Guia do usuário do BPA Conformidade e correção de configuração v5.1

Introdução

O aplicativo CnR (Configuration Compliance and Remediation, Conformidade e correção de configuração) permite que os operadores de rede realizem verificações de conformidade de configuração de dispositivos para políticas personalizadas construídas a partir de blocos de configuração. Os operadores criam manualmente ou automaticamente blocos de configuração usando o sistema de configurações de dispositivos selecionados. Os usuários também podem estabelecer regras que se apliquem a esses blocos, com condições de regras potencialmente derivadas de valores obtidos do aplicativo RefD. Os operadores podem executar convenientemente verificações de conformidade de acordo com um cronograma ou iniciá-las instantaneamente.

O aplicativo apresenta um painel de controle intuitivo, apresentando uma visão geral abrangente das violações de conformidade, oferecendo resumos e visualizações detalhadas nos níveis de bloco do dispositivo e da configuração.

O aplicativo inclui uma estrutura robusta de remediação para lidar com infrações de conformidade. Essa estrutura aproveita fluxos de trabalho e modelos — tanto modelos de configuração, conhecidos como modelos de configuração dourados (GCTs) quanto modelos de processo — para simplificar o processo de correção. Da mesma forma que as verificações de conformidade, as tarefas de remediação podem ser programadas para serem executadas em um cronograma ou acionadas imediatamente para solucionar violações imediatamente.

O painel de controle de Conformidade e Correção do portal de próxima geração (Next-Gen) tem recursos projetados para aprimorar o gerenciamento de segurança de rede, simplificar procedimentos de conformidade e simplificar atividades de correção. O painel fornece um resumo abrangente da conformidade de ativos e políticas, facilitando para os operadores de rede avaliar a integridade de sua rede e garantir que os dispositivos estejam em conformidade com protocolos de segurança rigorosos.

Os blocos de configuração podem ser gerados automaticamente e depois editados ou adicionados manualmente, oferecendo um equilíbrio entre automação e personalização. A identificação precisa do sistema de blocos de configuração e mecanismos de controle de acesso granulares, incluindo configurações detalhadas de usuário, grupo e permissão em interfaces clássicas e modernas, garantem que as configurações de rede permaneçam seguras e nas mãos de pessoal confiável. Esses recursos fornecem um poderoso conjunto de ferramentas para organizações que buscam manter altos padrões de conformidade e segurança de rede.

O que há de novo

Foram apresentados os seguintes recursos e aprimoramentos principais:

- Um painel de relatórios abrangente para gerar, exibir e fazer download de relatórios de conformidade
- Capacidade de executar auditorias de conformidade off-line por meio do upload de configurações do dispositivo sem a integração do dispositivo usando o Asset Manager
- Capacidade de configurar padrões na configuração de blocos para mascarar dados confidenciais de configuração de dispositivos
- Capacidade de exportar dados de grade de resumo de conformidade de ativos e políticas como arquivos CSV
- Exibir e comparar as configurações de correção geradas com as configurações em execução do dispositivo
- Melhorias nos blocos para suportar o aumento de violações se a configuração existir
- Permitir uma experiência de usuário conectado em páginas de criação e edição de políticas para iniciação cruzada em componentes filho, como a página de criação de blocos
- Aprimoramento nas tarefas de conformidade criação e edição de páginas para lançamento cruzado na página de edição de política

Componentes

Compatibilidade e correção suportam os seguintes controladores e tipos de dispositivos:

Controlador	Tipos de SO
NSO (6.5)	IOS XE, IOS XR, NX-OS, JunOS, Nokia SR-OS
CNC (6,0)	IOS XE, IOS XR, NX-OS
NDFC (3.2.0 / Fabric v12.2.2)	NX-OS
Cisco Catalyst Center (2.3.5)	IOS XE, IOS XR Conformidade validada apenas
CVP (7.2.5)	FX-OS (FTD). Conformidade validada apenas
Direcionar para dispositivo (D2D)	IOS XE, IOS XR, JunOS

Note: O suporte ao Nokia SR-OS através do controlador NSO só é aplicável para o recurso de conformidade de configuração. A correção não é suportada para dispositivos Nokia.

Note: O recurso de conformidade funciona com a configuração de dispositivos no formato da Interface de Linha de Comando (CLI - Command Line Interface) da Cisco e no formato do tipo YAML para dispositivos Juniper e Nokia. Atualmente, a estrutura não suporta outros formatos como Netconf, JSON, XML, etc.

Como parte da versão v5.0, o aplicativo clássico CnR (Compliance and Remediation) foi substituído. Todos os recursos do CnR agora estão totalmente integrados e disponíveis no portal de próxima geração.

Pressupostos e pré-requisitos

Os pré-requisitos a seguir são necessários para o uso eficaz do caso de uso CnR.

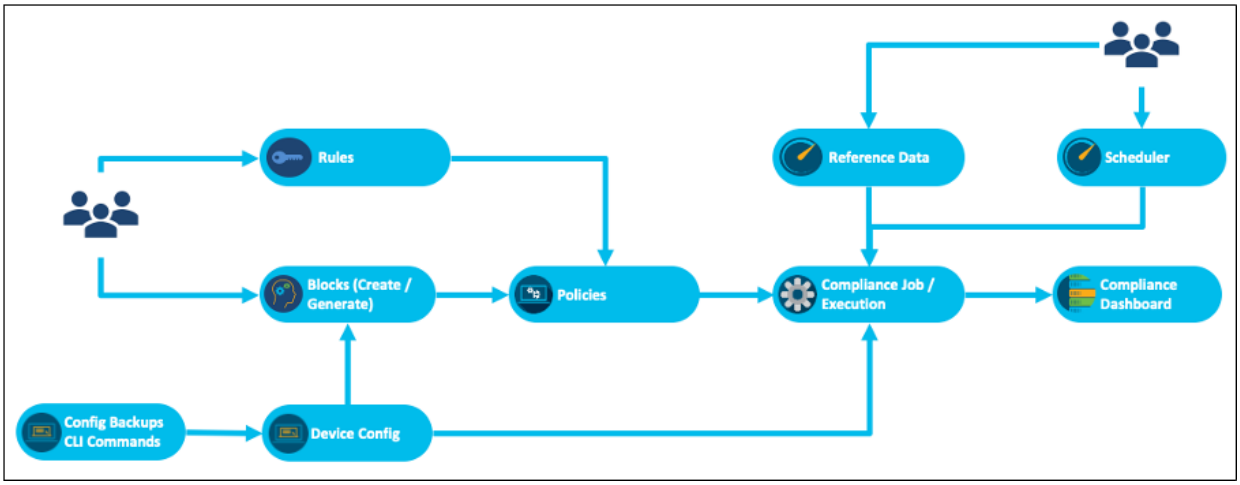
- A chave de direito de assinatura para o caso de uso CnR deve ser carregada.
- O controlador e os dispositivos relevantes devem ser integrados e estar disponíveis como parte do BPA Asset Manager. Consulte a seção Gerenciador de ativos no Guia do usuário do BPA para obter detalhes.
- Os ativos integrados precisam ser agrupados de acordo com os requisitos do cliente em grupos de ativos no portal de próxima geração.

Painel de Conformidade

O painel de controle de conformidade fornece uma exibição resumida das violações em todos os dispositivos durante o tempo selecionado. Os dados do mês atual são exibidos por padrão. Os usuários podem alterar a janela de tempo para exibir dados históricos sobre violações de conformidade. O mês atual é o modo de exibição padrão selecionado.

Note: O painel de conformidade preterido na interface de usuário clássica foi removido e não está mais disponível. O painel disponível no portal de próxima geração deve ser usado.

Diagrama de Fluxo de Conformidade de Configuração



Visão Geral do Componente de Conformidade de Configuração

As violações de conformidade exibidas no painel de controle são preenchidas quando um Job de Conformidade é executado para uma política em relação a uma lista de ativos. A política de conformidade é criada adicionando-se uma lista de configurações de bloco juntamente com as regras de conformidade necessárias. A regra de conformidade pode ter verificações com valores estáticos ou variáveis dinâmicas para as quais os dados são buscados do aplicativo RefD. Um Job de Conformidade pode ser executado sob demanda ou como uma programação única ou recorrente.

A conformidade da configuração inclui os seguintes recursos importantes:

- Criação de blocos: Os blocos são criados manualmente ou gerados automaticamente usando o modelo Analisador de texto de modelo (TTP). Eles podem ser estáticos ou dinâmicos (com variáveis).
- Criação de regras: As regras validam as variáveis nos blocos. Os valores de regra podem ser definidos estaticamente ou recuperados dinamicamente do sistema de dados de referência (RefD) durante o tempo de execução.
- Criação de política: As políticas são criadas selecionando-se a lista de blocos e as regras correspondentes. Os dados das regras podem ser estáticos ou extraídos da estrutura RefD dinamicamente no tempo de execução.
- Criação de trabalho de conformidade: Os jobs de conformidade são criados selecionando uma política e um grupo de ativos (contendo uma lista de ativos) para executar a verificação de conformidade. Os usuários podem optar por recuperar a configuração do dispositivo a partir da estrutura de backup ou executar comandos em tempo real por meio de modelos de processo nos dispositivos durante a execução. Buscar a configuração do backup ajuda na auditoria offline de dispositivos sem a necessidade de se conectar a um dispositivo ativo. Os trabalhos podem ser agendados ou executados sob demanda.
- Violações de conformidade: Exibir violações de conformidade no painel.

Resumo de conformidade de ativos

A guia Resumo da conformidade de ativos é um recurso essencial projetado para fornecer uma visão geral abrangente das violações de conformidade em todos os dispositivos em uma rede. Essa guia permite que os usuários identifiquem rapidamente problemas de conformidade, garantindo que todos os dispositivos sigam as políticas e os padrões estabelecidos. A interface é equipada com recursos avançados de filtragem e pesquisa, facilitando a navegação e a análise de dados de conformidade.

Recursos Principais

- Resumo de violações por dispositivo: A guia exibe uma exibição resumida das violações de conformidade para cada dispositivo, fornecendo aos usuários um rápido instantâneo do status de conformidade geral categorizado por níveis de gravidade, como crítico, alto, médio e baixo.

- Informações detalhadas sobre violação: Para cada dispositivo, a janela pop-up fornece informações detalhadas sobre as políticas violadas e o usuário pode detalhar ainda mais o bloco e a linha de configuração que causou a violação.

Exibir Resumo de Conformidade de Ativo

- Opções avançadas de filtragem: Os filtros localizados na parte superior e esquerda da guia permitem que os usuários restrinjam os dados exibidos na grade. Os usuários podem filtrar por intervalo de datas, Grupo de ativos, Família de produtos e muito mais, permitindo uma análise focada de dados de conformidade.
- Funcionalidade de pesquisa: Um campo de pesquisa está disponível para refinar ainda mais os dados na grade. Os usuários podem localizar rapidamente dispositivos específicos ou gerenciar por controlador inserindo palavras-chave ou frases relevantes.
- Intervalo de datas personalizável: Por padrão, o mês atual é selecionado no filtro de intervalo de datas, fornecendo os dados de conformidade mais recentes. No entanto, os usuários podem personalizar o intervalo de datas para exibir dados.
- Filtros: Vários filtros, como Família de produtos, Grupo de ativos e Tipo de auditoria, estão disponíveis. Aplique o filtro para atualizar a grade.

Resumo de conformidade de ativos

- Exportar como CSV: Um recurso disponível para ajudar os usuários a obter uma cópia local da conformidade de configuração de ativos para análise, emissão de relatórios e arquivamento off-line. Para exportar dados como um arquivo CSV, selecione Exportar como CSV no ícone Mais Opções. O arquivo CSV baixado contém os dados exibidos atualmente na grade, respeitando todos os filtros aplicados.

Resumo de conformidade de ativos: Exportar como CSV

Detalhes do arquivo CSV para conformidade de ativos

O arquivo CSV inclui todas as colunas visíveis na grade Resumo da conformidade de ativos, como nome do dispositivo, instância do controlador (gerenciada por), família de produtos do dispositivo, status de conformidade do dispositivo, contagem de violações por gravidade (por exemplo, Crítica, Principal, Secundária, Aviso, Informações, Desconhecida) e a data em que a conformidade foi verificada pela última vez para o dispositivo.

Se a grade tiver paginação, a exportação incluirá todos os registros nas páginas, não apenas a página visível.

Como abrir e usar o arquivo CSV para conformidade de ativos

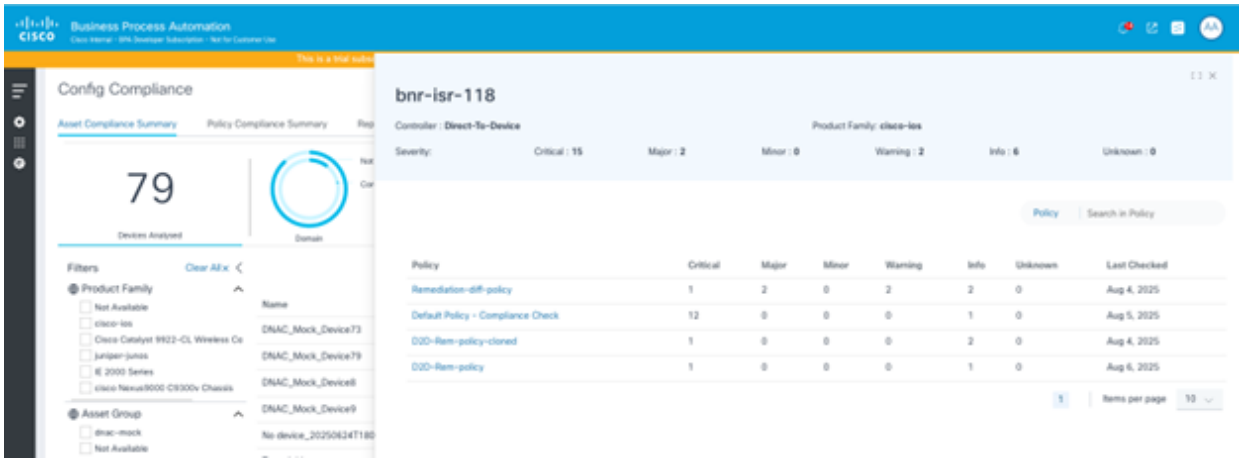
1. Abra o arquivo CSV baixado no Excel ou em qualquer aplicativo de planilha compatível.
2. Verifique se o conteúdo corresponde ao que é mostrado na grade Resumo de conformidade de ativos, incluindo resultados filtrados.

	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											

Resumo de conformidade de ativos: Arquivo CSV aberto no aplicativo Excel

Exibindo o Resumo de Conformidade do Ativo por Política

Clicar em uma linha da grade Resumo da conformidade de ativos exibe os detalhes das violações de ativos, categorizadas pelas diferentes políticas nas quais o dispositivo é validado. Isso serve como uma exibição detalhada para que os usuários visualizem a contagem de violações por gravidade em cada política.



Resumo de conformidade de ativos: Resumo de Conformidade por Política

---

Note: É de notar o seguinte.
- O hiperlink na coluna Política direciona os usuários para a página de detalhes da Política
- Clicar em uma linha exibe a página Detalhes da violação para a política selecionada

---

Exibindo Detalhes da Violação

A página Detalhes da Violação exibe violações em nível de bloco e de regra sobrepostas na configuração do dispositivo. Além disso, os usuários também podem visualizar a configuração de bloqueio e as configurações de correção sugeridas.

Para exibir a página Detalhes da Violação da página Resumo da Conformidade de Ativos juntamente com a divisão do nível da política:

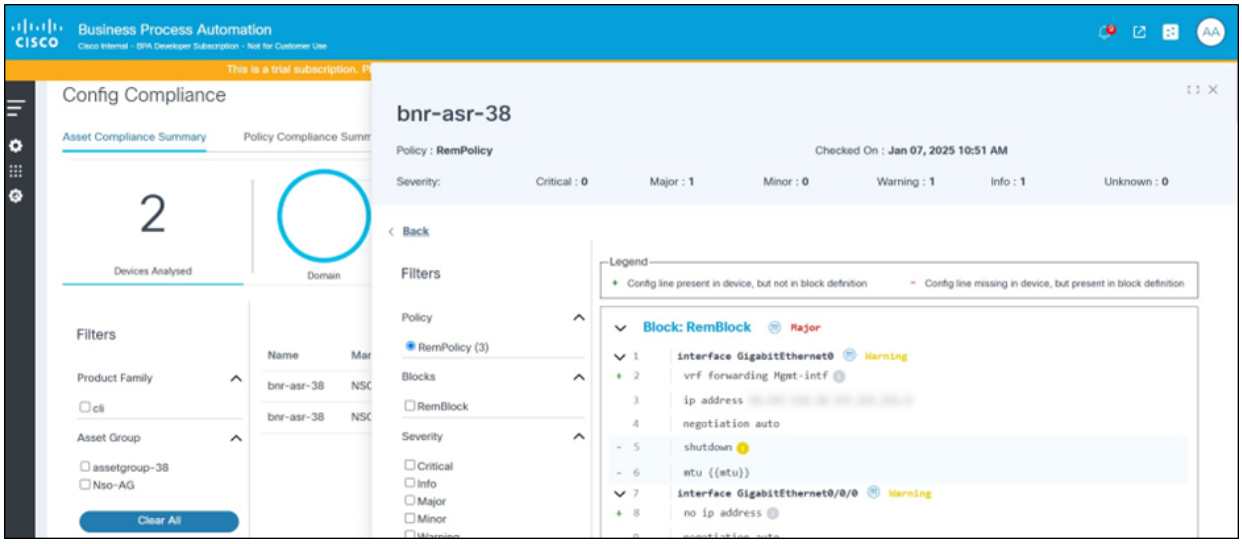
1. Selecione uma linha na grade Conformidade de ativos. Uma janela pop-up será exibida. A

grade exibe uma divisão dos detalhes de conformidade por política.
2. Selecione uma linha na grade. A página Detalhes da violação é exibida.

Para exibir a página Detalhes das Violações na grade Resumo de Conformidade da Política:

1. Selecione a Grade de Conformidade com Política.
2. Selecione uma linha > Grade de ativos afetados.
3. Selecione uma linha. A página Detalhes das Violações é exibida.

O lado direito da página Detalhes das Violações mostra os blocos de configuração do dispositivo e sobrepõe as violações no topo dela. As violações são listadas nas linhas de configuração correspondentes. No caso de uma falha de condição, a faixa de opções violação fornece detalhes do nome da regra, da condição e da configuração esperada (conforme definido na regra) versus a configuração recuperada da configuração do dispositivo.



Violações de conformidade de ativos

Símbolos de Bloco

- Um sinal "+" em uma linha implica que a configuração não é esperada de acordo com a configuração de bloco, mas também está presente na configuração do dispositivo.
- Um sinal "-" em uma linha indica que a configuração é esperada de acordo com a configuração do bloco, mas está ausente na configuração do dispositivo.

Filtros

A seção de filtro no lado esquerdo da página permite que os usuários executem as seguintes ações:

- Alterar a política; isso atualiza a página e carrega as violações para a política selecionada recentemente
- Marque as caixas de seleção Blocos para exibir violações relevantes aos blocos selecionados
- Marque as caixas de seleção Severidade para exibir violações com o(s) nível(is) de severidade fornecido(s)
- Marque as caixas de seleção Tipo de violação para exibir violações do tipo selecionado:
    - Incompatibilidade de ordem: A ordem das linhas de configuração do dispositivo não corresponde à ordem definida na configuração de bloco
    - Configuração Ausente: Exibir linhas de configuração esperadas de acordo com a configuração de bloco, mas ausentes na configuração do dispositivo
    - Configuração adicional: Exibir linhas de configuração que não são esperadas de acordo com a configuração de bloco, mas também presentes na configuração do dispositivo
    - Falhas de regra: Falhas de uma ou mais condições em regras.
    - Blocos ausentes: O bloco de configuração de dispositivo inteiro está ausente ou não corresponde à configuração de bloco definida.
    - Blocos ignorados: Este bloco de configuração foi ignorado porque as condições do filtro de bloco não foram atendidas.

Exibindo e Comparando a Configuração de Correção

A página Configuração da correção exibe a configuração gerada para o dispositivo selecionado para cada um dos blocos em uma determinada política. A configuração é gerada e considera os detalhes do bloco e da regra presentes na política, bem como a configuração do dispositivo recuperada durante a execução da conformidade. Os usuários podem atualizar a configuração na mesma página. Essa configuração gerada pode ser enviada por push para o dispositivo usando o recurso de trabalhos de correção. Além disso, esta página fornece uma opção para que os usuários comparem a configuração gerada com a configuração atual do dispositivo em execução. O usuário pode especificar um ou mais comandos para recuperar a configuração atual do dispositivo.

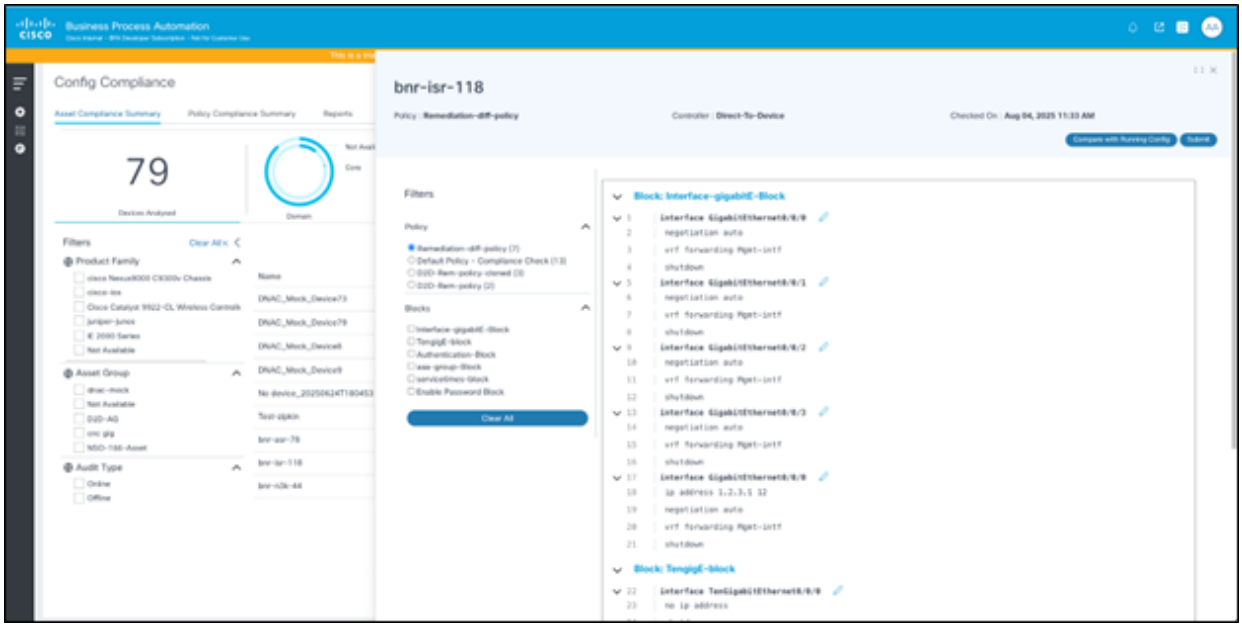
Para exibir a página Configuração de remediação na grade Conformidade de ativos:

1. Clique na guia Resumo da conformidade de ativos.
2. Na grade de conformidade de ativos na coluna Ação , selecione o ícone Mais Opções > Exibir Configuração de Correção. A página Configuração da correção é exibida.

Para exibir a página Configuração da correção da grade de Conformidade com a política:

1. Clique na guia Policy Compliance Summary.
2. Na grade de conformidade com a política, selecione a linha desejada. A grade Ativos afetados é exibida.

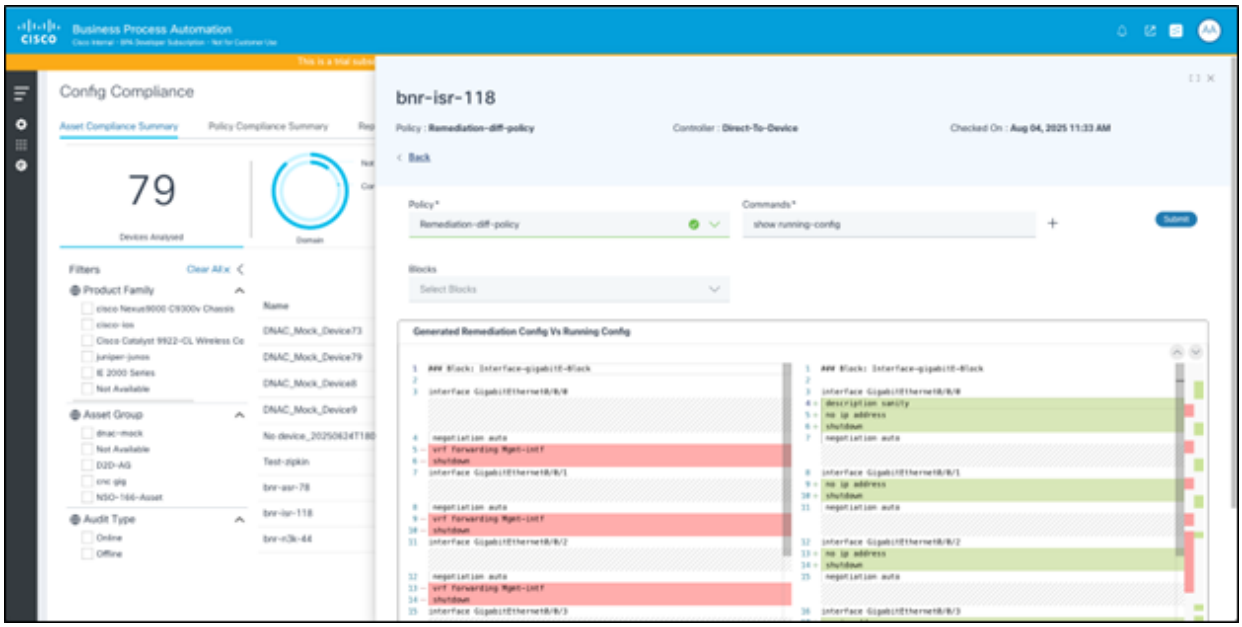
3. Na coluna Ação, selecione o ícone Mais opções > Selecionar Exibir configuração de reparo. A página Configuração da correção é exibida.



Página Config. de Correção

A página Configuração da correção exibe o seguinte:

- Configuração de correção gerada: A configuração gerada é exibida no lado direito da página, junto com a opção para que os usuários editem os blocos de configuração e enviem as alterações a serem salvas
- Filtros: Os filtros podem ser usados para selecionar uma política e, opcionalmente, selecionar um ou mais blocos para ver a configuração gerada correspondente
- Compare com Running Config: Clique em Compare with Running Config para exibir uma página detalhada que permite aos usuários comparar a configuração gerada com a configuração de execução do dispositivo



Página Comparar com Configuração em Execução

A página Comparar com configuração em execução exibe o seguinte:

- Opção para selecionar uma política: A política selecionada na página anterior é pré-selecionada.
- Uma caixa de texto para inserir um ou mais comandos a serem executados no dispositivo
- Um botão Submit para executar o(s) comando(s) no dispositivo e recuperar a configuração
- Opção para exibir e filtrar blocos: Por padrão, todos os blocos na política são mostrados; os usuários podem selecionar blocos individuais conforme necessário
- Um Visualizador de comparação de configuração exibindo a configuração gerada e a configuração do dispositivo lado a lado, com realces para as diferenças

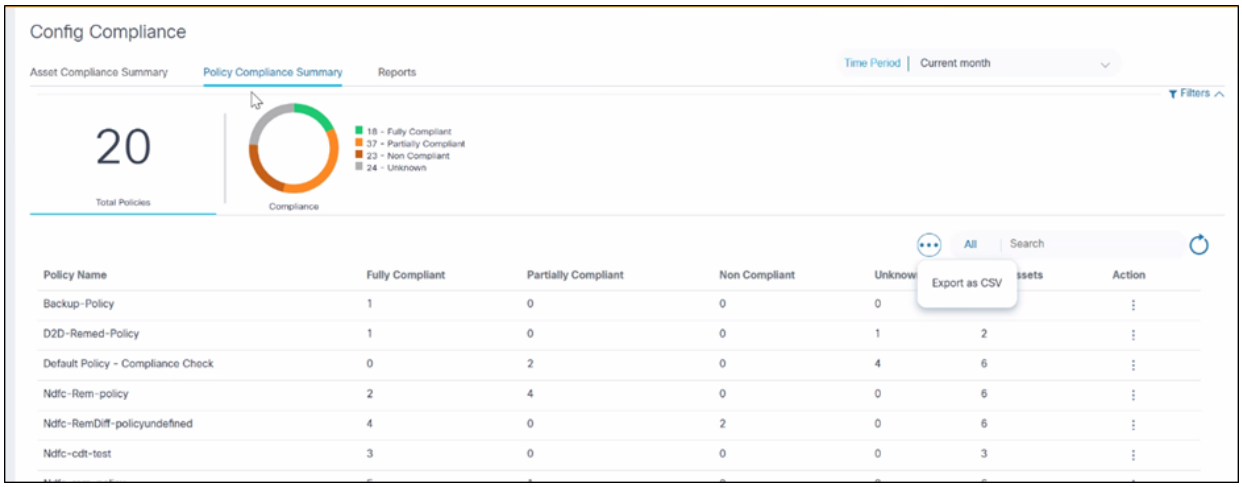
Resumo de Conformidade de Política

A guia Policy Compliance Summary foi criada para fornecer uma visão geral clara e concisa do status de conformidade dos dispositivos em relação às políticas definidas. Essa guia ajuda os usuários a avaliar rapidamente o cenário de conformidade e a identificar áreas de preocupação. A guia categoriza os dispositivos com base em seu status de conformidade, facilitando a rápida compreensão e o gerenciamento da conformidade.

Status de conformidade:

- Totalmente compatível: Todos os dispositivos atendem a todas as regras de conformidade para a respectiva política.
- Parcialmente compatível: Alguns dispositivos cumprem as regras, mas outros não.
- Não compatível: Nenhum dispositivo está em conformidade com a política.
- Desconhecido: A conformidade da política não pode ser verificada devido a problemas com

a conexão de rede ou à indisponibilidade de backups.



Resumo de Conformidade de Política com exportação de CSV

Exportar como CSV para Conformidade com Políticas

O recurso Exportar como CSV ajuda os usuários a obter uma cópia local da conformidade com políticas para análise off-line, emissão de relatórios e arquivamento. Para exportar dados como um arquivo CSV, selecione Exportar como CSV no ícone Mais Opções. O arquivo CSV baixado contém os dados exibidos atualmente na grade, respeitando todos os filtros aplicados.

Detalhes do arquivo CSV para conformidade com políticas

O arquivo CSV inclui o nome da política, a contagem total de ativos validados e a divisão da contagem pelo status de conformidade (ou seja, totalmente compatível, parcialmente compatível, não compatível e desconhecido). Se a grade tiver paginação, a exportação incluirá todos os registros em todas as páginas, não apenas aqueles exibidos na página atual.

Como abrir e usar o arquivo CSV para conformidade com políticas

1. Abra o arquivo CSV baixado no Excel ou em qualquer aplicativo de planilha compatível.
2. Verifique se o conteúdo corresponde ao que é mostrado na grade Resumo de conformidade de política, incluindo resultados filtrados.

	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						

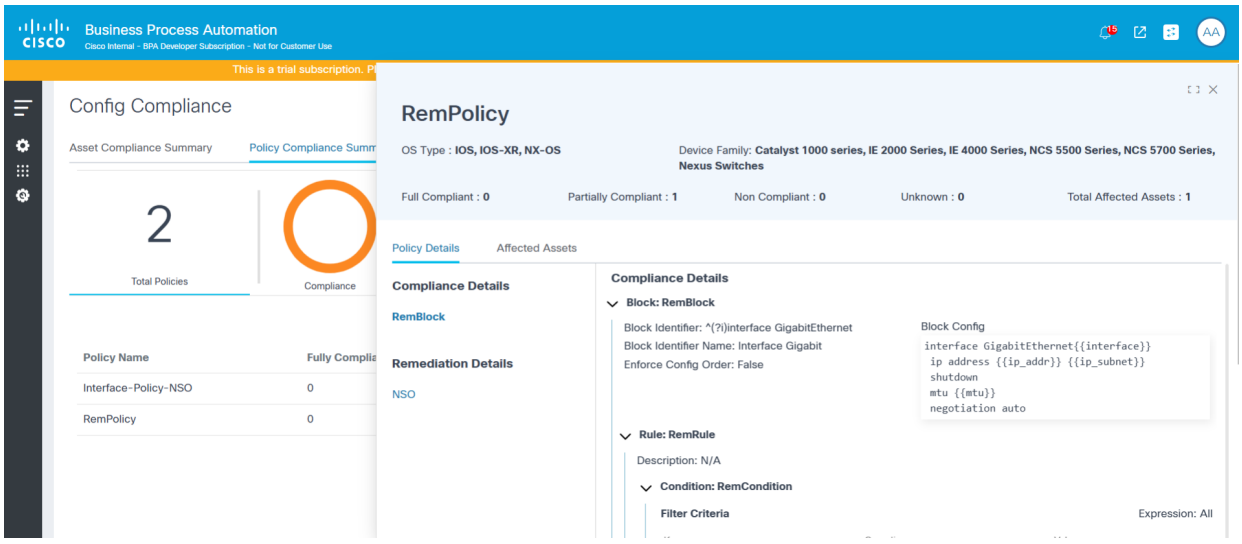
Conformidade com políticas: Detalhes da política

Exibindo Detalhes da Política

Para exibir detalhes da política:

1. Selecione uma política no ícone Mais Opções na coluna Ação.
2. Selecione Exibir detalhes da política. A página Detalhes da política é exibida.

Note: A página Detalhes da Política é uma view somente para leitura de todas as informações da política, incluindo blocos, regras e condições. Os usuários podem clicar em hiperlinks na página que navega diretamente para o bloco relevante.



Conformidade com políticas: Detalhes da política

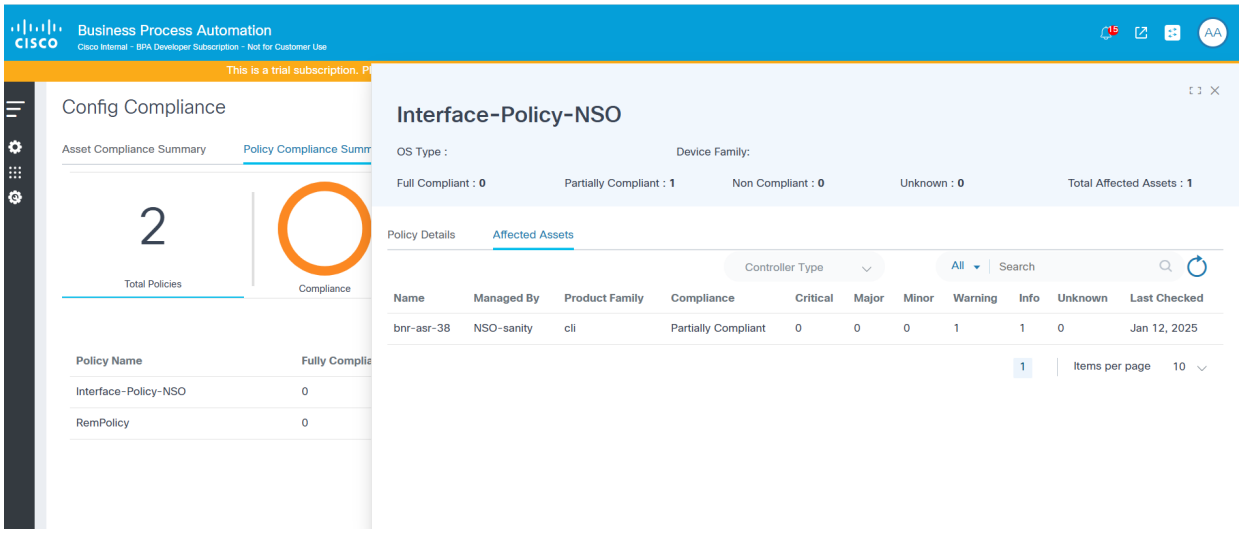
Exibindo ativos afetados

A guia Ativos afetados exibe a lista de ativos analisados em cada política e a contagem de

violação dividida por gravidade. Os dispositivos podem ser filtrados usando a lista suspensa Tipo de controlador e a caixa de pesquisa.

Para exibir Ativos afetados na guia Resumo de conformidade de política:

1. Selecione uma linha. A janela Política de conformidade é aberta.
2. Clique na guia Ativos afetados.



Conformidade com políticas: Ativos afetados

Note: A guia Ativos afetados fornece ações para abrir a página Exibir detalhes da violação e a página Exibir configuração da correção. Consulte o Resumo de conformidade de ativos para obter mais informações.

Relatórios

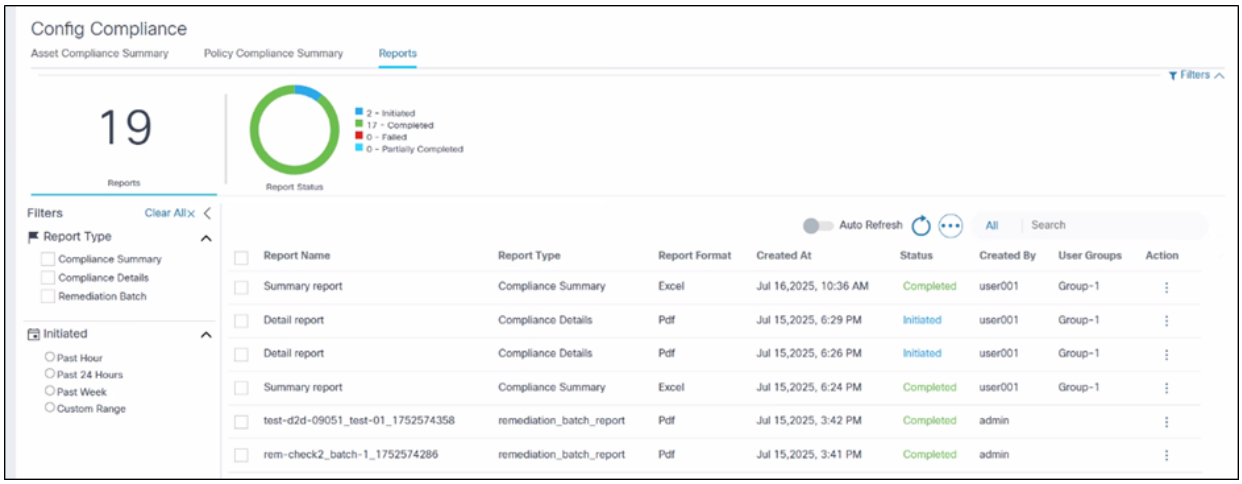
A seção de relatórios foi projetada para fornecer informações abrangentes sobre a conformidade do dispositivo, identificar violações e facilitar os esforços de correção. O aplicativo oferece uma interface fácil de usar para geração, exibição, download e gerenciamento de vários tipos de relatórios de conformidade.

