

BPAユーザガイド設定のコンプライアンスと修復v5.1

- [はじめに](#)
- [最新情報](#)
 - [コンポーネント](#)
- [前提条件](#)
- [コンプライアンスダッシュボード](#)
 - [設定準拠フロー図](#)
 - [資産コンプライアンスの概要](#)
 - [アセットコンプライアンスのためのCSVファイルの詳細](#)
- [資産準拠のためのCSVファイルのオープンと使用](#)
 - [違反の詳細の表示](#)
 - [是正構成の表示と比較](#)
 - [ポリシー準拠の概要](#)
 - [ポリシー準拠用にCSVとしてエクスポート](#)
 - [ポリシー準拠用のCSVファイルの詳細](#)
 - [ポリシー準拠のためのCSVファイルのオープンと使用](#)
- [レポート](#)
 - [レポートダッシュボード](#)
 - [レポート設定](#)
 - [レポートの生成](#)
 - [レポートのダウンロードと表示](#)
 - [設定準拠性の概要レポートについて](#)
 - [レポートの削除](#)
- [コンプライアンスジョブ](#)
 - [主な特長](#)
 - [コンプライアンスジョブの作成](#)
- [オフライン監査ジョブの作成](#)
 - [コンプライアンス・ジョブの編集](#)
- [今すぐ実行またはコンプライアンスジョブの再実行](#)
 - [コンプライアンスジョブの削除](#)
 - [コンプライアンスジョブの終了](#)
 - [コンプライアンスジョブの履歴](#)
- [修復ジョブ](#)
 - [設定修復のフロー図](#)
 - [是正ジョブリスト](#)
 - [是正ジョブの作成および編集](#)
 - [修復実行：デバイスのリスト](#)
- [設定：ブロックとルール](#)
 - [ブロックの機能](#)
 - [ルールの機能](#)
 - [ブロックライフサイクルとの統合](#)

- [リストブロック](#)
 - [機能ブロックの詳細](#)
- [ブロックとルールの追加または編集](#)
- [Ignore Line構文の使用](#)
- [違反の発生](#)
- [ルール管理](#)
 - [ルールの詳細の追加または編集](#)
 - [ルール違反の追加または編集](#)
- [動的なユーザ定義ブロック – ベストプラクティス](#)
- [ルールおよび非RefDルールにおけるルール階層および参照先統合の理解](#)
- [参照先統合](#)
 - [コンプライアンスルール値の構文](#)
 - [変数のタイプ](#)
 - [非参照D規則](#)
 - [変数の使用](#)
 - [実行](#)
 - [ブロックの詳細の表示](#)
 - [ブロックの削除](#)
- [設定：自動ブロック生成](#)
 - [自動ブロック生成](#)
- [ブロック識別子](#)
 - [リストブロック識別子](#)
 - [ブロックIDを作成または編集](#)
- [設定：ポリシー](#)
 - [ポリシーの一覧表示](#)
 - [ポリシーの追加と編集](#)
 - [ポリシーの詳細](#)
 - [ブロックを選択ダイアログ](#)
 - [条件付きフィルタ](#)
 - [Remediationセクション](#)
 - [GCT機能の自動生成](#)
- [ロールとアクセスコントロール](#)
 - [静的なアクセス許可の一覧](#)
 - [定義済みロール](#)
 - [アクセスポリシー](#)
- [オフラインコンプライアンス](#)
 - [デバイスバックアップ設定の使用](#)
 - [コンプライアンスジョブでのオフライン監査作成機能の使用](#)
- [Ingesterによる構成の展開](#)
- [参考資料](#)
- [API ドキュメント](#)
- [トラブルシューティング](#)
 - [ダッシュボード](#)
 - [コンプライアンスジョブ](#)
 - [コンプライアンス規則](#)
 - [コンプライアンスログの監視](#)

はじめに

Configuration Compliance and Remediation(CnR)アプリケーションを使用すると、ネットワークオペレータは、構成ブロックから構成されたカスタム定義ポリシーのデバイス構成コンプライアンスチェックを実行できます。オペレータは、選択したデバイス構成からシステムを使用して、構成ブロックを手動で作成するか、自動的に生成します。ユーザは、これらのブロックに適用する規則を設定することもできます。この場合、規則の条件はRefDアプリケーションから取得した値から導出される可能性があります。オペレータは、スケジュールに従ってコンプライアンスチェックを簡単に実行したり、チェックを即座に開始したりできます。

直感的なダッシュボードを備え、コンプライアンス違反の包括的な概要を表示し、デバイスおよび構成ブロックレベルの概要と詳細なビューを提供します。

このアプリケーションには、コンプライアンス違反を処理するための堅牢な修復フレームワークが含まれています。このフレームワークでは、ゴールデンコンフィギュレーションテンプレート(GCT)とプロセステンプレートと呼ばれる設定テンプレートの両方であるワークフローとテンプレートを活用して、修復プロセスを合理化します。コンプライアンスチェックと同様に、修復タスクをスケジュールに従って実行するようにプログラムすることも、違反に迅速に対処するためにすぐにトリガーすることもできます。

次世代(次世代)ポータルコンプライアンスと修復ダッシュボードには、ネットワークセキュリティ管理を強化し、コンプライアンス手順を合理化し、修復アクティビティを簡素化するように設計された機能があります。このダッシュボードには、資産およびポリシーのコンプライアンスに関する包括的なサマリーが表示されます。これにより、ネットワークオペレータはネットワークの健全性を簡単に評価し、デバイスが厳密なセキュリティプロトコルに準拠していることを確認できます。

構成ブロックは自動的に生成し、手動で編集または追加できるため、自動化とカスタマイズのバランスを取ることができます。従来のインターフェイスと最新のインターフェイスの間でユーザ、グループ、およびアクセス許可の詳細な設定を含め、システムが構成ブロックを正確に特定し、きめ細かいアクセス制御メカニズムを使用することで、ネットワーク構成の安全性と信頼性の高い担当者による保護を維持できます。これらの機能は、高度なネットワークコンプライアンスとセキュリティ標準の維持を検討している組織に強力なツールセットを提供します。

最新情報

次の主要機能と拡張機能が導入されました。

- コンプライアンスレポートを生成、表示、ダウンロードできる包括的なレポートダッシュボード

- Asset Managerを使用してデバイスをオンボーディングせずにデバイス設定をアップロードすることで、オフラインでコンプライアンス監査を実行できる
- ブロック設定でパターンを設定し、機密のデバイス設定データをマスクする機能
- ポリシーおよび資産準拠概要グリッドデータをCSVファイルとしてエクスポートする機能
- 生成された修復設定を表示し、デバイスの実行設定と比較する
- 設定が存在する場合に違反を発生させることをサポートするブロックの機能拡張
- ポリシーの作成および編集ページで接続されたユーザエクスペリエンスを有効にし、ブロック作成ページなどの子コンポーネントを相互起動する
- コンプライアンスジョブの機能強化によるページの作成と編集によるポリシー編集ページの相互起動

コンポーネント

コンプライアンスと修復は、次のコントローラとデバイスタイプをサポートします。

コントローラ	OS Types
nso (6.5)	IOS XE、IOS XR、NX-OS、JunOS、Nokia SR-OS
CNC(6.0)	IOS XE、IOS XR、NX-OS
NDFC (3.2.0/ファブリックv12.2.2)	NX-OS
Cisco Catalyst Center(2.3.5)	IOS XE、IOS XR検証済みコンプライアンスのみ
FMC (7.2.5)	FX-OS(FTD)。 検証済みコンプライアンスのみ
デバイスへの直接接続(D2D)	IOS XE、IOS XR、JunOS

 注: NSOコントローラ経由のNokia SR-OSサポートは、設定コンプライアンス機能にのみ適用されます。修復はNokiaデバイスではサポートされていません。

 注: コンプライアンス機能は、JuniperおよびNokiaデバイス用のシスココマンドラインインターフェイス(CLI)形式およびYAMLに類似した形式のデバイス設定で動作します。現在、フレームワークはNetconf、JSON、XMLなどの他の形式をサポートしていません。

v5.0リリースの一部として、Compliance and Remediation(CnR)クラシックアプリケーションは廃止されました。すべてのCnR機能が完全に統合され、次世代ポータルで使用できるようになりました。

前提条件

CnRの使用例を効果的に使用するには、次の前提条件が必要です。

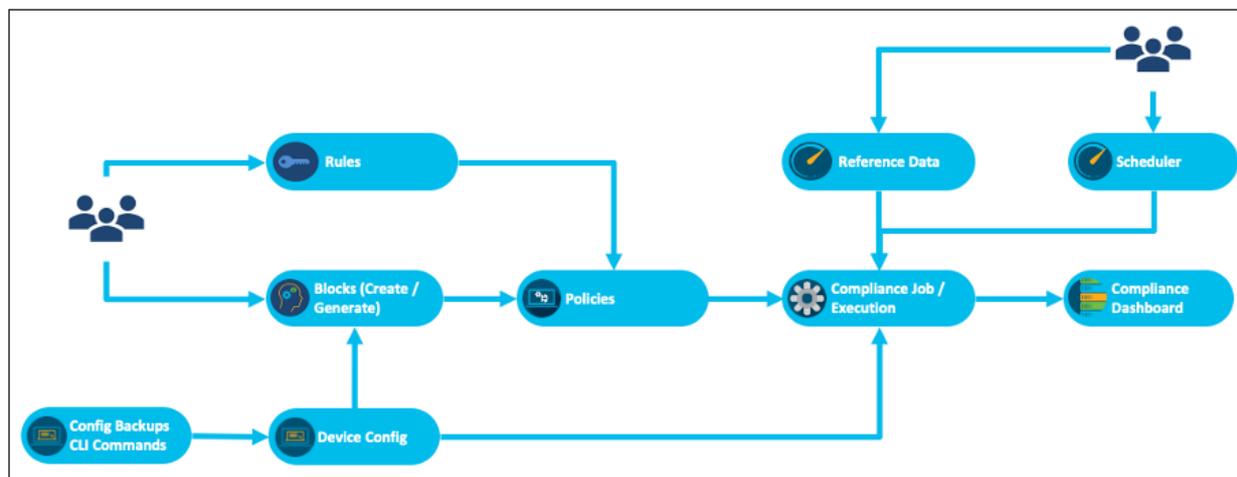
- CnRユースケースのサブスクリプション権限キーをアップロードする必要があります。
- 関連するコントローラとデバイスはオンボーディングされ、BPA Asset Managerの一部として使用できる必要があります。詳細については、『[BPAユーザガイド](#)』の「アセットマネージャ」セクションを参照してください。
- オンボーディングされた資産は、顧客要件に従ってNext-Gen Portalの資産グループにグループ化する必要があります。

コンプライアンスダッシュボード

コンプライアンスダッシュボードには、選択した期間におけるすべてのデバイスの違反の概要が表示されます。デフォルトでは、現在の月のデータが表示されます。ユーザーは、タイム・ウィンドウを変更して、コンプライアンス違反に関する履歴データを表示できます。現在の月がデフォルトの選択ビューです。

 注：クラシックUIの廃止されたコンプライアンスダッシュボードは削除され、使用できなくなりました。次世代ポータルで利用可能なダッシュボードを使用する必要があります。

設定準拠フロー図



構成コンプライアンスコンポーネントの概要

ダッシュボードに表示されるコンプライアンス違反は、資産のリストに対してポリシーのコンプライアンスジョブが実行されたときに入力されます。コンプライアンスポリシーは、必要なコンプライアンスルールとともにブロック設定のリストを追加して作成します。コンプライアンスルールには、RefDアプリケーションからデータをフェッチする静的値または動的変数を使用したチェックを含めることができます。コンプライアンスジョブは、オンデマンドで実行することも、1回限りのスケジュールまたは繰り返しのスケジュールとして実行することもできます。

設定のコンプライアンスには、次の重要な機能が含まれます。

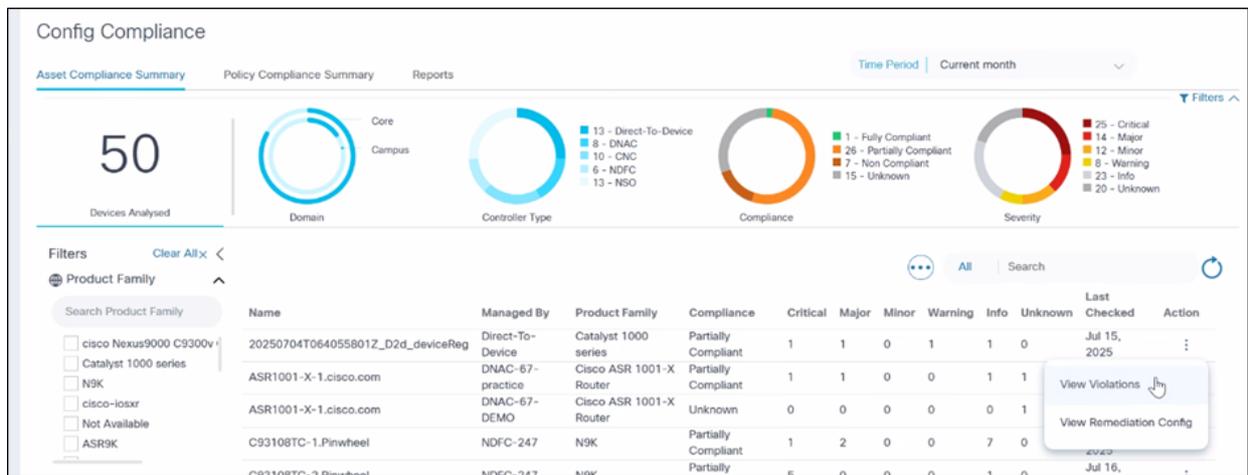
- ブロックの作成：ブロックは手動で作成されるか、テンプレートテキストパーサー(TTP)テンプレートを使用して自動的に生成されます。スタティックまたはダイナミック（変数を使用）にすることができます。
- ルールの作成：ルールはブロック内の変数を検証します。ルール値は静的に設定することも、実行時に参照データ(RefD)システムから動的に取得することもできます。
- ポリシーの作成：ブロックのリストと対応するルールを選択して、ポリシーを作成します。ルールのデータは、実行時に動的にRefDフレームワークからフェッチされた静的データです。
- コンプライアンスジョブの作成：コンプライアンスジョブは、ポリシーと資産グループ（資産のリストを含む）を選択してコンプライアンスチェックを実行することによって作成されます。ユーザは、バックアップフレームワークからデバイス設定を取得するか、実行中にデバイス上のプロセステンプレートを使用してライブコマンドを実行するかを選択できます。バックアップから設定を取得すると、ライブデバイスに接続する必要なく、デバイスのオフライン監査に役立ちます。ジョブは、スケジュール設定することも、オンデマンドで実行することもできます。
- コンプライアンス違反：ダッシュボードでコンプライアンス違反を表示します。

資産コンプライアンスの概要

Asset Compliance Summaryタブは、ネットワーク内のすべてのデバイスのコンプライアンス違反の包括的な概要を提供するために設計された重要な機能です。このタブでは、コンプライアンスの問題を迅速に特定し、すべてのデバイスが確立されたポリシーと標準に準拠していることを確認できます。このインターフェイスには強力なフィルタリング機能と検索機能が搭載されており、コンプライアンスデータのナビゲートと分析が容易です。

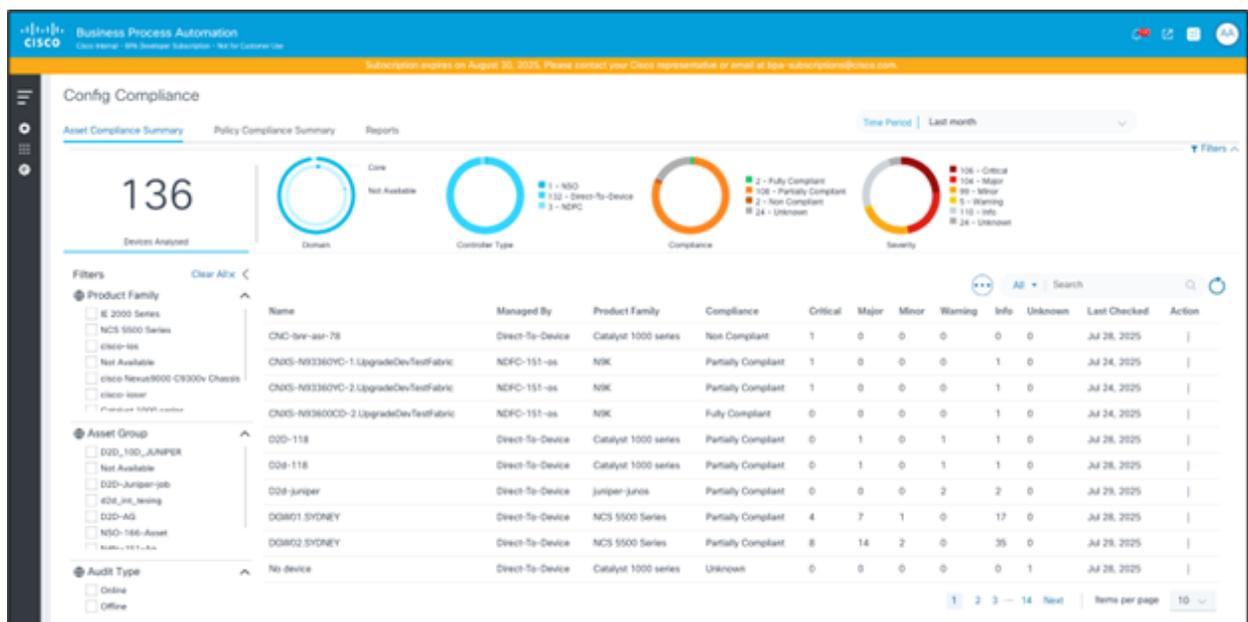
主な特長

- デバイスごとの違反の概要：このタブには、各デバイスのコンプライアンス違反の概要が表示されます。重大、高、中、低などの重大度レベルによって分類された全体的なコンプライアンスステータスの簡単なスナップショットがユーザに提供されます。
- 詳細な違反情報：各デバイスのポップアップウィンドウに、違反したポリシーの詳細情報が表示され、違反の原因となったブロックと設定行にさらにドリルダウンできます。



資産準拠の概要の表示

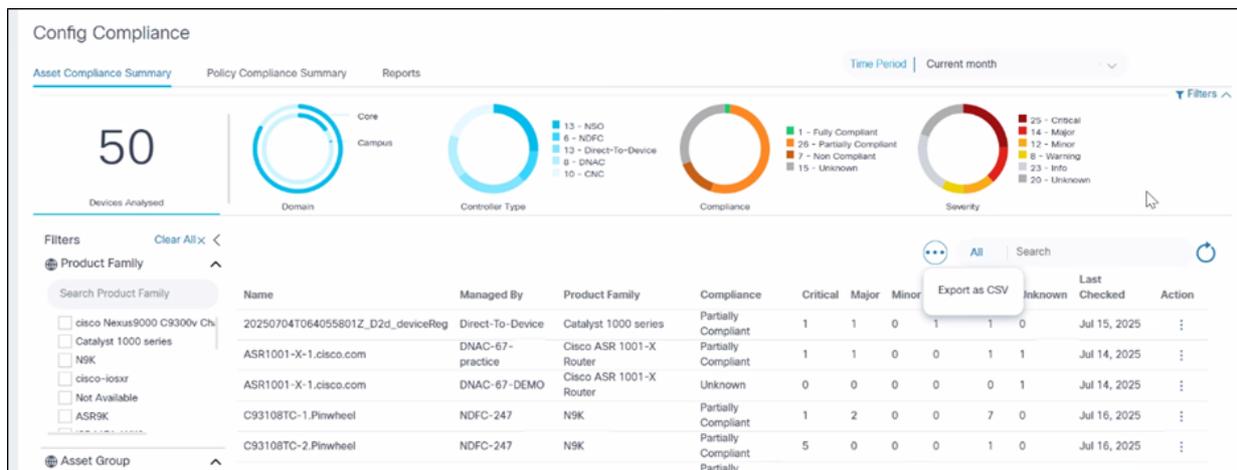
- 高度なフィルタリングオプション：タブの左上にあるフィルタを使用すると、グリッドに表示されるデータを絞り込むことができます。ユーザーは、日付範囲、資産グループ、製品ファミリーなどを基準にフィルタを適用して、コンプライアンスデータを集中的に分析できます。
- 検索機能：検索フィールドを使用して、グリッド内のデータをさらに絞り込むことができます。ユーザーは、関連するキーワードやフレーズを入力して、特定のデバイスをすばやく見つけたり、コントローラで管理したりできます。
- カスタマイズ可能な日付範囲：デフォルトでは、日付範囲フィルタで現在の月が選択され、最新のコンプライアンスデータが表示されます。ただし、データを表示するように日付範囲をカスタマイズできます。
- フィルタ：製品ファミリー、資産グループ、監査タイプなど、複数のフィルタを使用できます。フィルタを適用してグリッドをリフレッシュします。



資産コンプライアンスの概要

- CSVとしてエクスポート：オフライン分析、レポート、アーカイブの目的で、資産構成コンプライアンスのローカルコピーを取得するのに役立つ機能です。データをCSVファイルとし

てエクスポートするには、More OptionsアイコンからExport as CSVを選択します。ダウンロードしたCSVファイルには、適用されているフィルタに従ってグリッドに現在表示されているデータが含まれています。



資産準拠の概要：CSV形式でエクスポート

アセットコンプライアンスのためのCSVファイルの詳細

CSVファイルには、デバイス名、コントローラインスタンス(管理者)、デバイスの製品ファミリー、デバイスのコンプライアンスステータス、重大度別の違反数(クリティカル、メジャー、マイナー、警告、情報、不明など)、デバイスのコンプライアンスが最後にチェックされた日付など、資産準拠の概要グリッドに表示されるすべての列が含まれます。

グリッドにページ区切りがある場合、エクスポートには表示されているページだけでなく、ページをまたぐすべてのレコードが含まれます。

資産準拠のためのCSVファイルのオープンと使用

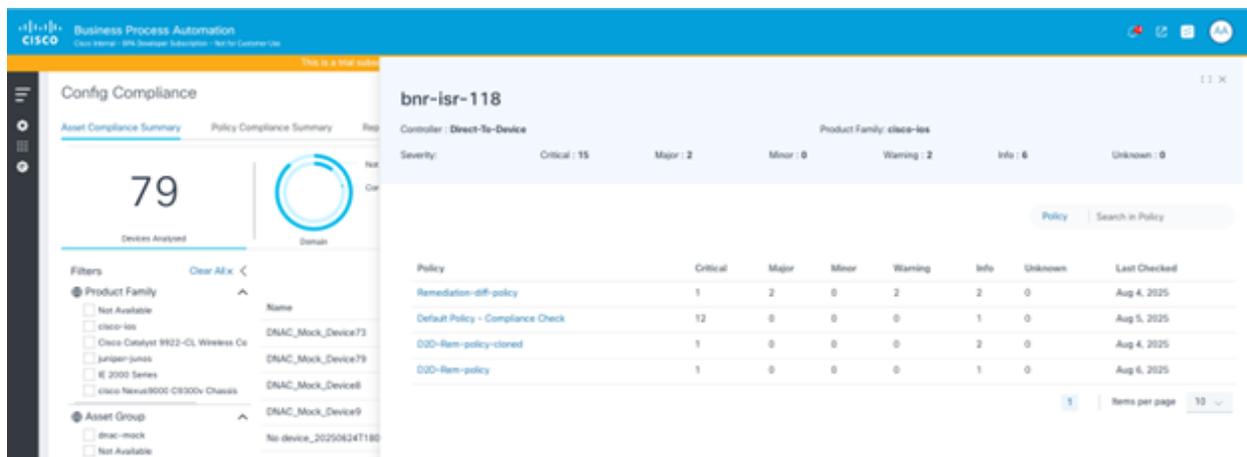
1. ダウンロードしたCSVファイルをExcelまたは互換性のあるスプレッドシートアプリケーションで開きます。
2. フィルタリングされた結果を含め、コンテンツが資産準拠サマリーグリッドに表示されている内容と一致していることを確認します。

	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	0	1	1	04-Aug-25
4	D2d-juniper	Direct-To-Device	juniper-junos	Partially Compliant	0	0	0	0	2	2	06-Aug-25
5	DNAC_Mock_Device0	DNAC-Mock	Cisco Catalyst 9922-CL Wireless Controller for Cloud	Unknown	0	0	0	0	0	0	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	0	2	6	06-Aug-25
8	bnr-n3k-44	NSO-166	cisco Nexus9000 C9300v Chassis	Partially Compliant	12	0	0	0	0	3	05-Aug-25
9											

資産準拠の概要：CSVファイルをExcelアプリケーションで開く

ポリシー別の資産準拠サマリーの表示

[Asset Compliance Summary]グリッドの行をクリックすると、デバイスが検証されるさまざまなポリシーによって分類された資産違反の詳細が表示されます。これは、ユーザが各ポリシーの重大度ごとの違反数を表示するための詳細なビューとして機能します。



資産コンプライアンスの概要：ポリシー別コンプライアンスサマリー



注：次の点に注意してください。

- [ポリシー]列のハイパーリンクをクリックすると、ポリシーの詳細ページに移動します
- 行をクリックすると、選択したポリシーの違反の詳細ページが表示されます。

違反の詳細の表示

Violation Detailsページには、デバイス設定にオーバーレイされたブロックレベルおよびルールレベルの違反が表示されます。また、ユーザはブロック設定と推奨される修復設定を表示することもできます。

ポリシーレベルの分割とともに「資産準拠概要」ページから「違反詳細」ページを表示するには、次の手順に従います。

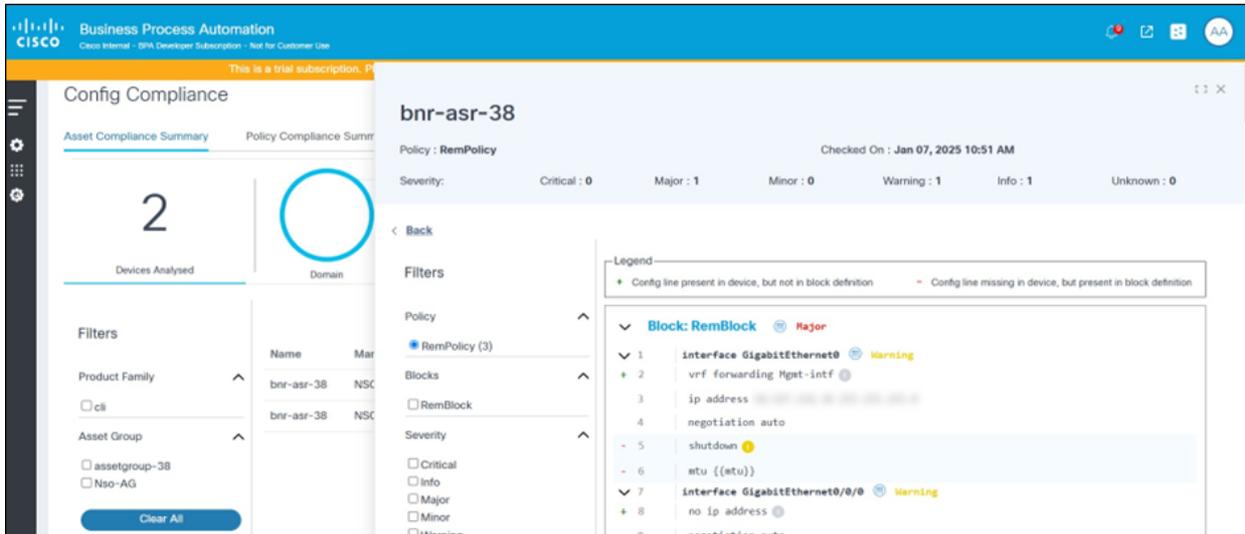
1. 資産準拠グリッドで行を選択します。ポップアップが表示されます。グリッドには、コンプライアンスの詳細がポリシー別に分割されて表示されます。
2. グリッドで行を選択します。「違反の詳細」ページが表示されます。

ポリシーコンプライアンスサマリグリッドから違反の詳細ページを表示するには、次の手順を実行します。

1. Policy Compliance Gridを選択します。
2. 行を選択し、影響を受けるアセットグリッドを選択します。

3. 行を選択します。「違反の詳細」ページが表示されます。

Violations Detailsページの右側には、デバイス設定ブロックが表示され、その上に違反がオーバーレイされます。違反は、対応する設定行に対して一覧表示されます。条件が満たされない場合、違反リボンには、規則名、条件、および（規則で定義されている）予期される設定と、デバイス設定から取得された設定の比較に関する詳細が表示されます。



