BPA User Guide Configuration Compliance and Remediation v5.1

简介

配置合规性和补救(CnR)应用允许网络操作员对从配置块构建的自定义策略执行设备配置合规性检查。操作员使用系统手动定制或自动生成所选设备配置的配置块。用户还可以建立适用于这些块的规则，规则条件可能源自从RefD应用程序获得的值。操作人员可以方便地按照时间表执行合规性检查或立即启动检查。

该应用拥有直观的控制面板，可全面概述违规情况，提供设备和配置块级别的摘要和详细视图。

该应用包括用于处理合规性违规的强大补救框架。此框架利用工作流程和模板(包括称为金牌配置模板(GCT)的配置模板和流程模板)来简化补救流程。与合规性检查类似，补救任务也可以编程为按时间表运行或立即触发以迅速解决违规问题。

下一代（下一代）门户的Compliance and Remediation控制面板具备多项功能，旨在增强网络安全管理、简化合规程序以及简化补救活动。控制面板提供资产和策略合规性的全面摘要，使网络运营商可以轻松评估其网络的运行状况，并确保设备符合严格的安全协议。

配置块可以自动生成并手动编辑或添加，从而在自动化和自定义之间实现平衡。系统精确识别配置块和精细的访问控制机制，包括传统和现代接口上的详细用户、组和权限设置，确保网络配置保持安全并掌握在受信任人员手中。这些功能为希望保持高网络合规性和安全标准的组织提供了强大的工具集。

新特性

引入了以下主要功能和增强功能：

- 一个全面的报告控制面板，用于生成、查看和下载合规性报告
- 能够通过上传设备配置执行离线合规性审核，而无需使用资产管理器自行激活设备
- 能够在块配置中配置模式以屏蔽敏感设备配置数据
- 能够将策略和资产合规性摘要网格数据导出为CSV文件
- 根据设备运行配置查看和比较生成的补救配置
- 块中的增强功能，可在配置存在时支持引发违规
- 在策略创建和编辑页面中启用互联用户体验，以交叉启动子组件，如块创建页面
- 合规性作业增强创建和编辑页面以交叉启动到策略编辑页面

组件

合规性和补救支持以下控制器和设备类型：

控制器	操作系统类型
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/交换矩阵v12.2.2）	NX-OS
思科Catalyst中心(2.3.5)	IOS XE、IOS XR。仅限经过验证的合规性
FMC(7.2.5)	FX-OS(FTD)。 仅限经过验证的合规性
直接到设备(D2D)	IOS XE、IOS XR、JunOS

注意：通过NSO控制器提供诺基亚SR-OS支持仅适用于配置合规性功能。Nokia设备不支持补救。

注意：合规性功能适用于思科命令行界面(CLI)格式和Juniper和Nokia设备的类似YAML格式的设备配置。目前，框架不支持Netconf、JSON、XML等其他格式。

作为v5.0版本的一部分，已弃用合规性和补救(CnR)传统应用程序。所有CnR功能现已完全集成并在下一代门户中可用。

假设和前提条件

要有效使用CnR使用案例，需要满足以下前提条件。

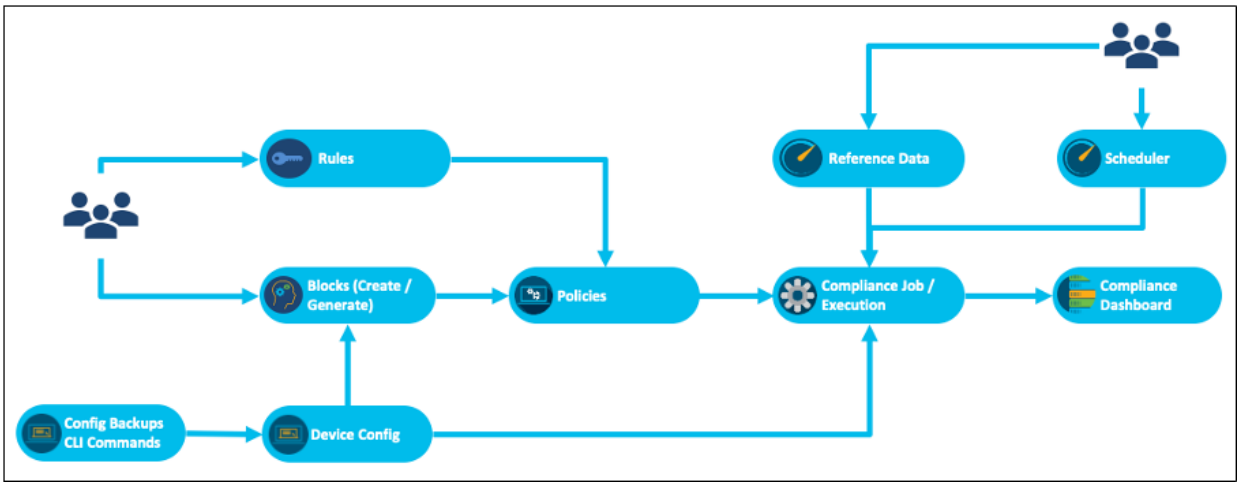
- 应上传CnR使用案例的订用授权密钥。
- 相关控制器和设备应已入网并作为BPA资产管理器的一部分提供。有关详细信息，请参阅BPA用户指南中的Asset Manager部分。
- 入网资产需要根据客户需求在下一代门户中分组为资产组。

合规性控制面板

合规性控制面板提供所选时间所有设备上的违规的汇总视图。默认显示当前月份的数据。用户可以更改时间窗口，以查看有关违反合规性的历史数据。当前月份是默认的选定视图。

注意：传统UI中已弃用的合规性控制面板已删除，不再可用。应使用下一代门户中可用的控制面板。

配置合规性流程图



配置合规性组件概述

针对资产列表为策略运行合规性作业时，控制面板中显示的合规性违规会被填充。通过添加块配置列表以及必要的合规性规则来创建合规性策略。合规性规则可以检查从RefD应用程序获取其数据的静态值或动态变量。合规性作业可以按需运行，也可以作为一次性或定期计划运行。

配置合规性包括以下重要功能：

- 阻止创建:使用模板文本解析器(TTP)模板手动创建或自动生成块。它们可以是静态的或动态的（带有变量）。
- 规则创建:规则将验证块中的变量。在执行期间，可以静态设置规则值，也可以从参考数据(RefD)系统动态检索规则值。
- 策略创建:通过选择块列表和相应的规则来创建策略。规则的数据可以是在运行时从RefD框架动态获取的静态数据。
- 合规性作业创建:通过选择要运行合规性检查的策略和资产组（包含资产列表），可以创建合规性作业。用户可选择从备份框架中检索设备配置，或在执行期间通过设备上的进程模板运行实时命令。从备份获取配置有助于离线审核设备，而无需连接到实时设备。可以计划作业或按需运行作业。
- 违反合规性:在控制面板上查看合规性违规。

资产合规性摘要

Asset Compliance Summary选项卡是一项基本功能，旨在全面概述网络中所有设备的合规性违规情况。此选项卡允许用户快速确定合规性问题，确保所有设备符合既定策略和标准。该界面具备强大的过滤和搜索功能，便于导航和分析合规性数据。

主要特点

- 每个设备的违规摘要:该选项卡显示每个设备的合规性违规的摘要视图，使用户可以快速了解按严重性级别（如严重、高、中和低）分类的总体合规性状态。
- 详细的违规信息:对于每个设备，弹出窗口提供关于违规策略的详细信息，用户可以进一步深入查看导致违规的块和配置行。

查看资产合规性摘要

- 高级过滤选项:位于选项卡顶部和左侧的过滤器允许用户缩小显示在网格中的数据的范围。用户可以按日期范围、资产组、产品系列等进行过滤，从而实现对合规性数据的集中分析。
- 搜索功能:搜索字段可用于进一步细化网格中的数据。用户可以通过输入相关关键字或短语来快速定位特定设备或按控制器进行管理。
- 可定制的日期范围:默认情况下，在日期范围筛选器中选择当前月份，提供最新的符合性数据。但是，用户可以自定义日期范围以查看数据。
- 过滤器:可以使用多个过滤器，如产品系列、资产组和审核类型。应用过滤器以刷新网格。

资产合规性摘要

- 导出为CSV:一项功能，可帮助用户获取资产配置合规性的本地副本，以用于离线分析、报告

和存档目的。要将数据导出为CSV文件，请从更多选项图标中选择Export as CSV。下载的CSV文件包含当前显示在网格中的数据，并遵循任何应用的过滤器。

资产合规性摘要：导出为CSV

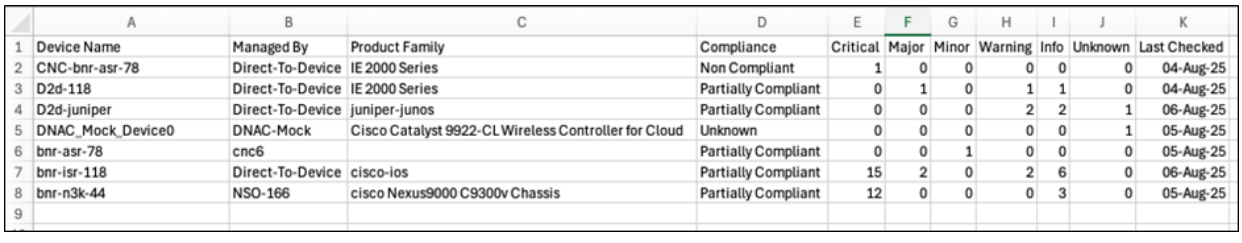
资产合规性的CSV文件详细信息

CSV文件包括Asset Compliance Summary网格中可见的所有列，例如设备名称、控制器实例（管理者）、设备的产品系列、设备合规性状态、按严重性划分的违规计数（例如，严重、主要、次要、警告、信息、未知）以及最后检查设备合规性的日期。

如果网格具有分页，则导出包括跨页的所有记录，而不仅仅是可见的页。

打开和使用CSV文件以实现资产合规性

1. 在Excel或任何兼容的电子表格应用程序中打开下载的CSV文件。
2. 确保内容与“资产合规性摘要”网格中显示的内容匹配，包括筛选的结果。



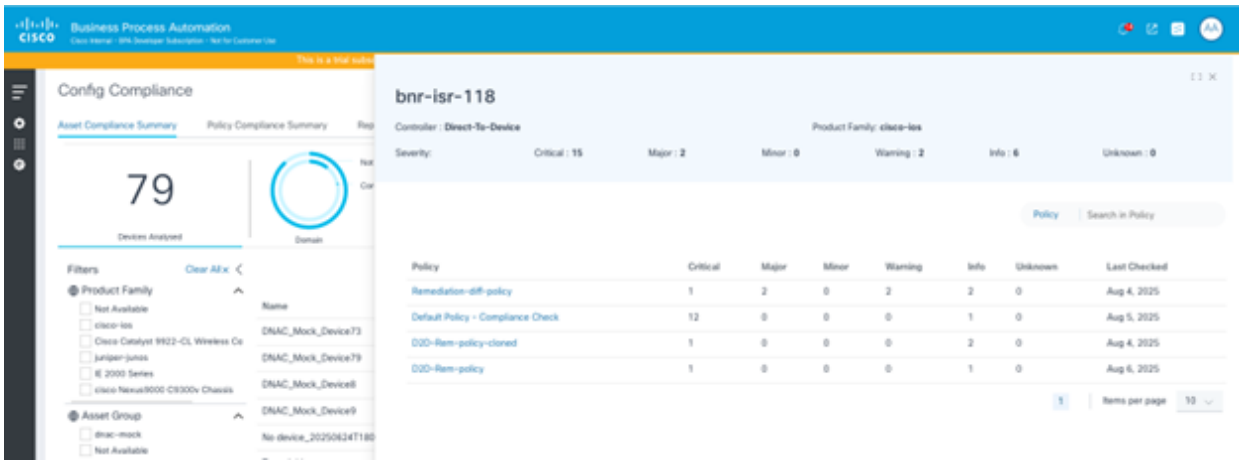
	A	B	C	D	E	F	G	H	I	J	K
1	Device Name	Managed By	Product Family	Compliance	Critical	Major	Minor	Warning	Info	Unknown	Last Checked
2	CNC-bnr-asr-78	Direct-To-Device	IE 2000 Series	Non Compliant	1	0	0	0	0	0	04-Aug-25
3	D2d-118	Direct-To-Device	IE 2000 Series	Partially Compliant	0	1	0	1	1	0	04-Aug-25
4	D2d-juniper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

资产合规性摘要：在Excel应用程序中打开的CSV文件

按策略查看资产合规性摘要

点击Asset Compliance Summary网格中的某一行，将显示资产违规的详细信息，按设备验证所依据的不同策略分类。此视图为用户提供了一个详细的视图，用于按严重性查看每个策略中的违规计

数。



资产合规性摘要：按策略列出的合规性摘要

注意：应该注意以下几点。
- Policy列中的超链接将用户定向到Policy details页面
— 点击某一行将显示所选策略的Violation details页面

查看违规详细信息

Violation Details页面显示设备配置上覆盖的块和规则级违规。此外，用户还可以查看块配置和建议的补救配置。

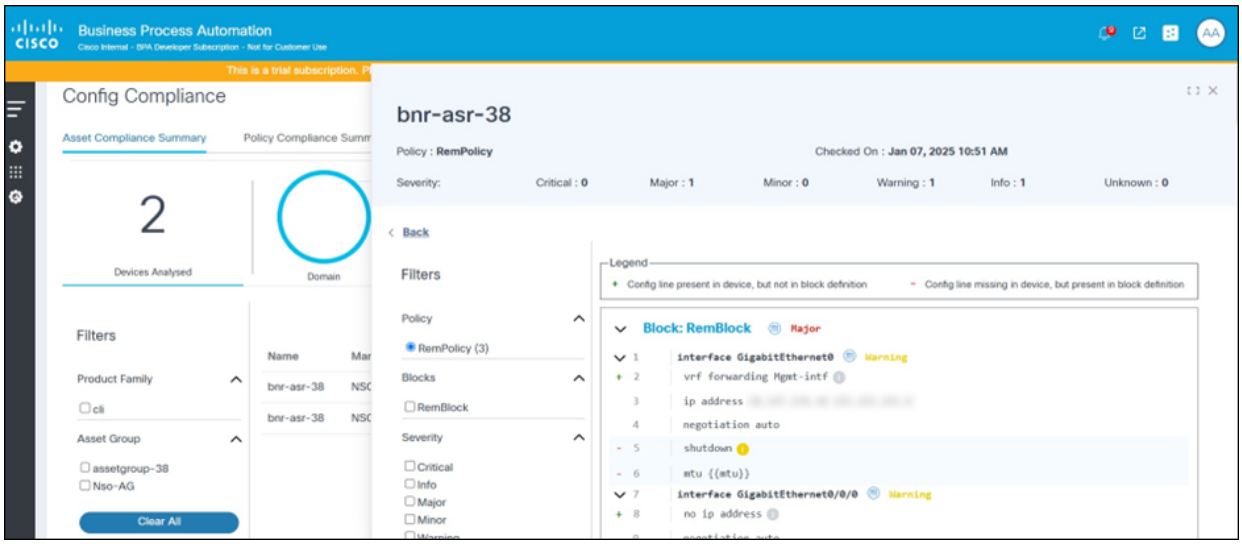
要从资产合规性摘要页面以及策略级别拆分查看Violation Details页，请执行以下操作：

1. 在“资产合规性”网格中选择行。系统随即会显示一个弹出窗口。网格按策略显示合规性详细信息的细分。
2. 在网格中选择一行。系统将显示Violation Details页面。

要从Policy Compliance Summary网格中查看Violations Details页，请执行以下操作：

1. 选择Policy Compliance Grid。
2. 选择行>受影响的资产网格。
3. 选择一行。系统将显示Violations Details页面。

Violations Details页面的右侧显示设备配置块，并将违规叠加在其上。系统会根据相应的配置行列出违规。 在条件发生故障的情况下，违规功能区会提供规则名称、条件、预期配置（如规则中所定义）和从设备配置中检索到的配置的详细信息。



违反资产合规性

块符号

- 行上的“+”符号表示根据块配置，不需要该配置，但设备配置中还会有该配置。
- 针对某一行的“ — ”符号表示该配置按块配置进行配置，但在设备配置中缺失。

过滤器

页面左侧的过滤器部分允许用户执行以下操作：

- 更改策略；这将刷新页面并加载新选定策略的违规
- 选中Blocks复选框以查看与所选块相关的违规
- 选择Severity复选框以查看具有给定严重性级别的违规
- 选中Violation Type复选框以查看所选类型的违规：
  - 订单不匹配:设备配置行的顺序与块配置中定义的顺序不匹配
  - 缺少配置:查看根据块配置预期但设备配置中缺少的配置行
  - 其他配置:查看根据块配置不预期但额外出现在设备配置中的配置行
  - 规则失败:规则中的一个或多个条件失败。
  - 缺少块：整个设备配置块缺失或与定义的块配置不匹配。
  - 跳过的块:由于不符合块过滤器条件，因此跳过此配置块。

查看和比较补救配置

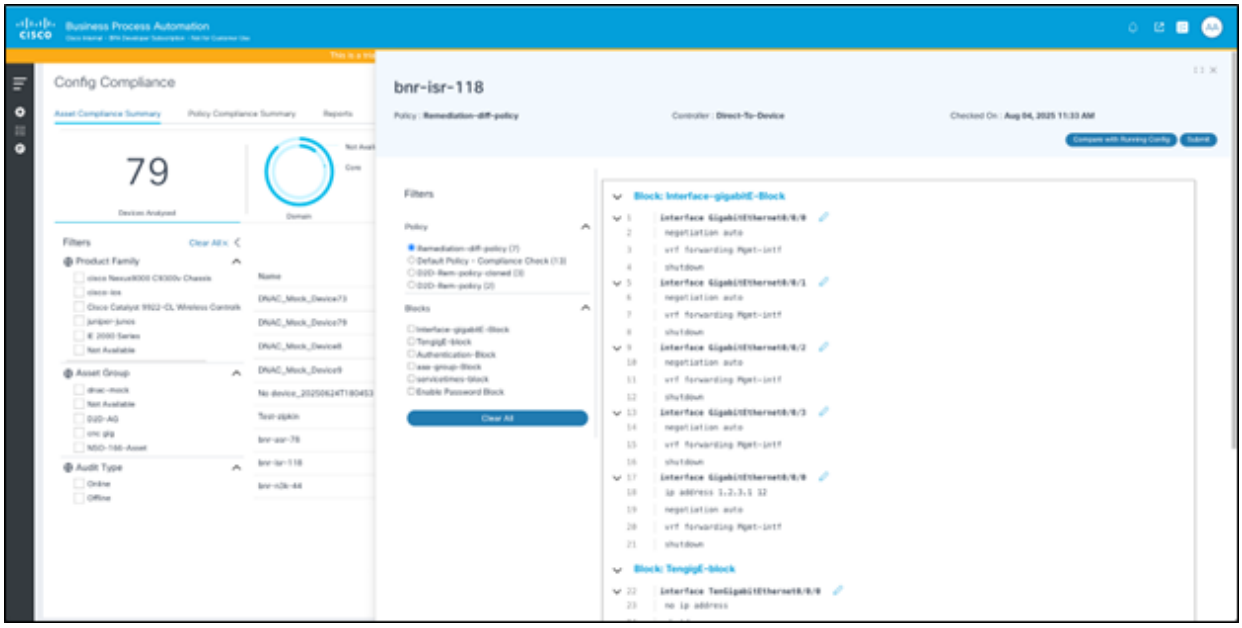
Remediation Config页面显示给定策略中每个块的所选设备生成的配置。生成配置时，会考虑策略中存在的阻止和规则详细信息，以及在合规性执行期间检索的设备配置。用户可以选择在同一页面中更新配置。可使用补救作业功能将此生成的配置推送到设备。此外，此页面为用户提供了一个选项，用于将生成的配置与当前设备的运行配置进行比较。用户可以指定一个或多个命令来检索当前设备配置。

要从资产合规性网格中查看Remediation Config(补救配置)页：

1. 点击Asset Compliance Summary选项卡。
2. 在“操作”列的资产合规性网格中，选择更多选项图标> 查看补救配置。系统将显示Remediation Config页面。

要从策略合规性网格中查看Remediation Config页，请执行以下操作：

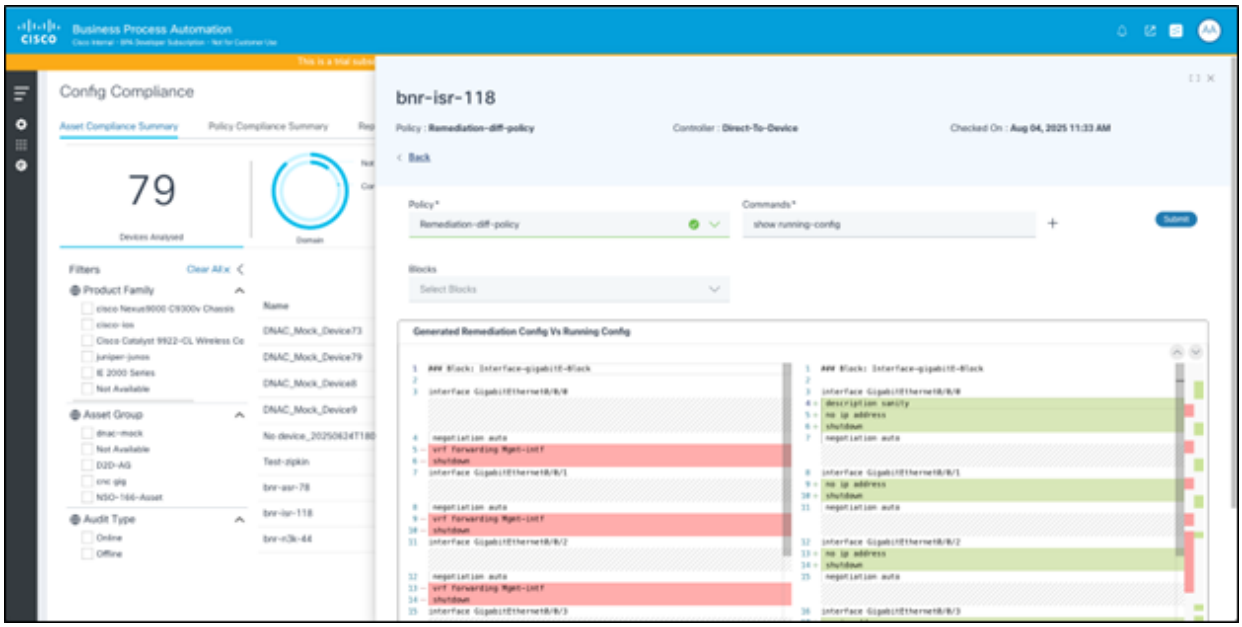
1. 单击Policy Compliance Summary选项卡。
2. 在策略符合性网格中，选择所需的行。系统随即会显示受影响的资产(Affected Assets)网格。
3. 在Action列中，选择More Options图标> Select View Remediation Config。系统将显示Remediation Config页面。



补救配置页

Remediation Config页面显示以下内容：

- 生成的补救配置:生成的配置会显示在页面右侧，用户还可以选择编辑配置块并提交要保存的更改
- 过滤器:过滤器可用于选择策略，然后选择一个或多个块以查看相应的生成配置
- 请比较运行配置:单击Compare with Running Config以显示详细页面，该页面允许用户将生成的配置与设备的运行配置进行比较



“与运行配置比较”页

Compare with Running Config页显示以下内容：

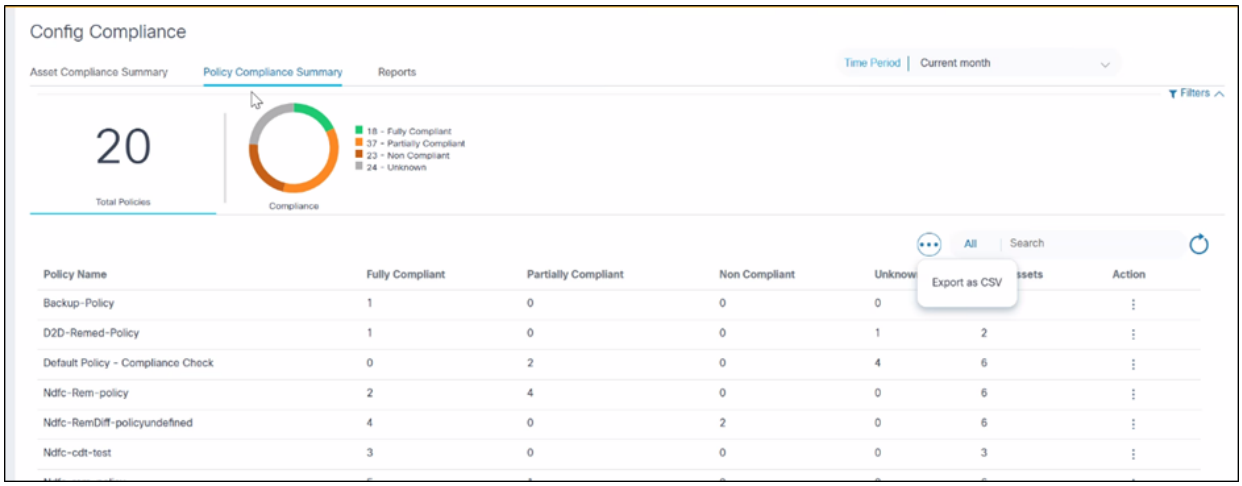
- 用于选择策略的选项:上一页中选定的策略已预先选定。
- 一个文本框，用于输入要在设备上执行的一个或多个命令
- 一个Submit按钮，用于在设备上运行命令并检索配置
- 用于查看和筛选块的选项:默认情况下，会显示策略中的所有块；用户可以根据需要选择单个块
- 配置比较查看器并行显示生成的配置和设备配置，并突出显示差异

策略合规性摘要

Policy Compliance Summary选项卡旨在根据定义的策略提供设备合规状态的清晰而简明的概述。此选项卡可帮助用户快速评估合规性形势并确定需要关注的领域。该选项卡根据设备的合规性状态对设备进行分类，便于您轻松了解并简要管理合规性。

合规性状态：

- 完全合规:所有设备均满足相应策略的所有合规性规则。
- 部分合规:有些设备符合规则，但有些设备不符合规则。
- 不合规:没有设备符合策略。
- 未知:由于网络连接存在问题或备份不可用，因此无法检查策略是否一致。



CSV导出的策略合规性摘要

导出为CSV以实现策略合规性

导出为CSV功能可帮助用户获取策略合规性的本地副本，以用于离线分析、报告和存档目的。要将数据导出为CSV文件，请从更多选项图标中选择Export as CSV。下载的CSV文件包含当前显示在网格中的数据，并遵循任何应用的过滤器。

策略合规性的CSV文件详细信息

CSV文件包括策略名称、已验证资产的总计数以及按合规状态（即，完全合规、部分合规、不合规和未知）细分的计数。 如果网格有分页，导出将包括所有页面中的所有记录，而不仅仅是当前页面上显示的记录。