Painel de Relatórios

O painel de controle de relatórios serve como o hub central para todas as atividades de relatório de conformidade. Os usuários podem gerenciar seus relatórios com eficiência a partir dessa única interface. As principais funcionalidades disponíveis no painel de relatórios incluem:

- Exibindo relatórios: Os usuários podem exibir uma lista de todos os relatórios gerados, incluindo nome, tipo, política associada, formato, data de criação e status atual (por exemplo, Iniciado, Concluído, Falha, Parcialmente Concluído)
- Download de relatórios: Os relatórios, uma vez gerados, podem ser baixados para análise off-line ou para fins de arquivamento; a coluna Ação fornece opções para download
- Excluindo relatórios: Os usuários têm a capacidade de remover relatórios antigos ou desnecessários do painel, ajudando a manter um ambiente de relatórios limpo e organizado
- Filtragem e pesquisa: O painel oferece amplas opções de filtragem, permitindo que os usuários localizem rapidamente relatórios específicos com base em critérios como Tipo de relatório (por exemplo, Detalhes de conformidade, Resumo de conformidade, Lote de remediação), Política e Status de início (por exemplo, Hora passada, Últimas 24 horas, Semana passada, Intervalo personalizado); uma barra de pesquisa também está disponível
- Monitoramento do status do relatório: Um resumo visual (ou seja, um gráfico de pizza) indica o status dos relatórios, exibindo quantos são iniciados, concluídos, reprovados ou parcialmente concluídos.

O painel Relatórios é a página inicial sob a guia Relatórios no painel Conformidade e correção.



Painel de Relatórios

- Os tipos de relatório disponíveis incluem:
  - Relatório de resumo de conformidade
  - Relatório detalhado de conformidade
  - Relatório de Lote de Remediação
- Use filtros para selecionar o seguinte:
  - Tipo de relatório
  - Política
  - Período de tempo iniciado (a lista de relatórios é filtrada com base no período selecionado)
- Opção de atualizar automaticamente a lista de relatórios

Configurações de relatório

As Configurações de Relatórios permitem que um administrador configure os principais parâmetros relacionados aos relatórios, com base nos requisitos de implantação e de negócios. Os seguintes parâmetros estão disponíveis para configuração:

- Excluir automaticamente relatórios com mais de (dias): Qualquer relatório mais antigo do que essa duração será excluído do sistema
- Máximo de blocos a serem selecionados por política em um Relatório de resumo de conformidade: Ajuda a manter o número de guias no arquivo do Excel em um limite legível
- Máximo de Ativos a serem selecionados em um Relatório Detalhado de Conformidade: Ajuda a limitar o número de arquivos PDF gerados para um determinado relatório detalhado

Lista de tarefas de conformidade

Geração de relatórios

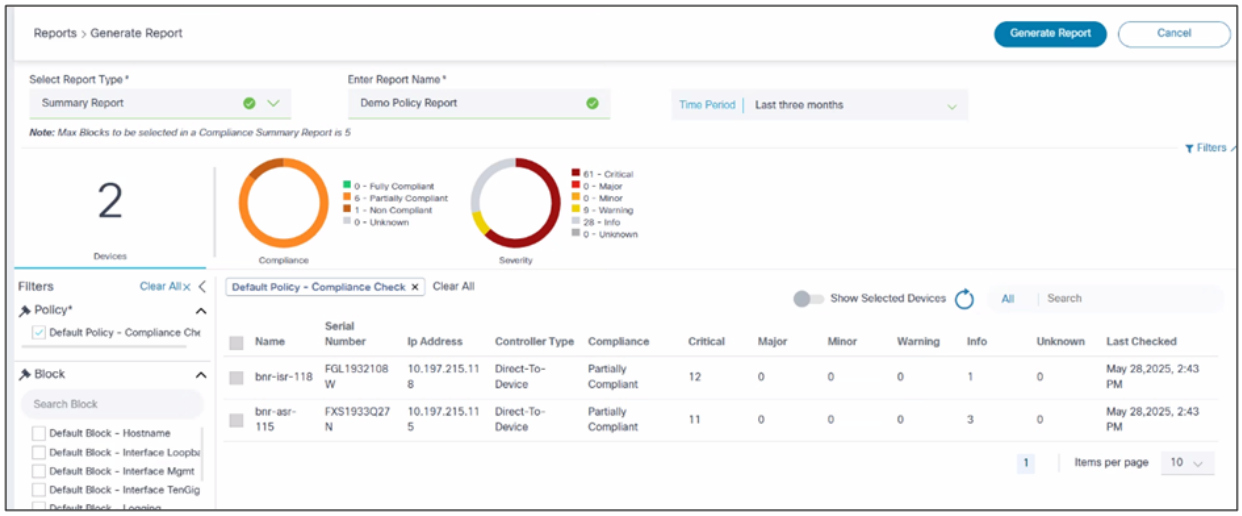
O aplicativo oferece uma interface dedicada para gerar novos relatórios de conformidade, permitindo que os usuários selecionem o tipo de relatório, definam o escopo e apliquem filtros específicos. O processo de geração de relatório é iniciado na ação "Gerar relatório" na página Painel de controle Relatório.

Os principais aspectos da geração de relatórios incluem:

- Selecionando o tipo de relatório: Os usuários podem escolher entre os diferentes tipos de relatório a seguir
    - Relatório resumido: Fornece uma visão geral da conformidade em todos os dispositivos para as políticas selecionadas
    - Relatório detalhado: Oferece uma visualização detalhada mais granular, fornecendo informações detalhadas sobre violações específicas para cada dispositivo
- Nomeando o relatório: Os usuários devem fornecer um nome relevante para o relatório gerado
- Seleção de Período de Tempo: Os relatórios podem ser gerados para períodos específicos, como "mês atual" ou intervalos personalizados, para se concentrarem em dados recentes de conformidade
- Applying Filters: As opções de filtragem abrangentes permitem que os usuários reduzam o escopo do relatório
    - Política: Selecione uma ou mais políticas de conformidade a serem incluídas no relatório. A seleção da política é obrigatória
    - Bloqueio: Nas políticas selecionadas, escolha blocos de configuração específicos a serem incluídos no relatório. A seleção de blocos é opcional
    - Grupo de ativos: Os usuários podem filtrar os ativos no escopo selecionando um ou mais grupos de ativos
- Seleção de ativos: Aplicável apenas a relatórios detalhados
    - Os usuários podem selecionar dispositivos específicos para os quais o relatório deve

ser gerado
- A tabela de ativos exibe detalhes como Nome, Número de série, Endereço IP, Gerenciado por e status de conformidade atual com contagens para diferentes níveis de gravidade

Para gerar um Relatório de Resumo de Conformidade:

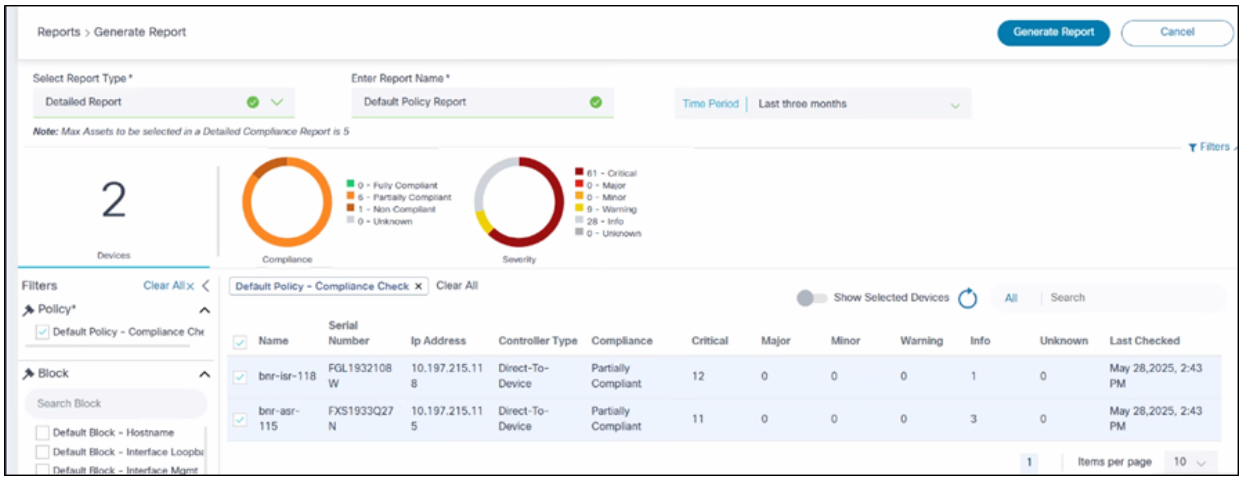


Gerar relatório de resumo

1. Selecione Relatório de resumo na lista suspensa Selecionar tipo de relatório.
2. Insira um nome de relatório.
3. Selecione um intervalo de tempo. As políticas e os blocos serão listados com base nessa seleção.
4. Selecione uma política. Políticas adicionais também podem ser selecionadas.
5. Opcionalmente, selecione Blocos. Se nenhum for selecionado, todos os blocos serão incluídos.
6. Selecione os grupos de ativos, o status de conformidade e os níveis de gravidade necessários.
7. Clique em Gerar relatório.

- Na página Lista de relatórios, o status do relatório é definido como Iniciado
- Após a conclusão, o status muda para Concluído. Se alguns dos sub-relatórios falharem, o status mudará para Parcialmente concluído
- Se toda a geração do relatório falhar, uma notificação será exibida e o status mudará para Falha
- Depois de concluída, a opção de download estará disponível. Os usuários podem fazer download de um arquivo zip que contém os relatórios do Excel

Para gerar um Relatório Detalhado de Conformidade:



Gerar relatório detalhado

1. Selecione Relatório detalhado na lista suspensa Selecionar tipo de relatório.
2. Insira um nome de relatório.
3. Selecione um intervalo de tempo. As políticas e os blocos serão listados com base nessa seleção.
4. Selecione uma política. Políticas adicionais também podem ser selecionadas.
5. Opcionalmente, selecione Blocos. Se nenhum for selecionado, todos os blocos serão incluídos.
6. Selecione os grupos de ativos, o status de conformidade e os níveis de gravidade necessários.
7. Selecione os ativos necessários na grade. Os usuários têm a opção de "Selecionar todos" os dispositivos e "Mostrar dispositivos selecionados".
8. Clique em Gerar relatório.

- Na página Lista de relatórios, o status do relatório é definido como Iniciado
- Após a conclusão, o status muda para Concluído. Se alguns dos sub-relatórios falharem, o status mudará para Parcialmente concluído
- Se toda a geração do relatório falhar, uma notificação será exibida e o status mudará para Falha

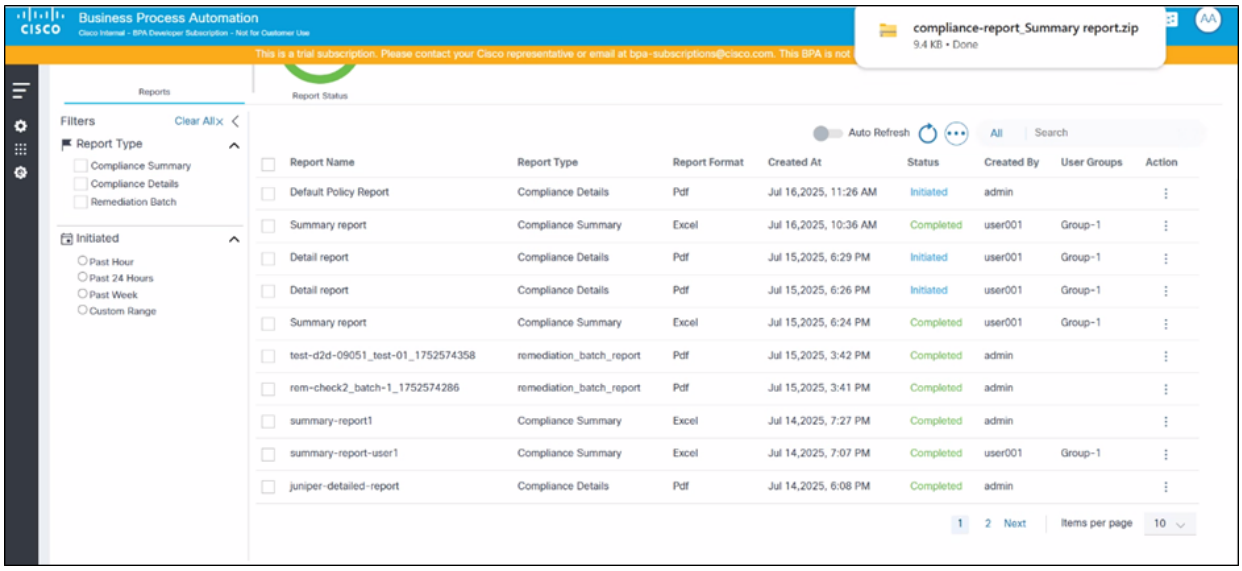
Download e exibição de relatórios

Os relatórios concluídos podem ser baixados usando o ícone Download na linha desejada da grade do Painel de Relatórios.

Entendendo o Relatório de resumo de conformidade de configuração

O relatório Resumo de conformidade é um arquivo zip que contém relatórios PDF individuais, com um PDF gerado por dispositivo. Esse tipo de relatório oferece uma visão geral da violação de conformidade por política, juntamente com detalhes de violação de mapeamento de detalhamento

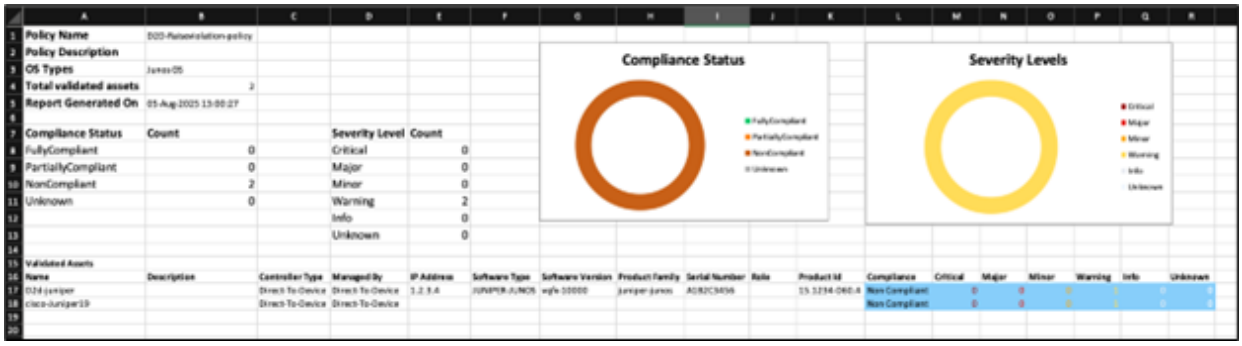
em nível de bloco em relação aos dispositivos.



Relatório de resumo de conformidade

Cada relatório do Excel inclui as seguintes planilhas e fornece as seguintes informações:

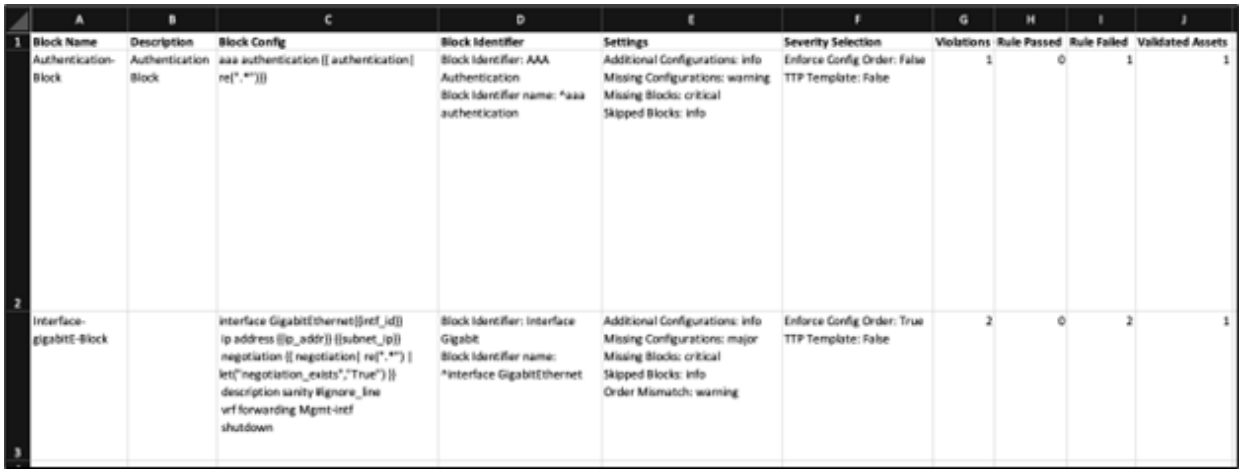
- Resumo da política:
  - Detalhes da visão geral, como nome da política, descrição, tipo(s) de SO e total de ativos validados
  - Uma exibição de grade e gráfico da contagem de ativos validados dividida por status de conformidade (por exemplo, Totalmente compatível, Parcialmente compatível, Não compatível e Desconhecido)
  - Uma exibição de grade e gráfico da contagem total de violações dividida por nível de gravidade (por exemplo, Crítica, Principal, Secundária, Informações de Advertência e Desconhecida)
  - Uma grade de ativos com detalhes do dispositivo, status de conformidade e contagem de violações para cada nível de gravidade



Planilha de resumo da política

- Resumo do bloco:
  - Detalhes de bloqueio, como nome do bloco, descrição, configuração do bloco,

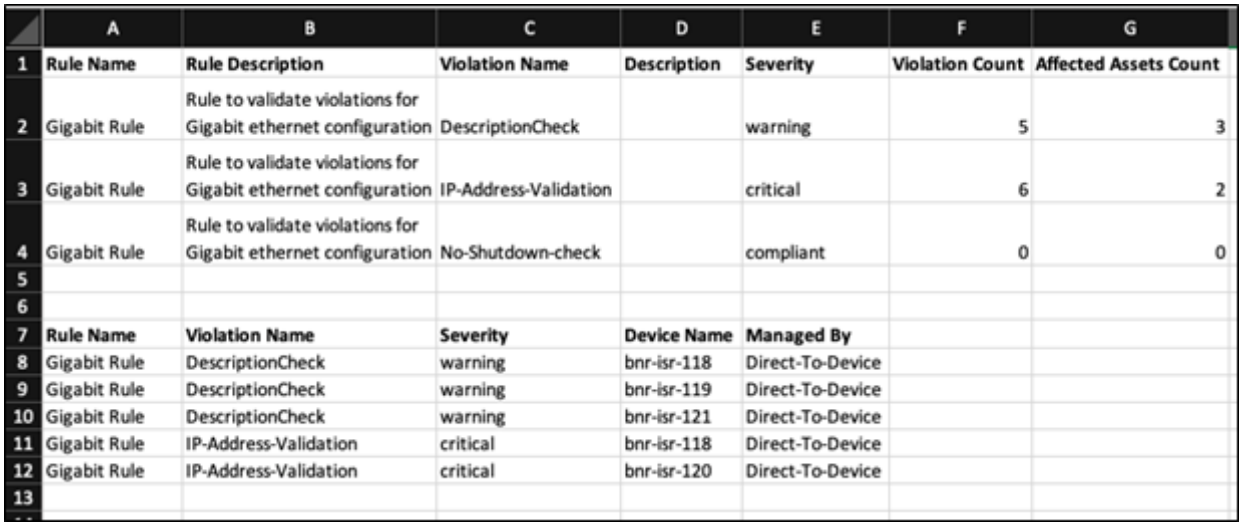
detalhes do identificador de bloco e configurações de severidade de violação de bloco
    - Contagem de violações, regras aprovadas, regras com falha e ativos validados para o bloco especificado



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

Planilha de resumo do bloco

- Detalhes da regra e da violação por bloco:
- A grade de nível de violação exibe uma lista de nomes de regra, descrição, nome da violação, nível de severidade da descrição, contagem de violações vistas nos ativos e contagem dos ativos afetados
- A grade de nível de dispositivo exibe o mapeamento entre regra, violação, gravidade, nome do dispositivo e nome do controlador (gerenciado por)



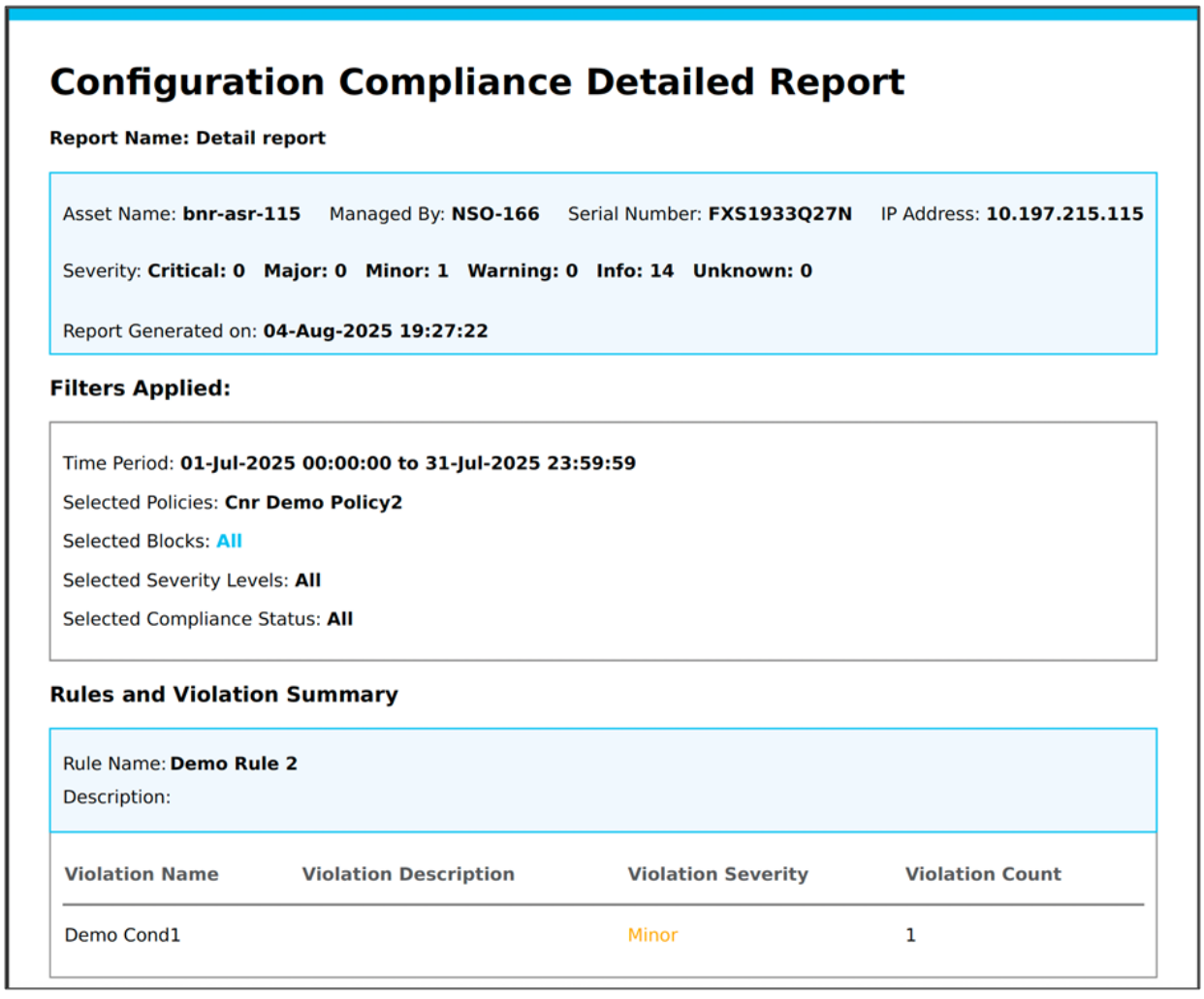
	A	B	C	D	E	F	G
1	Rule Name	Rule Description	Violation Name	Description	Severity	Violation Count	Affected Assets Count
2	Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	DescriptionCheck		warning	5	3
3	Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	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							

Relatório de Detalhes de Conformidade

O relatório de detalhes de Conformidade contém as seguintes informações:

- Nome do relatório: Identifica o nome do relatório
    - Nome do ativo: Especifica o dispositivo para o qual a verificação de conformidade foi executada

    - Outros detalhes do ativo: Inclui detalhes como o endereço IP e o número de série, se houver
    - Severity: Fornece uma contagem resumida de violações por nível de gravidade
    - Relatório gerado em: Indica a marca de data e hora de quando o relatório foi criado
- Filtros aplicados: Descreve os detalhes dos critérios de filtragem específicos usados para gerar um relatório específico, garantindo transparência e reprodutibilidade. Isso inclui o período, as políticas selecionadas, os blocos, os níveis de gravidade e os status de conformidade
- Resumo de regras e violações: Lista cada regra que foi avaliada e fornece um resumo das violações encontradas para essa regra. A grade de resumo mostra o Nome da violação, Descrição, Severidade e o número de vezes que essa violação ocorreu
- Detalhes da violação: Oferece detalhes explícitos sobre cada linha de configuração de dispositivo para os blocos selecionados, juntamente com os detalhes de violação para cada linha



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**

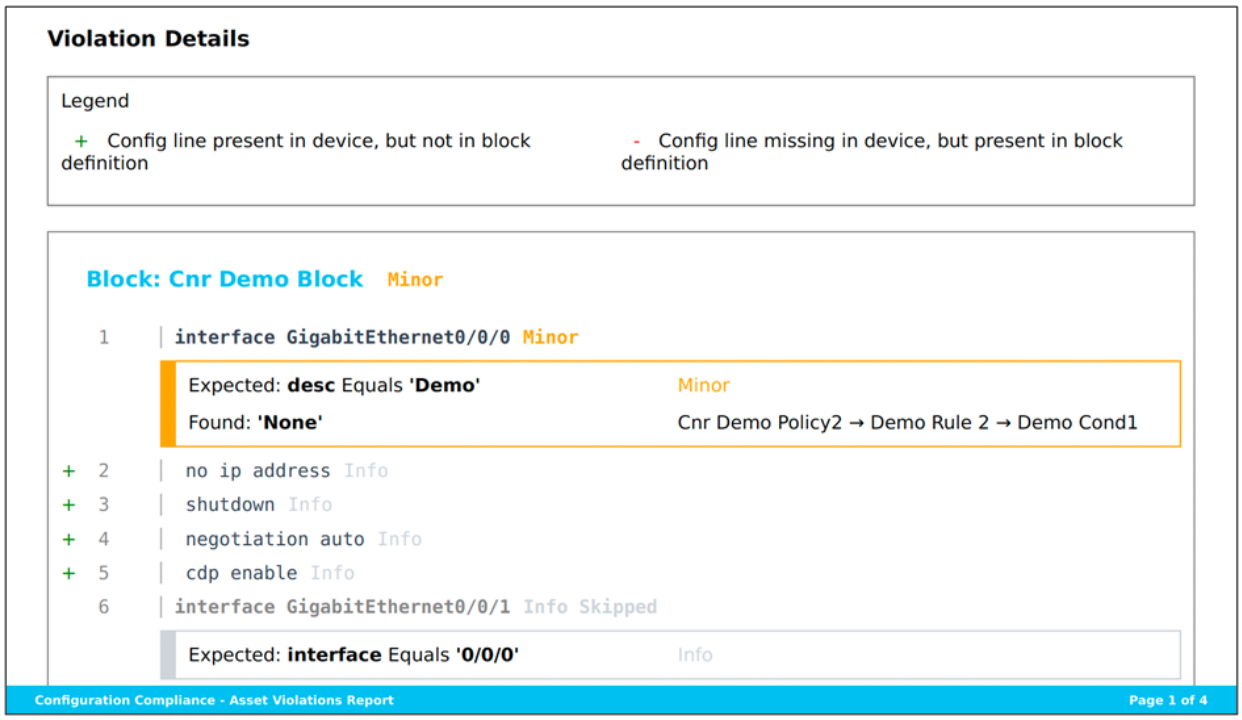
Rules and Violation Summary

Rule Name: **Demo Rule 2**

Description:

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

Relatório Detalhado de Conformidade - Exemplo em PDF Página 1

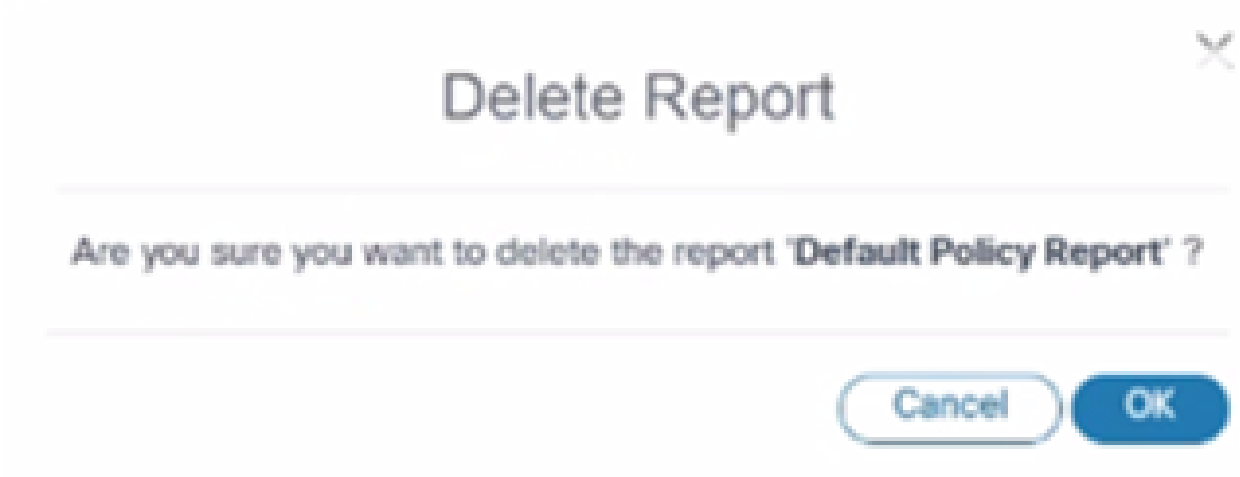


Relatório detalhado de conformidade - exemplo de PDF Página 2

Note: O relatório em PDF do lote de correções criado na página Lote de correções também pode ser baixado e exibido na lista de relatórios.

Excluir relatórios

Os relatórios podem ser excluídos individualmente selecionando o ícone Excluir ou em massa marcando as caixas de seleção dos relatórios e selecionando o ícone Mais Opções > Excluir.



Lista de tarefas de conformidade

Note: A exclusão de um relatório apenas remove os arquivos de relatório e a entrada do

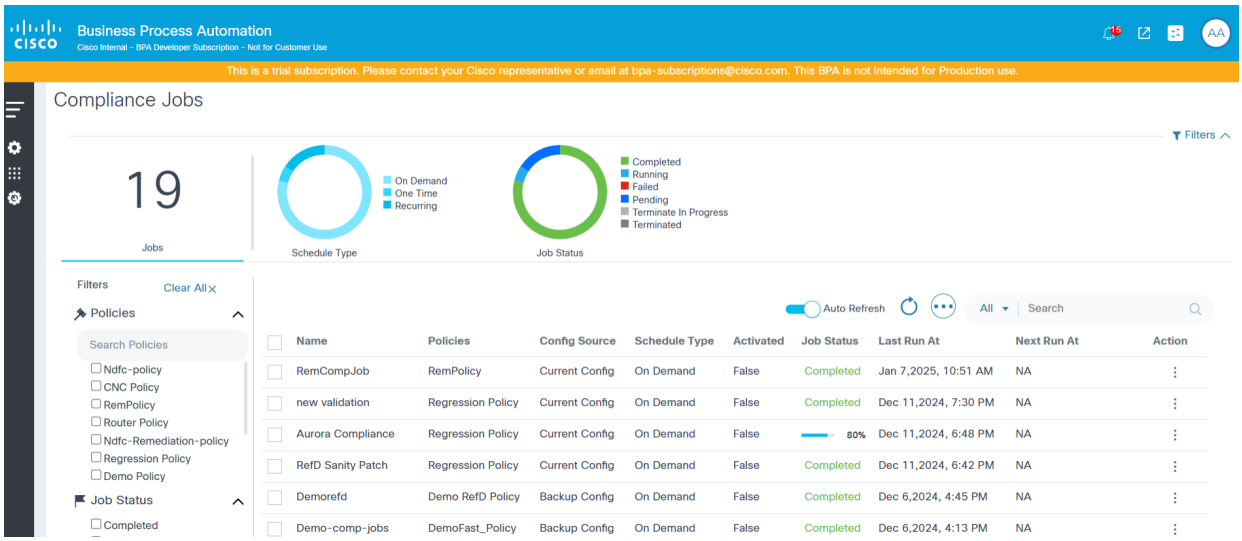
painel de relatórios; os detalhes de execução de conformidade subjacentes são mantidos.

Trabalhos de conformidade

O recurso Jobs de Conformidade no portal de Próxima Geração foi projetado para ajudar os usuários a criar, gerenciar e executar Jobs de Conformidade em políticas e grupos de ativos selecionados. Esses trabalhos podem ser programados para serem executados em intervalos regulares ou sob demanda, garantindo que todos os ativos sejam verificados consistentemente quanto à conformidade.

Recursos Principais

- Listar trabalhos de conformidade: Exibir todos os Jobs de Conformidade definidos, com opções para fazer auditoria off-line, filtrar, criar, editar, excluir e executar jobs.
- Trabalhos Agendados e Sob Demanda: Configurar jobs para execução em intervalos programados ou executá-los imediatamente, conforme necessário.
- Controle de acesso fino: O acesso aos Jobs de Conformidade é controlado com base nas permissões do usuário, garantindo que os usuários vejam apenas os jobs relacionados às políticas para as quais têm acesso.
- Opções de filtragem: Filtre trabalhos por políticas, status do trabalho, tipo de agendamento e intervalo de datas para facilitar a navegação e o gerenciamento.



Lista de tarefas de conformidade

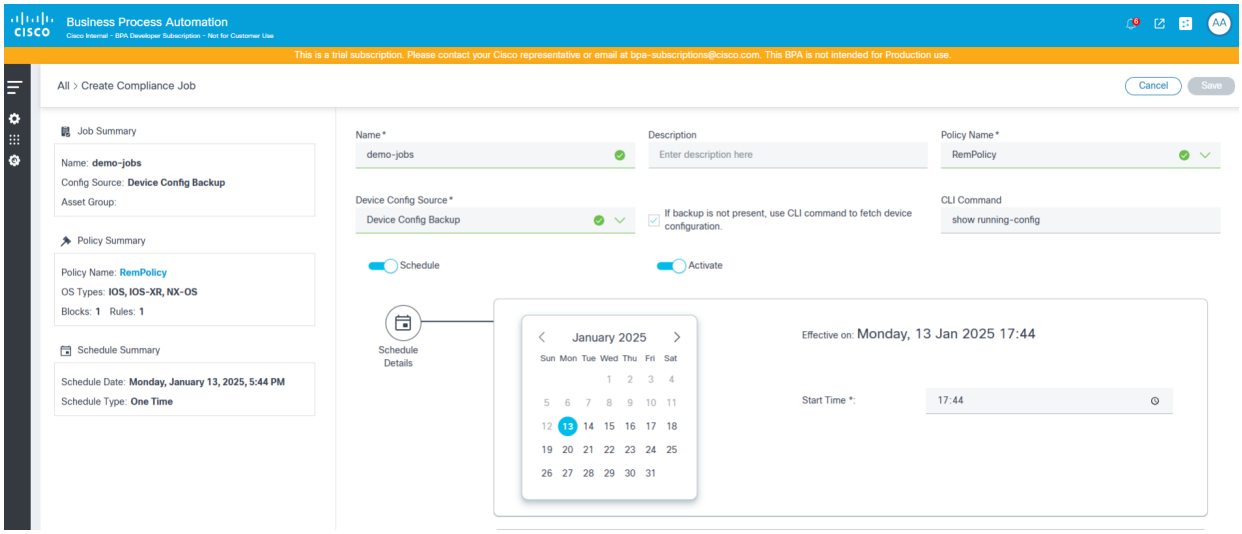
Criando Jobs de Conformidade

A página Criação de Job de Conformidade inclui os seguintes atributos:

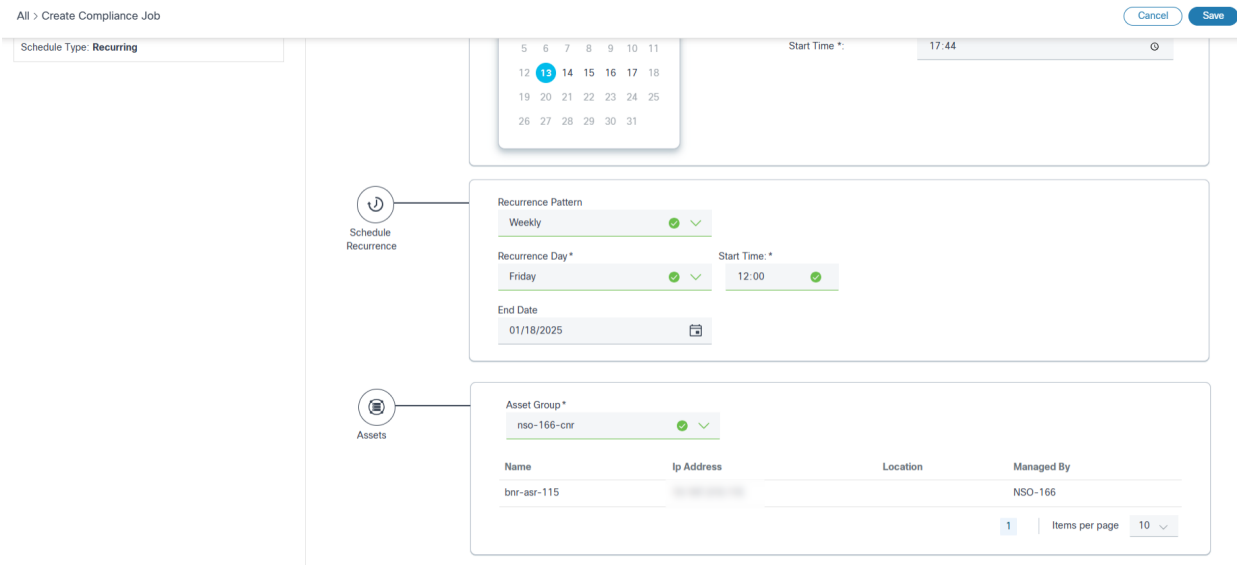
- Nome: Nome do trabalho
- Descrição: Uma descrição opcional
- Nome da política: Uma lista suspensa para selecionar uma política a ser executada, potencialmente filtrada por políticas de acesso configuradas para o usuário conectado
- Origem da configuração do dispositivo: Uma lista suspensa para selecionar a origem para buscar a configuração do dispositivo (configuração atual ou backup de configuração do dispositivo) para executar o trabalho de conformidade e uma caixa de seleção para indicar se deve fazer fallback para um comando CLI se o backup não estiver presente.