資産コンプライアンス違反

ブロックシンボル

- 行に対する「+」記号は、ブロック設定に従って設定が行われるのではなく、デバイス設定に追加で存在することを意味します。
- 行に対する「-」記号は、ブロック設定に従って設定されることが予期されますが、デバイス設定には含まれません。

フィルタ

ページの左側にあるフィルタセクションでは、次のアクションを実行できます。

- ポリシーを変更します。ページが更新され、新しく選択したポリシーの違反がロードされます。
- Blocksチェックボックスをオンにすると、選択したブロックに関連する違反が表示されます
- 指定された重大度レベルの違反を表示するには、重大度のチェックボックスをオンにします
- 選択したタイプの違反を表示するには、「違反タイプ」チェックボックスをオンにします。
 - 注文の不一致：デバイス構成行の注文が、ブロック構成で定義されている注文と一致しません
 - Missing Config：ブロック設定に従って必要だが、デバイス設定に含まれていない設定行を表示します。
 - 追加設定：ブロック設定では予期されないが、デバイス設定に追加されている設定行

を表示します。

- 。 ルールの失敗：ルール内の1つ以上の条件の失敗。
- 。 Missing Blocks：デバイス設定ブロック全体が欠落しているか、定義されているブロック設定と一致していません。
- 。 スキップされたブロック：ブロックフィルタ条件が満たされていないため、この構成ブロックはスキップされます。

是正構成の表示と比較

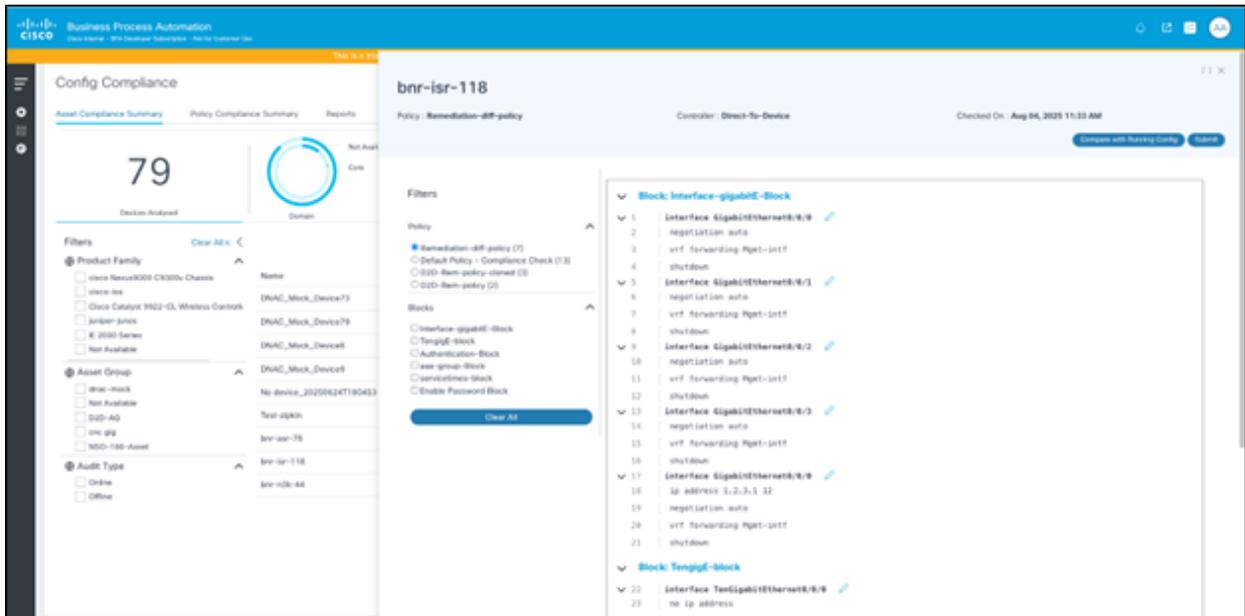
Remediation Configページには、特定のポリシーの各ブロックについて、選択したデバイス用に生成された設定が表示されます。設定が生成され、ポリシーに存在するブロックとルールの詳細、およびコンプライアンスの実行中に取得されたデバイス設定が考慮されます。ユーザは、同じページで設定を更新することもできます。この生成された設定は、修復ジョブ機能を使用してデバイスにプッシュできます。また、このページには、生成された設定を現在のデバイスの実行コンフィギュレーションと比較するオプションがあります。ユーザは、現在のデバイス設定を取得する1つ以上のコマンドを指定できます。

Asset ComplianceグリッドでRemediation Configページを表示するには、次の手順に従います。

1. Asset Compliance Summaryタブをクリックします。
2. Action列のasset complianceグリッドで、More Options icon > View Remediation Configの順に選択します。Remediation Configページが表示されます。

ポリシーコンプライアンスグリッドから修復設定ページを表示するには、次の手順を実行します。

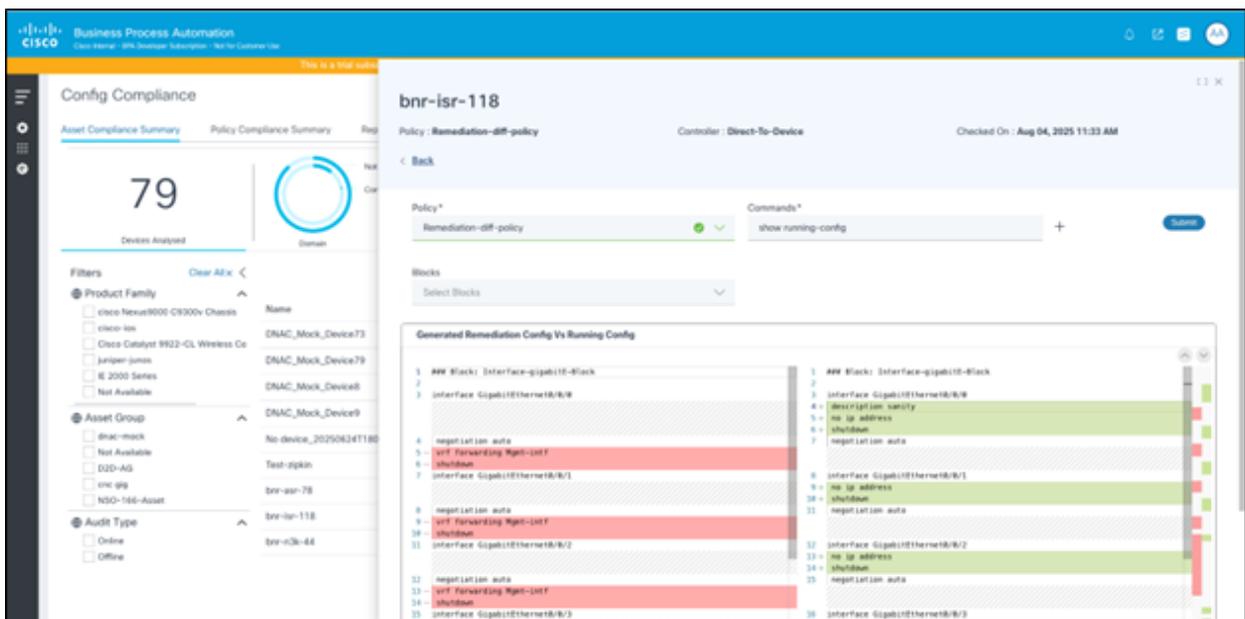
1. Policy Compliance Summaryタブをクリックします。
2. ポリシーコンプライアンスグリッドで、目的の行を選択します。影響を受けるアセットグリッドが表示されます。
3. Action列で、More Optionsアイコン> View Remediation Configの順に選択します。Remediation Configページが表示されます。



修復構成ページ

Remediation Configページには次の情報が表示されます。

- 生成された是正構成：生成された構成がページの右側に表示され、ユーザが構成ブロックを編集して保存する変更を送信するためのオプションも表示されます
- フィルタ：フィルタを使用してポリシーを選択し、オプションで1つ以上のブロックを選択して、対応する生成済み設定を表示できます
- Compare with Running Config: Compare with Running Configをクリックすると詳細ページが表示され、生成された設定とデバイスの実行コンフィギュレーションを比較できます



「Running Config」ページとの比較

Compare with Running Configページには、次の情報が表示されます。

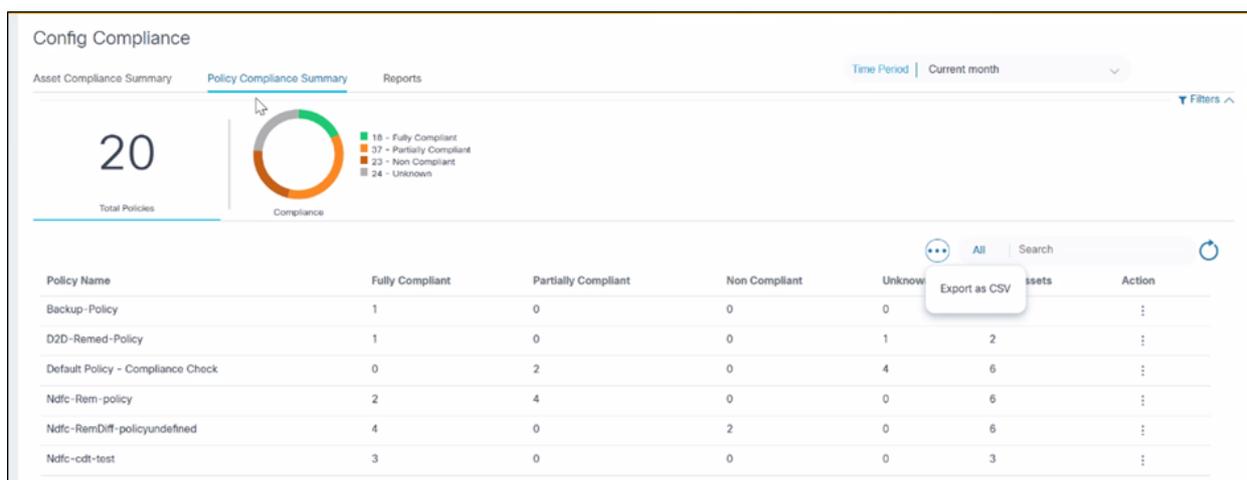
- ポリシーを選択するオプション：前のページで選択したポリシーが事前に選択されています。
- デバイスで実行する1つ以上のコマンドを入力するテキストボックス
- Submitボタン：デバイスでコマンドを実行し、設定を取得します。
- ブロックを表示およびフィルタするオプション：デフォルトでは、ポリシー内のすべてのブロックが表示されます。必要に応じて個々のブロックを選択できます
- Config Diff Viewer：生成された構成とデバイス構成を並べて表示し、相違点を強調表示します。

ポリシー準拠の概要

Policy Compliance Summaryタブには、定義済みのポリシーに対するデバイスのコンプライアンスステータスがわかりやすく簡潔に表示されます。このタブでは、コンプライアンス状況を迅速に評価し、問題のある領域を特定できます。このタブでは、コンプライアンスのステータスに基づいてデバイスが分類されるため、コンプライアンスを簡単に理解して管理できます。

準拠ステータス：

- 完全準拠：すべてのデバイスが、それぞれのポリシーに関するすべてのコンプライアンスルールを満たしています。
- 部分的な準拠：一部のデバイスはルールに準拠していますが、他のデバイスはルールに準拠していません。
- 非準拠：ポリシーに準拠するデバイスはありません。
- Unknown：ネットワーク接続に問題があるか、バックアップが利用できないため、ポリシーの適合性を確認できません。



CSVエクスポートによるポリシー準拠の概要

ポリシー準拠用にCSVとしてエクスポート

CSV形式でエクスポート機能を使用すると、オフラインでの分析、レポート、アーカイブを目的として、ポリシー準拠のローカルコピーを取得できます。データをCSVファイルとしてエクスポートするには、More OptionsアイコンからExport as CSVを選択します。ダウンロードしたCSVファイルには、適用されているフィルタに従ってグリッドに現在表示されているデータが含まれています。

ポリシー準拠用のCSVファイルの詳細

CSVファイルには、ポリシー名、検証された資産の合計数、コンプライアンスのステータス（完全準拠、一部準拠、非準拠、不明など）別の合計数が含まれます。グリッドにページ区切りがある場合、エクスポートには、現在のページに表示されているレコードだけでなく、すべてのページのすべてのレコードが含まれます。

ポリシー準拠のためのCSVファイルのオープンと使用

1. ダウンロードしたCSVファイルをExcelまたは互換性のあるスプレッドシートアプリケーションで開きます。
2. フィルタ処理された結果を含め、コンテンツがポリシー準拠概要グリッドに表示されている内容と一致していることを確認します。

	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						

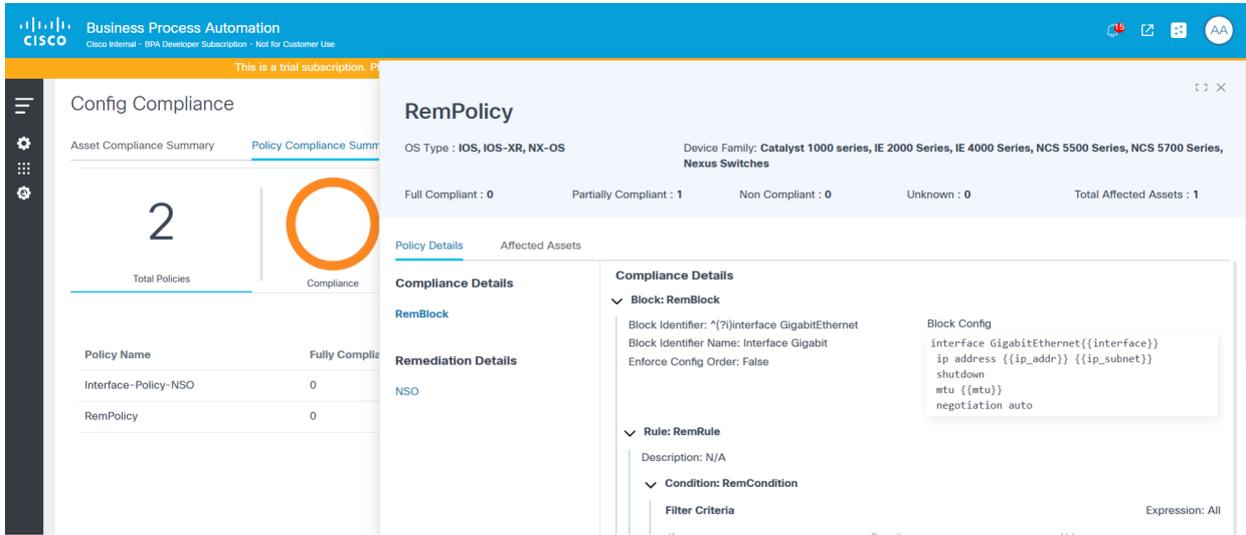
ポリシーのコンプライアンス：ポリシーの詳細

ポリシーの詳細の表示

ポリシーの詳細を表示するには

1. Actionカラムの下にあるMore Optionsアイコンからポリシーを選択します。
2. View Policy Detailsを選択します。Policy Detailsページが表示されます。

 注意: 「ポリシーの詳細」ページは、ブロック、ルールおよび条件を含むすべてのポリシー情報の読取り専用ビューです。ユーザーは、ページ内のハイパーリンクをクリックして、関連するブロックに直接移動できます。



The screenshot shows the Cisco Business Process Automation interface. The main content area is titled 'RemPolicy' and displays compliance information for 'OS Type: IOS, IOS-XR, NX-OS' and 'Device Family: Catalyst 1000 series, IE 2000 Series, IE 4000 Series, NCS 5500 Series, NCS 5700 Series, Nexus Switches'. The compliance status is shown as 'Full Compliant: 0', 'Partially Compliant: 1', 'Non Compliant: 0', 'Unknown: 0', and 'Total Affected Assets: 1'. The 'Policy Details' section shows 'Block: RemBlock' with 'Block Identifier: ^(?:)interface GigabitEthernet' and 'Block Identifier Name: Interface Gigabit'. The 'Rule: RemRule' section shows 'Description: N/A' and 'Condition: RemCondition' with 'Filter Criteria' and 'Expression: All'. A 'Block Config' window is open, showing the configuration for 'interface GigabitEthernet' with 'ip address', 'shutdown', 'mtu', and 'negotiation auto'.

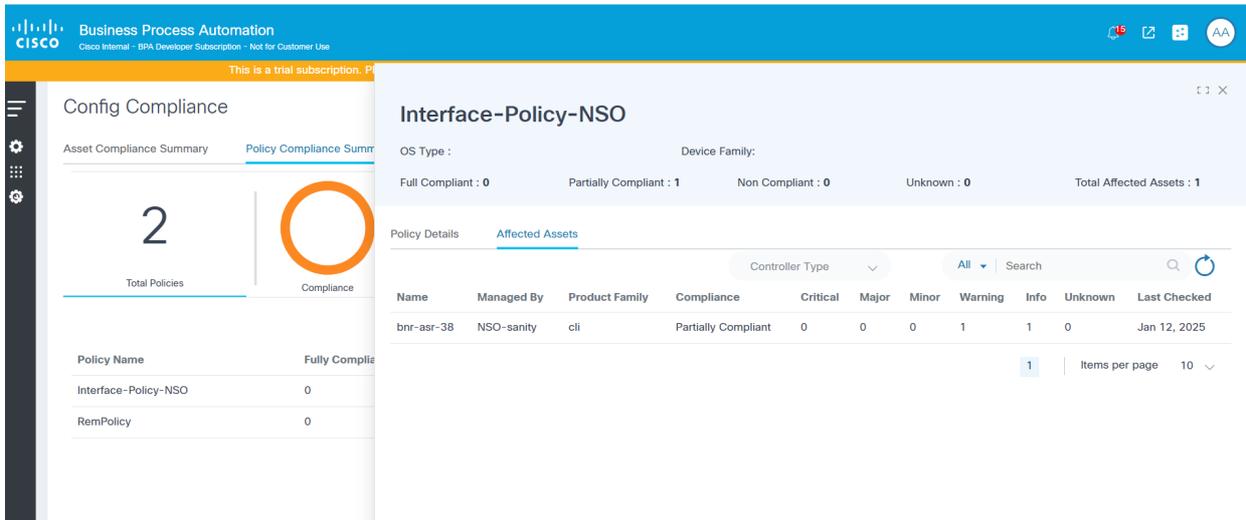
ポリシーのコンプライアンス：ポリシーの詳細

影響を受ける資産の表示

影響を受ける資産タブには、各ポリシーで分析された資産のリストと、重大度で分割された違反数が表示されます。デバイスをフィルタリングするには、Controller Type ドロップダウンリストと検索ボックスを使用します。

Policy Compliance Summary タブから Affected Assets を表示するには、次の手順に従います。

1. 行を選択します。コンプライアンスポリシーウィンドウが開きます。
2. Affected Assets タブをクリックします。



The screenshot shows the Cisco Business Process Automation interface. The main content area is titled 'Interface-Policy-NSO' and displays compliance information for 'OS Type:' and 'Device Family:'. The compliance status is shown as 'Full Compliant: 0', 'Partially Compliant: 1', 'Non Compliant: 0', 'Unknown: 0', and 'Total Affected Assets: 1'. The 'Affected Assets' tab is active, showing a table of affected assets. The table has columns for Name, Managed By, Product Family, Compliance, Critical, Major, Minor, Warning, Info, Unknown, and Last Checked. The table contains one row: 'bnr-asr-38', 'NSO-sanity', 'cli', 'Partially Compliant', '0', '0', '0', '1', '1', '0', 'Jan 12, 2025'. The 'Items per page' is set to 10.

 注: 「影響を受ける資産」タブには、「違反詳細の表示」ページおよび「是正構成の表示」ページを開くためのアクションがあります。詳細については、「資産準拠の概要」を参照してください。

レポート

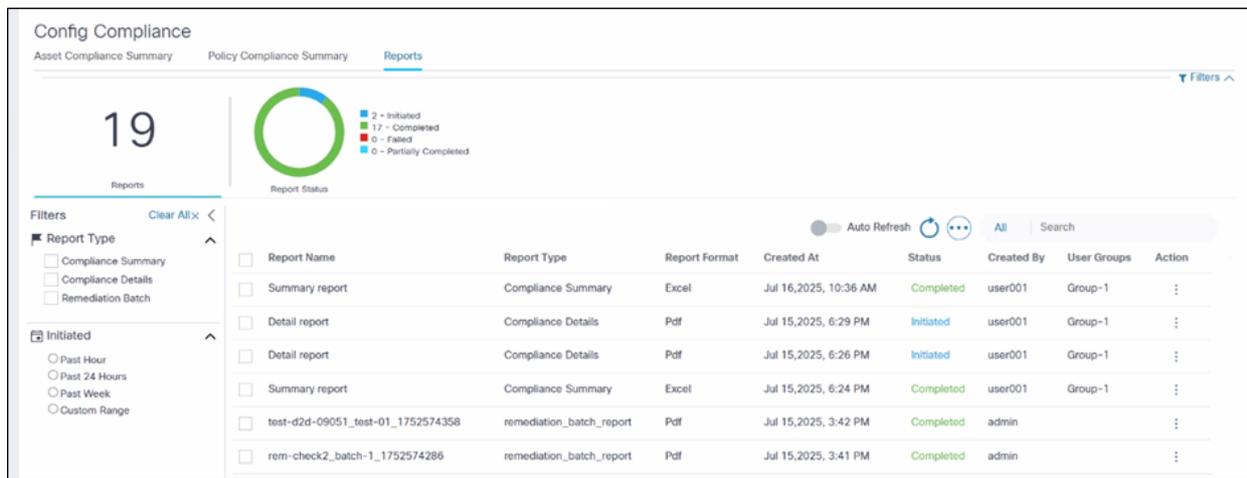
レポートセクションは、デバイスのコンプライアンスに関する包括的な洞察を提供し、違反を特定して、修復の取り組みを促進するように設計されています。このアプリケーションは、さまざまなタイプのコンプライアンスレポートを生成、表示、ダウンロード、および管理するための使いやすいインターフェイスを提供します。

レポートダッシュボード

レポートダッシュボードは、すべてのコンプライアンスレポートアクティビティの中央ハブとして機能します。ユーザは、この単一のインターフェイスからレポートを効率的に管理できます。レポートダッシュボードで使用できる主な機能は次のとおりです。

- レポートの表示：ユーザは、生成されたすべてのレポートのリストを表示できます。これには、名前、タイプ、関連付けられたポリシー、形式、作成日、および現在のステータス（開始、完了、失敗、一部完了など）が含まれます
- レポートのダウンロード：レポートは生成後、オフライン分析またはアーカイブの目的でダウンロードできます。[アクション]列には、ダウンロードのオプションが表示されます
- レポートの削除：古いレポートや不要なレポートをダッシュボードから削除できるため、整理されたクリーンなレポート環境を維持できます
- フィルタリングと検索：ダッシュボードには豊富なフィルタリングオプションが用意されており、レポートタイプ（コンプライアンスの詳細、コンプライアンスの概要、修復バッチなど）、ポリシー、開始ステータス（過去1時間、過去24時間、過去1週間、カスタム範囲など）に基づいて、特定のレポートをすばやく見つけることができます。検索バーも使用できます
- レポートステータスマonitoring：レポートのステータスを視覚的に示すサマリー（円グラフなど）で、開始、完了、失敗、または部分的に完了したレポート数が表示されます。

レポートダッシュボードは、「コンプライアンスと是正」ダッシュボードの「レポート」タブのランディングページです。



レポートダッシュボード

- 使用可能なレポートタイプは次のとおりです。
 - コンプライアンスサマリーレポート
 - コンプライアンス詳細レポート
 - 是正バッチレポート
- フィルタを使用して、次の項目を選択します。
 - レポートの種類
 - ポリシー
 - 開始期間 (選択した期間に基づいてレポート・ リストがフィルタされます)
- レポートリストを自動更新するオプション

レポート設定

レポート構成を使用すると、管理者は、導入およびビジネス要件に基づいて、レポートに関連する主要なパラメータを構成できます。設定には次のパラメータを使用できます。

- 次より古いレポートの自動削除 (日) : この期間より古いレポートはすべてシステムから削除されます
- コンプライアンスサマリーレポートでポリシーごとに選択される最大ブロック数:Excelファイル内のタブ数を読み取り可能な制限に保ちます
- コンプライアンス詳細レポートで選択される最大資産 : 特定の詳細レポートに生成されるPDFファイルの数を制限できます。

コンプライアンスジョブリスト

レポートの生成

このアプリケーションには、新しいコンプライアンスレポートを生成するための専用インターフェイスが用意されており、ユーザはレポートタイプの選択、範囲の定義、および特定のフィルタ

の適用を行うことができます。レポート生成プロセスは、「レポートダッシュボード」ページの「レポートの生成」アクションから開始されます。

レポート生成の主な特徴は次のとおりです。

- レポート・タイプの選択：次の異なるレポート・タイプから選択できます
 - サマリーレポート：選択したポリシーのすべてのデバイスのコンプライアンスの概要が表示されます。
 - 詳細レポート：各デバイスの特定の違反に関する詳細な情報を提供し、より詳細なビューを提供します。
- レポートの命名：生成されたレポートに関連する名前を指定する必要があります
- 期間の選択: 「今月」やカスタム範囲など、特定の期間に関するレポートを生成して、最新のコンプライアンスデータに焦点を当てることができます
- フィルタの適用：包括的なフィルタリングオプションにより、レポートの範囲を絞り込むことができます
 - ポリシー：レポートに含める1つ以上のコンプライアンスポリシーを選択します。ポリシーの選択は必須です
 - ブロック：選択したポリシー内で、レポートに含める特定の設定ブロックを選択します。ブロック選択はオプションです
 - 資産グループ：ユーザーは、1つ以上の資産グループを選択して、範囲内の資産をフィルタできます
- 資産選択：詳細レポートにのみ適用されます
 - ユーザーは、レポートを生成する対象となる特定のデバイスを選択できます
 - 資産テーブルには、名前、シリアル番号、IPアドレス、管理者、現在のコンプライアンスステータスなどの詳細が、異なる重大度レベルのカウントとともに表示されます

コンプライアンスサマリーレポートを生成するには、次の手順に従います。

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	Partially Compliant	12	0	0	0	1	0	May 28, 2025, 2:43 PM
bnr-asr-115	FXS1933027 N	10.197.215.11 5	Direct-To-Device	Partially Compliant	11	0	0	0	3	0	May 28, 2025, 2:43 PM

サマリーレポートの生成

1. Select Report Type ドロップダウンリストで、Summary Reportを選択します。

- レポート名を入力します。
- 時間範囲を選択します。ポリシーとブロックは、この選択に基づいて一覧表示されます。
- ポリシーを選択します。追加のポリシーを選択することもできます。
- 必要に応じて、「ブロック」を選択します。何も選択しない場合は、すべてのブロックが含まれます。
- 必要な資産グループ、コンプライアンスステータス、および重大度レベルを選択します。
- [Generate Report] をクリックします。

- レポーターリストページでは、レポートステータスが開始済みに設定されます。
- 完了すると、ステータスがCompletedに変わります。一部のサブレポートが失敗すると、ステータスが部分的に完了に変わります
- レポート生成全体が失敗すると、通知が表示され、ステータスが「失敗」に変わります
- 完了すると、ダウンロードオプションが使用可能になります。ユーザは、Excelレポートを含むzipファイルをダウンロードできます

コンプライアンス詳細レポートを生成するには、次の手順に従います。

詳細レポートの生成

- Select Report Type ドロップダウンリストで、Detailed Report を選択します。
- レポート名を入力します。
- 時間範囲を選択します。ポリシーとブロックは、この選択に基づいて一覧表示されます。
- ポリシーを選択します。追加のポリシーを選択することもできます。
- 必要に応じて、「ブロック」を選択します。何も選択しない場合は、すべてのブロックが含まれます。
- 必要な資産グループ、コンプライアンスステータス、および重大度レベルを選択します。
- グリッドから必要なアセットを選択します。ユーザは、「すべてのデバイスを選択」および「選択したデバイスを表示」のオプションを使用できます。
- [Generate Report] をクリックします。

- レポーターリストページでは、レポートステータスが開始済みに設定されます。
- 完了すると、ステータスがCompletedに変わります。一部のサブレポートが失敗すると、ス

