,Nexus Switches | admin      | Static      | Manual     | No           | :      |

## 配置塊清單

## 新增或編輯塊和規則

Add或Edit Block頁用於捕獲和管理有關塊的基本資訊。本頁概述了以下部分：

- 基本塊詳細資訊:

Basic Details部分包括：

- 塊名稱:塊的指定名稱
- 說明:塊的用途或功能的簡要概述或說明
- 作業系統類型：與塊關聯的作業系統型別
- 裝置系列:與該塊相容的裝置類別或組
- 塊識別符號選擇:用於為塊選擇唯一識別符號的選項
- 新增或編輯塊識別符號詳細資訊:如果沒有合適的塊識別符號，使用者可以使用相同的欄位新增或編輯以下塊識別符號詳細資訊：
  - 塊識別符號名稱:為塊識別符號指定的特定名稱
  - 模式:塊識別符號遵循的模式或格式
  - 多重:切換以指示是否將配置塊視為多行配置

**Cisco Business Process Automation**  
Cisco Internal | BPA Developer Subscription | Not for Customer Use  
This is a trial subscription. Please contact your Cisco representative or email at bpa-subscriptions@cisco.com. This BPA is not intended for Production use.

All > Edit Block

**Block Details**

Enter Block Details

Block Name \*  
Block: bsr-ssr-38-ruleduplicate

OS Type \*  
IOS

Device Family \*  
3 selected

Block Identifier \*  
Interface GigabitEthernet

Block Identifier Pattern \*  
\*{N}interface GigabitEthernet

Block Description

Block Details

Block Config

Block Rules

Rules

Cancel Submit

## 新增或編輯塊 — 塊詳細資訊

- Block Config:

Block Config部分包括：

- Config Block: 表示包含不同變數的裝置配置。此配置概述了如何在系統中設定和管理裝置。
- TTP模板: 指示是否將該塊指定為模板轉換協定(TTP)模板，從而幫助確定用作跨裝置轉換或標準化配置的模板的塊。

All > Edit Block

**Block Details**

Enter Block Details

Block Name \*  
Enter Block Name

OS Type \*  
3 selected

Device Family \*  
Nexus Switches

Block Identifier \*  
Select / Create Block Identifier

Block Description

Block Details

Block Config

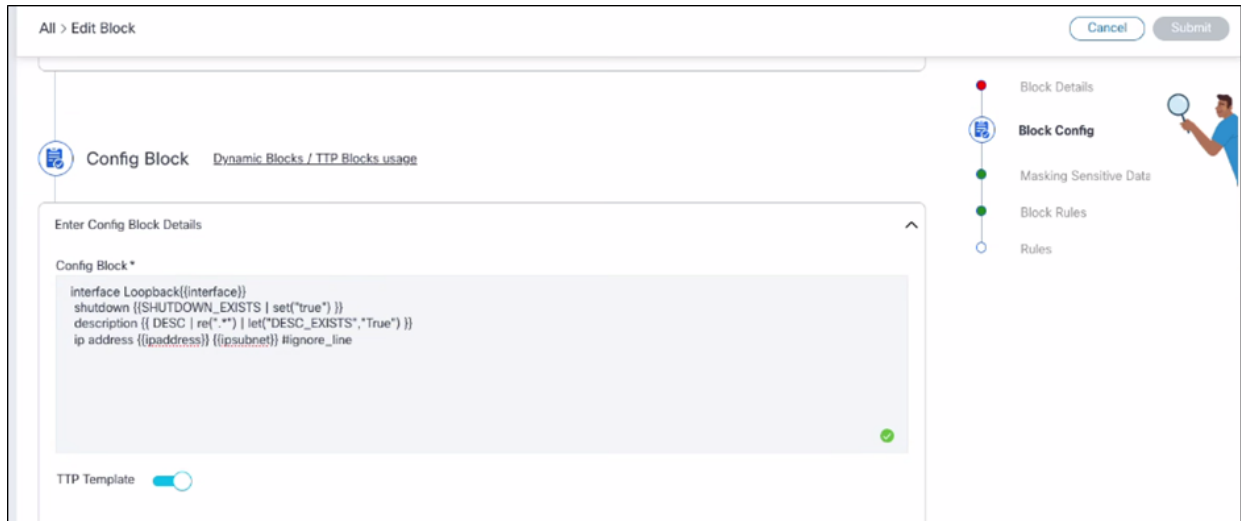
Masking Sensitive Data

Block Rules

Rules

Cancel Submit

## 阻止詳細資訊



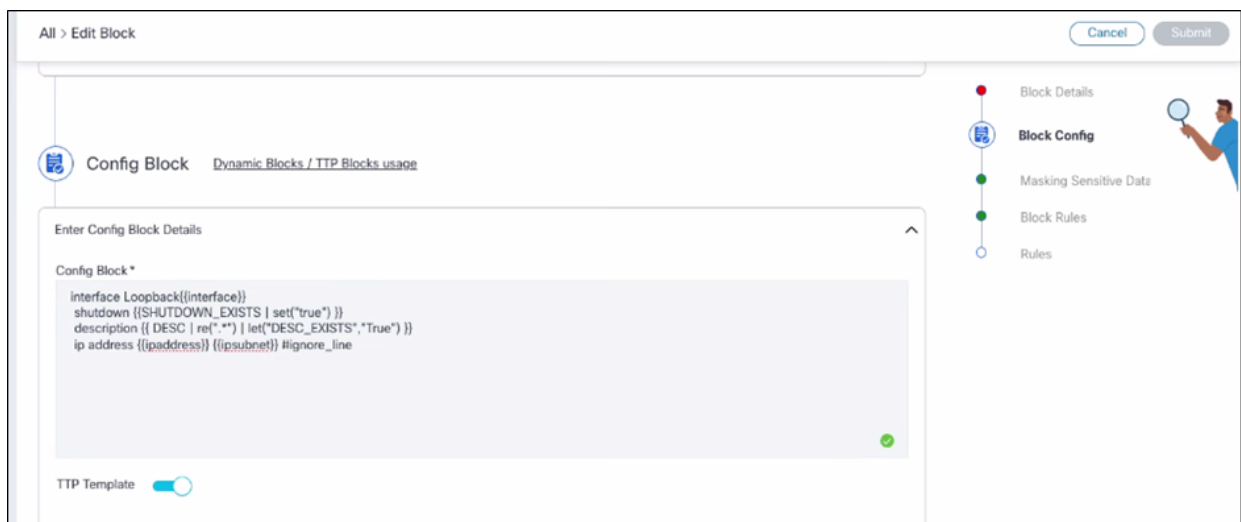
## 阻止配置

## 使用忽略行語法

Ignore Line Syntax 允許使用者在塊中特定配置行的末尾新增註釋，以指示系統跳過該行上的任何合規性檢查或違規。這可以防止該線在報表或儀表板中顯示為違規。

完成以下步驟以使用 Ignore Line 語法：

1. 找到要從合規性檢查中排除的配置行（如ip地址）。



## 忽略線路語法

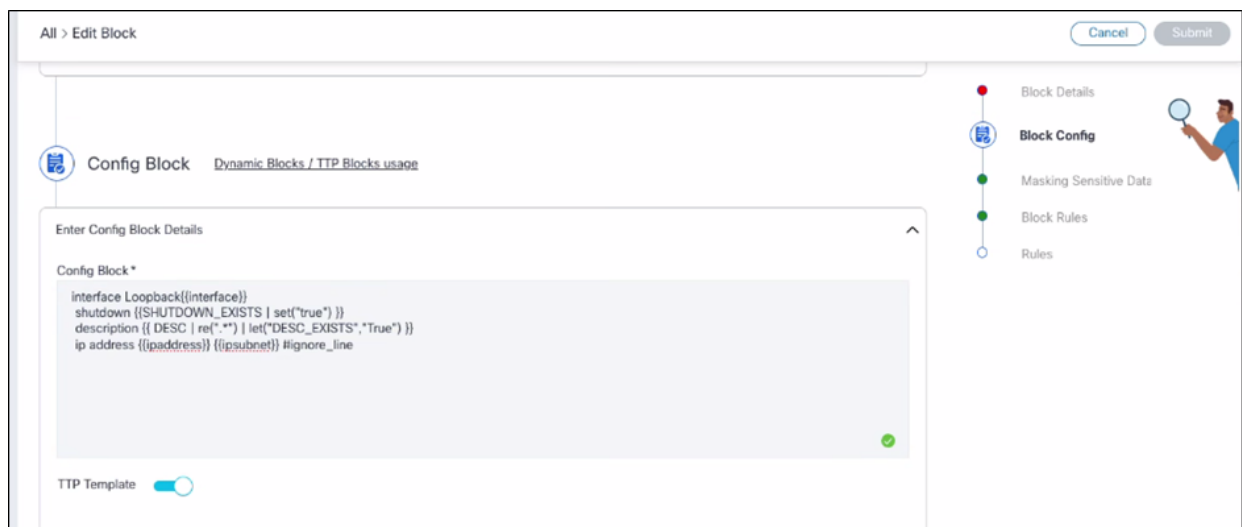
2. 在該行的末尾使用註釋語法「#ignore\_line」追加該行。範例：ip address {{ipAddress}} {{ipSubnet}} #ignore\_line

## 引發違規

塊配置中的此模板文本解析器(TTP)功能可用於指示如果存在特定行，是否應該引發衝突。

完成以下步驟以使用TTP功能：

1. 在block create or edit頁的Block Config部分中，找到要控制的配置行。
2. 使用set或let命令定義TTP變數，如下所示：
  - 如果存在配置行關閉，請使用set命令定義變數，如下所示：  
關機 | {{SHUTDOWN\_FLAG | set("true")}}
  - 如果使用者在配置行中有現有變數（如說明{{DESC}}），請使用let命令，如下所示：  
說明{{ DESC | re(".\*") | let("DESC\_EXISTS", "True")}}
3. 在規則中使用這些變數（上述示例中的SHUTDOWN\_FLAG或DESC\_EXISTS）可引發違規。



引發違規

效果:

如果「shutdown」或「description config」行在裝置配置中可用，則違規將顯示在儀表板頁面上。違規的嚴重性取決於建立規則時所做的選擇。

- 遮蔽敏感資料:

遮蔽敏感資料是一項功能，允許使用者使用正規表示式定義模式，以標識和遮蔽裝置配置中的敏感資訊（如密碼或金鑰）。這通過用指定的掩碼(例如「\*\*\*」)替換匹配的資料，防止敏感資料在違規檢視或補救配置差異中顯示。