Note: A opção Device Config Backup funciona somente se o controlador subjacente suportar o recurso de backup.

- Variáveis Definidas pelo Usuário: Caixa de texto editável para namespace disponível quando a política selecionada tem variáveis definidas pelo usuário
- Detalhes da Agenda: Seção para selecionar vários parâmetros de agendamento, como data/hora de início e término, padrão de recorrência, etc.
- Ativos: Selecione um grupo de ativos para identificar a lista de dispositivos para executar a conformidade
- Agendamento: Alternar para ativar ou desativar a execução do job dentro do cronograma (ocasional ou recorrente); Se desativado, o job é executado imediatamente
- Está Ativo: Indica se o agendamento selecionado está ativo ou não



Criando Jobs de Conformidade



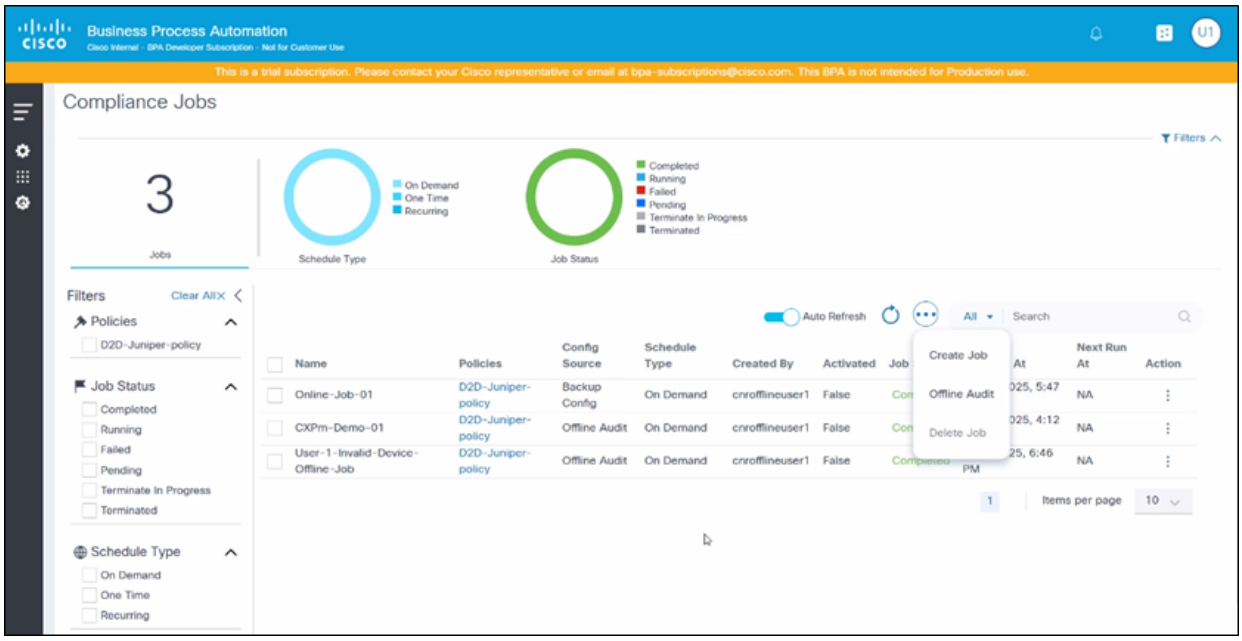
Criando trabalhos de conformidade 2

Criando Trabalhos de Auditoria Off-line

O recurso de auditoria off-line em tarefas de conformidade permite que os usuários realizem verificações de conformidade nas configurações do dispositivo sem exigir que os dispositivos sejam integrados no BPA. Os usuários podem carregar manualmente a configuração do dispositivo como um arquivo. Várias configurações de dispositivo podem ser compactadas e carregadas juntas como um arquivo zip. Depois de carregados, esses arquivos de configuração são analisados e os Jobs de Conformidade podem ser criados usando o conteúdo desses arquivos como origem. Os resultados das auditorias off-line são exibidos no painel de conformidade juntamente com os resultados da auditoria on-line.

A página Auditoria Off-line inclui os seguintes atributos:

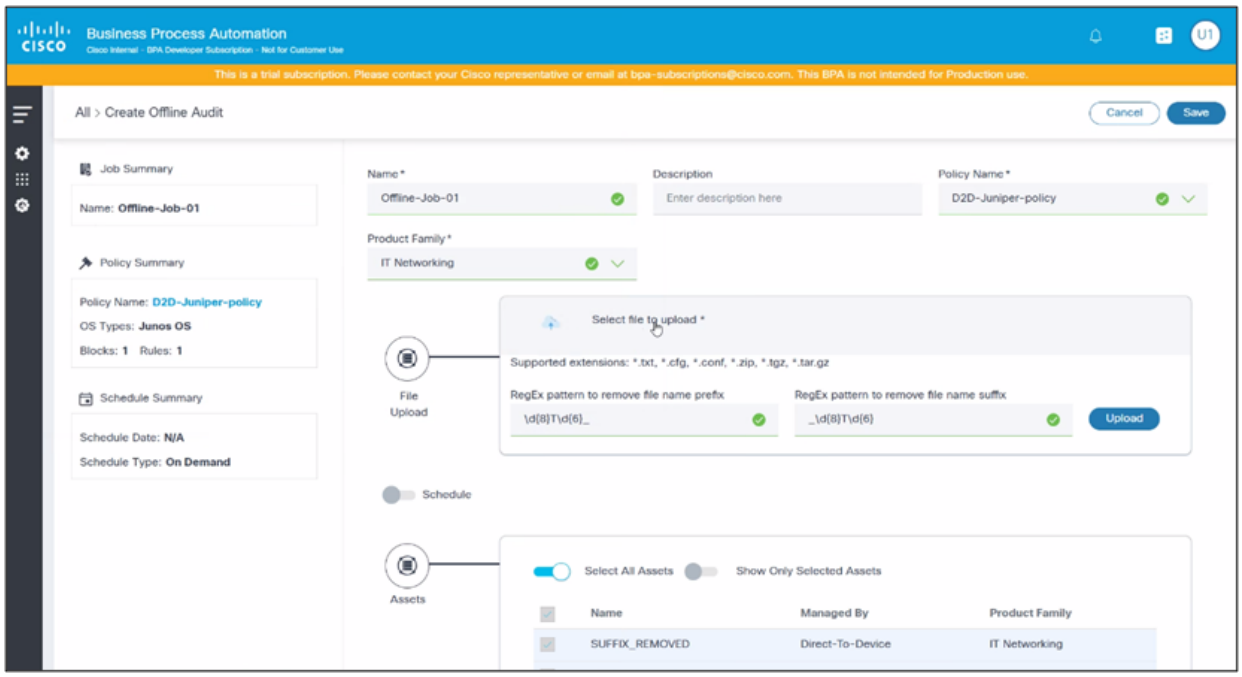
- Nome: Nome do trabalho
- Descrição: Uma descrição opcional
- Nome da política: Uma lista suspensa para selecionar uma política a ser executada, potencialmente filtrada por políticas de acesso configuradas para o usuário conectado
- Linha de produtos: Uma lista suspensa para selecionar a família de produtos
- Upload de arquivo: Usar o recurso de auditoria off-line para carregar os arquivos de configuração manualmente; Isso é feito por meio de uma interface de upload na qual você seleciona os arquivos no sistema local
- Agendamento: Alternar para ativar a agenda
- Ativos: Mostra a lista de dispositivos de acordo com o conteúdo do arquivo carregado



Selecionar Auditoria Offline

Para criar jobs de auditoria off-line:

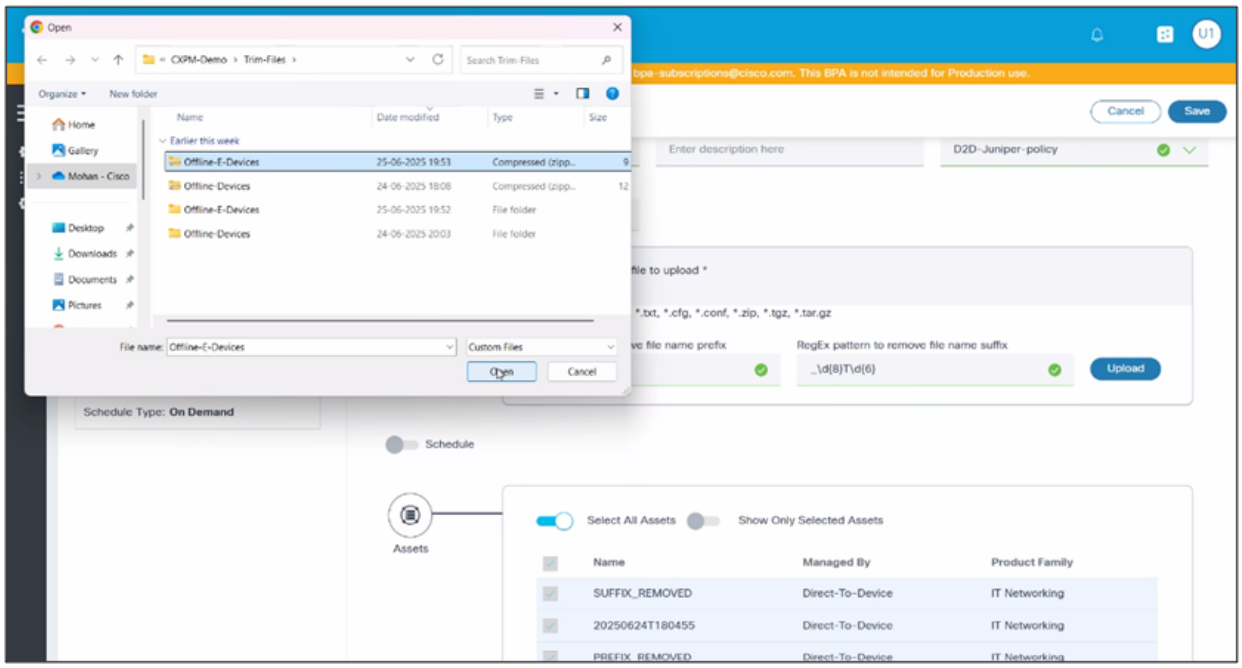
1. Selecione Auditoria off-line no ícone Mais opções.



Carregar arquivo

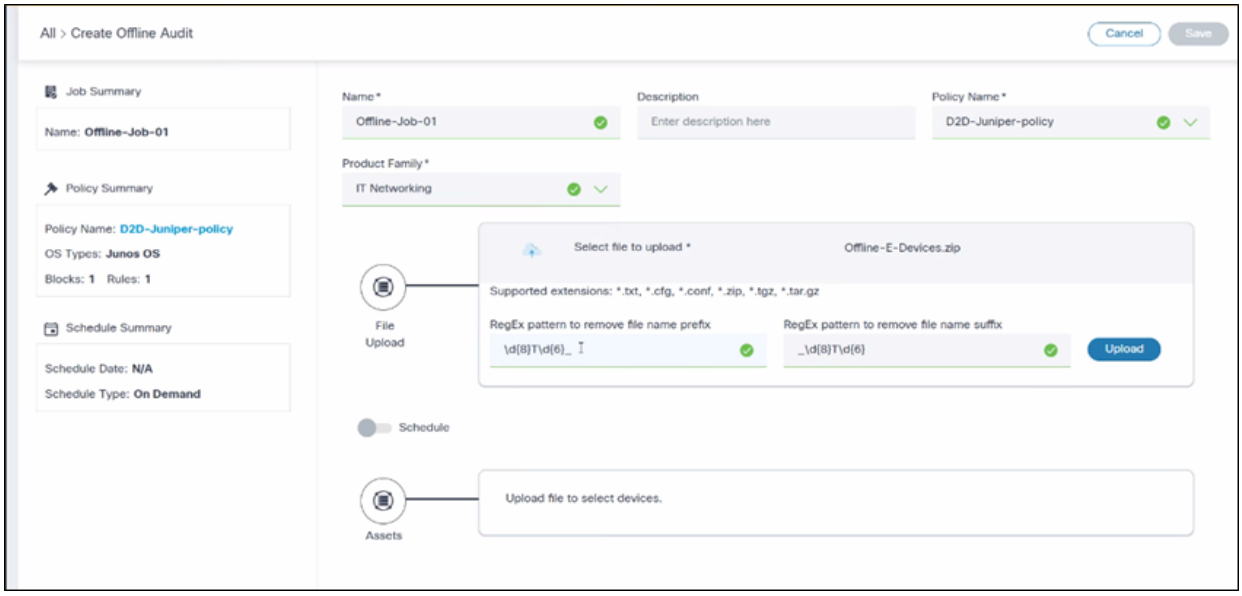
2. Clique em Selecionar arquivo para carregar arquivos de configuração.

Note: Os tipos de arquivo suportados incluem (.txt,.cfg,.conf,.zip,.tgz,.tar.gz).



Arquivos da Área de Trabalho

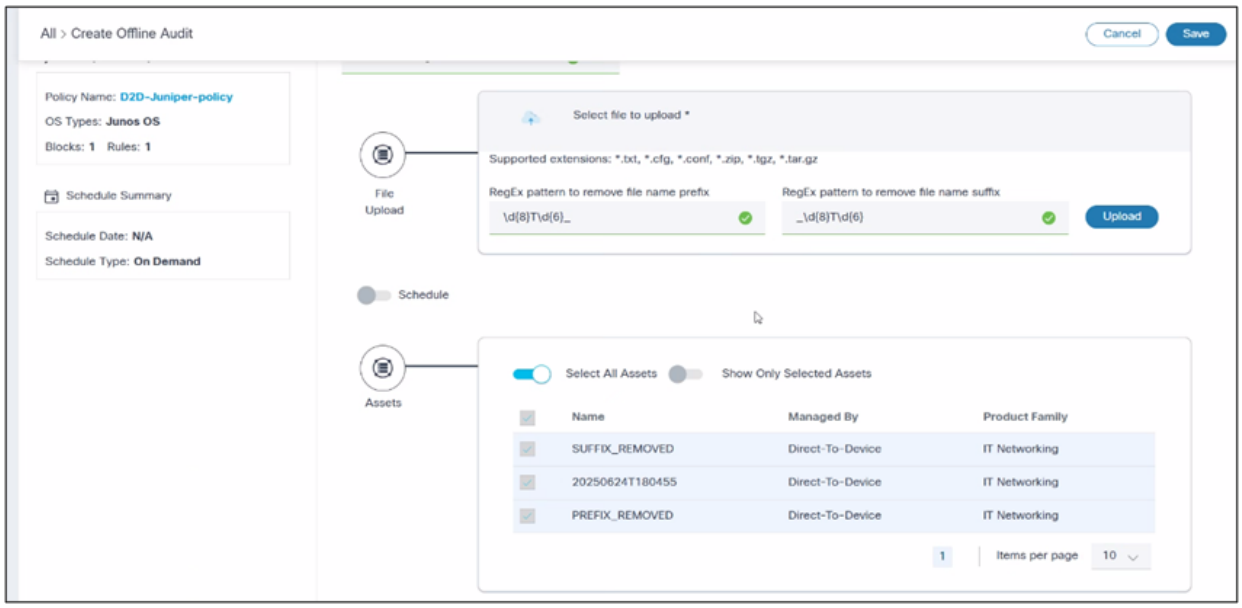
3. Se os arquivos de configuração forem compactados em uma pasta ou arquivo, extraia os arquivos antes de carregá-los.



Padrão Regex

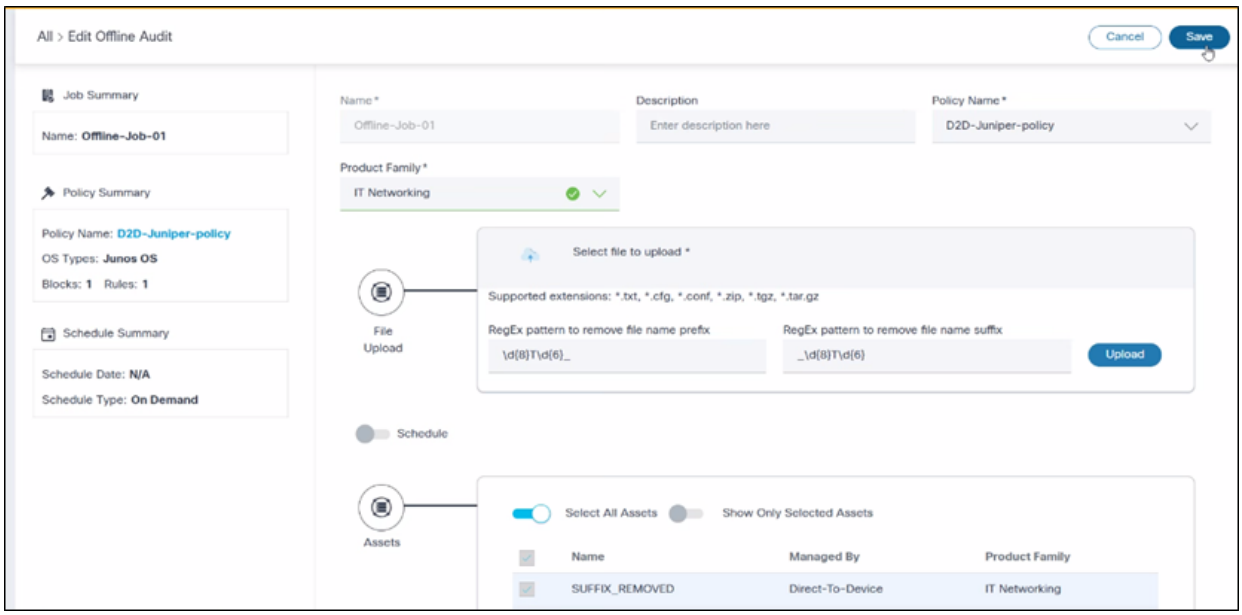
4. Aplique o padrão Regex para o corte do nome do arquivo (opcional).

Note: Use padrões de aparagem de prefixo ou sufixo (regex) para padronizar ou simplificar os nomes de arquivos carregados para facilitar o processamento.



Carregar os arquivos

5. Clique em Fazer upload. Uma mensagem de confirmação é exibida, indicando que os arquivos foram salvos no banco de dados e foram carregados com êxito.



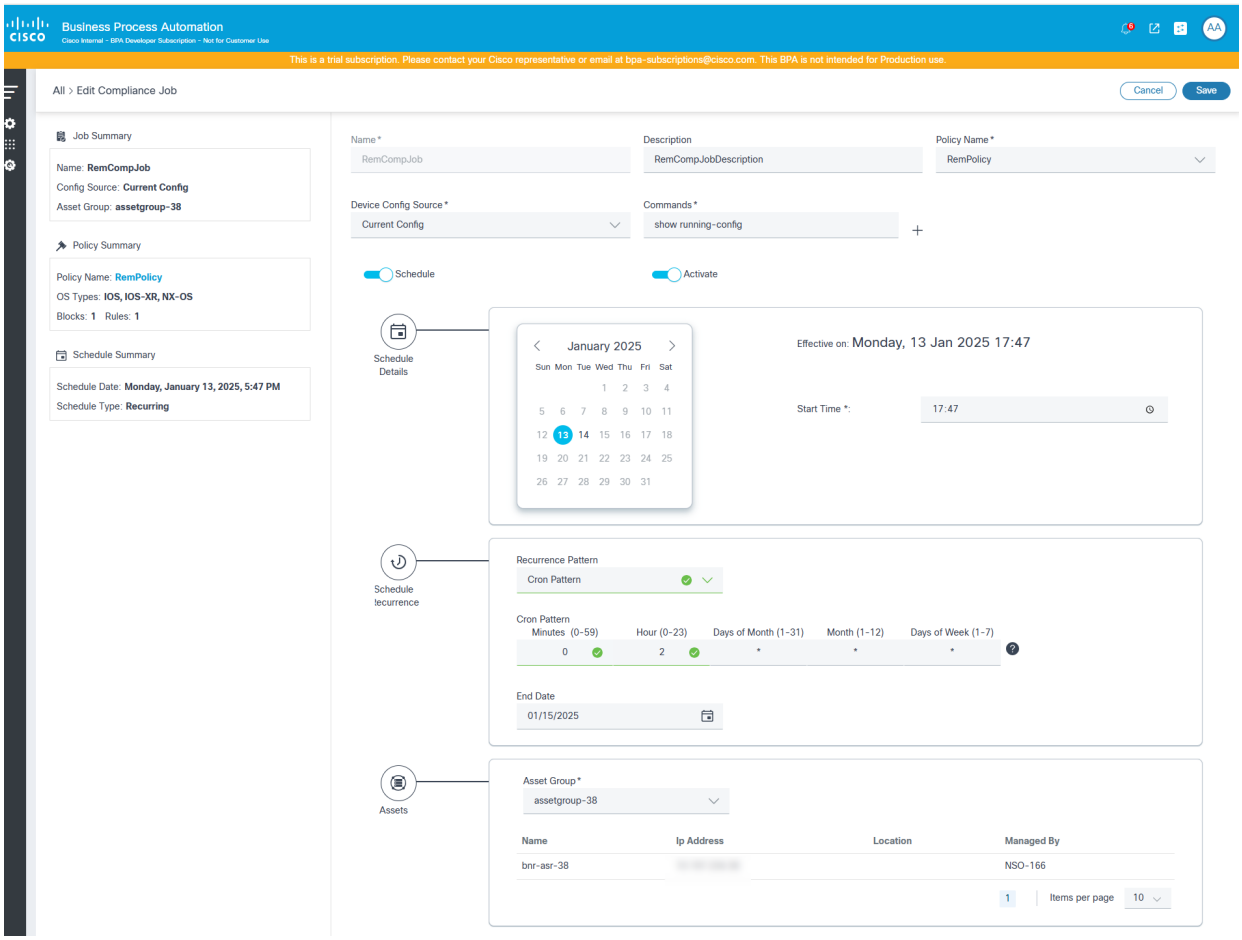
Salvar Auditoria Offline

6. Clique em Salvar para criar o trabalho de auditoria offline.

Editando Jobs de Conformidade

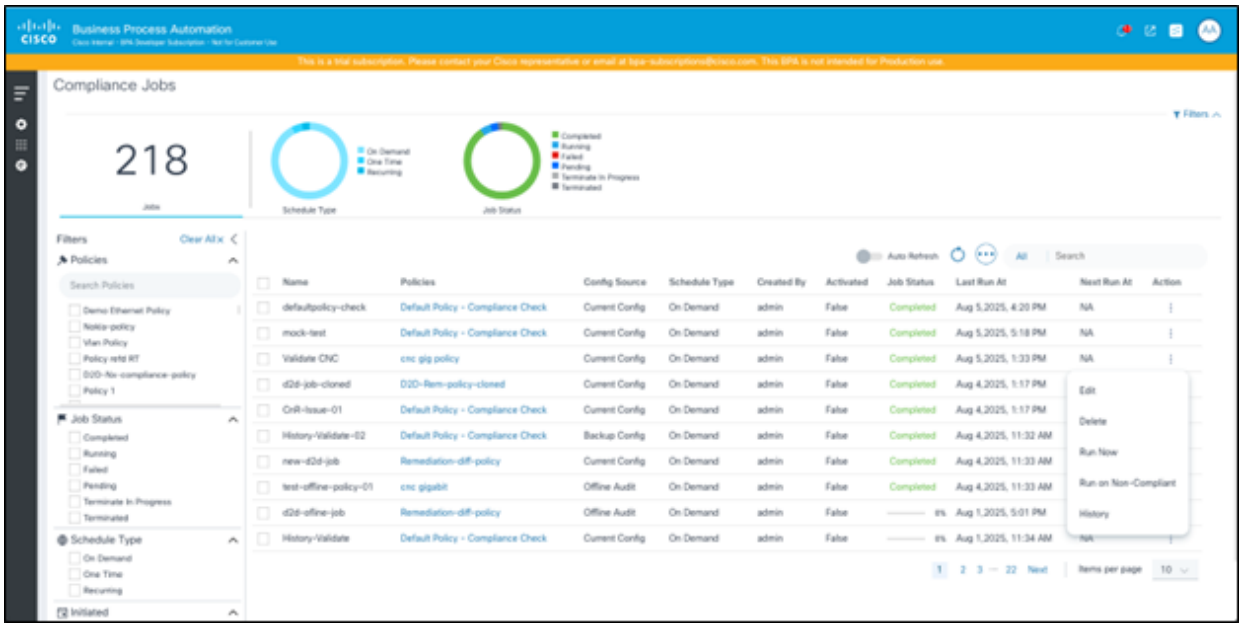
Para editar Jobs de Conformidade, siga as etapas fornecidas em Criação de Jobs de Conformidade.

Note: O nName da tarefa não é editável.



Editando Job de Conformidade

Executar agora ou Executar novamente os trabalhos de conformidade



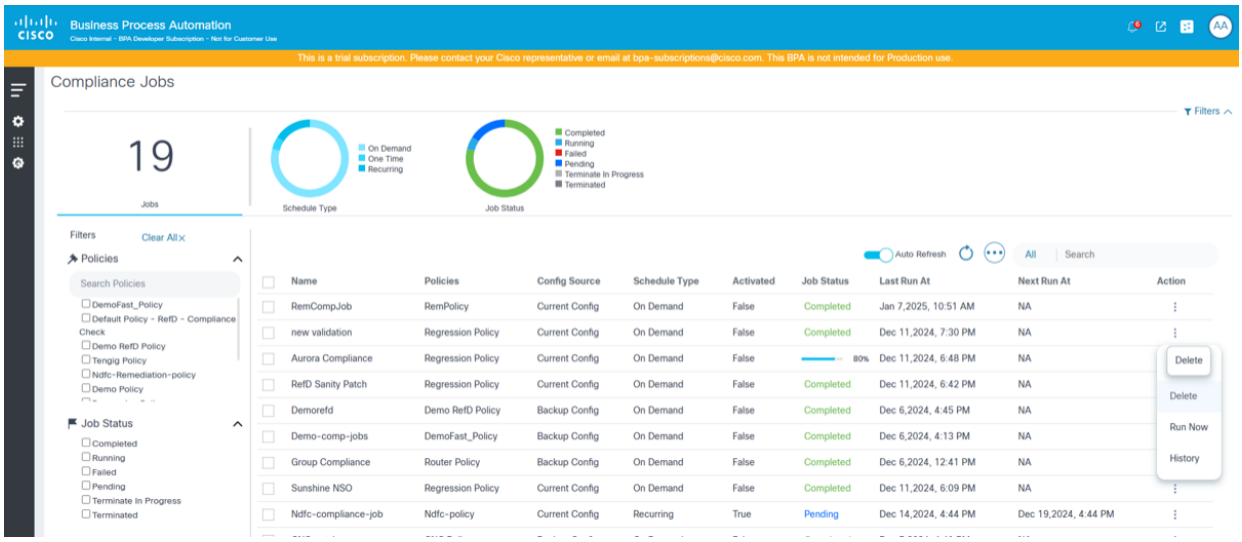
Trabalho de Conformidade - Executar Agora e Executar em Não Compatível

A grade Jobs de Conformidade tem uma opção para executar um job sob demanda selecionando Executar Agora no ícone Mais Opções. Se um job tiver uma execução existente, os usuários poderão selecionar Executar em Não Compatível no ícone Mais Opções. Esta ação executa o job de conformidade apenas na lista de ativos que não estão marcados como Totalmente Compatíveis na execução anterior.

Excluindo Trabalhos de Conformidade

O portal fornece uma opção para excluir um ou mais Jobs de Conformidade se o usuário tiver a função RBAC (Role Based Access Control) correta. Os trabalhos não podem ser excluídos quando uma execução está em andamento. Os usuários podem optar por excluir um ou vários Jobs de Conformidade.

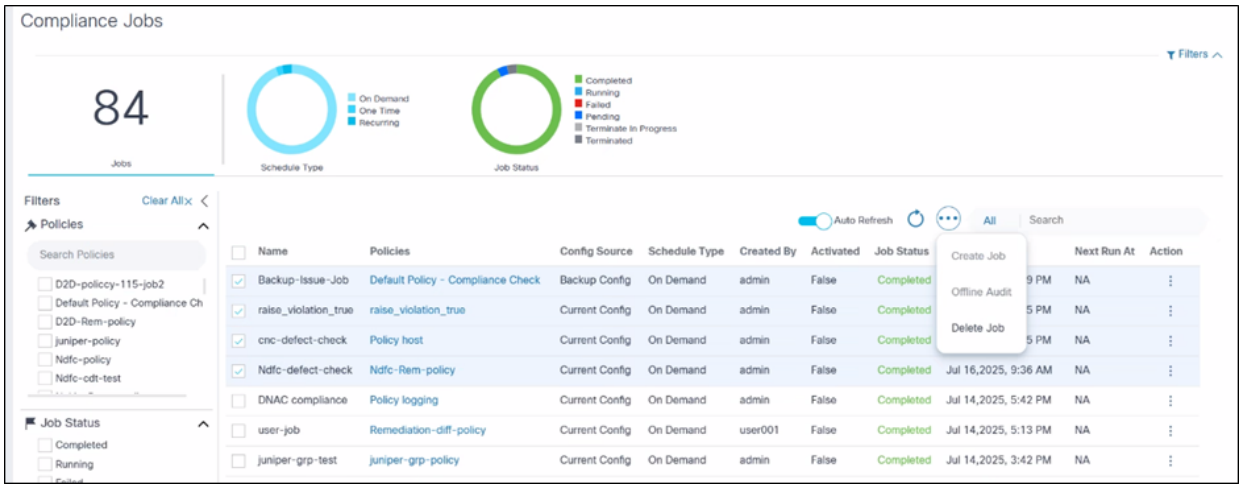
Para deletar um Job de Conformidade:



Deletando um Único Job de Conformidade

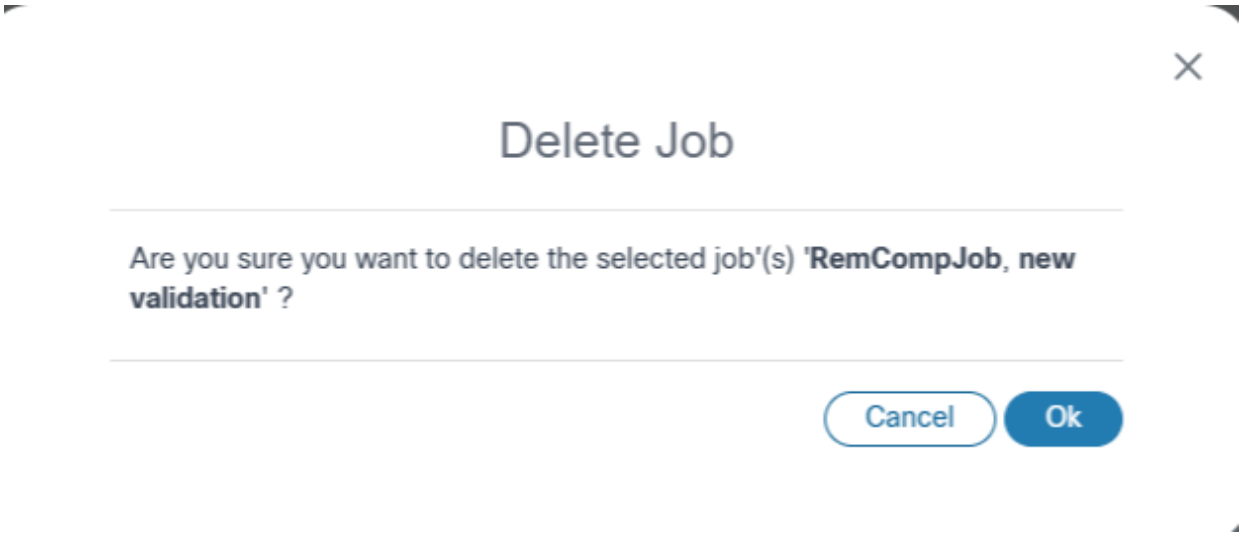
1. Na página Jobs de Conformidade, selecione o ícone Mais Opções > Deletar no job a ser deletado.

OU



Deletando Vários Jobs de Conformidade

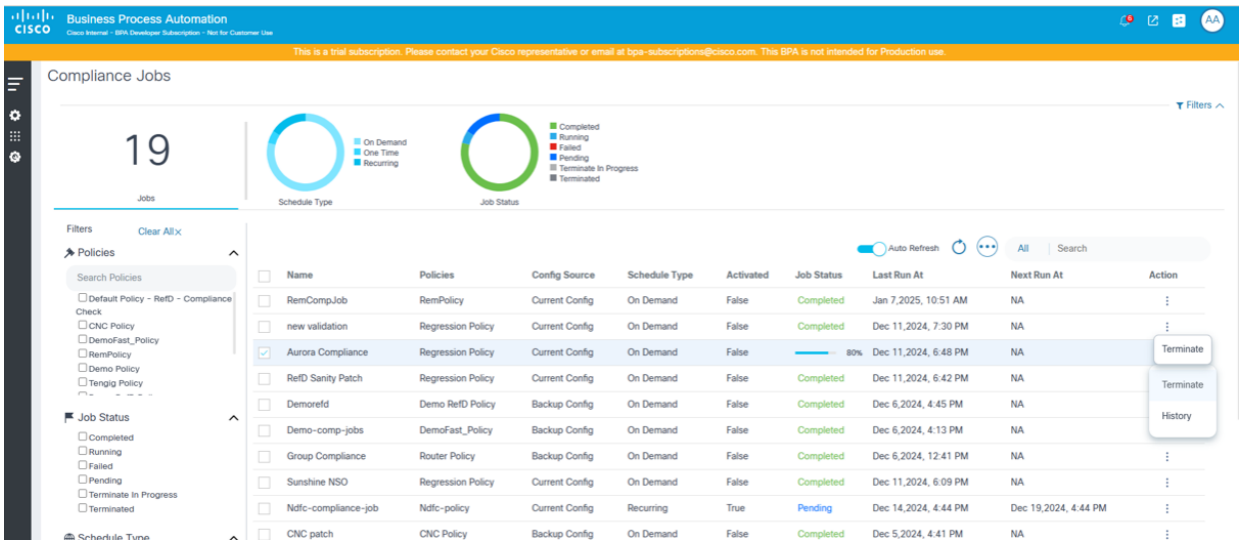
Para excluir vários Trabalhos de Conformidade, marque as caixas de seleção dos trabalhos a serem excluídos e selecione Mais Opções > Excluir Trabalho. Uma confirmação é exibida.



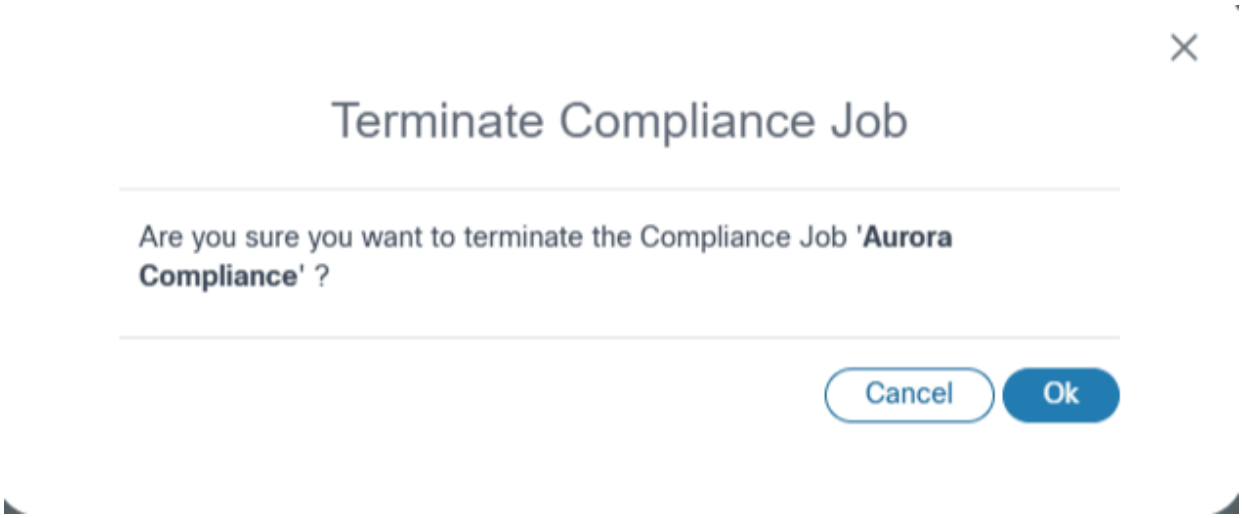
Confirmação de Deleção de Trabalho de Conformidade

Encerrando Trabalhos de Conformidade

O portal fornece aos usuários uma opção para encerrar uma execução em execução de um determinado job. Quando um trabalho é finalizado, os dispositivos em execução no momento concluem sua execução e cancelam todas as execuções de dispositivos na fila.