打开和使用CSV文件以实现策略合规性

1. 在Excel或任何兼容的电子表格应用程序中打开下载的CSV文件。
2. 确保内容与“策略合规性摘要”网格中显示的内容匹配，包括过滤的结果。

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

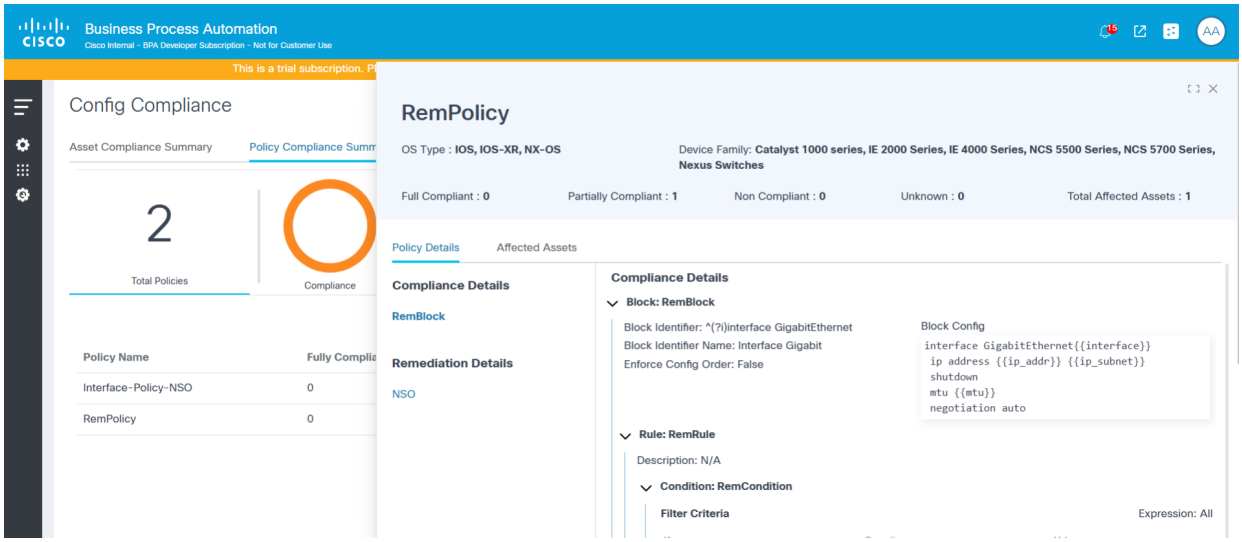
策略合规性：策略详细信息

查看策略详细信息

要查看策略详细信息，请执行以下操作：

1. 从操作列下的更多选项图标中选择策略。
2. 选择查看策略详细信息。系统随即会显示Policy Details页面。

注意：Policy Details页是所有策略信息（包括块、规则和条件）的只读视图。用户可以点击直接导航到相关块的页面中的超链接。



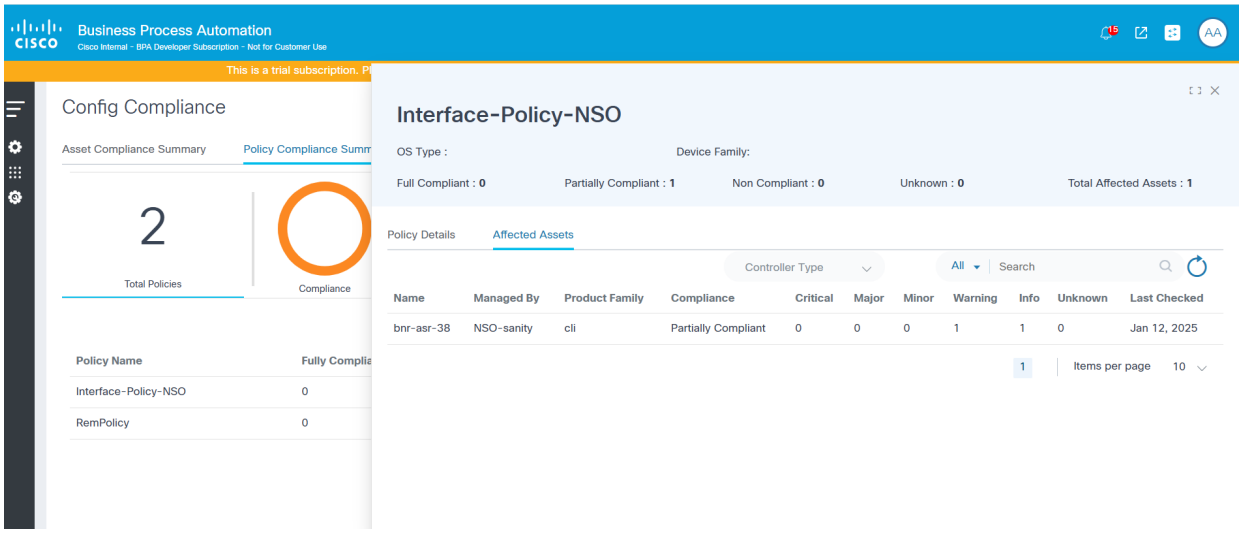
策略合规性：策略详细信息

查看受影响的资产

Affected Assets选项卡显示每个策略下分析的资产列表以及按严重性划分的违规计数。可以使用Controller Type下拉列表和搜索框过滤设备。

要从Policy Compliance Summary选项卡查看受影响的资产，请执行以下操作：

1. 选择一行。Compliance Policy窗口打开。
2. 单击Affected Assets选项卡。



策略合规性：受影响的资产

注意：Affected Assets选项卡提供用于打开View Violation Details页和View Remediation Config页的操作。有关详细信息，请参阅资产合规性摘要。

报告

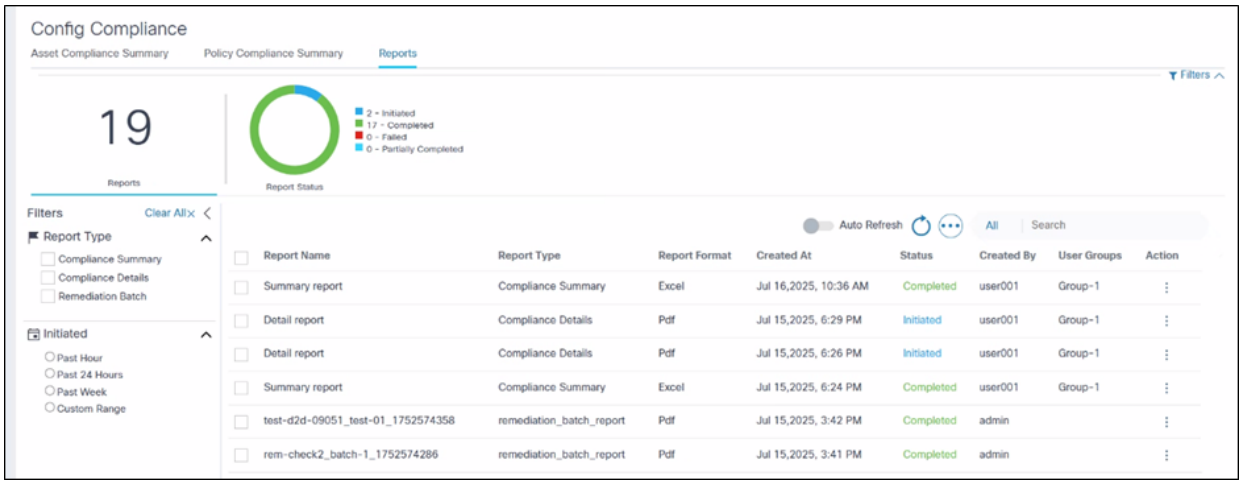
报告部分旨在提供关于设备合规性的全面见解、识别违规行为并促进补救工作。该应用程序提供了一个用户友好的界面，可用于生成、查看、下载和管理各种类型的合规性报告。

报告控制面板

Reporting Dashboard是所有合规性报告活动的中心中心。用户可以通过此单一界面高效地管理其报告。Reports Dashboard上可用的主要功能包括：

- 查看报表:用户可以查看所有生成的报告的列表，包括其名称、类型、关联策略、格式、创建日期和当前状态（例如，已启动、已完成、失败、部分已完成）
- 下载报告:报告一旦生成，就可以下载以进行离线分析或存档；“操作”(Action)列提供下载选项
- 删除报告:用户可以从控制面板中删除旧的或不必要的报告，从而帮助维护一个干净有序的报告环境
- 过滤和搜索:控制面板提供了广泛的过滤选项，允许用户根据报告类型（如Compliance Details、Compliance Summary、Remediation Batch）、策略和启动状态（如Past Hour、Past 24 Hours、Past Week、Custom Range）等条件快速查找特定报告；酒店还设有搜索栏
- 报告状态监控:可视摘要（如饼图）指示报告的状态，显示有多少报告已启动、已完成、失败或部分已完成。

Reporting dashboard是Compliance and Remediation控制面板上Reports选项卡下的登录页。



报告控制面板

- 可用的报告类型包括：
  - 合规性摘要报告
  - 合规性详细报告
  - 补救批处理报告
- 使用过滤器选择以下项：
  - 报告类型
  - 策略
  - Initiated Time period（根据所选的时间范围过滤报告列表）
- 用于自动刷新报告列表的选项

报告配置

报告配置使管理员能够根据部署和业务需求配置与报告相关的关键参数。以下参数可用于配置：

- 自动删除早于（天）的报告:任何比此持续时间更早的报告都将从系统中删除
- 合规性摘要报告中每个策略要选择的最大块数:帮助将Excel文件中的选项卡数量限制为可读数
- 要在合规性详细报告中选择的最大资产:帮助限制为给定详细报告生成的PDF文件数量

合规性作业列表

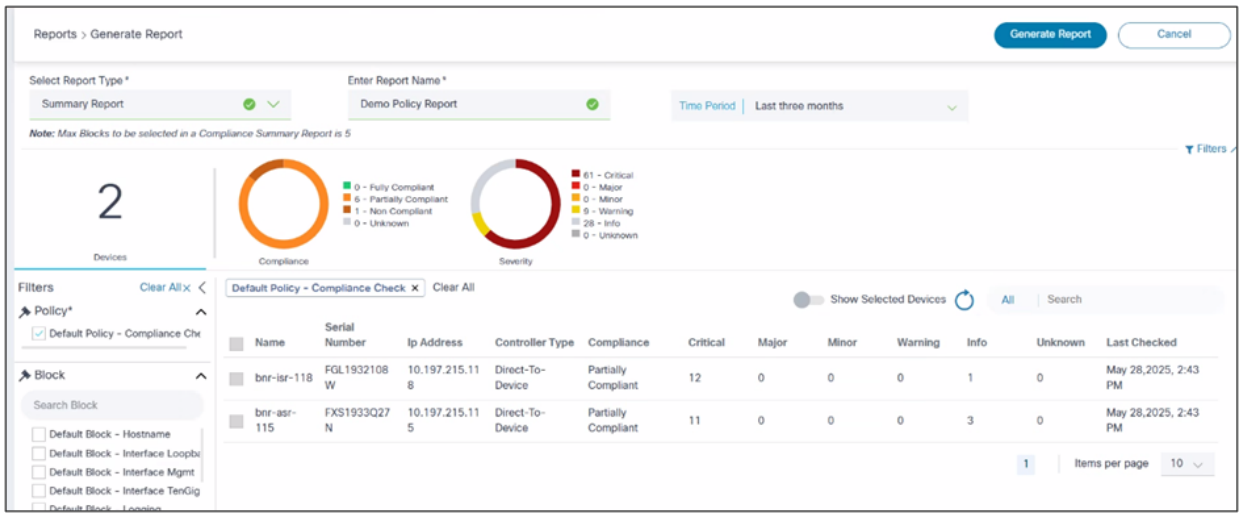
生成报告

该应用程序提供用于生成新合规性报告的专用界面，允许用户选择报告类型、定义范围以及应用特定过滤器。报告生成过程通过“报告”(Reporting)控制面板页面下的“生成报告”(Generate Report)操作启动。

报告生成的主要方面包括：

- 选择报告类型:用户可以在以下不同报告类型之间进行选择
  - 总结报告:提供所选策略的所有设备的合规性概述
  - 详细报告:提供更精细的详细视图，提供关于每个设备特定违规的深入信息
- 报告命名:用户需要提供所生成报告的相关名称
- 时间段选择:可以针对特定时间段（如“当前月份”或自定义范围）生成报告，以重点关注最近的合规性数据
- 应用过滤器:综合过滤选项使用户能够缩小报告的范围
  - Policy（策略）：选择要包括在报告中的一个或多个合规性策略。策略选择是必需的
  - 阻止:在选定的策略中，选择要包括在报告中的特定配置块。块选择是可选的
  - 资产组:用户可以通过选择一个或多个资产组来过滤范围内的资产
- 资产选择:这仅适用于详细报告
  - 用户可以选择应为其生成报告的特定设备
  - 资产表显示了详细信息，例如名称、序列号、IP地址、管理者和当前合规状态，以及不同严重性级别的计数

要生成合规性摘要报告，请执行以下操作：

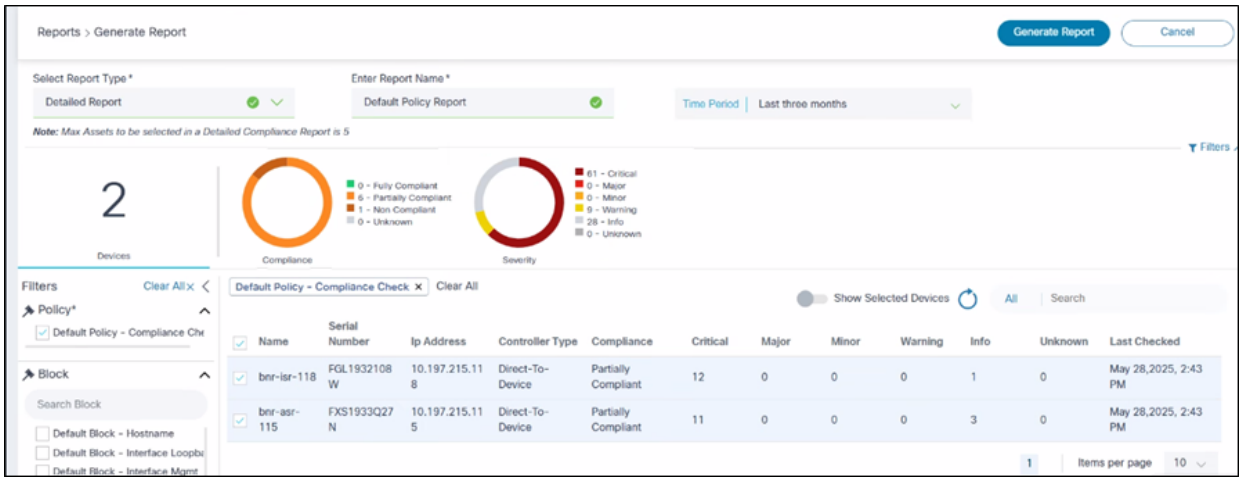


生成摘要报告

1. 在选择报告类型下拉列表中选择摘要报告。
2. 输入报表名称。
3. 选择时间范围。系统将根据此选择列出策略和块。
4. 选择策略。还可以选择其他策略。
5. 或者，选择Blocks。如果未选择任何内容，则包括所有块。
6. 选择所需的资产组、合规性状态和严重性级别。
7. 单击 Generate Report。

- 在报告列表页面中，报告状态设置为Initiated
- 完成后，状态更改为已完成。如果某些子报告失败，状态将更改为部分完成
- 如果整个报告生成失败，将显示通知并将状态更改为“失败”
- 完成后，即可使用下载选项。用户可以下载包含Excel报告的zip文件

要生成合规性详细报告，请执行以下操作：



生成详细报告

1. 在选择报告类型下拉列表中选择详细报告。
2. 输入报表名称。
3. 选择时间范围。系统将根据此选择列出策略和块。
4. 选择策略。还可以选择其他策略。
5. 或者，选择Blocks。如果未选择任何内容，则包括所有块。
6. 选择所需的资产组、合规性状态和严重性级别。
7. 从网格中选择所需的资源。用户可以选择“全选”设备和“显示所选设备”。
8. 单击 Generate Report。

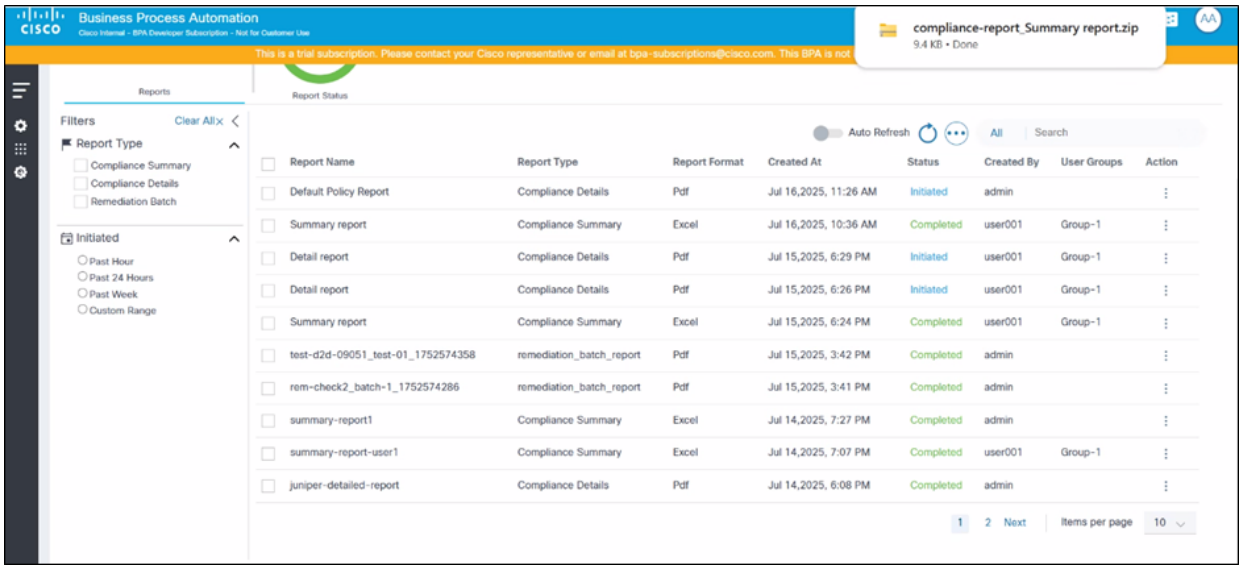
- 在报告列表页面中，报告状态设置为Initiated
- 完成后，状态更改为已完成。如果某些子报告失败，状态将更改为部分完成
- 如果整个报告生成失败，将显示通知并将状态更改为“失败”

下载和查看报告

已完成的报告可使用报告控制面板网格中所需行中的下载图标下载。

了解配置合规性摘要报告

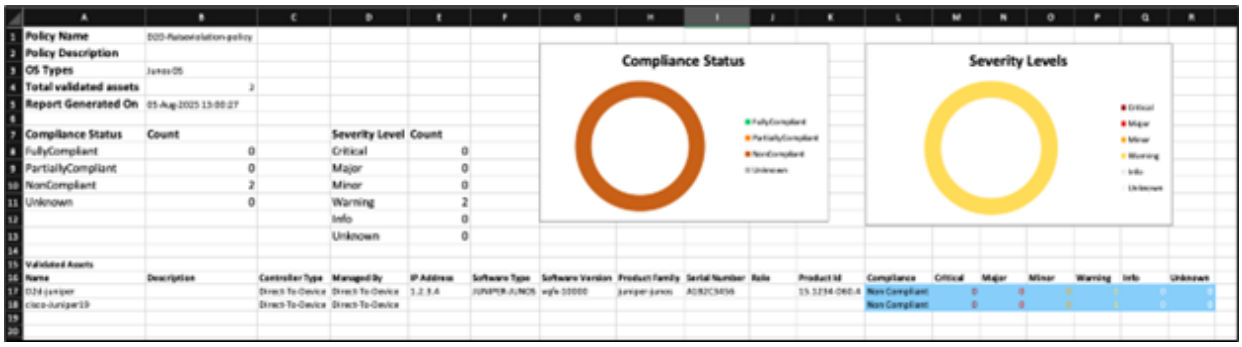
“合规性摘要”报告是包含单个PDF报告的zip文件，每个设备生成一个PDF。此报告类型提供每个策略的合规性违规的概述，以及针对设备的块级向下钻取映射违规详细信息。



合规性摘要报告

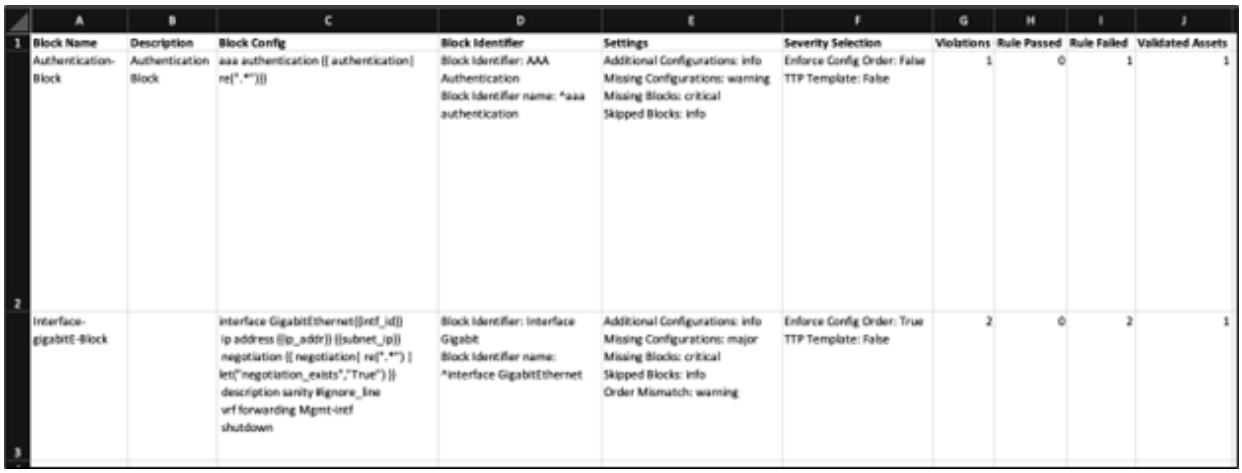
每个Excel报告包含以下工作表，并提供以下信息：

- 策略摘要:
  - 概述详细信息，例如策略名称、说明、操作系统类型和验证资产总数
  - 按合规性状态（如完全合规、部分合规、不合规和未知）拆分的已验证资产计数的网格和图表视图
  - 按严重性级别划分的总违规计数网格和图表视图（例如，严重、重大、次要、警告信息和未知）
  - 包含设备详细信息、合规性状态和每个严重性级别的违规计数的资产网格



策略摘要表

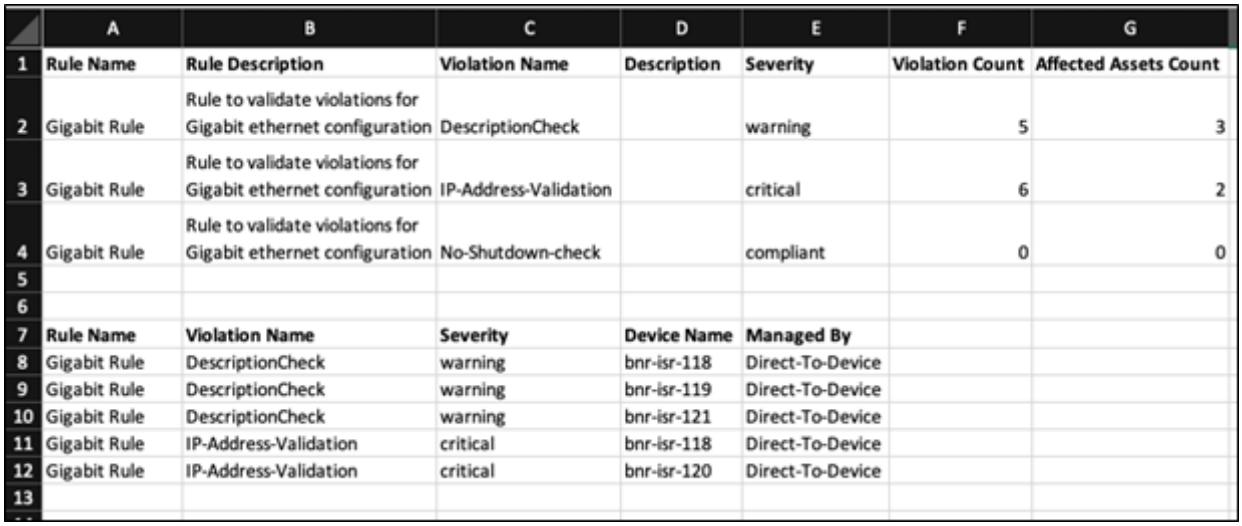
- 阻止摘要:
  - 阻止详细信息，如阻止名称、说明、阻止配置、阻止标识符详细信息和阻止违规严重性设置
  - 给定块的违规、通过的规则、失败的规则和已验证资产的计数



	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

阻止摘要工作表

- 每个块的规则和违规详细信息：
- 违规级别网格显示规则名称、说明、违规名称、说明严重性级别、在资产中看到的违规计数以及受影响的资产计数的列表
- 设备级网格显示规则、违规、严重性、设备名称和控制器名称（受管）之间的映射