ステータスが部分的に完了に変わります

- レポート生成全体が失敗すると、通知が表示され、ステータスが「失敗」に変わります

レポートのダウンロードと表示

完了したレポートは、レポートダッシュボードグリッドの目的の行にあるダウンロードアイコンを使用してダウンロードできます。

設定準拠性の概要レポートについて

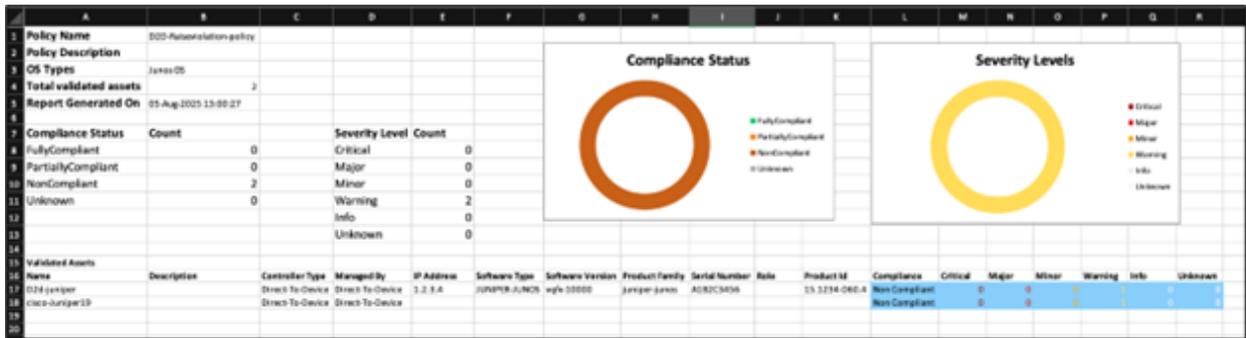
コンプライアンスサマリーレポートは、デバイスごとに1つのPDFが生成された個別のPDFレポートを含むzipファイルです。このレポートタイプでは、ポリシーごとのコンプライアンス違反の概要と、デバイスに対するブロックレベルのドリルダウンマッピング違反の詳細が示されます。

Report Name	Report Type	Report Format	Created At	Status	Created By	User Groups	Action
<input type="checkbox"/> Default Policy Report	Compliance Details	Pdf	Jul 16, 2025, 11:26 AM	Initiated	admin		⋮
<input type="checkbox"/> Summary report	Compliance Summary	Excel	Jul 16, 2025, 10:36 AM	Completed	user001	Group-1	⋮
<input type="checkbox"/> Detail report	Compliance Details	Pdf	Jul 15, 2025, 6:29 PM	Initiated	user001	Group-1	⋮
<input type="checkbox"/> Detail report	Compliance Details	Pdf	Jul 15, 2025, 6:26 PM	Initiated	user001	Group-1	⋮
<input type="checkbox"/> Summary report	Compliance Summary	Excel	Jul 15, 2025, 6:24 PM	Completed	user001	Group-1	⋮
<input type="checkbox"/> test-d2d-09051_test-01_1752574358	remediation_batch_report	Pdf	Jul 15, 2025, 3:42 PM	Completed	admin		⋮
<input type="checkbox"/> rem-check2_batch-1_1752574286	remediation_batch_report	Pdf	Jul 15, 2025, 3:41 PM	Completed	admin		⋮
<input type="checkbox"/> summary-report1	Compliance Summary	Excel	Jul 14, 2025, 7:27 PM	Completed	admin		⋮
<input type="checkbox"/> summary-report-user1	Compliance Summary	Excel	Jul 14, 2025, 7:07 PM	Completed	user001	Group-1	⋮
<input type="checkbox"/> juniper-detailed-report	Compliance Details	Pdf	Jul 14, 2025, 6:08 PM	Completed	admin		⋮

コンプライアンスサマリーレポート

各Excelレポートには次のシートが含まれ、次の情報が提供されます。

- ポリシーサマリ:
 - ポリシー名、説明、OSタイプ、検証済み資産合計などの概要の詳細
 - 検証済み資産数をコンプライアンス・ステータス（完全準拠、一部準拠、非準拠、不明など）別に表示するグリッドおよびチャート・ビュー
 - 違反総数を重大度レベルで分割したグリッドビューおよびグラフビュー（クリティカル、メジャー、マイナー、警告情報、不明など）
 - デバイスの詳細、コンプライアンスステータス、各重大度レベルの違反数を示す資産グリッド



ポリシーの概要シート

• ブロックの概要:

- ブロック名、説明、ブロック設定、ブロック識別子の詳細、ブロック違反の重大度設定などのブロックの詳細
- 特定のブロックに対する違反数、合格したルール、失敗したルール、検証されたアセット

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

ブロック概要シート

- ブロックごとのルールと違反の詳細 :
- 違反レベルグリッドには、ルール名、説明、違反名、説明の重大度レベル、資産全体で見られた違反の数、および影響を受ける資産の数のリストが表示されます
- デバイスレベルグリッドには、ルール、違反、重大度、デバイス名、コントローラ名 (管理者) のマッピングが表示されます

	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							

コンプライアンス詳細レポート

コンプライアンス詳細レポートには、次の情報が含まれます。

- レポート名：レポートの名前を示します。
 - 資産名：コンプライアンスチェックが実行されたデバイスを指定します
 - その他の資産詳細:IPアドレスやシリアル番号などの詳細（存在する場合）が含まれます。
 - 重大度：重大度レベル別の違反の要約数を示します。
 - レポート生成日：レポートが作成された時点のタイムスタンプを示します。
- 適用されるフィルタ：特定のレポートの生成に使用される特定のフィルタ基準の詳細の概要を示し、透明性と再現性を確保します。これには、期間、選択したポリシー、ブロック、重大度レベル、およびコンプライアンスステータスが含まれます
- ルールと違反の概要：評価された各ルールを一覧表示し、そのルールに対して検出された違反の概要を提供します。要約グリッドには、違反名、説明、重大度、この違反が発生した回数が表示されます
- Violation Details：選択したブロックの各デバイス設定行に関する詳細と、各行の違反の詳細を表示します

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

コンプライアンス詳細レポート – サンプルPDFページ1

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

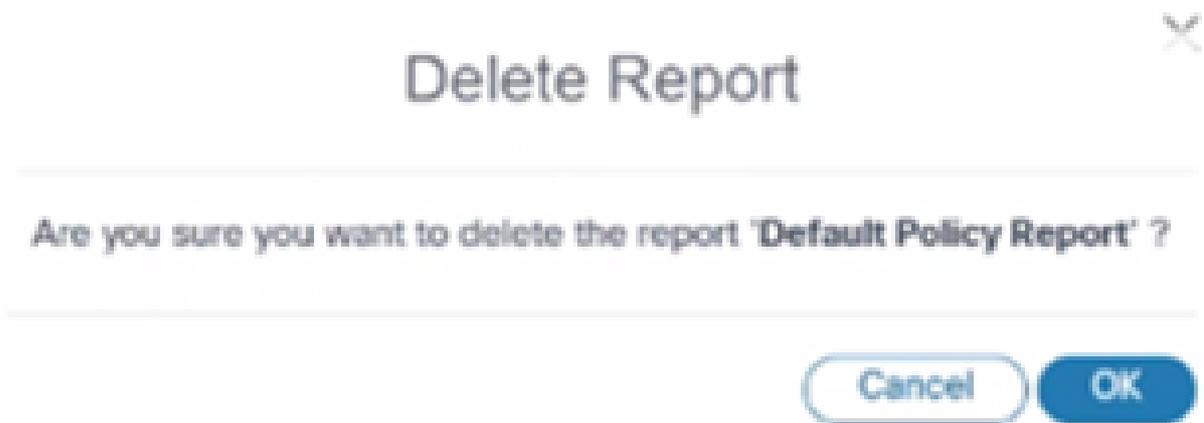
1	interface GigabitEthernet0/0/0 Minor	
		Expected: desc Equals 'Demo' Minor
		Found: 'None' Cnr Demo Policy2 → Demo Rule 2 → Demo Cond1
+ 2	no ip address Info	
+ 3	shutdown Info	
+ 4	negotiation auto Info	
+ 5	cdp enable Info	
6	interface GigabitEthernet0/0/1 Info Skipped	
		Expected: interface Equals '0/0/0' Info

コンプライアンス詳細レポート – サンプルPDFページ2

 注: 「是正バッチ」ページで作成した是正バッチPDFレポートは、レポートリストからダウンロードして表示することもできます。

レポートの削除

レポートを個別に削除するには、削除アイコンを選択します。レポートを一括で削除するには、レポートのチェックボックスをオンにして、その他のオプションアイコン> 削除の順に選択します。



コンプライアンスジョブリスト

 注: レポートを削除すると、レポートファイルとレポートダッシュボードのエントリのみが削除されます。基礎となるコンプライアンス実行の詳細は保持されます。

コンプライアンスジョブ

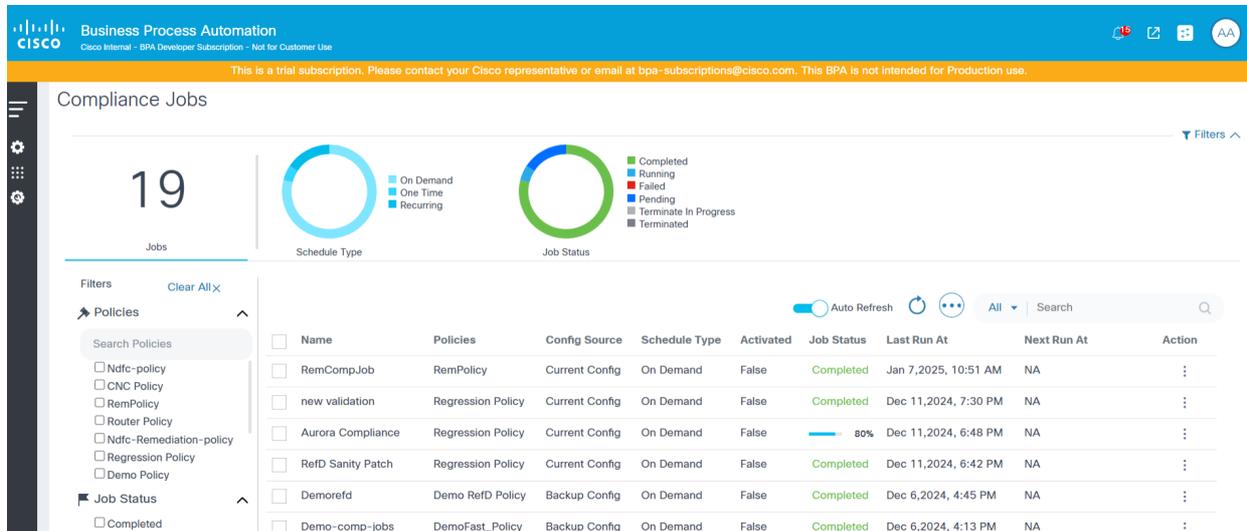
Next-Genポータルコンプライアンスジョブ機能は、選択したポリシーおよび資産グループでコンプライアンスジョブを作成、管理、および実行できるように設計されています。これらのジョブは、定期的に行うようにスケジュールしたり、オンデマンドで実行したりできるため、すべての資産のコンプライアンスが一貫してチェックされます。

主な特長

- コンプライアンスジョブの一覧表示: 定義済みのコンプライアンスジョブをすべて表示します。ジョブのオフライン監査、フィルタ、作成、編集、削除、および実行のオプションがあります。
- スケジュール済みジョブとオンデマンドジョブ: スケジュールされた間隔で実行されるよう

にジョブを設定するか、必要に応じてすぐに実行します。

- きめ細かなアクセス制御：コンプライアンスジョブへのアクセスはユーザの権限に基づいて制御され、ユーザはアクセス権のあるポリシーに関連するジョブのみを表示できます。
- フィルタリングオプション：ポリシー、ジョブのステータス、スケジュールのタイプ、日付範囲でジョブをフィルタリングし、ナビゲーションと管理を容易にします。



コンプライアンスジョブリスト

コンプライアンスジョブの作成

コンプライアンスジョブの作成ページには、次の属性が含まれます。

- Name：ジョブの名前
- 説明：オプションの説明
- Policy Name：実行するポリシーを選択するためのドロップダウンリスト。ログインユーザ用に設定されたアクセスポリシーによってフィルタリングされる場合もあります。
- Device Config Source：コンプライアンスジョブを実行するためのデバイス設定（Current ConfigまたはDevice Config Backup）を取得するソースを選択するためのドロップダウンリスト、およびバックアップが存在しない場合にCLIコマンドにフォールバックするかどうかを示すチェックボックス。

 注: Device Config Backupオプションは、基盤となるコントローラがバックアップ機能をサポートしている場合にのみ機能します。

- ユーザー定義変数：選択したポリシーにユーザー定義変数がある場合に、使用可能な名前空間の編集可能なテキストボックス
- スケジュールの詳細：開始日と終了日/時刻、繰り返しパターンなどのさまざまなスケジュールパラメータを選択するセクション。
- 資産：コンプライアンスを実行するデバイスのリストを識別する資産グループを選択するセ

クシオン

- スケジュール：スケジュールに従ったジョブの実行を有効または無効に切り替えます（1回限りまたは反復）。無効の場合、ジョブはただちに実行されます
- 「有効」:選択したスケジュールが有効かどうかを示します

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

All > Create Compliance Job

Cancel Save

Job Summary

Name: demo-jobs
Config Source: Device Config Backup
Asset Group:

Policy Summary

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

Schedule Summary

Schedule Date: Monday, January 13, 2025, 5:44 PM
Schedule Type: One Time

Name*: demo-jobs
Description: Enter description here
Policy Name*: RemPolicy

Device Config Source*: Device Config Backup
If backup is not present, use CLI command to fetch device configuration.

CLI Command: show running-config

Schedule: Activate:

Schedule Details

Effective on: Monday, 13 Jan 2025 17:44
Start Time*: 17:44

コンプライアンスジョブの作成

All > Create Compliance Job

Cancel Save

Schedule Type: Recurring

Start Time*: 17:44

Schedule Recurrence

Recurrence Pattern: Weekly
Recurrence Day*: Friday
Start Time*: 12:00
End Date: 01/18/2025

Assets

Asset Group*: nso-166-cnr

Name	Ip Address	Location	Managed By
bnf-asr-115			NSO-166

1 | Items per page: 10

コンプライアンスジョブの作成2

オフライン監査ジョブの作成

コンプライアンスジョブのオフライン監査機能を使用すると、デバイスをBPAにオンボーディングしなくても、デバイス設定のコンプライアンスチェックを実行できます。ユーザは、デバイス設定をファイルとして手動でアップロードできます。複数のデバイス設定を圧縮し、zipファイルとしてまとめてアップロードできます。アップロードされると、これらのコンフィギュレーションファイルが解析され、これらのファイルの内容をソースとして使用してコンプライアンスジョブを作成できます。オフライン監査の結果は、コンプライアンスダッシュボードにオンライン監

査の結果と一緒に表示されます。

「オフライン監査」ページには、次の属性があります。

- Name : ジョブの名前
- 説明 : オプションの説明
- Policy Name : 実行するポリシーを選択するためのドロップダウンリスト。ログインユーザーに設定されたアクセスポリシーによってフィルタリングされる場合もあります。
- 製品ファミリ : 製品ファミリを選択するためのドロップダウンリスト
- ファイルのアップロード : オフライン監査機能を使用して、コンフィギュレーションファイルを手動でアップロードします。アップロードは、ローカルシステムからファイルを選択するアップロードインターフェイスを介して実行されます
- スケジュール : スケジュールをオンに切り替えます。
- アセット : アップロードされたファイルの内容に従ってデバイスのリストを表示

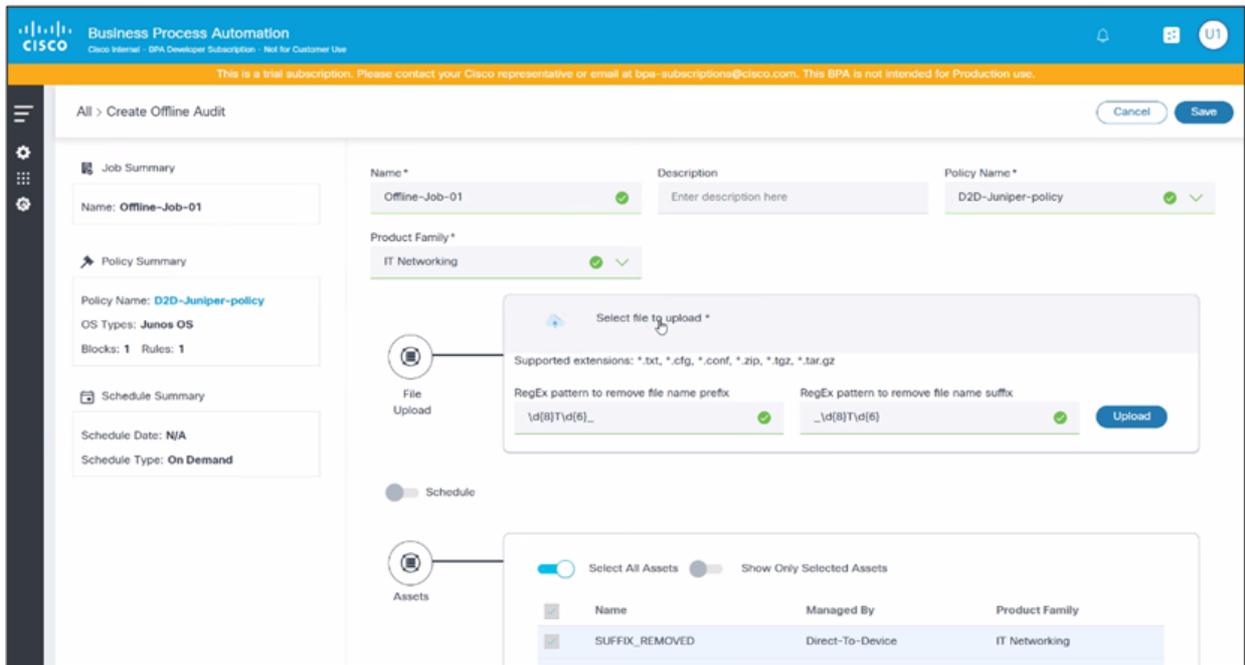
The screenshot shows the Cisco Business Process Automation (BPA) interface. The main heading is 'Compliance Jobs'. There are three summary cards: 'Jobs' with a value of 3, 'Schedule Type' with a legend for On Demand, One Time, and Recurring, and 'Job Status' with a legend for Completed, Running, Failed, Pending, Terminate In Progress, and Terminated. Below these are filter sections for Policies, Job Status, and Schedule Type. The main table lists jobs with columns for Name, Policies, Config Source, Schedule Type, Created By, Activated, Job, Next Run At, and Action. A context menu is open over the 'Offline Audit' job, showing options like 'Create Job', 'Delete Job', and 'Next Run At'.

Name	Policies	Config Source	Schedule Type	Created By	Activated	Job	Next Run At	Action
Online-Job-01	D2D-Juniper-policy	Backup Config	On Demand	cnrofflineuser1	False	Con	025, 5:47	NA
CXpm-Demo-01	D2D-Juniper-policy	Offline Audit	On Demand	cnrofflineuser1	False	Con	025, 4:12	NA
User-1-Invalid-Device-Offline-Job	D2D-Juniper-policy	Offline Audit	On Demand	cnrofflineuser1	False	Completed	25, 6:46	NA

オフライン監査の選択

オフライン監査ジョブを作成するには、次の手順に従います。

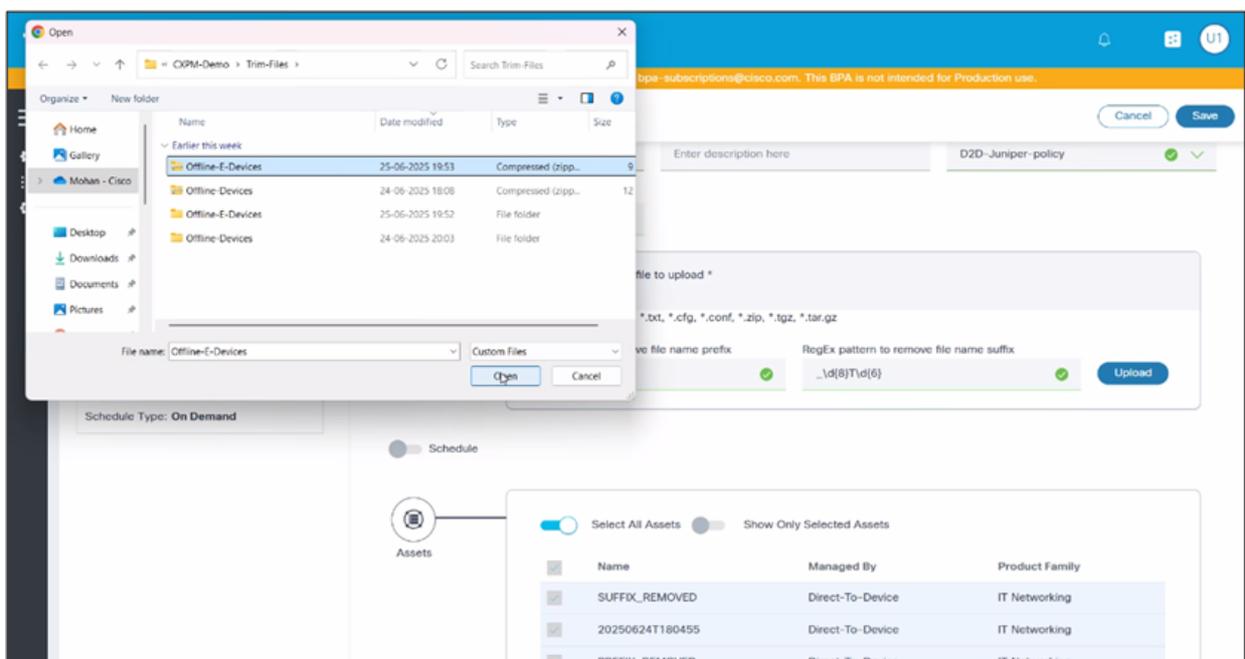
1. More OptionsアイコンからOffline Auditを選択します。



ファイルのアップロード

2. Select file to uploadをクリックして、コンフィギュレーションファイルをアップロードします。

注: サポートされるファイルタイプは、(.txt,.cfg,.conf,.zip,.tgz,.tar.gz)です。



デスクトップファイル

3. コンフィギュレーションファイルがフォルダまたはアーカイブに圧縮されている場合は、アップロードする前にファイルを抽出します。

All > Create Offline Audit Cancel Save

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* **Offline-Job-01** ✓ Description Enter description here Policy Name* **D2D-Juniper-policy** ✓ ✓

Product Family* **IT Networking** ✓ ✓

Select file to upload * **Offline-E-Devices.zip**

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

RegEx pattern to remove file name prefix ✓ RegEx pattern to remove file name suffix ✓ Upload

File Upload

Schedule

Assets

Upload file to select devices.

正規表現パターン

4. ファイル名のトリミングに正規表現パターンを適用します (オプション)。

注 : アップロードされたファイル名を標準化または簡素化して処理を容易にするために、TUseのプレフィクスまたはサフィックストリミングパターン (正規表現)。

All > Create Offline Audit Cancel Save

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
<input checked="" type="checkbox"/> SUFFIX_REMOVED	Direct-To-Device	IT Networking
<input checked="" type="checkbox"/> 20250624T180455	Direct-To-Device	IT Networking
<input checked="" type="checkbox"/> PREFIX_REMOVED	Direct-To-Device	IT Networking

1 | Items per page 10

ファイルのアップロード

5. [Upload] をクリックします。ファイルがデータベースに保存され、正常にアップロードされたことを示す確認メッセージが表示されます。

All > Edit Offline Audit Cancel Save

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*

Product Family*

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

File Upload

Schedule

Assets

Select All Assets
 Show Only Selected Assets

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

オフライン監査の保存

6. Saveをクリックして、オフライン監査ジョブを作成します。

コンプライアンス・ジョブの編集

コンプライアンスジョブを編集するには、「[コンプライアンスジョブの作成](#)」に記載されている手順に従います。

注：ジョブNameは編集できません。

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: Schedule
Activate: Activate

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

Schedule Recurrence
Recurrence Pattern: Cron Pattern
Cron Pattern: 0 2 * * *
End Date: 01/15/2025

Assets
Asset Group*: assetgroup-38

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

コンプライアンスジョブの編集

今すぐ実行またはコンプライアンスジョブの再実行

Compliance Jobs

218 Jobs

Filters: Policies, Job Status, Schedule Type

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 CNC	cnc gpg policy	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
OrR-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 gpgabi	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	Completed	Aug 1, 2025, 5:01 PM		NA
History-validate	Default Policy - Compliance Check	Current Config	On Demand	admin	False	Completed	Aug 1, 2025, 11:34 AM		

コンプライアンスジョブ - 今すぐ実行して非準拠で実行

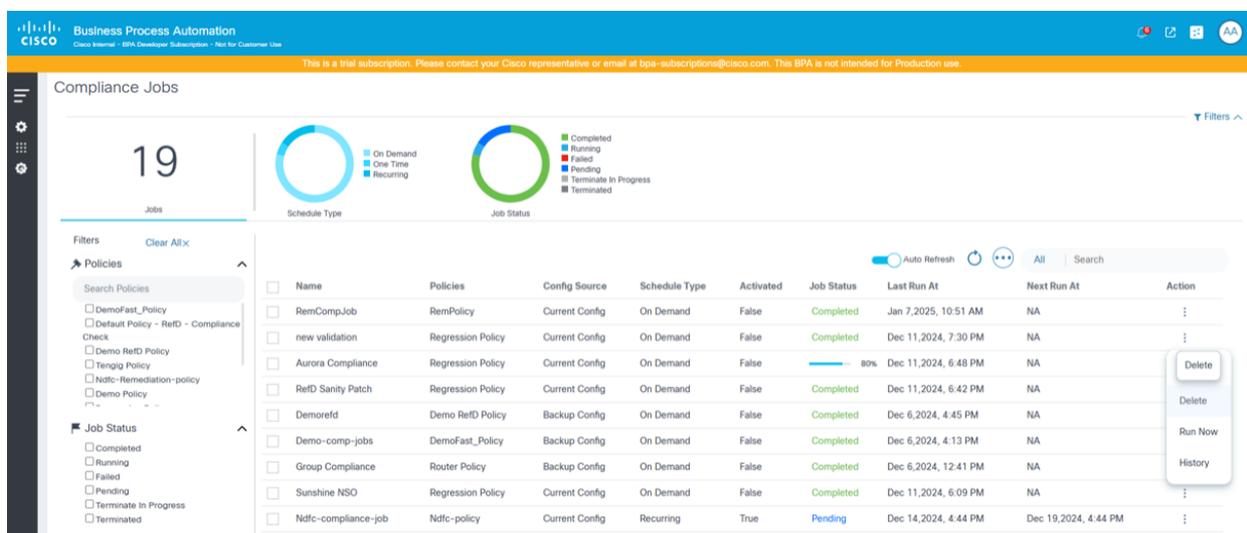
コンプライアンスジョブグリッドには、オンデマンドでジョブを実行するオプションがあります

。そのためには、その他のオプションアイコンから今すぐ実行を選択します。ジョブに既存の実行がある場合、ユーザはMore OptionsアイコンからRun on Non-Compliantを選択できます。このアクションは、前の実行で完全準拠としてマークされていないアセットのリストでのみ準拠ジョブを実行します。

コンプライアンスジョブの削除

ポータルには、ユーザが正しいロールベースアクセスコントロール(RBAC)ロールを持っている場合に、1つ以上のコンプライアンスジョブを削除するオプションがあります。実行中のジョブは削除できません。ユーザは、1つまたは複数のコンプライアンスジョブを削除するように選択できます。

コンプライアンス・ジョブを削除するには、次の手順に従います。



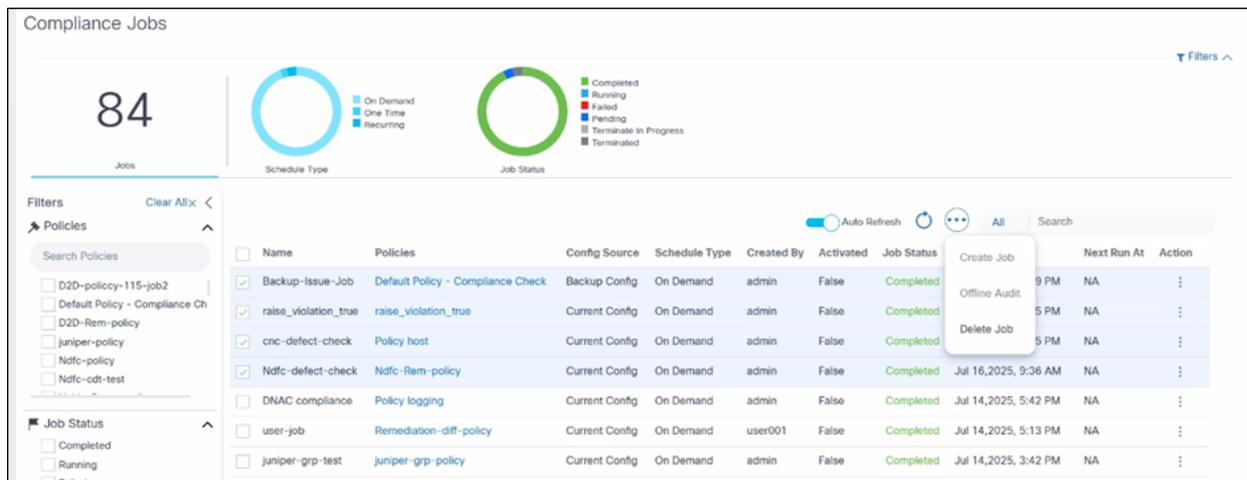
The screenshot displays the 'Compliance Jobs' interface. At the top, there are two donut charts: 'Schedule Type' (On Demand, One Time, Recurring) and 'Job Status' (Completed, Running, Failed, Pending, Terminate In Progress, Terminated). Below these are filters for Policies and Job Status. The main table lists various jobs, including 'Aurora Compliance', which is highlighted with a 'Delete' button in the Action column.