Encerrando Trabalhos de Conformidade

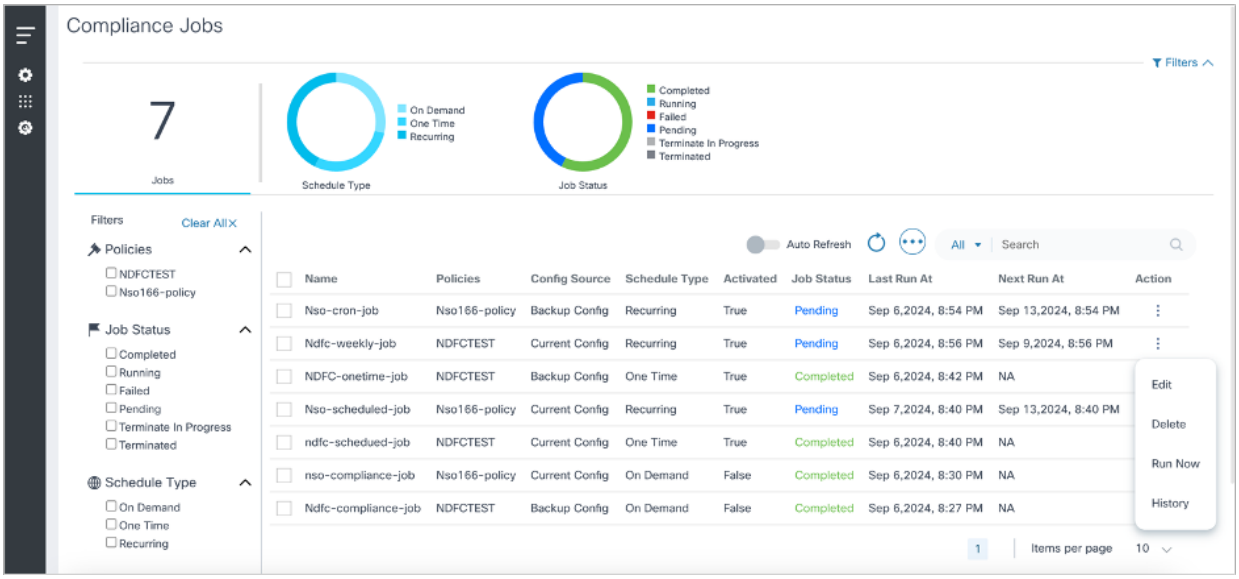


Confirmação de Finalização de Trabalho de Conformidade

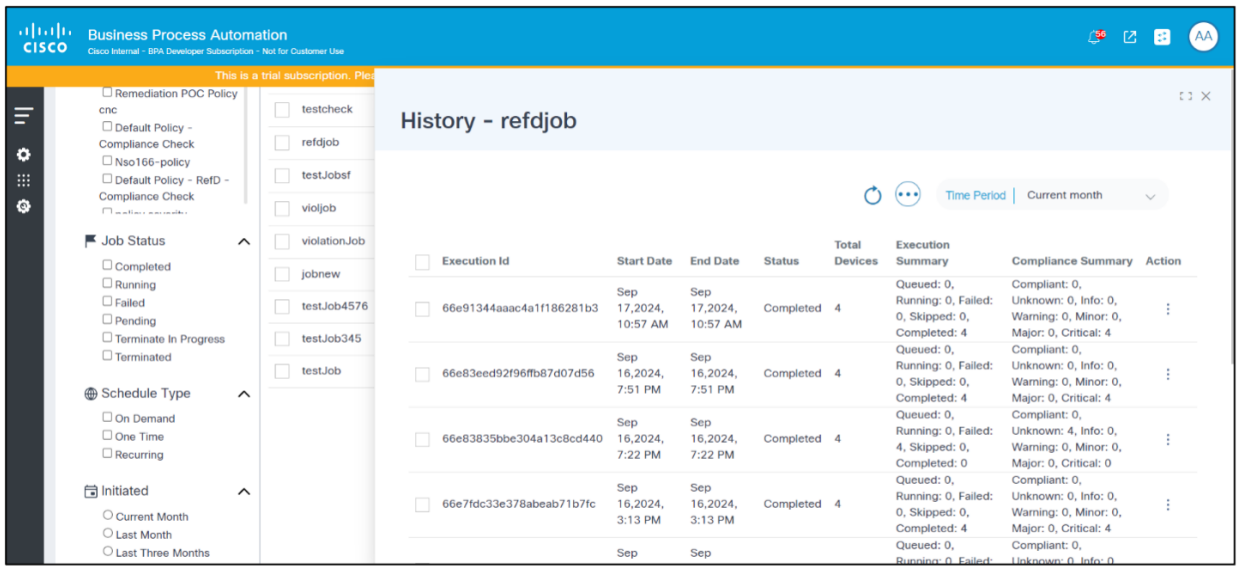
Histórico de Trabalhos de Conformidade

A opção Histórico no Job de Conformidade mostra a lista de execuções do job selecionado, filtrada pelo intervalo de datas da programação.

Para exibir o histórico de um Job de Conformidade, na página Jobs de Conformidade, selecione o ícone Mais Opções > Histórico. A página Histórico é exibida.



Histórico de Trabalho de Conformidade

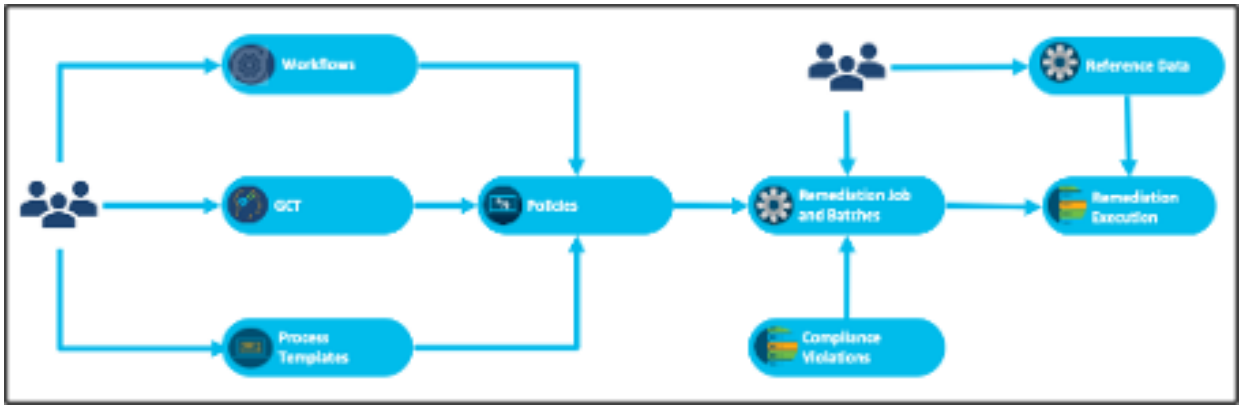


Página Histórico

Trabalhos de Correção

A Estrutura de correção permite que os operadores corrijam as violações de conformidade listadas no painel de controle de conformidade. Essa estrutura usa fluxos de trabalho, GCTs e modelos de processo.

Diagrama de Fluxo de Correção de Configuração



Visão geral do Configuration Remediation

O caso de uso de correção de configuração permite que os operadores corrijam violações de configuração em dispositivos que usam Trabalhos de Correção. A política de conformidade é configurada primeiro com o fluxo de trabalho apropriado, modelos GCT e modelos de processo por tipo de controlador. Um Trabalho de Correção é executado para uma política em relação a uma lista de ativos afetados. Durante a correção, os valores a serem aplicados em um dispositivo podem ser buscados de várias fontes de dados, incluindo o resultado da execução de conformidade, o aplicativo RefD e a configuração do dispositivo existente. O fluxo de trabalho

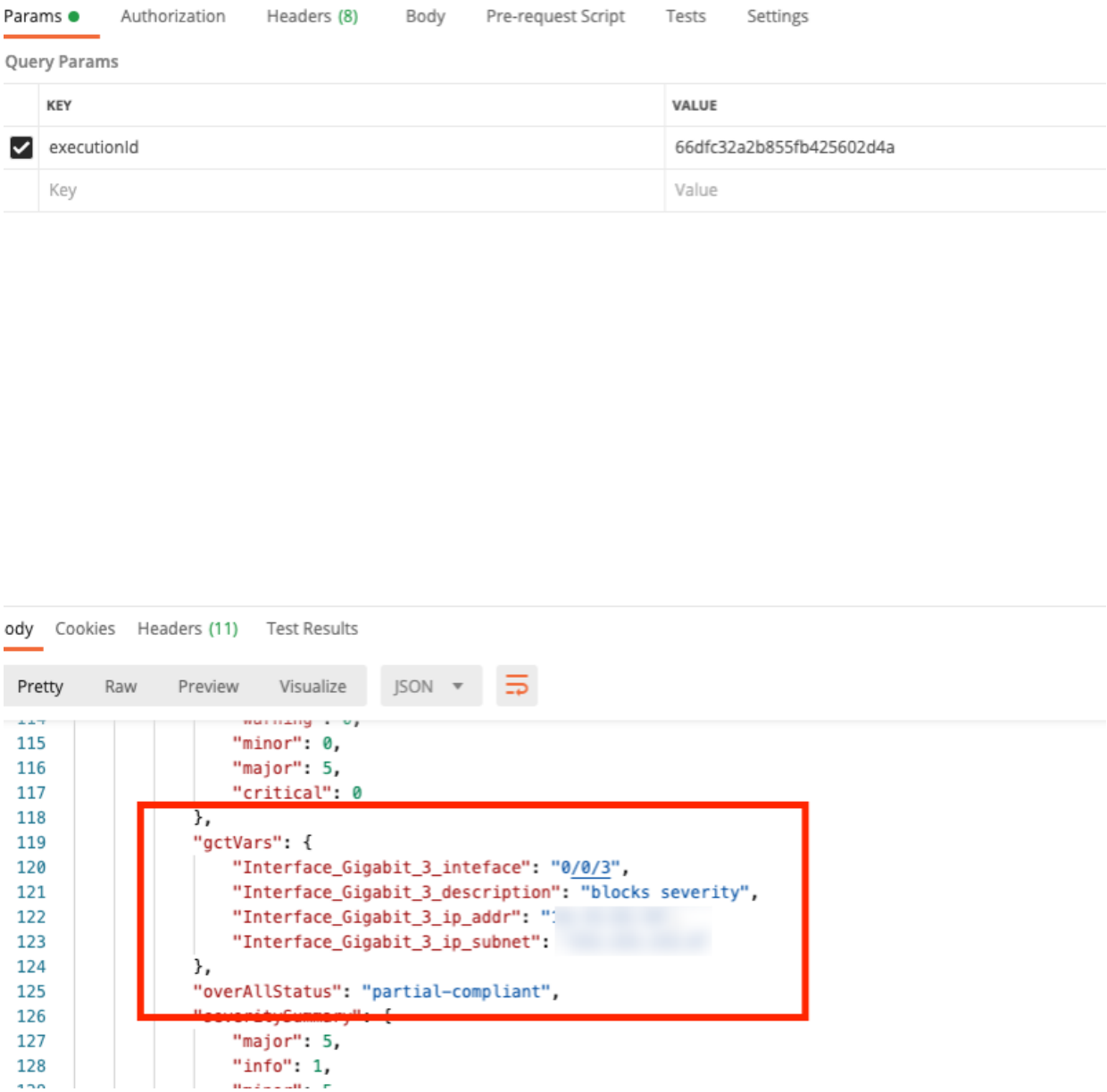
pode ser personalizado de acordo com o requisito específico do cliente para acomodar etapas adicionais durante a correção.

As etapas mais importantes do recurso de remediação são explicadas abaixo:

Modelo GCT

Os GCTs são um recurso central do BPA usado para aplicar alterações de configuração em dispositivos que usam modelos específicos de controlador.

- Criação de um modelo GCT que atualize as configurações do dispositivo, resolvendo violações de conformidade
- A estrutura suporta mapeamento automático de variáveis se as variáveis dentro do modelo GCT estiverem de acordo com a seguinte sintaxe:
    - Para blocos de configuração de dispositivo único: **<>_<>** Exemplo: management_interface_ipv4_addr, management_interface_ipv4_subnet
    - Vários blocos de configuração de dispositivo estão planejados para uma versão futura
- Se "Block Identifier Name" e "Variable Name from block" contiverem espaços, estes espaços deverão ser substituídos por sublinhados ("_") (por exemplo, se "Block Identifier Name" for "Management Interface" e "Variable Name" for "IPV4_ADDR", o nome da variável no GCT deverá ser "Management_Interface_IPV4_ADDR")
- Os usuários podem verificar a saída "gctVars" da execução do dispositivo de conformidade para ver se a sintaxe e os mapeamentos das variáveis GCT estão corretos; Para obter a execução do dispositivo de conformidade, use as seguintes APIs REST:
    - Obter execuções para localizar a ID de execução
        - URL: /api/v1.0/compliance-remediation/compliance-executions
        - Método: GET
    - Obter Execuções de Dispositivo usando a ID de execução
        - URL: https://<>/bpa/api/v1.0/compliance-remediation/compliance-device-executions?executionId=<>
        - Método: GET



Variáveis GCT - gctVars

- Para recuperar as variáveis do bloco, use a seguinte API REST:
  - URL: https://<>/bpa/api/v1.0/compliance-remediation/utils/schema
  - Método: POST
  - Corpo: {"blockName": "<< nome do bloco >>" }
- Validar os modelos GCT aplicando os modelos aos dispositivos para simulação e confirmação
- Configurar os modelos GCT acima na política de conformidade

Fluxos de trabalho

A estrutura de remediação oferece os seguintes fluxos de trabalho de referência prontos para uso:

- PROCESSO DE CORREÇÃO: Esse fluxo de trabalho tem o conjunto comum de etapas envolvidas na execução da correção.
- SUBPROCESSO DE CORREÇÃO: Este fluxo de trabalho contém tarefas de atribuição variável, execução a seco GCT e confirmação GCT que podem ser personalizadas por outras equipes de acordo com os requisitos.

Ambos os fluxos de trabalho podem ser usados como estão, atualizados ou substituídos de acordo com as necessidades do cliente.

Modelos de processo

Os modelos de processo e de análise podem ser configurados de acordo com a política para executar verificações prévias e posteriores e comparar o resultado.

Políticas

A política CnR combina os fluxos de trabalho, modelos GCT e modelos de processo por tipo de dispositivo que pode ser usado para corrigir a configuração usando trabalhos.

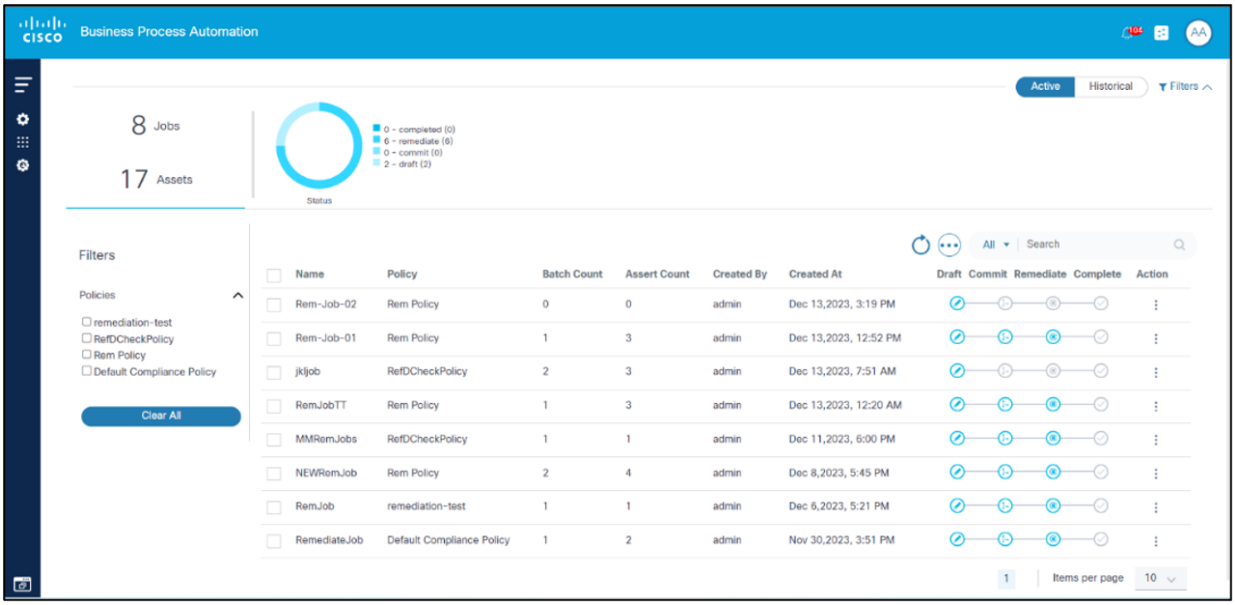
Trabalhos de Correção

Os trabalhos de remediação ajudam os operadores a aplicar políticas de remediação em uma lista selecionada de ativos afetados. O Trabalho de Correção pode ser executado sob demanda ou dentro do cronograma. Em tempo de execução, o fluxo de trabalho de remediação pode extrair dados de várias fontes, incluindo detalhes do dispositivo, detalhes de execução de conformidade e estrutura de RefD.

Lista de Trabalhos de Correção

Os usuários podem filtrar, classificar e exibir Trabalhos de Correção criados no painel da seguinte forma:

- Trabalhos: Exibe o total de trabalhos criados
- Ativos: Exibe o total de ativos criados
- Status: Exibe os trabalhos por status
- Ativo e histórico: Exibe tarefas Ativas ou Históricas (inativas), com base na seleção
- Políticas: Filtra Trabalhos de Correção por políticas
- Grade Principal: Exibe a lista padrão de trabalhos que podem ser classificados clicando no cabeçalho e inclui uma pesquisa por Nome e política com paginações
- Ações: Os trabalhos podem ser arquivados ou excluídos quando estiverem em um estado de rascunho ou concluído; um trabalho em execução não pode ser arquivado ou excluído

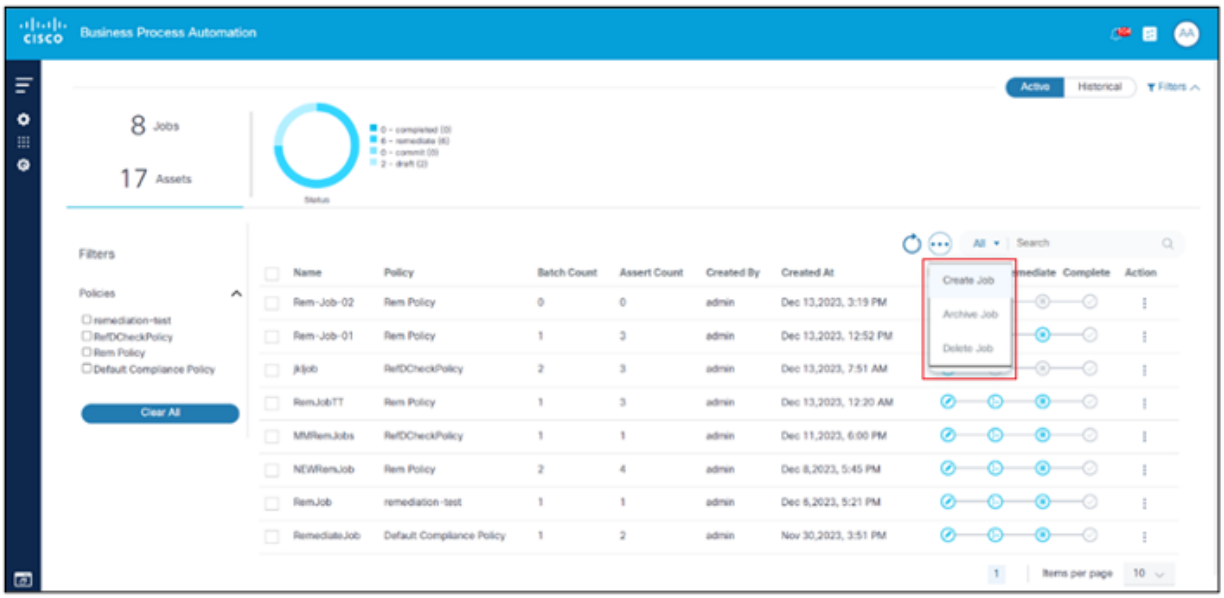


Lista de Trabalhos de Correção

Criando e Editando Jobs de Correção

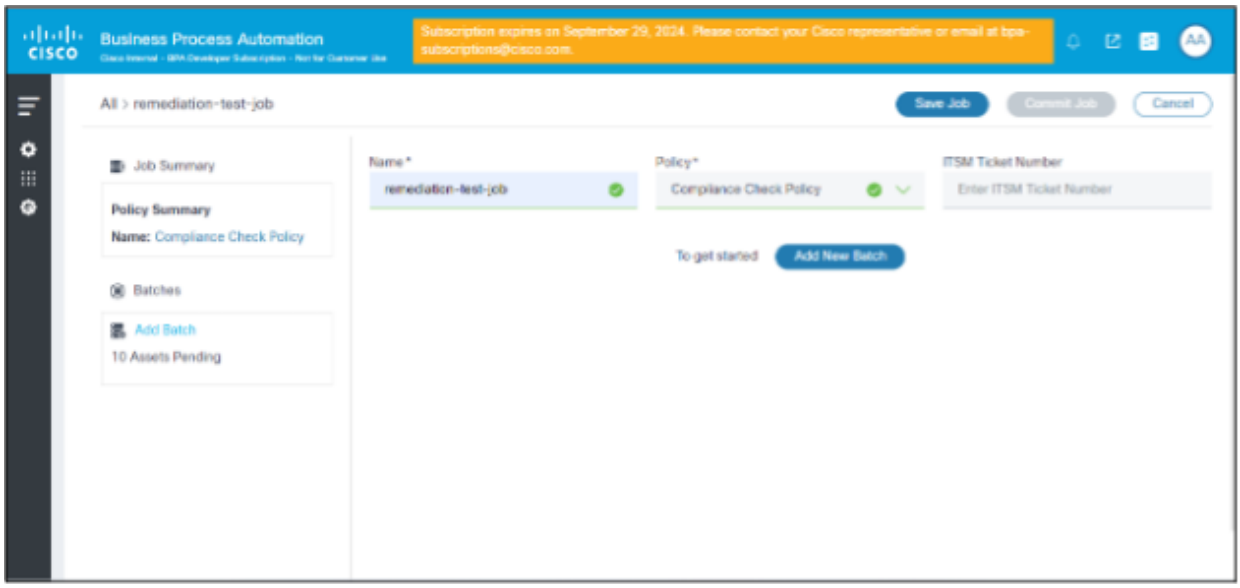
Os Trabalhos de remediação são criados na página Lista de trabalhos e podem ser criados executando as seguintes etapas:

1. Selecione o ícone Mais Opções > Criar Job. A página Criar Job é exibida.



Opções de Trabalhos de Correção

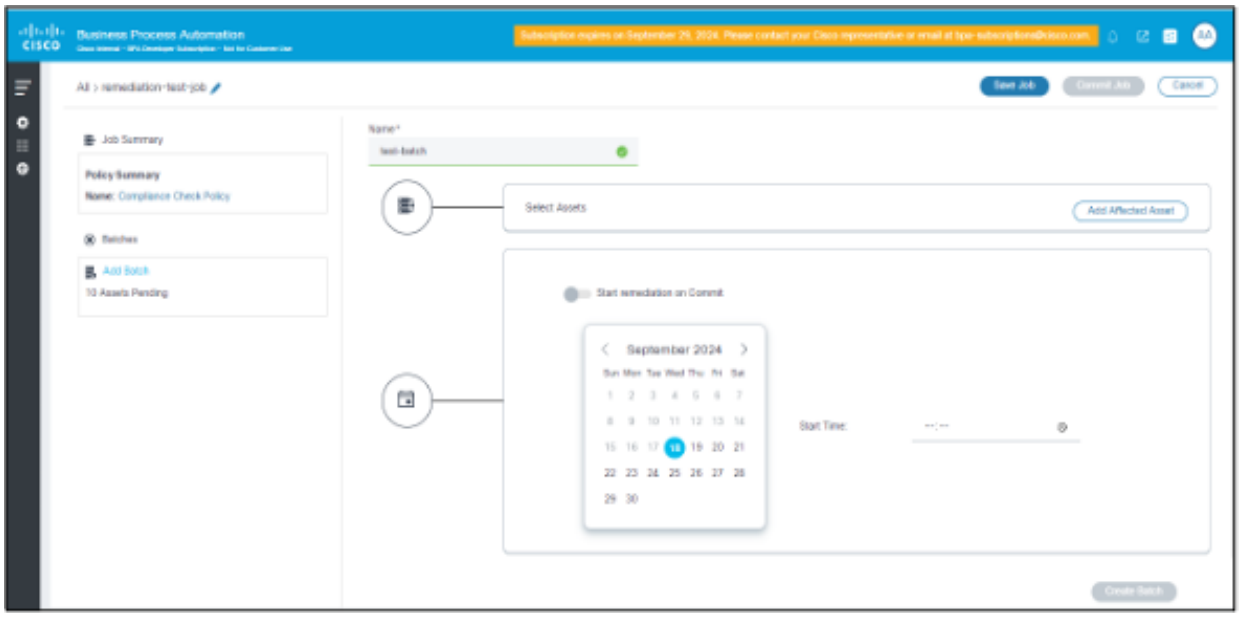
2. Complete ou edite os detalhes.



Trabalhos de correção: Detalhes

3. Clique em Save Job.

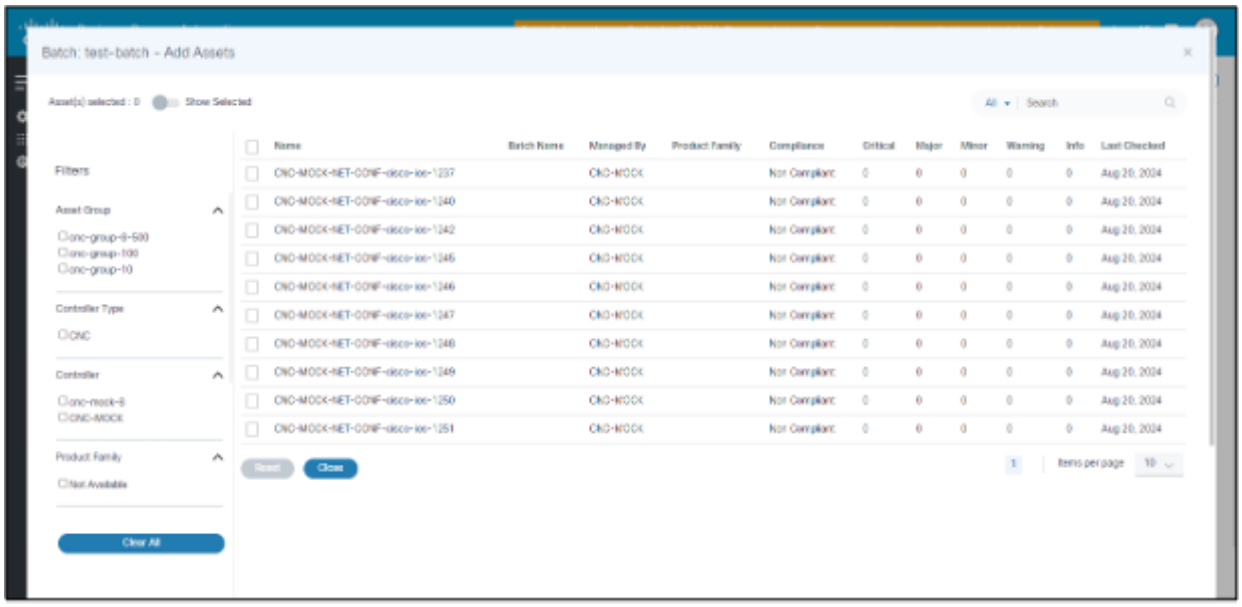
Para adicionar lotes a jobs na página Criar Job:



Trabalhos de correção: Adicionar lotes

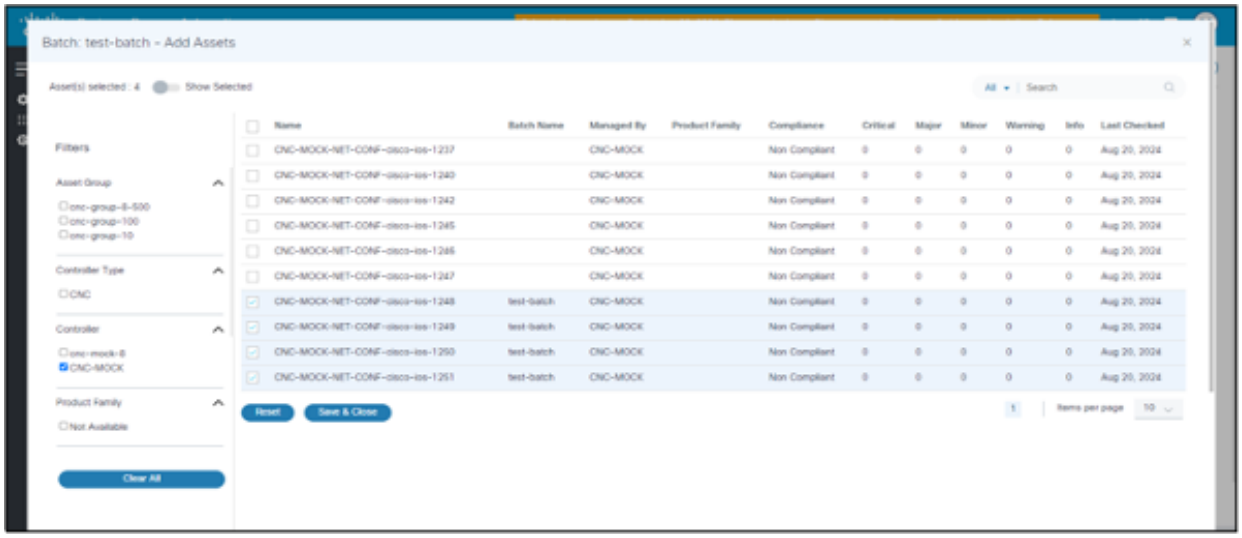
1. Clique em Adicionar novo lote.
2. Insira o Nome, Detalhes do ativo afetado e Detalhes da agenda.
3. Clique em Adicionar ativos afetados.
4. Na página Detalhes de ativos, selecione a lista de ativos afetados e clique em Salvar trabalho.
5. Filtre os ativos com base no Tipo de controlador, Controlador, Grupo de ativos e Família de produtos.
6. Quando os ativos estiverem selecionados, clique em Salvar e fechar para retornar à página

anterior.



Trabalhos de correção: Adicionar ativos afetados

Note: Os usuários têm a opção de aplicar filtros na página Ativos afetados



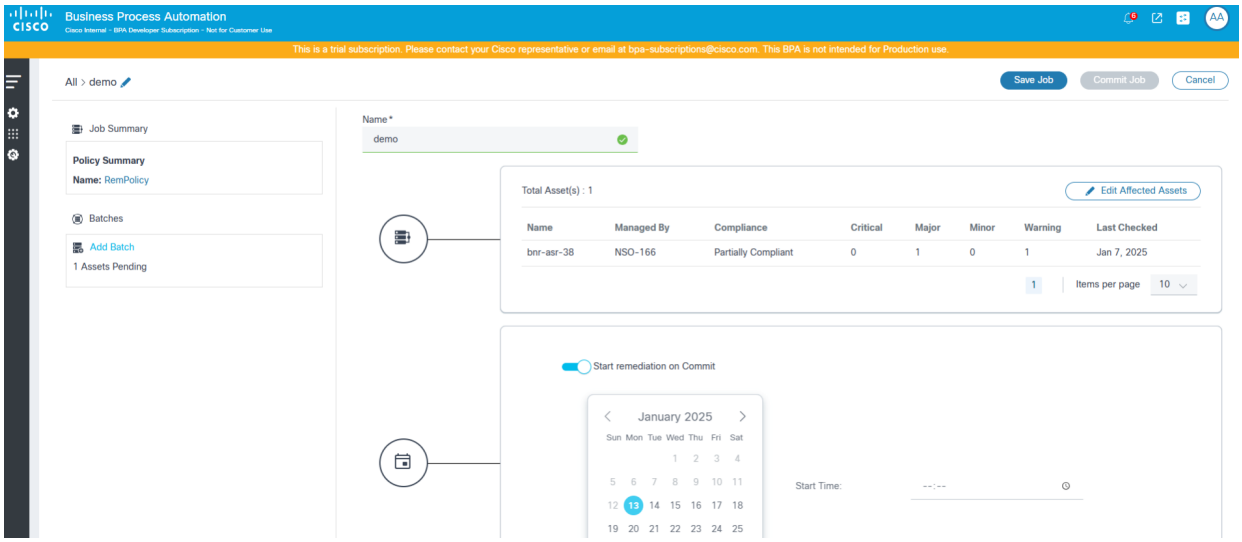
Trabalhos de correção: Adicionar filtros afetados

Depois que os ativos afetados forem adicionados, o lote poderá ser executado uma vez, seja ao salvar, seja em um horário futuro agendado.

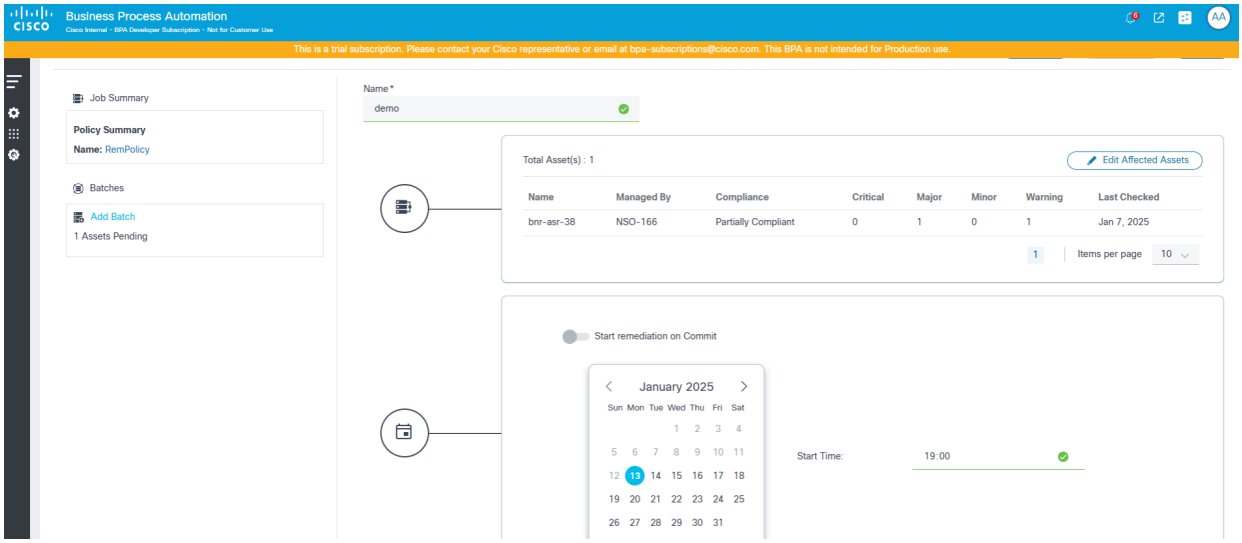
Note: Para executar o trabalho como Sob demanda, ative a alternância Iniciar remediação na confirmação. Se um usuário selecionar essa opção, a data e a hora não serão necessárias. Se o usuário selecionar a opção Ocasional, a data e a hora deverão ser fornecidas para que o job seja executado.

Um único Trabalho de Correção tem mais de um lote. Cada lote pode ser iniciado na confirmação ou em uma data e hora programadas.

Um lote de correção de confirmação pode ser executado sob demanda ou Agendado.



Trabalhos de correção: Sob demanda



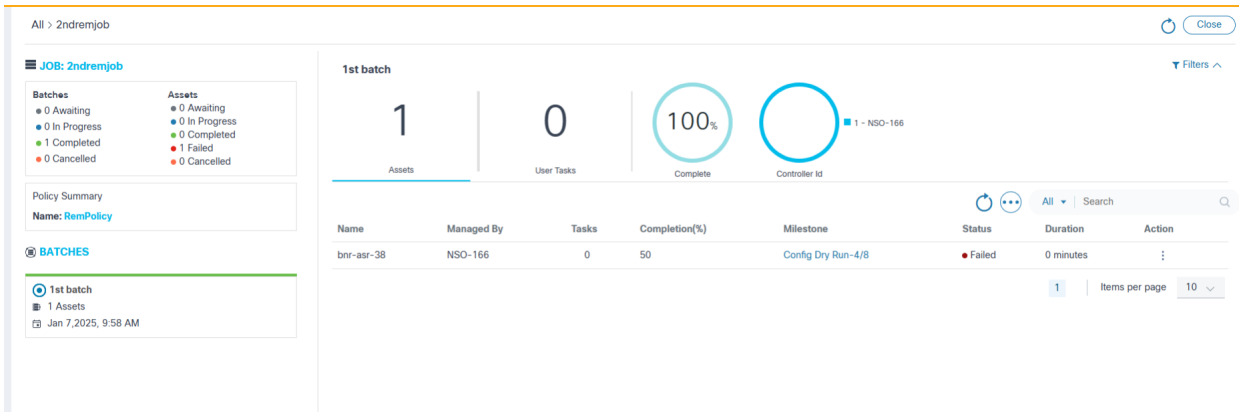
Trabalhos de correção: Uma Vez/Agendado

Execução da Correção: Lista de dispositivos

Depois que o trabalho de remediação é confirmado, a execução é disparada e o status do trabalho é exibido na página Listar dispositivos em Trabalhos de remediação. Os usuários podem aplicar filtros por ID do controlador, Nome, Gerenciado por, Família de produtos.