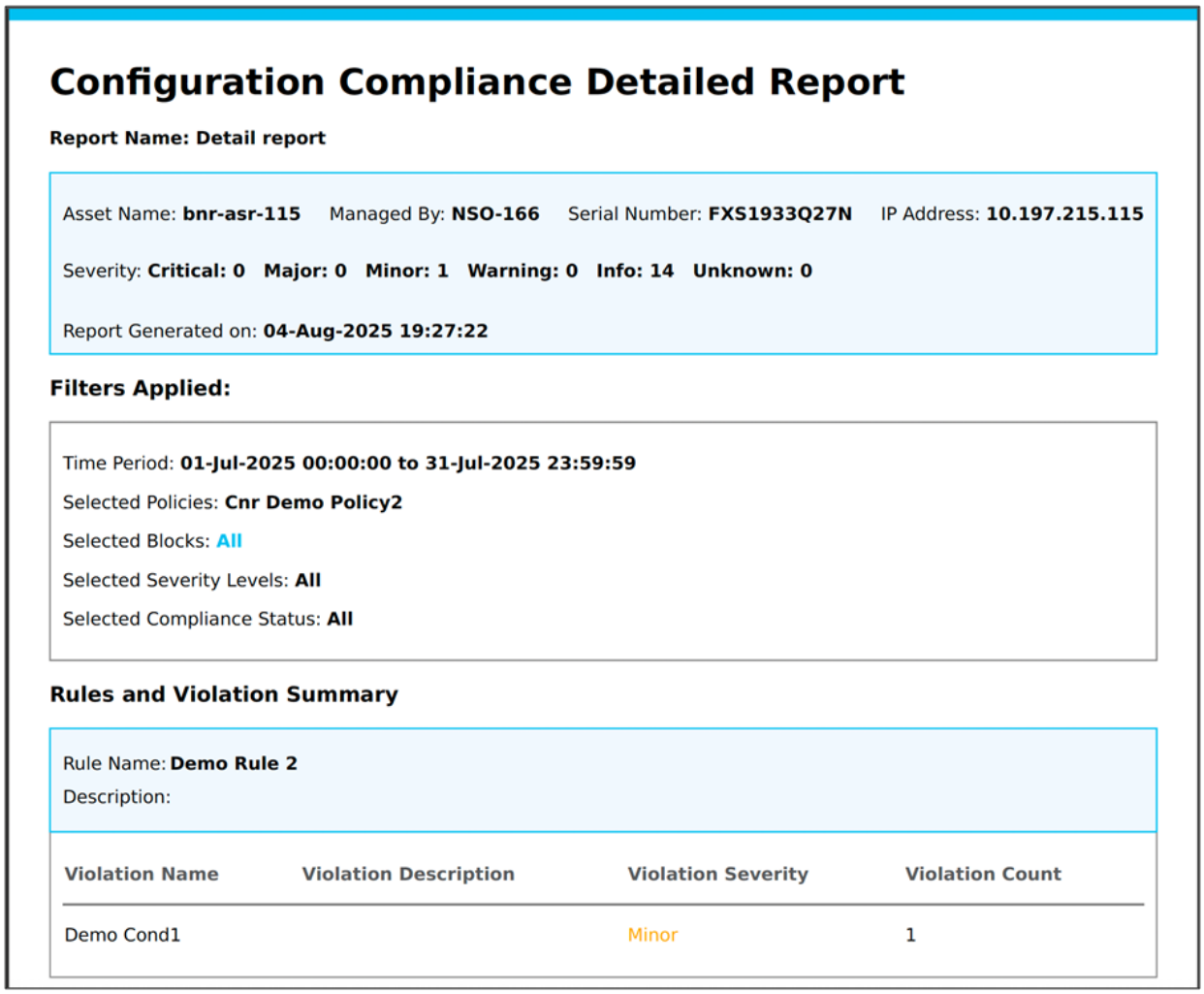


	A	B	C	D	E	F	G
1	Rule Name	Rule Description	Violation Name	Description	Severity	Violation Count	Affected Assets Count
2	Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	DescriptionCheck		warning	5	3
3	Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration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

合规性详细信息报告

合规性详细信息报告包含以下信息：

- 报告名:标识报告的名称
  - 资产名称:指定为其执行合规性检查的设备
  - 其他资产详情:包括IP地址和序列号等详细信息（如果有）
  - 严重级别:提供按严重性级别划分的违规摘要计数
  - 报告生成时间:指示创建报告时的时间戳
- 应用的过滤器：概述用于生成特定报告的特定过滤条件的详细信息，以确保透明度和可复制性。这包括时间段、选定的策略、块、严重性级别和合规性状态
- 规则和违规摘要:列出已评估的每个规则，并提供为该规则找到的违规的摘要。摘要网格显示违规名称、说明、严重性和发生此违规的次数
- 违规详细信息:提供有关所选块的每个设备配置行的明确详细信息以及每行的违规详细信息



Configuration Compliance Detailed Report

Report Name: Detail report

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

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

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

Filters Applied:

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

Selected Policies: **Cnr Demo Policy2**

Selected Blocks: **All**

Selected Severity Levels: **All**

Selected Compliance Status: **All**

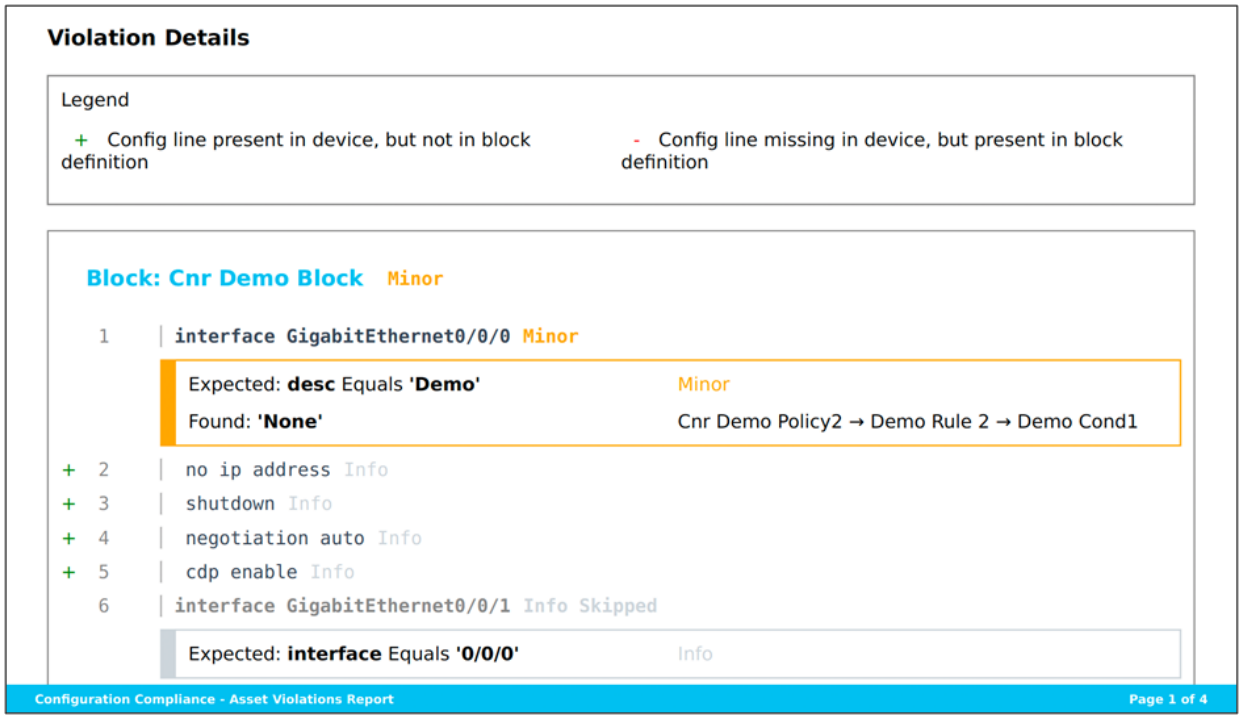
Rules and Violation Summary

Rule Name: **Demo Rule 2**

Description:

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

合规性详细报告 — 示例PDF第1页



Violation Details

Legend

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

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

Block: Cnr Demo Block Minor

```
  1   interface GigabitEthernet0/0/0 Minor
```

Expected: **desc** Equals **'Demo'** Minor

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

```
+ 2   no ip address Info
+ 3   shutdown Info
+ 4   negotiation auto Info
+ 5   cdp enable Info
  6   interface GigabitEthernet0/0/1 Info Skipped
```

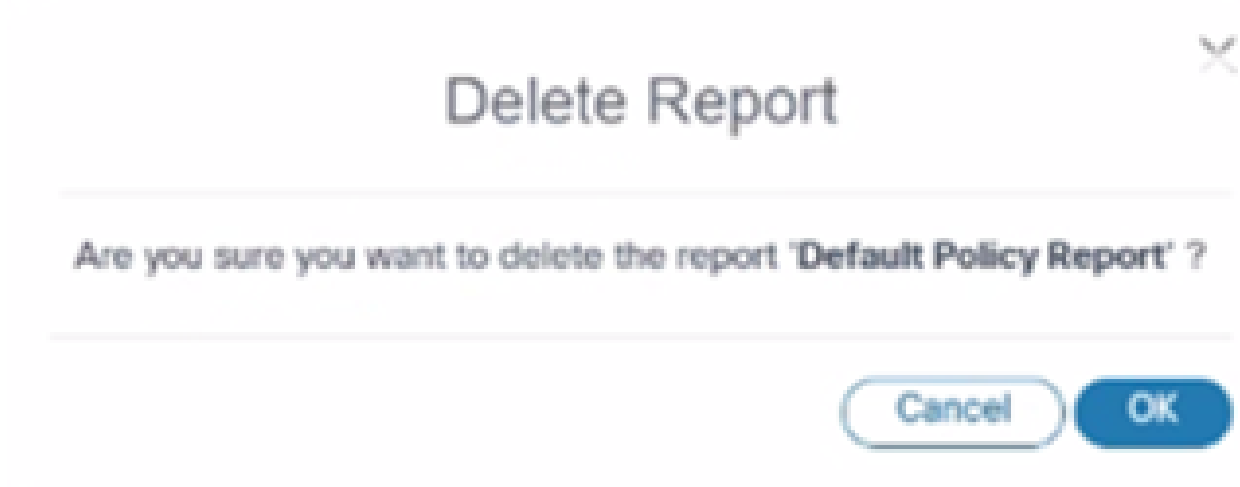
Expected: **interface** Equals **'0/0/0'** Info

合规性详细报告 — 示例PDF第2页

注意：从Remediation批处理页创建的补救批处理PDF报告也可以下载并从报告列表查看。

删除报告

通过选择Delete图标可以单独删除报告，也可以通过选中报告的复选框并选择更多选项图标> Delete来批量删除报告。



合规性作业列表

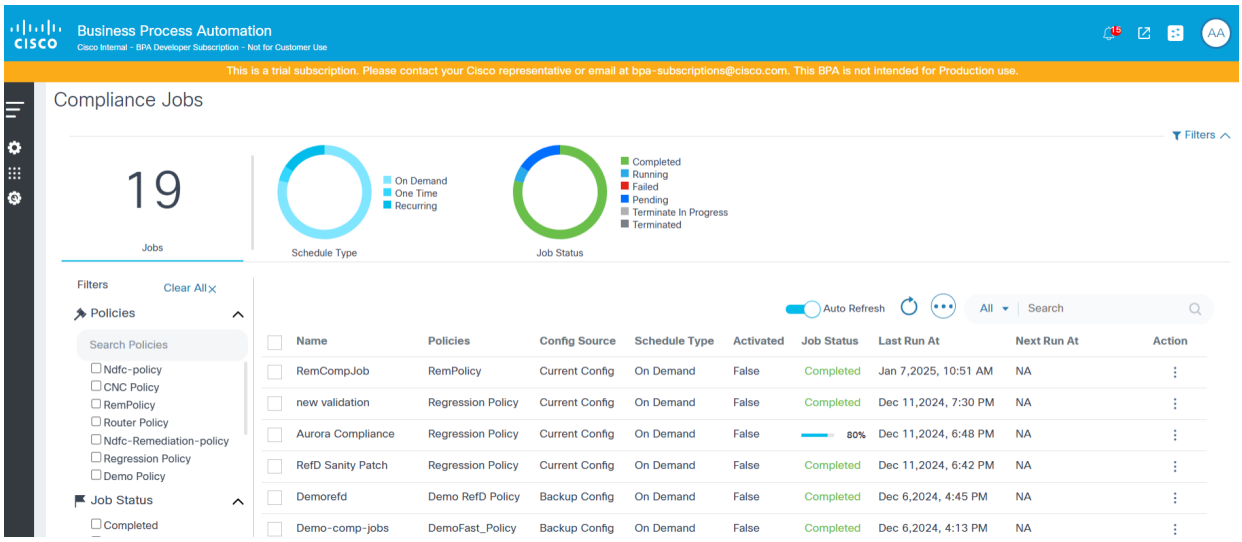
注意：删除报告仅会从报告控制面板中删除报告文件和条目；基本合规性执行详细信息将保留。

合规性作业

下一代门户中的“合规性作业”功能旨在帮助用户创建、管理和执行选定策略和资产组的合规性作业。这些作业可以计划定期运行或按需执行，从而确保对所有资产进行一致的合规性检查。

主要特点

- 列出合规性作业:查看所有已定义的合规性作业，以及脱机审核、筛选、创建、编辑、删除和执行作业的选项。
- 计划作业和按需作业:设置作业以计划的时间间隔运行，或者根据需要立即执行。
- 精细的访问控制：根据用户权限控制对合规性作业的访问权限，从而确保用户只能看到与他们有权访问的策略相关的作业。
- 过滤选项:按策略、作业状态、计划类型和日期范围过滤作业，以便轻松导航和管理。



合规性作业列表

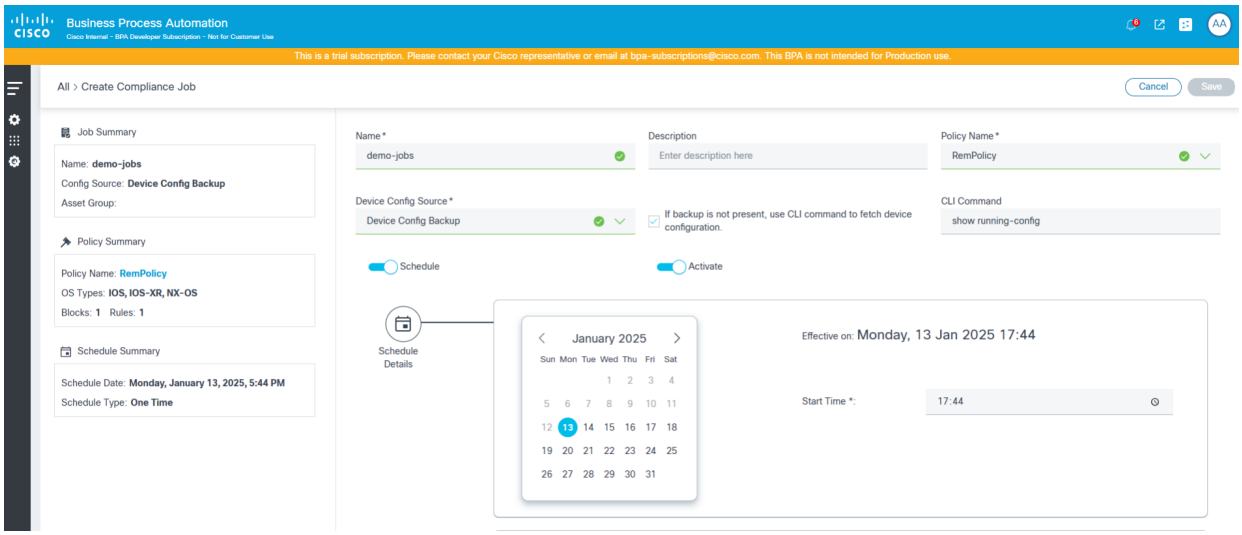
创建合规性作业

Compliance Job Create页包含以下属性：

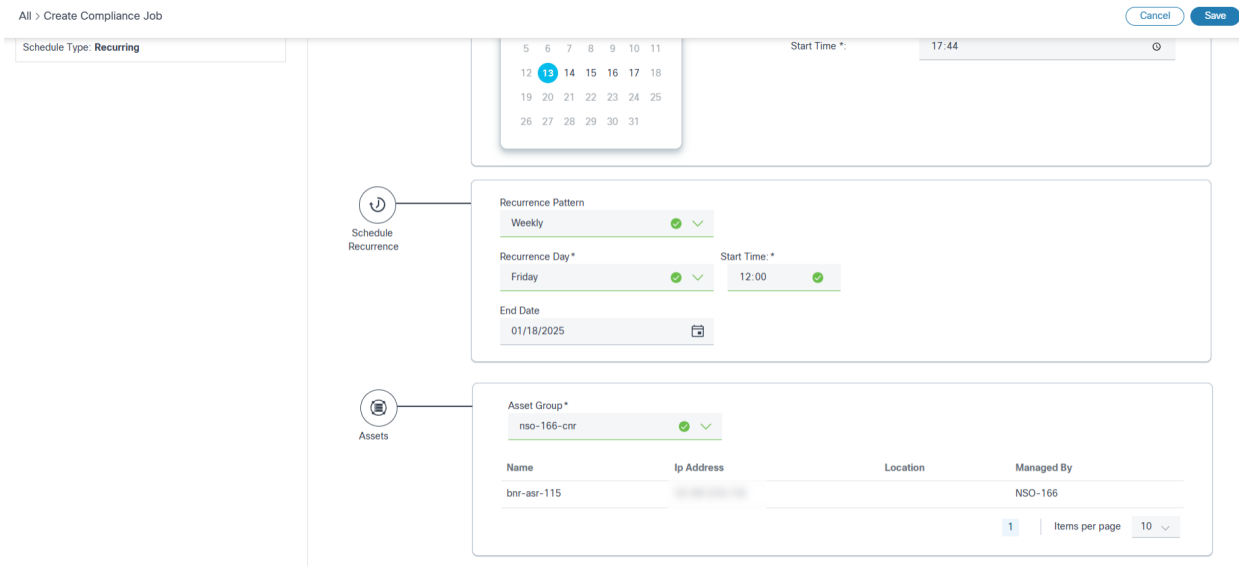
- 名称：作业的名称
- 描述:可选说明
- 策略名称：用于选择要运行的策略的下拉列表，可能按为登录用户配置的访问策略进行过滤
- 设备配置源:一个下拉列表，用于选择要为运行合规性作业获取设备配置的源（当前配置或设备配置备份），以及一个复选框，用于指示在没有备份时是否回退到CLI命令。

注意：仅当底层控制器支持备份功能时，Device Config Backup选项才起作用。

- 用户定义的变量:选定策略具有用户定义的变量时可用命名空间的可编辑文本框
- 计划详情:此部分用于选择各种计划参数，如开始和结束日期/时间、定期模式等。
- 资产:用于选择资产组的部分，用于标识要运行合规性的设备列表
- 进度:切换以启用或禁用按计划运行作业（一次性或重复）；如果禁用，作业将立即执行
- 处于活动状态:指示所选计划是否处于活动状态



创建合规性作业



创建合规性作业2

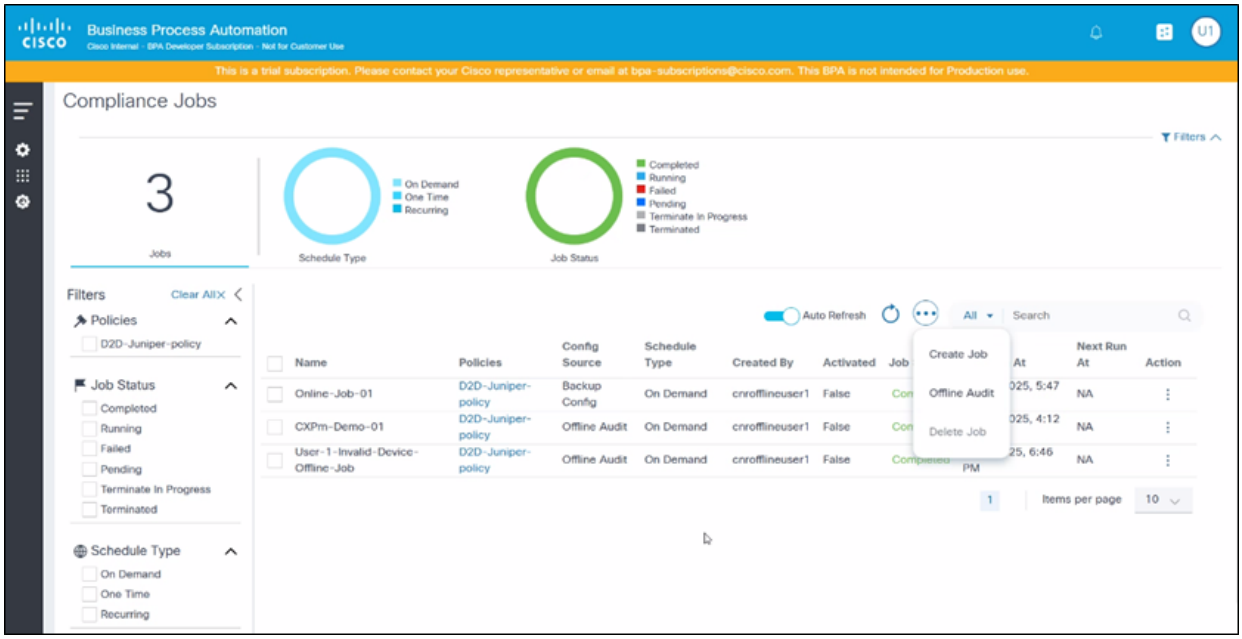
创建脱机审核作业

Compliance Jobs中的Offline Audit功能允许用户对设备配置执行合规性检查，而无需将设备注册到BPA。用户可以手动将设备配置上传为文件。可以将多个设备配置压缩并以zip文件的形式一起上传。上传后，将解析这些配置文件，并使用这些文件内容作为源创建合规性作业。然后，脱机审核的结果将与联机审核结果一起显示在合规性控制面板上。

Offline Audit页包含以下属性：

- 名称：作业的名称
- 描述:可选说明
- 策略名称：用于选择要运行的策略的下拉列表，可能按为登录用户配置的访问策略进行过滤
- 产品系列：用于选择产品系列的下拉列表

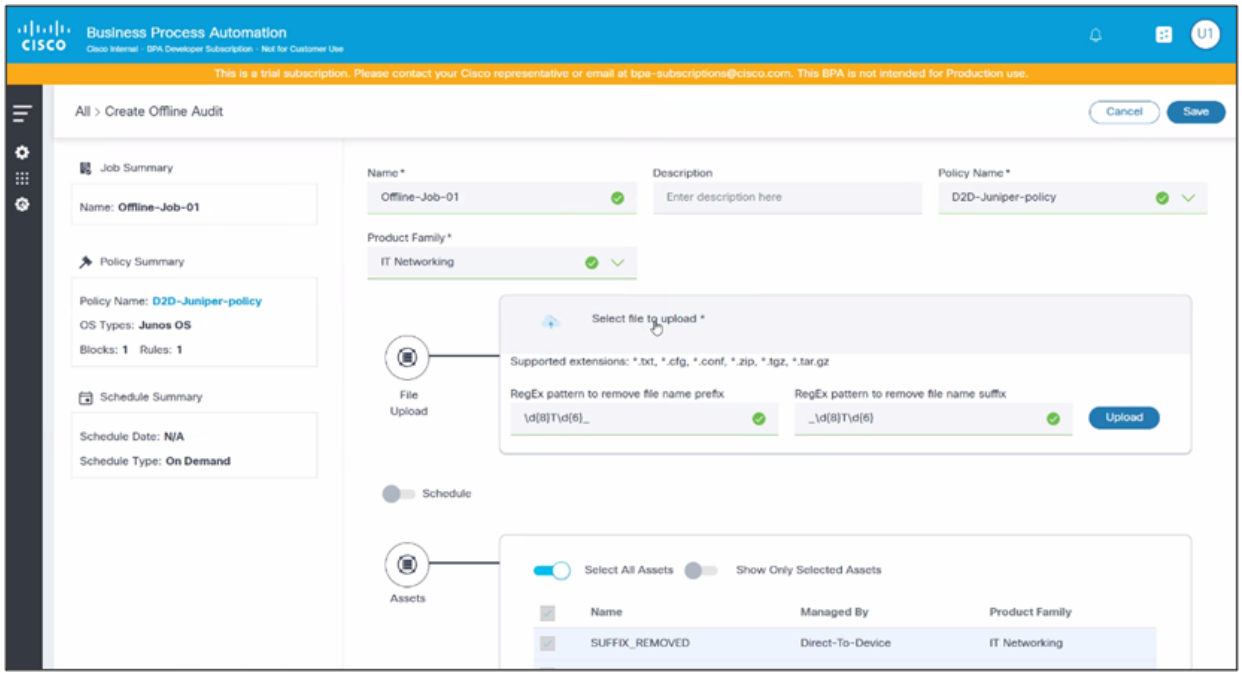
- 文件上传:使用离线审计功能手动上传配置文件；此操作通过上传界面完成，您可以在该界面中选择本地系统中的文件
- 进度:切换以打开计划
- 资产:按上传的文件内容显示设备列表