Name	Policies	Config Source	Schedule Type	Activated	Job Status	Last Run At	Next Run At	Action
RemCompJob	RemPolicy	Current Config	On Demand	False	Completed	Jan 7, 2025, 10:51 AM	NA	⋮
new validation	Regression Policy	Current Config	On Demand	False	Completed	Dec 11, 2024, 7:30 PM	NA	⋮
Aurora Compliance	Regression Policy	Current Config	On Demand	False	80%	Dec 11, 2024, 6:48 PM	NA	Delete
RefD Sanity Patch	Regression Policy	Current Config	On Demand	False	Completed	Dec 11, 2024, 6:42 PM	NA	Delete
Demorefd	Demo RefD Policy	Backup Config	On Demand	False	Completed	Dec 6, 2024, 4:45 PM	NA	Run Now
Demo-comp-jobs	DemoFast_Policy	Backup Config	On Demand	False	Completed	Dec 6, 2024, 4:13 PM	NA	History
Group Compliance	Router Policy	Backup Config	On Demand	False	Completed	Dec 6, 2024, 12:41 PM	NA	⋮
Sunshine NSO	Regression Policy	Current Config	On Demand	False	Completed	Dec 11, 2024, 6:09 PM	NA	⋮
Ndfc-compliance-job	Ndfc-policy	Current Config	Recurring	True	Pending	Dec 14, 2024, 4:44 PM	Dec 19, 2024, 4:44 PM	⋮

単一のコンプライアンス・ジョブの削除

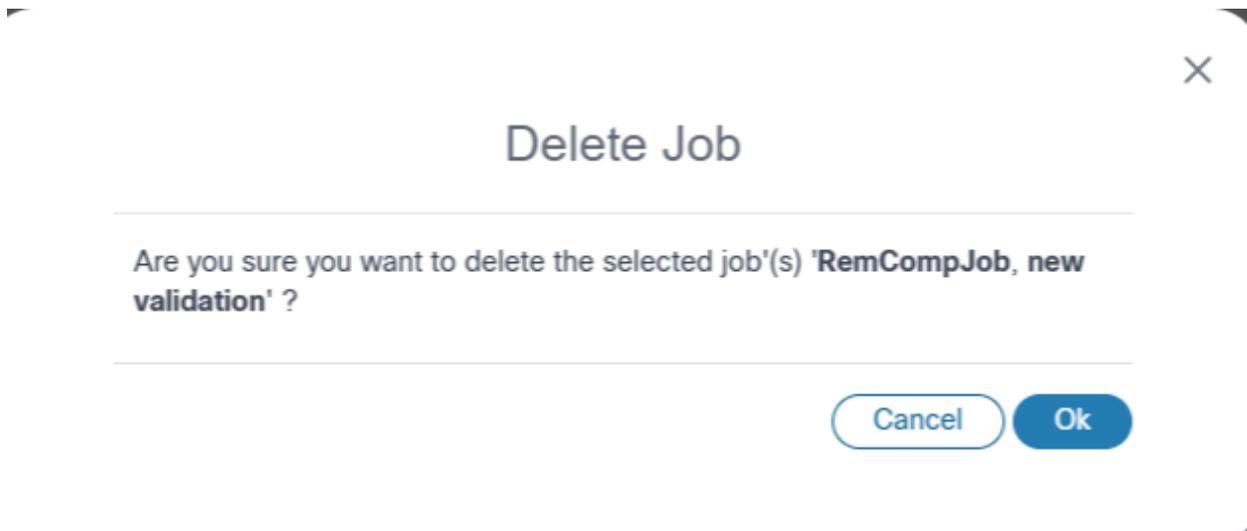
1. Compliance Jobsページで、削除するジョブに対してMore Optionsアイコン> Deleteを選択します。

または



複数のコンプライアンス・ジョブの削除

複数のコンプライアンスジョブを削除するには、削除するジョブのチェックボックスをオンにし、[その他のオプション] > [ジョブの削除]を選択します。確認が表示されます。



コンプライアンスジョブの削除の確認

コンプライアンスジョブの終了

ポータルでは、特定のジョブの実行中の実行を終了するオプションがユーザに提供されます。ジョブが終了すると、現在実行中のデバイスは実行を完了し、キューに登録された以降のデバイス実行をすべてキャンセルします。

Compliance Jobs

19 Jobs

Schedule Type: On Demand, One Time, Recurring

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

Name	Policies	Config Source	Schedule Type	Activated	Job Status	Last Run At	Next Run At	Action
RemCompJob	RemPolicy	Current Config	On Demand	False	Completed	Jan 7, 2025, 10:51 AM	NA	⋮
new validation	Regression Policy	Current Config	On Demand	False	Completed	Dec 11, 2024, 7:30 PM	NA	⋮
<input checked="" type="checkbox"/> Aurora Compliance	Regression Policy	Current Config	On Demand	False	80%	Dec 11, 2024, 6:48 PM	NA	Terminate
RefD Sanity Patch	Regression Policy	Current Config	On Demand	False	Completed	Dec 11, 2024, 6:42 PM	NA	⋮
Demorefid	Demo RefD Policy	Backup Config	On Demand	False	Completed	Dec 6, 2024, 4:45 PM	NA	⋮
Demo-comp-jobs	DemoFast_Policy	Backup Config	On Demand	False	Completed	Dec 6, 2024, 4:13 PM	NA	⋮
Group Compliance	Router Policy	Backup Config	On Demand	False	Completed	Dec 6, 2024, 12:41 PM	NA	⋮
Sunshine NSO	Regression Policy	Current Config	On Demand	False	Completed	Dec 11, 2024, 6:09 PM	NA	⋮
Ndfc-compliance-job	Ndfc-policy	Current Config	Recurring	True	Pending	Dec 14, 2024, 4:44 PM	Dec 19, 2024, 4:44 PM	⋮
CNC patch	CNC Policy	Backup Config	On Demand	False	Completed	Dec 5, 2024, 4:41 PM	NA	⋮

コンプライアンスジョブの終了

Terminate Compliance Job

Are you sure you want to terminate the Compliance Job 'Aurora Compliance' ?

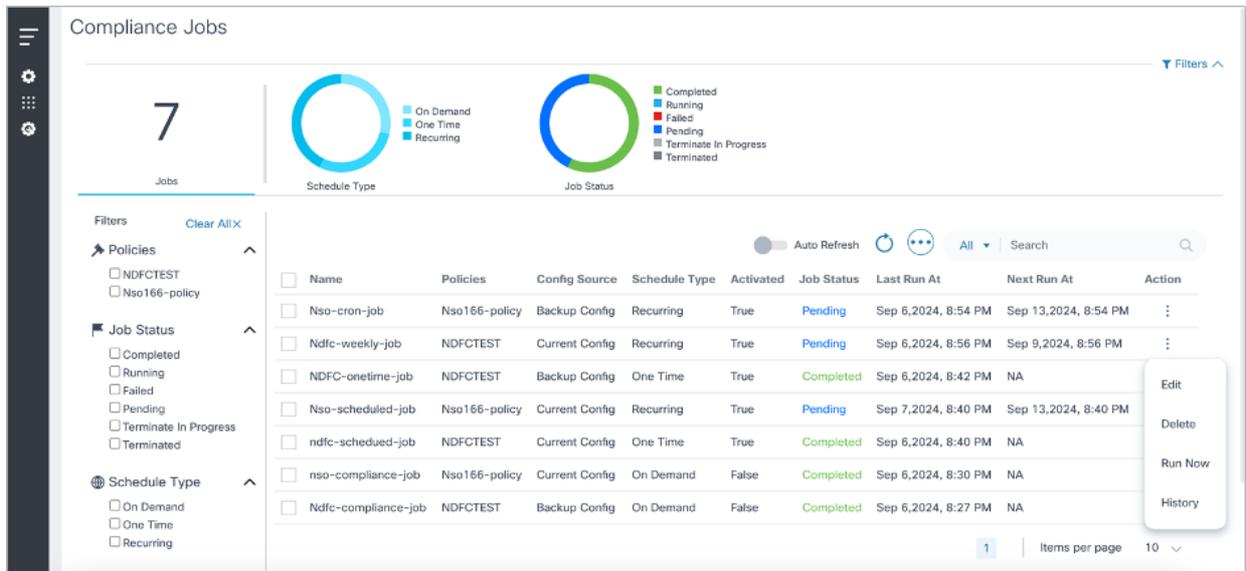
Cancel Ok

コンプライアンスジョブの終了確認

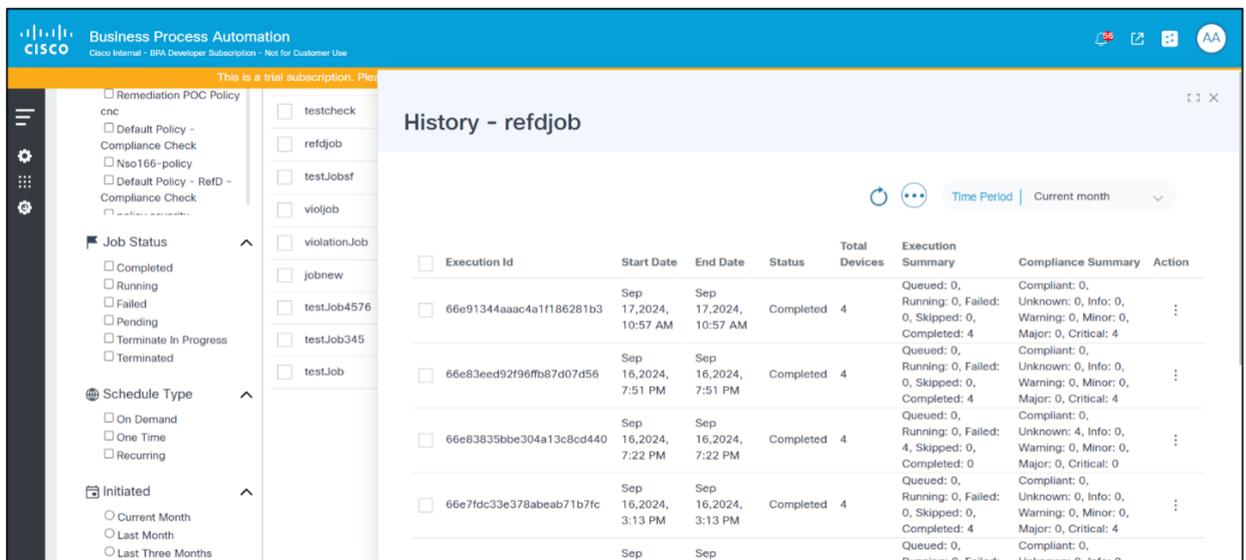
コンプライアンスジョブの履歴

コンプライアンスジョブの[履歴]オプションには、選択したジョブの実行のリストが、スケジュールの日付範囲でフィルタ処理されて表示されます。

コンプライアンスジョブの履歴を表示するには、コンプライアンスジョブページで、その他オプションアイコン>履歴の順に選択します。Historyページが表示されます。



コンプライアンスのジョブ履歴

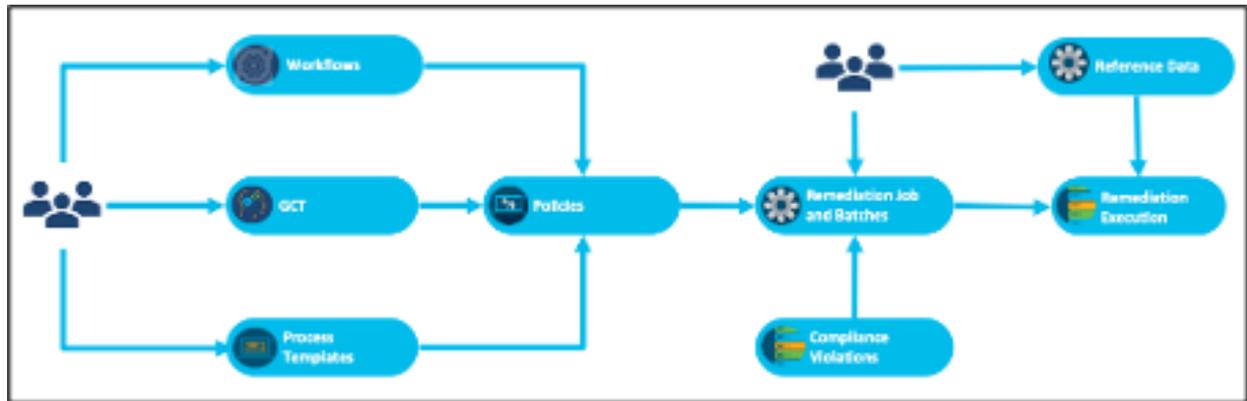


履歴ページ

修復ジョブ

是正フレームワークを使用すると、コンプライアンスダッシュボードに表示されたコンプライアンス違反を是正できます。このフレームワークでは、ワークフロー、GCT、およびプロセステンプレートを使用します。

設定修復のフロー図



設定の修復の概要

設定修復のユースケースにより、オペレータは修復ジョブを使用してデバイスの設定違反を修正できます。コンプライアンスポリシーは、最初にコントローラタイプごとに適切なワークフロー、GCTテンプレート、およびプロセステンプレートを使用して設定されます。是正ジョブは、影響を受ける資産のリストに対するポリシーに対して実行されます。修復時に、デバイスに適用される値は、コンプライアンス実行結果、参照アプリケーション、既存のデバイス設定など、さまざまなデータソースから取得できます。修正中の追加ステップに対応するために、特定の顧客要件に従ってワークフローをカスタマイズできます。

修復機能の最も重要な手順を次に説明します。

GCTテンプレート

GCTは、コントローラ固有のテンプレートを使用してデバイスに設定変更を適用するために使用されるBPAコア機能です。

- デバイス設定を更新するGCTテンプレートの作成、コンプライアンス違反の解決
- GCTテンプレート内の変数が次の構文に準拠している場合、フレームワークは自動変数マッピングをサポートします。
 - 単一デバイス構成ブロックの場合： <>_<>例：management_interface_ipv4_addr, management_interface_ipv4_subnet
 - 将来のリリースでは、複数のデバイス設定ブロックが計画されています
- 「ブロック識別子名」および「ブロックからの変数名」にスペースが含まれる場合、これらのスペースはアンダースコア(_)に置き換える必要があります(たとえば、「ブロック識別子名」が「管理インタフェース」で、「変数名」が「IPV4_ADDR」の場合、GCT内の変数名は「Management_Interface_IPV4_ADDR」になります)。
- ユーザーは、コンプライアンス・デバイス実行からの「gctVars」出力をチェックして、GCT変数の構文およびマッピングが正しいかどうかを確認できます。コンプライアンス・デバイス実行を取得するには、次のREST APIを使用します。
 - 実行IDを見つけるために実行を取得します
 - URL: /api/v1.0/compliance-remediation/compliance-execution
 - メソッド: GET
 - 実行IDを使用したデバイス実行の取得