- CARGO: exibe os detalhes de status de lotes e ativos e o nome da política selecionada para executar o trabalho de correção

- LOTES: exibe a lista de lotes como parte do trabalho de correção atual
- Atualização automática: exibe as opções para atualizar automaticamente a página a cada 30 segundos se o job estiver no estado em execução, atualizar a página ou cancelar para voltar à página anterior
- Detalhes do nível de lote: exibe os detalhes do resumo em nível de lote, incluindo contagem total de ativos, contagem de tarefas do usuário, porcentagem de conclusão e detalhes do controlador
- Grade de ativos: exibe a exibição de grade Ativo, incluindo tarefa do usuário, porcentagem de conclusão e marco atual para cada ativo



Execução da Correção: Lista de Dispositivos

Execução da Correção: Detalhes da tarefa do usuário embutido

Na lista de dispositivos, a coluna Tasks indica se um usuário tem alguma tarefa a ser executada.

Para exibir detalhes da tarefa do usuário em linha:

1. Selecione a contagem de tarefas. A janela de lista User Tasks é aberta.
2. Selecione uma tarefa. A janela Detalhes da tarefa do usuário é aberta.

As seguintes ações podem ser executadas em linha:

- Completo
- Repetir
- Cancel

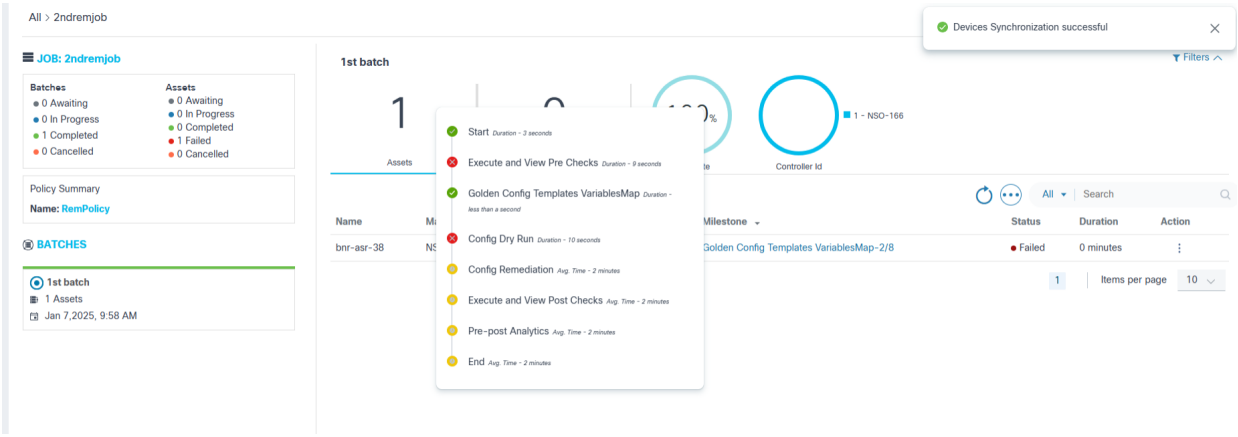
Execução da Correção: Detalhes da Etapa Embutida

Na lista de dispositivos, a coluna Marco indica o marco atual relacionado à correção do dispositivo fornecido.

Para exibir detalhes do marco embutido, selecione a coluna. A janela Detalhes do marco é aberta.

Os seguintes status estão disponíveis para etapas:

- Não iniciado
- Executando
- Concluído
- Falha



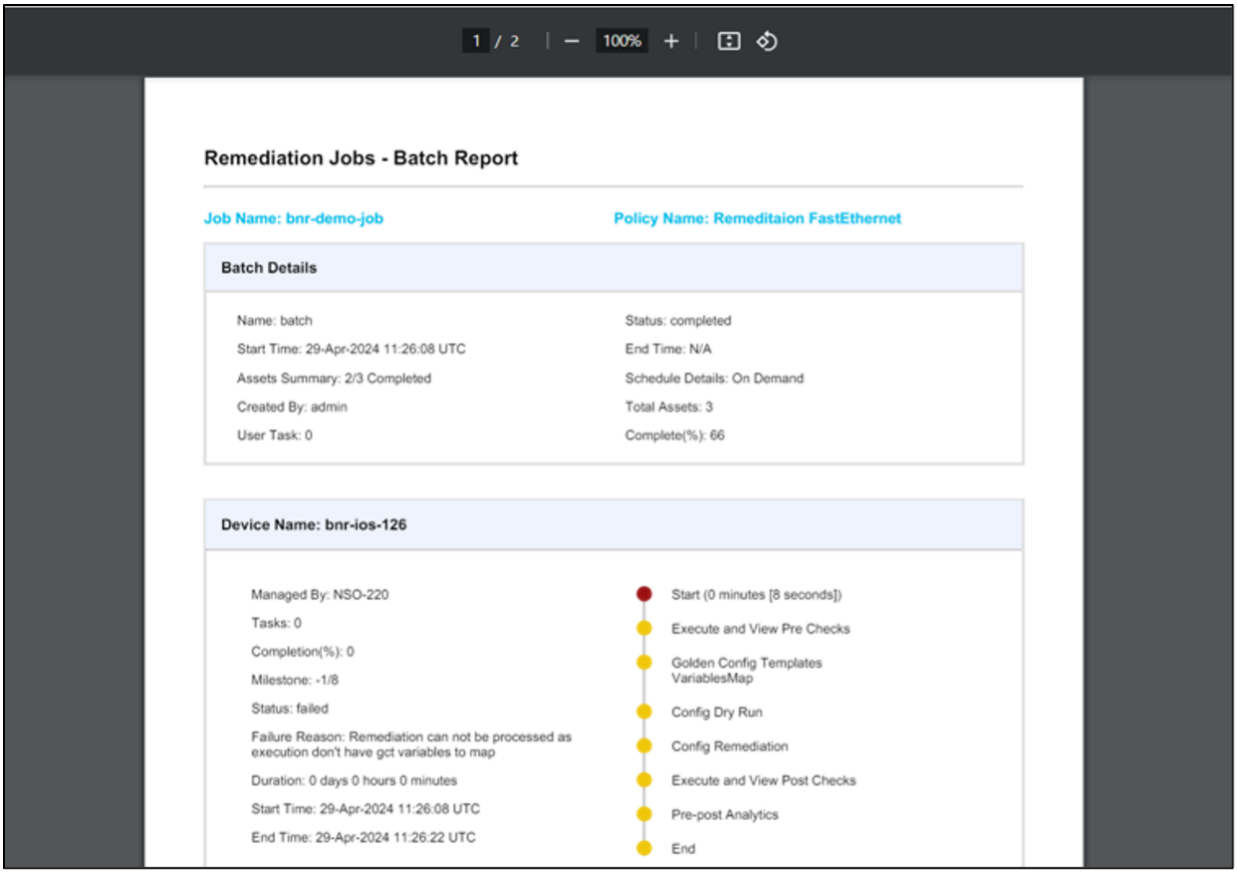
Execução da Correção: Detalhes da Etapa Embutida

Execução da Correção: Geração e download de relatórios PDF resumidos do lote

Os resumos de lote podem ser gerados e baixados.

Para fazer download do relatório resumido como um PDF por lote:

1. Selecione o ícone Mais Opções > Gerar Relatório. O sistema verifica internamente se o relatório está pronto. Quando o relatório estiver pronto, a opção Download Report estará ativada.
2. Selecione o ícone Mais Opções > Download do Relatório. O PDF é baixado.



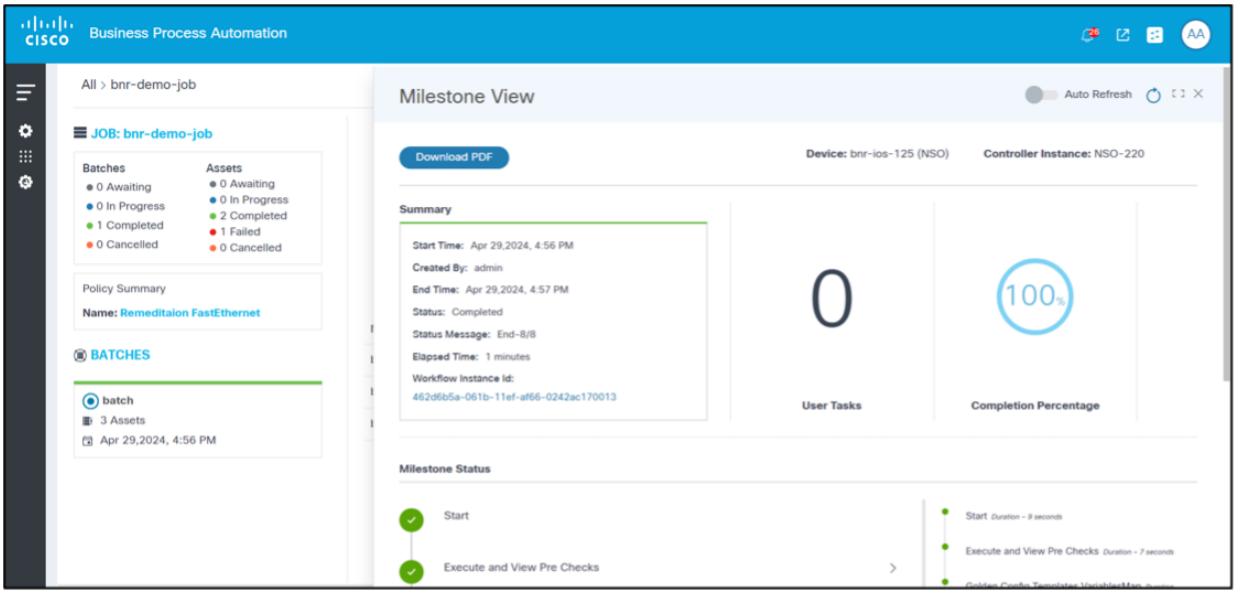
Relatório resumido de lote PDF

O Relatório de Lote de Trabalhos de Correção contém uma seção Detalhes do Lote, que fornece um resumo do lote de correção, como nome do trabalho, nome do lote, hora de início e término, total de ativos e status geral. Isso é seguido por uma seção de detalhes do dispositivo (uma seção por dispositivo) que inclui o nome do dispositivo, o status de remediação específico do dispositivo, o cronograma, a duração e a lista de marcos e o status.

Execução da Correção: Detalhes do dispositivo

Para exibir detalhes do dispositivo para marcos, selecione a página Detalhes do dispositivo. A página View de Etapa do Projeto é exibida.

Um resumo da correção para o dispositivo dado com um status de etapa detalhado é exibido, incluindo a saída do comando das principais etapas concluídas. Por exemplo, as saídas do comando de modelo de processo, a saída de execução a seco do GCT e o conteúdo da saída de diferença de análise podem ser exibidos.



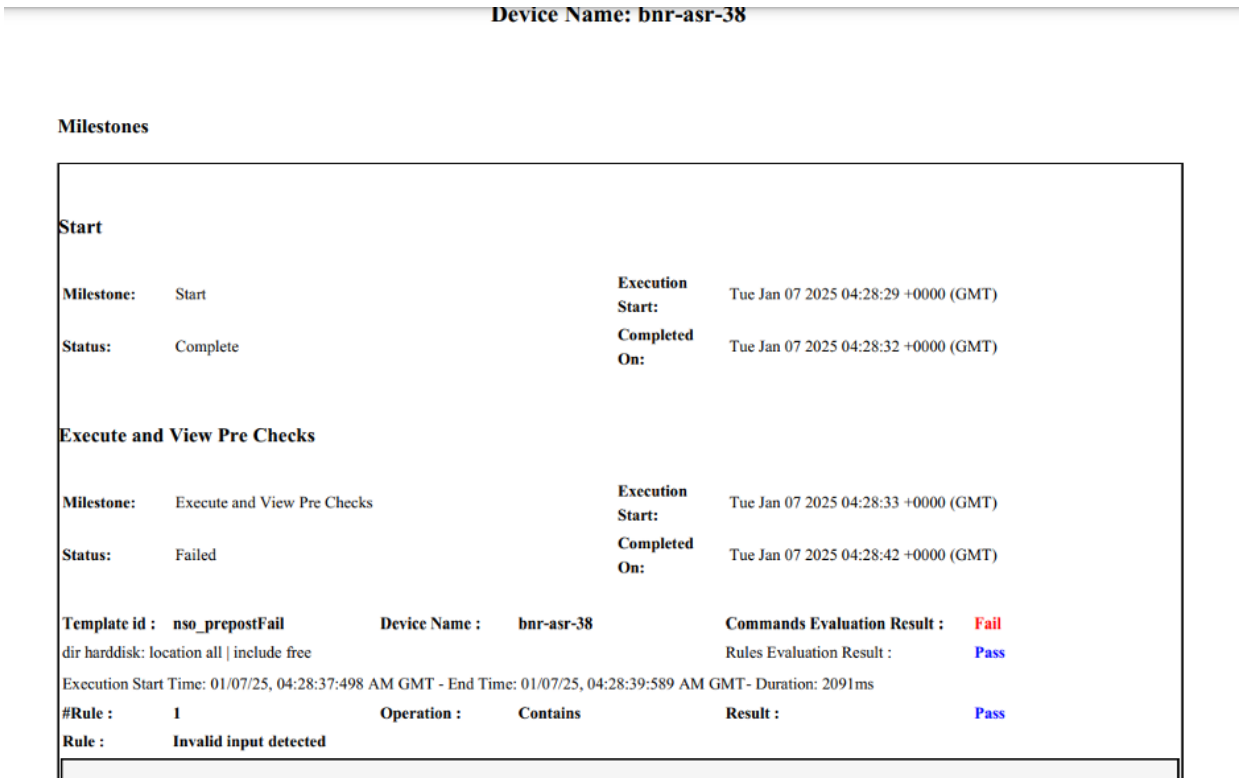
Execução da Correção: Exibição de Marco

Execução da Correção: Detalhes do dispositivo - Relatório de marco

Para exibir o relatório de etapas do projeto:

1. Selecione a página Device Details. A página View de Etapa do Projeto é exibida.
2. Clique em Download de PDF. O Relatório de exibição de etapas do projeto é gerado e baixado como mostrado abaixo.

Este relatório fornece detalhes de marco mais elaborados e conteúdo correspondente para a correção de dispositivo selecionada.



Device Name: bnr-asr-38

Milestones

Start

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

Execute and View Pre Checks

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

Template id : **nso_prepostFail** **Device Name :** **bnr-asr-38** **Commands Evaluation Result :** **Fail**

dir harddisk: location all | include free Rules Evaluation Result : **Pass**

Execution Start Time: 01/07/25, 04:28:37:498 AM GMT - End Time: 01/07/25, 04:28:39:589 AM GMT- Duration: 2091ms

#Rule : **1** **Operation :** **Contains** **Result :** **Pass**

Rule : **Invalid input detected**

Execução da Correção: Detalhes do dispositivo - Relatório em PDF do Milestone View

Configuração: Blocos e regras

Funcionalidade dos blocos

Os blocos de configuração são elementos essenciais para criar e aplicar políticas de conformidade em sistemas de gerenciamento de rede. Eles representam configurações de CLI de dispositivo, como aquelas para interfaces, Border Gateway Protocol (BGP) do roteador e muito mais. A seguir estão os principais recursos dos blocos de configuração:

- Modularidade: Os blocos de configuração permitem a criação de políticas modulares, permitindo que os administradores definam e gerenciem seções separadas de configurações de dispositivos de forma independente. Essa modularidade simplifica o processo de atualização e manutenção das políticas de conformidade.
- Granularidade: Ao dividir as configurações de dispositivos em partes menores e gerenciáveis, os administradores podem executar verificações de conformidade precisas e aplicar padrões específicos. Isso garante que cada parte da configuração do dispositivo siga as políticas necessárias.
- Reutilização: Uma vez definidos, os blocos de configuração podem ser reutilizados em várias políticas e dispositivos de conformidade. Essa capacidade de reutilização reduz a redundância e garante a consistência no gerenciamento da configuração.
- Bloco de configuração estática: Um bloco de configuração estática representa a configuração do dispositivo bruto sem nenhuma variável.

Exemplo: O bloco a seguir pode ser usado para executar uma verificação de conformidade na interface TwentyFiveGigE0/0/0/31

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

- Bloco de configuração dinâmica: Um bloco de configuração dinâmica representa a configuração do dispositivo que inclui variáveis que permitem mais adaptáveis e reutilizáveis. Esses blocos funcionam como um modelo TTP, aplicando-se às configurações do dispositivo e buscando os valores das variáveis. As condições podem ser adicionadas às regras para validar essas variáveis. Consulte https://ttp.readthedocs.io/en/latest/Overview.html para obter mais detalhes sobre TTP.

  Exemplo: O bloco a seguir pode ser usado para executar uma verificação de conformidade em todas as interfaces TwentyFiveGigE

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

Bloco de Configuração Dinâmica com Sub-Hierarquias: Esse bloco funciona como um bloco de configuração dinâmica e é usado para recuperar valores de configurações de dispositivo que têm várias hierarquias.

Exemplo: O exemplo a seguir demonstra uma configuração de dispositivo e o bloco dinâmico correspondente usado para recuperar valores de uma estrutura hierárquica.

Configuração do dispositivo que tem estrutura hierárquica:

```
router bgp 12.34
address-family ipv4 unicast
  router-id 1.1.1.X
!
vrf CT2S2
  rd 102:103
  !
  neighbor 10.1.102.XXX
  remote-as 102.XXX
  address-family ipv4 unicast
```

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

Dynamic Block Configuration para analisar a configuração acima.

```
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
```

Funcionalidade das regras

As regras permitem que os usuários definam condições para validar em relação às variáveis presentes em um bloco de configuração. Como parte de uma execução, o mecanismo de conformidade analisa a configuração do dispositivo, localiza instâncias correspondentes de instâncias de bloco do dispositivo, lê valores fora das linhas e executa condições definidas nas regras em relação aos valores. O resultado, quer as linhas de configuração tenham alguma violação ou não, é armazenado para exibição no painel.

As regras de configuração agora fazem parte do ciclo de vida de criação de blocos. Portanto, não há uma página separada para exibir regras. As regras podem ser listadas, criadas e atualizadas na página de criação ou atualização de bloco correspondente.

Na estrutura da CnR, as regras desempenham um papel crucial na validação de configurações em relação a condições específicas. Esta seção fornece uma visão geral de como as regras são integradas e gerenciadas no sistema.

- Propósito: As regras permitem que os usuários definam condições usadas para validar variáveis presentes em um bloco de configuração
- Processo de execução:
  - O mecanismo de conformidade analisa a configuração do dispositivo
  - Identifica instâncias correspondentes de instâncias de bloqueio de dispositivo
  - Extrai valores das linhas de configuração
  - Aplica as condições definidas nas regras a esses valores
  - Os resultados que indicam violações são armazenados e exibidos no painel

Integração com o ciclo de vida do bloco

- Integração do ciclo de vida: As regras de configuração agora são parte integrante do ciclo de vida de criação de blocos
- Gerenciamento:
    - As regras são listadas, criadas e atualizadas diretamente nas páginas usadas para a criação de blocos ou atualizações
    - Não há uma página separada dedicada à visualização de regras, otimizando seu gerenciamento dentro do ciclo de vida do bloco

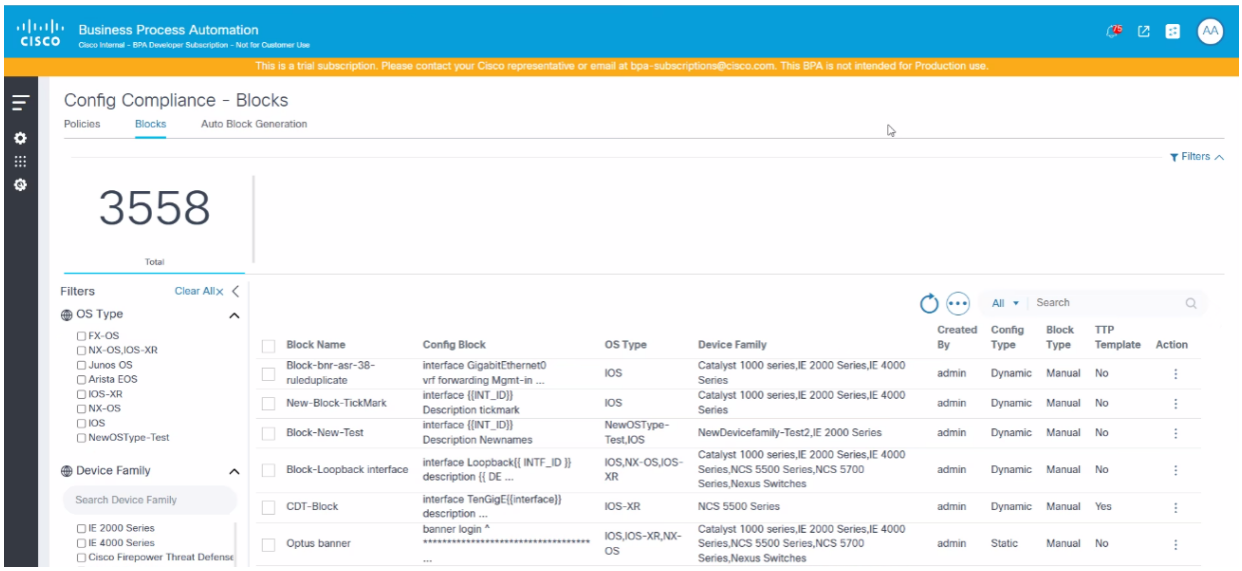
Essa integração garante que as verificações de conformidade sejam incorporadas perfeitamente ao processo de gerenciamento de configuração, permitindo o monitoramento e o gerenciamento eficientes de configurações de dispositivos em relação a regras predefinidas.

Blocos de Lista

A página Blocos lista todos os blocos de configuração e fornece ações para gerar, adicionar, editar, excluir, importar e exportar blocos. Os usuários podem filtrar, classificar e exibir detalhes de bloqueio.

Detalhes do Bloco de Recursos

- Contagem total: Exibe o número total de blocos criados
- Opções de filtro:
    - Tipos de SO e família de dispositivos: Permite que os usuários filtrem blocos com base nos critérios selecionados
- Grade Principal:
    - Exibe uma lista padrão de blocos
    - Os usuários podem classificar a lista clicando nos cabeçalhos das colunas
    - Inclui um recurso de pesquisa que permite aos usuários pesquisar por todos os atributos ou especificamente por Nome do bloco
    - Oferece suporte à paginação para facilitar a navegação na lista
- Ações:
    - Editar: Os usuários podem modificar blocos existentes
    - DELETE: Os usuários podem remover blocos da lista



Lista de Blocos de Configuração

Adição ou Edição de Blocos e Regras

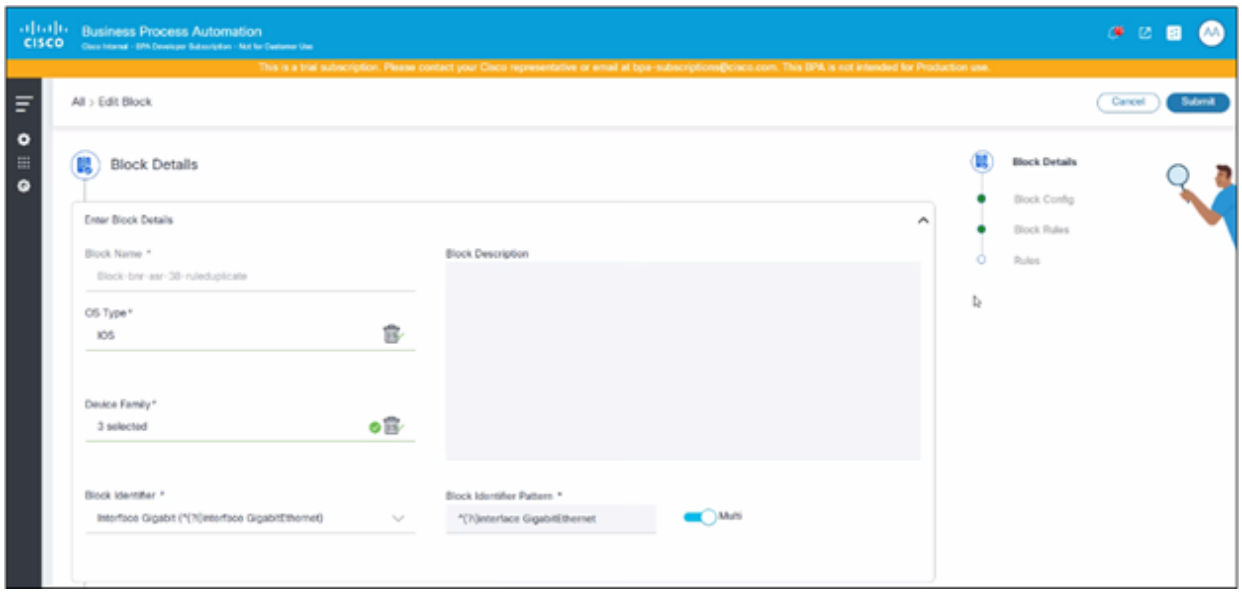
A página Adicionar ou Editar Bloco foi projetada para capturar e gerenciar informações essenciais relacionadas aos blocos. Esta página destaca as seguintes seções:

- Detalhes Básicos de Bloco:

  A seção Detalhes Básicos inclui:

  - Nome do bloco: Nome designado para o bloco
  - Descrição: Uma breve visão geral ou explicação do objetivo ou da funcionalidade do bloco
  - Tipo de SO: Tipo de sistema operacional associado ao bloco
  - Família de dispositivos: Categoria ou grupo de dispositivos compatíveis com o bloco
  - Seleção de identificador de bloco: Opções para selecionar um identificador exclusivo para o bloco
  - Adicionar ou editar detalhes do identificador de bloco: Se não houver um identificador de bloco adequado, os usuários poderão usar os mesmos campos para adicionar ou editar os seguintes detalhes do identificador de bloco:

    - Nome do identificador de bloco: O nome específico dado ao identificador de bloco
    - Padrão: O padrão ou formato que o identificador de bloco segue
    - Múltiplo: Alternar para indicar se o bloco de configuração deve ser tratado como uma configuração de várias linhas

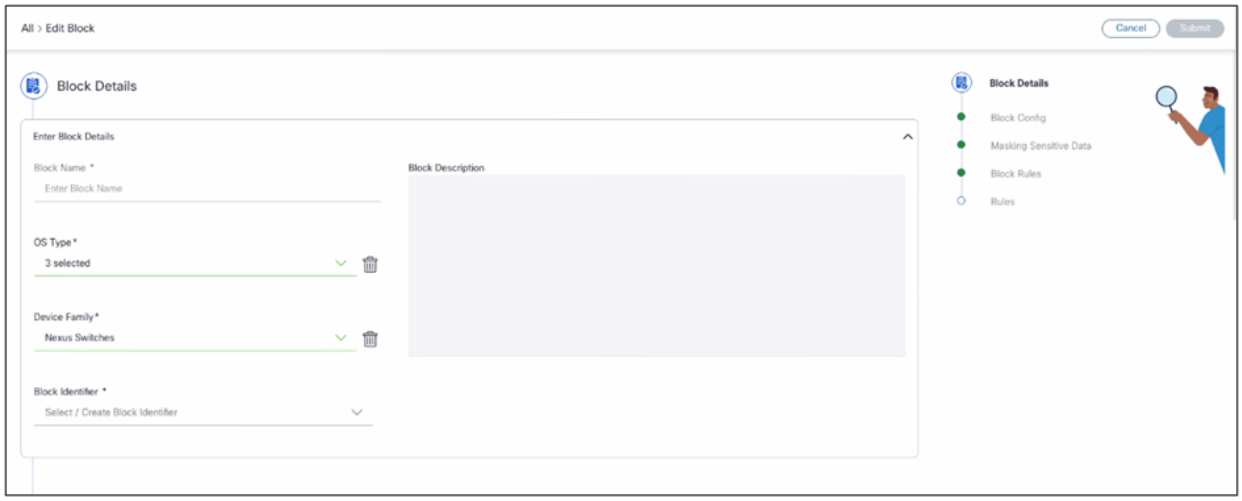


Adicionar ou Editar Blocos - Detalhes do Bloqueio

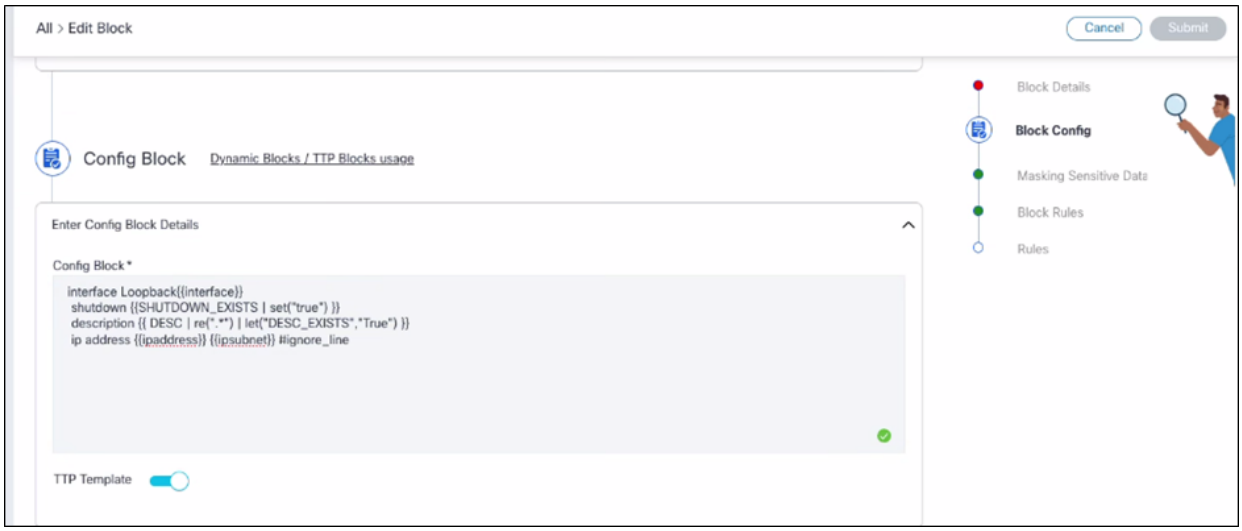
- Bloquear configuração:

A seção Block Config inclui:

- Bloco de configuração: Representa a configuração de um dispositivo, incorporando diferentes variáveis. Essa configuração descreve como o dispositivo deve ser configurado e gerenciado no sistema.
- Modelo HTTP: Indica se o bloco é designado como um Modelo de protocolo de transformação de modelo (TTP - Template Transformation Protocol), ajudando a identificar os blocos usados como modelos para transformar ou padronizar configurações entre dispositivos.



Detalhes do Bloco



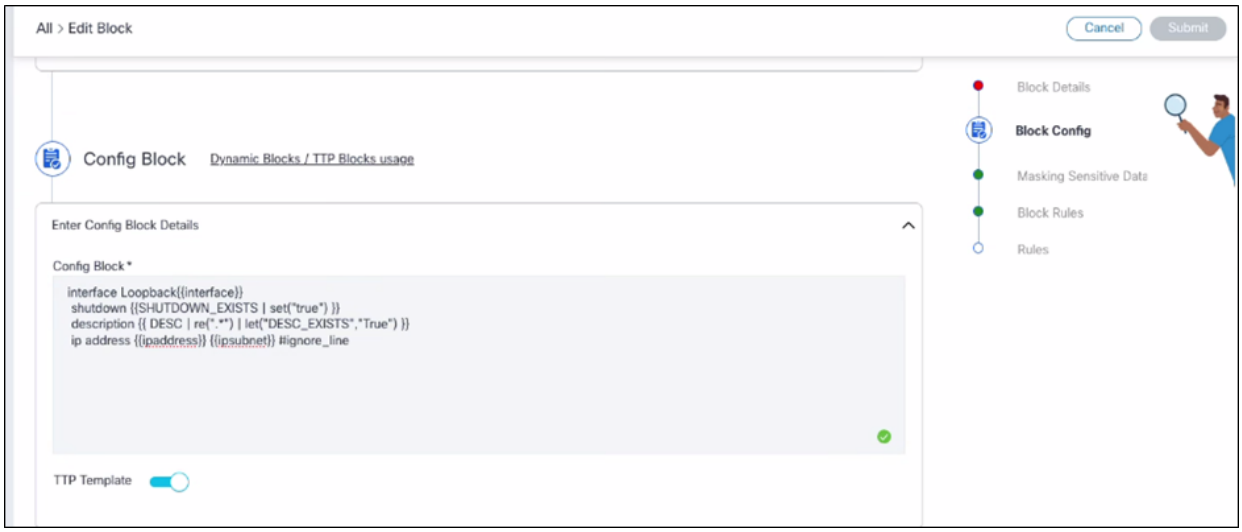
Bloquear configuração

Usando a sintaxe Ignorar linha

A sintaxe Ignorar linha permite que os usuários adicionem um comentário ao final de uma linha de configuração específica em um bloco para instruir o sistema a ignorar qualquer verificação de conformidade ou violação nessa linha. Isso evita que a linha apareça como uma violação em relatórios ou no painel.

Conclua as seguintes etapas para usar Ignorar sintaxe de linha:

1. Localize a linha de configuração a ser excluída das verificações de conformidade (por exemplo, endereço IP).



Ignorar Sintaxe de Linha

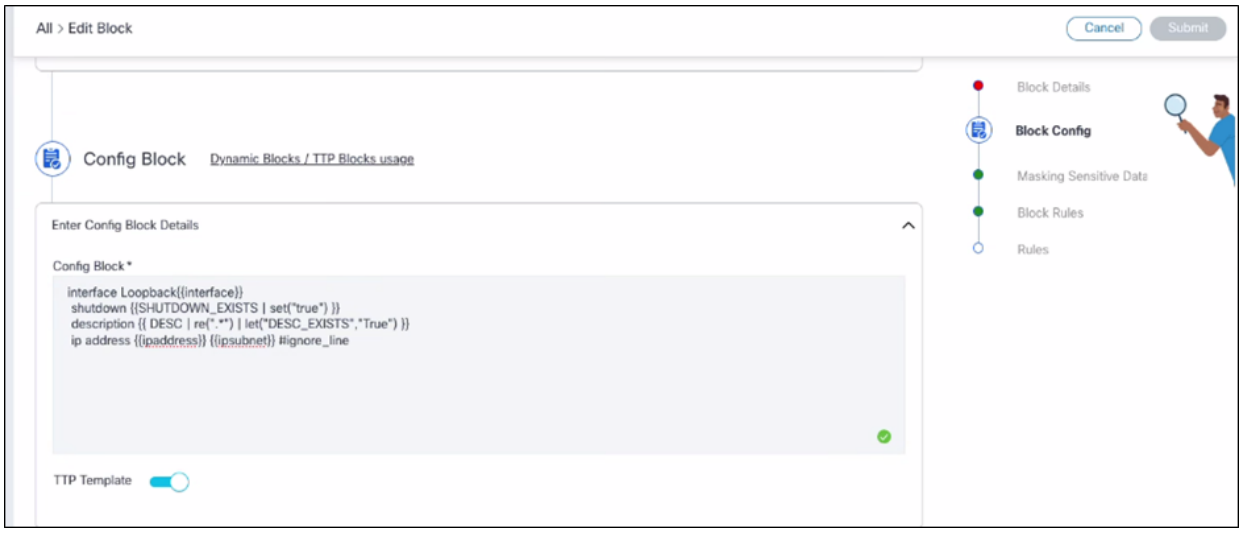
2. Acrescente a linha usando a sintaxe de comentário "#ignore_line" no final da linha. Exemplo: endereço ip {{ipAddress}} {{ipSubnet}} #ignore_line

Aumentando a violação

Esta funcionalidade do Analisador de Texto de Modelo (TTP) na configuração de bloco pode ser usada para indicar se uma violação deve ser gerada se uma linha específica existir.

Conclua as seguintes etapas para usar a funcionalidade TTP:

1. Na seção Block Config da página block create or edit, localize a linha de configuração a ser controlada.
2. Defina uma variável TTP usando o comando set ou let da seguinte maneira:
   - Se o desligamento da linha de configuração existir, use o comando set para definir uma variável da seguinte maneira:
     fechamento | {{SHUTDOWN_FLAG | set("true")}}"
   - Se os usuários tiverem uma variável existente na linha de configuração como descrição {{DESC}}, use o comando let da seguinte forma:
     descrição {{ DESC | re(".*") | let("DESC_EXISTS", "True") }}
3. Use essas variáveis (SHUTDOWN_FLAG ou DESC_EXISTS no exemplo acima) em uma regra para acionar violações.



Gerar violações

Efeito:

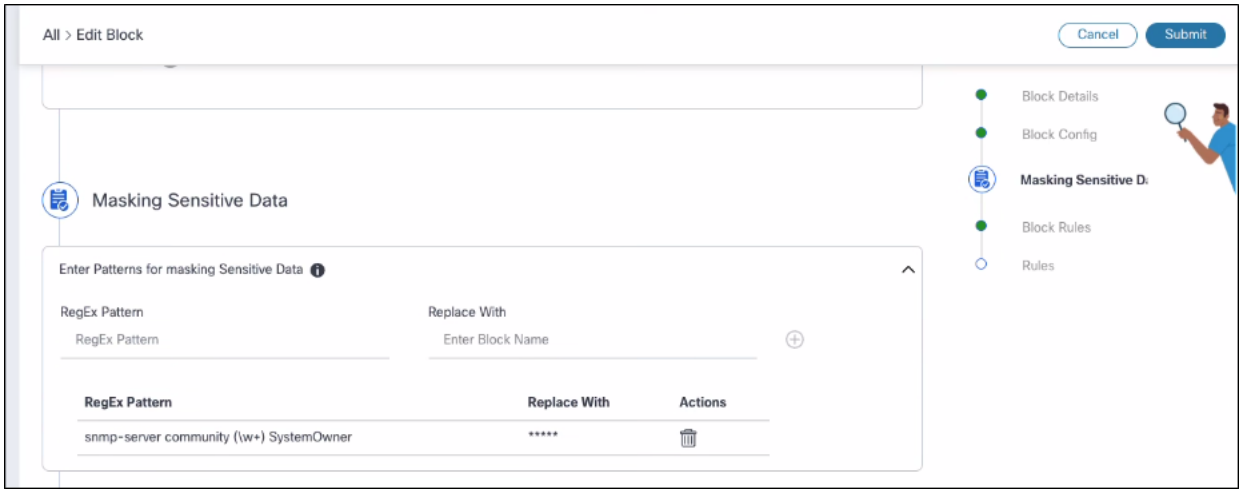
Uma violação será exibida na página do painel de controle se as linhas "shutdown" ou "description config" estiverem disponíveis na configuração do dispositivo. A gravidade da violação depende da seleção feita na criação da regra.