要遮蔽敏感資料，請完成以下步驟：

1. 在掩碼敏感資料部分中：
  - 新增多個正規表示式(regex)模式以識別敏感資料

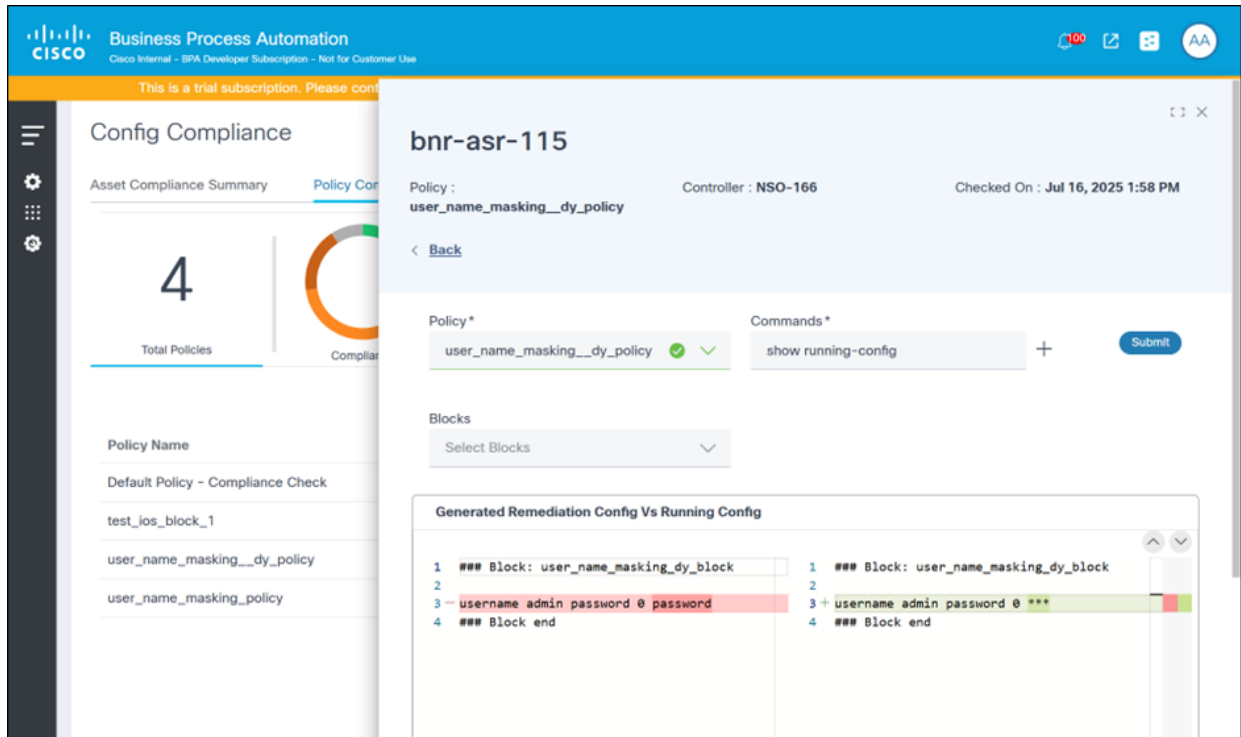
- 指定替換字串以遮罩匹配的資料(例如,「」)。例如,Regex模式可以用密碼填充(以匹配任何以「password」開頭、後跟一個字的文本),並且替換應該是。
2. 根據需要新增任意多的regex模式;它們以網格格式顯示

遮蔽敏感資料

3. 從清單中刪除不再需要的任何模式。
4. 系統使用正規表示式查詢匹配的敏感裝置配置資料,並將其替換為指定的掩碼(例如「\*\*\*」)。
- 此掩碼用於以下頁面:
- 合規性控制面板>受影響的資產>查看違規頁面:UI中顯示的配置資料,以及根據這些違規詳細資訊生成的資產合規性報告

「遮罩檢視違例中的敏感資料」頁

- Compliance dashboard > View Remediation Config > View Remediation Diff頁:裝置配置資料根據塊的掩碼設定顯示被遮蔽的敏感資料



在補救差異頁中遮蔽敏感資料

- 阻止規則 ( 嚴重性選擇 ) :

Block Rules部分包括 :

- 強制配置順序:確保在符合性檢查期間,配置行以正確的順序顯示。符合性引擎根據預期訂單檢查配置行的順序。
- 嚴重性選擇:允許使用者為塊內的違規指定嚴重性級別。嚴重性級別有助於有效地確定合規性問題的優先順序並對其進行管理。
- 組態順序不相符:確定配置行的順序差異,並在裝置配置行的順序與預期順序不匹配時發出警報。
- 缺少配置:
  - 檢測缺少的配置行
  - 突出顯示裝置配置中缺少的預期配置行
  - 檢查整個裝置配置塊是否缺失或與定義的塊配置不匹配
- Additional Config:
  - 標識意外的配置行
  - 顯示裝置配置中存在但根據塊配置不需要的配置行
- 跳過的塊:
  - 指示未檢查的配置塊
  - 如果塊不符合指定的過濾條件,則會跳過該塊

All > Edit Block Cancel Submit

**Block Rules**

Enter Block Rules Details

Enforce Config Order ☒

| Severity Selection           | Critical                         | Major                 | Minor                 | Warning                          | Info                             | Compliant                        |   |
|------------------------------|----------------------------------|-----------------------|-----------------------|----------------------------------|----------------------------------|----------------------------------|---|
| Configuration Order Mismatch | <input type="radio"/>            | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            | ✓ |
| Missing Config               | <input type="radio"/>            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/>            | <input type="radio"/>            | <input checked="" type="radio"/> | ✓ |
| Additional Config            | <input type="radio"/>            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/>            | ✓ |
| Missing Blocks               | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | ✓ |
| Skipped Blocks               | <input type="radio"/>            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/>            | ✓ |

Block Details  
Block Config  
Masking Sensitive Da  
**Block Rules**  
Rules

## 新增或編輯塊塊規則

## 規則管理

在CnR框架中，使用者可以通過「新增或編輯塊」介面管理塊規則。此功能的結構如下節所示：

 附註：如果使用者不想引發特定塊級違規，可以選擇嚴重性級別「Compliant」。

- 規則配置：
  - 使用者可以設定和管理合規性引擎用於驗證配置的規則
  - 使用者可以根據需要建立、編輯或刪除規則
- 規則清單：
  - 提供所有已建立規則的完整清單，提供其詳細資訊的檢視
  - 使用者可以編輯現有規則或刪除不再需要的規則

All > Edit Block Cancel Submit

Skipped Blocks ☒ ☐ ☐ ☐ ☐ ☐ ☒

**Rules**

Enter Rules Details Add Rule

 **Default Rule - Router ISIS** ✎ 🗑

Violations :

Violation 1

Violation 2

 **Default RefD Rule - Router ISIS** ✎ 🗑

Violations :

Violation 1

Violation 2

Block Details  
Block Config  
Block Rules  
**Rules**

## 新增和編輯配置塊

## 新增或編輯規則詳細資訊

- 規則名稱:
  - 為規則分配唯一名稱以便標識
  - 此欄位是必填欄位，以確保可以清楚地識別每個規則
- 預設規則:
  - 指定是否應將規則設定為預設規則
  - 使用者可以啟用此設定以使規則成為符合性框架中的預設值
- 說明:
  - 提供有關規則的其他上下文或資訊
  - 此欄位為可選欄位，但有助於說明文檔和清晰度
- 違規:
  - 管理與該規則關聯的違規清單
  - 使用者可以根據需要新增、編輯或刪除違規

|   | 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        | NSQ-166          | cisco Nexus9000 C9300v Chassis                       | Partially Compliant | 12       | 0     | 0     | 0       | 3    | 0       | 05-Aug-25    |
| 9 |                   |                  |                                                      |                     |          |       |       |         |      |         |              |

新增或編輯Blocks規則：新增或編輯規則

## 新增或編輯規則違規

規則違規是遵從性執行中的一個關鍵元件，詳細說明了需要執行的特定檢查。以下是如何建立和管理規則違規的概述：

- 基本模式:
  - 使用者介面元素:此模式允許使用者使用圖形使用者介面(GUI)建立規則違規。此方法通常更易於使用，且便於那些不願意參與編碼工作的使用者使用。
  - 逐步指導:指導使用者使用預定義的UI元素定義檢查的過程。
- 進階模式:
  - 類似JSON的代碼格式:對於對編碼感到滿意的使用者，此模式允許通過以結構化、類似JSON的格式鍵入規則來建立規則違規。
  - 靈活性和精度:此方法為定義複雜的規則檢查提供了更大的靈活性和精確度。

**Edit Violation**

Violation Name\*  
Violation 1

Severity\*  
Critical

Violation Message  
Enter violation message

Basic ☒ Advance

Filter **1**  
isis = 'CORE' x Add Filter

Condition **1**  
loopback\_int (Group) x Add Condition

Filter  
Add Filter

Condition  
prefix\_sid = '33' x Add Condition

## 建立或編輯規則違規 — 基本模式

**Config Compliance**

Asset Compliance Summary Policy Compliance Summary Reports

79 Devices Analyzed

Filters

- Product Family
  - Cisco Nexus9000 C9300v Chassis
  - Cisco ISE
  - Cisco Catalyst 9302-CL Wireless Controller
  - Juniper Junos
  - E 2000 Series
  - Not Available
- Asset Group
  - dnac-check
  - Not Available
  - SD-WAN
  - SD-WAN
  - SD-WAN-Asset
- Asset Type
  - Online
  - Offline

Policy: Remediation-df-policy

Controller: Direct-To-Device

Checked On: Aug 04, 2025 11:33 AM

Filters

- Policy
  - Remediation-df-policy (7)
  - Default Policy - Compliance Check (3)
  - SD-WAN-policy-check (2)
  - SD-WAN-policy (2)
- Blocks
  - Interface-gigabitE-Block
  - TenGigE-Block
  - Authentication-Block
  - aaa-group-Block
  - services-Block
  - Enable Password-Block

Block: Interface-gigabitE-Block

- Interface GigabitEthernet0/0/0
- negotiation auto
- vrf forwarding Mgmt-intf
- shutdown
- Interface GigabitEthernet0/0/1
- negotiation auto
- vrf forwarding Mgmt-intf
- shutdown
- Interface GigabitEthernet0/0/2
- negotiation auto
- vrf forwarding Mgmt-intf
- shutdown
- Interface GigabitEthernet0/0/3
- negotiation auto
- vrf forwarding Mgmt-intf
- shutdown
- Interface GigabitEthernet0/0/4
- ip address 1.2.3.3 32
- negotiation auto
- vrf forwarding Mgmt-intf
- shutdown