- URL: `https://<>/bpa/api/v1.0/compliance-remediation/compliance-device-execution?executionId=<>`
- メソッド : 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": ":",
123         "Interface_Gigabit_3_ip_subnet": ":",
124     },
125     "overAllStatus": "partial-compliant",
126     "severitySummary": {
127         "major": 5,
128         "info": 1,
129         "critical": 0
130     }

```

GCT変数 – gctVars

- ブロックから変数を取得するには、次のREST APIを使用します。
 - URL: `https://<>/bpa/api/v1.0/compliance-remediation/utils/schema`
 - 方法 : POST
 - 本文 : `{"blockName": "<<ブロック名>>"}`
- ドライランとコミットの両方のデバイスにテンプレートを適用して、GCTテンプレートを検証します。
- コンプライアンスポリシーで上記のGCTテンプレートを設定します

修復フレームワークには、以下の事前設定済みの参照ワークフローが用意されています。

- 是正プロセス：このワークフローには、是正の実行に関連する共通の一連のステップがあります。
- 是正サブプロセス：このワークフローには、変数の割り当て、GCTドライ実行、およびGCTコミットタスクが含まれます。これらのタスクは、要件に従って他のチームによってカスタマイズできます。

どちらのワークフローも、お客様のニーズに応じて、そのまま使用、更新、または交換できます。

プロセステンプレート

ポリシーに対してプロセステンプレートと分析テンプレートを設定し、事前チェックと事後チェックを実行して出力を比較できます。

ポリシー

CnRポリシーは、デバイスタイプごとにワークフロー、GCTテンプレート、およびプロセステンプレートを統合し、ジョブを使用して設定を修正するために使用できます。

修復ジョブ

修復ジョブは、オペレータが影響を受ける資産の選択したリストに修復ポリシーを適用するのに役立ちます。是正ジョブは、オンデマンドまたはスケジュールに従って実行できます。実行時に、修復ワークフローは、デバイスの詳細、コンプライアンス実行の詳細、RefDフレームワークなどのさまざまなソースからデータを取得できます。

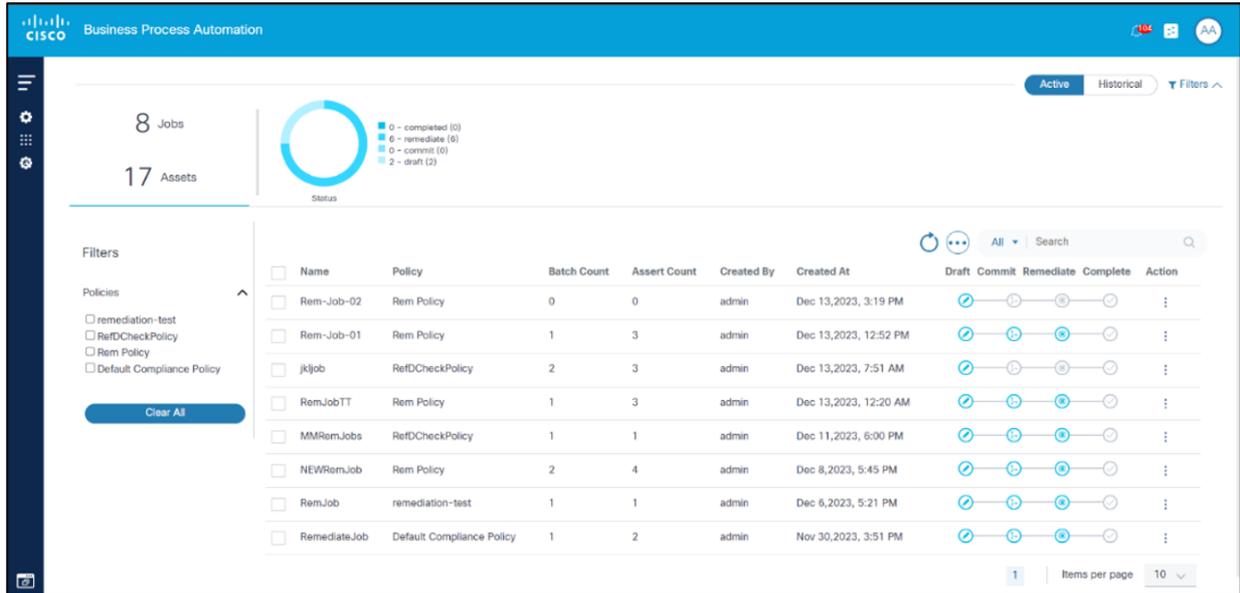
是正ジョブリスト

ユーザは、ダッシュボードで作成された是正ジョブを次のようにフィルタ、並べ替え、表示できます。

- ジョブ：作成されたジョブの合計数を表示します
- 資産：作成された資産合計を表示します。
- ステータス：ステータス別にジョブを表示します。
- ActiveおよびHistorical：選択に基づいて、ActiveまたはHistorical(inactive)ジョブを表示します
- ポリシー：ポリシーに基づいて修復ジョブをフィルタリング
- メイングリッド：ヘッダーをクリックして並べ替えられるジョブのデフォルトリストが表示

され、名前とポリシーによる検索が含まれます(ページ区切り)。

- アクション：ジョブがドラフト状態または完了状態の場合、アーカイブまたは削除できます。実行中のジョブはアーカイブまたは削除できません



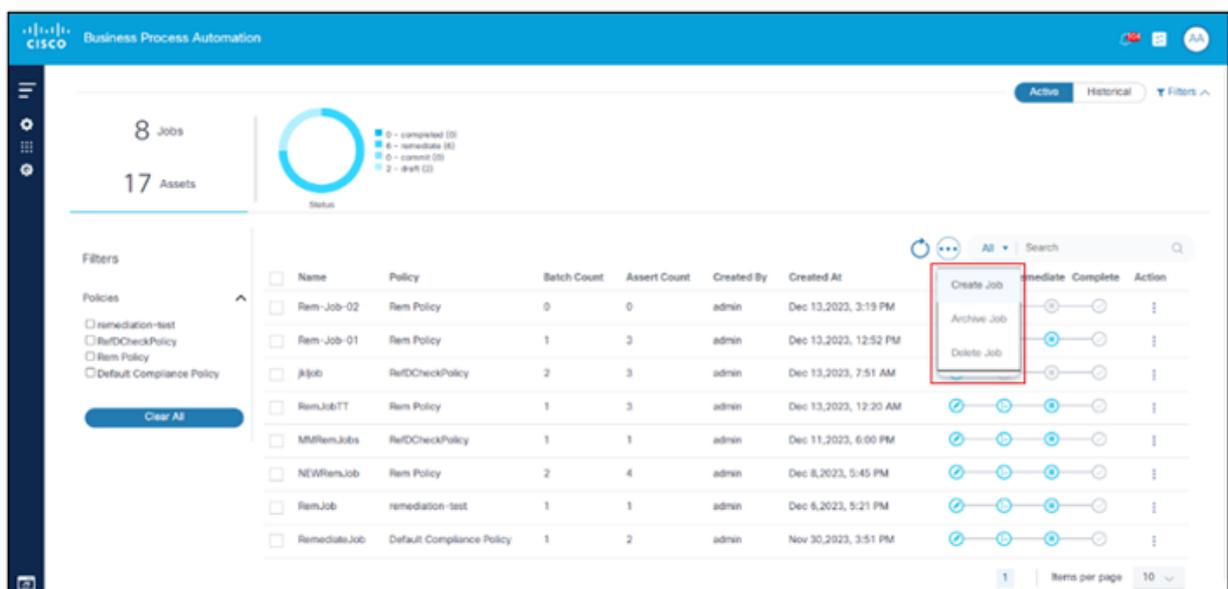
Name	Policy	Batch Count	Assert Count	Created By	Created At	Draft	Commit	Remediate	Complete	Action
Rem-Job-02	Rem Policy	0	0	admin	Dec 13, 2023, 3:19 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	⋮
Rem-Job-01	Rem Policy	1	3	admin	Dec 13, 2023, 12:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	⋮
jkjob	RefDCheckPolicy	2	3	admin	Dec 13, 2023, 7:51 AM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	⋮
RemJobTT	Rem Policy	1	3	admin	Dec 13, 2023, 12:20 AM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	⋮
MMRemJobs	RefDCheckPolicy	1	1	admin	Dec 11, 2023, 6:00 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	⋮
NEWRemJob	Rem Policy	2	4	admin	Dec 8, 2023, 5:45 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	⋮
RemJob	remediation-test	1	1	admin	Dec 6, 2023, 5:21 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	⋮
RemediateJob	Default Compliance Policy	1	2	admin	Nov 30, 2023, 3:51 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	⋮

是正ジョブリスト

是正ジョブの作成および編集

是正ジョブは「ジョブリスト」ページから作成します。次の手順を実行して作成できます。

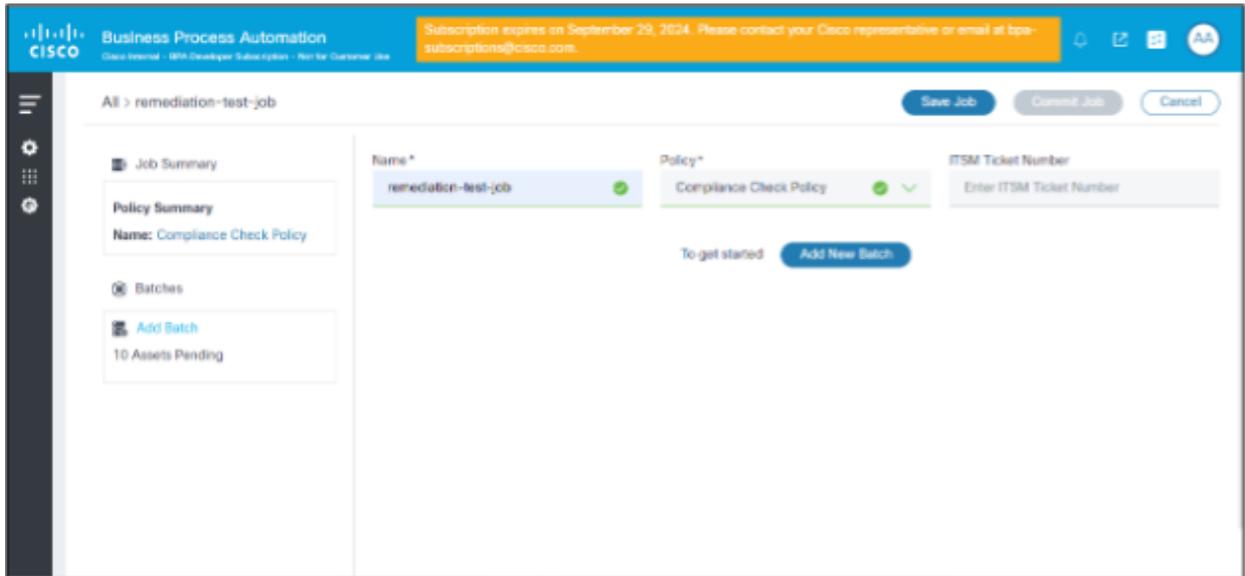
1. More Optionsアイコン> Create Jobを選択します。Create Jobページが表示されます。



Name	Policy	Batch Count	Assert Count	Created By	Created At	Draft	Commit	Remediate	Complete	Action
Rem-Job-02	Rem Policy	0	0	admin	Dec 13, 2023, 3:19 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	⋮
Rem-Job-01	Rem Policy	1	3	admin	Dec 13, 2023, 12:52 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	⋮
jkjob	RefDCheckPolicy	2	3	admin	Dec 13, 2023, 7:51 AM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	⋮
RemJobTT	Rem Policy	1	3	admin	Dec 13, 2023, 12:20 AM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	⋮
MMRemJobs	RefDCheckPolicy	1	1	admin	Dec 11, 2023, 6:00 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	⋮
NEWRemJob	Rem Policy	2	4	admin	Dec 8, 2023, 5:45 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	⋮
RemJob	remediation-test	1	1	admin	Dec 6, 2023, 5:21 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	⋮
RemediateJob	Default Compliance Policy	1	2	admin	Nov 30, 2023, 3:51 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	⋮

是正ジョブのオプション

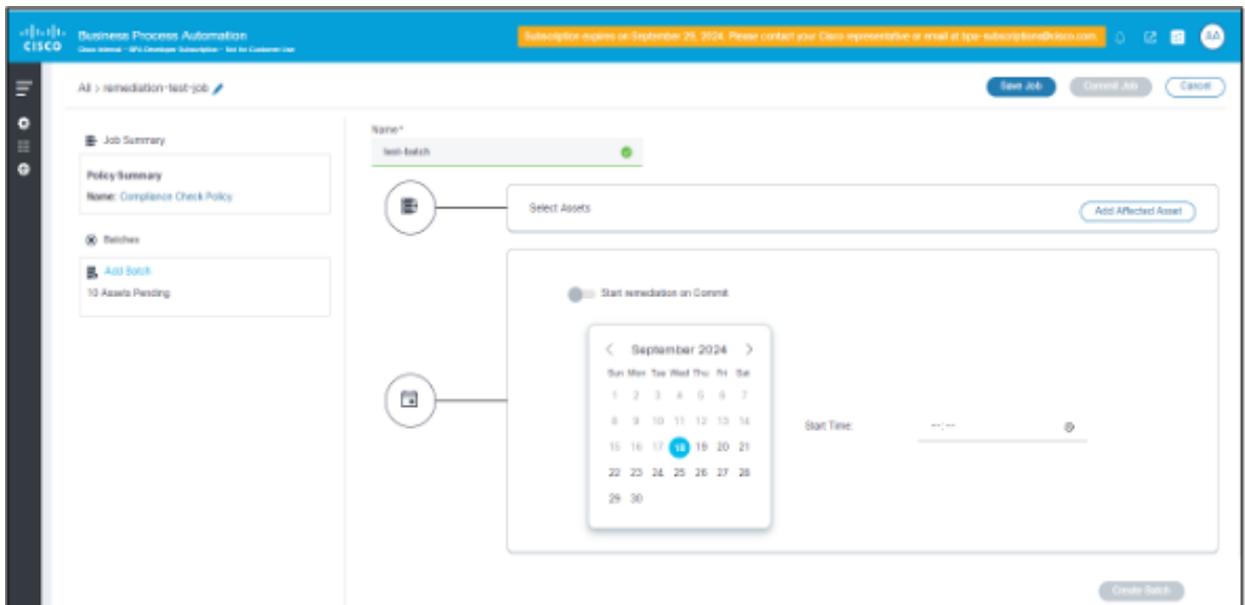
2. 詳細を入力または編集します。



是正ジョブ : 詳細

3. Save Jobをクリックします。

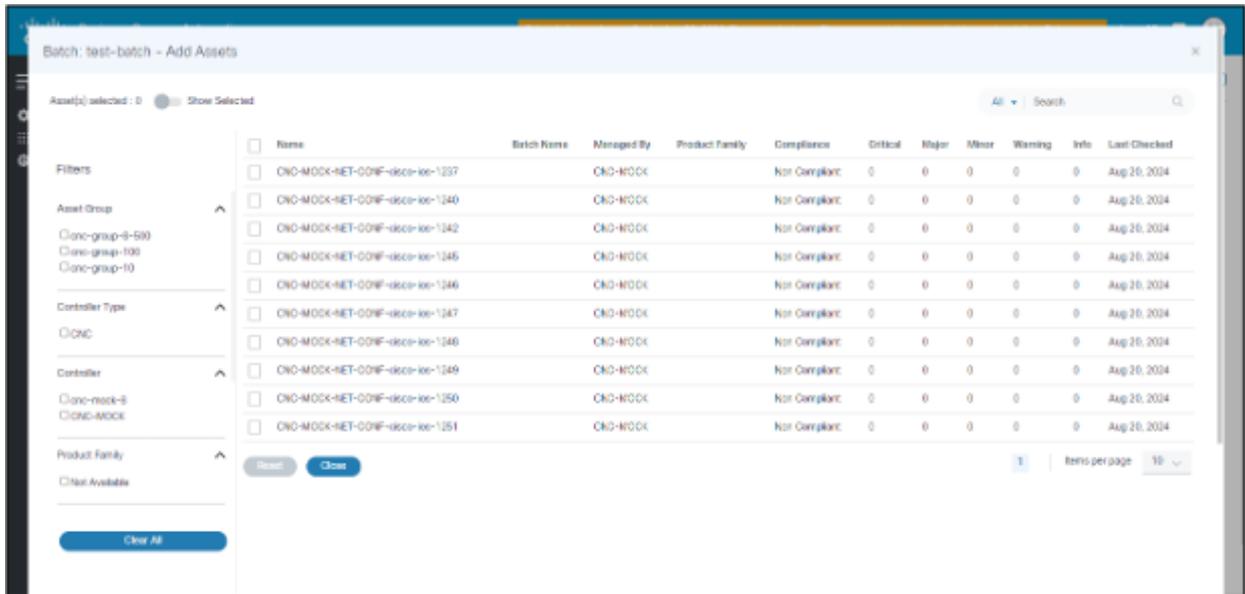
「ジョブの作成」ページからジョブにバッチを追加する手順は、次のとおりです。



是正ジョブ : バッチの追加

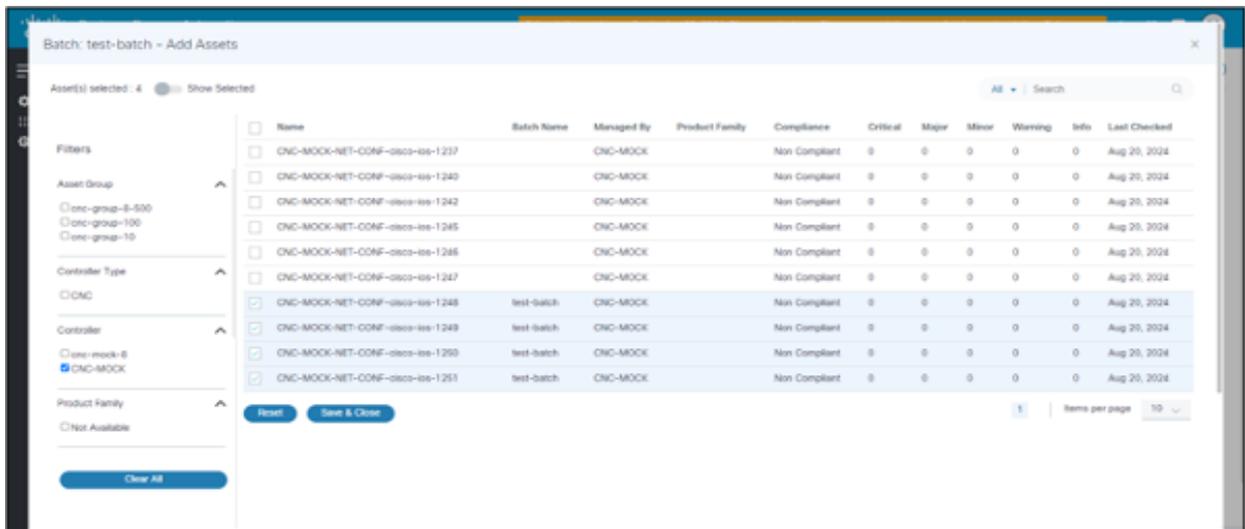
1. Add New Batchをクリックします。
2. 名前、影響を受ける資産の詳細、およびスケジュールの詳細を入力します。
3. Add Affected Assetsをクリックします。
4. Assets Detailsページで、影響を受けるアセットのリストを選択し、Save Jobをクリックします。

5. コントローラタイプ、コントローラ、資産グループ、および製品ファミリに基づいて資産をフィルタします。
6. アセットを選択したら、Save & Closeをクリックして前のページに戻ります。



修復ジョブ：影響を受ける資産の追加

注:影響を受けるアセットページでフィルタを適用することもできます



修復ジョブ：影響を受けるフィルタの追加

影響を受ける資産が追加されると、保存時またはスケジュールされた将来の時刻に1回だけバッチを実行できます。

注：ジョブをオンデマンドで実行するには、[コミット時に修復を開始]切り替えを有効にします。ユーザーがこのオプションを選択した場合、日付と時刻は不要です。ユーザーがOne-Timeオプションを選択する場合、ジョブを実行するには日付と時刻を指定する必要があります

✎ ます。

1つの是正ジョブに複数のバッチがあります。各バッチは、コミット時またはスケジュールされた日時に開始できます。

オンコミット修復バッチは、オンデマンドで実行することも、スケジュールして実行することもできます。

The screenshot shows the Cisco Business Process Automation interface for a remediation job named 'demo'. The job is currently in a pending state with 1 asset. The configuration includes a table of affected assets and a calendar for scheduling. The 'Start remediation on Commit' toggle is checked, and the start date is set to January 13, 2025. The start time is currently blank.

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

修復ジョブ：オンデマンド

The screenshot shows the same remediation job configuration, but the 'Start remediation on Commit' toggle is now turned off. The start time has been set to 19:00. The calendar still shows the start date as January 13, 2025.

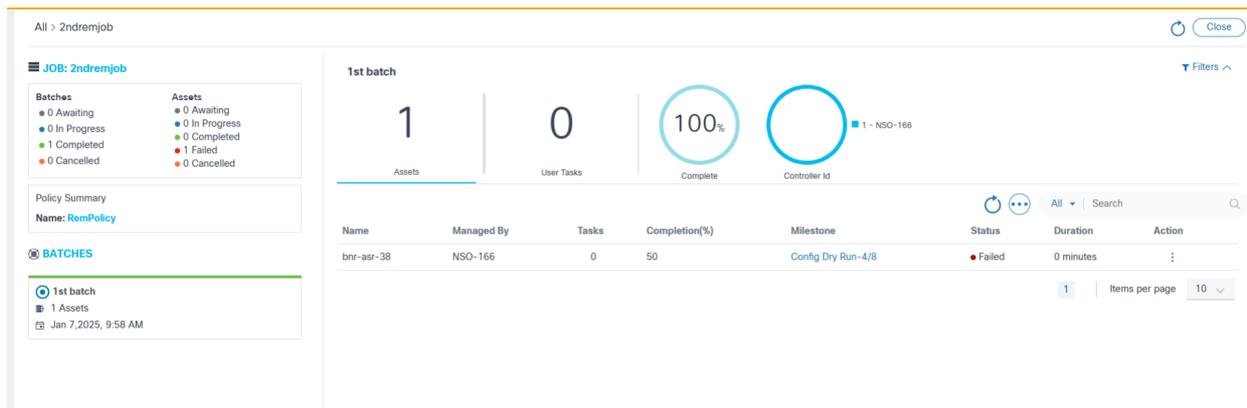
Name	Managed By	Compliance	Critical	Major	Minor	Warning	Last Checked
bnr-asr-38	NSO-166	Partially Compliant	0	1	0	1	Jan 7, 2025

修復ジョブ：1回/スケジュール

修復実行：デバイスのリスト

是正ジョブがコミットされると、実行がトリガーされ、「是正ジョブ」の「デバイスのリスト」ページにジョブのステータスが表示されます。ユーザは、コントローラID、名前、管理者、製品ファミリーでフィルタを適用できます。

- ジョブ：バッチおよび資産のステータス詳細と、是正ジョブを実行するために選択したポリシーの名前が表示されます。
- バッチ：現在の是正ジョブの一部としてバッチのリストを表示します。
- 自動更新：ジョブが実行状態の場合は30秒ごとにページを自動更新する、ページを更新する、前のページに戻る場合はキャンセルするオプションを表示します
- バッチ・レベル詳細：合計資産数、ユーザー・タスク数、完了率およびコントローラ詳細を含むバッチ・レベル要約詳細が表示されます。
- アセットグリッド：各アセットのユーザタスク、完了率、現在のマイルストーンを含むアセットグリッドビューを表示します



修復の実行：デバイスリスト

修復実行：インラインユーザタスクの詳細

デバイスリストのTasks列には、実行するタスクがユーザにあるかどうかが表示されます。

インライン・ユーザー・タスクの詳細を表示する手順は、次のとおりです。

1. タスク数を選択します。User Tasksリストウィンドウが開きます。
2. タスクを選択します。「ユーザタスク詳細」ウィンドウが開きます。

インラインから次のアクションを実行できます。

- 完了
- 再試行
- Cancel

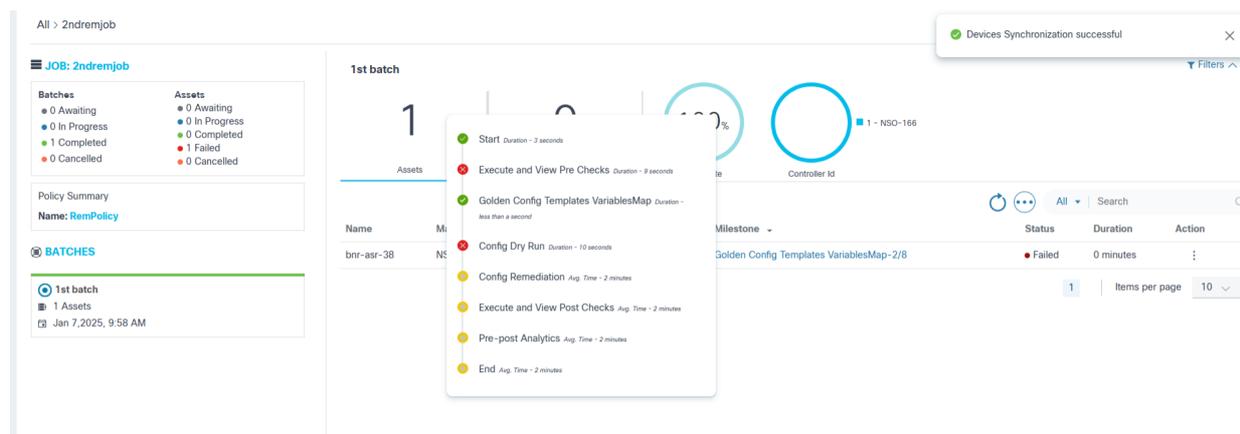
修復実行：インラインマイルストーンの詳細

デバイスリストのMilestone列には、特定のデバイスの修復に関連する現在のマイルストーンが表示されます。

インラインマイルストーンの詳細を表示するには、列を選択します。「マイルストーン詳細」ウィンドウが開きます。

マイルストーンに対して次のステータスを使用できます。

- 未開始
- 実行中
- 完了
- Failed (故障)



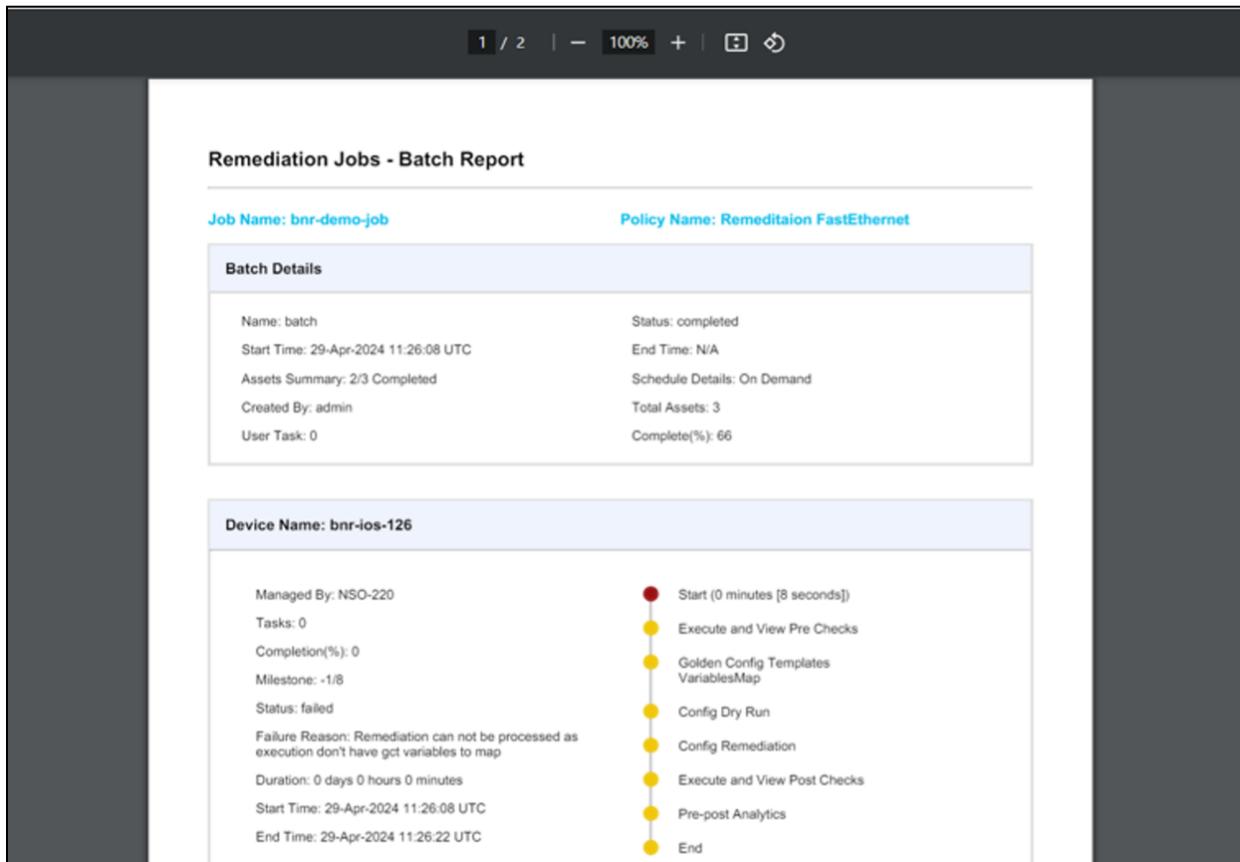
修復実行：インラインマイルストーンの詳細

是正の実行：バッチ要約PDFレポートの生成およびダウンロード

バッチ要約は、生成およびダウンロードできます。

要約レポートをバッチごとにPDF形式でダウンロードする手順は、次のとおりです。

1. More Optionsアイコン> Generate Reportの順に選択します。レポートの準備が整っているかどうか内部的にチェックされます。レポートの準備が整うと、「レポートのダウンロード」オプションが使用可能になります。
2. More Optionsアイコン> Download Reportの順に選択します。PDFがダウンロードされます。



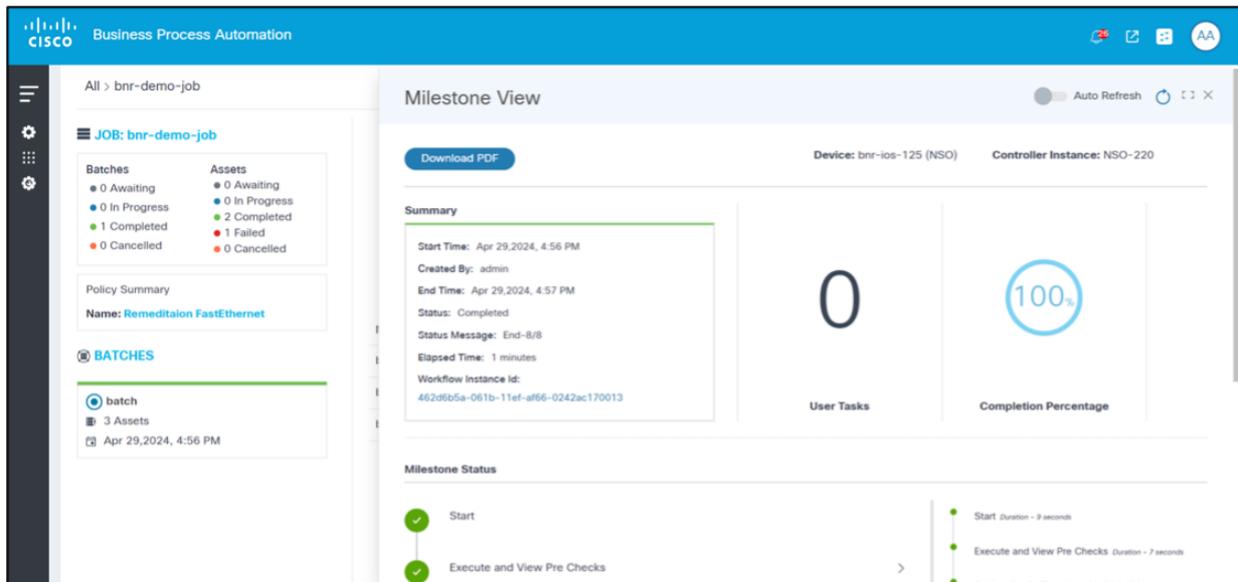
バッチ要約レポートPDF

是正ジョブバッチレポートには「バッチ詳細」セクションが含まれます。このセクションには、ジョブ名、バッチ名、開始時刻と終了時刻、総資産数、全体的なステータスなど、是正バッチの概要が表示されます。その後、デバイスの詳細セクション（デバイスごとに1セクション）が続きます。このセクションには、デバイス名、デバイス固有の修復ステータス、タイムライン、期間、マイルストーンのリスト、およびステータスが含まれます。

修復実行：デバイスの詳細

マイルストーンのデバイスの詳細を表示するには、「デバイスの詳細」ページを選択します。「マイルストーンビュー」ページが表示されます。

特定のデバイスの修復の概要と、完了した主要マイルストーンのコマンド出力を含む、マイルストーンの詳細ステータスが表示されます。たとえば、プロセステンプレートのコマンド出力、GCTドライラン出力、および分析差分出力の内容を表示できます。



是正の実行：マイルストーンビュー

修復実行：デバイスの詳細 – マイルストーンレポート

マイルストーンレポートを表示する手順は、次のとおりです。

1. Device Detailsページを選択します。「マイルストーンビュー」ページが表示されます。
2. Download PDFをクリックします。マイルストーンビューレポートが生成され、次のようにダウンロードされます。

このレポートには、選択したデバイスの修復に関する、より詳細なマイルストーンの詳細と対応する内容が表示されます。

Milestones

Start			
Milestone:	Start	Execution Start:	Tue Jan 07 2025 04:28:29 +0000 (GMT)
Status:	Complete	Completed On:	Tue Jan 07 2025 04:28:32 +0000 (GMT)
Execute and View Pre Checks			
Milestone:	Execute and View Pre Checks	Execution Start:	Tue Jan 07 2025 04:28:33 +0000 (GMT)
Status:	Failed	Completed On:	Tue Jan 07 2025 04:28:42 +0000 (GMT)
Template id :	nso_prepostFail	Device Name :	bnr-asr-38
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

修復実行：デバイスの詳細 – マイルストーン表示PDFレポート

設定：ブロックとルール

ブロックの機能

設定ブロックは、ネットワーク管理システムでコンプライアンスポリシーを作成および適用するために不可欠な要素です。これらは、インターフェイス、ルータのBorder Gateway Protocol(BGP)などのデバイスCLI設定を表します。設定ブロックの主な機能は次のとおりです。

- モジュール方式：構成ブロックにより、モジュラ式のポリシーを作成できます。管理者は、デバイス構成の個々のセクションを個別に定義および管理できます。このモジュール方式により、コンプライアンスポリシーの更新と維持のプロセスが簡素化されます。
- 細分性：デバイス構成をより小さく管理可能な部分に分割することで、管理者は正確なコンプライアンスチェックを実行し、特定の標準を適用できます。これにより、デバイス設定のすべての部分が必要なポリシーに従うことが保証されます。
- 再利用：一度定義すると、複数のコンプライアンスポリシーおよびデバイスで設定ブロックを再利用できます。この再利用により、冗長性が軽減され、構成管理の一貫性が確保されます。
- スタティック設定ブロック：スタティック設定ブロックは、Rawデバイスの設定を表します。変数は含まれません。

例：次のブロックを使用して、TwentyFiveGigE0/0/0/31インターフェイスのコンプライアンスチェックを実行できます

```
interface TwentyFiveGigE0/0/0/31
  description au01-inv-5g-08 enp94s0f0
  no shutdown
  load-interval 30
  !2transport
```

- **ダイナミックコンフィギュレーションブロック**：ダイナミックコンフィギュレーションブロックはデバイス設定を表します。この設定には、適応性と再利用性を高める変数が含まれません。これらのブロックはTTPテンプレートのように機能し、デバイス設定に適用して変数の値を取得します。ルールに条件を追加して、これらの変数を検証できます。TTPの詳細については、<https://ttp.readthedocs.io/en/latest/Overview.html>を参照してください。

例：次のブロックを使用すると、すべてのTwentyFiveGigEインターフェイスでコンプライアンスチェックを実行できます

```
interface TwentyFiveGigE{{INTERFACE_ID}}
  description {{DESCRIPTION}}
  no shutdown
  load-interval {{LOAD_INTERVAL}}
  !2transport
```

サブ階層を持つ動的構成ブロック：このブロックは動的構成ブロックと同様に機能し、複数の階層を持つデバイス構成から値を取得するために使用されます。

例：次の例は、デバイス設定と、階層構造から値を取得するために使用される対応するダイナミックブロックを示しています。

階層構造を持つデバイス設定：

```
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
```

上記の設定を解析するためのダイナミックブロック設定。