选择脱机审核

要创建脱机审核作业，请执行以下操作：

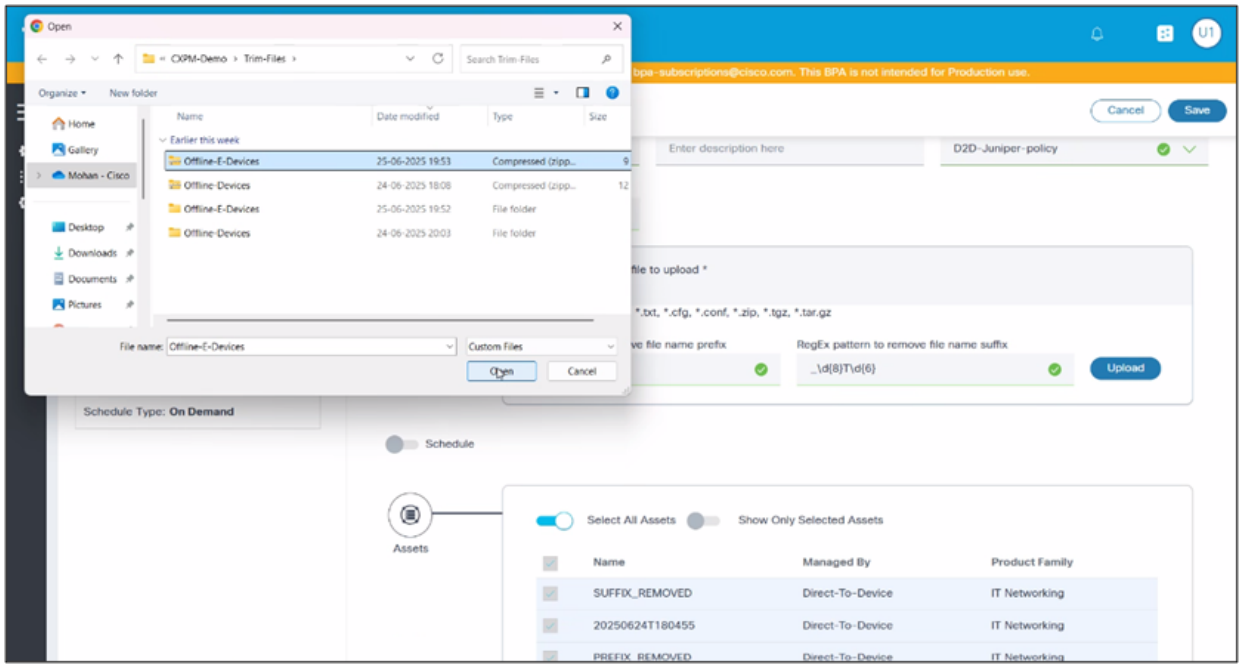
1. 从更多选项图标中选择脱机审核。



上载文件

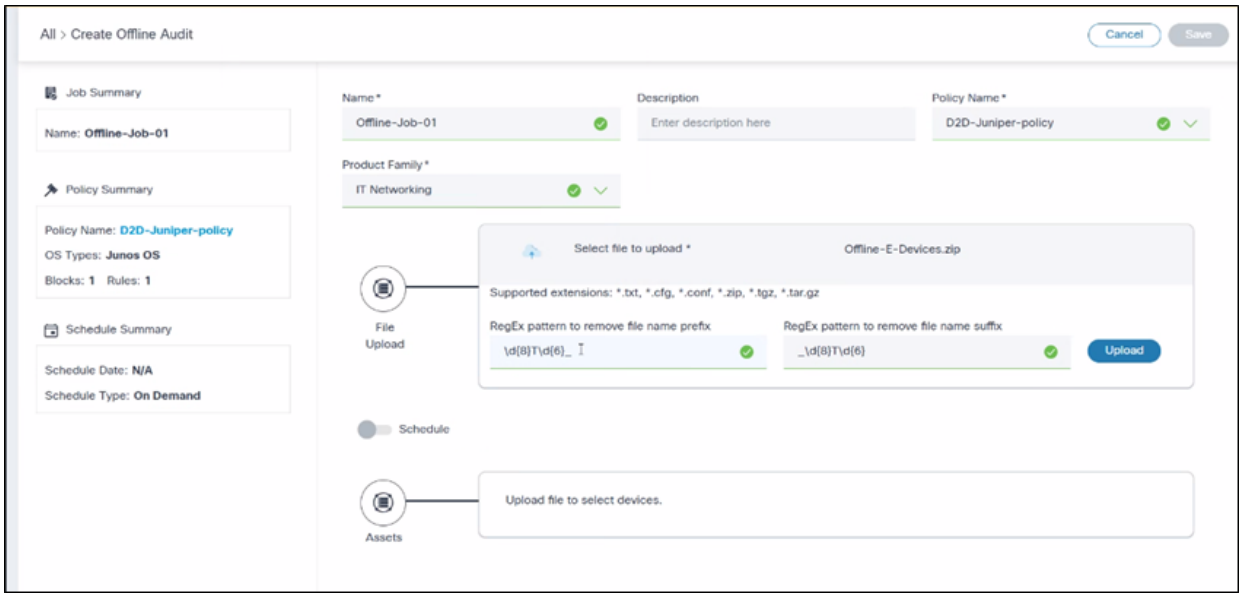
2. 点击选择要上传的文件以上传配置文件。

注意：支持的文件类型包括(.txt、.cfg、.conf、.zip、.tgz、tar.gz)。



桌面文件

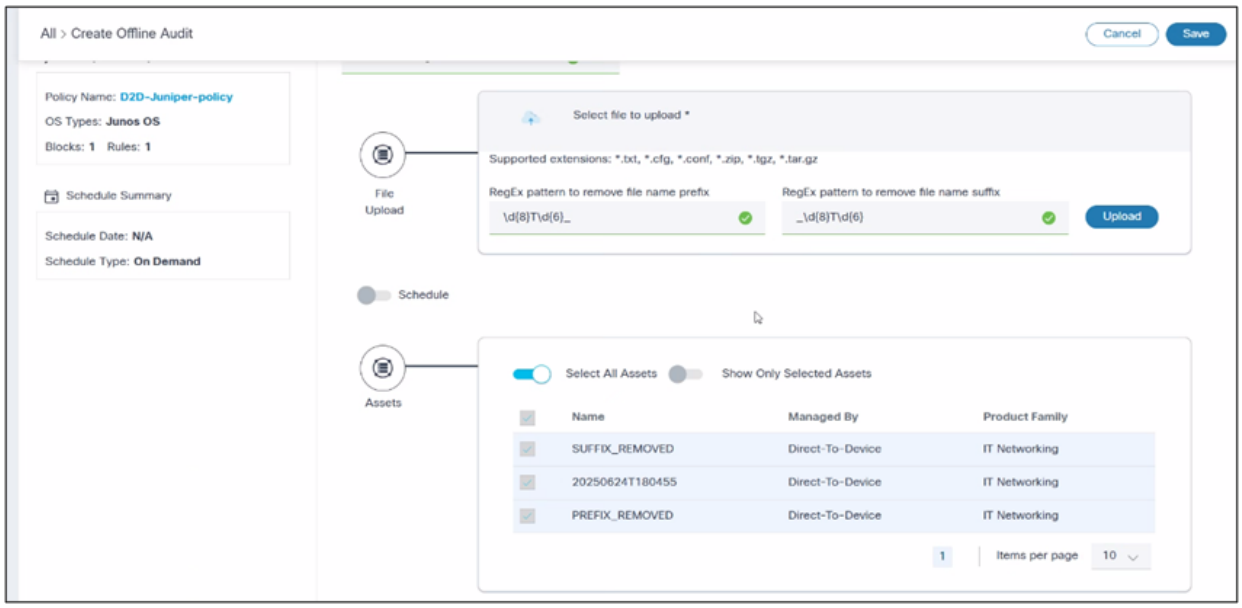
3. 如果配置文件在文件夹或存档文件中进行压缩，请在上传之前解压缩这些文件。



Regex模式

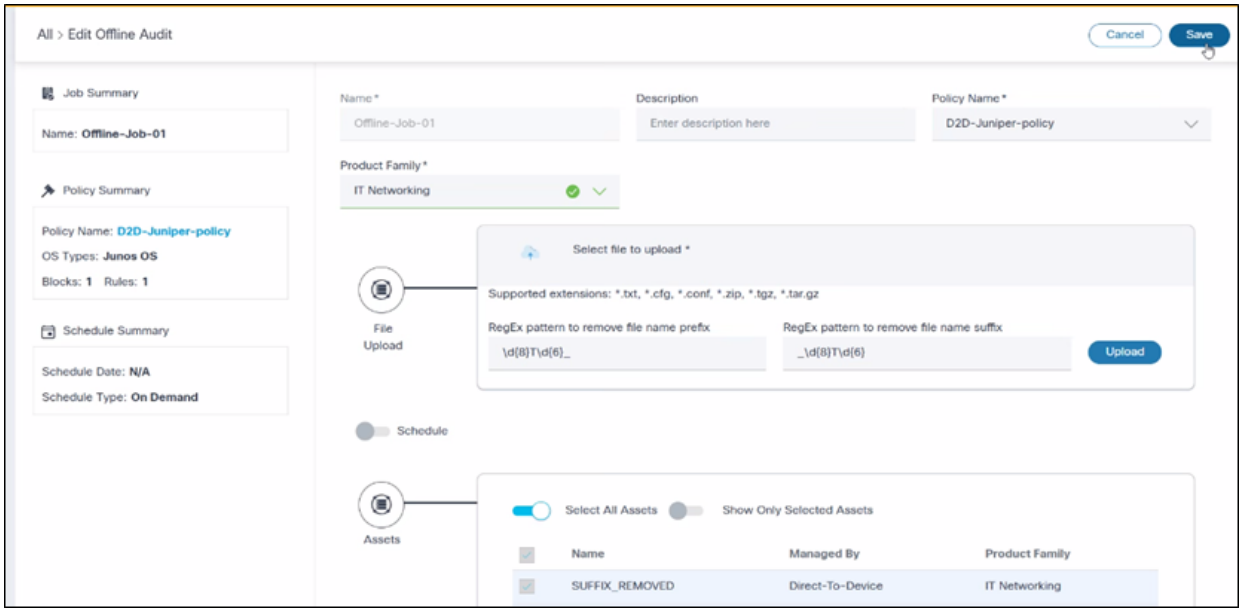
4. 应用Regex模式进行文件名修整（可选）。

注意：使用前缀或后缀修剪模式(regex)标准化或简化已上传的文件名，以简化处理。



上传文件

5. 单击Upload。系统将显示确认消息，表示文件已保存在数据库中并已成功上传。



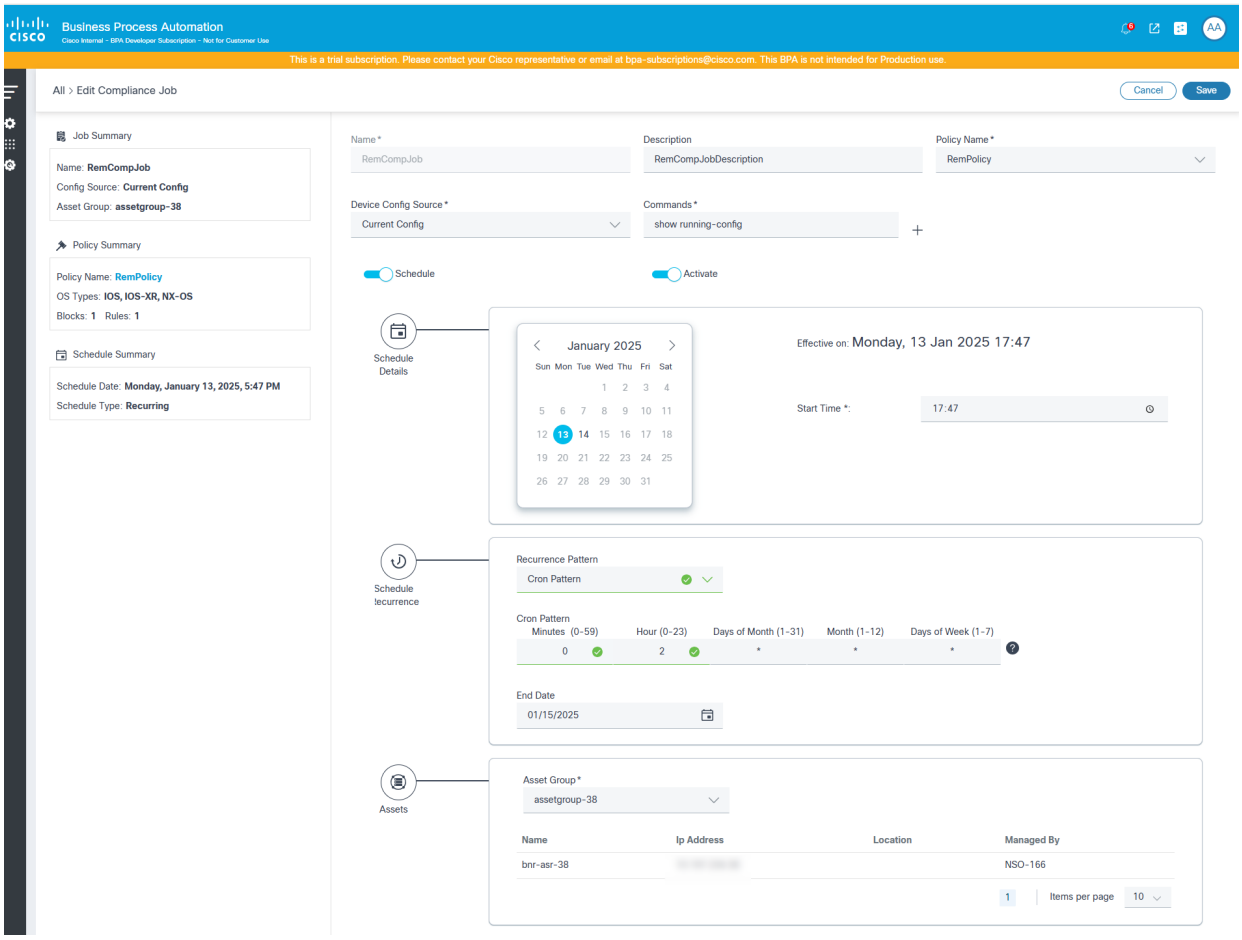
保存脱机审核

6. 单击Save以创建脱机审核作业。

编辑合规性作业

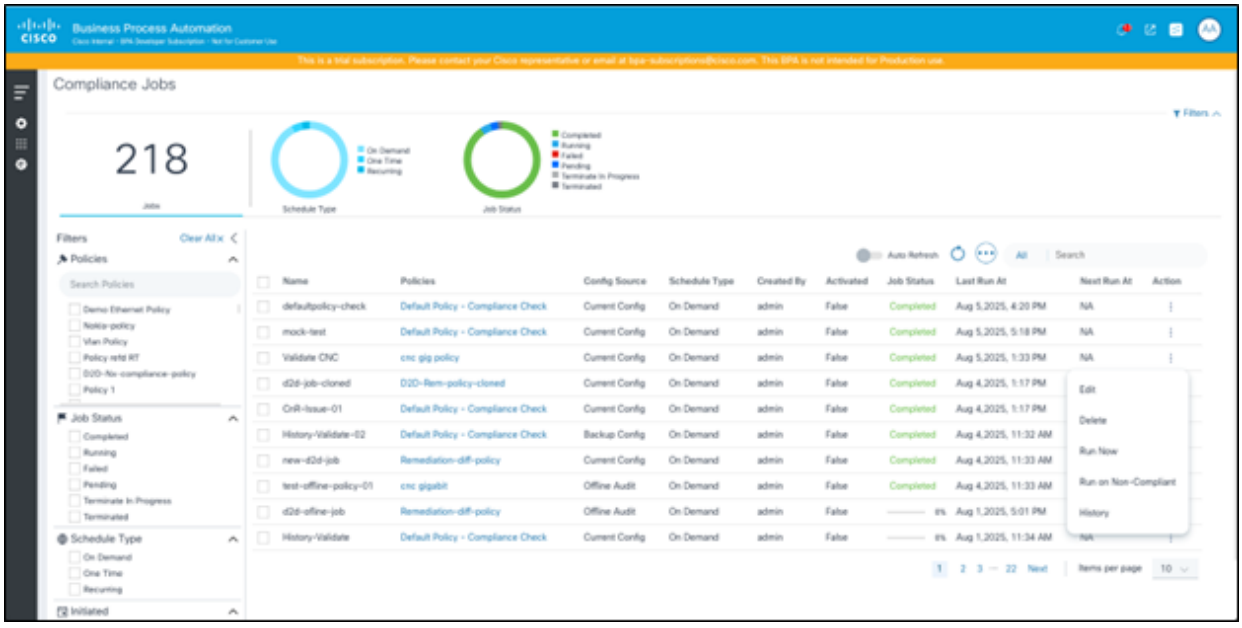
要编辑合规性作业，请按照创建合规性作业中提供的步骤操作。

注意：作业名称不可编辑。



编辑合规性作业

立即运行或重新运行合规性作业



合规性作业 — 立即运行和不合规运行

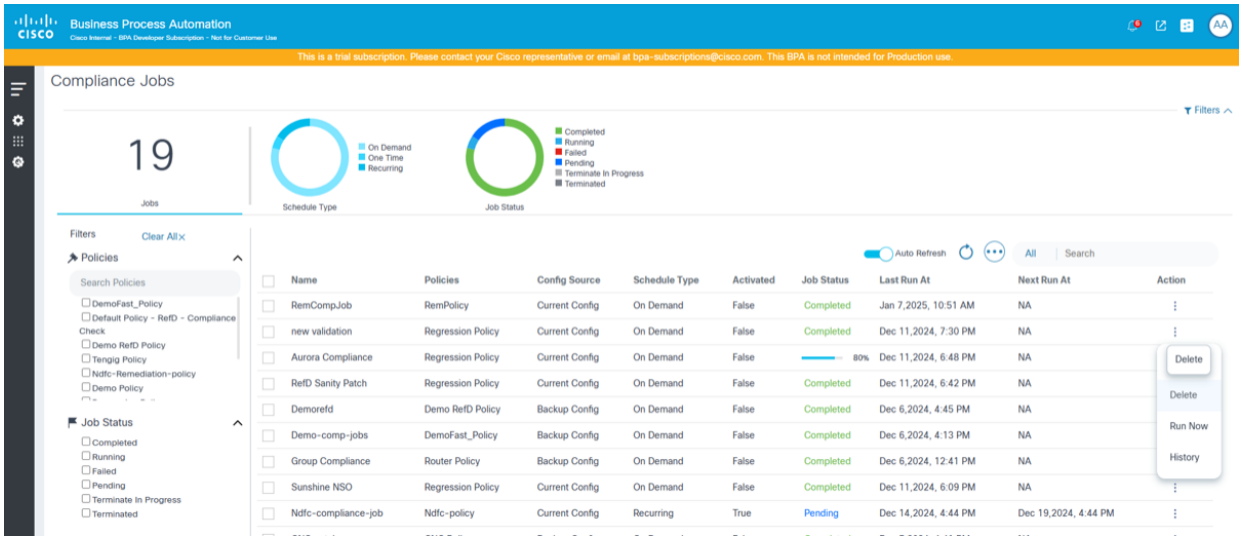
Compliance Jobs网格有一个选项，可通过从More Options图标中选择Run Now来按需运行作业。

如果作业已执行，则用户可以从更多选项图标中选择在不合规时运行。此操作仅对在上一次执行中未标记为完全兼容的资产列表运行合规性作业。

删除合规性作业

如果用户具有正确的基于角色的访问控制(RBAC)角色，门户会提供删除一个或多个合规性作业的选项。在执行过程中无法删除作业。用户可以选择删除一个或多个合规性作业。

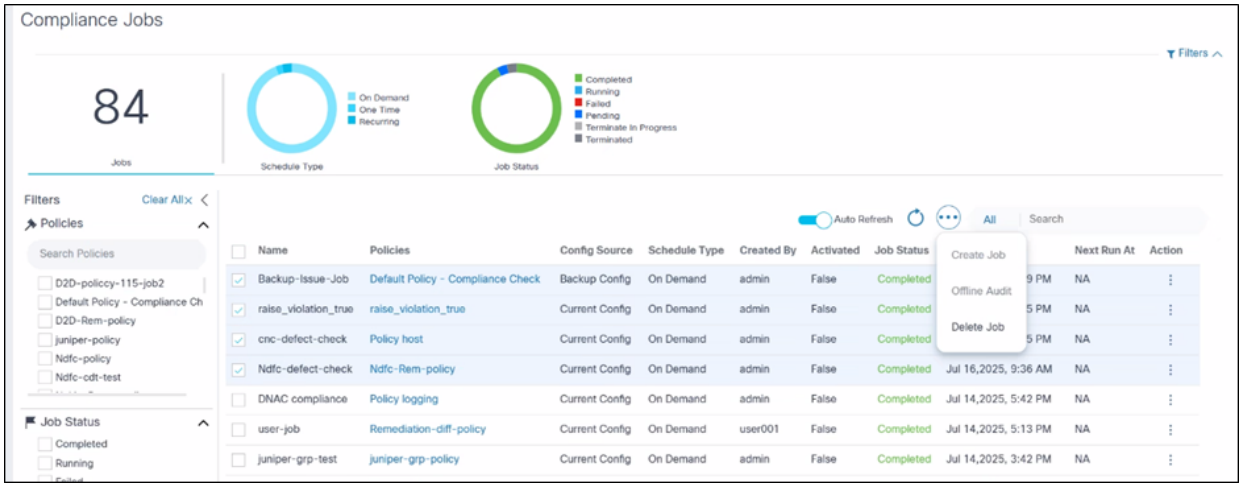
删除符合性作业的步骤：



删除单个符合性作业

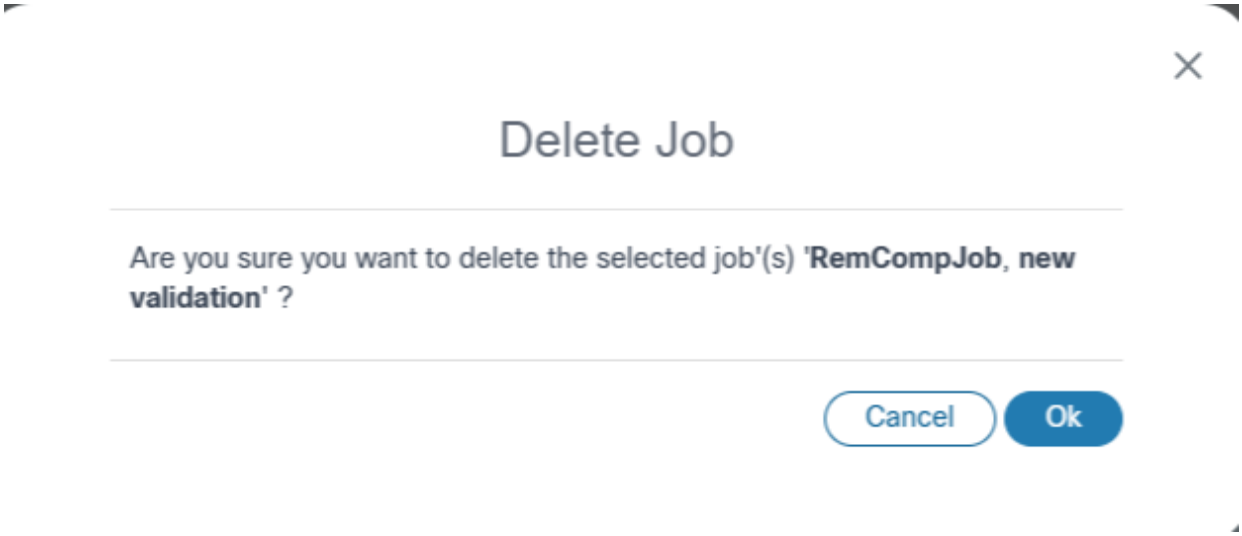
1. 在Compliance Jobs页面中，选择要删除的作业上的More Options图标> Delete。

或者



删除多个合规性作业

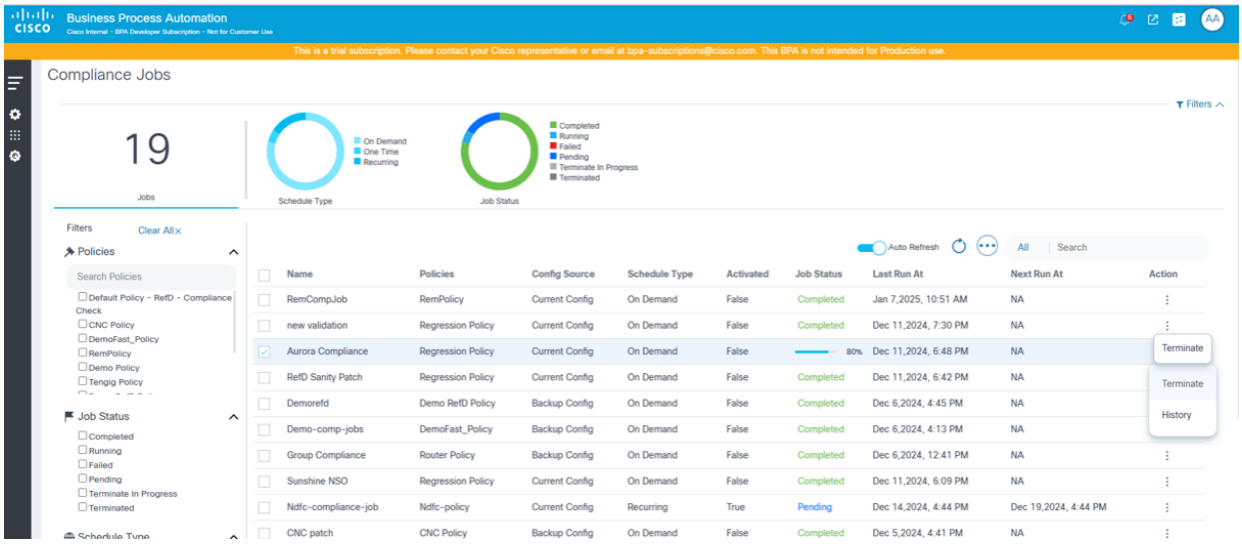
要删除多个符合性作业，请选择要删除的作业的复选框，然后选择更多选项>删除作业。系统随即会显示确认。