- Dados confidenciais da máscara:

Os dados confidenciais de máscara são um recurso que permite aos usuários definir padrões usando expressões regulares para identificar e mascarar informações confidenciais (como senhas ou chaves) em configurações de dispositivos. Isso evita que dados confidenciais sejam exibidos em exibições de violação ou em diferenças de configuração de correção substituindo os dados correspondentes por uma máscara especificada (por exemplo, "***").

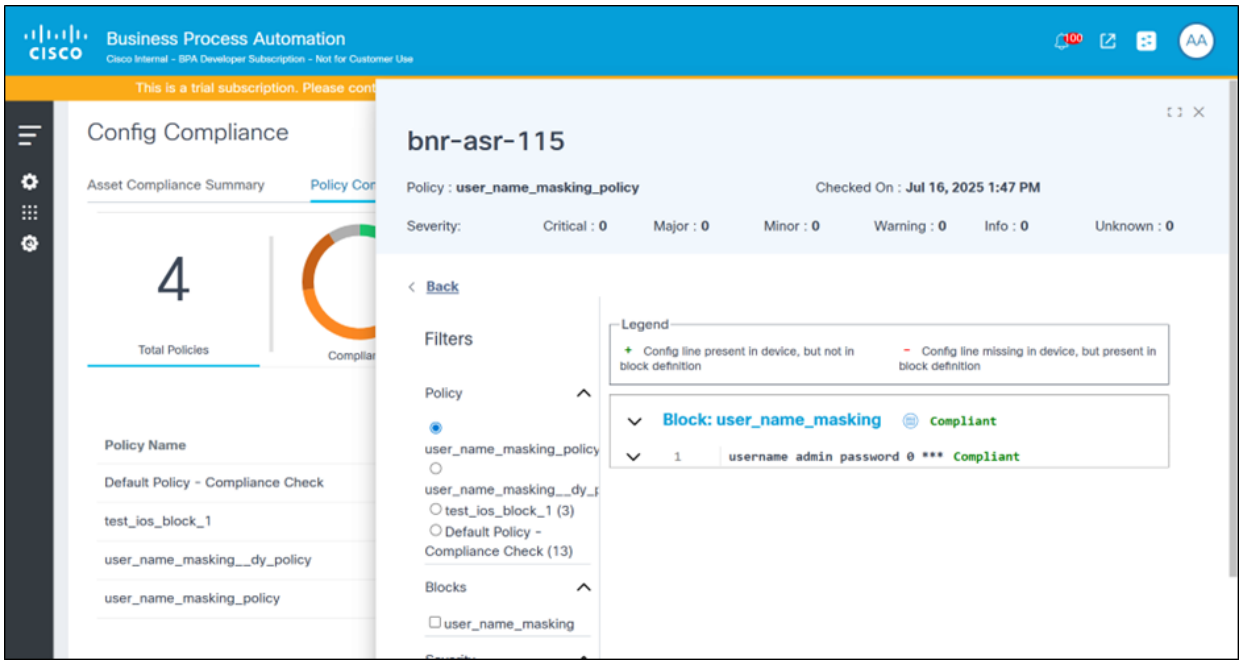
Para mascarar os dados confidenciais, faça o seguinte:

1. Na seção Dados Confidenciais da Máscara:
    - Adicionar vários padrões de expressão regular (regex) para identificar dados confidenciais
    - Especifique a string de substituição para mascarar os dados correspondentes (por exemplo, ""). Por exemplo, o padrão Regex pode ser preenchido com uma senha (para corresponder qualquer texto que comece com "senha" seguido por uma palavra) e a substituição deve ser .
2. Adicione quantos padrões regex forem necessários; eles são exibidos em um formato de grade



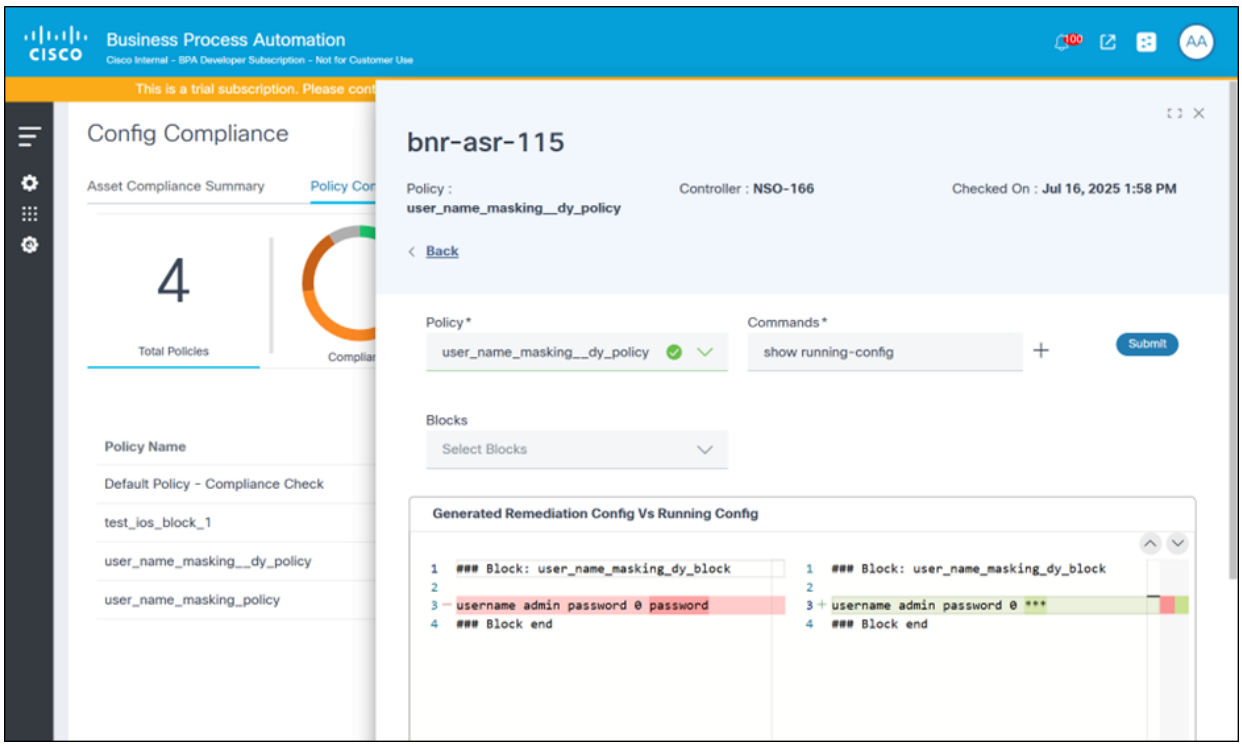
Mascarar Dados Confidenciais

3. Exclua qualquer padrão da lista se não for mais necessário.
4. O sistema usa as expressões regulares para localizar dados de configuração de dispositivo sensíveis correspondentes e substituí-los pela máscara especificada (por exemplo, "***"). Essa máscara é usada nas seguintes páginas:
    - Painel de Controle de Conformidade > Ativos Afetados > Página Exibir violações: Os dados de configuração exibidos na interface do usuário, bem como o relatório de conformidade de ativos gerado com base nesses detalhes de violação



Mascarar dados confidenciais na página Exibir violações

- Painel de Controle de Conformidade > Exibir Configuração de Correção > Página Exibir Diferença de Correção: Os dados de configuração do dispositivo exibem dados confidenciais mascarados de acordo com as configurações de máscara do bloco

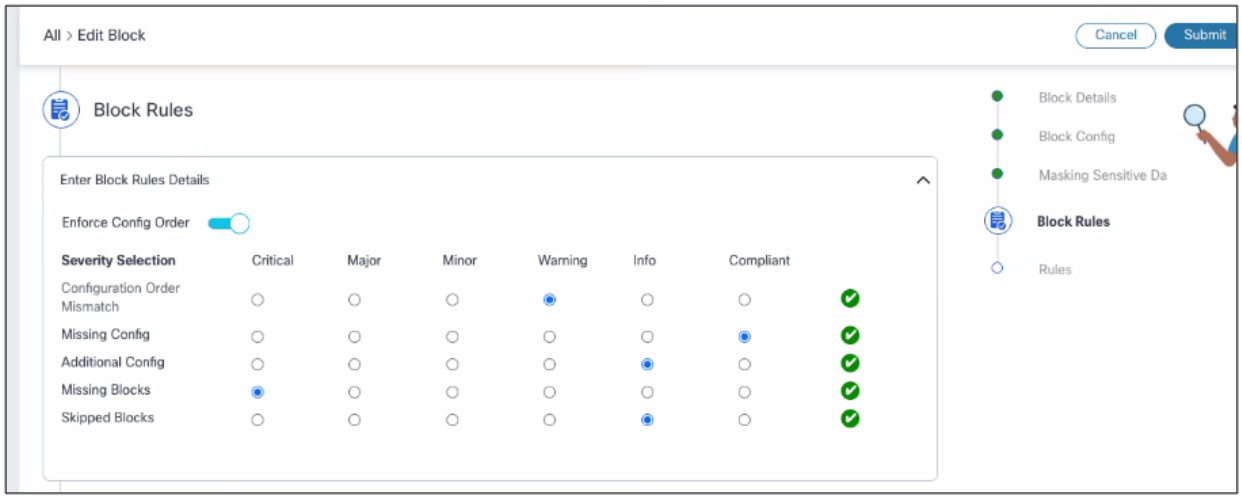


Mascarar dados confidenciais na página de comparação de remediação

- Regras de bloqueio (seleção de severidade):

  A seção Regras de bloqueio inclui:

- Aplicar pedido de configuração: Garante que as linhas de configuração sejam exibidas na ordem correta durante as verificações de conformidade. O mecanismo de conformidade verifica a sequência de linhas de configuração em relação à ordem esperada.
- Seleção de severidade: Permite que os usuários designem um nível de gravidade para violações dentro de um bloco. Os níveis de gravidade ajudam a priorizar e gerenciar problemas de conformidade com eficiência.
- Incompatibilidade do pedido de configuração: Identifica discrepâncias na ordem das linhas de configuração e emite alertas quando a sequência das linhas de configuração do dispositivo não corresponde à ordem esperada.
- Configuração Ausente:
  - Detecta linhas de configuração ausentes
  - Destaca as linhas de configuração esperadas que estão ausentes na configuração do dispositivo
  - Verifica se o bloco de configuração de dispositivo inteiro está ausente ou não corresponde à configuração de bloco definida
- Configuração adicional:
  - Identifica linhas de configuração inesperadas
  - Exibe as linhas de configuração presentes na configuração do dispositivo, mas não esperadas de acordo com a configuração do bloco
- Blocos ignorados:
  - Indica blocos de configuração que não estão verificados
  - O bloco será ignorado se não atender às condições de filtro especificadas



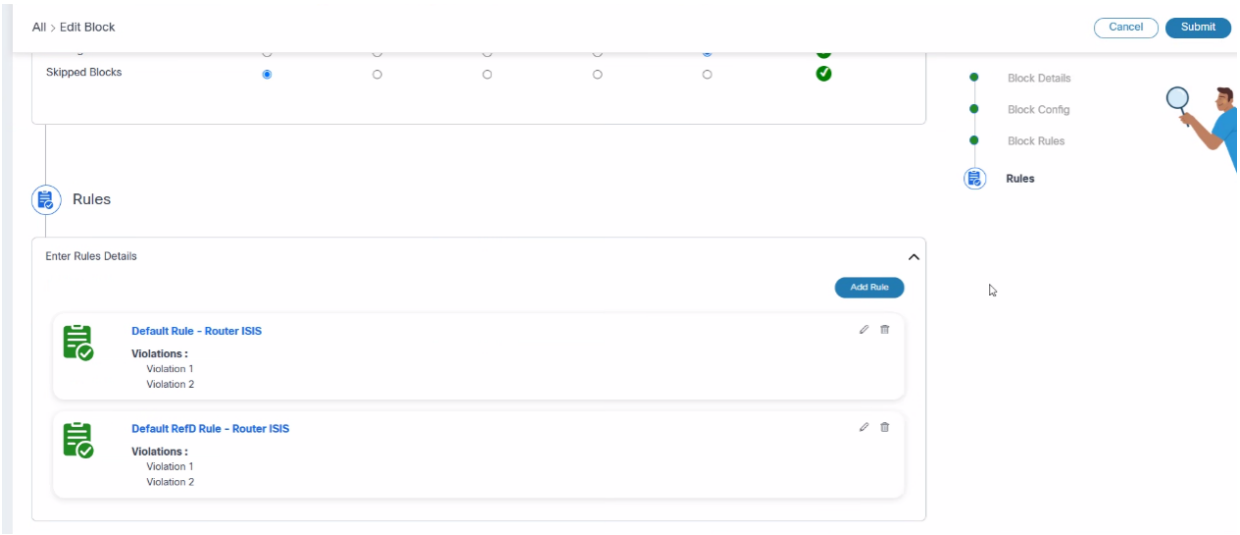
Adicionar ou editar blocos-regras de bloqueio

Gerenciamento de regras

Na estrutura do CnR, os usuários podem gerenciar regras de bloqueio por meio da interface "Adicionar ou editar blocos". Essa funcionalidade é estruturada conforme mostrado na seção abaixo:

Note: Se um usuário não quiser elevar uma violação específica de nível de bloco, o nível de gravidade "Compatível" pode ser selecionado.

- Configuração de regras:
  - Os usuários podem definir e gerenciar regras que o mecanismo de conformidade usa para validar configurações
  - Os usuários podem criar, editar ou excluir regras conforme necessário
- Lista de regras:
  - Fornece uma lista abrangente de todas as regras criadas, oferecendo visibilidade de seus detalhes
  - Os usuários podem editar regras existentes ou excluir as regras que não são mais necessárias



Adicionando e editando blocos de configuração

Adição ou Edição de Detalhes da Regra

- Nome da regra:
  - Atribuir um nome exclusivo à regra para identificação
  - Este campo é obrigatório para garantir que cada regra possa ser reconhecida distintamente
- Regra padrão:
  - Especificar se a regra deve ser definida como padrão
  - Os usuários podem habilitar essa configuração para tornar a regra um padrão na estrutura de conformidade
- Descrição:
  - Fornece contexto ou informações adicionais sobre a regra
  - Este campo é opcional, mas pode ser útil para documentação e clareza
- Violações:
  - Gerenciar a lista de violações associadas à regra

- Os usuários podem adicionar, editar ou excluir violações conforme necessário

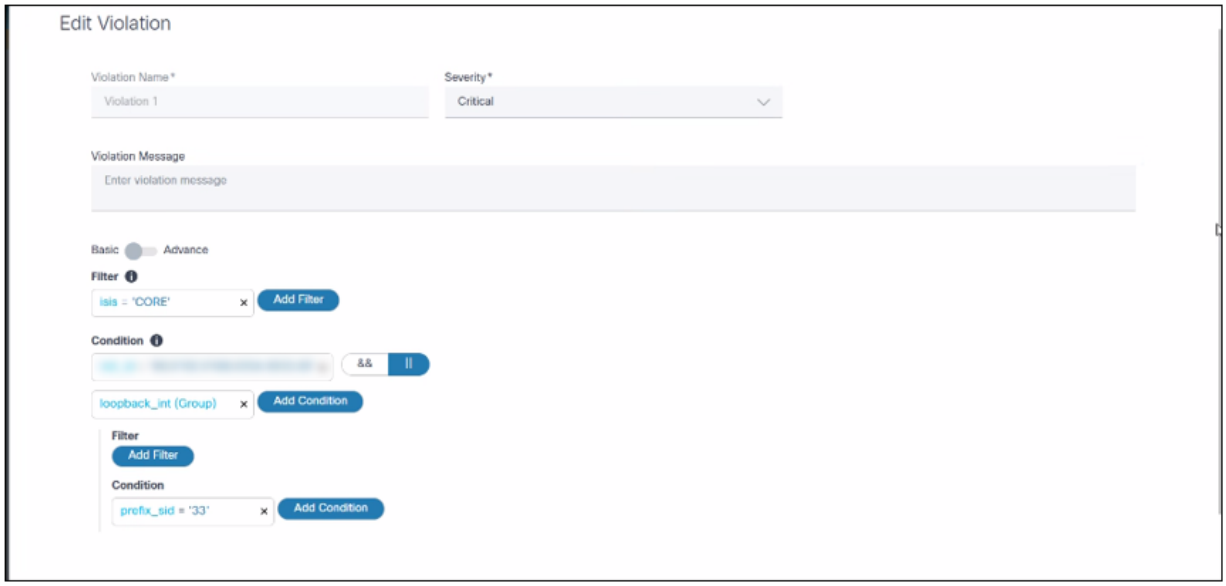
	A	B	C	D	E	F	G	H	I	J	K
1	Device Name	Managed By	Product Family	Compliance	Critical	Major	Minor	Warning	Info	Unknown	Last Checked
2	CNC-bnr-asr-78	Direct-To-Device	IE 2000 Series	Non Compliant	1	0	0	0	0	0	04-Aug-25
3	D2d-118	Direct-To-Device	IE 2000 Series	Partially Compliant	0	1	0	1	1	0	04-Aug-25
4	D2d-juniper	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											

Adicionar ou editar blocos-regras: Adicionar ou Editar Regra

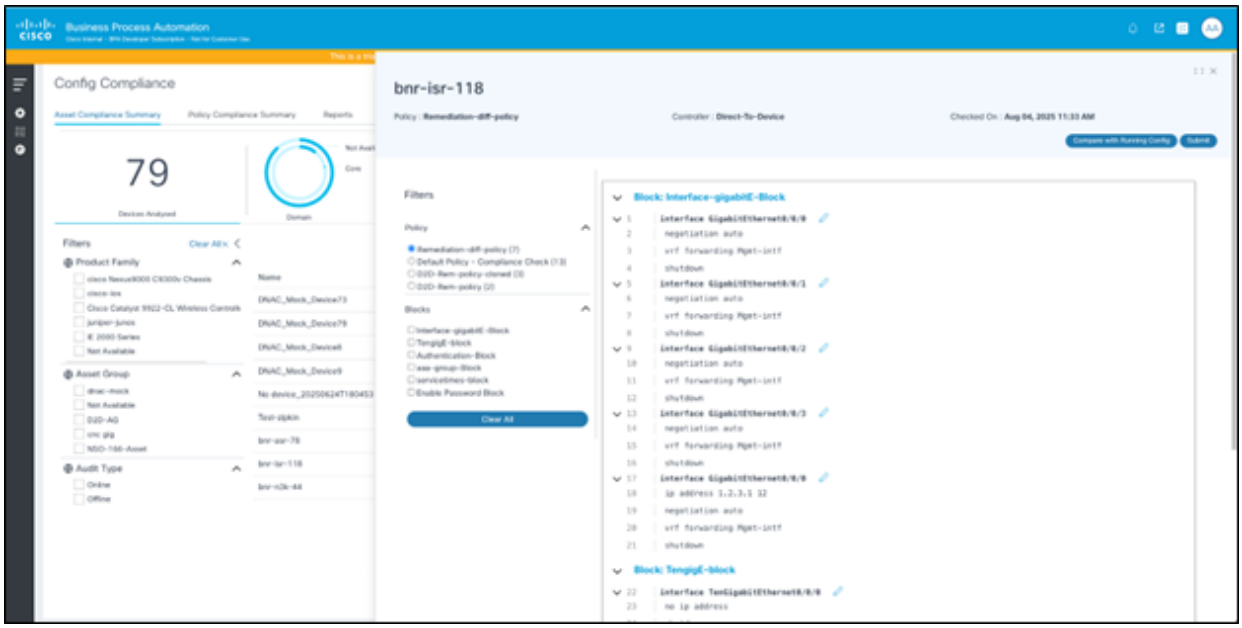
Adição ou Edição de Violações de Regra

As violações de regra são um componente crítico na execução da conformidade, detalhando as verificações específicas que precisam ser executadas. A seguir, uma visão geral de como as violações de regra podem ser criadas e gerenciadas:

- Modo Básico:
  - Elementos da interface do usuário: Esse modo permite que os usuários criem violações de regra usando uma Interface Gráfica do Usuário (GUI). Essa abordagem é normalmente mais fácil de usar e acessível para aqueles que preferem não se envolver com a codificação.
  - Orientação passo a passo: Os usuários são orientados pelo processo de definição de verificações usando elementos de UI predefinidos.
- Modo avançado:
  - Formato de código do tipo JSON: Para usuários que se sentem à vontade com a codificação, este modo permite a criação de violações de regras, digitando-as em um formato estruturado semelhante a JSON.
  - Flexibilidade e precisão: Esse método fornece maior flexibilidade e precisão para definir verificações de regras complexas.



Criar ou Editar Violações de Regra - Modo Básico



Criar ou Editar Violações de Regra - Modo Avançado

As violações de regra têm as seguintes seções:

- Nome da violação: Nome da violação
- Severity: Define a severidade de conformidade se essa violação falhar durante uma execução
- Mensagem de violação: A mensagem é exibida quando uma verificação de violação falha
- Critérios de filtragem de violação: Aplica as condições de violação em que variáveis de esquema que não são de grupo podem ser usadas
  - Utilizado nos critérios de filtragem para definir condições com base em elementos de dados individuais que não fazem parte de um grupo
  - Permite que os usuários selecionem critérios de acordo com a hierarquia e a estrutura

dos dados, garantindo uma filtragem precisa e relevante

- Condições das regras: Condições reais para verificar a conformidade aqui as variáveis de esquema de grupo e não grupo podem ser usadas
  - Ambos os tipos de variáveis são empregados em regras para criar condições abrangentes
  - Variáveis de grupo: Permitir a aplicação de condições às recolhas de dados conexos, assegurando controlos exaustivos no âmbito de grupos estruturados
  - Variáveis Não-Grupo: Permitir a aplicação de condições a elementos de dados independentes, proporcionando flexibilidade na aplicação de regras

Blocos dinâmicos definidos pelo usuário - Práticas recomendadas

- Certifique-se de que os nomes de variáveis sejam exclusivos em cada bloco.
- Evite usar variáveis em nomes de grupos.
- Para configurações de sub-hierarquia, use "<group>" em blocos.

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

- Para capturar valores para linhas de configuração semelhantes em uma única variável, use a variável da seguinte forma: `{{ <<var-name>> | linha | joinmatches(',') }}`. Coloque a linha de configuração dentro de `{{ start }}` e `{ end }}` conforme demonstrado no exemplo a seguir:

Configuração do dispositivo	Bloquear configuração
ip domain list vrf Mgmt-intf core.cisco.com ip domain list cisco.com ip domain list east.cisco.com ip domain list west.cisco.com	{{_start_}} ip domain list {{ domains | _linha_ | joinmatches(‘,’) }} {{ _end_ }} ip domain list vrf {{ vrf_name }} {{ vrf_domain }}

- Para capturar um valor que contém espaços de uma linha de configuração, use a variável no bloco como mostrado na tabela abaixo: `{{ <<var-name>> | re(".*") }}`

Configuração do dispositivo	Bloquear configuração
interface HundredGigE0/0/1/31	interface {{ INTF_ID }}

Configuração do dispositivo	Bloquear configuração
description Interface : 12ylaa01 Hg0/0/1/31 mtu 9216	description {{ INTF_DESC | re(".*") }} mtu 9216

Noções Básicas sobre Hierarquia de Regras e Integração de RefD em Regras e Regras Não-RefD

No Dynamic Block TTP, há dois esquemas distintos que determinam como as configurações são estruturadas e validadas.

- Esquema Baseado em Grupo:
  - Este esquema organiza configurações de maneira hierárquica, estabelecendo um relacionamento pai-filho entre elementos
  - Ideal para configurações complexas em que os elementos são logicamente aninhados e inter-relacionados
  - As regras podem ser definidas para validar as relações hierárquicas e dependências entre diferentes elementos de configuração
- Esquema Não Baseado em Grupo:
  - As configurações são estruturadas em um formato simples, com todos os elementos existentes no mesmo nível sem relações hierárquicas
  - Adequado para configurações mais simples onde a hierarquia não é necessária
  - É possível definir regras para garantir que cada elemento de configuração atenda a critérios específicos

Integração de RefD

- Finalidade da referência:
  - Função: Serve como uma ferramenta para gerenciar variáveis locais e externas dentro da estrutura BPA
  - Funcionalidade:
    - Busca dinâmica: Facilita a recuperação e o gerenciamento dinâmicos de dados variáveis, permitindo que as verificações de conformidade se adaptem às alterações de dados em tempo real
    - Interação de API: Oferece APIs para casos de uso de BPA para acessar e gerenciar essas variáveis e valores dinâmicos, garantindo uma integração tranquila nos fluxos de trabalho de conformidade

Sintaxe dos Valores da Regra de Conformidade

O caso de uso CnR integra-se à estrutura de RefD para utilizar dados dinamicamente em

verificações de conformidade e fluxos de trabalho de correção. Uma análise detalhada de como essa integração funciona, focando particularmente na sintaxe e nos tipos de variáveis usadas, é mostrada abaixo:

- Palavra-chave: A sintaxe deve começar com "RefD"
- Parâmetros: O parâmetro "key" é obrigatório na sintaxe
- Exemplo:

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

Tipos de Variáveis

- Variáveis Definidas pelo Usuário:
  - Configurado durante a criação de trabalhos de conformidade.
  - Escopo: Aplicável a todas as execuções do job especificado
  - Sintaxe: `{$VarName}`
  - Exemplo: `{$SITE}`
- Variáveis do sistema
  - Predefinido pela estrutura com base nos dados de contexto disponíveis durante a execução
  - Atualmente, a estrutura fornece acesso ao objeto do dispositivo
  - Sintaxe: `{{#VarName}`
  - Examples:
    - `{{#device.deviceIdentifier}}` - Representa o identificador do dispositivo
    - `{{#device.additionalAttributes.serialNumber}}` - Representa o número de série do dispositivo
- Variáveis TTP
  - Presente na configuração de bloco
  - Sintaxe: `{{ VarName }}`
  - Exemplo: `{{ INT_ID }}`

Regras não RefD

- Essas regras são como regras RefD, mas não começam com a palavra-chave "RefD"
- Exemplo:

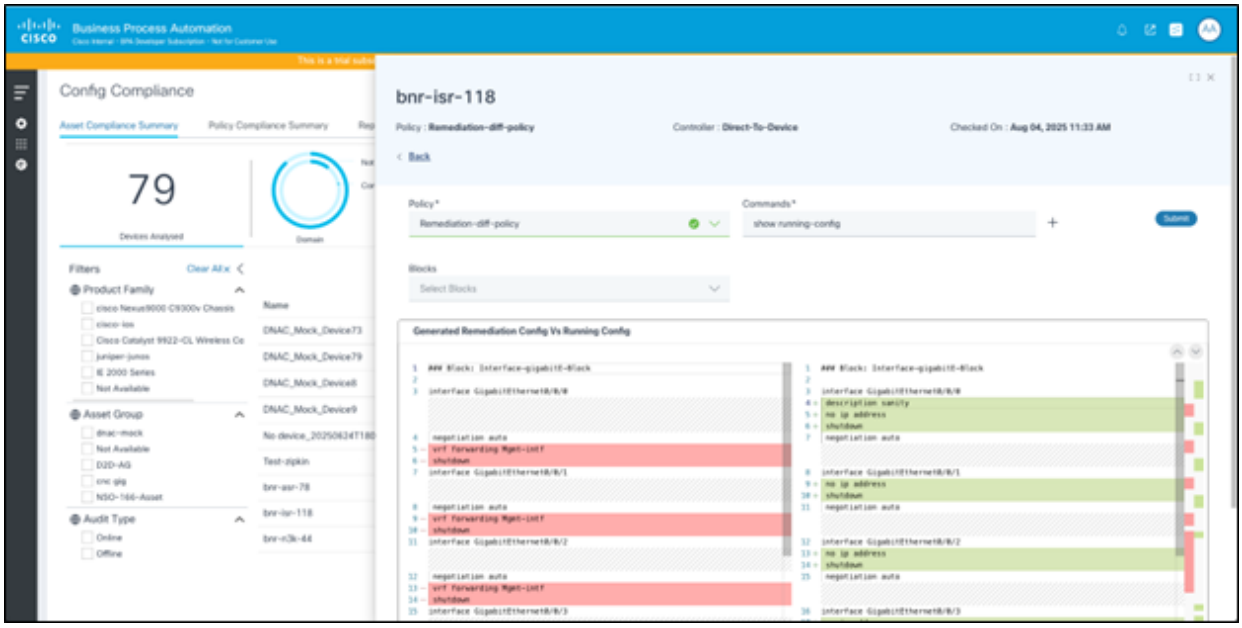
```
plaintext
Copy Code
{$int_id}.{{#device}}.{{ mtu_val }}
```

Uso Variável

- Variáveis Definidas pelo Usuário: Representado como `{$Var}`
- Variáveis do sistema: Representado como `{{#Var}}`, expondo atributos como deviceIdentifier, controllerId, controllerType etc.
- Variáveis TTP: Representado entre chaves duplas como `{{var}}`

Execução

- Durante a criação do trabalho, seus valores podem ser definidos se as variáveis $ forem especificadas
- Os valores combinados das variáveis são comparados com a configuração do dispositivo buscado para garantir a conformidade



Configuração do dispositivo:

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

Regras de configuração: RefD

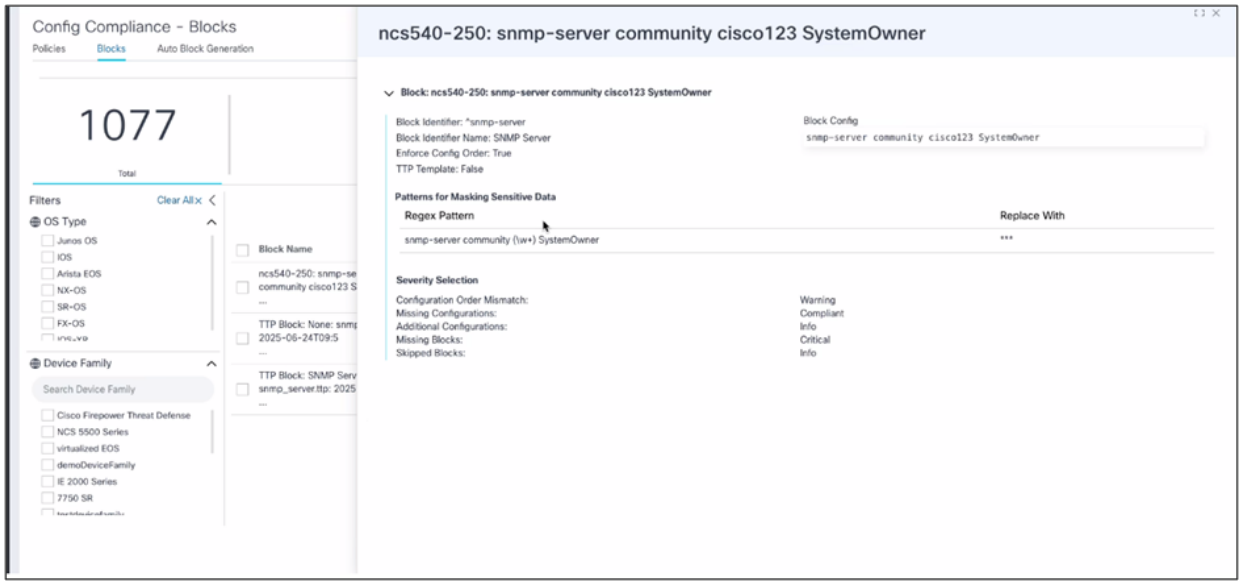
Exibindo detalhes do bloco

Para acessar detalhes do bloco:

1. Navegue até a página Blocos.
2. Selecione ou clique na linha na grade para exibir os detalhes do bloco específico.A página Detalhes do Bloco é exibida no lado direito da tela.

Note: Esta página fornece uma view somente para leitura de todas as informações relacionadas ao bloco, incluindo blocos associados, regras e violações.

Clicar em hiperlinks, se houver, nos detalhes redireciona os usuários para o bloco relevante ou informações relacionadas.



Exibição de Detalhes do Bloco

Excluindo blocos

O portal permite que os usuários excluam um ou mais blocos, desde que tenham as permissões RBAC apropriadas. Os usuários podem executar essas ações executando as seguintes etapas:

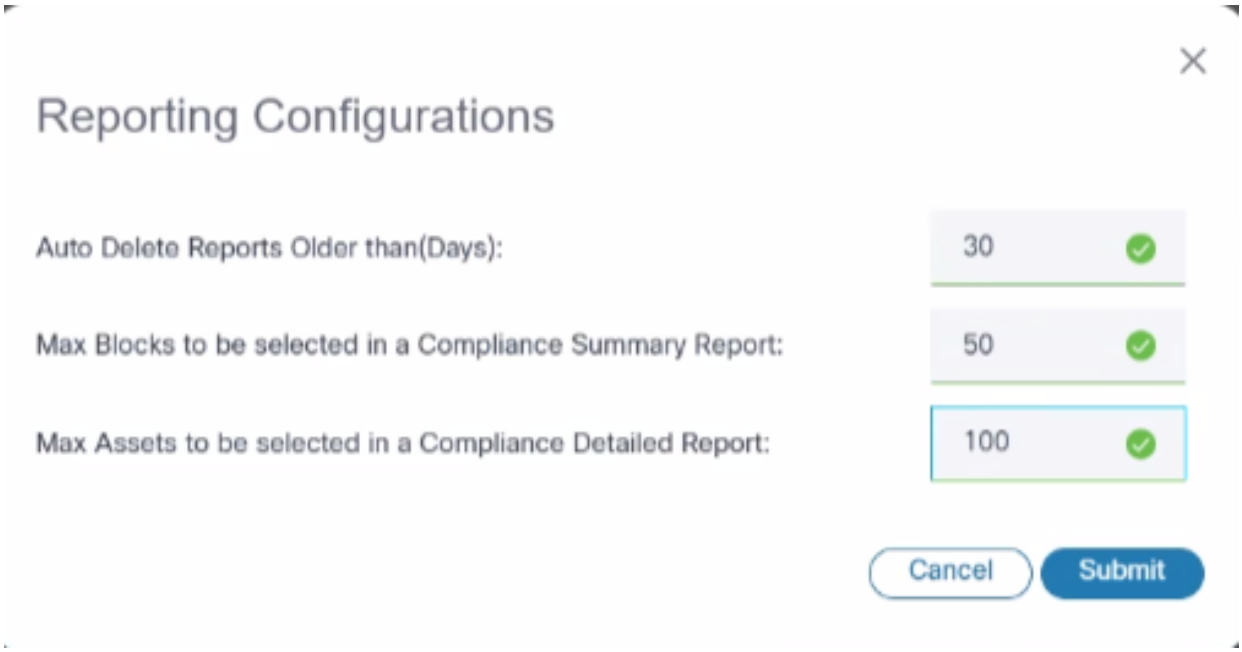
Para exclusão de bloco único:

1. Navegue até a página Blocos.

2. Clique no ícone Mais Opções ao lado do bloco a ser excluído.
3. Selecione a opção Excluir. Uma mensagem de confirmação é exibida.

Para exclusão de vários blocos:

1. Navegue até a página Blocos.
2. Marque as caixas de seleção ao lado de cada bloco a ser excluído.
3. Clique no ícone Mais Opções e selecione Excluir. Uma mensagem de confirmação.

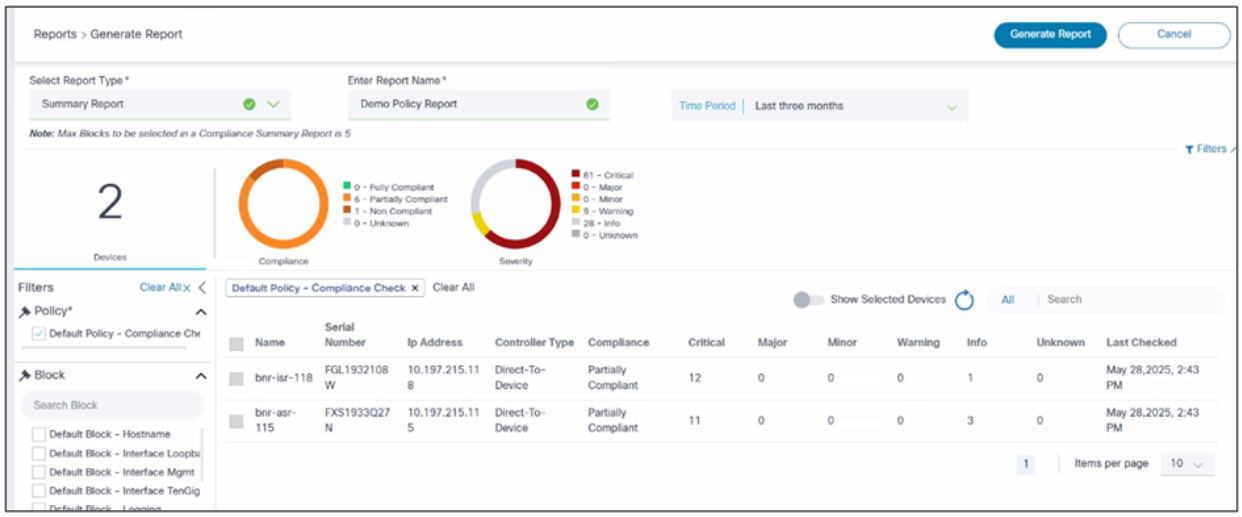


Excluir Bloco

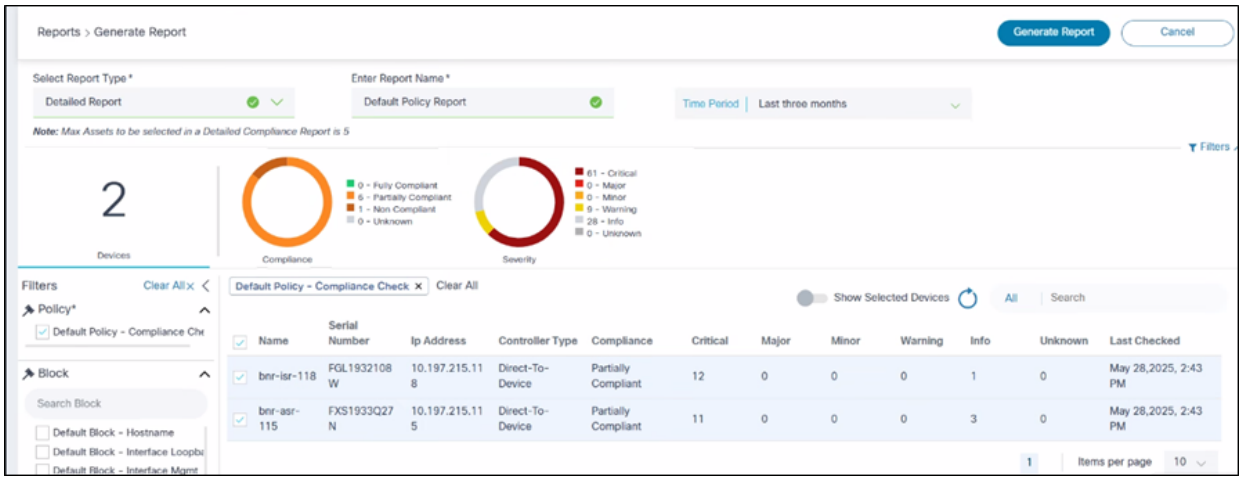
Configuração: Geração de Blocos Automáticos

A geração de blocos permite que os usuários criem blocos automaticamente com base na configuração de um dispositivo. Essa automação reduz o tempo e o esforço necessários para a criação manual e facilita para os usuários a edição de blocos adicionando ou removendo variáveis, em vez de começar do zero.