```
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
```

ルールの機能

規則を使用すると、構成ブロックに存在する変数に対して検証する条件を定義できます。実行の一部として、コンプライアンスエンジンはデバイス設定を解析し、デバイスブロックインスタンスの一致するインスタンスを検索し、行から値を読み取り、その値に対してルールで定義されている条件を実行します。設定行に違反があるかどうかにかかわらず、結果はダッシュボードに保存されて表示されます。

設定ルールは、ブロック作成ライフサイクルの一部になりました。したがって、ルールを表示するための個別のページはありません。ルールは、対応するブロックの作成ページまたは更新ページに表示、作成、および更新できます。

CnRフレームワークでは、ルールは指定された条件に対して設定を検証する際に重要な役割を果たします。このセクションでは、ルールをシステム内で統合および管理する方法の概要を説明します。

- 目的：ルールを使用すると、設定ブロック内に存在する変数の検証に使用する条件を定義できます
- 実行プロセス:
 - コンプライアンスエンジンがデバイス設定を解析します
 - デバイスブロックインスタンスの一致するインスタンスを特定
 - 設定行から値を抽出します。
 - ルールで定義された条件を次の値に適用します
 - 違反を示す結果が保存され、ダッシュボードに表示されます

ブロックライフサイクルとの統合

- ライフサイクルの統合：構成ルールは、ブロック作成ライフサイクルに不可欠な要素になりました
- 管理:
 - ルールは、ブロックの作成または更新に使用されるページ内に直接表示、作成、および更新されます

- 。ルールを表示するための専用のページがないため、ブロックのライフサイクル内で管理を合理化できます

この統合により、コンプライアンスチェックが構成管理プロセスにシームレスに組み込まれ、事前定義されたルールに対するデバイス構成の効率的な監視と管理が可能になります。

リストブロック

Blocksページには、すべての設定ブロックが一覧表示され、ブロックの生成、追加、編集、削除、インポート、およびエクスポートを行うアクションが提供されます。ユーザは、ブロックの詳細をフィルタ、並べ替え、表示できます。

機能ブロックの詳細

- 。合計数：作成されたブロックの合計数が表示されます。
- 。フィルタ オプション：
 - 。OSタイプおよびデバイスファミリ：ユーザは選択した条件に基づいてブロックをフィルタリングできます。
- 。メイングリッド：
 - 。ブロックの既定の一覧を表示します
 - 。ユーザは、列ヘッダーをクリックしてリストをソートできます
 - 。すべての属性または特定のブロック名で検索できる検索機能を備えています。
 - 。リスト内を簡単に移動できるページネーションをサポート
- 。Actions：
 - 。編集：ユーザは既存のブロックを変更できます。
 - 。削除：ユーザはリストからブロックを削除できます

The screenshot shows the Cisco Business Process Automation interface for 'Config Compliance - Blocks'. The page header includes the Cisco logo and 'Business Process Automation' text. Below the header, there is a navigation bar with 'Policies', 'Blocks', and 'Auto Block Generation' tabs. A large number '3558' is displayed as the total count of blocks. The main content area features a table of configuration blocks with the following columns: Block Name, Config Block, OS Type, Device Family, Created By, Config Type, Block Type, TTP Template, and Action. The table lists several blocks, including 'Block-bnr-asr-38-ruleduplicate', 'New-Block-TickMark', 'Block-New-Test', 'Block-Loopback interface', 'CDT-Block', and 'Optus banner'. The interface also includes a filter sidebar on the left with options for OS Type and Device Family, and a search bar at the top right.

構成ブロックの一覧

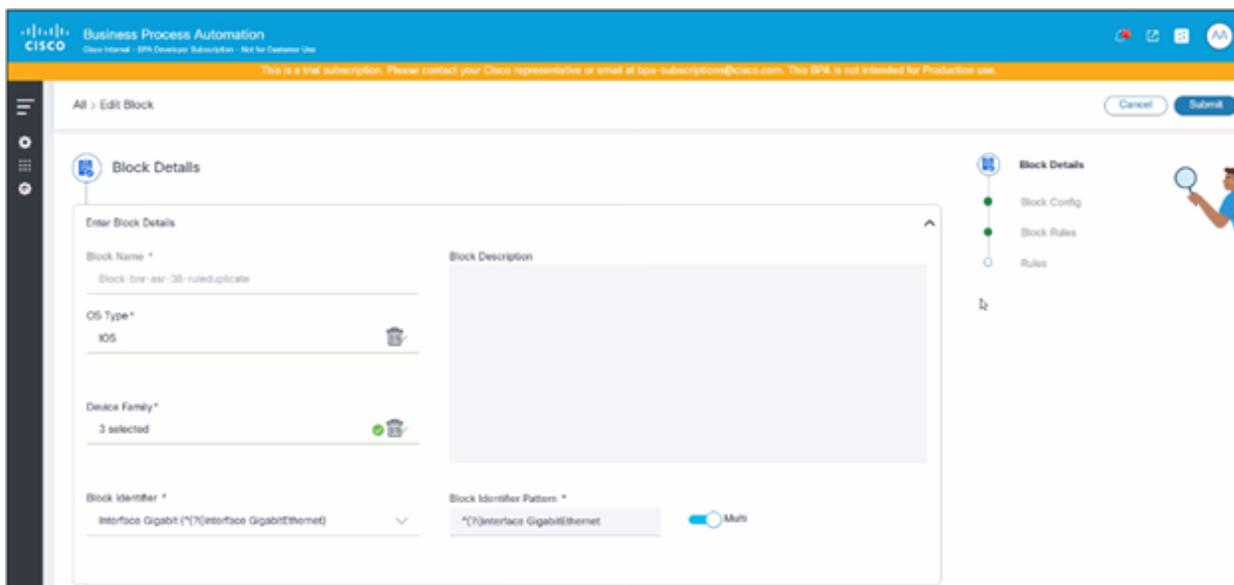
ブロックとルールの追加または編集

AddまたはEdit Blockページは、ブロックに関する重要な情報をキャプチャして管理するように設計されています。このページでは、次のセクションの概要を説明します。

- 基本ブロック詳細:

Basic Detailsセクションには、次の項目があります。

- ブロック名：ブロックに指定された名前
- 説明：ブロックの目的または機能の簡単な概要または説明
- OS Type：ブロックに関連付けられているオペレーティングシステムのタイプ
- デバイスファミリ：ブロックと互換性のあるデバイスのカテゴリまたはグループ
- ブロック識別子の選択：ブロックの一意の識別子を選択するためのオプション
- ブロック識別子の詳細を追加または編集する：適切なブロック識別子が存在しない場合、ユーザーは同じフィールドを使用して、次のブロック識別子の詳細を追加または編集できます。
- ブロック識別子名：ブロック識別子に与えられる特定の名前
- パターン：ブロック識別子が従うパターンまたは形式
- Multi：設定ブロックを複数行の設定として扱うかどうかを指定します



ブロックを追加、編集する – ブロックの詳細

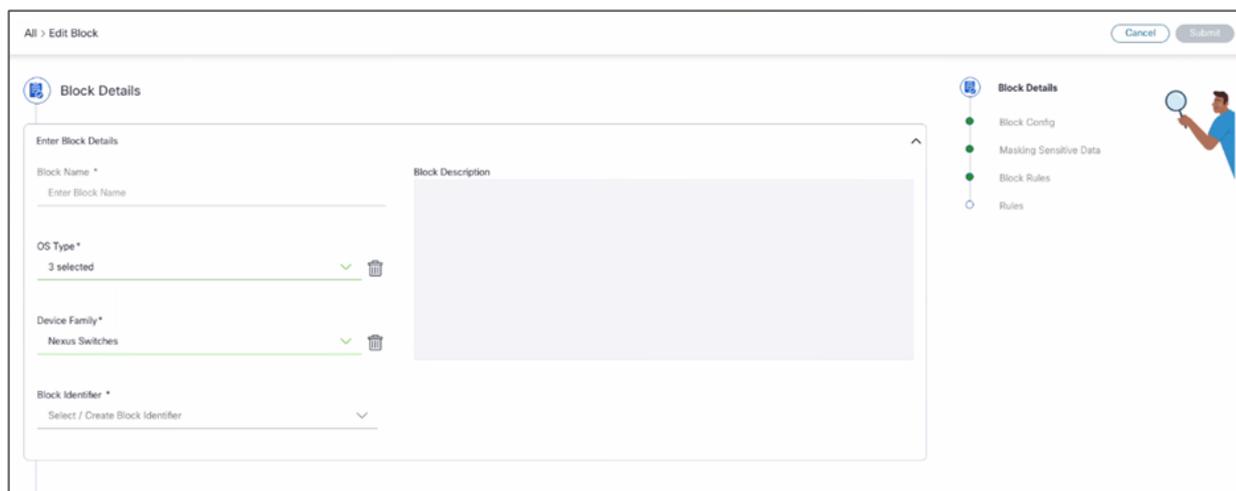
- ブロック構成:

Block Configセクションには次の内容が含まれます。

- 設定ブロック：さまざまな変数を組み込んだデバイスの設定を表します。この設定では、デ

バイスをシステム内で設定および管理する方法の概要を示します。

- TTPテンプレート：ブロックがTemplate Transformation Protocol(TTP)テンプレートとして指定されているかどうかを示し、複数のデバイス間で設定を変換または標準化するためのテンプレートとして使用されるブロックの識別に役立ちます。



The screenshot shows the 'Edit Block' interface. The main area is titled 'Block Details' and contains a form with the following fields:

- Block Name ***: A text input field with the placeholder 'Enter Block Name'.
- OS Type ***: A dropdown menu showing '3 selected'.
- Device Family ***: A dropdown menu showing 'Nexus Switches'.
- Block Identifier ***: A dropdown menu with the option 'Select / Create Block Identifier'.
- Block Description**: A large text area for entering a description.

On the right side, there is a sidebar with a navigation menu:

- Block Details (selected)
- Block Config
- Masking Sensitive Data
- Block Rules
- Rules

At the top right, there are 'Cancel' and 'Submit' buttons.

ブロックの詳細



The screenshot shows the 'Edit Block' interface, now displaying the 'Config Block' section. The main area is titled 'Config Block' and contains a form with the following fields:

- Config Block ***: A text area containing the following configuration snippet:

```
interface Loopback{{interface}}
shutdown {{SHUTDOWN_EXISTS | set("true") }}
description {{ DESC | re(".*") | let("DESC_EXISTS", "True") }}
ip address {{ipaddress}} {{ipsubnet}} #ignore_line
```
- TTP Template**: A toggle switch that is currently turned on.

On the right side, the sidebar navigation menu is updated:

- Block Details
- Block Config (selected)
- Masking Sensitive Data
- Block Rules
- Rules

At the top right, there are 'Cancel' and 'Submit' buttons.

ブロック構成

Ignore Line構文の使用

Ignore Line Syntaxを使用すると、ブロック内の特定の設定行の末尾にコメントを追加して、その行のコンプライアンスチェックや違反をスキップするようにシステムに指示できます。これにより、レポートまたはダッシュボードで品目が違反として表示されなくなります。

Ignore Line Syntaxを使用するには、次の手順を実行します。

1. コンプライアンスチェックから除外する設定行を探します (ipアドレスなど)。



行構文を無視

2. 行の末尾にコメント構文「#ignore_line」を使用して行を追加します。例: ip address {{ipAddress}} {{ipSubnet}} #ignore_line

違反の発生

ブロック構成のこのテンプレートテキストパーサー(TTP)機能を使用すると、特定の行が存在する場合に違反を発生させるかどうかを指定できます。

TTP機能を使用するには、次の手順を実行します。

1. ブロックの作成または編集ページのブロック設定セクションで、制御する設定行を見つけます。
2. 次のように、setまたはletコマンドを使用してTTP変数を定義します。
 - 設定行のshutdownが存在する場合は、setコマンドを使用して次のように変数を定義します。
シャットダウン| {{SHUTDOWN_FLAG | set("true")}}
 - description {{DESC}}のような既存の変数が設定行にある場合は、letコマンドを次のように使用します。
説明{{ DESC | re(".*") | let("DESC_EXISTS", "True") }}
3. ルールでこれらの変数 (前述の例ではSHUTDOWN_FLAGまたはDESC_EXISTS) を使用して違反を発生させます。



違反の発生

作用:

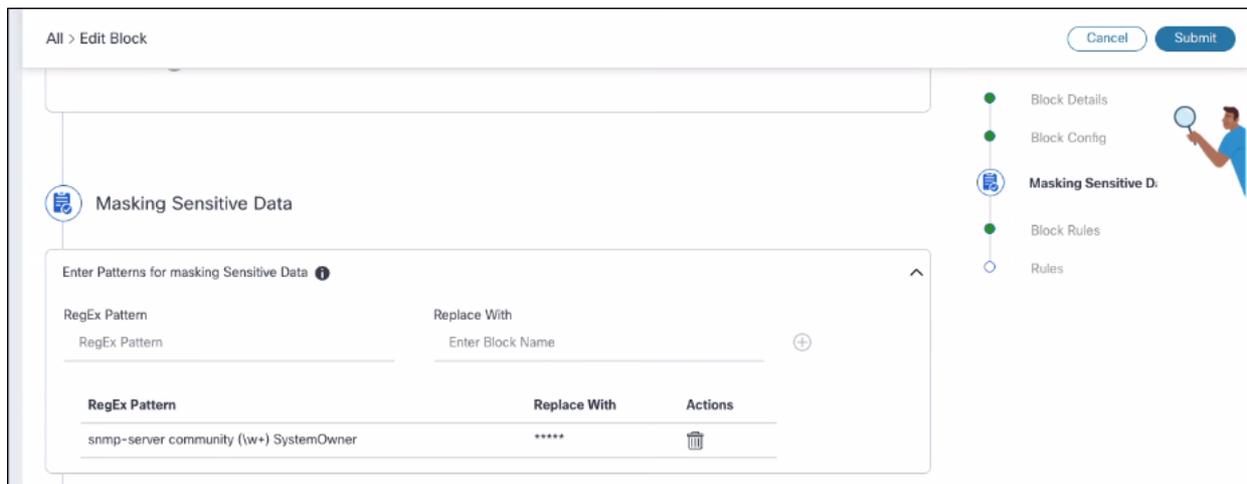
デバイス設定で「shutdown」行または「description config」行が使用できる場合、違反がダッシュボードページに表示されます。違反の重大度は、ルールの作成で行われた選択によって異なります。

- 機密データのマスク:

機密データのマスク機能は、ユーザが正規表現を使用してパターンを定義し、デバイス設定の機密情報（パスワードやキーなど）を特定してマスクできるようにします。これにより、一致するデータを指定されたマスク（「***」など）で置き換えることで、機密データが違反ビューや修復設定の違いに表示されることを防ぎます。

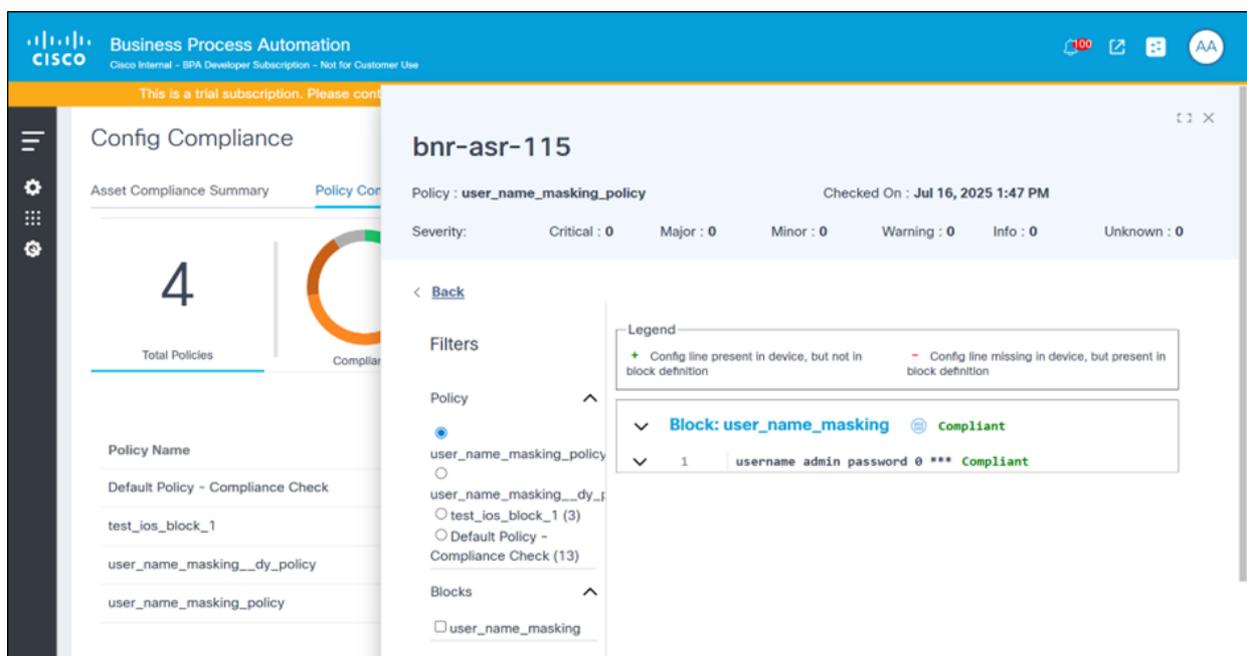
機密データをマスクするには、次の手順に従います。

1. [機密データのマスク]セクションで、次の操作を行います。
 - 機密データを識別するための複数の正規表現(regex)パターンの追加
 - 一致したデータをマスクする置換文字列を指定します（「」など）。たとえば、正規表現パターンには、「password」で始まり、その後に単語が続くテキストに一致するように、パスワードを入力できます。置換文字列はです。
2. 正規表現パターンを必要な数だけ追加します。それらはグリッド形式で表示されます



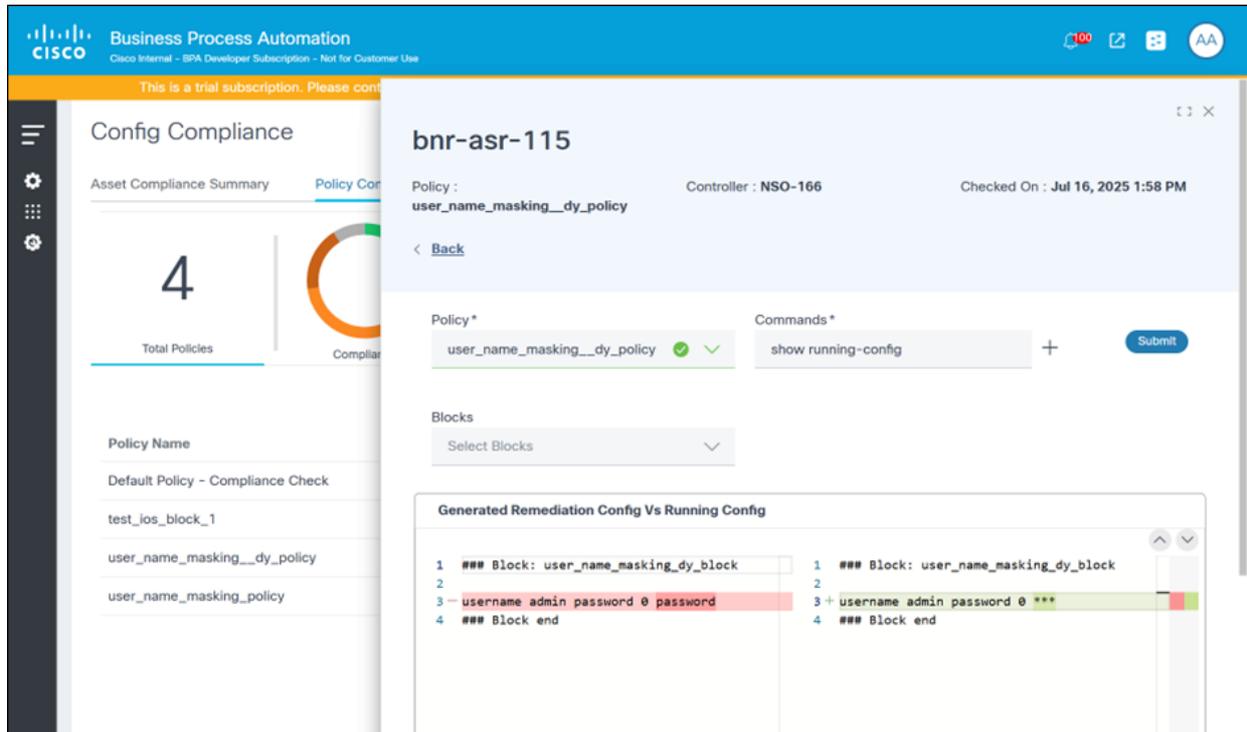
機密データのマスク

3. 不要になった場合は、リストからパターンを削除します。
4. システムは、正規表現を使用してデバイスの機密の設定データに一致するものを検索し、指定されたマスク(「***」など)に置き換えます。このマスキングは、次のページで使います。
 - コンプライアンスダッシュボード > 影響を受ける資産 > 違反の表示ページ:UIに表示される設定データと、これらの違反の詳細に基づいて生成される資産コンプライアンスレポート



違反の表示ページで機密データをマスクする

- コンプライアンスダッシュボード > 修復設定の表示 > 修復相違の表示：デバイス設定データには、ブロックのマスク設定に従って、マスクされた機密データが表示されます

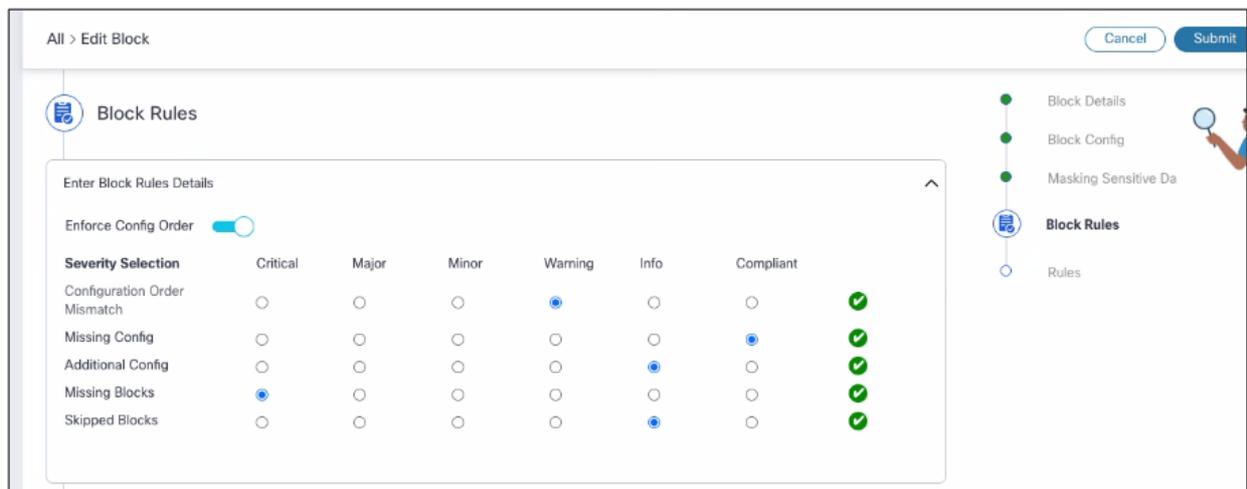


修復差分ページの機密データをマスクする

• ブロックルール (重大度の選択) :

「ブロック規則」セクションには、次の項目があります。

- 構成順序の強制：コンプライアンスチェック時に構成行が正しい順序で表示されるようにします。コンプライアンスエンジンは、構成行の順序を予期された順序と照合します。
- 重大度の選択：ユーザはブロック内の違反に重大度レベルを割り当てることができます。重大度レベルは、コンプライアンスの問題に対する優先順位の設定と管理を効果的に行うのに役立ちます。
- 構成順序の不一致：構成行の順序の不一致を特定し、デバイス構成行の順序が予期された順序と一致しない場合にアラートを表示します。
- 不足している構成：
 - 設定行の欠落を検出する
 - デバイスの設定に含まれていない設定行を強調表示します。
 - デバイス設定ブロック全体が欠落しているか、定義されたブロック設定と一致していないかを確認します
- 追加設定：
 - 予期しない設定行を特定します。
 - デバイス設定に存在するが、ブロック設定に従って予期されない設定行を表示します。
- スキップされたブロック：
 - チェックされていない設定ブロックを示します。
 - 指定したフィルタ条件を満たさないブロックはスキップされます



ブロックブロック規則を追加または編集する

ルール管理

CnRフレームワークでは、ユーザーは「ブロックの追加または編集」インターフェースを使用してブロック・ルールを管理できます。この機能は、次のセクションに示すように構成されています。

。

注： 特定のブロックレベル違反を発生させたくない場合は、重大度「Compliant」を選択できます。

- ルール設定:
 - ユーザは、コンプライアンスエンジンが設定を検証するために使用するルールを設定および管理できます
 - ユーザは必要に応じてルールを作成、編集、削除できます
- ルール一覧:
 - すべての作成済みルールの包括的なリストを提供し、ルールの詳細を可視化します。
 - ユーザは既存のルールを編集したり、不要になったルールを削除したりできます



構成ブロックの追加および編集

ルールの詳細の追加または編集

- [Rule Name] :
 - 識別のために規則に一意の名前を割り当てます
 - このフィールドは、各ルールを明確に認識するために必須です
- 既定の規則:
 - 規則を既定の規則として設定するかどうかを指定します
 - ユーザーはこの設定を有効にして、コンプライアンスフレームワーク内でルールを既定にすることができます
- [Description] :
 - 規則に関する追加のコンテキストまたは情報を提供します
 - このフィールドはオプションですが、説明と分かりやすさを保つために役立ちます
- 違反 :
 - ルールに関連付けられた違反の一覧を管理します
 - ユーザーは必要に応じて違反を追加、編集、削除できます

	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											

Add or Edit Blocks-Rules : ルールの追加または編集

ルール違反の追加または編集

ルール違反は、コンプライアンス実行の重要なコンポーネントであり、実行する必要がある特定のチェックの詳細を示します。ルール違反を作成および管理する方法の概要を次に示します。

- 基本モード:
 - ユーザインターフェイス要素 : このモードでは、グラフィカルユーザインターフェイス(GUI)を使用してルール違反を作成できます。この方法は、コーディングを行わないことを希望するユーザーにとって、通常は使いやすくアクセスしやすい方法です。
 - ステップバイステップのガイダンス : ユーザーは、事前定義されたUI要素を使用してチェックを定義するプロセスを通じてガイドされます。
- 詳細モード:
 - JSONに似たコード形式 : コーディングに慣れているユーザーのために、構造化されたJSONに似た形式で入力することで、ルール違反を作成できます。
 - 柔軟性と精度 : この方法では、複雑なルールチェックを定義する際の柔軟性と精度が向上します。

ルール違反の作成または編集 – 基本モード

ルール違反の作成または編集 – 詳細モード

ルール違反には、次のセクションがあります。

- 違反名：違反の名前
- 重大度：実行中にこの違反が失敗した場合のコンプライアンスの重大度を定義します
- 違反メッセージ：違反チェックが失敗すると、このメッセージが表示されます
- 違反フィルタ基準：非グループスキーマ変数を使用できる違反条件を適用します。
 - グループに含まれない個々のデータ要素に基づいて条件を設定するために、フィルタ条件で使用されます
 - データの階層と構造に従って基準を選択できるため、正確で関連性の高いフィルタリングが可能
- ルール条件：ここでコンプライアンスを確認するための実際の条件には、グループスキーマ

変数と非グループスキーマ変数の両方を使用できます

- 。両方のタイプの変数がルールで使用され、包括的な条件が作成されます
- 。グループ変数：関連するデータのコレクションに条件を適用し、構造化されたグループ内で十分なチェックを行うことができます
- 。非グループ変数：独立したデータ要素に条件を適用して、ルール適用の柔軟性を提供します。

動的なユーザ定義ブロック – ベストプラクティス

- 。変数名が各ブロック内で一意であることを確認します。
- 。グループ名に変数を使用することは避けてください。
- 。サブ階層の設定には、ブロック内で「<group>」を使用します。

例:

[https://ftp.readthedocs.io/en/latest/Writing%20templates/How%20to%20parse%20hierarchical%20\(configuration\)-to-parse-hierarchical-configuration-data](https://ftp.readthedocs.io/en/latest/Writing%20templates/How%20to%20parse%20hierarchical%20(configuration)-to-parse-hierarchical-configuration-data)

- 。1つの変数に含まれる類似した設定行の値を取得するには、その変数を `{{ <<var-name>> | line | joinmatches(',') }}` のように使用します。次の例のように、設定行を `{{ start }}` と `{{ end }}` の中に入れます。

デバイスの設定

```
ip domain list vrf Mgmt-intf core.cisco.com
ipドメインリストcisco.com
ipドメインリストeast.cisco.com
ipドメインリストwest.cisco.com
```

ブロック構成

```
{{_start_}}
ipドメインリスト{{ domains | _line_ |
joinmatches(',') }}
{{_end_}}
ip domain list vrf {{ vrf_name }} {{ vrf_domain }}
```

- 。設定行からスペースを含む値を取り込むには、次の表に示すように、ブロック内の変数を使用します。 `{{ <<var-name>> | re(".*") }}`

デバイスの設定

```
インターフェイスHundredGigE0/0/1/31
説明インターフェイス：12ylaa01 Hg0/0/1/31
mtu 9216
```

ブロック構成