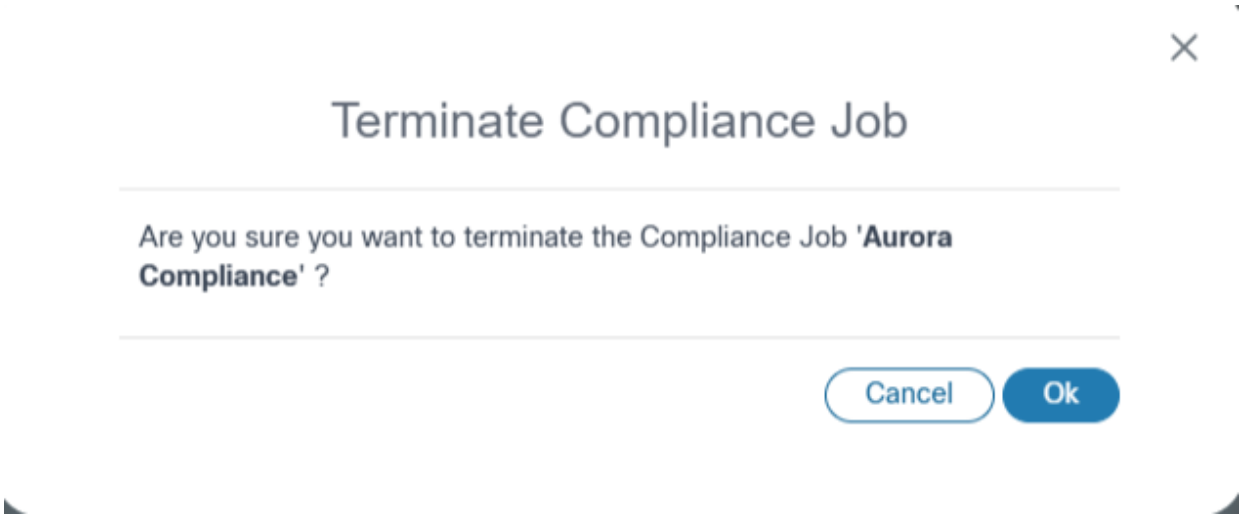
删除合规性作业确认

终止合规性作业

门户为用户提供终止给定作业的运行执行的选项。当作业终止时，当前运行的设备会完成它们的执行，并取消所有进一步排队等候的设备执行。



终止合规性作业

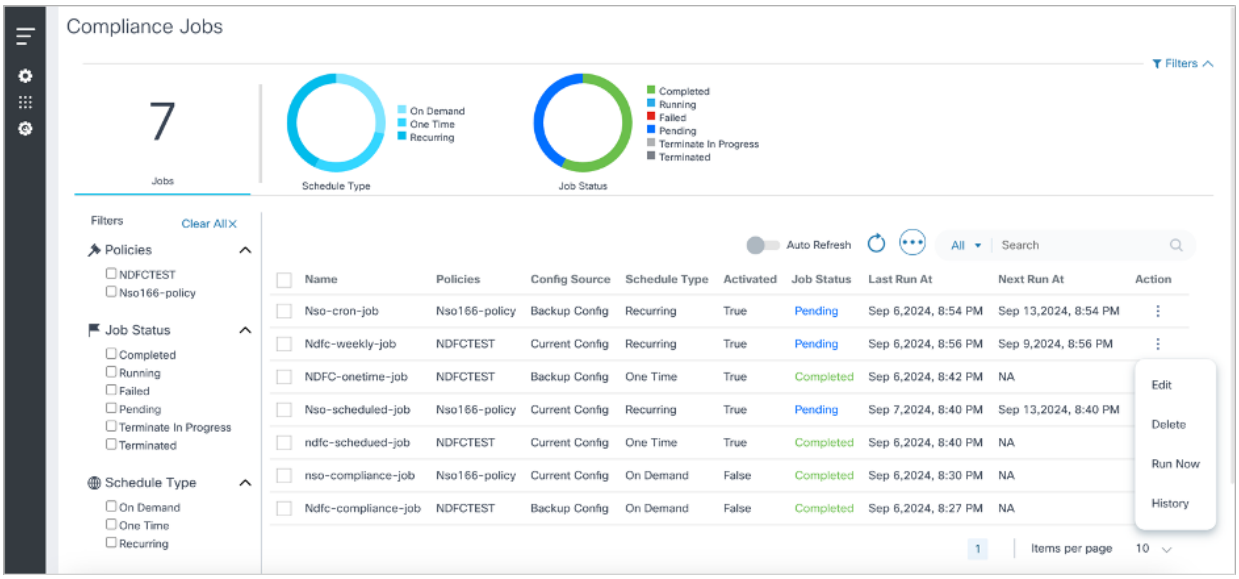


终止合规性作业确认

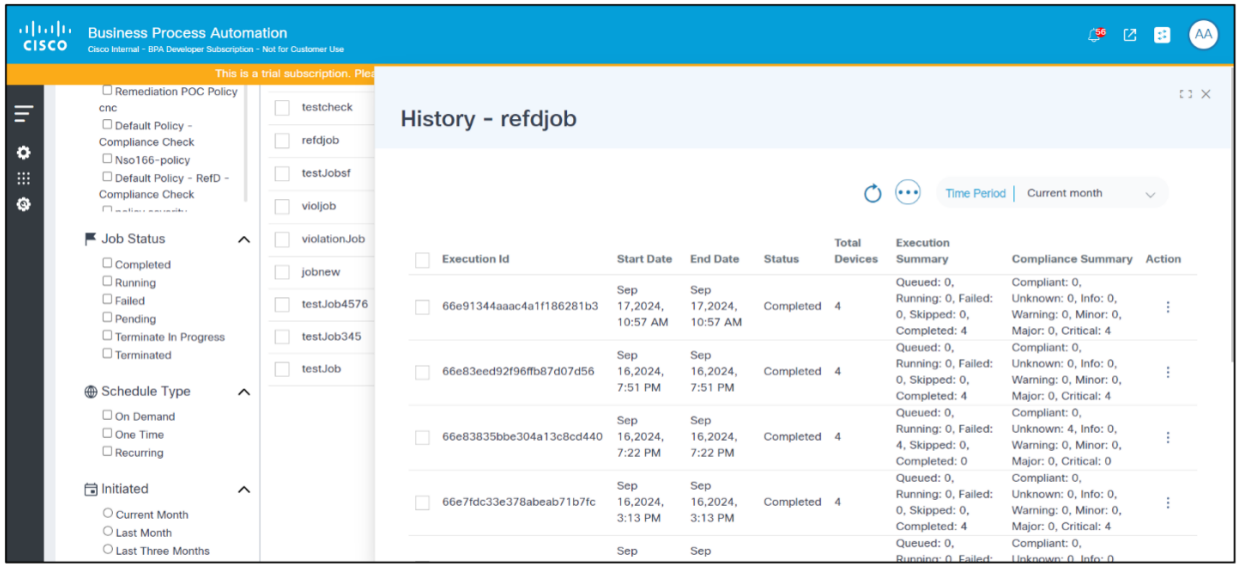
合规性作业历史记录

“符合性作业”中的“历史记录”选项显示按调度日期范围过滤的选定作业的执行列表。

要查看合规性作业的历史记录，请从合规性作业页中选择更多选项图标> 历史记录。系统随即会显示History页面。



合规性作业历史记录

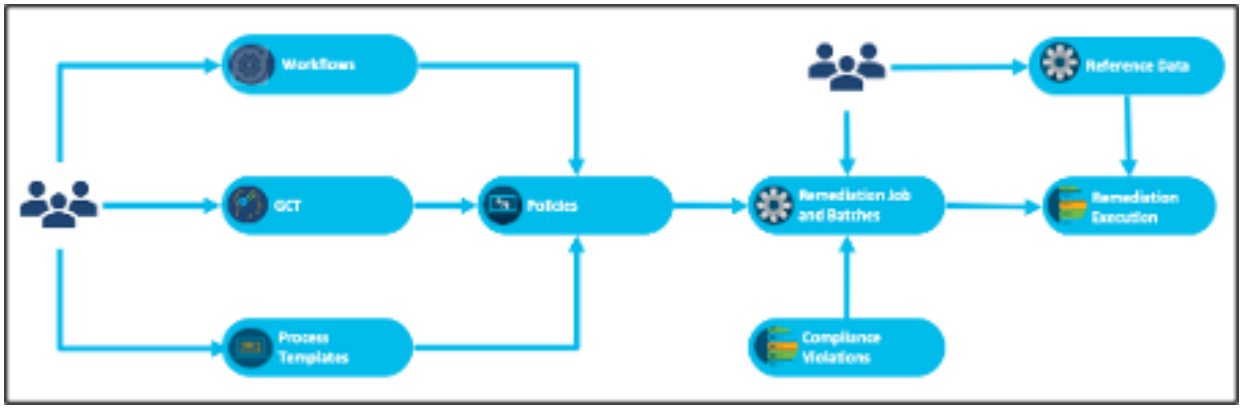


“历史记录”页

补救作业

Remediation Framework允许操作员补救合规性控制面板上列出的合规性违规。此框架使用工作流程、GCT和流程模板。

配置补救流程图



配置补救概述

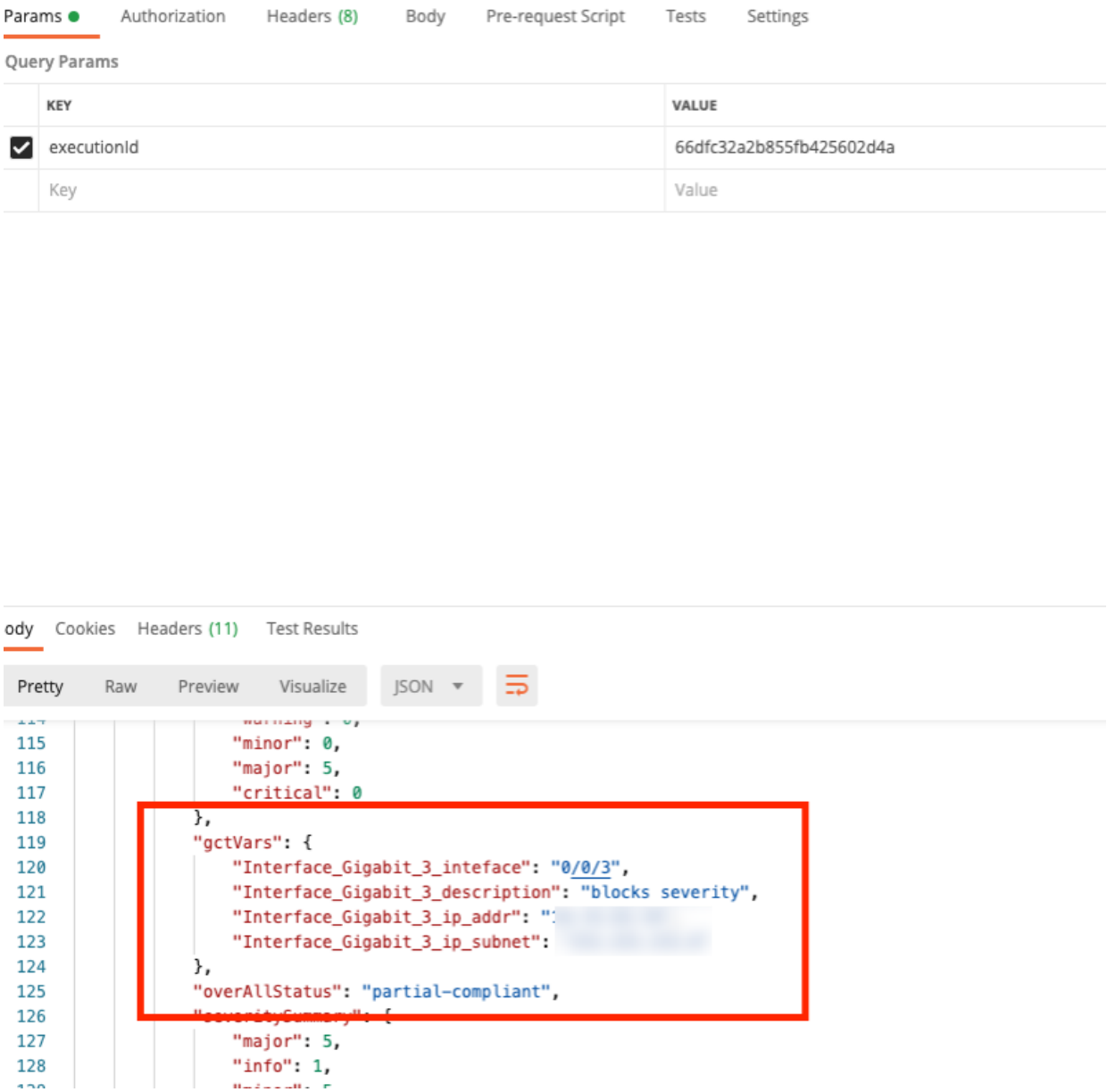
配置补救使用案例使操作员可以使用补救作业修复设备上的配置违规。首先使用相应的工作流程、GCT模板和每个控制器类型的流程模板配置合规性策略。针对受影响的资产列表为策略运行补救作业。在补救期间，可从各种数据源获取要应用于设备的值，包括合规性执行结果、RefD应用和现有设备配置。可以根据特定客户要求自定义工作流程，以在补救过程中执行其他步骤。

补救功能最重要的步骤说明如下：

GCT模板

GCT是BPA核心功能，用于使用特定于控制器的模板在设备上应用配置更改。

- 创建更新设备配置的GCT模板，解决合规性违规问题
- 如果GCT模板中的变量符合以下语法，则框架支持自动变量映射：
  - 对于单设备配置块：<>_<>。示例：management_interface_ipv4_addr、management_interface_ipv4_subnet
  - 未来版本中会规划多个设备配置块
- 如果“Block Identifier Name”和“Variable Name from block”包含空格，应将这些空格替换为下划线(“_”)（例如，如果“Block Identifier Name”为“Management Interface”，“Variable Name”为“IPV4_ADDR”，则GCT中的变量名称应为“Management_Interface_IPV4_ADDR”。）
- 用户可以检查合规性设备执行的“gctVars”输出，以查看GCT变量的语法和映射是否正确；要获取合规性设备执行，请使用以下REST API:
  - 获取执行以查找执行ID
    - URL:/api/v1.0/compliance-remediation/compliance-executions
    - 方法：GET
  - 使用执行ID获取设备执行
    - URL:https://<>/bpa/api/v1.0/compliance-remediation/compliance-device-executions?executionId=<>
    - 方法：GET



GCT变量 — gctVars

- 要从块中检索变量，请使用以下REST API:
  - URL:https://<>/bpa/api/v1.0/compliance-remediation/utils/schema
  - 方法：POST
  - 正文：{"blockName":"<< block name >>" }
- 通过将模板应用于设备来验证GCT模板，以便进行试运行和提交
- 在合规性策略中配置上述GCT模板

工作流程

补救框架提供以下开箱即用的参考工作流程：

- 补救流程:此工作流程具有补救执行中涉及的通用步骤集。
- 补救子流程:此工作流程包含变量分配、GCT试运行和GCT提交任务，其他团队可根据需要自

定义这些任务。

这两个工作流程均可根据客户需求原样使用、更新或更换。

流程模板

可以根据策略配置流程模板和分析模板，以运行预检查和后检查并比较输出。

策略

CnR策略将每个设备类型的工作流程、GCT模板和流程模板拼合在一起，这些模板可用于使用作业修复配置。

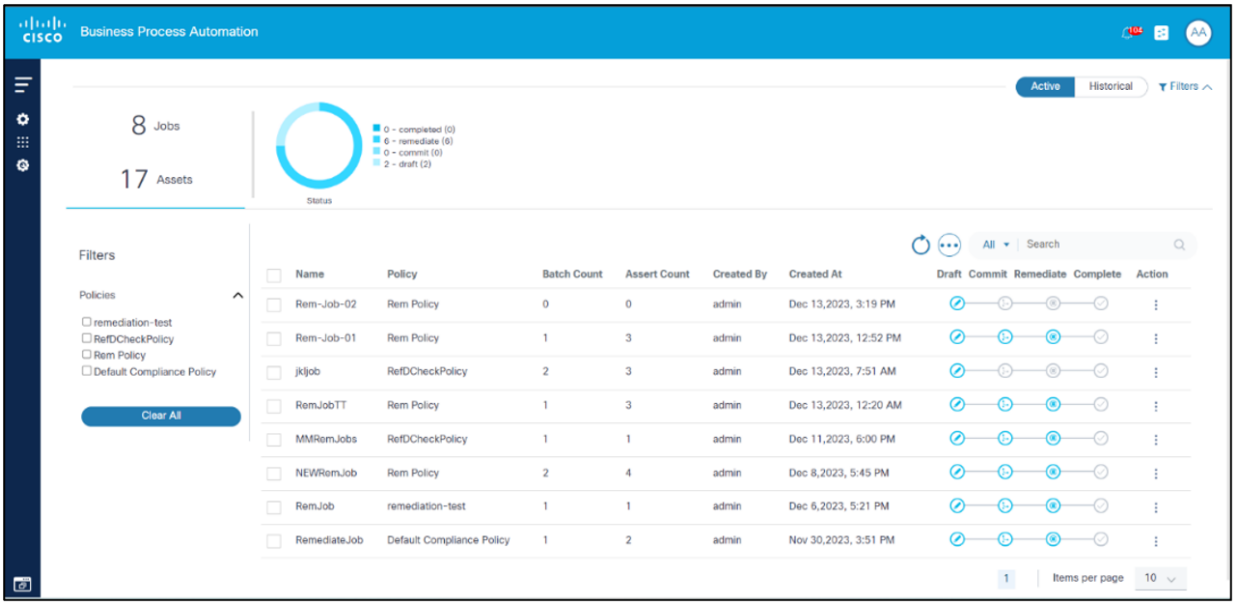
补救作业

补救作业帮助操作员针对受影响的资产的选定列表应用补救策略。补救作业可以按需或按计划执行。在运行时，补救工作流程可以从各种来源提取数据，包括设备详细信息、合规性执行详细信息和RefD框架。

补救作业列表

用户可以按如下方式过滤、排序和查看控制面板中创建的补救作业：

- 作业:显示创建的作业总数
- 资产:显示已创建的总资产
- 状态:按状态显示作业
- 活动和历史:根据选择显示有效或历史（无效）作业
- 策略:按策略过滤补救作业
- 主网格:显示默认作业列表，可通过单击标题进行排序，并包括按名称和策略搜索以及页面显示
- 操作:当作业处于草稿状态或已完成状态时，可以存档或删除作业；无法存档或删除正在运行的作业

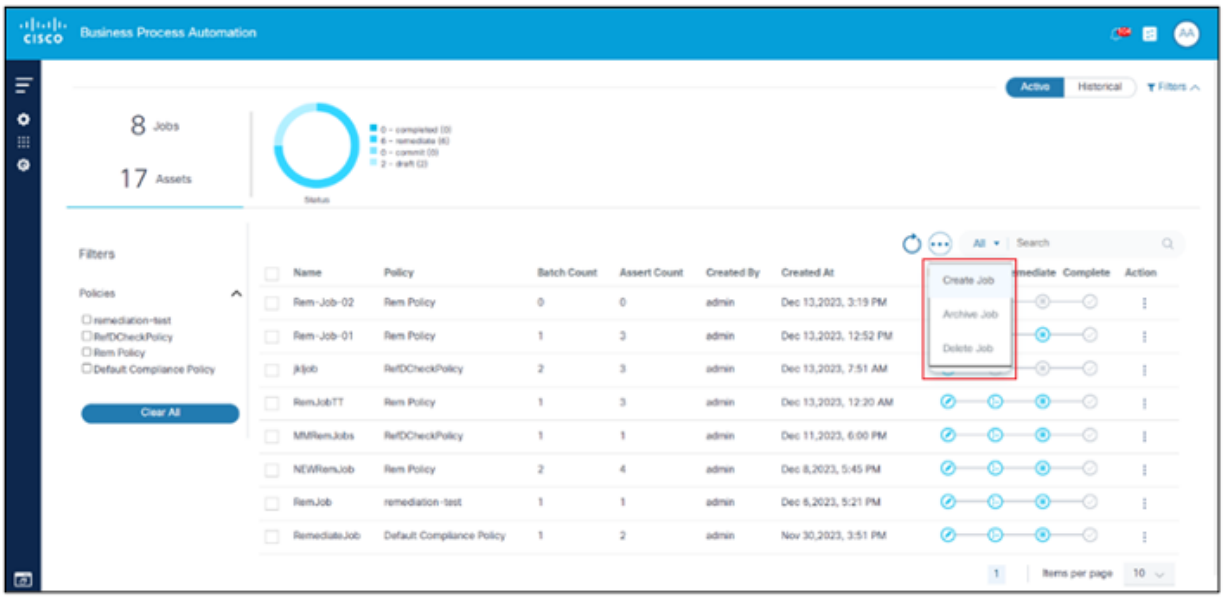


补救作业列表

创建和编辑补救作业

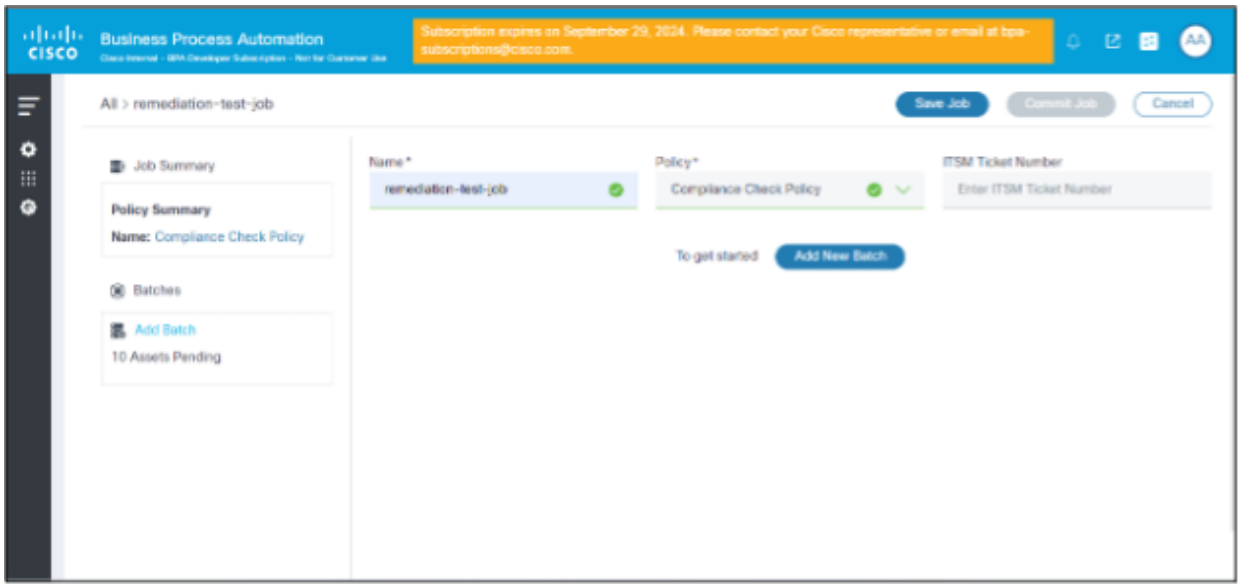
补救作业是从作业列表页面创建的，可通过执行以下步骤创建：

1. 选择更多选项图标> 创建作业。系统将显示Create Job页面。



补救作业选项

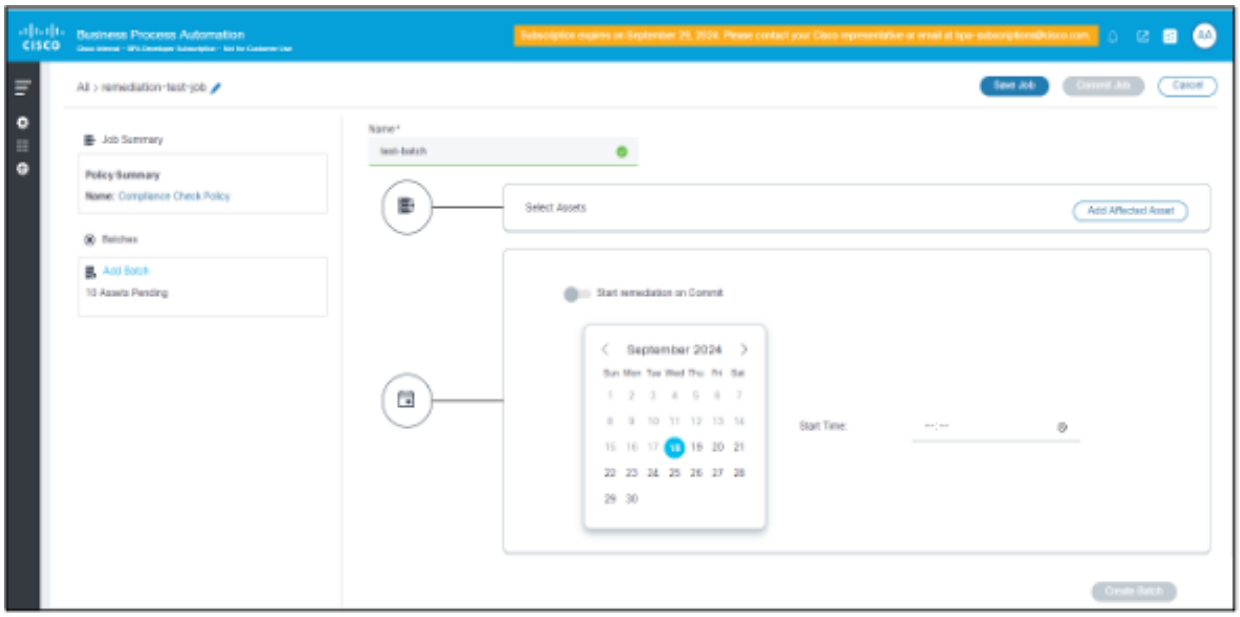
2. 完成或编辑详细信息。



补救作业：详细信息

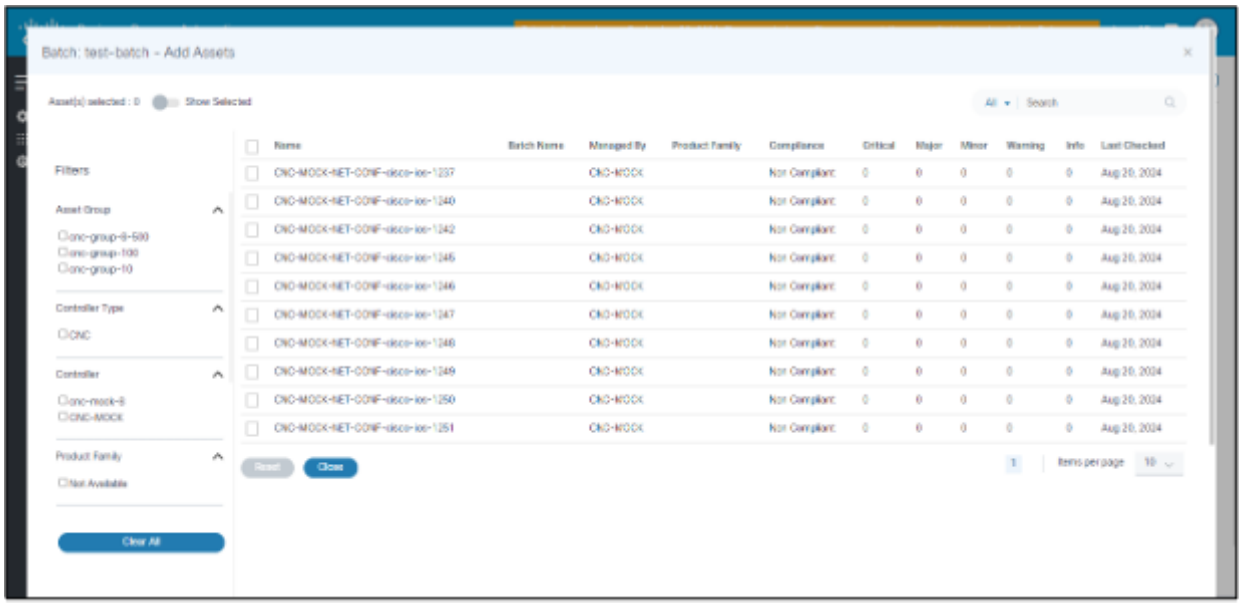
3. 单击Save Job。

要从“创建作业”页向作业添加批，请执行以下操作：



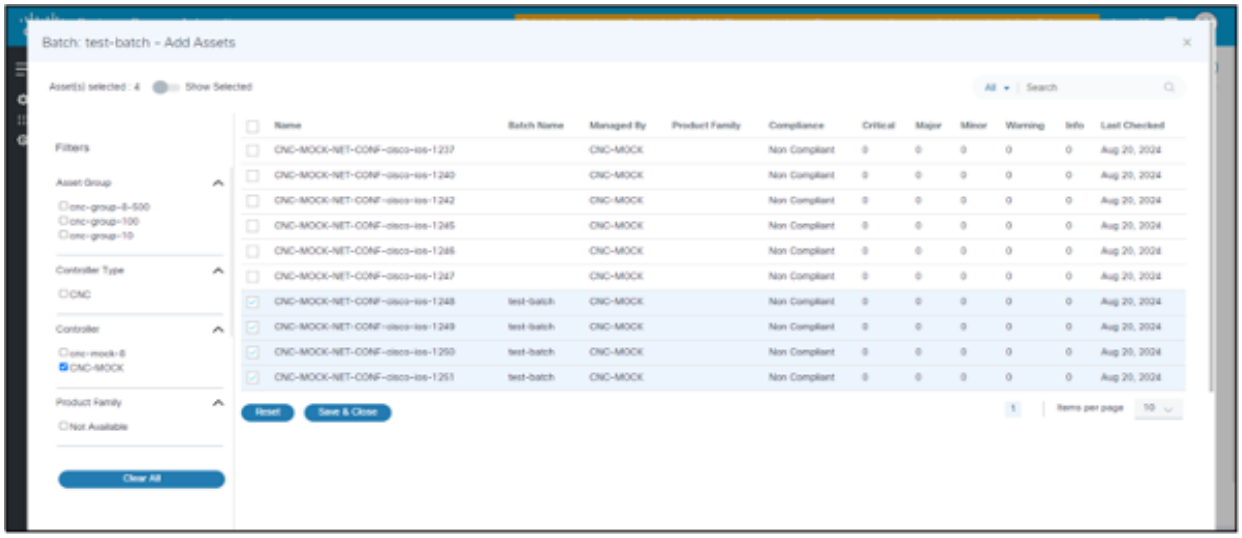
补救作业：添加批次

1. 点击添加新批处理。
2. 输入Name、Affected asset details和Schedule details。
3. 点击添加受影响的资产。
4. 在Assets Details页中，选择受影响的资产列表，然后点击Save Job。
5. 根据Controller Type、Controller、Asset Group和Product Family过滤资产。
6. 选择资源后，单击保存并关闭，返回上一页。