Block: TenGigE-Block

- Interface TenGigabitEthernet0/0/0
- no ip address

## 建立或編輯規則違規 — 高級模式

規則違規包含以下部分：

- 違規名稱: 違規的名稱
- 嚴重性: 定義在執行期間此違規失敗時的遵循性嚴重性
- 違規消息: 當違規檢查失敗時，將顯示該消息
- 違規過濾器條件: 應用可以使用非組架構變數的違規條件
  - 在篩選條件中用於根據不屬於組的各個資料元素設定條件
  - 使使用者能夠根據資料的層次結構和結構選擇標準，確保精確和相關過濾
- 規則條件: 可以使用組和非組架構變數在此檢查符合性的實際條件
  - 這兩種型別的變數都用於規則中，以建立全面的條件
  - 組變數: 允許對相關資料的收集應用條件，確保在結構化組內進行徹底檢查

- 非組變數:允許條件應用於獨立的資料元素，從而在規則應用中提供靈活性

## 動態使用者定義的塊 — 最佳實踐

- 確保變數名稱在每個塊中都是唯一的。
- 避免在組名中使用變數。
- 對於子層次結構配置，請在塊中使用「<group>」。

### 範例

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

- 要捕獲單個變數中類似配置行的值，請按如下方式使用該變數：{{ <<var-name>> |行 | joinmatches(',') }}。將配置行括在{{ start }}和{{ end }}內，如以下示例所示：

| 裝置配置                                        | 阻止配置                                                     |
|---------------------------------------------|----------------------------------------------------------|
| ip domain list vrf Mgmt-intf core.cisco.com | {{ _start_ }}                                            |
| ip domain list cisco.com                    | ip domain list {{ domains   _line_   joinmatches(',') }} |
| ip domain list east.cisco.com               | {{ _end_ }}                                              |
| ip domain list west.cisco.com               | ip domain list vrf {{ vrf_name }} {{ vrf_domain }}       |

- 要從配置行中捕獲包含空格的值，請在塊中使用如下表所示的變數：{{ <<var-name>> | re("。 \*") }}

| 裝置配置                          | 阻止配置                          |
|-------------------------------|-------------------------------|
| interface HundredGigE0/0/1/31 | interface {{ INTF_ID }}       |
| 說明介面：12ylaa01 Hg0/0/1/31      | 說明{{ INTF_DESC   re("。 *") }} |
| mtu 9216                      | mtu 9216                      |

## 瞭解規則層次和規則與非RefD規則中的RefD整合

在動態塊TTP中，有兩個不同的模式來確定如何構建和驗證配置。

- 基於組的方案:
  - 此架構以分層方式組織配置，在元素之間建立父子關係
  - 對於元素在邏輯上巢狀且相互關聯的複雜配置的理想情況
  - 可以定義規則來驗證不同配置元素之間的分層關係和依賴性
- 非基於組的方案:
  - 配置以平面格式構建，所有元素都存在於同一級別，沒有層次關係
  - 適用於不需要分層的較簡單配置
  - 可以設定規則以確保每個配置元素滿足特定條件

## RefD整合

- 參考文獻的目的:
  - 角色:充當在BPA框架內管理本地和外部變數的工具
  - 功能:
    - 動態提取:促進可變資料的動態檢索和管理，允許符合性檢查適應即時資料更改
    - API互動:為BPA使用案例提供API以訪問和管理這些動態變數和值，確保順利整合到合規性工作流程中

## 符合性規則值的語法

CnR使用案例與RefD框架整合，可在合規性檢查和補救工作流中動態利用資料。此整合工作方式的詳細分析如下，尤其側重於使用的語法和變數型別：

- 關鍵字:語法必須以「RefD」開頭
- 引數:語法中的「key」引數是必需的
- 範例：

plaintext

Copy Code

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

## 變數型別

- 使用者定義的變數:
  - 在建立合規性作業期間配置。
  - 範圍:適用於指定作業的所有執行
  - 語法:{{VarName}}
  - 範例：{{SITE}}
- 系統變數
  - 由框架根據執行期間可用的上下文資料預定義

- 目前，框架提供對裝置對象的訪問
- 語法:{{#VarName}}
- 範例:
  - {{#device.deviceIdentifier}} -表示裝置識別符號
  - {{#device.additionalAttributes.serialNumber}} — 表示裝置序列號
- TTP變數
  - 存在於塊配置中
  - 語法:{{ VarName }}
  - 範例 : {{ INT\_ID }}

## 非RefD規則

- 這些規則與RefD規則類似，但不以「RefD」關鍵字開頭
- 範例：

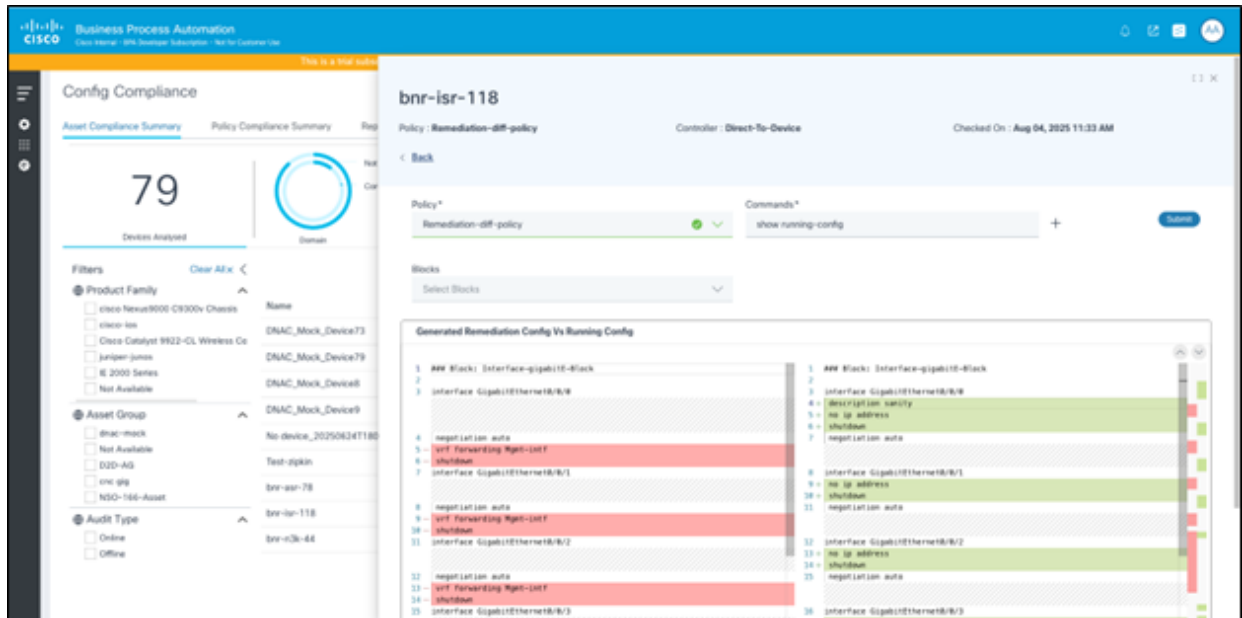
```
plaintext
Copy Code
{$int_id}.{{#device}}.{{ mtu_val }}
```

## 變數使用

- 使用者定義的變數:表示為{\$Var}
- 系統變數:表示為{{#Var}},顯示屬性，如deviceIdentifier、controllerId、controllerType等。
- TTP變數:在雙花括弧中表示為{{var}}

## 執行

- 在建立作業期間，如果指定了\$個變數，則可以設定它們的值
- 將來引數的組合值與獲取的裝置配置進行比較，以確保符合性



裝置組態

|    | 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 |                                   |                 |                     |               |         |              |

配置規則：參考號

## 檢視塊詳細資訊

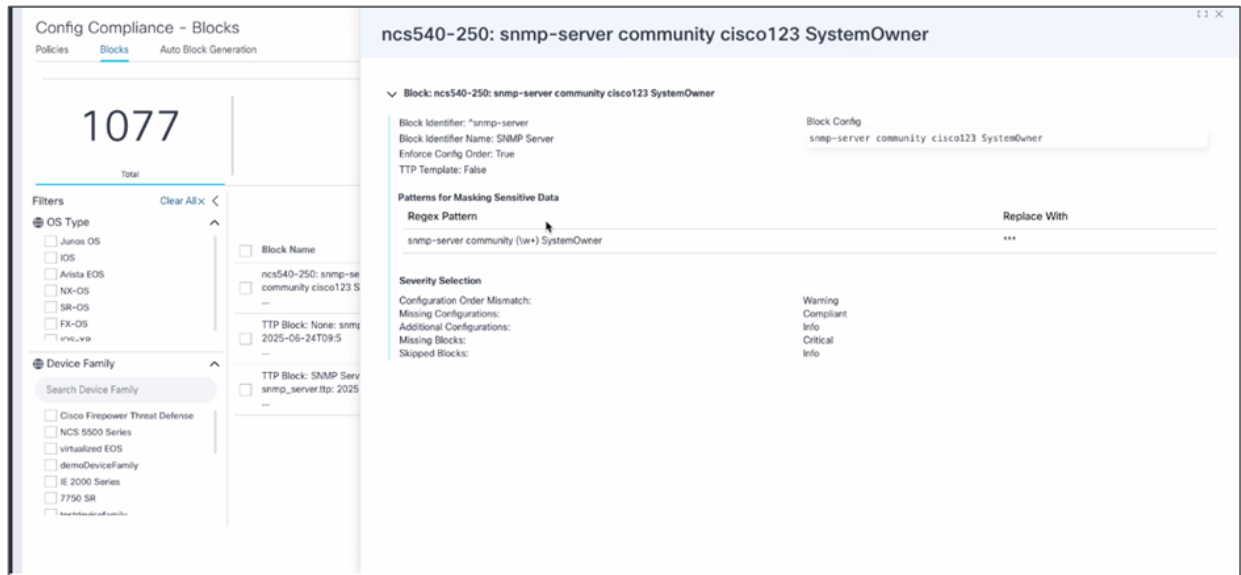
要訪問塊詳細資訊，請執行以下操作：

1. 導航到Blocks頁。
2. 選擇或按一下網格中的行以檢視特定塊的詳細資料。螢幕右側將顯示「Block Details」頁。



附註：此頁提供與該塊相關的所有資訊的只讀檢視，包括關聯的塊、規則和任何違規。

按一下詳細資訊中的超連結（如果有）會將使用者重定向到相關塊或相關資訊。



阻止詳細資訊檢視

## 刪除塊

門戶允許使用者刪除一個或多個塊，只要他們具有適當的RBAC許可權。使用者可以通過完成以下步驟執行這些操作：

對於單塊刪除：

1. 導航到Blocks頁。
2. 點選要刪除的塊旁邊的More Options圖示。
3. 選擇Delete選項。系統會顯示確認消息。

對於多塊刪除：

1. 導航到Blocks頁。
2. 選中每個要刪除的塊旁邊的覈取方塊。
3. 按一下More Options圖示，然後選擇Delete。確認消息。

×

Reporting Configurations

Auto Delete Reports Older than(Days):