Clique em uma linha para exibir detalhes de geração de bloco.

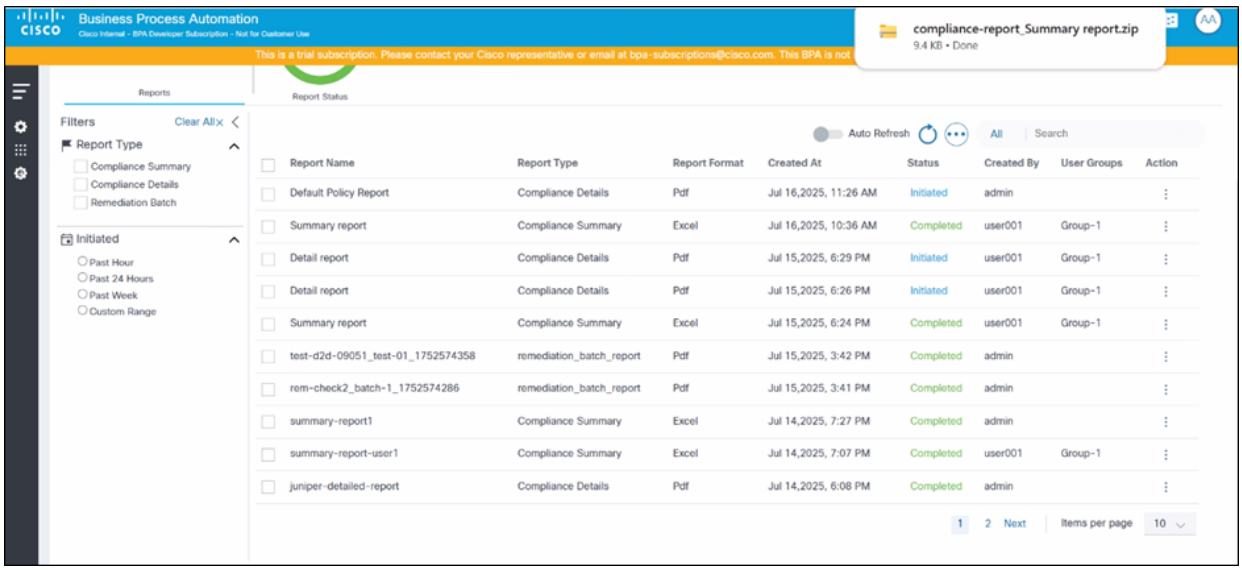


Lista de Geração de Bloqueio Automático - Exibir



Detalhes da Geração de Bloqueio Automático

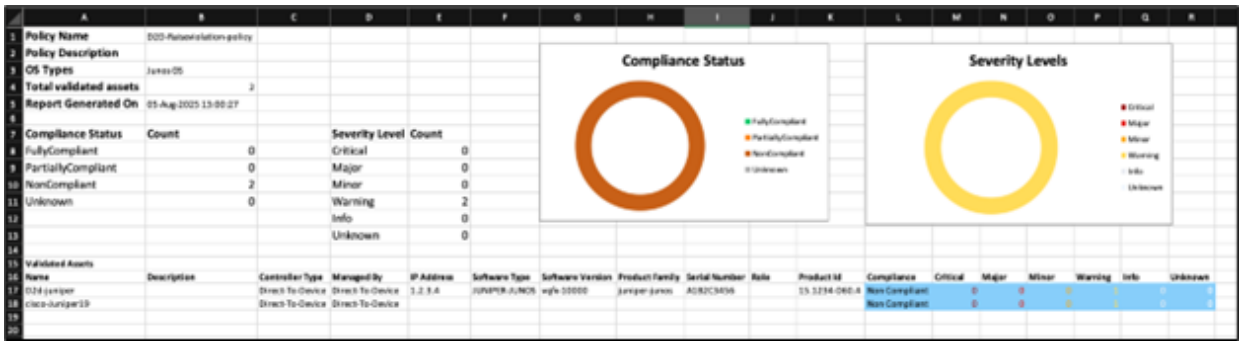
Geração de Blocos Automáticos



Lista de Geração de Bloqueio Automático

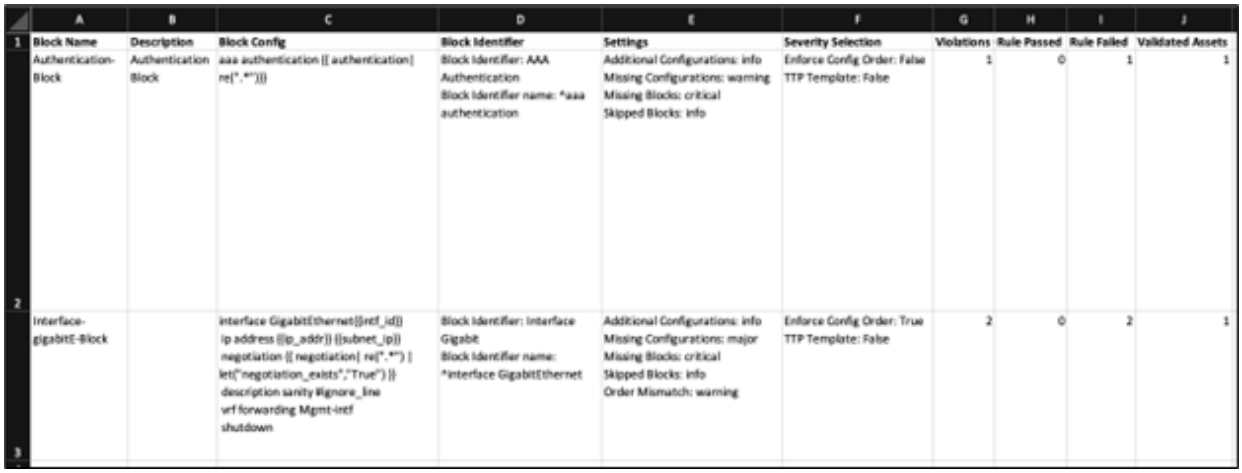
A página Geração Automática de Blocos inclui os seguintes campos:

- Gerar de: A origem a partir da qual os blocos são gerados. Ele tem as três opções a seguir:
  - Backup de configuração do dispositivo: O sistema seleciona uma configuração de dispositivo no caso de uso de backup



Backup da configuração do dispositivo

- Upload de arquivo: Uma janela de upload de arquivo é aberta para que os usuários carreguem a configuração do dispositivo



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

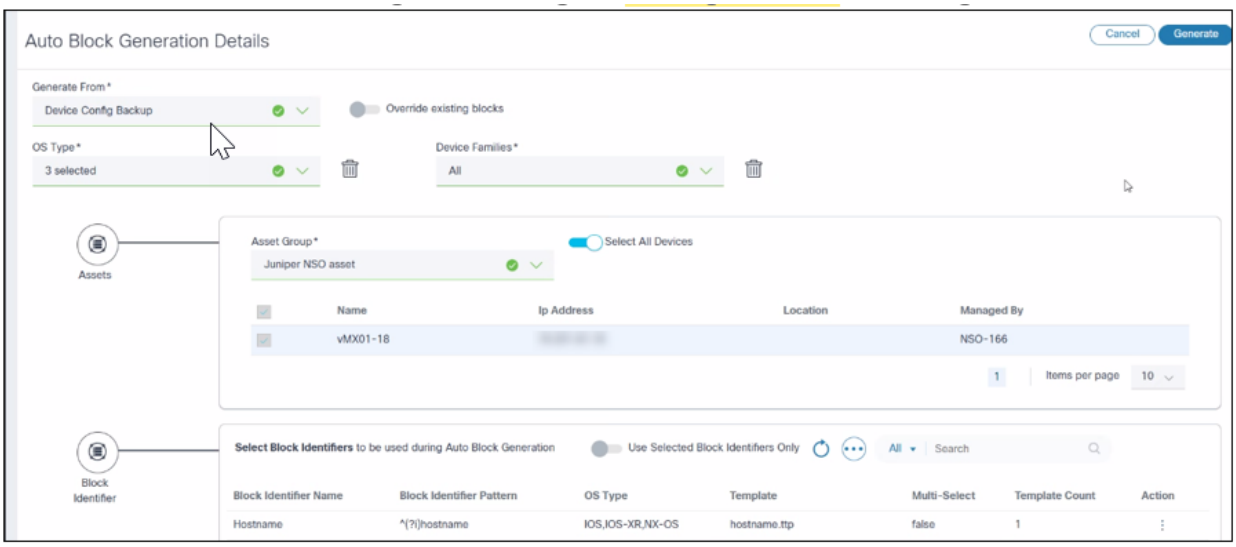
Upload de arquivo

- Configuração atual: Digite o comando de configuração CLI que o sistema usa para buscar a configuração do dispositivo.

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

Configuração atual

- Tipo de SO: Lista dos tipos de SO para os quais este bloco é relevante.
- Família de dispositivos: Lista de famílias de dispositivos para as quais este bloco é relevante.
- Ativos: O recurso Ativos oferece uma abordagem estruturada para selecionar dispositivos para gerar blocos dinâmicos
    - Seleção de grupo de ativos:
        - Permite que os usuários escolham um grupo predefinido de dispositivos, conhecido como grupo de ativos, que é usado para gerar blocos dinâmicos
        - Facilita o gerenciamento e a organização de dispositivos agrupando-os com base em critérios específicos, como local, tipo ou função
    - Seleção de dispositivo de subconjunto:
        - Os usuários têm a flexibilidade de selecionar um subconjunto específico de dispositivos dentro do grupo de ativos escolhido
        - Permite que os usuários se concentrem em um segmento específico de dispositivos, permitindo geração e gerenciamento de blocos mais direcionados



Geração de bloco

- Identificador de bloco: Fornece uma opção para que os usuários selecionem a lista de identificadores de bloco usados durante a geração do bloco. Ele também oferece recursos de gerenciamento de identificador de bloco em linha.

Identificador de bloco

Um identificador de bloco usa o CiscoConfParser para extrair um bloco de configuração de toda a configuração do dispositivo. Cada identificador de bloco deve ser associado a um padrão regex. Os usuários podem criar seus próprios identificadores de bloco ou atualizar identificadores de bloco existentes usando a interface do usuário ou a API. Atualmente, a plataforma fornece entre 55 e 60 identificadores de bloco padrão. Cada identificador é exclusivo de um tipo de SO e é carregado durante a implantação do aplicativo BPA por meio do serviço Ingester. Um modelo HTTP pode ser associado a cada identificador de bloco. O nome e o padrão de um identificador de bloco devem ser exclusivos.

Se a opção Multi estiver habilitada para o identificador de bloco, a estrutura de conformidade gerará vários blocos de configuração a partir das configurações correspondentes. Caso contrário, ele tratará todas as configurações correspondentes como um único bloco.

Exemplos de identificadores de bloco com a opção Multi True: interface, bgp de roteador, vrf, l2vpn etc.

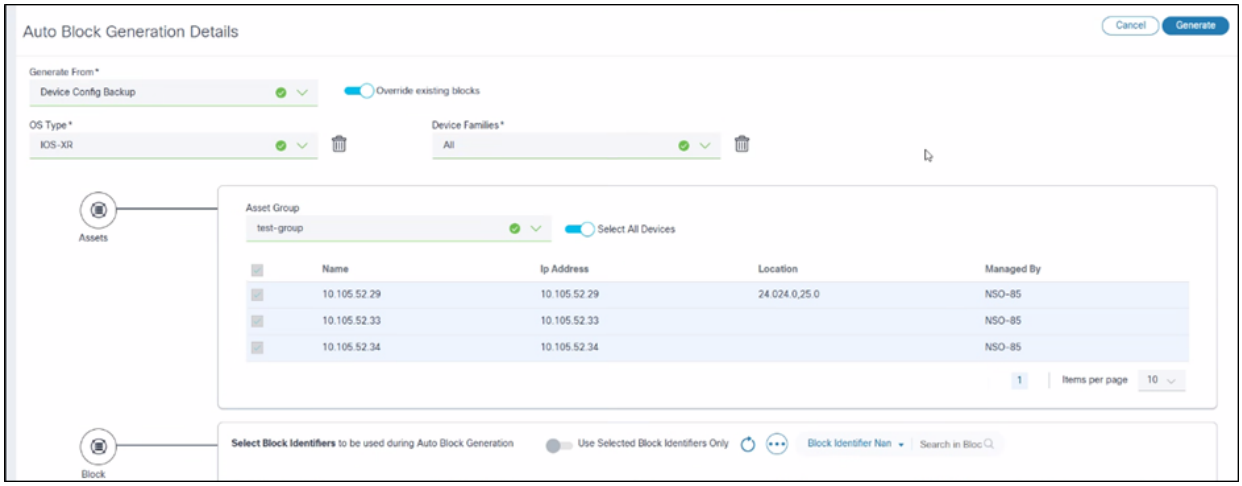
Exemplos de identificadores de bloco com a opção Multi False: logging, snmp-server, domain, etc.

Examples:

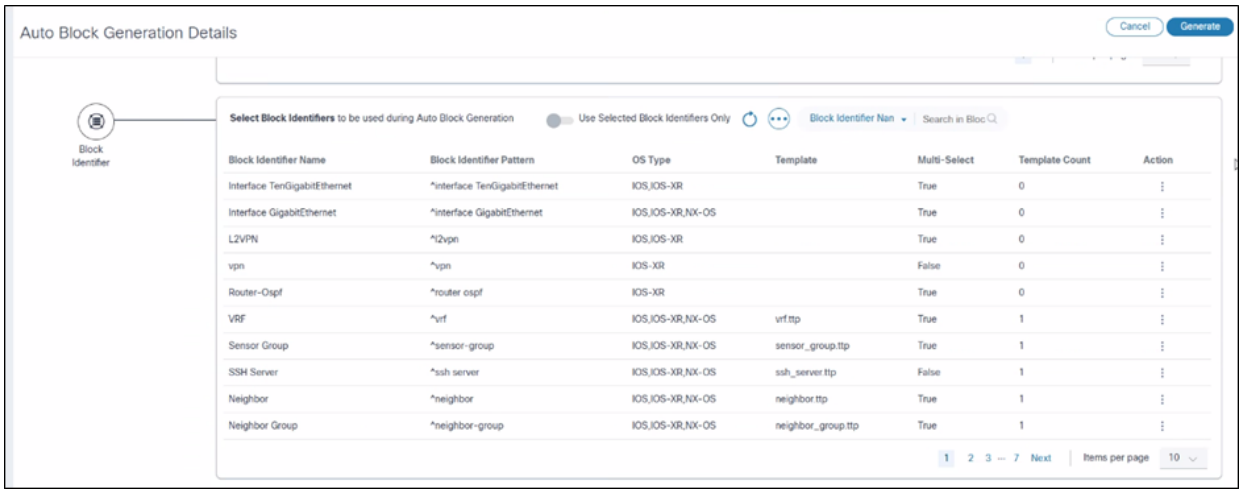
```
{
  “name”: “BundleEthernet Interface”,
  “osType”: [“IOS”, “IOS-XR”, “NX-OS”],
  “multi”: true,
  “blockIdentifier”: “^(?i)interface Bundle-Ether”,
  “templates”: [“parent_interface.ttp”]
}

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

Identificador de Bloco de Lista

Identificador de Bloco de Lista permite que os usuários exibam a lista de identificadores de bloco juntamente com funções de pesquisa e classificação. Este recurso está disponível na página Gerar blocos.

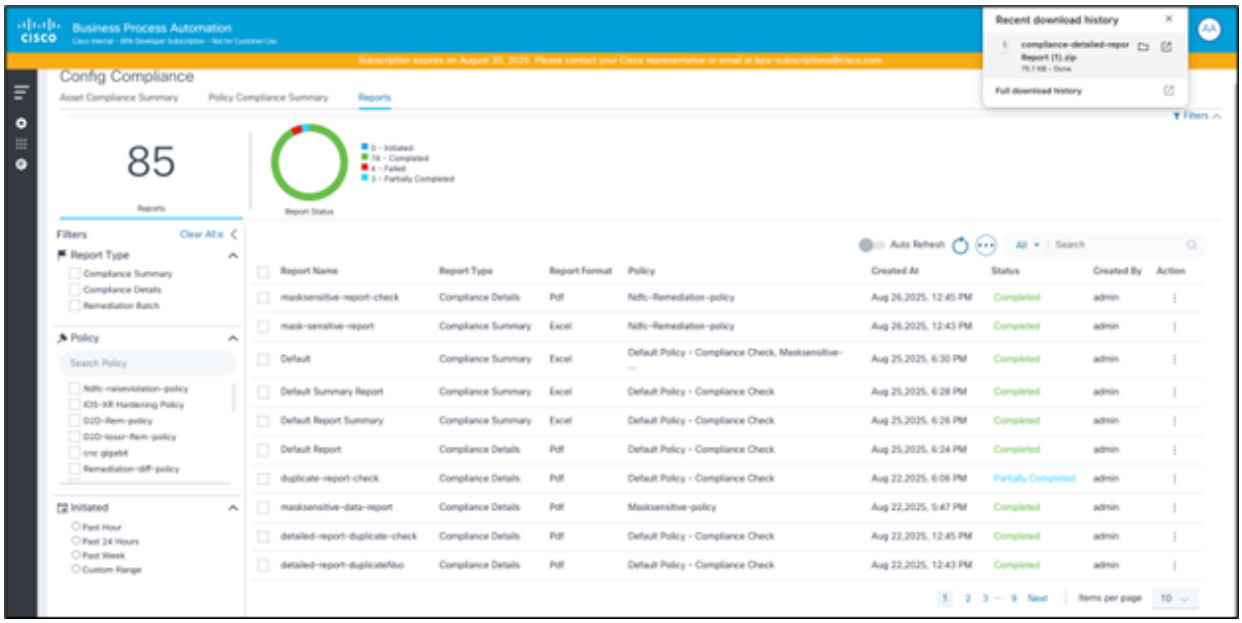


Lista de identificadores de bloco



Identificador de bloco

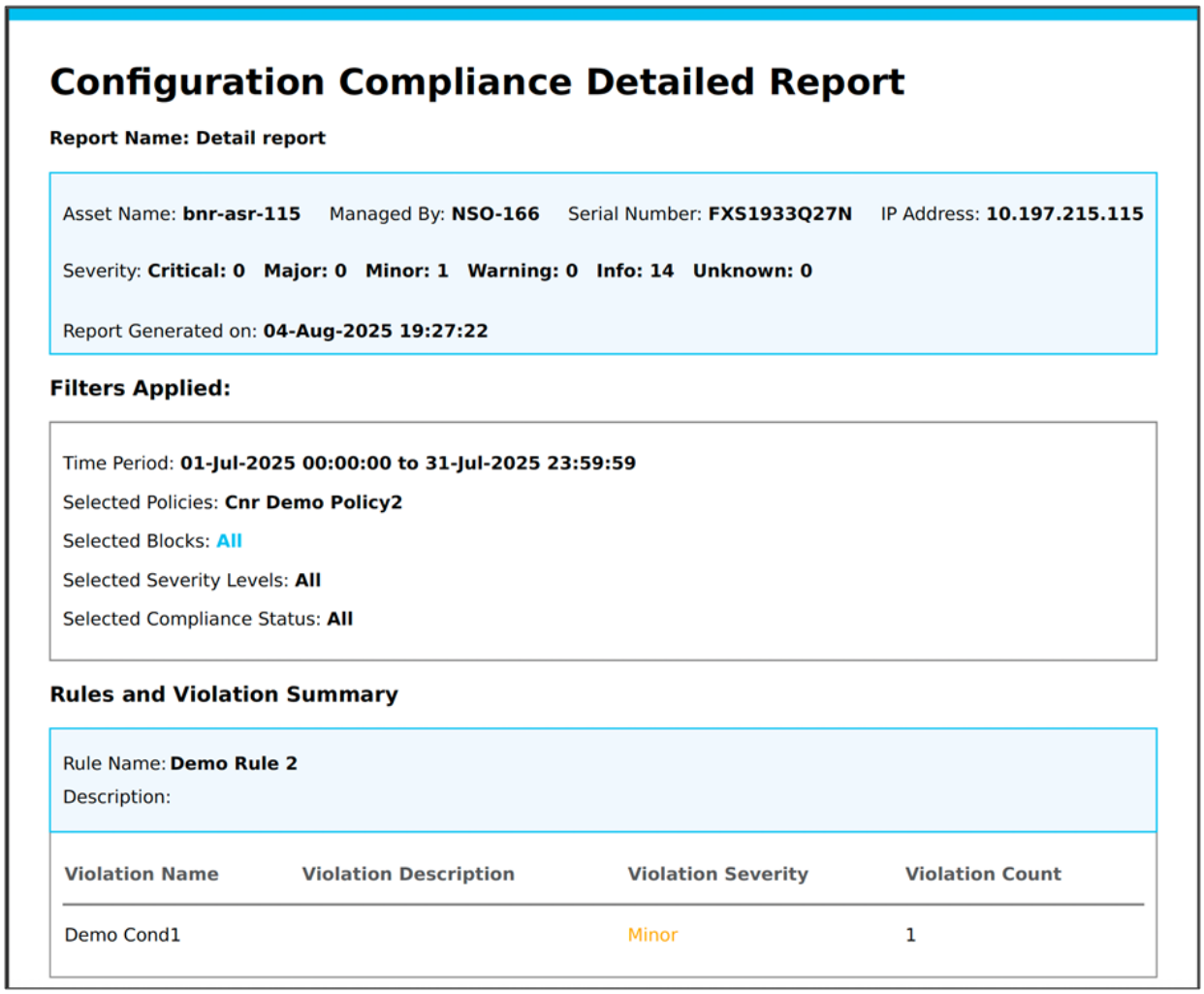
Criar ou Editar Identificador de Bloco



Editar identificador de bloco

A seção Lista de Identificadores de Bloco na página Geração Automática de Bloco fornece aos usuários as ferramentas para gerenciar identificadores de bloco de forma eficaz. As funcionalidades estão listadas abaixo:

- Criar identificadores de bloco
  - Os usuários podem adicionar novos identificadores de bloco à lista
  - Isso permite a introdução de identificadores exclusivos que podem ser usados para organizar e diferenciar blocos
- Editar identificadores de bloco
  - Identificadores de bloco existentes podem ser modificados
  - Permite atualizações ou correções de identificadores, garantindo que eles permaneçam precisos e relevantes para os blocos que representam
- Excluir Identificador de Bloco
  - Os usuários têm a opção de remover identificadores de bloco da lista
  - Facilita o gerenciamento de identificadores, permitindo a remoção daqueles que não são mais necessários ou aplicáveis



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

Excluir Identificador de Bloco

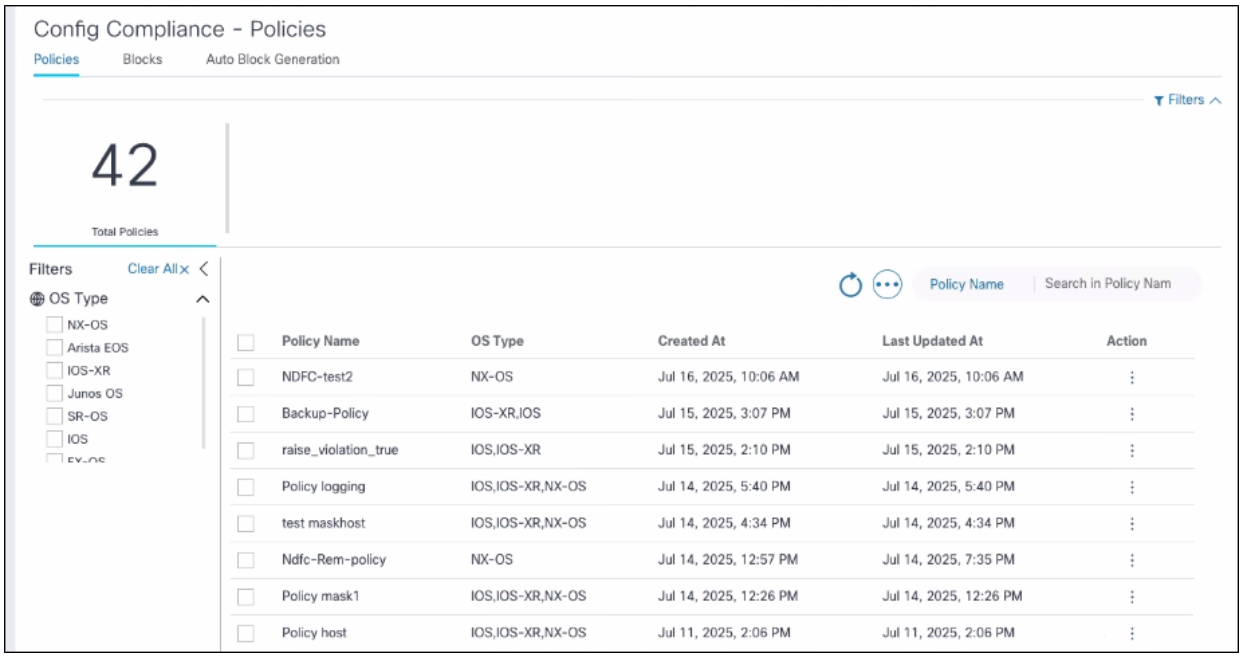
Configuração: Políticas

Um conjunto de políticas, regras e blocos para permitir a execução da conformidade pode ser definido na guia Policies. Uma política é um modelo definido pelo usuário que consiste em blocos de configuração e regras. Uma lista de blocos de configuração e uma lista de regras para cada bloco de configuração para criar uma política podem ser selecionadas.

Listar políticas

Uma lista de políticas pode ser exibida na guia Policies, que também fornece ações para adicionar, editar, excluir, importar e exportar políticas.

Note: As políticas são importadas ou exportadas junto com os blocos e regras relacionados.



Listar políticas

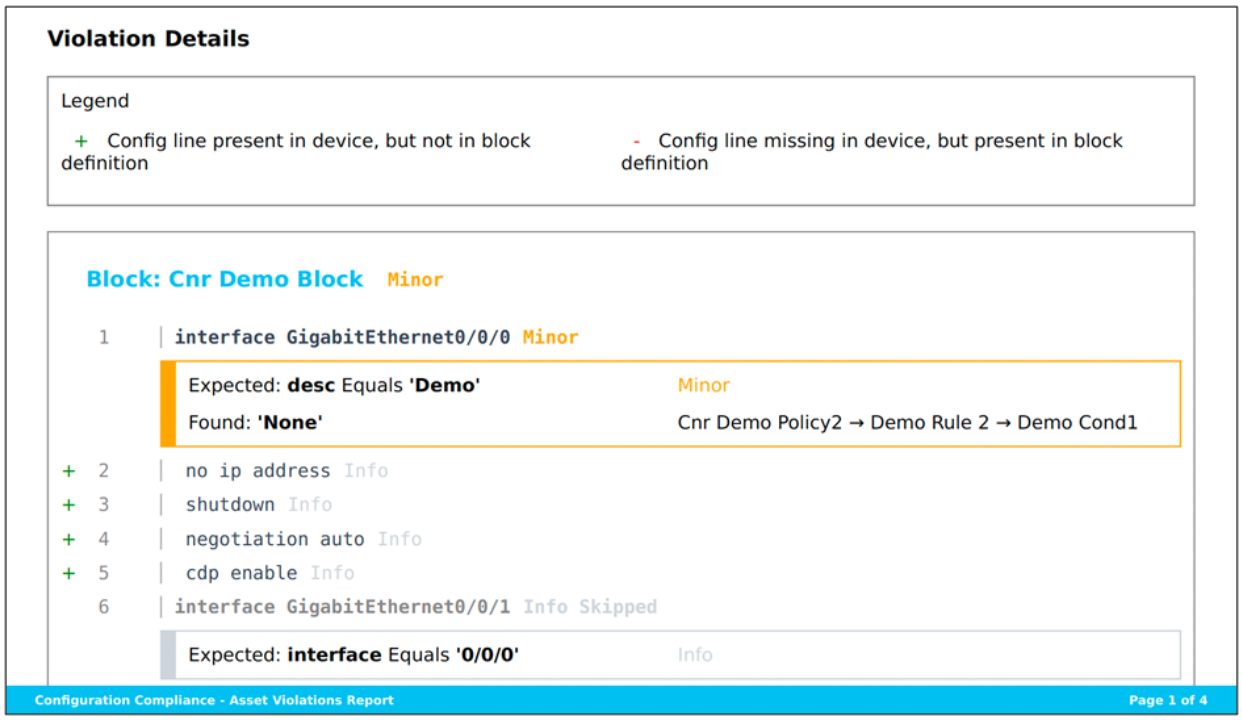
Adicionando e editando políticas

Esta seção descreve a página Adicionar Política e Editar Política:

Detalhes da política

- Nome da política: Nome da política
- Tipo de SO: Lista de tipos de SO com suporte para esta política
- Família de dispositivos: Lista de famílias de dispositivos com suporte para esta política
- Descrição da política (opcional): Descreve a política com uma breve descrição

Os campos Tipo de SO e Família do dispositivo são preenchidos automaticamente com base nos blocos selecionados na próxima seção.

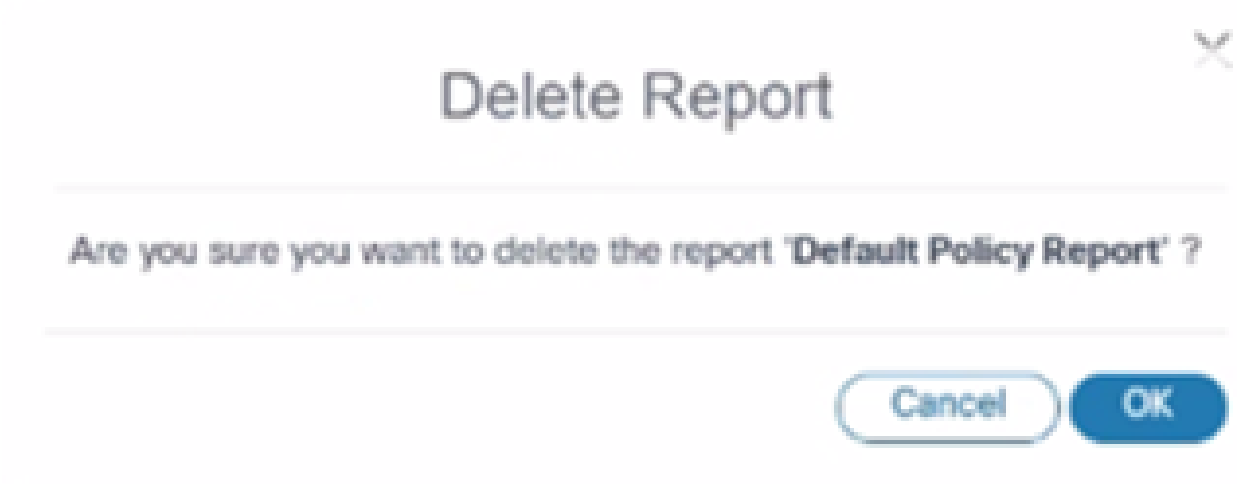


Políticas de configuração: Detalhes da política

Caixa de Diálogo Selecionar Blocos

O recurso "Select Blocks" é uma interface amigável projetada para ajudar os usuários na escolha de blocos de configuração para inclusão em uma política. Suas funcionalidades estão listadas nesta seção:

- Caixa de diálogo pop-up
  - Propósito: Oferece um espaço dedicado para que os usuários selecionem blocos de configuração sem sair da página atual
  - Interação do usuário: Garante um processo de seleção intuitivo apresentando opções em uma caixa de diálogo separada e focalizada
- Adicionar e Selecionar Opções
  - Várias Seleções: Os usuários podem escolher um ou mais blocos de configuração para incluir em uma política
  - Flexibilidade: Suporta a inclusão de vários blocos com base nos requisitos de política específicos do usuário
- Recursos de navegação
  - Filtros: Permite que os usuários limitem a lista de blocos disponíveis com base em critérios específicos, facilitando a localização de blocos relevantes
  - Paginação: Organiza blocos em páginas gerenciáveis, melhorando a navegação por grandes conjuntos de dados
  - Recursos de pesquisa: Permite a localização rápida de blocos por nome ou outros identificadores, otimizando o processo de seleção



Seleção de Bloco

Os usuários podem criar novos blocos clicando em Criar na seção Seleção de bloco. Uma nova guia do navegador é iniciada de forma cruzada e os usuários podem criar um novo bloco. Depois de enviados, os usuários podem retornar à guia original e selecionar o bloco recém-criado para adicioná-lo à política.

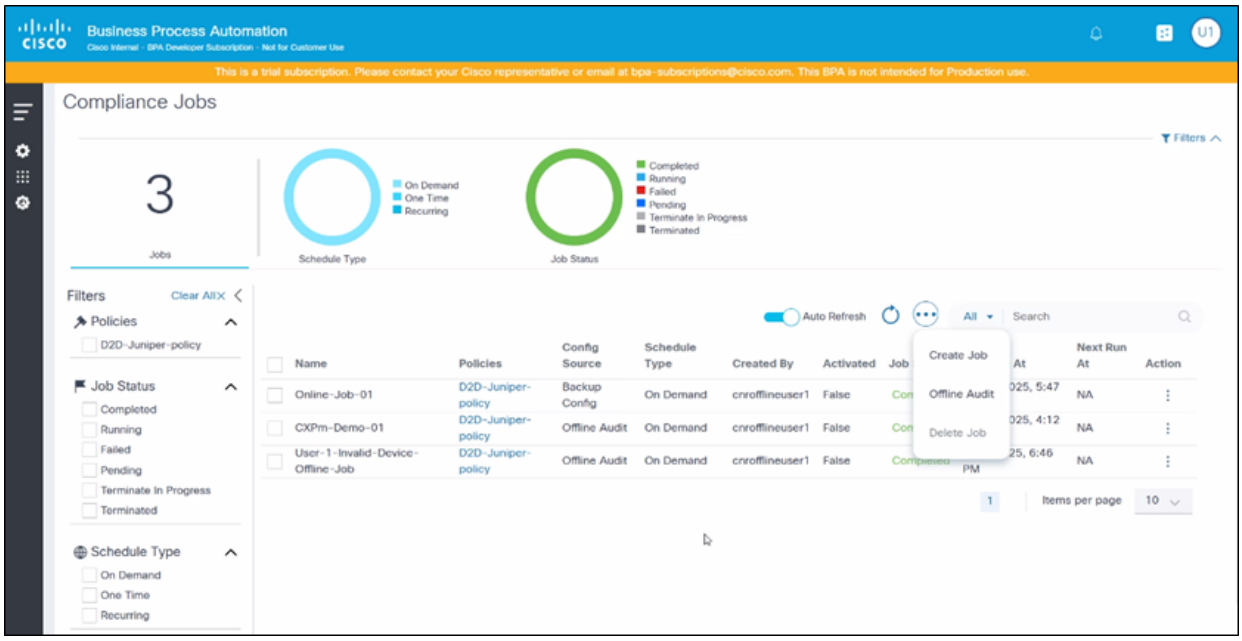
Filtros condicionais

O recurso Filtros condicionais é uma ferramenta avançada que permite aos usuários aplicar critérios específicos aos blocos de configuração, garantindo verificações de conformidade precisas e direcionadas.

- Permite que os usuários apliquem configurações ou executem verificações de conformidade em blocos de configuração selecionados com base em condições predefinidas
- Concentra recursos e esforços em blocos relevantes filtrando aqueles que não atendem aos critérios especificados
- Os usuários podem definir condições que os blocos de configuração devem atender para serem incluídos em verificações de conformidade ou outros processos
- Somente os blocos correspondentes a essas condições são executados, enquanto outros são ignorados, permitindo um controle mais preciso

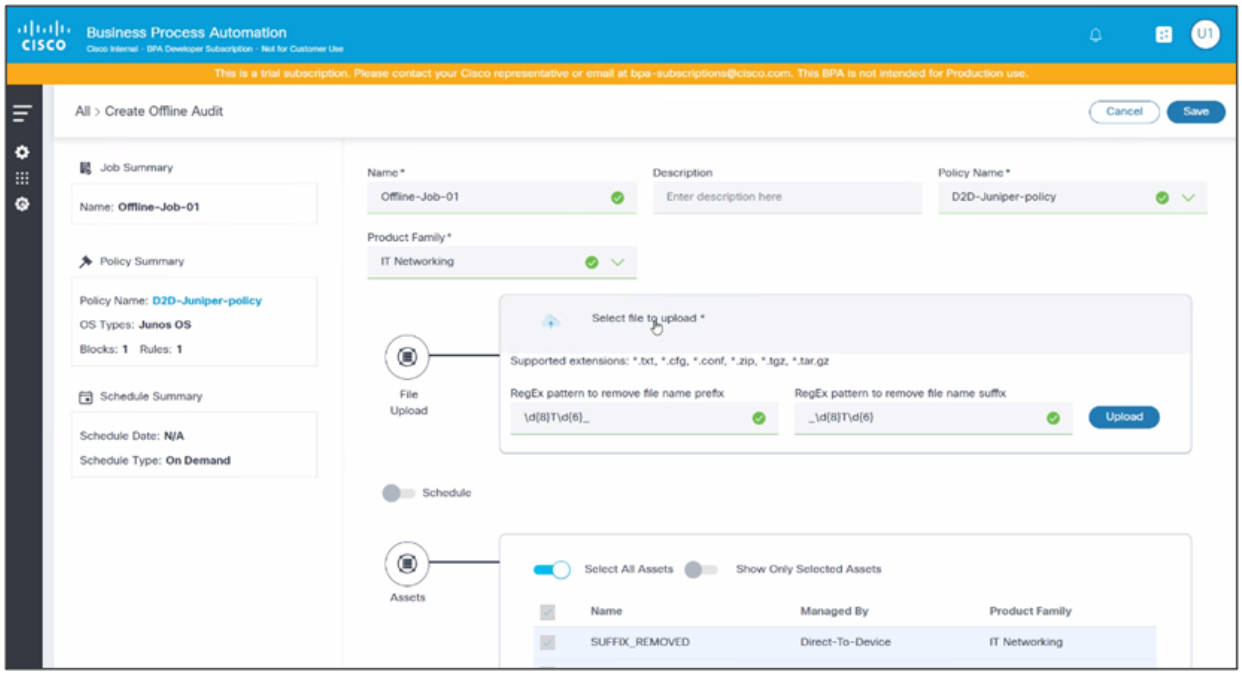
Exemplo de caso de uso:

- Verificações seletivas de conformidade: Se uma política tiver a intenção de verificar configurações em apenas duas interfaces específicas das 20 disponíveis, os usuários poderão definir condições para limitar as verificações de conformidade a apenas essas duas interfaces.



Filtros condicionais

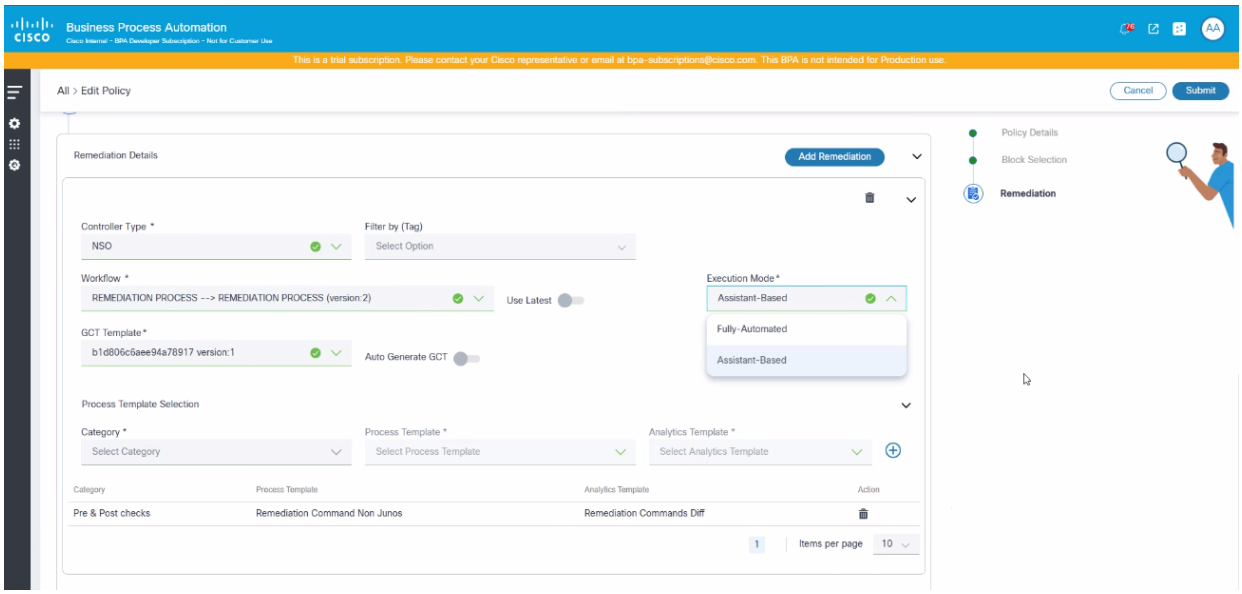
- Selecionar regras: Opção para selecionar uma ou mais regras para um determinado bloco de configuração.



Selecionar regras

Seção de correção

A página Policies fornece uma seção opcional para definir detalhes de remediação por tipo de controlador.



Políticas de configuração: Detalhes da correção

- Tipo de controlador: Lista de tipos de controlador com suporte para correção
- Fluxo de Trabalho de Correção: Fluxo de trabalho a ser executado para dispositivos do tipo de controlador selecionado
- Modelo GCT: Um ou mais modelos GCT a serem aplicados
- Modelo de processo: Um ou mais modelos de processo a serem executados como parte da pré-verificação e pós-verificação, juntamente com o modelo de análise correspondente.
- Modelo de pré-verificação: Lista opcional de modelos de processo a serem executados somente para pré-verificação
- Modelo de pós-verificação: Lista opcional de modelos de processo a serem executados somente para pós-verificação
- Modo de Execução:
  - Totalmente Automático: O processo de correção é executado automaticamente sem intervenção manual ou tarefas do usuário
  - Baseado em assistente: O sistema cria tarefas de usuário que exigem assistência manual durante o processo de correção

Gerar recurso GCT automaticamente

O recurso Gerar GCT automaticamente foi projetado para simplificar o processo de criação de modelos GCT necessários para correção. Funciona conforme detalhado abaixo:

- Gera automaticamente modelos GCT com base nos resultados e detalhes da execução da conformidade
- Automatiza o processo de criação de modelos
- Os modelos gerados são adaptados para resolver problemas identificados durante as verificações de conformidade, garantindo que as ações de correção se alinhem com as necessidades de conformidade

Funções e controle de acesso

Lista de Permissões Estáticas

O painel de controle Conformidade com a configuração no portal de última geração oferece suporte ao recurso RBAC do BPA com as seguintes permissões que representam como um bloco de texto dinâmico de configuração é exibido em uma representação de GUI para manipular as regras e condições:

Grupo	Ação	Descrição
ui-app	complianceDashboard.show	Mostrar/Ocultar Aplicativo de Painel de Conformidade
ui-app	remediationDashboard.show	Mostrar Aplicativo de Trabalhos de Correção
ui-app	complianceJobs.show	Mostrar aplicativo de trabalhos de conformidade
ui-app	complianceConfigurations.show	Mostrar aplicativo de configuração de conformidade
complianceDashboard	assetsComplianceSummary	Exibir resumo de conformidade de ativos
complianceDashboard	resumoDeConformidadeDaPolítica	Exibir resumo de conformidade de políticas
complianceDashboard	exibirViolações	Exibir detalhes da violação
complianceDashboard	policyComplianceAssetsSummary	Exibir ativos afetados
complianceDashboard	exibirRelatórios	Exibir painel de relatórios, configurações de relatórios e fazer download de relatórios
complianceDashboard	gerenciarRelatórios	Criar e excluir relatórios
complianceDashboard	gerenciarConfiguraçõesDeRelatório	Modificar configurações do relatório
painelDeremediação	exibirTrabalhosDeCorreção	Exibir Trabalhos de Correção
painelDeremediação	exibirMarcosDaCorreção	Exibir Etapas da Correção
painelDeremediação	gerenciarTrabalhosDeCorreção	Gerenciar Trabalhos de Correção, como criar, excluir, arquivar e manipular tarefas de usuário
complianceTrabalhos	exibirTrabalhodeConformidade	Exibir jobs e execuções de conformidade
complianceTrabalhos	gerenciarTrabalhodeConformidade	Gerenciar trabalhos de

Grupo	Ação	Descrição
		conformidade
conformidadeconfigurações	exibirConformidadeConfigurações	Exibir configurações de conformidade, como políticas, blocos, regras, geração de blocos, identificadores de blocos e modelos TTP
conformidadeconfigurações	gerenciarPolíticasDeConformidade	Gerenciar políticas de conformidade
conformidadeconfigurações	manageComplianceBlocks	Gerenciar blocos e regras de conformidade e identificadores de bloco
conformidadeconfigurações	manageComplianceBlockGeneration	Gerenciar geração de bloco de conformidade e modelos TTP

Funções predefinidas

O caso de uso Conformidade com a configuração e Correção tem as funções predefinidas listadas na tabela abaixo:

Note: Os administradores podem criar ou atualizar funções de acordo com os requisitos do cliente.

Função	Descrição	Permissões
Administrador de conformidade	Função de administrador com todas as permissões relacionadas à conformidade	Aplicativos de IU: Mostrar Gerenciador de Ativos - Mostrar Grupo de Ativos - Exibir Painel de Conformidade - Mostrar trabalhos de conformidade - Mostrar configuração de conformidade Ativo: Exibir Lista de Ativos - Exibir configuração de backup para ativos

Função	Descrição	Permissões
		- Configuração de backup - Executar Ações de Dispositivos Habilitados por Controlador Grupo de ativos: - Exibir Grupos de Ativos - Gerenciar grupos de ativos - Criar grupos de ativos dinâmicos Configuração de backup: Exibir, comparar e fazer download de backups de configuração de dispositivos Política de restauração de backup: Exibir políticas de restauração de backup Painel de conformidade: - Exibir resumos de conformidade dos ativos - Exibir resumos de conformidade das políticas - Exibir violações - Exibir ativos afetados Criar e excluir relatórios Exibir painel de relatórios, configurações de relatórios e fazer download de relatórios Modificar configurações do relatório: Trabalhos de conformidade Exibir jobs e execuções de conformidade - Gerenciar trabalhos de conformidade Configurações de conformidade: - Exibir configurações de

Função	Descrição	Permissões
		conformidade, como políticas, blocos e regras - Gerenciar políticas de conformidade - Gerenciar blocos de conformidade, regras e identificadores de bloco - Gerenciar a geração de blocos de conformidade e modelos TTP Aplicativos de IU: - Mostrar o Asset Manager - Mostrar Grupo de Ativos - Exibir Painel de Conformidade - Mostrar trabalhos de conformidade - Mostrar configuração de conformidade Ativo: Exibir Lista de Ativos - Exibir configuração de backup para ativos - Configuração de backup - Executar Ações de Dispositivos Habilitados por Controlador Grupo de ativos: - Exibir Grupos de Ativos - Gerenciar grupos de ativos - Criar grupos de ativos dinâmicos Configuração de backup: Exibir, comparar e fazer download de backups de configuração de dispositivos Política de restauração de backup: Exibir políticas de restauração de backup Painel de conformidade: - Exibir resumo de conformidade de
Operador de Conformidade	Função de operador com todas as permissões de conformidade, exceto para gerenciamento de configuração	

Função	Descrição	Permissões
		ativos - Exibir resumo de conformidade de políticas - Exibir violações - Exibir ativos afetados Criar e excluir relatórios Exibir painel de relatórios, configurações de relatórios e fazer download de relatórios Trabalhos de conformidade: Exibir jobs e execuções de conformidade - Gerenciar trabalhos de conformidade Configurações de conformidade: Exibir configurações de conformidade, como políticas, blocos e regras Aplicativos de IU: - Mostrar o Asset Manager - Mostrar Grupo de Ativos - Exibir Painel de Conformidade - Mostrar trabalhos de conformidade - Mostrar configuração de conformidade
Conformidade Somente Leitura	Fornece todas as permissões somente leitura relacionadas ao caso de uso de conformidade	Ativo: Exibir Lista de Ativos - Exibir configuração de backup para ativos - Executar Ações de Dispositivos Habilitados por Controlador Grupo de ativos: - Exibir Grupos de Ativos Configuração de backup: Exibir,

Função	Descrição	Permissões
		comparar e fazer download de backups de configuração de dispositivos Política de restauração de backup: Exibir políticas de restauração de backup Painel de conformidade: Exibir resumo de conformidade de ativos - Exibir resumo de conformidade de políticas - Exibir violações - Exibir ativos afetados Exibir painel de relatórios, configurações de relatórios e fazer download de relatórios Trabalhos de conformidade: Exibir jobs e execuções de conformidade Configurações de conformidade: Exibir configurações de conformidade, como políticas, blocos e regras Aplicativos de IU: - Mostrar o Asset Manager - Mostrar Grupo de Ativos - Exibir painel de remediação
Administrador de correções/Operador de correções	Função de operador com todas as permissões relacionadas à correção	Ativo: - Exibir lista de ativos Grupo de ativos: - Exibir Grupos de Ativos Gerenciar grupos de ativos - Criar grupos de ativos dinâmicos

Função	Descrição	Permissões
Remediação Somente Leitura	Fornece todas as permissões somente leitura relacionadas ao caso de uso de remediação	Painel de correção: - Exibir Trabalhos de Correção - Visualizar etapas de correção - Exibir resumo de conformidade de ativos - Gerenciar trabalhos de correção, como criar, excluir, arquivar e manipular tarefas do usuário - Exibir ativos afetados Aplicativos de IU: - Mostrar o Asset Manager - Mostrar Grupo de Ativos - Exibir painel de remediação Ativo: - Exibir lista de ativos Grupo de ativos: - Exibir Grupos de Ativos Criar grupos de ativos dinâmicos Painel de correção: - Exibir Trabalhos de Correção - Visualizar etapas de correção - Exibir resumo de conformidade de ativos - Exibir ativos afetados

Políticas de acesso

O recurso Access Policies (Políticas de acesso) garante que os usuários tenham acesso apropriado a políticas de conformidade e grupos de ativos específicos. Esse recurso melhora a

segurança e a eficiência operacional permitindo que os administradores definam e apliquem controles de acesso com base nas funções e responsabilidades do usuário. As Políticas de acesso são gerenciadas por meio da página Política de acesso, na qual os administradores podem criar, editar e atribuir políticas a usuários ou grupos. Os administradores podem definir permissões granulares, especificando quais políticas de conformidade e grupos de ativos cada usuário ou grupo pode exibir, editar ou gerenciar. Esse nível de detalhes ajuda a manter um controle rígido sobre as informações confidenciais e as operações críticas.

Depois que a política de acesso é definida, os dados são restritos em todas as páginas de conformidade e remediação na interface do usuário de última geração, com base na lista de políticas e ativos CnR aos quais o usuário atual tem acesso.

Para fornecer acesso de usuário:

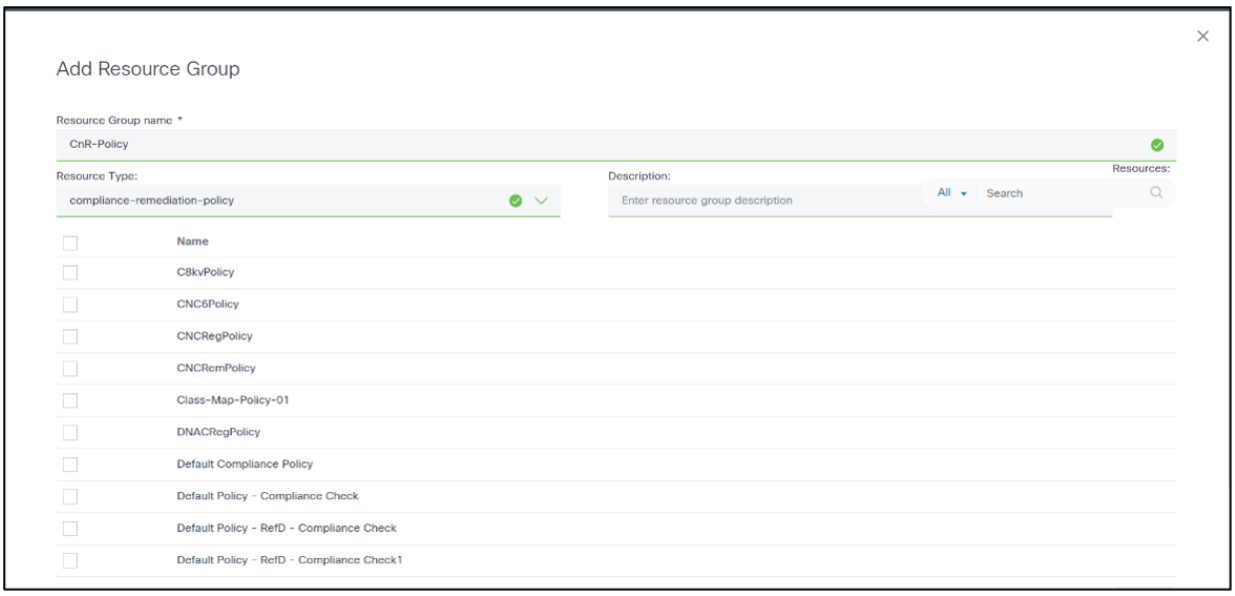
 Note: As permissões só podem ser fornecidas por administradores.

---

1. Crie usuários e atribua a eles um grupo de usuários.
2. Crie funções de usuário e atribua-as aos grupos de usuários criados.
3. Adicionar ativo(s) a um grupo de ativos.
4. Criar grupo(s) de recursos para atribuir recurso(s) de política de conformidade.
5. Crie uma política de acesso e selecione grupos de usuários, grupos de ativos e grupos de recursos relevantes.

Criando grupo de recursos

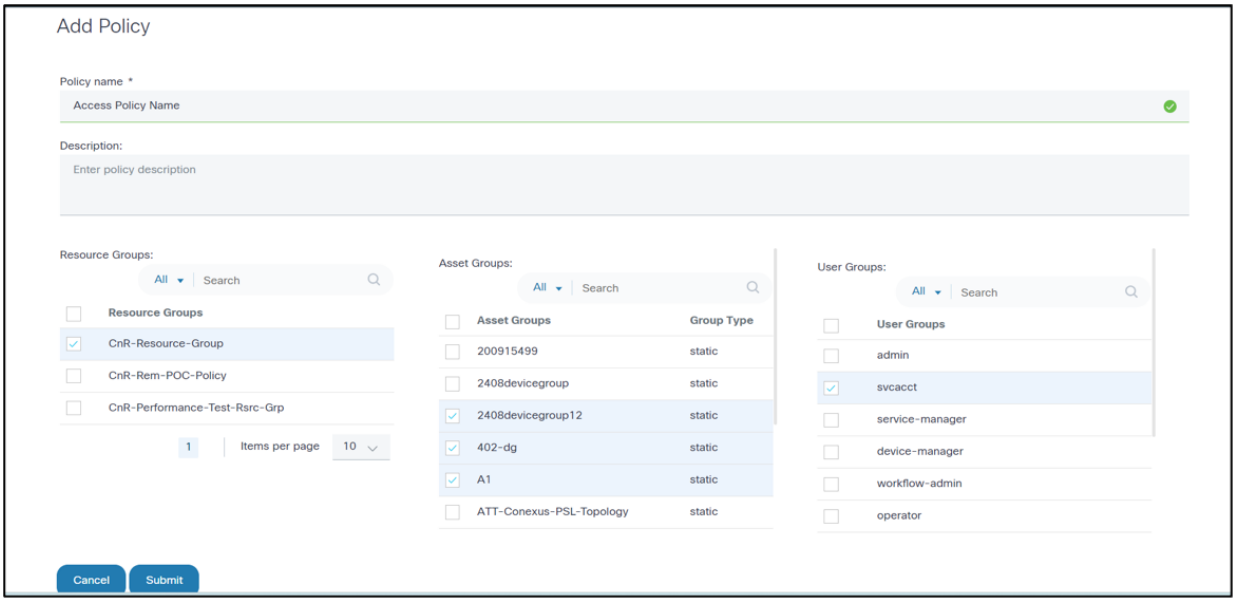
Crie um Grupo de Recursos usando a política de correção de conformidade na lista suspensa Tipo de Recurso e selecione as políticas de conformidade que precisam receber acesso ao respectivo grupo de usuários.



Criar grupo de recursos

Criar política de acesso

Crie uma política de acesso com grupos de recursos e grupos de ativos que precisem dar permissão ao(s) grupo(s) de usuários.



Criar política de acesso

Conformidade off-line

O recurso Conformidade off-line permite que os usuários executem verificações de conformidade em configurações de dispositivos que não estão disponíveis por meio de dispositivos ativos no inventário de ativos.

Os usuários podem executar a conformidade off-line usando a configuração de backup do dispositivo ou criando uma auditoria off-line em Trabalhos de Conformidade. Os resultados das execuções podem ser exibidos no painel de controle Conformidade.

Usando configuração de backup de dispositivo

Os administradores podem carregar manualmente um arquivo zip que contenha a configuração atual de um conjunto desejado de dispositivos. Esse recurso está disponível na seção Device Config - Upload (Configuração do dispositivo - Carregar) do aplicativo Backup & Restore. Depois que as configurações do dispositivo forem carregadas, uma tarefa de conformidade para os dispositivos desejados pode ser criada selecionando Device Backup Config como a origem da configuração do dispositivo. Durante a execução, a configuração do dispositivo carregado é recuperada do aplicativo de backup e a verificação de conformidade é executada nele.

Usando o recurso Criar Auditoria Off-line em Jobs de Conformidade

Para executar a conformidade com uma configuração de dispositivo off-line, os usuários podem selecionar Auditoria off-line no ícone Mais opções na página Jobs de Conformidade. Isso permite que os usuários carreguem manualmente um arquivo zip contendo a configuração atual diretamente no aplicativo Compliance. Durante a execução, a configuração do dispositivo carregado é analisada e a verificação de conformidade é executada.

Implantação de configurações por meio do Ingester

O carregamento de artefatos de configuração de conformidade pode ser automatizado usando a estrutura do Ingester. Depois que os artefatos são desenvolvidos, eles podem ser exportados, empacotados e implantados no ambiente de destino usando as seguintes etapas.

- Crie o pacote NPM usando os seguintes comandos:

```
mkdir <

      >
cd  <

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

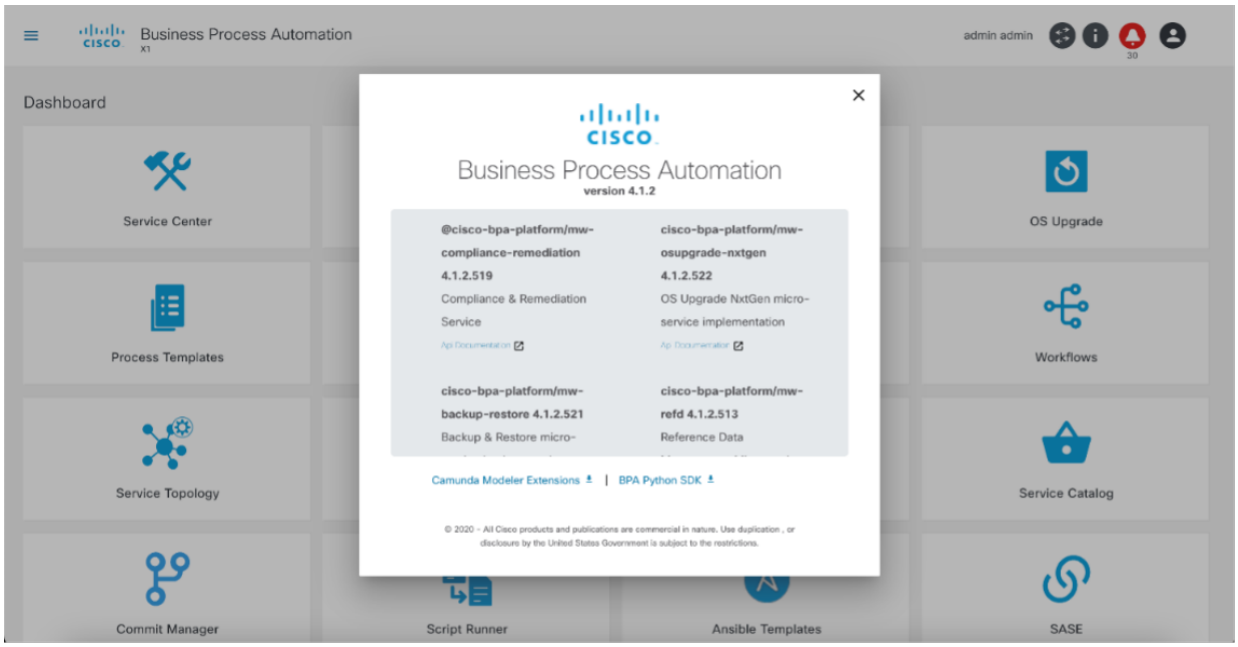
- Exportar configurações do portal do BPA (IU clássica)
    - Navegue até BPA Classic UI > Conformidade e correção da configuração > Configurações
    - Exportar "Modelos HTTP/Identificadores de bloco/Blocos/Regras/Políticas"
- Renomeie os arquivos exportados da seguinte maneira:
    - Modelos TTP: <<nome do arquivo>>.cnrttptemplate.json
    - Identificadores de bloco: <<filename>>.cnrblockidentifier.json
    - Blocos: <<filename>>.cnrblock.json
    - Regras: <<nome do arquivo>>.cnrrule.json
    - Políticas: <<filename>>.cnrpolicy.json
- Dados de inclusão do pacote (.tgz)
    - Copie todos os arquivos exportados para o pacote npm criado na "etapa 1"
    - Execute o comando `npm pack` dentro do pacote npm para criar o arquivo ".tgz"
- Implantação de dados de inclusão (.tgz) no ambiente de nó único do BPA
    - Copie o arquivo .tgz para a pasta <<BPA core bundle>>/packages/data no servidor onde o pacote BPA foi implantado
    - Reinicie o servidor Ingester (docker restart ingester-service)
- Implantação de dados do Ingester (.tgz) no ambiente de vários nós do BPA
    - Copie o arquivo .tgz para a pasta /opt/bpa/packages/data no servidor onde os gráficos do leme estão implantados
    - Reimplantar pod do Ingester (`kubectl rollout restart deployment ingester-service -n bpa-ns`)

Referências

Nome	Descrição
TTP	Analisador de Texto de Modelo usado em blocos de configuração
Analisador Conf	Analisador do campo de configuração usado para analisar a configuração do dispositivo CLI

Documentação da API

Os detalhes da documentação da API para conformidade e correção podem ser encontrados no pop-up Sobre a interface de usuário clássica:



Sobre BPA (IU clássica)

Troubleshooting

Painel

Os resultados recentes do trabalho de conformidade não são exibidos

Observação: Os resultados recentes do trabalho de conformidade não são exibidos no painel do portal de próxima geração.

Causa potencial 1: O painel tem uma seleção de intervalo de datas, que assume como padrão o "Mês atual". Se um novo mês tiver começado recentemente (por exemplo, hoje é o primeiro do mês), as execuções executadas antes de ontem (último dia do mês anterior) não serão exibidas.

Análise: Verifique se o intervalo de datas correto está selecionado no painel, incluindo os dias do mês anterior, se necessário, para mostrar os dados de violações apropriados.

Causa potencial 2: Um usuário diferente pode ter executado um Trabalho de Conformidade na mesma combinação de política e/ou ativo. O painel mostra as violações encontradas durante a execução mais recente dentro do intervalo de datas selecionado.

Análise: Como administrador (ou usuário com acesso a todos os Jobs de Conformidade), revise a lista de Jobs de Conformidade e seu histórico para determinar quais combinações de política ou grupo de ativos são executadas.

Trabalhos de conformidade

Status de execução inteiro definido como "Ignorado"

Observação: Durante a execução de Jobs de Conformidade, um status de execução inteiro é marcado como "Ignorado". Nenhuma violação foi relatada.

Causa potencial: Uma execução existente para o mesmo job ainda está em execução.

Análise: Um Trabalho de Conformidade pode ter apenas uma execução no estado em execução em um determinado momento. Verifique se uma execução anterior ainda está em execução. As execuções que estiverem paralisadas ou em execução por um período prolongado podem ser encerradas/

Status do dispositivo definido como "Ignorado"

Observação: Em uma execução de Trabalho de Conformidade, o status de alguns dos dispositivos é marcado como "Ignorado".

Causa potencial: O recurso de conformidade não está habilitado para o tipo de controlador ao qual o dispositivo pertence.

Análise: A política de conformidade se aplica somente a dispositivos dentro do grupo de ativos que têm o recurso habilitado.

Status do dispositivo definido como "Falha"

Observação: Em uma execução de Job de Conformidade, o status de alguns dispositivos é marcado como "Com Falha".

Causa potencial: Erros de tempo de execução ocorridos durante o processo de execução de conformidade. Esses erros podem ser erros de código ou configurações incorretas em políticas, blocos, regras, identificadores de bloco, etc.

Análise:

API para localizar o motivo dos erros de tempo de execução:

1. Obter execuções para localizar a ID de execução

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

execuções de conformidade

Método: GET

2. Obter Execuções de Dispositivo usando a ID de execução

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

   compliance-device-executions?

   executionId=<< id-de-execução >>

   Método: GET

Regras de conformidade

Regras Exibir Valor Vazio

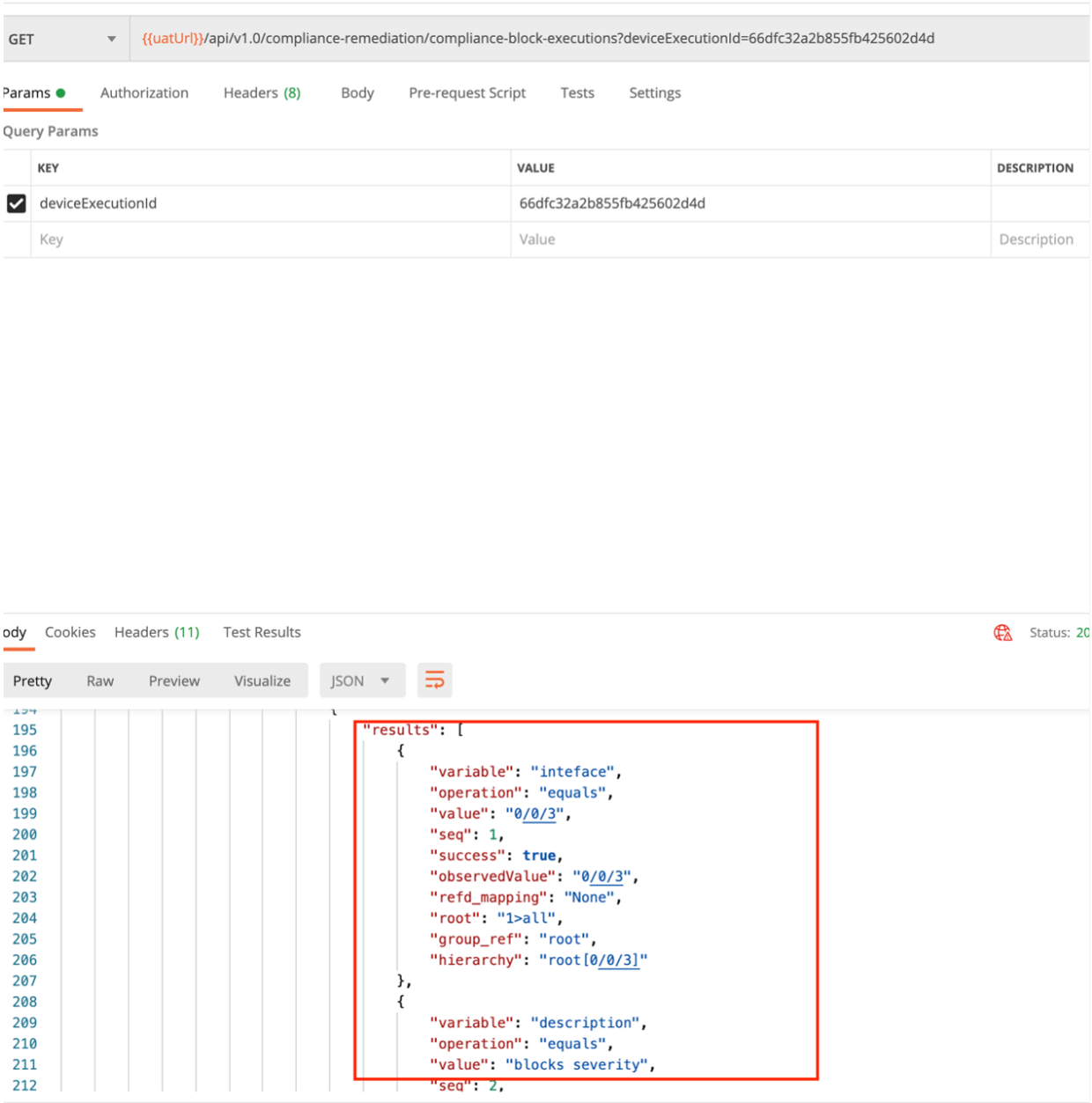
Observação: Durante a execução de um Job de Conformidade, as variáveis de regra exibem valores vazios.

Análise:

1. Se os dados estiverem sendo recuperados do aplicativo RefD, confirme se as chaves RefD estão no formato correto. Se estiverem, confirme se o aplicativo RefD tem dados para a chave vinculada à variável de conformidade nas regras. Além disso, verifique se a chave RefD correta está sendo enviada do aplicativo de conformidade verificando os logs do serviço de conformidade. Consulte Noções Básicas sobre Hierarquia de Regras e Integração de RefD em Regras e Regras Não-RefD.
2. Verifique o resultado da execução do bloco de conformidade usando a seguinte API:

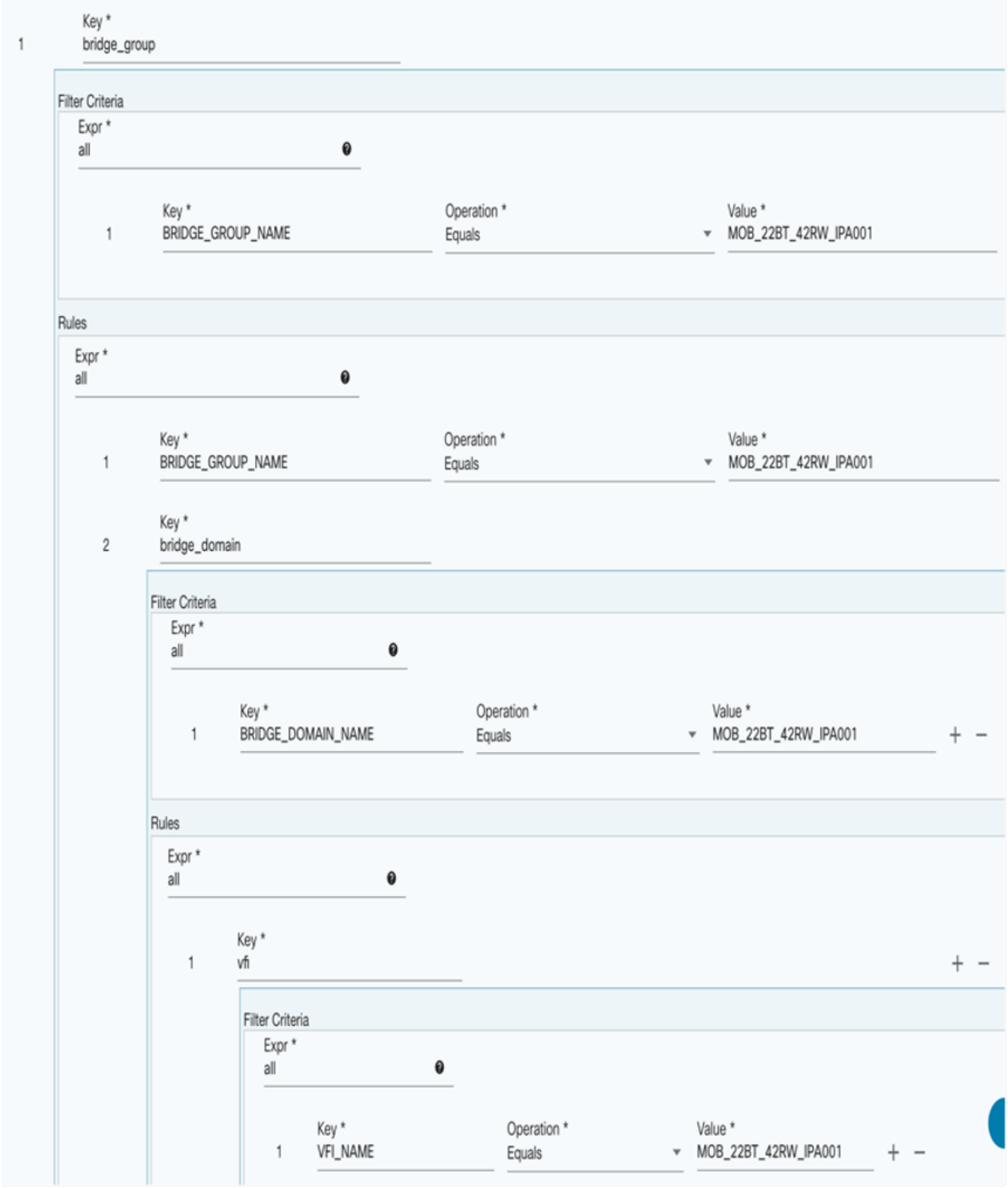
   URL: /api/v1.0/compliance-remediation/compliance-block-executions?deviceExecutionId=<>

   Método: GET



Resultados da Execução do Bloco de Conformidade

3. Verifique se o bloco tem sub-hierarquias ou uma única hierarquia e verifique se as regras estão configuradas de acordo com a hierarquia.



Resultados da Execução do Bloco de Conformidade

4. Verifique se o analisador TTP está extraindo o valor da configuração do dispositivo executando o seguinte script python:

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

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

```
"""

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

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

Monitorando logs de conformidade

Env. de nó único:

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

Env. Kubernetes de vários nós:

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

Monitoramento de registros Kibana:

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.