补救作业：添加受影响的资产

注意：用户可选择在“受影响的资产”(Affected Assets)页面应用过滤器



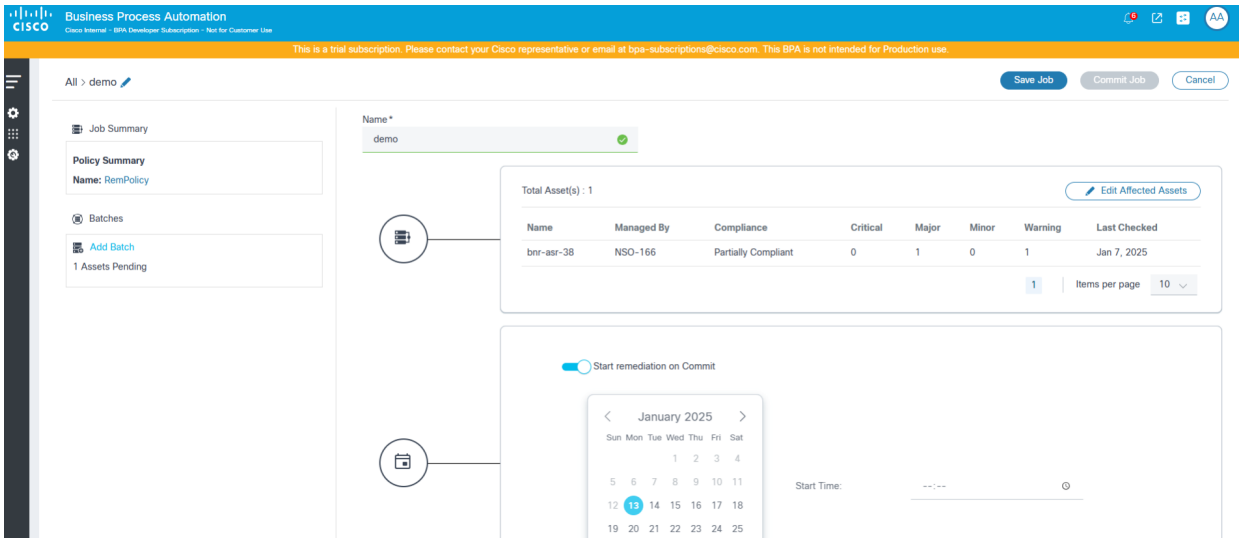
补救作业：添加受影响的过滤器

添加受影响的资产后，可以在保存时或在计划的将来时间运行一次批处理。

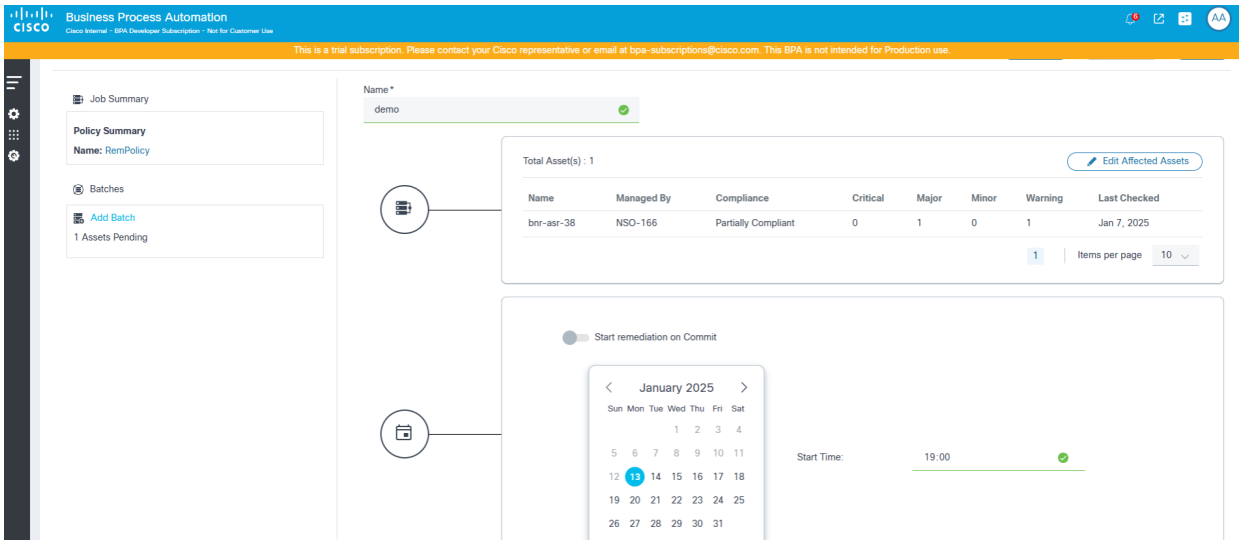
注意：要以On Demand形式运行作业，请启用Start remediation on Commit切换。如果用户选择此选项，则不需要日期和时间。如果用户选择One-Time选项，则必须提供执行作业的日期和时间。

单个补救作业有多个批处理。可以在提交时或在计划的日期和时间启动每个批处理。

提交后补救批处理可以按需或计划运行。



补救作业：按需

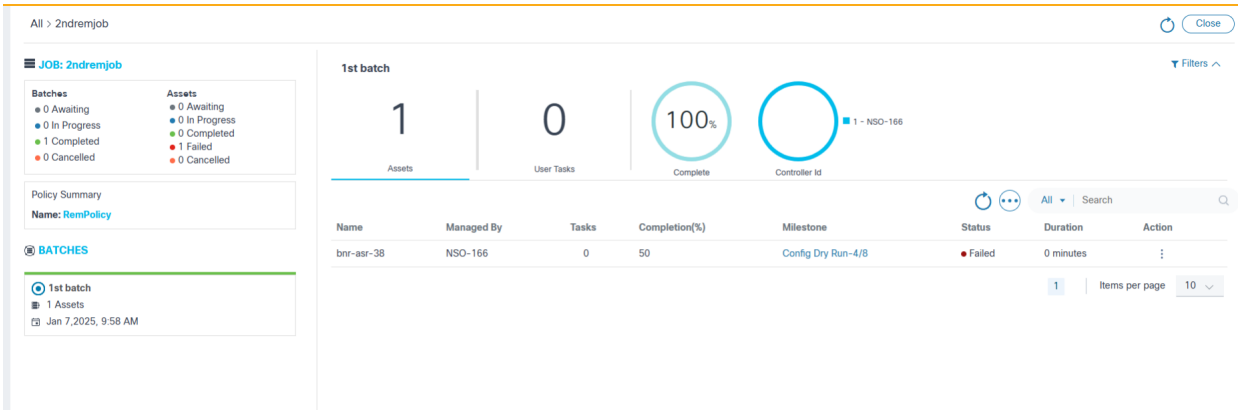


补救作业：一次/计划

补救执行：设备列表

提交补救作业后，将触发执行操作，作业的状态将显示在Remediation Jobs下的List Devices页面中。用户可以按控制器ID、名称、管理者和产品系列应用过滤器。

- 工作:显示批和资产的状态详细信息以及选定运行补救作业的策略的名称
- 批:显示作为当前补救作业一部分的批处理列表
- 自动刷新:显示以下选项：如果作业处于运行状态，则每隔30秒自动刷新页面；刷新页面；或显示取消以返回上一页
- 批次级别详细信息:显示批层汇总详细信息，包括资产总计数、用户任务计数、完成百分比和控制器详细信息
- 资产网格:显示资产网格视图，包括每个资产的用户任务、完成百分比和当前里程碑



补救执行：设备列表

补救执行：内联用户任务详细信息

在设备列表中，Tasks列指示用户是否具有任何要执行的任务。

要查看内联用户任务详细信息，请执行以下操作：

1. 选择任务计数。User Tasks列表窗口打开。
2. 选择一项任务.User Task Details窗口打开。

可以从内联执行以下操作：

- 完成
- 重试
- 取消

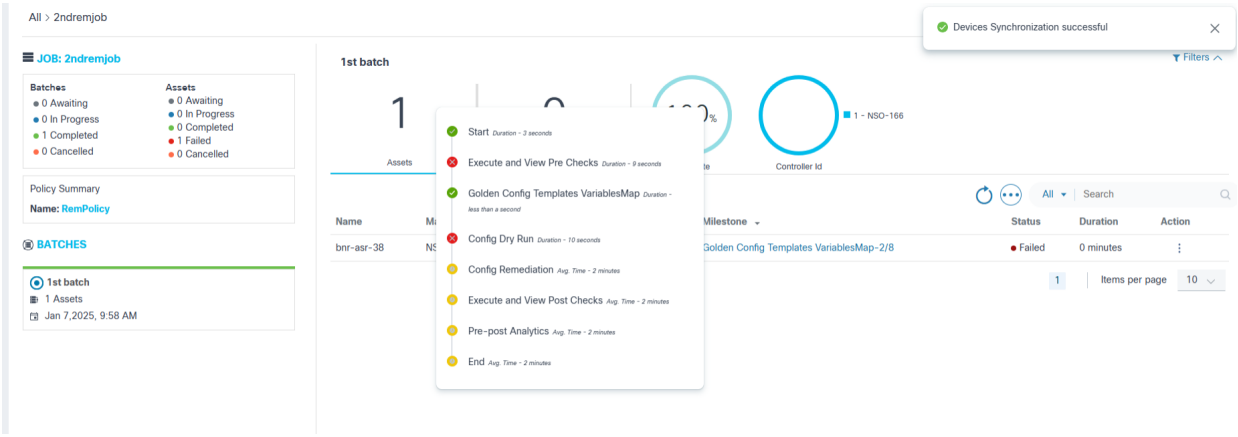
补救执行：内联里程碑详细信息

在设备列表中，Milestone列指示与给定设备的补救相关的当前里程碑。

要查看内联里程碑详细信息，请选择该列。Milestone Details窗口打开。

以下状态可用于里程碑：

- 未开始
- 正在运行
- Completed
- 失败



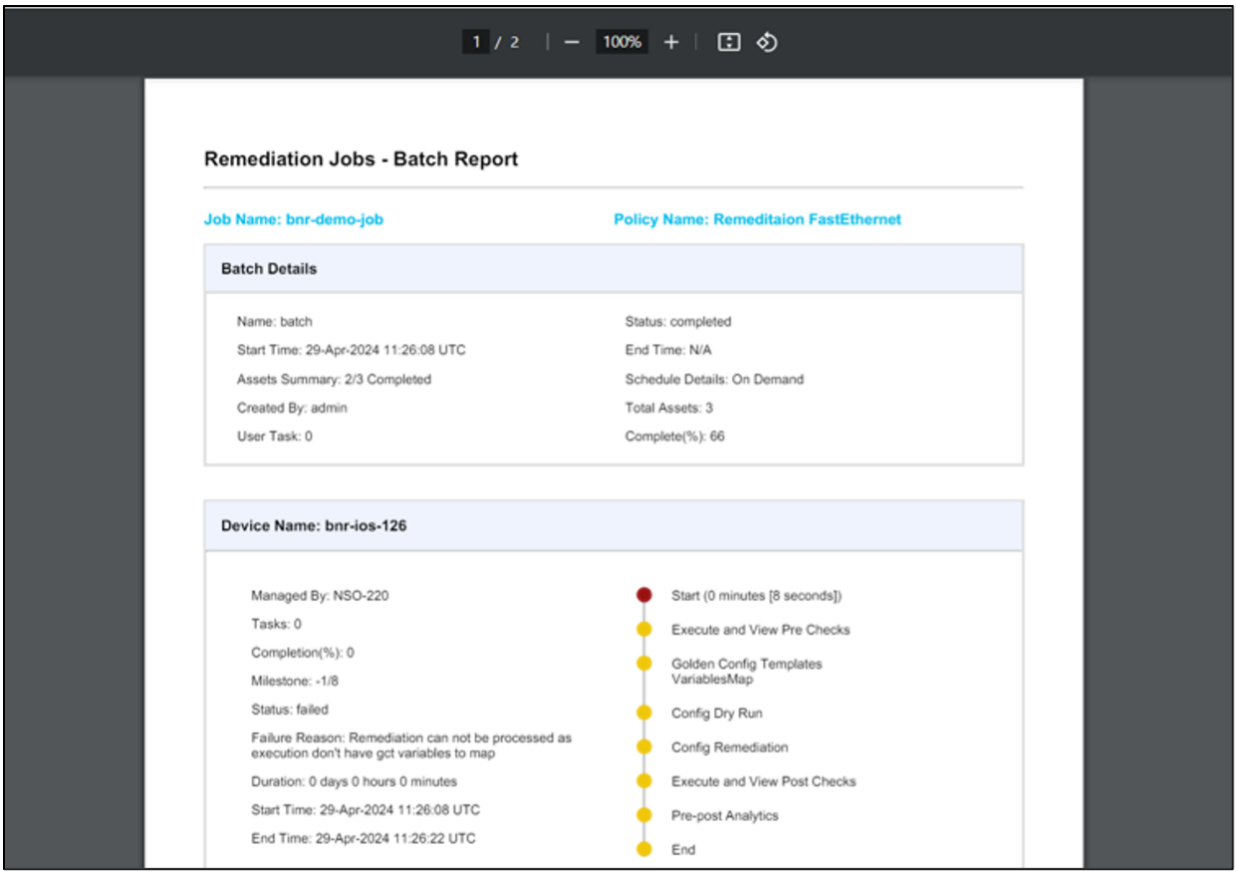
补救执行：内联里程碑详细信息

补救执行：生成和下载批摘要PDF报告

可以生成和下载批次摘要。

要以PDF格式下载每批摘要报告，请执行以下操作：

1. 选择更多选项图标> 生成报告。系统在内部检查报告是否准备就绪。报告准备就绪后，将启用Download Report选项。
2. 选择更多选项图标> 下载报告。PDF下载。



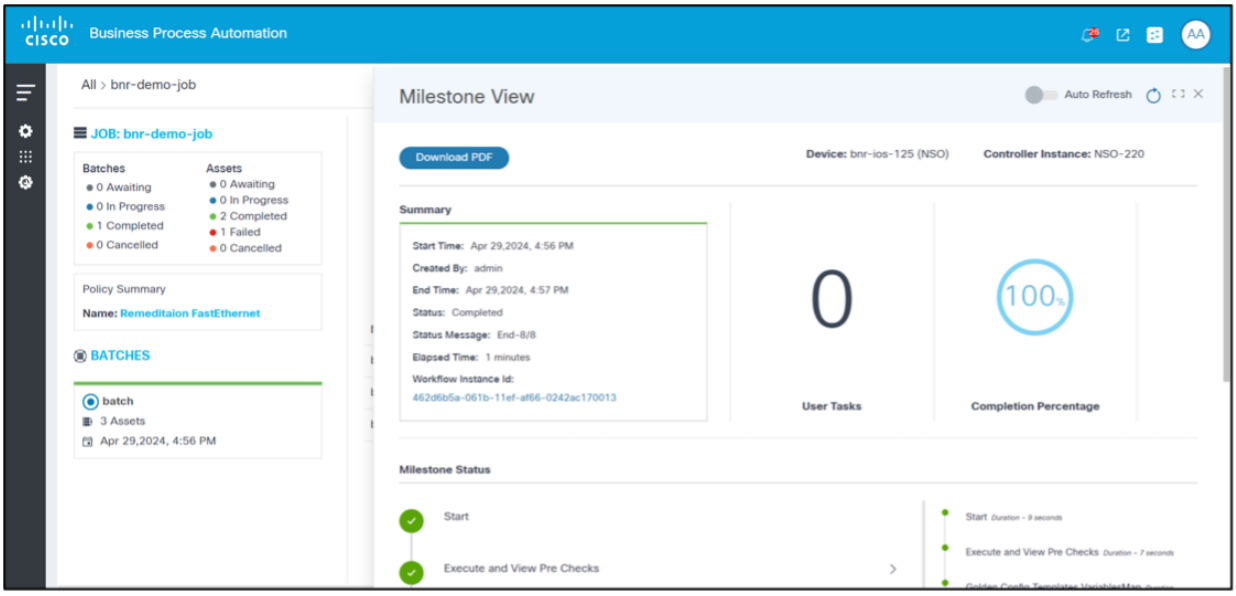
批次摘要报告PDF

补救作业批处理报告包含批处理详细信息部分，该部分提供补救批处理的摘要，例如作业名称、批处理名称、开始和结束时间、总资产以及总体状态。然后是设备详细信息部分（每个设备一个部分），其中包括设备名称、设备特定补救状态、时间表、持续时间和里程碑列表以及状态。

补救执行：设备详细信息

要查看里程碑的设备详细信息，请选择Device Details页面。系统随即会显示“里程碑视图”页面。

显示具有详细里程碑状态的给定设备的补救摘要，包括已完成关键里程碑的命令输出。例如，可以查看process template命令输出、GCT干运行输出和分析差异输出内容。



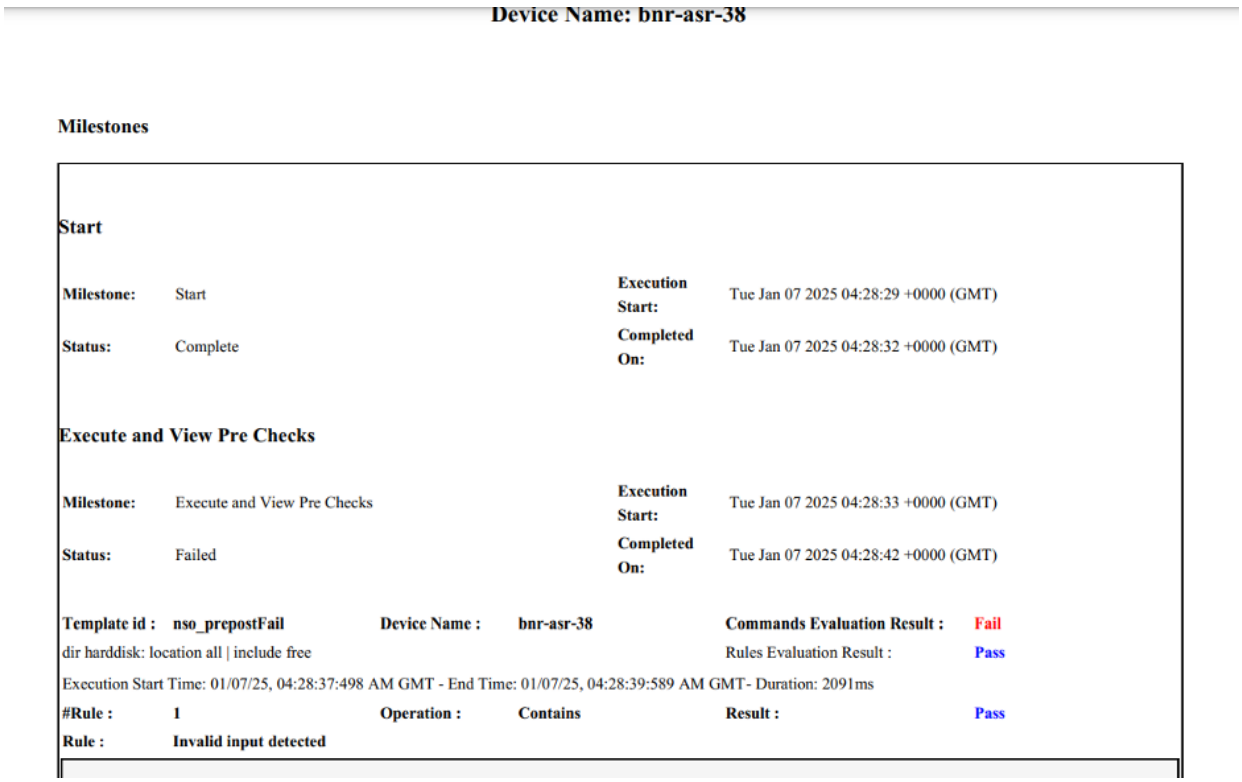
补救执行：里程碑视图

补救执行：设备详细信息 — 里程碑报告

要查看里程碑报告，请执行以下操作：

1. 选择Device Details页。系统随即会显示“里程碑视图”页面。
2. 单击下载PDF。生成并下载“里程碑视图报告”(Milestone View Report)如下所示。

此报告为所选设备补救提供更详细的里程碑详情和相应内容。



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				

补救执行：设备详细信息 — 里程碑视图PDF报告

配置:块和规则

块的功能

配置块是在网络管理系统中创建和实施合规性策略的基本元素。它们代表设备CLI配置，例如用于接口、路由器边界网关协议(BGP)等的配置。以下是配置块的主要功能：

- 模块化:配置块允许模块化策略创建，使管理员能够独立定义和管理设备配置的离散部分。这种模块化简化了更新和维护合规性策略的流程。
- 粒度:通过将设备配置拆分为更小、更易于管理的部分，管理员可以执行准确的合规性检查并强制执行特定标准。这可确保设备配置的每个部分都遵循所需的策略。
- 可重用性：定义后，配置块可在多个合规性策略和设备上重复使用。这种可重用性减少了冗余并确保配置管理的一致性。
- 静态配置块:静态配置块表示不带任何变量的原始设备配置。

  示例：以下块可用于对TwentyFiveGigE0/0/0/31接口运行合规性检查

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

- 动态配置块:动态配置块代表设备配置，包括允许更灵活且可重复使用的变量。这些块功能与TTP模板类似，应用于设备配置并获取变量的值。可以将条件添加到规则以验证这些变量。有关TTP的详细信息，请参阅https://ttp.readthedocs.io/en/latest/Overview.html。

  示例：以下块可用于对所有TwentyFiveGigE接口运行合规性检查

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

具有子层次结构的动态配置块:此块的功能类似于动态配置块，用于从具有多个层次的设备配置中检索值。

示例：以下示例演示设备配置，以及用于从分层结构检索值的相应动态块。

具有分层结构的设备配置：

```
router bgp 12.34
address-family ipv4 unicast
  router-id 1.1.1.X
!
vrf CT2S2
  rd 102:103
  !
  neighbor 10.1.102.XXX
  remote-as 102.XXX
  address-family ipv4 unicast
    send-community-ebgp
    route-policy vCE102-link1.102 in
    route-policy vCE102-link1.102 out
  !
  !
  neighbor 10.2.102.XXX
  remote-as 102.XXX
  address-family ipv4 unicast
    route-policy vCE102-link2.102 in
    route-policy vCE102-link2.102 out
  !
  !
vrf AS65000
  rd 102:XXX
  !
  neighbor 10.1.37.X
  remote-as 65000
  address-family ipv4 labeled-unicast
    route-policy PASS-ALL in
    route-policy PASS-ALL out
```