30

✓

Max Blocks to be selected in a Compliance Summary Report:

50

✓

Max Assets to be selected in a Compliance Detailed Report:

100

✓

Cancel

Submit

刪除塊

## 組態:自動生成塊

塊生成允許使用者根據裝置的配置自動建立塊。這種自動化減少了手動建立所需的時間和精力，並且使使用者可以通過新增或刪除變數來更輕鬆地編輯塊，而不是從頭開始。

按一下某一行可檢視塊生成詳細資訊。

Reports > Generate Report

Generate Report

Cancel

Select Report Type\*

Summary Report

Enter Report Name\*

Demo Policy Report

Time Period

Last three months

Note: Max Blocks to be selected in a Compliance Summary Report is 5

Filters

2

Devices

Compliance

Severity

0 - Fully Compliant

6 - Partially Compliant

1 - Non Compliant

0 - Unknown

61 - Critical

0 - Major

0 - Minor

9 - Warning

28 - Info

0 - Unknown

Filters

Clear All

Default Policy - Compliance Check

Clear All

Show Selected Devices

All

Search

Policy\*

Default Policy - Compliance Check

Block

Search Block

Default Block - Hostname

Default Block - Interface Loopback

Default Block - Interface Mgmt

Default Block - Interface TenGig

Default Block - Location

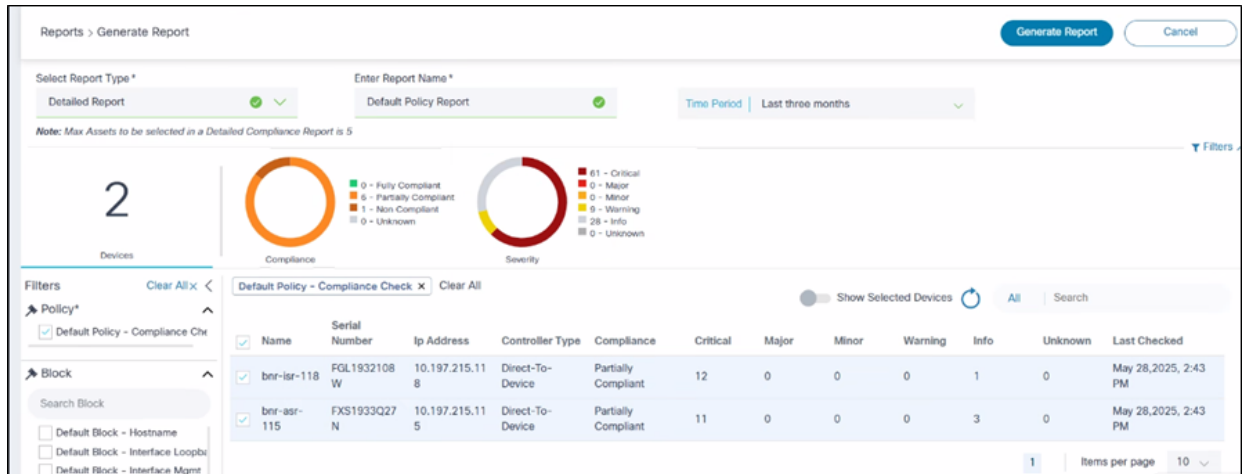
| Name        | Serial Number | Ip Address      | Controller Type  | Compliance          | Critical | Major | Minor | Warning | Info | Unknown | Last Checked          |
|-------------|---------------|-----------------|------------------|---------------------|----------|-------|-------|---------|------|---------|-----------------------|
| bnr-lsr-118 | FGL1932108 W  | 10.197.215.11 8 | Direct-To-Device | Partially Compliant | 12       | 0     | 0     | 0       | 1    | 0       | May 28, 2025, 2:43 PM |
| bnr-asr-115 | FXS1933Q27 N  | 10.197.215.11 5 | Direct-To-Device | Partially Compliant | 11       | 0     | 0     | 0       | 3    | 0       | May 28, 2025, 2:43 PM |

1

Items per page

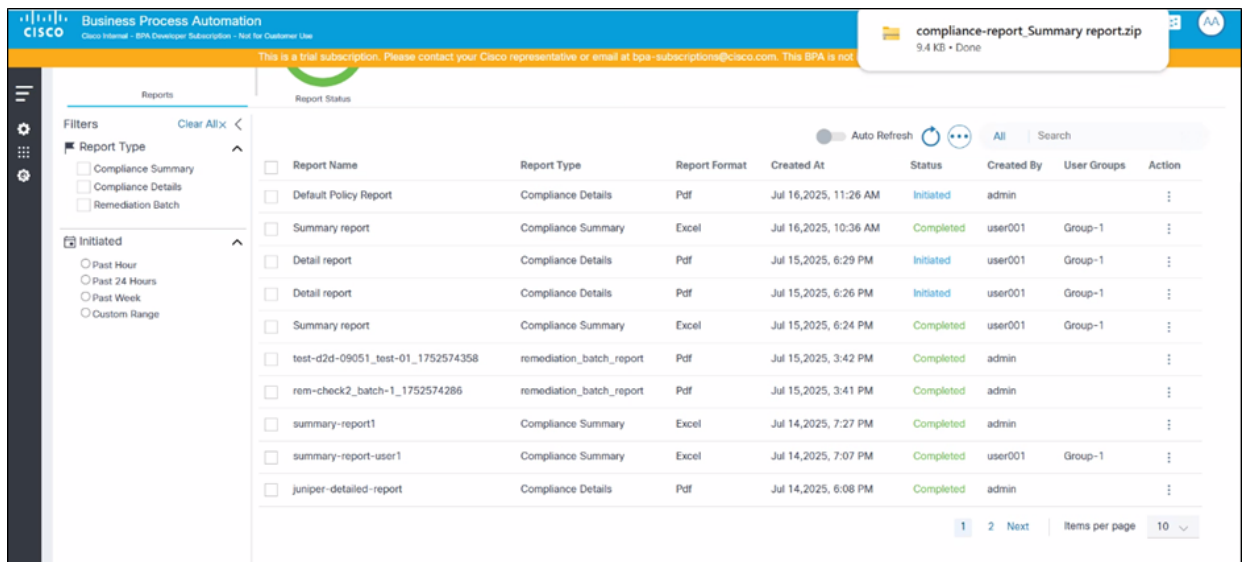
10

自動阻止生成清單 — 檢視



自動塊生成詳細資訊

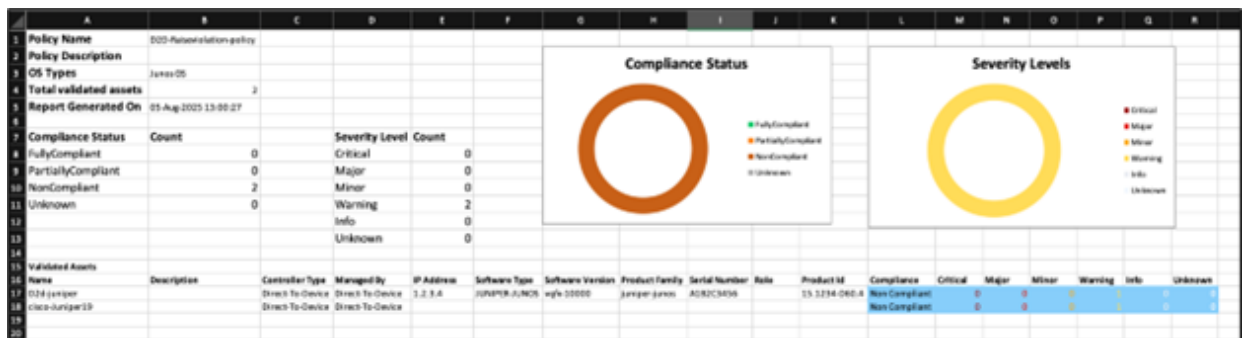
自動生成塊



自動阻止生成清單

Automatic Block Generation頁包含以下欄位：

- 生成自:從中生成塊的源。它有以下三個選項：
  - Device Config Backup:系統從備份用例中選擇裝置配置



## 裝置配置備份

- 檔案上傳:將開啟一個檔案上傳視窗，供使用者上傳裝置配置

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

## 檔案上傳

- 當前配置:輸入系統用於獲取裝置配置的CLI配置命令。

|    | 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<br>Gigabit ethernet configuration | DescriptionCheck      |             | warning          | 5               | 3                     |
| 3  | Gigabit Rule | Rule to validate violations for<br>Gigabit ethernet configuration | IP-Address-Validation |             | critical         | 6               | 2                     |
| 4  | Gigabit Rule | Rule to validate violations for<br>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 |              |                                                                   |                       |             |                  |                 |                       |

## 當前配置

- 作業系統類型：與此塊相關的OS型別清單。
- 裝置系列:與此塊相關的裝置系列的清單。
- 資產:Assets功能提供了一種結構化方法來選擇用於生成動態塊的裝置
  - 資產組選擇:
    - 允許使用者選擇預定義的裝置組（稱為資產組），用於生成動態塊
    - 根據特定條件（如位置、型別或功能）對裝置進行分組，從而方便裝置的管理和組織
  - 子集裝置選擇:
    - 使用者可以靈活地從所選資產組中選擇特定裝置子集
    - 使使用者能夠專注於特定裝置段，從而能夠進行更有針對性的資料塊生成和管理

Auto Block Generation Details

Generate From\*  
Device Config Backup ✓ ✓ ☐ Override existing blocks

OS Type\*  
3 selected ✓ ✓ ☐

Device Families\*  
All ✓ ✓ ☐

Asset Group\*  
Juniper NSO asset ✓ ✓ ☒ Select All Devices

| Name     | Ip Address | Location | Managed By |
|----------|------------|----------|------------|
| vMX01-18 |            |          | NSO-166    |