```
インターフェイス{{ INTF_ID }}
説明{{ INTF_DESC | re(".*") }}
mtu 9216
```

ルールおよび非RefDルールにおけるルール階層および参照先統合の理解

ダイナミックブロックTTPには、設定の構造と検証の方法を決定する2つの異なるスキーマがあります。

- グループベーススキーマ:
 - このスキーマでは、設定が階層的に整理され、要素間に親子関係が確立されます
 - 要素が論理的にネストされ、相互に関連する複雑な構成に最適
 - ルールを定義して、異なる構成要素間の階層関係と依存関係を検証できます
- 非グループベーススキーマ:
 - 構成はフラットな形式で構成され、すべての要素は同じレベルに存在し、階層関係はありません
 - 階層を必要としない、より単純な構成に適している
 - 各構成要素が特定の基準を満たしていることを確認するルールを設定できます

参照先統合

- 参照Dの目的:
 - ロール:BPAフレームワーク内のローカルおよび外部変数を管理するためのツールとして機能します。
 - 機能:
 - 動的フェッチ：可変データの動的な取得と管理を容易にし、コンプライアンスチェックをリアルタイムのデータ変更に適応させます。
 - APIのインタラクション:BPAのユースケースにAPIを提供して、これらの動的変数と値にアクセスして管理し、コンプライアンスワークフローへのスムーズな統合を実現します

コンプライアンスルール値の構文

CnRのユースケースはRefDフレームワークと統合され、コンプライアンスチェックと修復ワークフロー内でデータを動的に利用します。この統合の仕組み、特に使用される構文と変数のタイプに関する詳細な説明を次に示します。

- キーワード：構文は「RefD」で始まる必要があります
- パラメータ：構文では「key」パラメータは必須です
- 例：

Copy Code

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

変数のタイプ

- ユーザー定義変数:
 - コンプライアンスジョブの作成時に設定されます。
 - 範囲：指定したジョブのすべての実行に適用されます
 - 構文: `{{VarName}}`
 - 例: `{{SITE}}`
- システム変数
 - 実行中に使用可能なコンテキストデータに基づいてフレームワークによって事前定義
 - 現在、フレームワークはデバイスオブジェクトへのアクセスを提供します
 - 構文: `{{#VarName}}`
 - 例:
 - `{{#device.deviceIdentifier}}`：デバイスIDを表します
 - `{{#device.additionalAttributes.serialNumber}}`：デバイスのシリアル番号を表します
- TTP変数
 - ブロック構成に存在する
 - 構文: `{{ VarName }}`
 - 例: `{{ INT_ID }}`

非参照D規則

- これらの規則はRefD規則に似ていますが、「RefD」キーワードで始まるものではありません
- 例：

plaintext

Copy Code

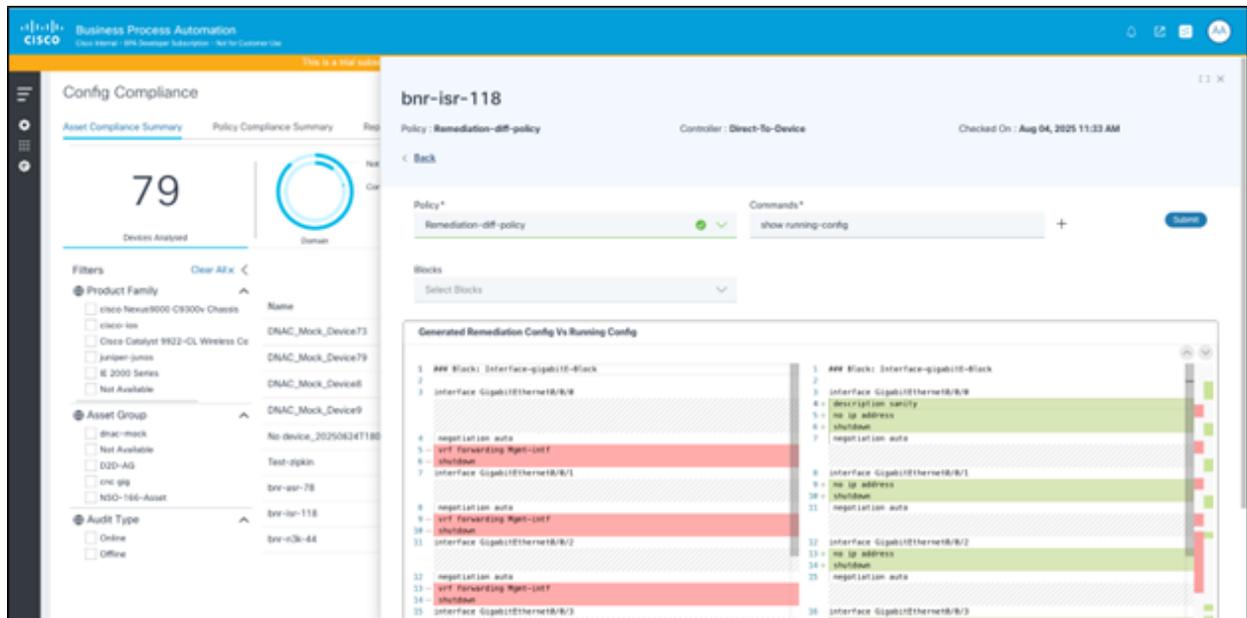
```
{{int_id}}.{{#device}}.{{ mtu_val }}
```

変数の使用

- ユーザー定義変数: `{{Var}}`として表されます
- システム変数: `{{#Var}}`として表され、`deviceIdentifier`、`controllerId`、`controllerType`などの属性を公開します。
- TTP変数：二重の中かっこで囲んで`{{var}}`と表されます

実行

- ジョブの作成時に\$変数を指定すると、その値を設定できます
- 変数の組み合わせ値は、コンプライアンスを確保するために、フェッチされたデバイス設定と比較されます



デバイス設定

	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						

構成ルール : RefD

ブロックの詳細の表示

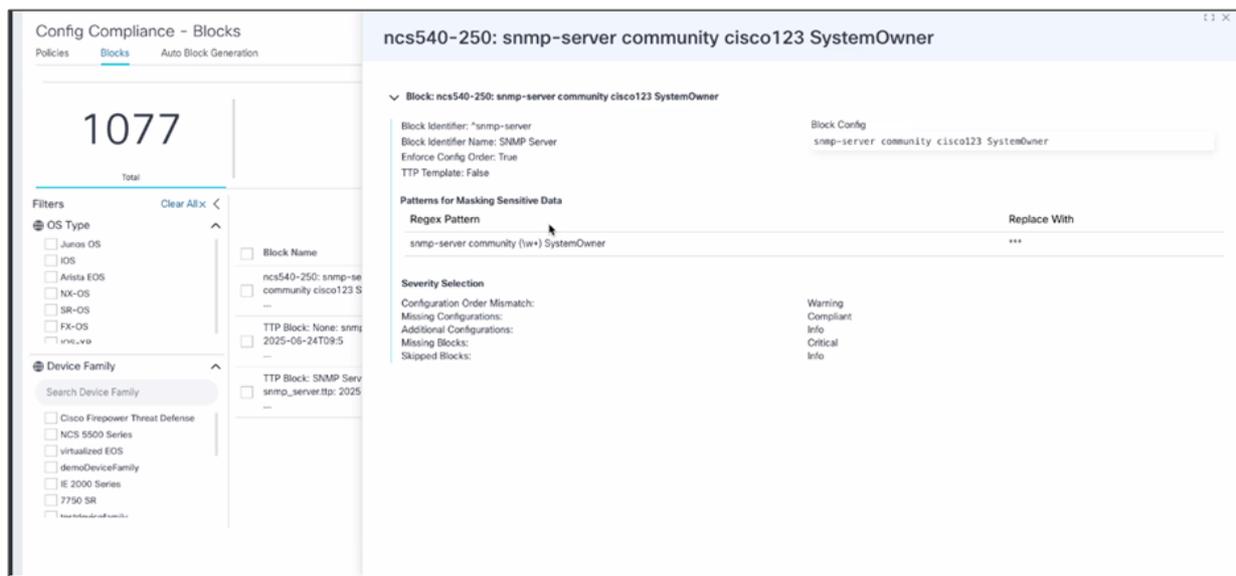
ブロックの詳細にアクセスするには :

1. Blocksページに移動します。
2. グリッドの行を選択またはクリックして、特定のブロックの詳細を表示します。「ブロック

の詳細」ページが画面右側に表示されます。

 注：このページには、ブロックに関連するすべての情報（関連するブロック、ルール、および違反を含む）が読み取り専用で表示されます。

詳細内のハイパーリンクをクリックすると、関連するブロックまたは関連情報にリダイレクトされます。



ブロックの詳細ビュー

ブロックの削除

ポータルでは、適切なRBAC権限を持っているユーザが1つ以上のブロックを削除できます。ユーザは、次の手順を実行することで、これらのアクションを実行できます。

シングルブロック削除の場合：

1. Blocksページに移動します。
2. 削除するブロックの横にあるMore Optionsアイコンをクリックします。
3. Deleteオプションを選択します。確認メッセージが表示されます。

複数ブロックの削除の場合：

1. Blocksページに移動します。
2. 削除する各ブロックの横にあるチェックボックスをオンにします。
3. More Optionsアイコンをクリックして、Deleteを選択します。確認メッセージ。

Reporting Configurations

Auto Delete Reports Older than(Days): ✔

Max Blocks to be selected in a Compliance Summary Report: ✔

Max Assets to be selected in a Compliance Detailed Report: ✔

ブロックを削除

設定：自動ブロック生成

ブロック生成により、ユーザはデバイスの設定に基づいてブロックを自動的に作成できます。この自動化により、手動での作成に必要な時間と労力が軽減され、ユーザは最初から作業を開始するのではなく、変数を追加または削除することでブロックを編集しやすくなります。

行をクリックすると、ブロック生成の詳細が表示されます。

Reports > Generate Report

Select Report Type* Enter Report Name* Time Period | Last three months

Summary Report Demo Policy Report

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

2

Devices



Compliance



Severity

Filters Clear All x

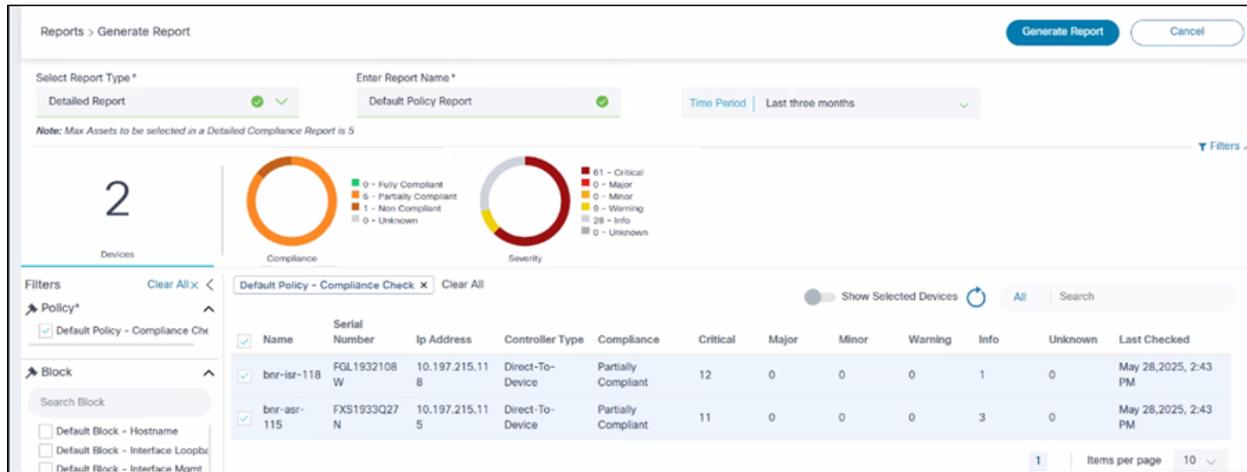
Policy* Default Policy - Compliance Check X Clear All

Default Policy - Compliance Chx Show Selected Devices All | Search

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	FXS1933027 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

自動ブロック生成リスト - ビュー



自動ブロック生成の詳細

自動ブロック生成

Report Name	Report Type	Report Format	Created At	Status	Created By	User Groups	Action
Default Policy Report	Compliance Details	Pdf	Jul 16, 2025, 11:26 AM	Initiated	admin		
Summary report	Compliance Summary	Excel	Jul 16, 2025, 10:36 AM	Completed	user001	Group-1	
Detail report	Compliance Details	Pdf	Jul 15, 2025, 6:29 PM	Initiated	user001	Group-1	
Detail report	Compliance Details	Pdf	Jul 15, 2025, 6:26 PM	Initiated	user001	Group-1	
Summary report	Compliance Summary	Excel	Jul 15, 2025, 6:24 PM	Completed	user001	Group-1	
test-d2d-09051_test-01_1752574358	remediation_batch_report	Pdf	Jul 15, 2025, 3:42 PM	Completed	admin		
rem-check2_batch-1_1752574286	remediation_batch_report	Pdf	Jul 15, 2025, 3:41 PM	Completed	admin		
summary-report1	Compliance Summary	Excel	Jul 14, 2025, 7:27 PM	Completed	admin		
summary-report-user1	Compliance Summary	Excel	Jul 14, 2025, 7:07 PM	Completed	user001	Group-1	
juniper-detailed-report	Compliance Details	Pdf	Jul 14, 2025, 6:08 PM	Completed	admin		

自動ブロック生成リスト

「自動ブロック生成」ページには、次のフィールドがあります。

- 生成元：ブロックが生成されるソース。次の3つのオプションがあります。
 - デバイス設定のバックアップ：システムはバックアップユースケースからデバイス設定を選択します

Policy Name		200-PasswordPolicy													
Policy Description															
OS Types		Junos OS													
Total validated assets		2													
Report Generated On		05-Aug-2023 15:00:27													
Compliance Status		Count		Severity Level		Count									
Fully Compliant	0	Critical	0	Partially Compliant	0	Major	0								
Non-Compliant	2	Minor	0	Unknown	0	Warning	2								
Unknown	0	Info	0	Unknown	0	Unknown	0								

Validated Assets												Compliance					
Name	Description	Controller Type	Managed By	IP Address	Software Type	Software Version	Product Family	Serial Number	Role	Product ID	Compliance	Critical	Major	Minor	Warning	Info	Unknown
024-juniper		Direct-To-Device	Direct-To-Device	1.2.3.4	JUNOSR JUNOS	ngfe 00000	Juniper-junos	AD82C409		03-3234-000-0	Non-Compliant	0	0	0	0	0	0
030-juniper19		Direct-To-Device	Direct-To-Device								Non-Compliant	0	0	0	0	0	0

デバイス設定のバックアップ

- ファイルのアップロード：ユーザがデバイス設定をアップロードできるファイルのアップロードウィンドウが開きます

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

ファイルのアップロード

- Current Config：システムがデバイス設定を取得するために使用するCLI設定コマンドを入力します。

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

現在の構成

- OS Type : このブロックが関連するOSタイプのリスト。
- デバイスファミリ : このブロックが関連するデバイスファミリのリスト。
- アセット : アセット機能は、ダイナミックブロックを生成するデバイスを選択するための構造化アプローチを提供します
 - 資産グループの選択:
 - ユーザは、事前に定義されたデバイスグループ (資産グループ) を選択できます。このグループは、動的ブロックの生成に使用されます
 - 場所、タイプ、機能などの特定の基準に基づいてデバイスをグループ化することで、デバイスの管理と編成を容易にします
 - サブセットデバイス選択:
 - ユーザは、選択した資産グループ内から特定のデバイスのサブセットを柔軟に選択できます
 - ユーザは特定のデバイスセグメントに集中できるため、よりターゲットを絞ったブロックの生成と管理が可能

Auto Block Generation Details

Generate From*
 Device Config Backup Override existing blocks

OS Type*
 3 selected

Device Families*
 All

Assets
 Asset Group*
 Juniper NSO asset Select All Devices

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

Block Identifier
 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	*(?)hostname	IOS,IOS-XR,NX-OS	hostname.ttp	false	1	

ブロック生成

- ブロック識別子 : ユーザがブロック生成時に使用するブロック識別子のリストを選択するオプションを提供します。また、ブロック識別子管理機能もインラインで提供します。

ブロック識別子

ブロックIDは、[CiscoConfParser](#)を使用して、デバイス設定全体から設定ブロックを抽出します。各ブロックIDは、正規表現パターンに関連付ける必要があります。ユーザは、UIまたはAPIを使用して、独自のブロック識別子を作成したり、既存のブロック識別子を更新したりできます。現在、このプラットフォームでは、推定55 ~ 60個のデフォルトブロックIDが提供されています。各識別子はOSタイプに固有であり、Ingesterサービスを介したBPAアプリケーションの導入時にロードされます。TTPテンプレートは、各ブロックIDに関連付けることができます。ブロック識別子の名前とパターンは両方とも一意である必要があります。

ブロックIDに対してMultiオプションが有効になっている場合、コンプライアンスフレームワークは、一致した設定から複数の設定ブロックを生成します。それ以外の場合は、一致するすべての設定を1つのブロックとして扱います。

MultiオプションがTrueのブロック識別子（インターフェイス、router bgp、vrf、l2vpnなど）の例

MultiオプションがFalseのブロック識別子の例：ロギング、snmp-server、ドメインなど

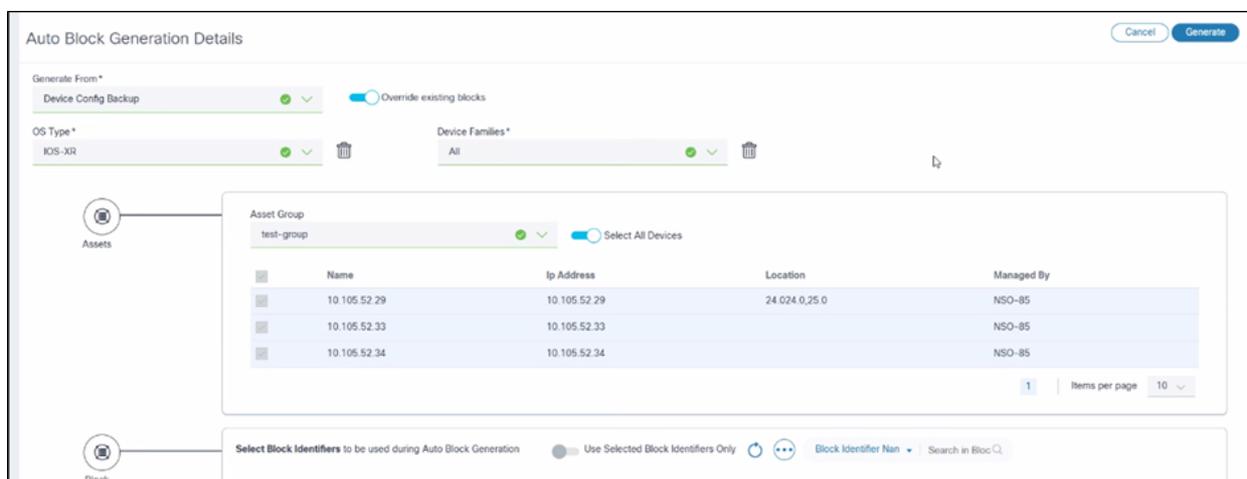
例:

```
{
  "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"]
}
```

リストブロック識別子

[ブロックIDを一覧表示]を使用すると、検索および並べ替え機能と共にブロックIDの一覧を表示できます。この機能は、Generate Blocksページで使用できます。



The screenshot shows the 'Auto Block Generation Details' page. It includes a 'Generate From*' dropdown set to 'Device Config Backup', an 'Override existing blocks' toggle, and dropdowns for 'OS Type*' (IOS-XR) and 'Device Families*' (All). Below these is an 'Assets' section with an 'Asset Group' dropdown set to 'test-group' and a 'Select All Devices' toggle. A table displays the following data:

Name	Ip Address	Location	Managed By
10.105.52.29	10.105.52.29	24 024 0,25 0	NSO-85
10.105.52.33	10.105.52.33		NSO-85
10.105.52.34	10.105.52.34		NSO-85

At the bottom, there is a 'Block' section with a 'Select Block Identifiers to be used during Auto Block Generation' toggle, a 'Use Selected Block Identifiers Only' radio button, and a search bar for 'Block Identifier Name'.

ブロックIDリスト

Auto Block Generation Details

Block Identifier

Select Block Identifiers to be used during Auto Block Generation Use Selected Block Identifiers Only Block Identifier Name Search in Bloc

Block Identifier Name	Block Identifier Pattern	OS Type	Template	Multi-Select	Template Count	Action
Interface TenGigabitEthernet	*interface TenGigabitEthernet	IOS,IOS-XR		True	0	
Interface GigabitEthernet	*interface GigabitEthernet	IOS,IOS-XR,NX-OS		True	0	
L2VPN	*l2vpn	IOS,IOS-XR		True	0	
vpn	*vpn	IOS-XR		False	0	
Router-Ospf	*router ospf	IOS-XR		True	0	
VRF	*vrf	IOS,IOS-XR,NX-OS	vrf.ttp	True	1	
Sensor Group	*sensor-group	IOS,IOS-XR,NX-OS	sensor_group.ttp	True	1	
SSH Server	*ssh server	IOS,IOS-XR,NX-OS	ssh_server.ttp	False	1	
Neighbor	*neighbor	IOS,IOS-XR,NX-OS	neighbor.ttp	True	1	
Neighbor Group	*neighbor-group	IOS,IOS-XR,NX-OS	neighbor_group.ttp	True	1	

1 2 3 ... 7 Next Items per page 10

ブロック識別子

ブロックIDを作成または編集

Business Process Automation

Config Compliance

Asset Compliance Summary Policy Compliance Summary Reports

85 Reports

Report Status

Filters

Report Type

Policy

Initiated

Report Name	Report Type	Report Format	Policy	Created At	Status	Created By	Action
mask-sensitive-report-check	Compliance Details	Pdf	Nflic-Remediation-policy	Aug 26, 2025, 12:45 PM	Completed	admin	
mask-sensitive-report	Compliance Summary	Excel	Nflic-Remediation-policy	Aug 26, 2025, 12:43 PM	Completed	admin	
Default	Compliance Summary	Excel	Default Policy - Compliance Check, Mask-sensitive-	Aug 25, 2025, 6:30 PM	Completed	admin	
Default Summary Report	Compliance Summary	Excel	Default Policy - Compliance Check	Aug 25, 2025, 6:28 PM	Completed	admin	
Default Report Summary	Compliance Summary	Excel	Default Policy - Compliance Check	Aug 25, 2025, 6:26 PM	Completed	admin	
Default Report	Compliance Details	Pdf	Default Policy - Compliance Check	Aug 25, 2025, 6:24 PM	Completed	admin	
duplicate-report-check	Compliance Details	Pdf	Default Policy - Compliance Check	Aug 22, 2025, 6:06 PM	Partially Completed	admin	
mask-sensitive-data-report	Compliance Details	Pdf	Mask-sensitive-policy	Aug 22, 2025, 5:47 PM	Completed	admin	
detailed-report-duplicate-check	Compliance Details	Pdf	Default Policy - Compliance Check	Aug 22, 2025, 12:45 PM	Completed	admin	
detailed-report-duplicatefix	Compliance Details	Pdf	Default Policy - Compliance Check	Aug 22, 2025, 12:43 PM	Completed	admin	

1 2 3 ... 9 Next Items per page 10

ブロックIDを編集

「自動ブロック生成」ページの「ブロック識別子リスト」セクションには、ブロック識別子を効果的に管理するためのツールが用意されています。機能は次のとおりです。

- ブロック識別子を作成
 - ユーザはリストに新しいブロック識別子を追加できます
 - これにより、ブロックの整理と区別に使用できる一意の識別子を導入できます
- ブロック識別子を編集
 - 既存のブロック識別子は変更可能
 - 識別子の更新または修正を可能にし、識別子が表すブロックに関連する正確な識別子を維持できるようにします。
- ブロックIDを削除

- 。 ユーザは、リストからブロック識別子を削除することができます
- 。 不要になった識別子や適用可能でない識別子を削除できるため、識別子の管理が容易になります。

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

ブロックIDを削除

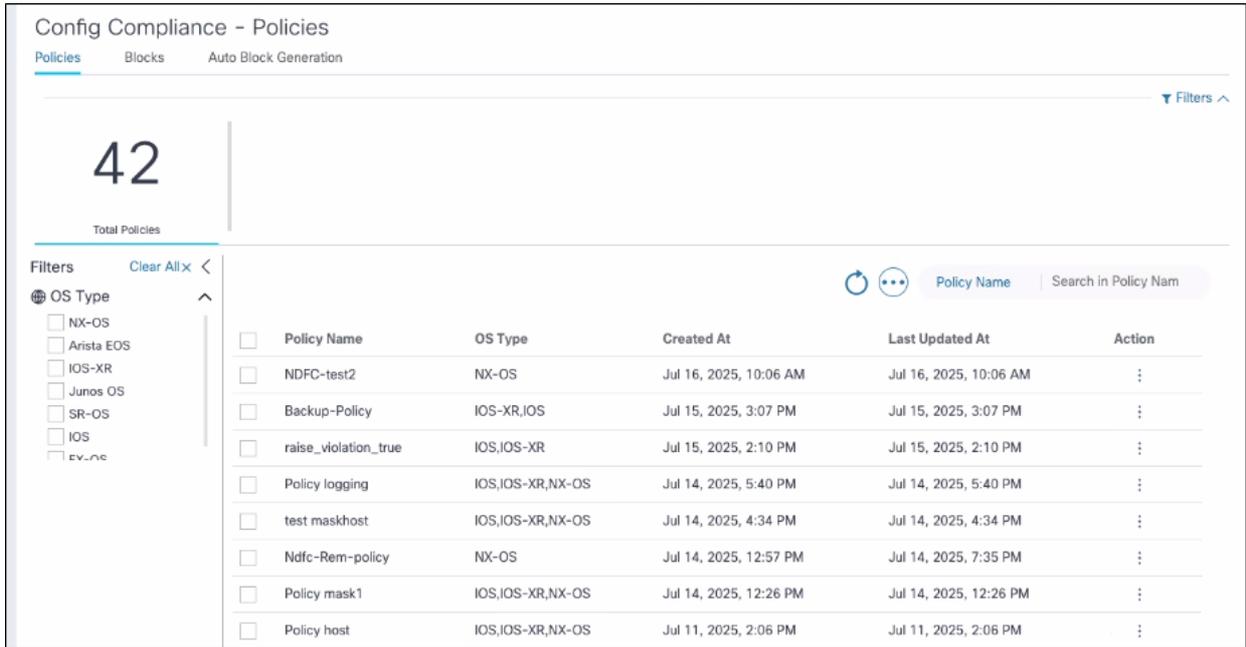
設定：ポリシー

Policiesタブでは、コンプライアンス実行を有効にする一連のポリシー、ルール、およびブロックを定義できます。ポリシーは、設定ブロックとルールで構成されるユーザ定義のテンプレートです。ポリシーを作成するための設定ブロックのリストと各設定ブロックのルールのリストを選択できます。

ポリシーの一覧表示

Policiesタブにポリシーのリストを表示できます。このタブには、ポリシーの追加、編集、削除、インポート、エクスポートのアクションもあります。

 注：ポリシーは、関連するブロックおよびルールとともにインポートまたはエクスポートされます。



<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	⋮

ポリシーの一覧表示

ポリシーの追加と編集

このセクションでは、「ポリシーの追加」および「ポリシーの編集」ページの概要を説明します。

ポリシーの詳細

- ポリシー名：ポリシーの名前
- OS Type：このポリシーでサポートされているOSタイプのリスト
- デバイスファミリ：このポリシーでサポートされるデバイスファミリのリスト
- ポリシーの説明（オプション）：ポリシーを簡単な説明とともに説明します。

OS TypeフィールドとDevice Familyフィールドには、次のセクションで選択したブロックに基づいて、値が自動的に入力されます。

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

```

Configuration Compliance - Asset Violations Report Page 1 of 4

構成ポリシー：ポリシーの詳細

ブロックを選択ダイアログ

「ブロックの選択」機能は、ユーザがポリシーに含める設定ブロックを選択できるように設計された使いやすいインターフェイスです。このセクションでは、その機能を示します。

- ポップアップダイアログ
 - 目的：ユーザが現在のページから移動せずに設定ブロックを選択できる専用スペースを提供します。
 - ユーザインタラクション：オプションを個別の専用ダイアログボックスに表示することで、直感的な選択プロセスを実現します。
- オプションの追加と選択
 - 複数選択：ユーザは、ポリシーに含める構成ブロックを1つ以上選択できます
 - 柔軟性：ユーザ固有のポリシー要件に基づいて、さまざまなブロックを含めることができます。
- ナビゲーション機能
 - フィルタ：ユーザは特定の条件に基づいて使用可能なブロックのリストを絞り込むことができます。これにより、関連するブロックを見つけやすくなります
 - ページネーション：ブロックを管理しやすいページに編成し、大量のデータのナビゲーションを改善します。
 - 検索機能：名前または他の識別子によるブロックの迅速な場所を指定できるため、選択プロセスが合理化されます

Delete Report



Are you sure you want to delete the report 'Default Policy Report' ?