1 Items per page 10

Select Block Identifiers to be used during Auto Block Generation ☐ Use Selected Block Identifiers Only

| Block Identifier Name | Block Identifier Pattern | OS Type          | Template     | Multi-Select | Template Count | Action |
|-----------------------|--------------------------|------------------|--------------|--------------|----------------|--------|
| Hostname              | ^([?i])hostname          | IOS,IOS-XR,NX-OS | hostname.ttp | false        | 1              |        |

## 塊生成

- 塊識別符號:為使用者提供了一個選項，用於選擇在塊生成期間使用的塊識別符號清單。它還內聯提供塊識別符號管理功能。

## 塊識別符號

塊識別符號使用[CiscoConfParser](#)從整個裝置配置中提取配置塊。每個塊識別符號應與正規表示式模式相關聯。使用者可以使用UI或API建立自己的塊識別符號或更新現有塊識別符號。該平台目前提供大約55-60個預設塊識別符號。每個識別符號對於OS型別是唯一的，並且在BPA應用部署期間通過Ingestor服務載入。TTP模板可以與每個塊識別符號相關聯。塊識別符號的名稱和模式必須是唯一的。

如果為塊識別符號啟用了Multi選項，則相容性框架將從匹配的配置生成多個配置塊。否則，它會將所有匹配的配置視為一個塊。

Multi選項True的塊標識符示例：interface、router bgp、vrf、l2vpn等

Multi option False的塊標識符示例：日誌記錄、snmp-server、域等

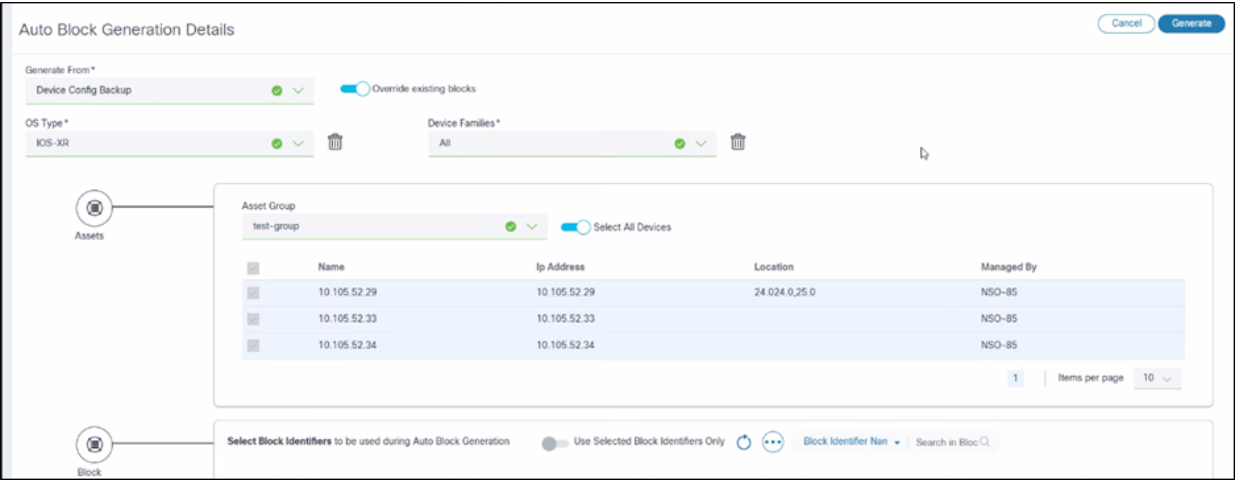
範例:

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

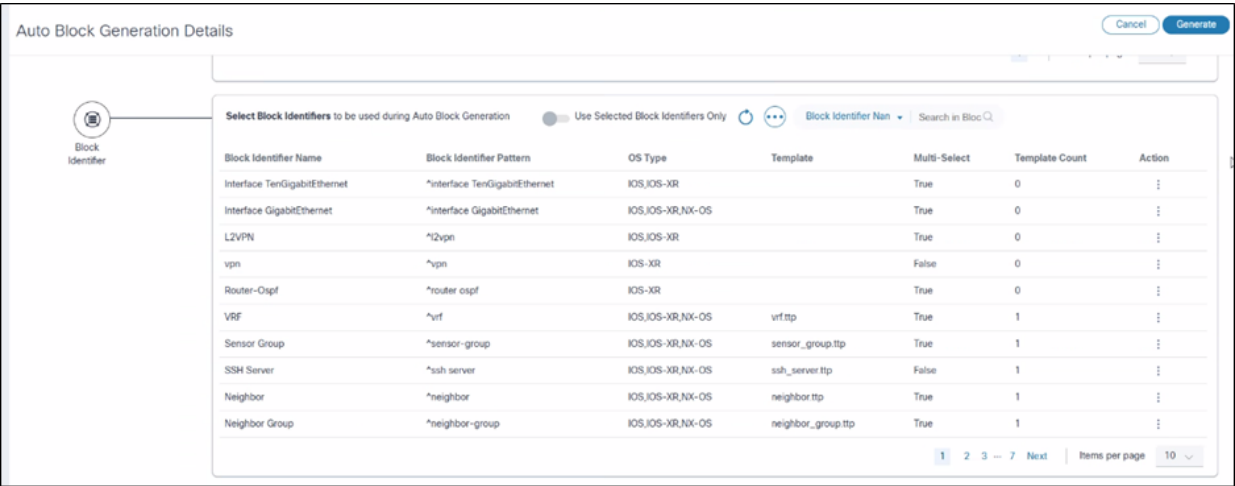
```
{
  "name": "Loopback Interface",
  "osType": ["IOS", "IOS-XR", "NX-OS"],
  "multi": true,
  "blockIdentifier": "^(?i)interface Loopback",
  "templates": ["parent_interface.ttp"]
}
```

清單塊識別符號

清單塊識別符號允許使用者檢視塊識別符號清單以及搜尋和排序功能。Generate Blocks頁中提供了此功能。

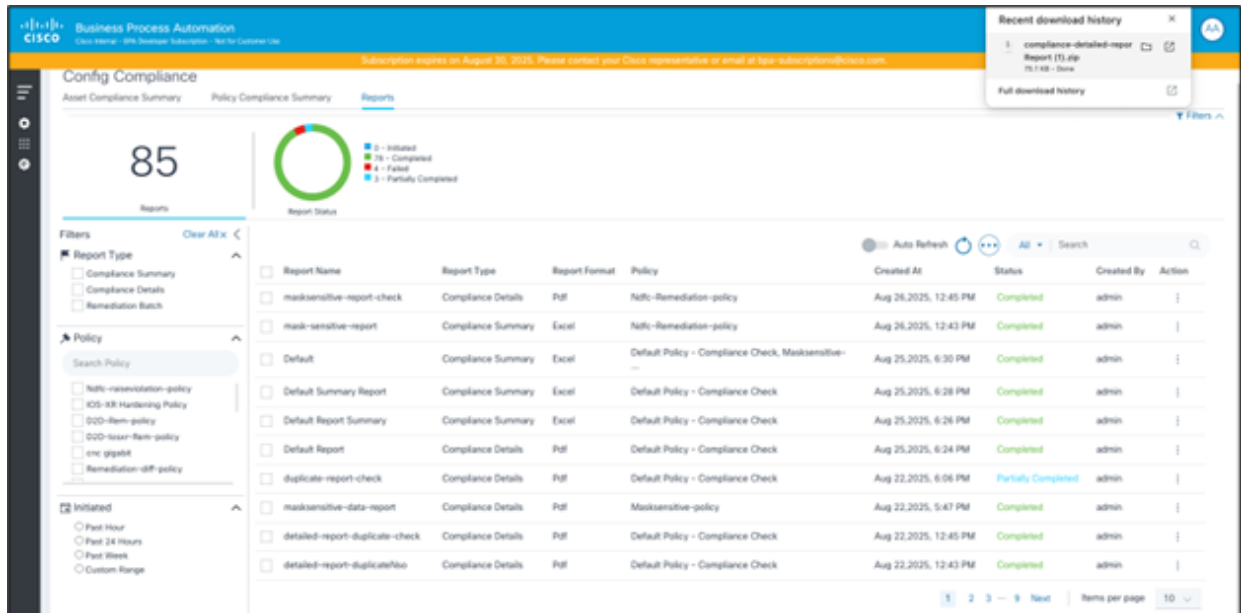


阻止識別符號清單



塊識別符號

建立或編輯塊識別符號



## 編輯塊識別符號

Auto Block Generation頁上的Block Identifier List部分為使用者提供有效管理塊識別符號的工具。功能如下所示：

- 建立塊識別符號
  - 使用者可以向清單中新增新的塊識別符號
  - 這允許引入可用於組織和區分塊的唯一識別符號
- 編輯塊識別符號
  - 可以修改現有的塊識別符號
  - 允許更新或更正識別符號，以確保識別符號保持準確並與識別符號所代表的塊相關
- 刪除塊識別符號
  - 使用者可以選擇從清單中刪除塊識別符號
  - 通過允許刪除不再需要的識別符號或不再適用的識別符號來簡化識別符號管理

# 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               |

刪除塊識別符號

## 組態:政策

可以在Policies頁籤上定義一組策略、規則和塊以啟用合規性執行。策略是由配置塊和規則組成的使用者定義模板。可以選擇用於建立策略的配置塊清單和每個配置塊的規則清單。

## 列出策略

策略清單可以顯示在Policies頁籤上，該頁籤還提供用於新增、編輯、刪除、匯入和匯出策略的操作。



附註：策略將隨相關塊和規則一起匯入或匯出。

Config Compliance – Policies

Policies

Blocks

Auto Block Generation

42

Total Policies

Filters

Clear All x

OS Type

☐ NX-OS

☐ Arista EOS

☐ IOS-XR

☐ Junos OS

☐ SR-OS

☐ IOS

☐ EV-OS

Policy Name

Search in Policy Nam

| <input type="checkbox"/> | Policy Name          | OS Type          | Created At             | Last Updated At        | Action |
|--------------------------|----------------------|------------------|------------------------|------------------------|--------|
| <input type="checkbox"/> | NDFC-test2           | NX-OS            | Jul 16, 2025, 10:06 AM | Jul 16, 2025, 10:06 AM | ⋮      |
| <input type="checkbox"/> | Backup-Policy        | IOS-XR,IOS       | Jul 15, 2025, 3:07 PM  | Jul 15, 2025, 3:07 PM  | ⋮      |
| <input type="checkbox"/> | raise_violation_true | IOS,IOS-XR       | Jul 15, 2025, 2:10 PM  | Jul 15, 2025, 2:10 PM  | ⋮      |
| <input type="checkbox"/> | Policy logging       | IOS,IOS-XR,NX-OS | Jul 14, 2025, 5:40 PM  | Jul 14, 2025, 5:40 PM  | ⋮      |
| <input type="checkbox"/> | test maskhost        | IOS,IOS-XR,NX-OS | Jul 14, 2025, 4:34 PM  | Jul 14, 2025, 4:34 PM  | ⋮      |
| <input type="checkbox"/> | Ndfc-Rem-policy      | NX-OS            | Jul 14, 2025, 12:57 PM | Jul 14, 2025, 7:35 PM  | ⋮      |
| <input type="checkbox"/> | Policy mask1         | IOS,IOS-XR,NX-OS | Jul 14, 2025, 12:26 PM | Jul 14, 2025, 12:26 PM | ⋮      |
| <input type="checkbox"/> | Policy host          | IOS,IOS-XR,NX-OS | Jul 11, 2025, 2:06 PM  | Jul 11, 2025, 2:06 PM  | ⋮      |

## 列出策略

## 新增和編輯策略

本節概述了Add Policy and Edit Policy頁：

## 策略詳細資訊

- 策略名稱:策略名稱
- 作業系統類型：此策略支援的作業系統型別清單
- 裝置系列:此策略支援的裝置系列清單
- 策略說明 ( 可選 ) :用簡短描述描述策略

根據下一節中選定的塊，自動填充OS Type和Device Family欄位。

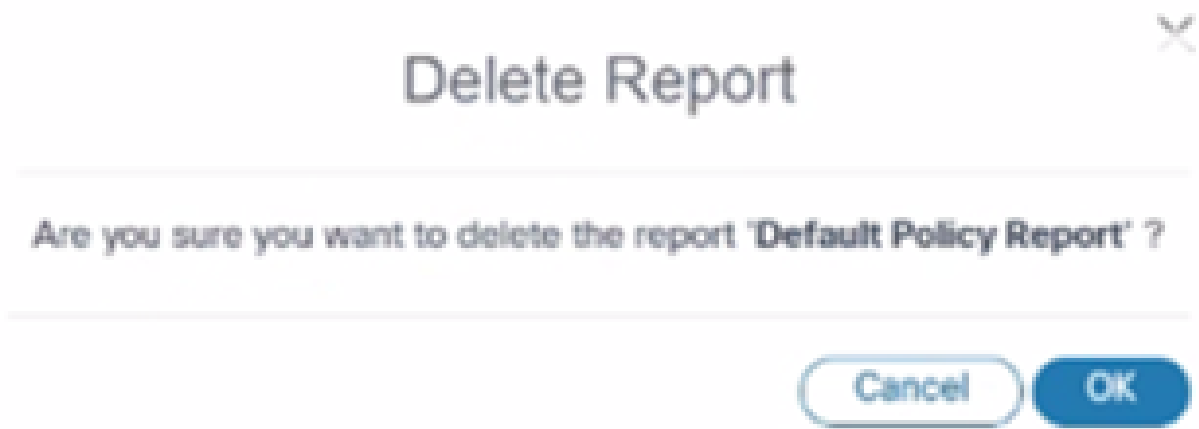
| Violation Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <div>Legend</div> <div> <div>+ Config line present in device, but not in block definition</div> <div>- Config line missing in device, but present in block definition</div> </div>                                                                                                                                                                                                                                                                                                               |  |
| <div>Block: Cnr Demo Block Minor</div> <div> <div>1   interface GigabitEthernet0/0/0 Minor</div> <div> <div>Expected: desc Equals 'Demo' Minor</div> <div>Found: 'None' Cnr Demo Policy2 → Demo Rule 2 → Demo Cond1</div> </div> <div>+ 2   no ip address Info</div> <div>+ 3   shutdown Info</div> <div>+ 4   negotiation auto Info</div> <div>+ 5   cdp enable Info</div> <div>6   interface GigabitEthernet0/0/1 Info Skipped</div> <div>Expected: interface Equals '0/0/0' Info</div> </div> |  |
| <div>Configuration Compliance - Asset Violations Report</div> <div>Page 1 of 4</div>                                                                                                                                                                                                                                                                                                                                                                                                             |  |

配置策略：策略詳細資訊

## 「選擇塊」對話方塊

「選擇塊」功能是一個使用者友好的介面，旨在幫助使用者選擇配置塊以包含在策略中。其功能在本節中列出：

- 彈出對話方塊
  - 目的:為使用者提供了專用空間，使用者無需離開當前頁面即可選擇配置塊
  - 使用者互動:通過在單獨的、重點突出的對話方塊中演示選項，確保直觀的選擇過程
- 新增和選擇選項
  - 多項選擇:使用者可以選擇一個或多個要包含在策略中的配置塊
  - 靈活性:支援根據使用者的特定策略要求包含各種塊
- 導航功能
  - 篩選條件：允許使用者根據特定條件縮小可用塊清單的範圍，從而更輕鬆地查詢相關塊
  - 分頁:將塊組織成可管理的頁面，從而改善通過大量資料的導航
  - 搜尋功能:允許按名稱或其他識別符號快速定位塊，從而簡化選擇過程



### 阻止選擇

使用者可以通過按一下「塊選擇」部分中的「建立」來建立新塊。新的瀏覽器頁籤會交叉啟動，使用者可以建立一個新塊。提交後，使用者可以返回到原始頁籤，並選擇新建立的塊以將其新增到策略中。

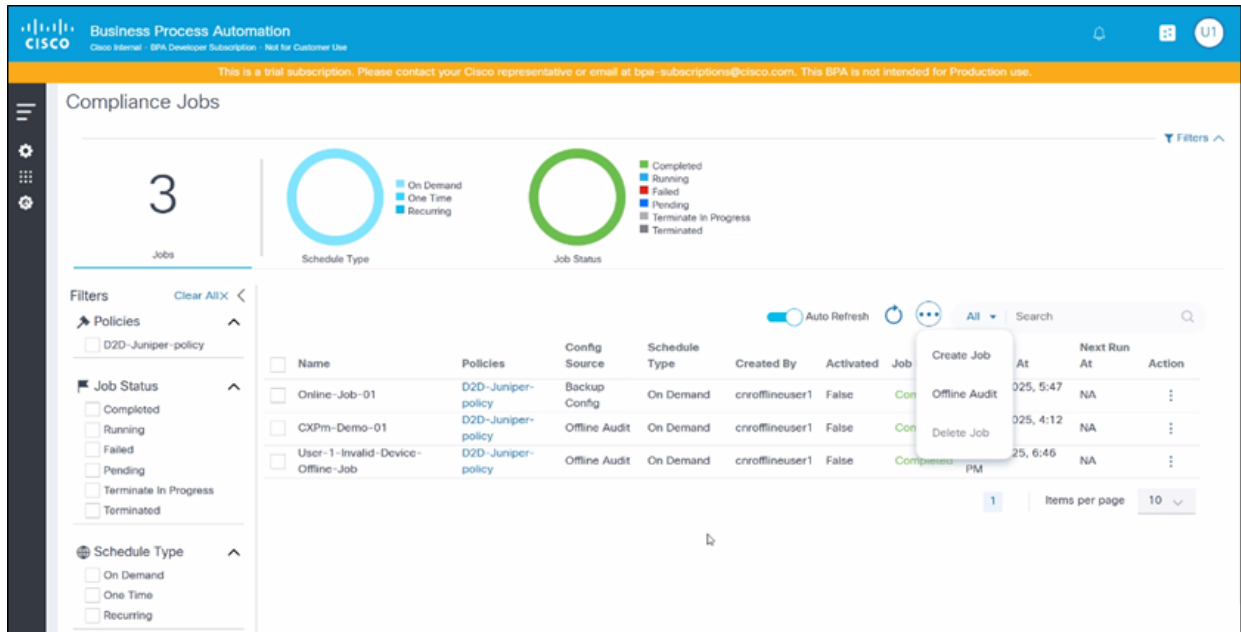
### 條件式篩選條件

條件過濾器功能是一種高級工具，允許使用者將特定條件應用到配置塊，從而確保準確和有目標的合規性檢查。

- 允許使用者根據預定義條件對選定的配置塊應用配置或運行符合性檢查
- 通過篩選出不符合指定標準的資源塊，將資源和工作集中在相關塊上
- 使用者可以定義配置塊必須滿足的條件，以便包括在合規性檢查或其他流程中
- 僅執行符合這些條件的塊，而忽略其他塊，從而允許更精確的控制

用例示例:

- 選擇性合規性檢查：如果某個策略旨在檢查可用的20個介面中的兩個特定介面上的配置，則使用者可以設定條件以將合規性檢查限制為僅檢查這兩個介面。



## 條件式篩選條件

- 選擇規則:用於為給定配置塊選擇一個或多個規則的選項。

**Create Offline Audit**

**Job Summary:** Name: Offline-Job-01

**Policy Summary:** Policy Name: D2D-Juniper-policy, OS Types: Junos OS, Blocks: 1, Rules: 1

**Schedule Summary:** Schedule Date: N/A, Schedule Type: On Demand

**File Upload:** Select file to upload. Supported extensions: \*.txt, \*.cfg, \*.conf, \*.zip, \*.tgz, \*.tar.gz. RegEx pattern to remove file name prefix: \d{8}T\d{6}\_ (checked). RegEx pattern to remove file name suffix: \_\d{8}T\d{6} (checked). Upload button.

**Assets:** Select All Assets (checked), Show Only Selected Assets. Table with columns: Name, Managed By, Product Family. Row: SUFFIX\_REMOVED, Direct-To-Device, IT Networking.