Cancel

OK

ブロック選択

新しいブロックを作成するには、[ブロックの選択]セクションの[作成]をクリックします。新しいブラウザタブがクロス起動し、ユーザは新しいブロックを作成できます。送信すると、ユーザは元のタブに戻り、新しく作成したブロックを選択してポリシーに追加できます。

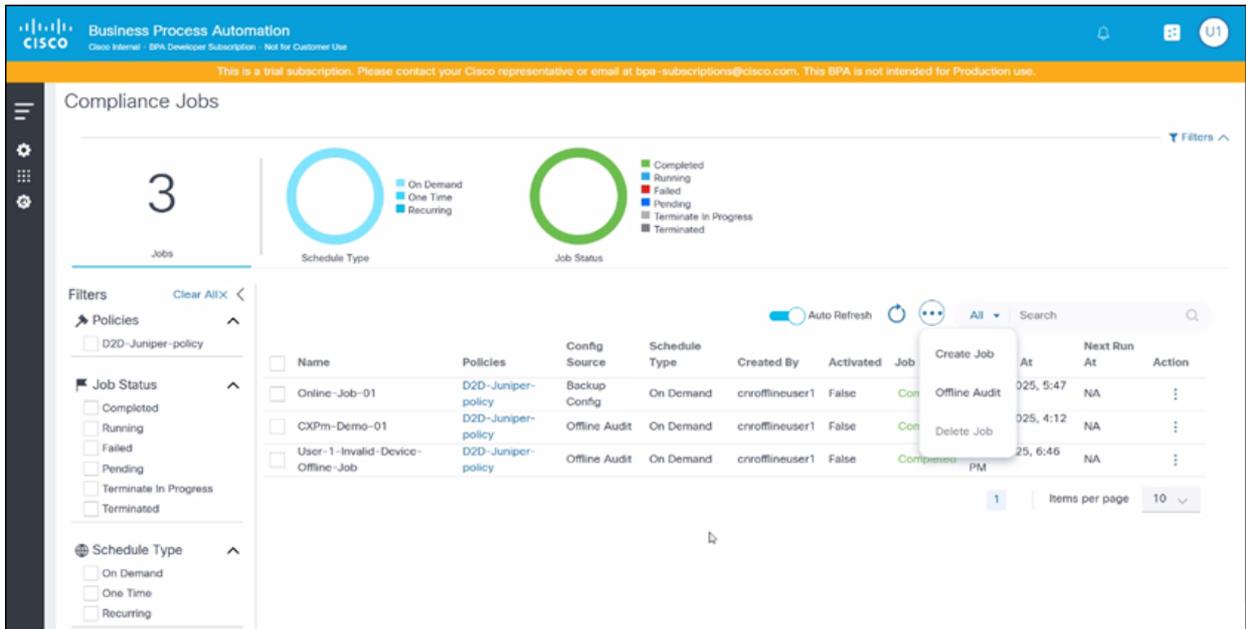
条件付きフィルタ

条件付きフィルタ機能は高度なツールで、ユーザは特定の基準を設定ブロックに適用し、正確で絞ったコンプライアンスチェックを実行できます。

- 事前定義済みの条件に基づいて、選択した構成ブロックに構成を適用したり、コンプライアンスチェックを実行したりできます。
- 指定された基準を満たさないブロックをフィルタリングして、リソースと作業を関連ブロックに集中させます。
- コンプライアンスチェックやその他のプロセスに構成ブロックを含めるために満たす必要がある条件を定義できます
- これらの条件に一致するブロックのみが実行され、他のブロックは無視されるため、より正確な制御が可能です

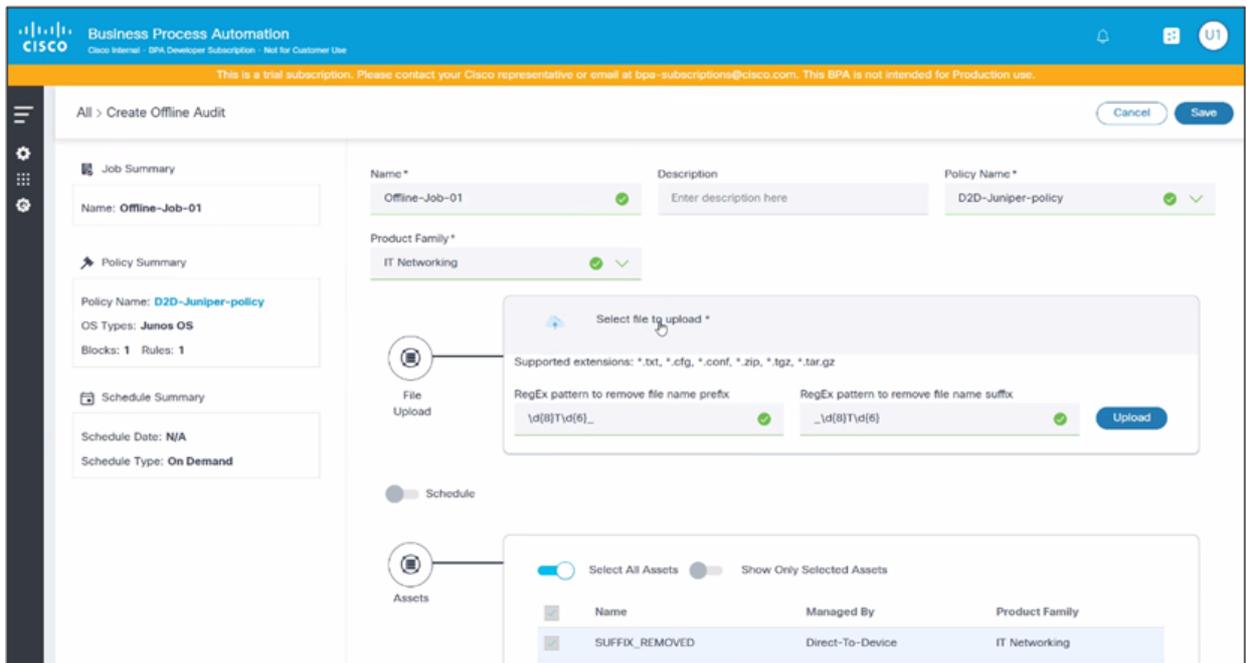
使用例:

- 選択的コンプライアンスチェック：ポリシーの目的が使用可能な20個のインターフェイスのうち2つの特定のインターフェイスでの設定のみをチェックすることである場合、ユーザは条件を設定して、コンプライアンスチェックをこれら2つのインターフェイスだけに制限できます。



条件付きフィルタ

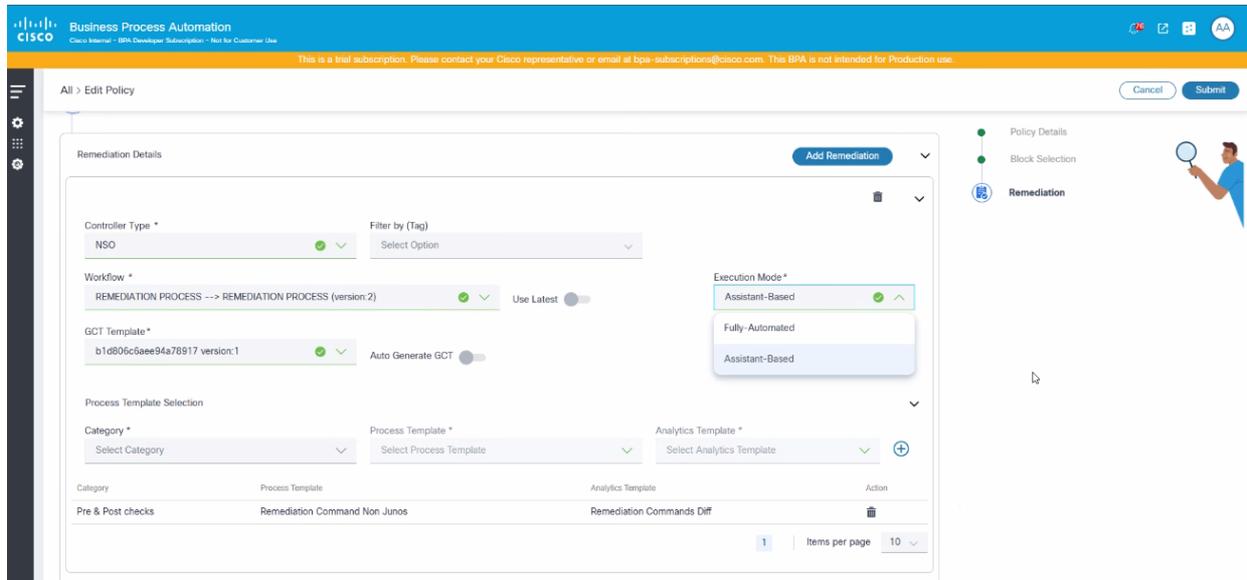
- [ルールを選択] : 特定の構成ブロックに対して1つ以上のルールを選択するオプション。



ルールの選択

Remediationセクション

Policiesページには、コントローラタイプごとの修復詳細を定義するオプションのセクションがあります。



設定ポリシー：修復の詳細

- Controller Type：修復をサポートするコントローラタイプのリスト
- 是正ワークフロー：選択したコントローラタイプのデバイスに対して実行されるワークフロー
- GCTテンプレート：適用する1つ以上のGCTテンプレート
- プロセステンプレート：チェック前とチェック後の両方のチェックの一部として、対応する分析テンプレートとともに実行される1つ以上のプロセステンプレート。
- 事前確認テンプレート：事前確認のためにのみ実行されるプロセス・テンプレートのオプション・リスト
- 小切手後テンプレート：小切手後にのみ実行されるプロセス・テンプレートのオプション・リスト
- 実行モード：
 - 完全自動：是正プロセスは、手動による介入やユーザタスクなしで自動的に実行されます
 - アシスタントベース：修復プロセス中に手動の支援を必要とするユーザタスクが作成されます

GCT機能の自動生成

Auto-Generate GCT機能は、修復に必要なGCTテンプレートの作成プロセスを合理化するように設計されています。次のように動作します。

- コンプライアンス実行の結果と詳細に基づいてGCTテンプレートを自動的に生成
- テンプレート作成プロセスを自動化
- 生成されたテンプレートは、コンプライアンスチェック中に特定された問題に対処するように調整され、修復アクションがコンプライアンスのニーズに合うようにします

ロールとアクセスコントロール

静的なアクセス許可の一覧

Next-Genポータルの設定準拠ダッシュボードでは、ルールと条件を処理するための設定のダイナミックテキストブロックがGUI表示でどのように表示されるかを表す次の権限を使用して、BPAのRBAC機能がサポートされています。

Group	アクション	説明
UIアプリケーション	コンプライアンスダッシュボード.show	コンプライアンスダッシュボードアプリの表示/非表示
UIアプリケーション	修復ダッシュボード.show	修復ジョブアプリの表示
UIアプリケーション	コンプライアンスジョブ.show	コンプライアンスジョブの表示アプリ
UIアプリケーション	コンプライアンス設定.show	コンプライアンス構成アプリの表示
コンプライアンスダッシュボード	資産コンプライアンス概要	資産準拠の概要の表示
コンプライアンスダッシュボード	ポリシーコンプライアンスの概要	ポリシーのコンプライアンスの概要の表示
コンプライアンスダッシュボード	違反の表示	違反の詳細の表示
コンプライアンスダッシュボード	ポリシーコンプライアンス資産の概要	影響を受ける資産の表示
コンプライアンスダッシュボード	レポートの表示	レポートダッシュボード、レポート設定の表示、およびレポートのダウンロード
コンプライアンスダッシュボード	レポートの管理	レポートの作成および削除
コンプライアンスダッシュボード	manageReportSettings	レポート設定の変更
修復ダッシュボード	修復ジョブの表示	是正ジョブの表示

Group	アクション	説明
修復ダッシュボード	修復マイルストーンの表示	修復マイルストーンの表示
修復ダッシュボード	修復ジョブの管理	ユーザタスクの作成、削除、アーカイブ、処理などの修復ジョブの管理
コンプライアンスジョブ	コンプライアンスジョブの表示	コンプライアンスジョブと実行の表示
コンプライアンスジョブ	コンプライアンスジョブの管理	コンプライアンスジョブの管理
コンプライアンス設定	コンプライアンス設定の表示	ポリシー、ブロック、ルール、ブロック生成、ブロック識別子、TTPテンプレートなどのコンプライアンス設定の表示
コンプライアンス設定	コンプライアンス管理ポリシー	コンプライアンスポリシーの管理
コンプライアンス設定	manageComplianceBlock	コンプライアンスブロックとルール、およびブロック識別子の管理
コンプライアンス設定	manageComplianceBlockGeneration	コンプライアンスブロック生成およびTTPテンプレートの管理

定義済みロール

設定のコンプライアンスと修復のユースケースには、次の表に示す定義済みのロールがあります。

 注：管理者は、顧客の要件に従ってロールを作成または更新できます。

ロール	説明	権限
コンプライアンス管理者	すべてのコンプライアンス関連の権限を持つ管理者ロール	UIアプリケーション: アセットマネージャの表示 - 資産グループの表示 - コンプライアンスダッシュボードの表示 - コンプライアンスジョブの表示 - コンプライアンス設定の表示

資産:

- アセットリストの表示
- 資産のバックアップ構成の表示
- バックアップ構成
- コントローラ対応デバイスアクションの実行

資産グループ:

- 資産グループの表示
- 資産グループの管理
- 動的資産グループの作成

バックアップ設定：デバイス設定のバックアップの表示、比較、ダウンロード

バックアップ復元ポリシー：バックアップ復元ポリシーの表示

コンプライアンスダッシュボード:

- 資産のコンプライアンス概要の表示
- ポリシーのコンプライアンス概要の表示
- 違反の表示
- 影響を受ける資産の表示
- レポートの作成および削除
- レポートダッシュボード、レポート設定、およびダウンロードレポートの表示
- レポート設定の変更：

コンプライアンスジョブ

- コンプライアンスジョブと実行の表示
- コンプライアンスジョブの管理

コンプライアンス設定:

- ポリシー、ブロック、ルールなどのコンプライアンス設定の表示

ロール

説明

権限

- コンプライアンスポリシーの管理
- コンプライアンスブロック、ルール、およびブロック識別子の管理
- コンプライアンスブロックの生成とTTPテンプレートの管理

UIアプリケーション:

- アセットマネージャの表示
- 資産グループの表示
- コンプライアンスダッシュボードの表示
- コンプライアンスジョブの表示
- コンプライアンス設定の表示

資産:

- アセットリストの表示
- 資産のバックアップ構成の表示
- バックアップ構成
- コントローラ対応デバイスアクションの実行

資産グループ:

- 資産グループの表示
- 資産グループの管理
- 動的資産グループの作成

バックアップ設定：デバイス設定のバックアップの表示、比較、ダウンロード

バックアップ復元ポリシー：バックアップ復元ポリシーの表示

コンプライアンスダッシュボード:

- 資産コンプライアンスの概要の表示
- ポリシーのコンプライアンスの概要の表示
- 違反の表示
- 影響を受ける資産の表示
- レポートの作成および削除

コンプライアンス演算子

構成管理を除くすべてのコンプライアンス権限を持つオペレータロール

ロール

説明

権限

レポートダッシュボード、レポート設定、およびダウンロードレポートの表示

コンプライアンスジョブ:

コンプライアンスジョブと実行の表示

-コンプライアンスジョブの管理

コンプライアンス設定:

ポリシー、ブロック、ルールなどのコンプライアンス設定の表示

UIアプリケーション:

-アセットマネージャの表示

-資産グループの表示

-コンプライアンスダッシュボードの表示

-コンプライアンスジョブの表示

-コンプライアンス設定の表示

資産:

アセットリストの表示

-資産のバックアップ構成の表示

-コントローラ対応デバイスアクションの実行

資産グループ:

-資産グループの表示

バックアップ設定: デバイス設定のバックアップの表示、比較、ダウンロード

バックアップ復元ポリシー: バックアップ復元ポリシーの表示

コンプライアンスダッシュボード:

資産準拠の概要の表示

コンプライアンス (読み取り専用)

コンプライアンスユースケースに関連するすべての読み取り専用アクセス許可を提供します

ロール

説明

権限

- ポリシーのコンプライアンスの概要の表示
 - 違反の表示
 - 影響を受ける資産の表示
- レポートダッシュボード、レポート設定の表示、およびレポートのダウンロード

コンプライアンスジョブ:

コンプライアンスジョブと実行の表示

コンプライアンス設定:

ポリシー、ブロック、ルールなどのコンプライアンス設定の表示

UIアプリケーション:

- アセットマネージャの表示
- 資産グループの表示
- 修復ダッシュボードの表示

資産:

- 資産リストの表示

資産グループ:

- 資産グループの表示
- 資産グループの管理
- 動的資産グループの作成

修復ダッシュボード:

- 修復ジョブの表示
- 修復マイルストーンの表示
- 資産コンプライアンスの概要の表示
- ユーザタスクの作成、削除、アーカイブ、処理などの修復ジョブを管理する
- 影響を受ける資産の表示

UIアプリケーション:

是正管理者/是正者

すべての修復関連の権限を持つオペレータロール

修復は読み取り専用

修復ユースケースに関連するすべての読み取り専用ア

ロール

説明

権限

アクセス許可を提供します

- アセットマネージャの表示
- 資産グループの表示
- 修復ダッシュボードの表示

資産:

- 資産リストの表示

資産グループ:

- 資産グループの表示
- 動的資産グループの作成

修復ダッシュボード:

- 修復ジョブの表示
- 修復マイルストーンの表示
- 資産コンプライアンスの概要の表示
- 影響を受ける資産の表示

アクセスポリシー

アクセスポリシー機能により、ユーザは特定のコンプライアンスポリシーと資産グループに適切にアクセスできるようになります。この機能を使用すると、管理者はユーザの役割と責任に基づいてアクセス制御を定義および適用できるため、セキュリティと運用効率が向上します。アクセスポリシーは、管理者がポリシーを作成、編集、およびユーザまたはグループに割り当てることができる[アクセスポリシー]ページで管理します。管理者は、詳細な権限を定義し、各ユーザまたはグループが表示、編集、管理できるコンプライアンスポリシーおよび資産グループを指定できます。このレベルの詳細は、機密情報や重要な操作を厳密に制御する上で役立ちます。

アクセスポリシーを定義すると、現在のユーザがアクセスできるCnRポリシーとアセットのリストに基づいて、次世代UIのすべてのコンプライアンスページと修復ページでデータが制限されます。

ユーザアクセスを提供するには：



注：アクセス許可を提供できるのは管理者だけです。

1. ユーザを作成し、それらをユーザグループに割り当てます。
2. ユーザロールを作成し、作成したユーザグループに割り当てます。
3. 資産グループに資産を追加します。
4. コンプライアンスポリシーリソースを割り当てるリソースグループを作成します。
5. アクセスポリシーを作成し、関連するユーザグループ、資産グループ、およびリソースグループを選択します。

リソースグループの作成

Resource Type ドロップダウンリストから compliance remediation-policy を使用してリソースグループを作成し、それぞれのユーザグループへのアクセス権を付与する必要があるコンプライアンスポリシーを選択します。

The screenshot shows a dialog box titled "Add Resource Group". It has a close button (X) in the top right corner. The "Resource Group name" field contains "CnR-Policy" with a green checkmark. The "Resource Type" dropdown is set to "compliance-remediation-policy" with a green checkmark and a dropdown arrow. The "Description" field is empty with a placeholder "Enter resource group description" and a search icon. Below the description field is a list of policies with checkboxes:

<input type="checkbox"/>	Name
<input type="checkbox"/>	C8kvPolicy
<input type="checkbox"/>	CNC6Policy
<input type="checkbox"/>	CNCRegPolicy
<input type="checkbox"/>	CNCRemPolicy
<input type="checkbox"/>	Class-Map-Policy-01
<input type="checkbox"/>	DNACRegPolicy
<input type="checkbox"/>	Default Compliance Policy
<input type="checkbox"/>	Default Policy - Compliance Check
<input type="checkbox"/>	Default Policy - RefD - Compliance Check
<input type="checkbox"/>	Default Policy - RefD - Compliance Check1

リソースグループの作成

アクセスポリシーの作成

ユーザグループに権限を付与する必要があるリソースグループと資産グループを含むアクセスポリシーを作成します。

The screenshot shows the 'Add Policy' configuration page. It features a 'Policy name' field with the value 'Access Policy Name' and a green checkmark. Below it is a 'Description' field with the placeholder text 'Enter policy description'. There are three selection panels: 'Resource Groups' with 'CnR-Resource-Group' selected, 'Asset Groups' with '2408devicegroup12', '402-dg', and 'A1' selected, and 'User Groups' with 'svcacct' selected. At the bottom, there are 'Cancel' and 'Submit' buttons.

アクセスポリシーの作成

オフラインコンプライアンス

オフラインコンプライアンス機能を使用すると、ユーザは、資産インベントリ内のアクティブなデバイスでは使用できないデバイス構成に対してコンプライアンスチェックを実行できます。

ユーザは、デバイスのバックアップ構成を使用するか、コンプライアンスジョブでオフライン監査を作成することで、オフラインコンプライアンスを実行できます。実行の結果は、コンプライアンスダッシュボードで確認できます。

デバイスバックアップ設定の使用

管理者は、必要なデバイスセットの実行コンフィギュレーションを含むzipファイルを手動でアップロードできます。この機能は、バックアップと復元アプリケーションのDevice Config - Uploadセクションで使用できます。デバイス設定をアップロードしたら、デバイス設定のソースとしてDevice Backup Configを選択することで、目的のデバイスのコンプライアンスジョブを作成できます。実行時に、アップロードされたデバイス設定がバックアップアプリケーションから取得され、コンプライアンスチェックが実行されます。

コンプライアンスジョブでのオフライン監査作成機能の使用

デバイス設定に対するコンプライアンスをオフラインで実行するには、コンプライアンスジョブページのその他オプションアイコンからオフライン監査を選択します。これにより、ユーザは実行コンフィギュレーションを含むzipファイルをコンプライアンスアプリケーションに手動で直接アップロードできます。実行中に、アップロードされたデバイス設定が解析され、コンプライアンスチェックが実行されます。

Ingesterによる構成の展開

Ingesterフレームワークを使用して、コンプライアンス構成アーティファクトのロードを自動化できます。アーチファクトを開発したら、次の手順を使用してエクスポート、パッケージ化、ターゲット環境への配布を行うことができます。

- 次のコマンドを使用して、NPMパッケージを作成します。

```
mkdir <
```

```
cd < >
```

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

- BPAポータル (クラシックUI) からの設定のエクスポート
 - BPA Classic UI > Configuration Compliance & Remediation > Configurationsの順に移動します。
 - 「TPテンプレート/ブロック識別子/ブロック/ルール/ポリシー」のエクスポート
- エクスポートされたファイルの名前を次のように変更します。
 - TTPテンプレート : <<filename>>.cnrttptemplate.json
 - ブロック識別子 : <<filename>>.cnrblockidentifier.json
 - ブロック : <<filename>>.cnrblock.json
 - ルール : <<filename>>.cnrrule.json
 - ポリシー : <<filename>>.cnrpolicy.json
- 入力データのパッケージ(.tgz)
 - エクスポートしたすべてのファイルを「ステップ1」で作成したnpmパッケージにコピーします。
 - npmパッケージ内で`npm pack`コマンドを実行し、「.tgz」ファイルを作成します。
- BPAシングルノード環境への入力データ(.tgz)の導入
 - BPAバンドルが導入されているサーバの<<BPA core bundle>>/packages/dataフォルダに.tgzファイルをコピーします
 - Ingesterサーバを再起動します(`docker restart ingester-service`)。
- BPAマルチノード環境へのIngesterデータ(.tgz)の導入

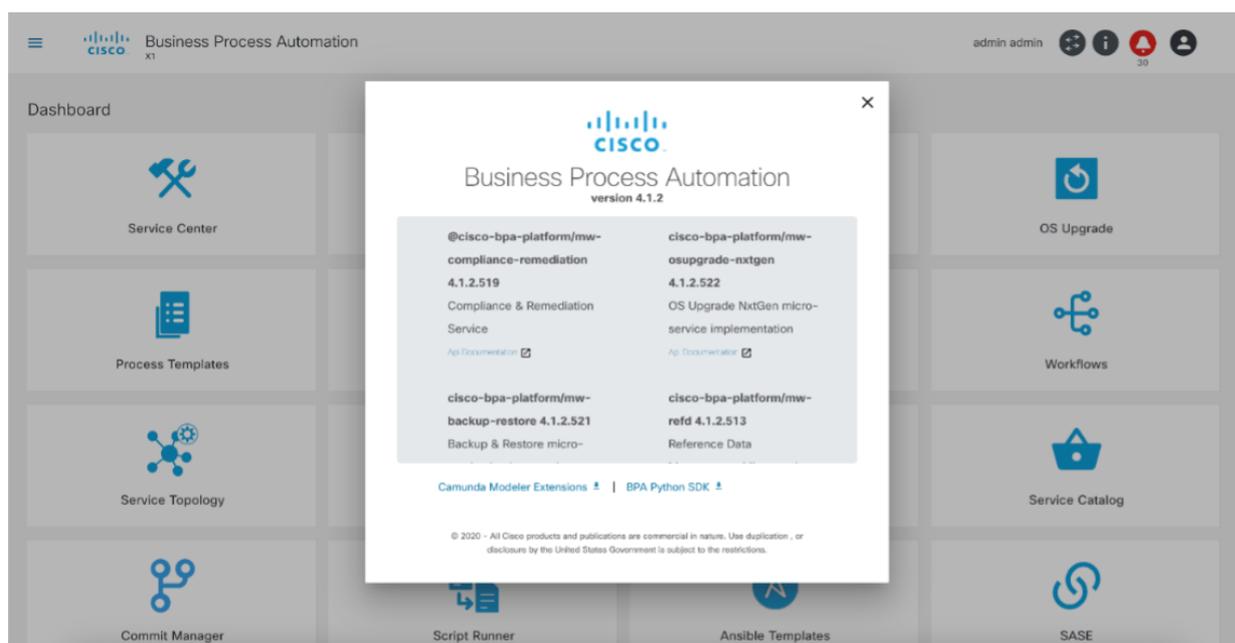
- .tgzファイルを、helmチャートが展開されているサーバの/opt/bpa/packages/dataフォルダにコピーします
- Ingesterポッドの再導入(kubectlロールアウトの再起動、導入ingester-service -n bpa-ns)

参考資料

[名前(Name)]	説明
TTP	設定ブロックで使用されるテンプレートテキストパーサー
会議パーサー	CLIデバイス設定の解析に使用される設定フィールドパーサー

API ドキュメント

コンプライアンスと修復に関するAPIドキュメントの詳細は、従来のUIの[バージョン情報]ポップアップで確認できます。



BPAバージョン情報 (クラシックUI)

トラブルシューティング

ダッシュボード

最近のコンプライアンスジョブの結果が表示されない

確認：最新のコンプライアンスジョブの結果は、次世代ポータルダッシュボードに表示されません。

考えられる原因1：ダッシュボードで日付範囲が選択されており、デフォルトで「今月」に設定されている。新しい月が最近開始された場合（たとえば、今日が最初の月である場合）、昨日（前月の最後の日）より前に実行された実行は表示されません。

分析：ダッシュボードで正しい日付範囲（必要に応じて前月の日数を含む）が選択されていることを確認し、適切な違反データが表示されるようにします。

考えられる原因2：異なるユーザーが同じポリシーまたは資産の組み合わせでコンプライアンスジョブを実行した可能性があります。ダッシュボードには、選択した日付範囲内の最後の実行時に見つかった違反が表示されます。

分析：管理者（またはすべてのコンプライアンスジョブへのアクセス権を持つユーザー）として、コンプライアンスジョブのリストとその履歴を確認し、実行するポリシーまたは資産グループの組み合わせを決定します。

コンプライアンスジョブ

実行ステータス全体が「スキップ済み」に設定される

確認：コンプライアンスジョブの実行中、実行ステータス全体が「スキップ済み」としてマークされます。違反は報告されません。

考えられる原因：同じジョブの既存の実行がまだ実行中です。

分析：コンプライアンスジョブでは、任意の時点で実行状態にできる実行は1つだけです。以前の実行がまだ実行されているかどうかを確認します。長時間スタックまたは実行中の実行は終了できません/

デバイスステータスが「スキップ済み」に設定される

確認：コンプライアンスジョブの実行では、一部のデバイスのステータスが「スキップ済み」とマークされます。

考えられる原因：デバイスが属するコントローラタイプのコンプライアンス機能が有効になっていません。

分析：コンプライアンスポリシーは、この機能が有効になっている資産グループ内のデバイスにのみ適用されます。

デバイスステータスが「Failed」に設定される

確認：コンプライアンスジョブの実行では、一部のデバイスのステータスが「Failed」とマークされます。

考えられる原因：コンプライアンス実行プロセス中に発生したランタイムエラーです。これらのエラーは、ポリシー、ブロック、ルール、ブロックIDなどのコードエラーや誤った設定である可能性があります。

分析：

ランタイムエラーの原因を特定するためのAPI:

1. 実行IDを見つけるために実行を取得します

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

コンプライアンス実行

メソッド：GET

2. 実行IDを使用したデバイス実行の取得

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

compliance-device-executionの場合

executionId=<< exeution-id >>

メソッド：GET

コンプライアンス規則

ルールに空の値が表示される

確認：コンプライアンスジョブの実行中、ルール変数には空の値が表示されます。

分析：

1. RefDアプリケーションからデータを取得する場合は、RefDキーが正しい形式であることを確認します。一致する場合は、RefDアプリケーションにルールのコンプライアンス変数にリンクされたキーのデータがあることを確認します。また、コンプライアンスサービスマニタリングを確認して、コンプライアンスアプリから正しいRefDキーが送信されていることを確認します。『[ルールおよび非参照Dルールにおけるルール階層および参照d統合について](#)』を参照してください。
2. 次のAPIを使用して、コンプライアンスブロックの実行結果を確認します。

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

メソッド: 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: 200

Pretty Raw Preview Visualize JSON

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

コンプライアンスブロックの実行の結果

3. ブロックにサブ階層または単一階層があるかどうかを確認し、ルールが階層に従って設定されていることを確認します。

1 Key*
bridge_group

Filter Criteria

Expr*
all

Key*	Operation*	Value*
1 BRIDGE_GROUP_NAME	Equals	MOB_22BT_42RW_IPA001

Rules

Expr*
all

Key*	Operation*	Value*
1 BRIDGE_GROUP_NAME	Equals	MOB_22BT_42RW_IPA001
2 Key* bridge_domain		

Filter Criteria

Expr*
all

Key*	Operation*	Value*	
1 BRIDGE_DOMAIN_NAME	Equals	MOB_22BT_42RW_IPA001	+ -

Rules

Expr*
all

Key*		
1 vfi		+ -

Filter Criteria

Expr*
all

Key*	Operation*	Value*	
1 VFI_NAME	Equals	MOB_22BT_42RW_IPA001	+ -

コンプライアンスブロックの実行の結果

4. 次のPythonスクリプトを実行して、TTPパーサーがデバイスコンフィギュレーションから値を抽出していることを確認します。

```
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)
```

コンプライアンスログの監視

シングルノード環境:

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

Multi Node Kubernetes Env:

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

Kibanaログ監視:

```
https://<< BPAホスト >>:30401
```

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。