## 選擇規則

## Remediation部分

Policies頁提供了一個可選部分，用於定義每個控制器型別的補救詳細資訊。

## 配置策略：修正詳細資訊

- 控制器型別:支援補救的控制器型別清單
- 修正工作流程:為所選控制器型別的裝置執行的工作流程
- GCT模板:要應用的一個或多個GCT模板
- 流程模板：要作為預檢查和後檢查的一部分執行的一個或多個流程模板以及相應的分析模板。
- 預檢查模板:可選的流程模板清單，這些模板僅用於預檢查
- Post Check模板:可選的流程模板清單，這些模板僅用於後檢查
- 執行模式:
  - 完全自動:自動運行補救流程，無需手動干預或使用任務
  - 基於助理:系統在補救過程中建立需要手動幫助的使用者任務

## 自動生成GCT功能

自動生成GCT功能旨在簡化建立補救所需的GCT模板的過程。其工作原理如下所述：

- 根據遵從性執行的結果和詳細資訊自動生成GCT模板
- 自動化模板建立流程
- 生成的模板經過定製，可解決在合規性檢查期間發現的問題，確保補救措施與合規性需求保持一致

## 角色和訪問控制

### 靜態許可權清單

下一代門戶中的配置合規性儀表板支援BPA的RBAC功能，具有以下許可權，這些許可權表示如何在GUI表示法中顯示配置動態文本塊，以便處理規則和條件：

| 群組      | 動作                              | 說明                               |
|---------|---------------------------------|----------------------------------|
| ui-app  | complianceDashboard.show        | 顯示/隱藏合規性儀表板應用                    |
| ui-app  | remediationDashboard.show       | 顯示修正作業應用                         |
| ui-app  | complianceJobs.show             | 顯示合規性作業應用                        |
| ui-app  | complianceConfigurations.show   | 顯示合規性配置應用                        |
| 合規性控制面板 | 資產合規性摘要                         | 檢視資產合規性摘要                        |
| 合規性控制面板 | 策略合規性摘要                         | 檢視策略符合性摘要                        |
| 合規性控制面板 | viewViolations                  | 檢視違規詳細資訊                         |
| 合規性控制面板 | 策略合規性資產摘要                       | 檢視受影響的資產                         |
| 合規性控制面板 | viewReport                      | 檢視報告控制面板、報告設定和下載報告               |
| 合規性控制面板 | 管理報告                            | 建立和刪除報告                          |
| 合規性控制面板 | manageReportSettings            | 修改報表設定                           |
| 補救控制面板  | viewRemediationJob              | 檢視修正作業                           |
| 補救控制面板  | viewRemediationMilestones       | 檢視修正里程碑                          |
| 補救控制面板  | 管理修正作業                          | 管理補救作業，如建立、刪除、存檔和處理使用者任務         |
| 合規性作業   | viewComplianceJob               | 檢視符合性作業和執行                       |
| 合規性作業   | 管理合規性作業                         | 管理合規性作業                          |
| 合規性配置   | viewCompliance配置                | 檢視合規性配置，如策略、塊、規則、塊生成、塊識別符號和TTP模板 |
| 合規性配置   | 管理合規性策略                         | 管理合規性策略                          |
| 合規性配置   | 管理合規性塊                          | 管理合規性塊和規則以及塊識別符號                 |
| 合規性配置   | manageComplianceBlockGeneration | 管理合規性塊生成和TTP模板                   |

## 預定義角色

配置合規性和補救使用情形具有下表列出的預定義角色：

 附註：管理員可以根據客戶要求建立或更新角色。

| 角色     | 說明                 | 許可權                 |
|--------|--------------------|---------------------|
| 合規性管理員 | 具有所有符合性相關許可權的管理員角色 | UI應用程式:             |
|        |                    | 顯示資產管理器             |
|        |                    | — 顯示資產組             |
|        |                    | — 檢視合規性儀表板          |
|        |                    | — 顯示合規性作業           |
|        |                    | — 顯示合規性配置           |
|        |                    | 資產:                 |
|        |                    | 檢視資產清單              |
|        |                    | — 檢視資產的備份配置         |
|        |                    | — 備份配置              |
|        |                    | — 執行啟用控制器的裝置操作      |
|        |                    | 資產組:                |
|        |                    | — 檢視資產組             |
|        |                    | — 管理資產組             |
|        |                    | — 建立動態資產組           |
|        |                    | 備份配置:檢視、比較和下載裝置配置備份 |
|        |                    | 備份還原策略:檢視備份還原策略     |
|        |                    | 合規性控制面板：            |
|        |                    | — 檢視資產的合規性摘要        |
|        |                    | — 檢視策略的符合性摘要        |
|        |                    | — 檢視違規              |
|        |                    | — 檢視受影響的資產          |
|        |                    | 建立和刪除報告             |
|        |                    | 檢視報告控制面板、報告設定和下載報告  |
|        |                    | 修改報告設定：             |
|        |                    | 合規性作業               |

角色

說明

許可權

檢視符合性作業和執行  
— 管理合規性作業

合規性配置:

- 檢視合規性配置，如策略、塊和規則
- 管理合規性策略
- 管理合規性塊、規則和塊識別符號
- 管理合規性塊生成和TTP模板

UI應用程式:

- 顯示資產管理器
- 顯示資產組
- 檢視合規性儀表板
- 顯示合規性作業
- 顯示合規性配置

資產:

- 檢視資產清單
- 檢視資產的備份配置
  - 備份配置
  - 執行啟用控制器的裝置操作

合規操作員

具有除配置管理以外的所有  
合規性許可權的操作員角色

資產組:

- 檢視資產組
- 管理資產組
- 建立動態資產組

備份配置:檢視、比較和下載裝置配置  
備份

備份還原策略:檢視備份還原策略

合規性控制面板：

- 檢視資產合規性摘要
- 檢視策略符合性摘要
- 檢視違規

| 角色    | 說明                   | 許可權                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                      | <ul style="list-style-type: none"> <li>— 檢視受影響的資產</li> <li>建立和刪除報告</li> <li>檢視報告控制面板、報告設定和下載報告</li> <li>法規遵從性工作:</li> <li>檢視符合性作業和執行</li> <li>— 管理合規性作業</li> <li>合規性配置:</li> <li>檢視策略、塊和規則等合規性配置</li> <li>UI應用程式:</li> <li>— 顯示資產管理器</li> <li>— 顯示資產組</li> <li>— 檢視合規性儀表板</li> <li>— 顯示合規性作業</li> <li>— 顯示合規性配置</li> <li>資產:</li> <li>檢視資產清單</li> <li>— 檢視資產的備份配置</li> <li>— 執行啟用控制器的裝置操作</li> </ul> |
| 合規性只讀 | 提供與符合性使用情形相關的所有只讀許可權 | 資產組: <ul style="list-style-type: none"> <li>— 檢視資產組</li> </ul> 備份配置:檢視、比較和下載裝置配置備份<br>備份還原策略:檢視備份還原策略<br>合規性控制面板 :<br>檢視資產合規性摘要 <ul style="list-style-type: none"> <li>— 檢視策略符合性摘要</li> <li>— 檢視違規</li> <li>— 檢視受影響的資產</li> </ul> 檢視報告控制面板、報告設定和下載報告                                                                                                                                                 |

| 角色          | 說明                  | 許可權                        |
|-------------|---------------------|----------------------------|
|             |                     | 告                          |
|             |                     | 法規遵從性工作:                   |
|             |                     | 檢視符合性作業和執行                 |
|             |                     | 合規性配置:                     |
|             |                     | 檢視策略、塊和規則等合規性配置            |
|             |                     | UI應用程式:                    |
|             |                     | — 顯示資產管理器                  |
|             |                     | — 顯示資產組                    |
|             |                     | — 檢視補救控制面板                 |
|             |                     | 資產:                        |
|             |                     | — 檢視資產清單                   |
| 補救管理員/補救操作員 | 具有所有補救相關許可權的操作員角色   | 資產組:                       |
|             |                     | — 檢視資產組                    |
|             |                     | 管理資產組                      |
|             |                     | — 建立動態資產組                  |
|             |                     | 補救控制面板:                    |
|             |                     | — 檢視修正作業                   |
|             |                     | — 檢視修正里程碑                  |
|             |                     | — 檢視資產合規性摘要                |
|             |                     | — 管理補救作業，如建立、刪除、存檔和處理使用者任務 |
|             |                     | — 檢視受影響的資產                 |
|             |                     | UI應用程式:                    |
|             |                     | — 顯示資產管理器                  |
|             |                     | — 顯示資產組                    |
|             |                     | — 檢視補救控制面板                 |
| 補救只讀        | 提供與補救使用情形相關的所有只讀許可權 | 資產:                        |
|             |                     | — 檢視資產清單                   |

資產組：

- 檢視資產組
- 建立動態資產組

補救控制面板：

- 檢視修正作業
- 檢視修正里程碑
- 檢視資產合規性摘要
- 檢視受影響的資產

## 訪問策略

「訪問策略」功能可確保使用者具有對特定合規性策略和資產組的適當訪問許可權。此功能允許管理員根據使用者角色和責任定義並實施訪問控制，從而增強安全性和運營效率。訪問策略通過「訪問策略」頁進行管理，管理員可以在該頁建立、編輯策略並將其分配給使用者或組。管理員可以定義精細許可權，指定每個使用者或組可以檢視、編輯或管理的符合性策略和資產組。這一級別的詳細資訊有助於保持對敏感資訊和關鍵操作的嚴格控制。

定義訪問策略後，根據當前使用者有權訪問的CnR策略和資產的清單，在下一代UI中的所有合規性和補救頁面上限制資料。

要提供使用者訪問許可權，請執行以下操作：



附註：許可權只能由管理員提供。

1. 建立使用者並將他們分配到使用者組。
2. 建立使用者角色並將其分配給建立的使用者組。
3. 將資產新增到資產組。
4. 建立資源組以分配合規性策略資源。
5. 建立訪問策略並選擇相關使用者組、資產組和資源組。

### 建立資源組

使用Resource Type下拉選單中的compliance remediation-policy建立資源組，並選擇需要授予其相

應使用者組訪問許可權的合規性策略。

Add Resource Group

Resource Group name \*

CnR-Policy

Resource Type:

compliance-remediation-policy

Description:

Enter resource group description

Resources:

☐

Name

☐

C8kvPolicy

☐

CNC6Policy

☐

CNCRegPolicy

☐

CNCRemPolicy

☐

Class-Map-Policy-01

☐

DNACRegPolicy

☐

Default Compliance Policy

☐

Default Policy - Compliance Check

☐

Default Policy - RefD - Compliance Check

☐

Default Policy - RefD - Compliance Check1

建立資源組

建立訪問策略

建立需要授予使用者組許可權的資源組和資產組的訪問策略。

Add Policy

Policy name \*

Access Policy Name

Description:

Enter policy description

Resource Groups:

All

Search

☐

Resource Groups

☒

CnR-Resource-Group

☐

CnR-Rem-POC-Policy

☐

CnR-Performance-Test-Rsrc-Grp

1

Items per page

10

Asset Groups:

All

Search

☐

Asset Groups

Group Type

☐

200915499

static

☐

2408devicegroup

static

☒

2408devicegroup12

static

☒

402-dg

static

☒

A1

static

☐

ATT-Conexus-PSL-Topology

static

User Groups:

All

Search

☐

User Groups

☐

admin

☒

svcaact

☐

service-manager

☐

device-manager

☐

workflow-admin

☐

operator

Cancel

Submit

建立訪問策略

# 離線符合性

離線符合性功能使使用者可以對資產清單中的活動裝置不可用的裝置配置運行符合性檢查。

使用者可以使用裝置備份配置或通過在合規性作業中建立離線稽核來運行離線合規性。執行結果可以在「遵循性」控制面板上檢視。

## 使用裝置備份配置

管理員可以手動上傳包含所需裝置組的運行配置的zip檔案。此功能在備份和還原應用程式的Device Config - Upload部分中提供。上傳裝置配置後，可以通過選擇Device Backup Config作為裝置配置的源來建立所需裝置的合規性作業。在執行期間，從備份應用程式檢索已上傳的裝置配置，並對該配置執行合規性檢查。

在符合性作業中使用建立離線稽核功能

要針對裝置配置離線運行合規性，使用者可從「合規性作業」頁上的更多選項圖示中選擇離線稽核。這允許使用者直接在合規性應用程式中手動上傳包含運行配置的zip檔案。在執行期間，將分析上載的裝置配置並執行合規性檢查。

## 通過Ingestor部署配置

使用Ingestor框架可以自動載入合規性配置對象。開發工件後，可以使用以下步驟將其匯出、打包並部署到目標環境中。

- 使用以下命令建立NPM軟體包：

```
mkdir <

>
cd <

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

- 從BPA門戶匯出配置（傳統UI）
  - 導航至BPA Classic UI > Configuration Compliance & Remediation > Configurations
  - 匯出「TTP模板/塊識別符號/塊/規則/策略」

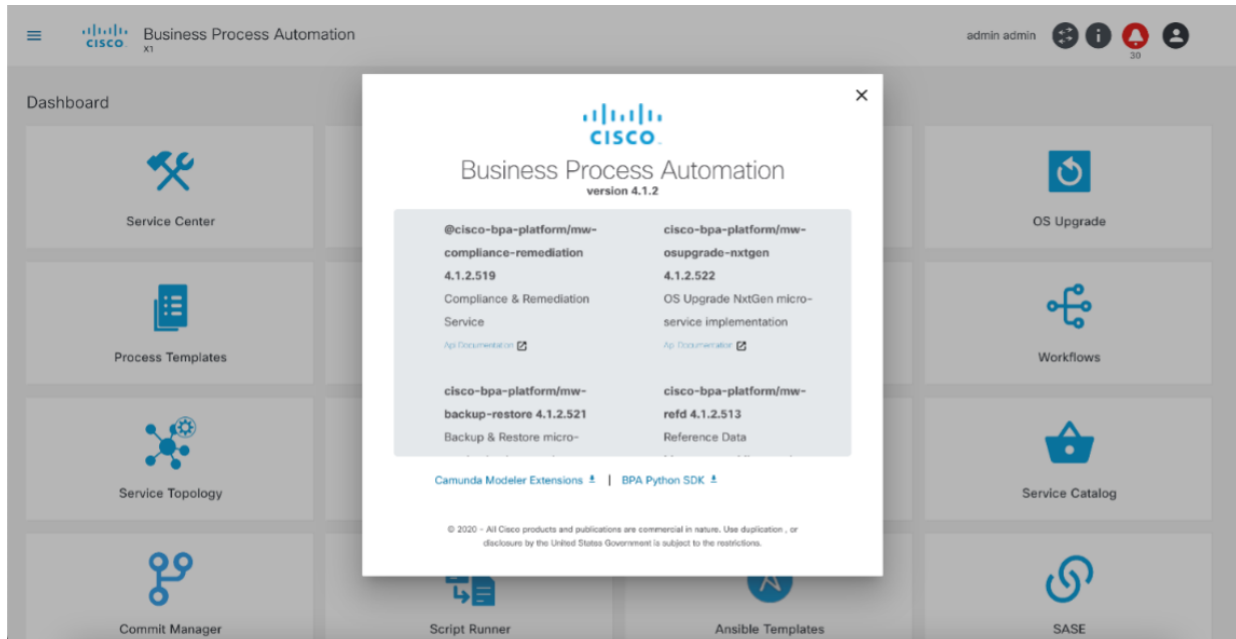
- 按如下方式重新命名匯出的檔案：
  - TTP模板：<<filename>>.cnrttptemplate.json
  - 塊識別符號：<filename>.cnrblockidentifier.json
  - 塊：<filename>.cnrblock.json
  - 規則：<filename>.cnrrule.json
  - 策略：<filename>.cnrpolicy.json
- 包入口資料(.tgz)
  - 將所有匯出檔案複製到「步驟1」中建立的npm包中
  - 在npm包中運行`npm pack`命令以建立「.tgz」檔案
- 將ingester資料(.tgz)部署到BPA單節點環境
  - 將.tgz檔案複製到部署BPA捆綁包的伺服器中的<<BPA core bundle>>/packages/data資料夾
  - 重新啟動Ingester伺服器(`docker restart ingester-service`)
- 將Ingester資料(.tgz)部署到BPA多節點環境
  - 將.tgz檔案複製到/opt/bpa/packages/data資料夾，該資料夾位於部署了舵圖的伺服器上
  - 重新部署Ingester pod(`kubectl rollout restart deployment ingester-service -n bpa-ns`)

## 參考資料

| 名稱    | 說明                  |
|-------|---------------------|
| TTP   | 配置塊中使用的模板文本解析器      |
| 會議解析器 | 用於分析CLI裝置配置的配置欄位分析器 |

## API 說明文件

有關合規性和補救的API文檔詳細資訊可在傳統UI關於彈出式視窗中找到：



BPA關於 ( 傳統UI )

## 疑難排解

### 控制面板

不顯示最近的合規性作業結果

觀察:最近的合規性作業結果不會顯示在下一代門戶控制面板中。

潛在原因1:控制面板具有日期範圍選擇，預設值為「當前月份」。如果最近開始了一個新月（例如，今天是該月的第一天），則不會顯示昨天（上個月的最後一天）之前執行的執行。

分析:確認儀表板中選定的日期範圍正確（如果需要，包括上個月的日期），以顯示正確的違規資料。

潛在原因2:其他使用者可能已在同一策略和/或資產組合上運行合規性作業。儀表板顯示所選日期範圍內最新運行期間發現的違規。

分析:以管理員（或有權訪問所有符合性作業的使用者）身份，檢視符合性作業的清單及其歷史記錄，以確定要執行哪些策略或資產組組合。

### 合規性作業

整個執行狀態設定為「已跳過」

觀察:運行合規性作業時，整個執行狀態標籤為「已跳過」。未報告任何違規。

潛在原因:同一作業的現有執行仍在運行。

分析:在任意給定時間點，一個符合性作業只能有一個處於運行狀態的執行。驗證早期執行是否仍在運行。如果執行停滯或長時間運行，可以終止/

裝置狀態設定為「已跳過」

觀察:在合規性作業執行中，某些裝置的狀態標籤為「已跳過」。

潛在原因:未為該裝置所屬的控制器型別啟用合規性功能。

分析:合規性策略僅適用於資產組中已啟用功能的裝置。

裝置狀態設定為「失敗」

觀察:在合規性作業執行中，某些裝置的狀態標籤為「失敗」。

潛在原因:合規性執行過程中發生的運行時錯誤。這些錯誤可能是代碼錯誤或策略、塊、規則、塊識別符號等中的配置不正確。

分析:

用於查詢運行時錯誤原因的API:

#### 1. 獲取執行以查詢執行ID

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

合規性執行

方法：GET

#### 2. 使用執行ID獲取裝置執行

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

合規性裝置執行？

executionId=<<< execution-id >>

方法：GET

## 合規性規則

### 規則顯示空值

觀察:在執行相容性作業期間，規則變數顯示空值。

分析:

1. 如果正在從RefD應用程式檢索資料，請確認RefD鍵的格式正確。如果是，請確認RefD應用程式具有連結到規則中符合性變數的金鑰的資料。此外，通過檢查合規性服務日誌來驗證是否從合規性應用傳送了正確的RefD金鑰。請參閱[瞭解規則層次結構和規則中的參考與非RefD規則的整合](#)。
2. 使用以下API檢查符合性塊執行結果：

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

方法：GET

GET [{{uatUrl}}/api/v1.0/compliance-remediation/compliance-block-executions?deviceExecutionId=66dfc32a2b855fb425602d4d](#)

Params ● Authorization Headers (8) Body Pre-request Script Tests Settings

Query Params

| KEY                                                   | VALUE                    | DESCRIPTION |
|-------------------------------------------------------|--------------------------|-------------|
| <input checked="" type="checkbox"/> deviceExecutionId | 66dfc32a2b855fb425602d4d |             |
| Key                                                   | Value                    | Description |

ody Cookies Headers (11) Test Results  Status: 20

Pretty Raw Preview Visualize JSON 

```
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
{
  "results": [
    {
      "variable": "interface",
      "operation": "equals",
      "value": "0/0/3",
      "seq": 1,
      "success": true,
      "observedValue": "0/0/3",
      "refd_mapping": "None",
      "root": "1>all",
      "group_ref": "root",
      "hierarchy": "root[0/0/3]"
    },
    {
      "variable": "description",
      "operation": "equals",
      "value": "blocks severity",
      "seq": 2,
```

合規性塊執行的結果

3. 驗證塊是否具有子層次結構或單個層次結構，並確保根據層次結構配置規則。

1

Key \*

bridge\_group

Filter Criteria

Expr \*

all

1

Key \*

BRIDGE\_GROUP\_NAME

Operation \*

Equals

Value \*

MOB\_22BT\_42RW\_IPA001

Rules

Expr \*

all

1

Key \*

BRIDGE\_GROUP\_NAME

Operation \*

Equals

Value \*

MOB\_22BT\_42RW\_IPA001

2

Key \*

bridge\_domain

Filter Criteria

Expr \*

all

1

Key \*

BRIDGE\_DOMAIN\_NAME

Operation \*

Equals

Value \*

MOB\_22BT\_42RW\_IPA001

+

-

Rules

Expr \*

all

1

Key \*

vfi

+

-

Filter Criteria

Expr \*

all

1

Key \*

VFI\_NAME

Operation \*

Equals

Value \*

MOB\_22BT\_42RW\_IPA001

+

-

合規性塊執行的結果

4. 通過運行以下python指令碼，驗證TTP解析器是否正在從裝置配置中提取值：

```

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)
```

## 監控合規性日誌

### 單節點環境:

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

### 多節點Kubernetes環境:

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

### Kibana Logs Monitoring:

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

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。