动态块配置，用于解析上述配置。

```
router bgp {{ ASN }}


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


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


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


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

规则的功能

规则允许用户定义条件以根据配置块中存在的变量进行验证。在执行过程中，合规性引擎会解析设备配置，查找设备块实例的匹配实例，从行中读取值，并针对这些值运行规则中定义的条件。结果（无论配置行是否有违规）将存储以在控制面板中显示。

配置规则现在是块创建生命周期的一部分。因此，没有单独的页面可查看规则。规则可以在相应的块创建或更新页面下列出、创建和更新。

在CnR框架中，规则在根据指定条件验证配置方面发挥着关键作用。本节概述如何在系统中集成和管理规则。

- 目的:规则允许用户定义用于验证配置块中存在的变量的条件
- 执行流程:
  - 合规引擎解析设备配置
  - 标识设备块实例的匹配实例
  - 从配置行提取值
  - 将规则中定义的条件应用于这些值
  - 指示违规的结果会存储并显示在控制面板中

与Block生命周期集成

- 生命周期集成：配置规则现在是块创建生命周期的有机组成部分
- 管理:
  - 规则直接在用于块创建或更新的页面中列出、创建和更新
  - 没有专用于查看规则的单独页面，简化了规则在块生命周期内的管理

此集成可确保将合规性检查无缝地纳入配置管理流程，从而能够根据预定义规则有效地监控和管理设备配置。

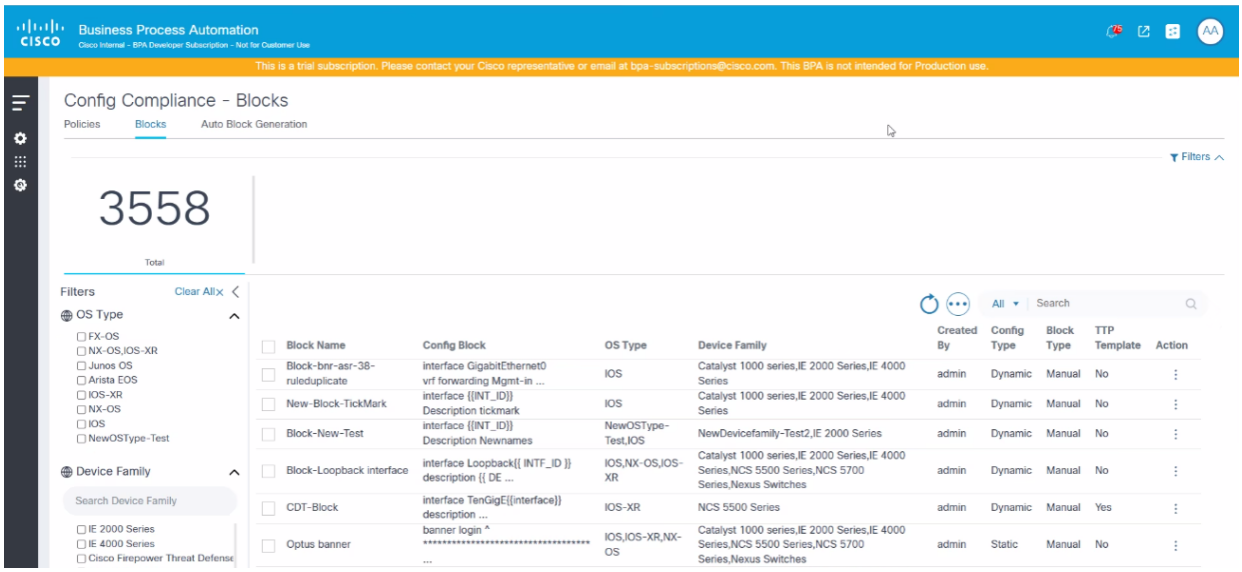
列表块

Blocks页面列出所有配置块，并提供用于生成、添加、编辑、删除、导入和导出块的操作。用户可以筛选、排序和查看阻止详细信息。

功能块的详细信息

- 总计数:显示已创建的块总数
- 过滤器选项:

    - 操作系统类型和设备系列:允许用户根据所选条件过滤块
- 主网格:
    - 显示默认块列表
    - 用户可以通过点击列标题对列表进行排序
    - 包括允许用户按所有属性或具体按块名称进行搜索的搜索功能
    - 支持分页功能，便于在列表中导航
- 操作:
    - 编辑:用户可以修改现有块
    - DELETE :用户可以从列表中删除块



配置块列表

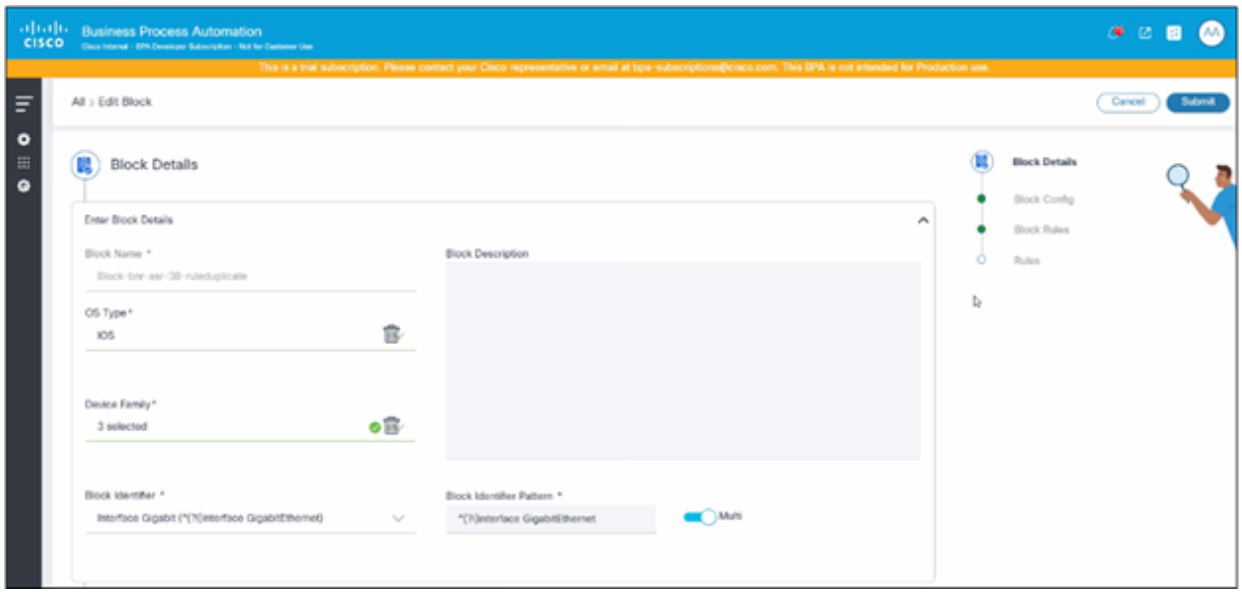
添加或编辑块和规则

Add或Edit Block页用于捕获和管理有关块的基本信息。本页概述了以下部分：

- 基本块详细信息:

  Basic Details部分包括：

    - 块名称:块的指定名称
    - 描述:块的用途或功能的简要概述或说明
    - 操作系统类型：与块关联的操作系统类型
    - 设备系列:与块兼容的设备类别或组
    - 块标识符选择:用于为块选择唯一标识符的选项
    - 添加或编辑块标识符详细信息:如果不存在合适的块标识符，用户可以使用相同的字段添加或编辑以下块标识符详细信息：
        - 块标识符名称:为块标识符指定的特定名称
        - 模式:块标识符遵循的模式或格式
        - 多:切换以指示是否将配置块视为多行配置

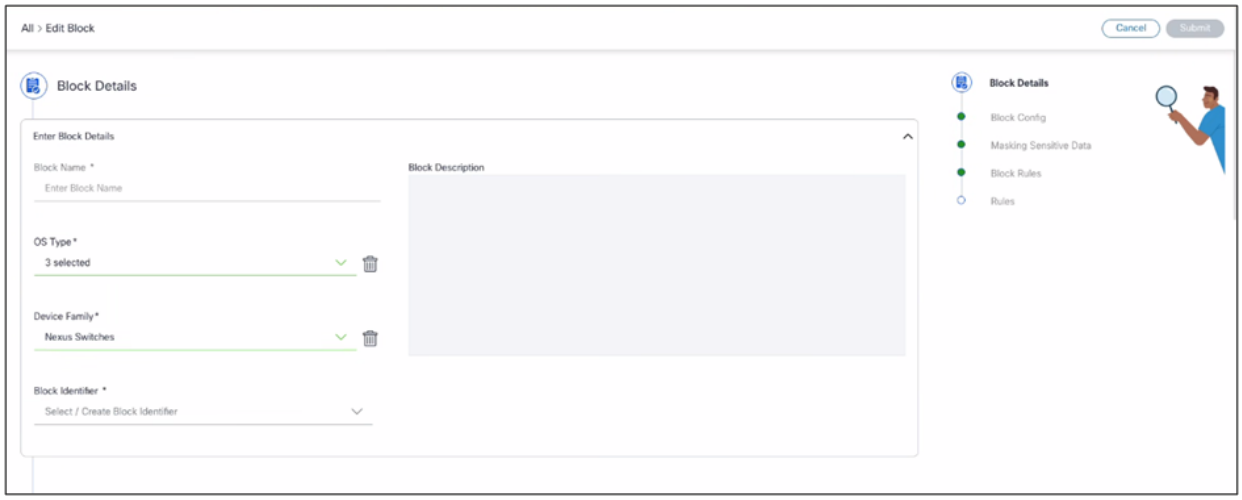


添加或编辑块 — 块详细信息

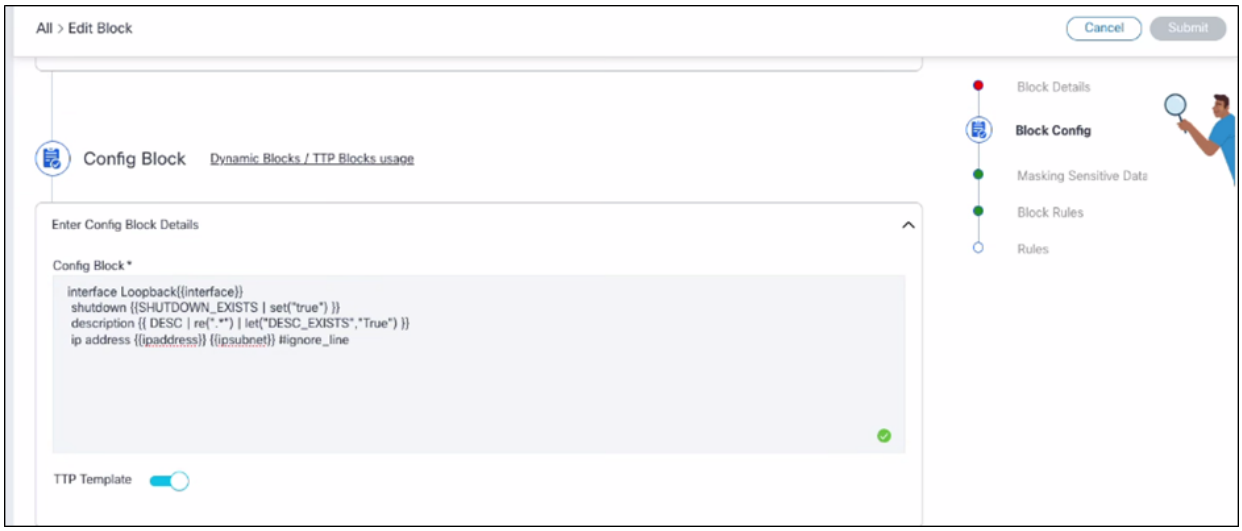
- 阻止配置:

Block Config部分包括：

- 配置块:表示包含不同变量的设备配置。此配置概述了如何在系统中设置和管理设备。
- TTP模板:指示是否将该块指定为模板转换协议(TTP)模板，以帮助识别用作模板来转换或标准化设备间配置的块。



阻止详细信息



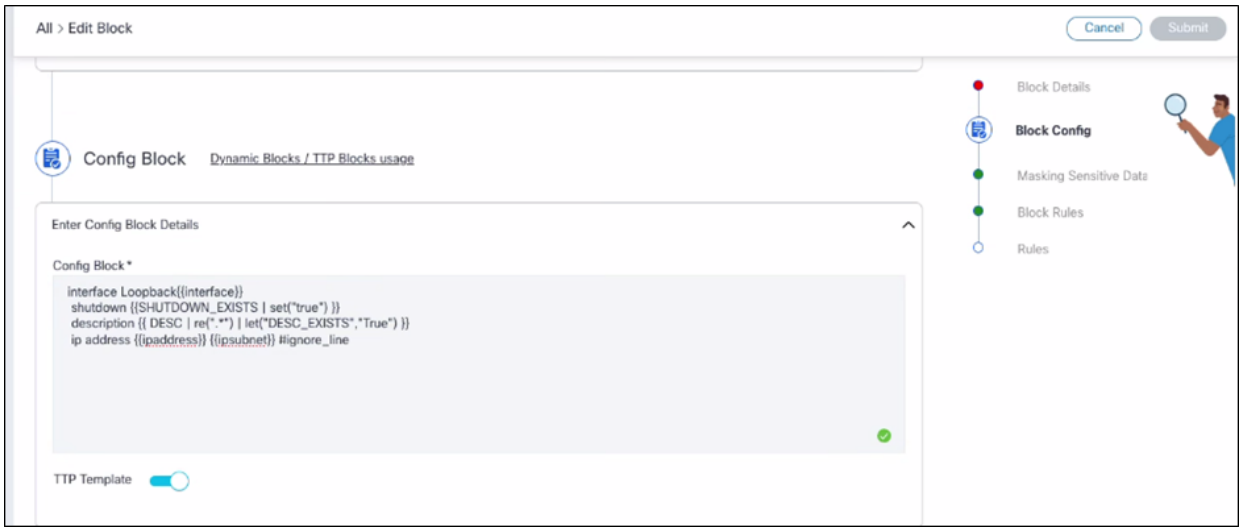
阻止配置

使用忽略线路语法

Ignore Line Syntax允许用户在块中特定配置行的末尾添加注释，以指示系统跳过该行上的任何合规性检查或违规。这样可以防止该线在报表或控制面板中显示为违规。

完成以下步骤以使用Ignore Line语法：

1. 找到要从合规性检查中排除的配置行（如ip地址）。



忽略线路语法

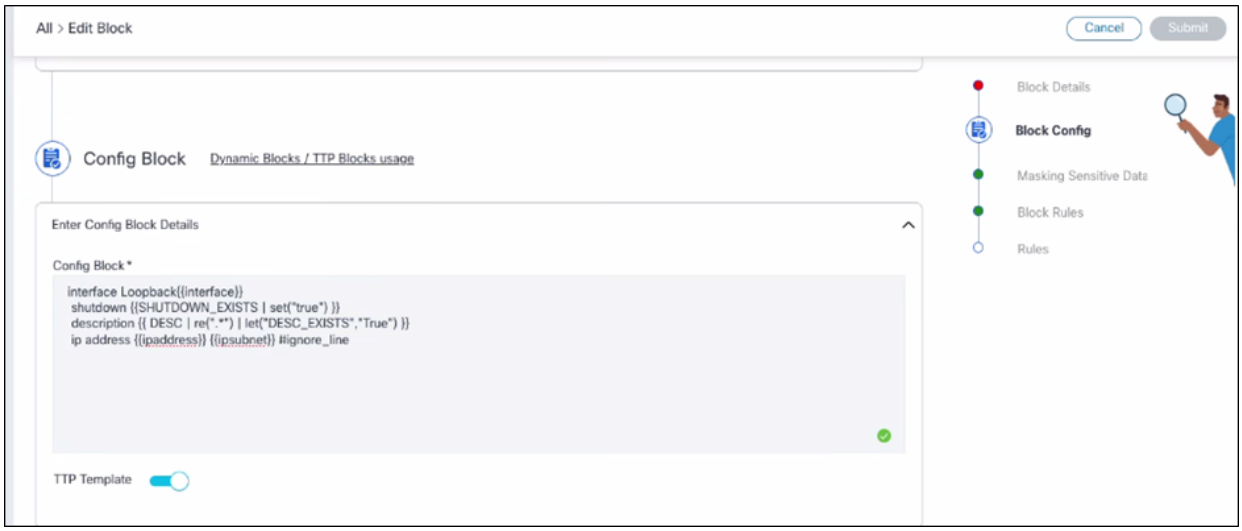
2. 在该行的末尾使用注释语法“#ignore_line”附加该行。示例：ip address {{ipAddress}} {{ipSubnet}}#ignore_line

引发违规

块配置中的此模板文本解析器(TTP)功能可用于指示如果存在特定行，是否应该引发违规。

完成以下步骤以使用TTP功能：

1. 在“阻止创建或编辑”页的“阻止配置”部分中，找到要控制的配置行。
2. 使用set或let命令定义TTP变量，如下所示：
   - 如果存在配置行关闭，请使用set命令定义变量，如下所示：
     shutdown | {{SHUTDOWN_FLAG | set("true")}"
   - 如果用户在配置行中有现有变量（如说明{{DESC}}），请使用let命令，如下所示：
     说明{{ DESC | re("。*") | let("DESC_EXISTS", "True")}}
3. 在规则中使用这些变量（上述示例中的SHUTDOWN_FLAG或DESC_EXISTS）引发违规。



引发违规

效果:

如果“shutdown”或“description config”行在设备配置中可用，则在控制面板页面上显示违规。违规的严重性取决于创建规则时所做的选择。

- 屏蔽敏感数据:

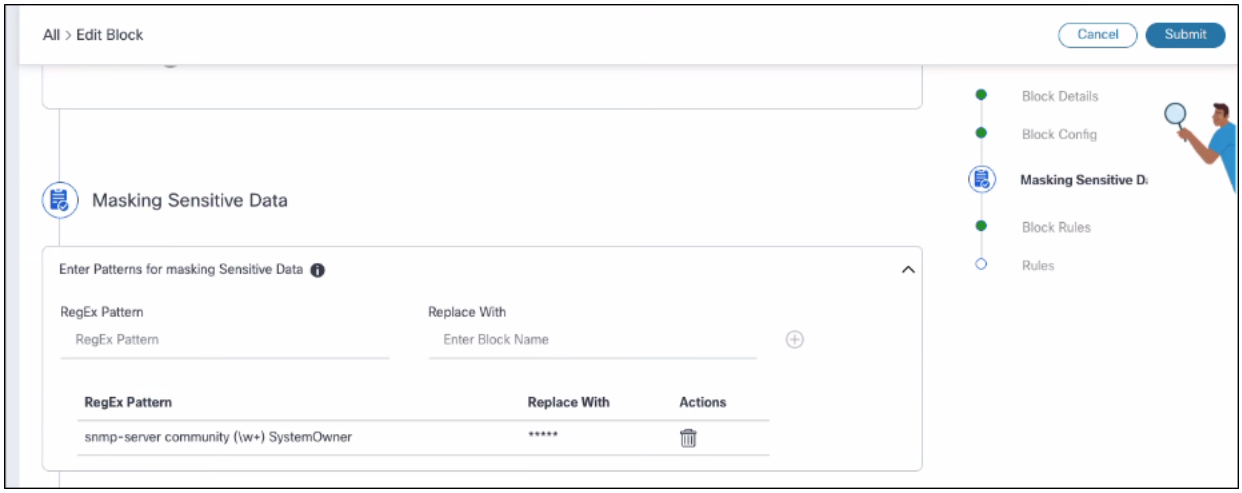
Mask Sensitive Data是一项允许用户使用正则表达式定义模式，以识别和屏蔽设备配置中的敏感信息（如密码或密钥）的功能。这通过用指定的掩码(例如“***”)替换匹配的数据，防止敏感数据在违规视图或补救配置差异中显示。

要屏蔽敏感数据，请完成以下步骤：

1. 在“掩码敏感数据”部分中：
   - 添加多个正则表达式(regex)模式以识别敏感数据

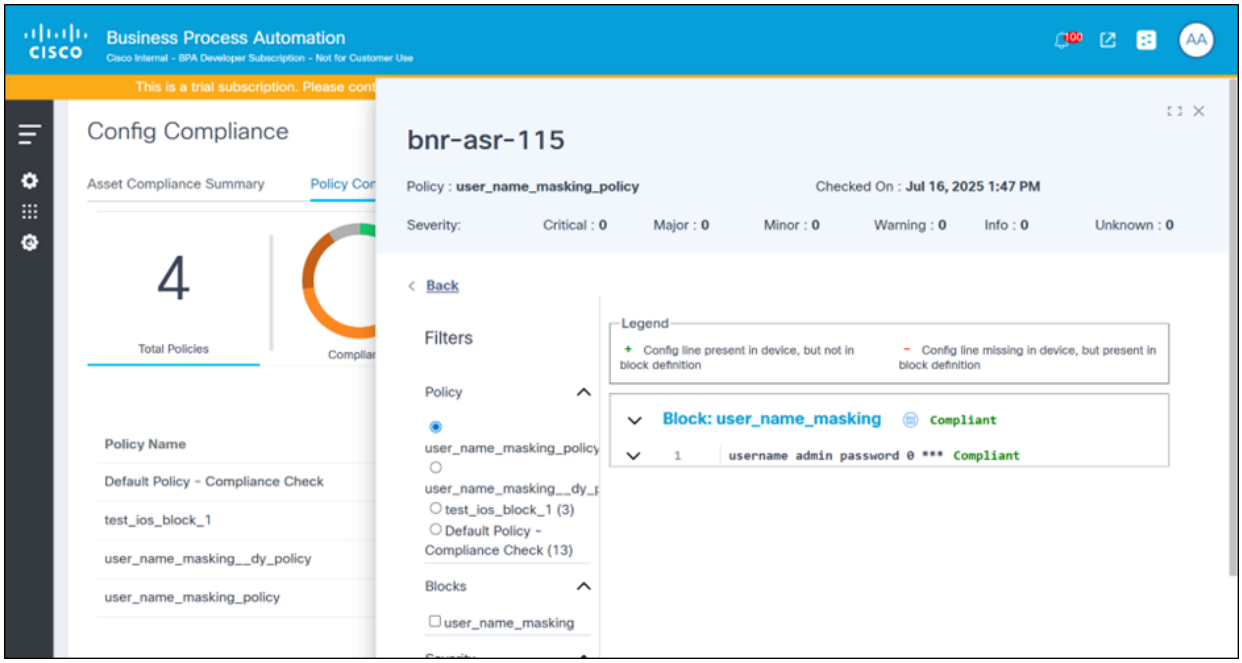
- 指定替换字符串以屏蔽匹配的数据(例如，“”)。例如，Regex模式可以用密码填充（以匹配以“password”开头后跟一个单词的任何文本），并且替换应该为。

2. 根据需要添加尽可能多的regex模式；它们以网格格式显示



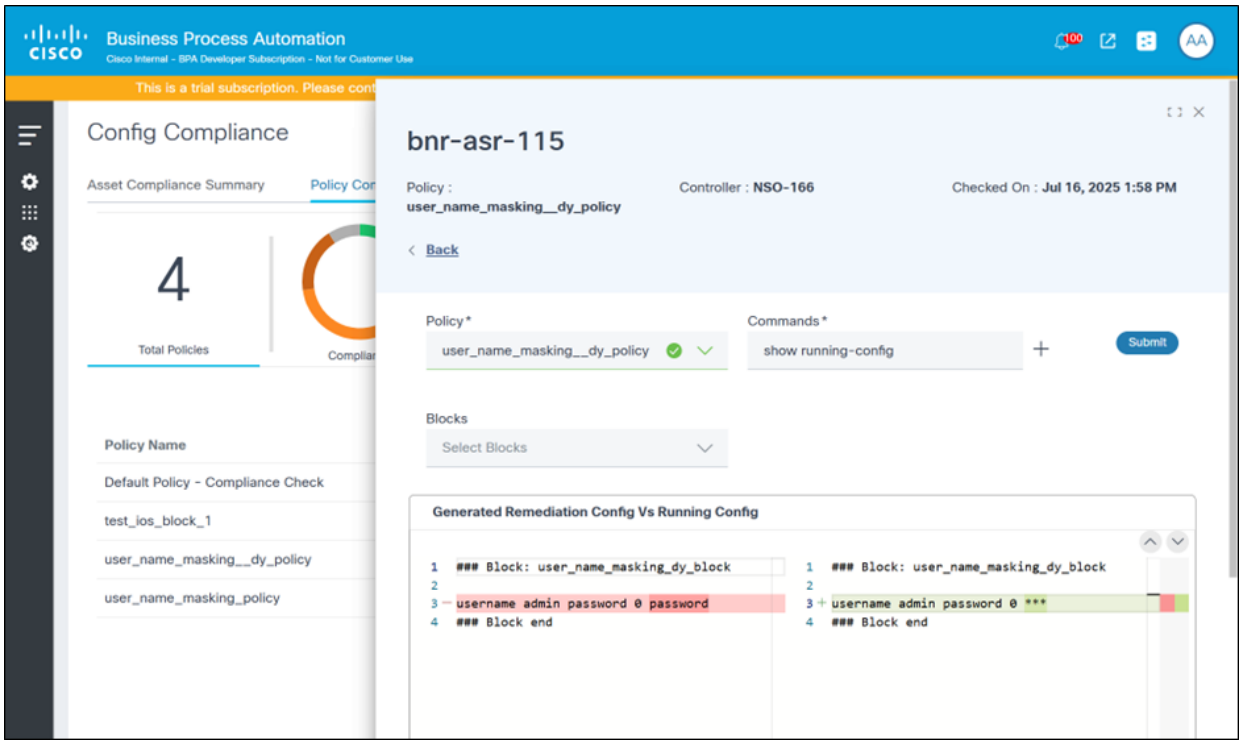
屏蔽敏感数据

3. 从列表中删除不再需要的任何模式。
4. 系统使用正则表达式查找匹配的敏感设备配置数据，并将其替换为指定的掩码(例如“***”)。 此掩码用于以下页面：
   - 合规性控制面板>受影响的资产>查看违规页面:UI中显示的配置数据，以及根据这些违规详细信息生成的资产合规性报告



在查看违规页面中屏蔽敏感数据

- 合规性控制面板>查看补救配置>查看补救差异(View Remediation Diff)页:设备配置数据根据块的掩码设置显示屏蔽的敏感数据

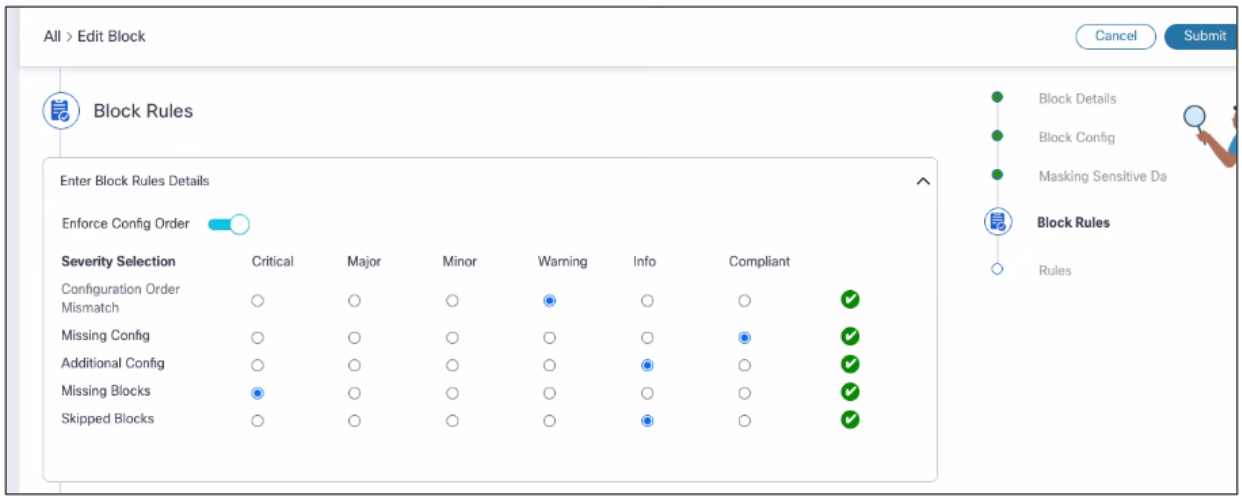


在补救差异页中屏蔽敏感数据

- 阻止规则（严重性选择）：

  Block Rules部分包括：

  - 强制配置顺序:确保配置行在合规性检查期间以正确的顺序显示。合规性引擎根据预期订单检查配置行的顺序。
  - 严重性选择：允许用户为块中的违规指定严重性级别。严重性级别有助于有效地确定和管理合规性问题。
  - 配置顺序不匹配:按照配置行的顺序识别差异，并在设备配置行的顺序与预期顺序不匹配时发出警报。
  - 缺少配置:
    - 检测缺少的配置行
    - 突出显示设备配置中没有的预期配置行
    - 检查整个设备配置块是否丢失或与定义的块配置不匹配
  - 其他配置:
    - 标识意外的配置行
    - 显示设备配置中存在但根据块配置不需要的配置行
  - 跳过的块:
    - 表示未检查的配置块
    - 如果块不符合指定的过滤条件，则会跳过该块



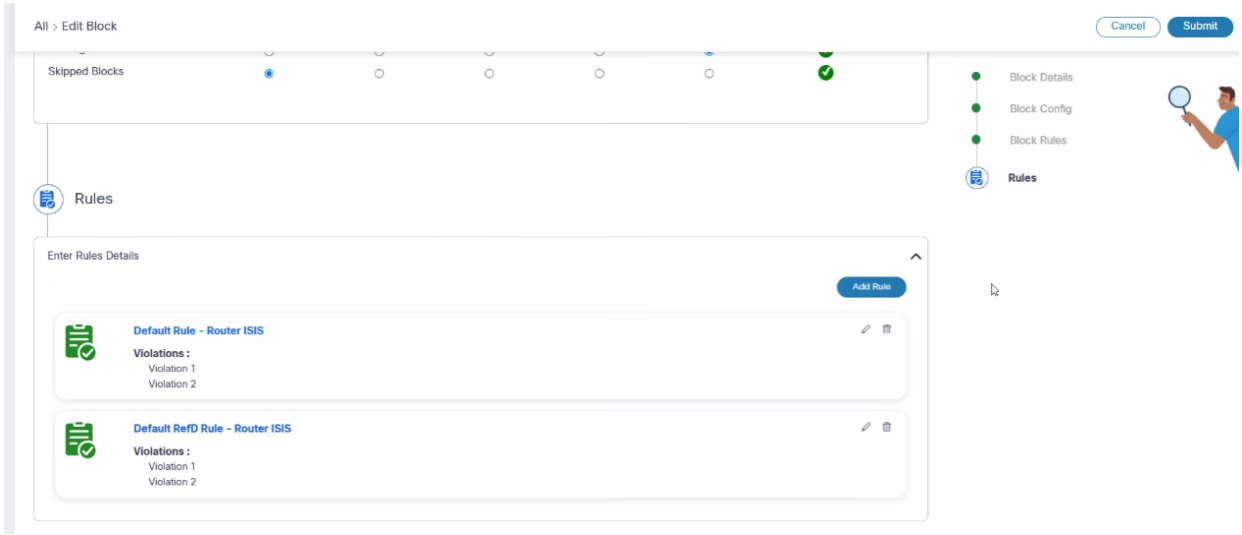
添加或编辑Block-Block规则

规则管理

在CnR框架中，用户可以通过“添加或编辑块”界面管理块规则。此功能的结构如下节所示：

> 注意：如果用户不想引发特定块级别违规，可以选择严重级别“Compliant”。

- 规则配置:
  - 用户可以设置和管理合规引擎用于验证配置的规则
  - 用户可以根据需要创建、编辑或删除规则
- 规则列表:
  - 提供所有已创建规则的全面列表，提供其详细信息的可视性
  - 用户可以编辑现有规则或删除不再需要的规则



添加和编辑配置块

添加或编辑规则详细信息

- 规则名称:
  - 为规则分配唯一名称以进行标识
  - 此字段为必填字段，以确保可以明确识别每个规则
- 默认规则:
  - 指定是否应将规则设置为默认规则
  - 用户可启用此设置以使规则成为合规性框架中的默认值
- 描述:
  - 提供有关规则的其他上下文或信息
  - 此字段为可选字段，但有助于文档和清晰度
- 违规:
  - 管理与规则关联的违规列表
  - 用户可以根据需要添加、编辑或删除违规

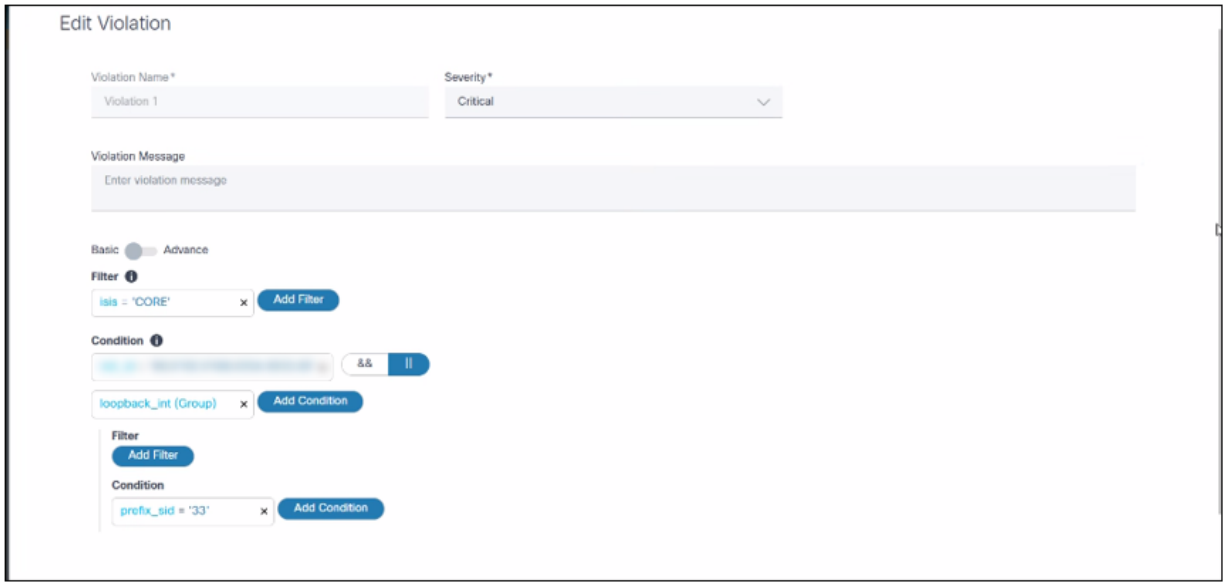
	A	B	C	D	E	F	G	H	I	J	K
1	Device Name	Managed By	Product Family	Compliance	Critical	Major	Minor	Warning	Info	Unknown	Last Checked
2	CNC-bnr-asr-78	Direct-To-Device	IE 2000 Series	Non Compliant	1	0	0	0	0	0	04-Aug-25
3	D2d-118	Direct-To-Device	IE 2000 Series	Partially Compliant	0	1	0	1	1	0	04-Aug-25
4	D2d-juniper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

添加或编辑Blocks规则：添加或编辑规则

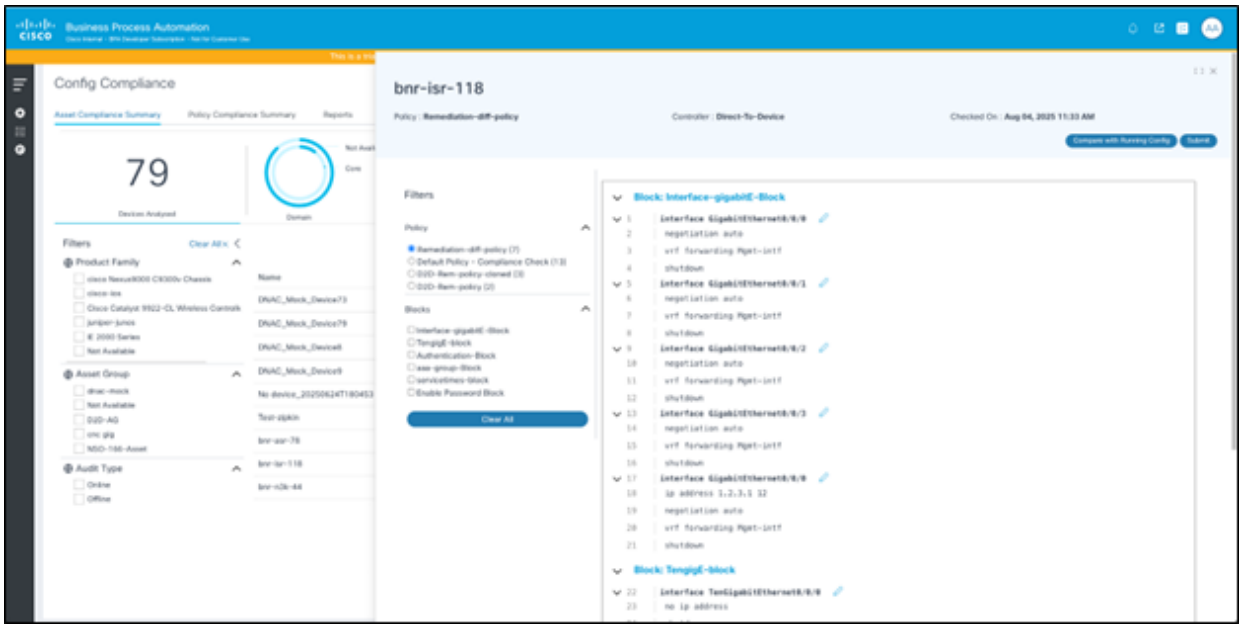
添加或编辑规则违规

规则违规是合规性执行中的一个关键组件，详细说明了需要执行的特定检查。以下概述如何创建和管理规则违规：

- 基本模式:
  - 用户界面元素:此模式允许用户使用图形用户界面(GUI)创建规则违规。 这种方法通常更便于用户使用，且便于那些不愿意使用编码的人使用。
  - 分步指导:使用预定义的UI元素指导用户完成检查定义过程。
- 高级模式:
  - 类似JSON的代码格式:对于习惯编码的用户，此模式允许以结构化、类似JSON的格式键入规则违规来创建规则。
  - 灵活性和精度:此方法为定义复杂的规则检查提供了更大的灵活性和精确度。



创建或编辑规则违规 — 基本模式



创建或编辑规则违规 — 高级模式

规则违规包括以下部分：

- 违规名称:违规名称
- 严重级别:定义在执行期间此违规失败时的合规性严重性
- 违规消息:违规检查失败时会显示该消息
- 违规过滤条件:应用可以使用非组架构变量的违规条件
  - 在过滤条件中用于根据不属于组的各个数据元素设置条件
  - 使用户能够根据数据的层次结构和选择标准，确保精确和相关过滤
- 规则条件:此处可以使用组和非组架构变量检查符合性的实际条件
  - 这两种类型的变量都用于规则中，以创建全面的条件
  - 组变量:允许对相关数据的收集应用条件，确保结构化组内进行全面检查

- 非组变量:允许条件应用于独立的数据元素，在规则应用中提供灵活性

动态用户定义的块 — 最佳实践

- 确保变量名称在每个块内是唯一的。
- 避免在组名中使用变量。
- 对于子层次结构配置，请在块中使用“<group>”。

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

- 要捕获单个变量中类似配置行的值，请使用以下变量：`{{ <<var-name>> |行 | joinmatches(',')}}`。将配置行包含在`{{ start }}`和`{{ end }}`内，如以下示例所示：

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

- 要从配置行捕获包含空格的值，请使用块中的变量，如下表所示：`{{ <<var-name>> | re("。*")}`

设备配置	阻止配置
interface HundredGigE0/0/1/31	interface {{ INTF_ID }}
描述接口：12ylaa01 Hg0/0/1/31	description {{ INTF_DESC | re("。*")}
mtu 9216	mtu 9216

了解规则层次结构以及规则与非RefD规则中的集成

在动态块TTP中，有两个不同的方案决定了如何构建和验证配置。

- 基于组的方案:
  - 此模式以分层方式组织配置，在元素之间建立父子关系
  - 适用于元素逻辑嵌套且相互关联的复杂配置
  - 可以定义规则，以验证不同配置元素之间的分层关系和依赖关系
- 非基于组的方案:
  - 配置以平面格式构建，所有元素存在于同一级别，没有层次关系
  - 适用于不需要层次结构的较简单配置
  - 可以设置规则以确保每个配置元素满足特定条件

RefD集成

- 参考文献的目的:
  - 角色:用作管理BPA框架中的本地和外部变量的工具
  - 功能:
    - 动态获取:促进动态检索和管理可变数据，允许符合性检查适应实时数据变化
    - API交互:为BPA使用案例提供API以访问和管理这些动态变量和值，从而确保顺利集成到合规性工作流程中

合规性规则值的语法

CnR使用案例与RefD框架集成，可在合规性检查和补救工作流程中动态利用数据。此集成工作原理的详细细分（尤其是重点介绍所用变量的语法和类型）如下所示：

- 关键字:语法必须以“RefD”开头
- 参数:在语法中，“key”参数是必需的
- 示例：

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

变量类型

- 用户定义的变量:
  - 在创建合规性作业期间配置。
  - 范围:适用于指定作业的所有执行
  - 语法:`{$VarName}`
  - 示例：`{$SITE}`
- 系统变量
  - 由框架根据执行期间可用的上下文数据预定义

    - 目前，框架提供对设备对象的访问
    - 语法:`{{#VarName}}`
    - 示例：
        - `{{#device.deviceIdentifier}}` — 表示设备标识符
        - `{{#device.additionalAttributes.serialNumber}}` — 表示设备序列号
- TTP变量
    - 存在于块配置中
    - 语法:`{{ VarName }}`
    - 示例：`{{ INT_ID }}`

非RefD规则

- 这些规则类似于RefD规则，但不以“RefD”关键字开头
- 示例：

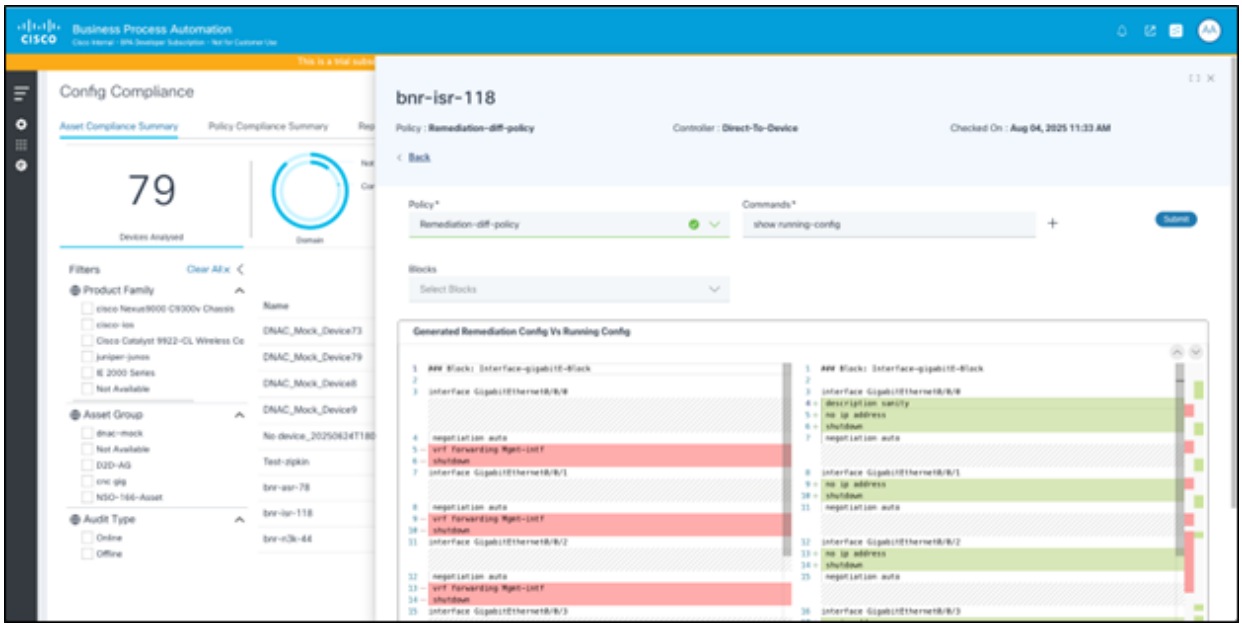
```
plaintext
Copy Code
{$int_id}.{{#device}}.{{ mtu_val }}
```

变量使用

- 用户定义的变量:表示为`{$Var}`
- 系统变量:表示为`{{#Var}}`,显示属性，例如deviceIdentifier、controllerId、controllerType等。
- TTP变量:在双花括号中表示为`{{var}}`

执行

- 在创建作业期间，如果指定了$变量，则可以设置它们的值
- 将变量中的组合值与获取的设备配置进行比较，以确保合规性



设备配置

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

配置规则:参考数据

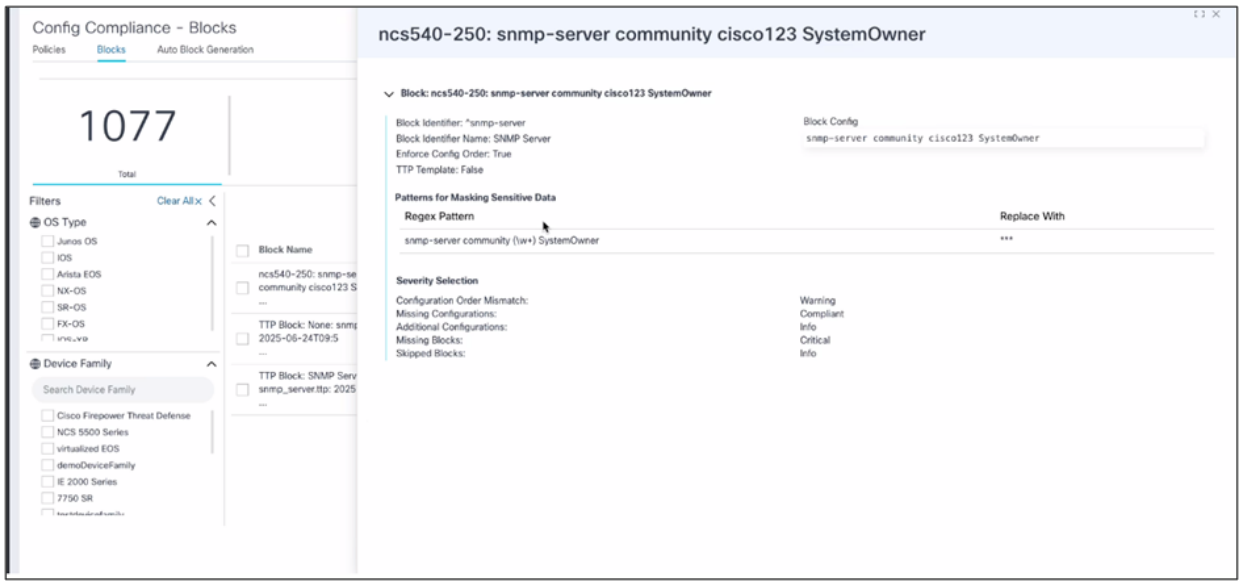
查看阻止详细信息

要访问阻止详细信息，请执行以下操作：

1. 导航到Blocks页面。
2. 选择或单击网格中的行以查看特定块的详细资料。屏幕右侧将显示Block Details页。

注意：此页面提供与块相关的所有信息的只读视图，包括关联的块、规则和任何违规。

点击详细信息中的超链接（如果有），会将用户重定向到相关块或相关信息。



阻止详细信息视图

删除块

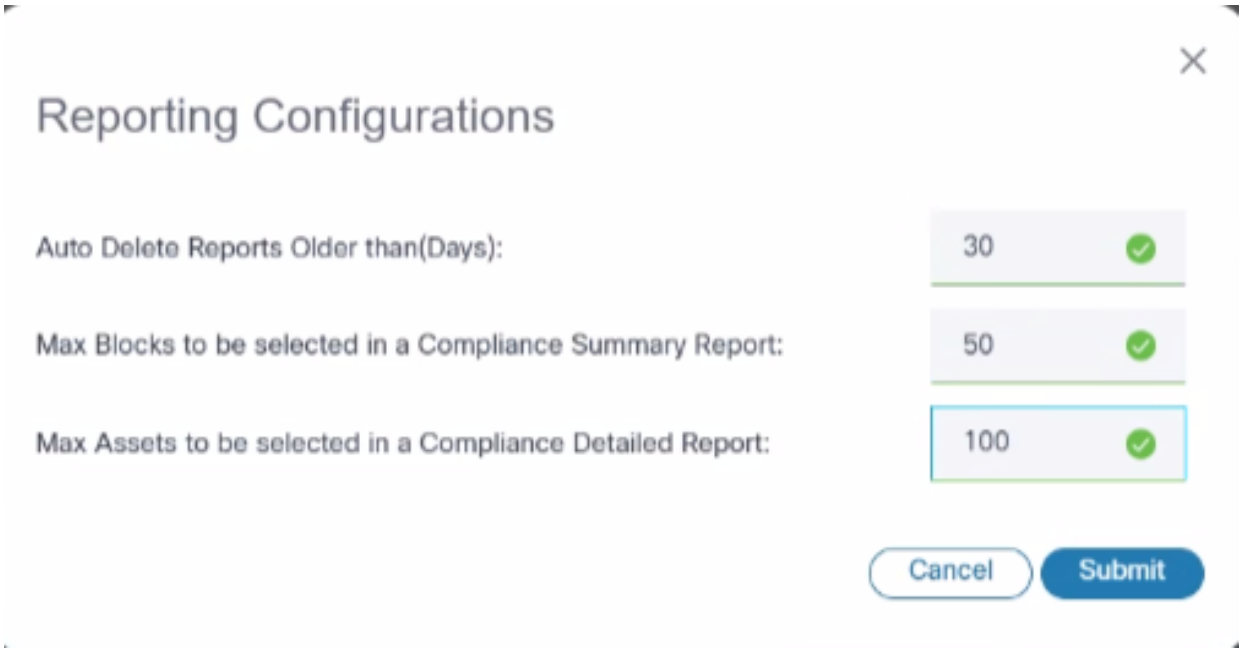
门户允许用户删除一个或多个块，只要他们具有适当的RBAC权限。用户可以通过完成以下步骤执行这些操作：

对于单块删除：

1. 导航到Blocks页面。
2. 点击要删除的块旁边的更多选项图标。
3. 选择Delete选项。系统随即会显示确认消息。

对于多块删除：

1. 导航到Blocks页面。
2. 选中要删除的每个块旁边的复选框。
3. 单击More Options图标并选择Delete。确认消息。

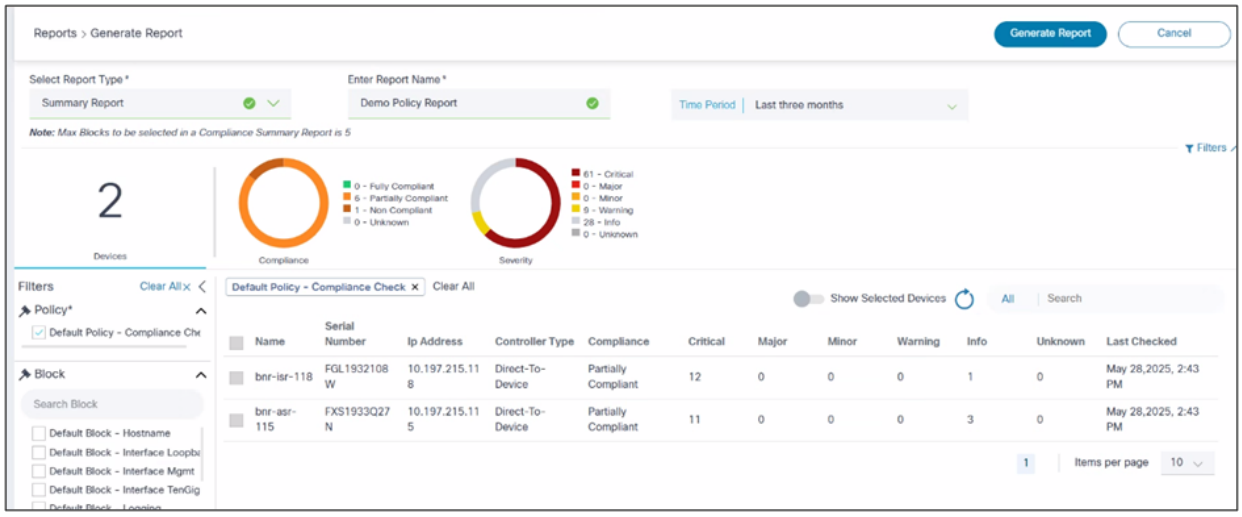


删除块

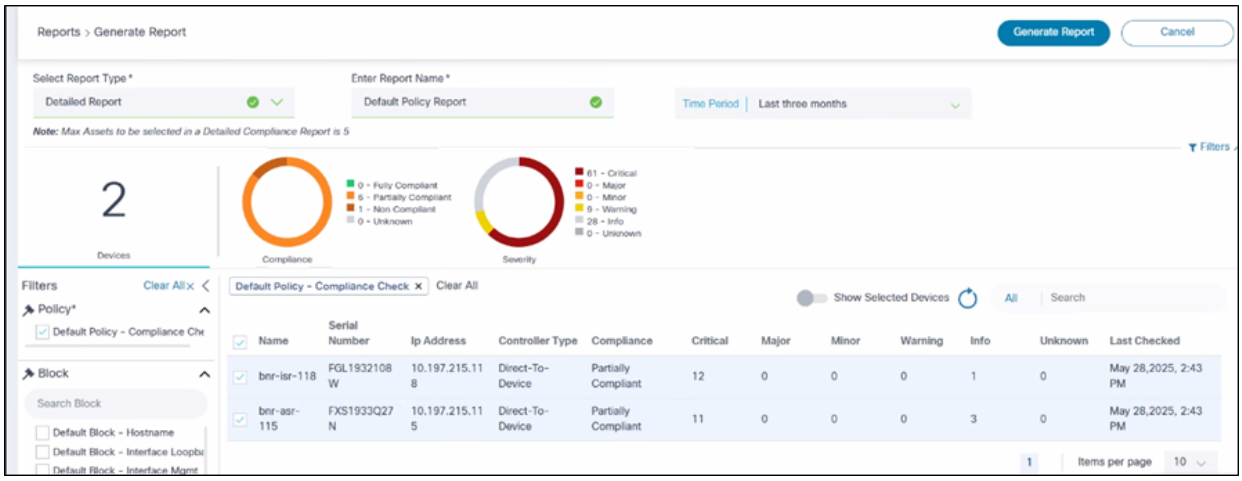
配置:自动生成块

块生成允许用户根据设备的配置自动创建块。这种自动化减少了手动创建所需的时间和精力，使用户可以通过添加或删除变量来更轻松地编辑块，而不是从头开始。

单击某一行可查看块生成详细信息。

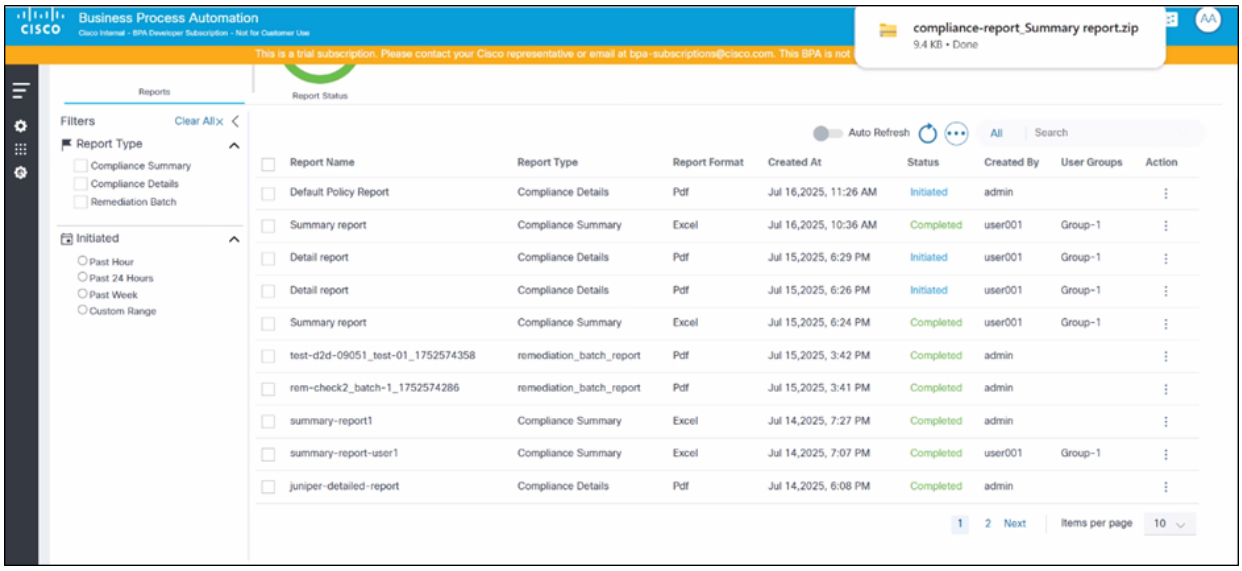


自动阻止生成列表 — 视图



自动块生成详细信息

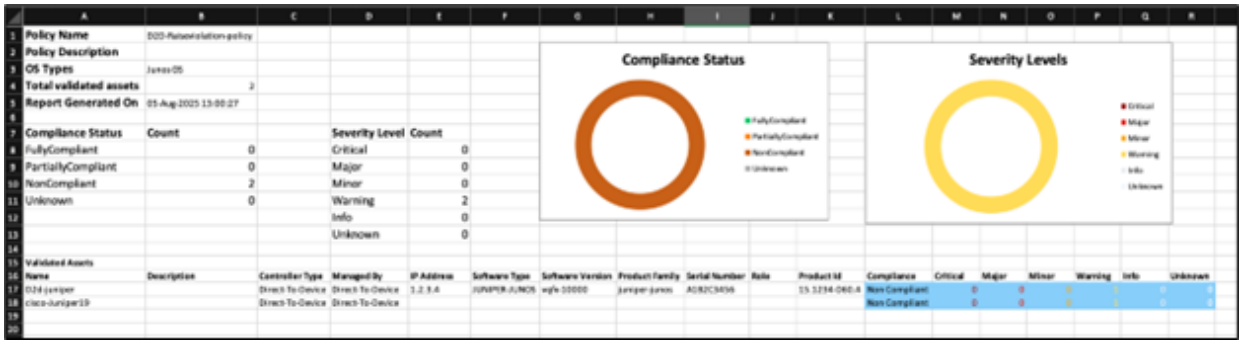
自动生成块



自动阻止生成列表

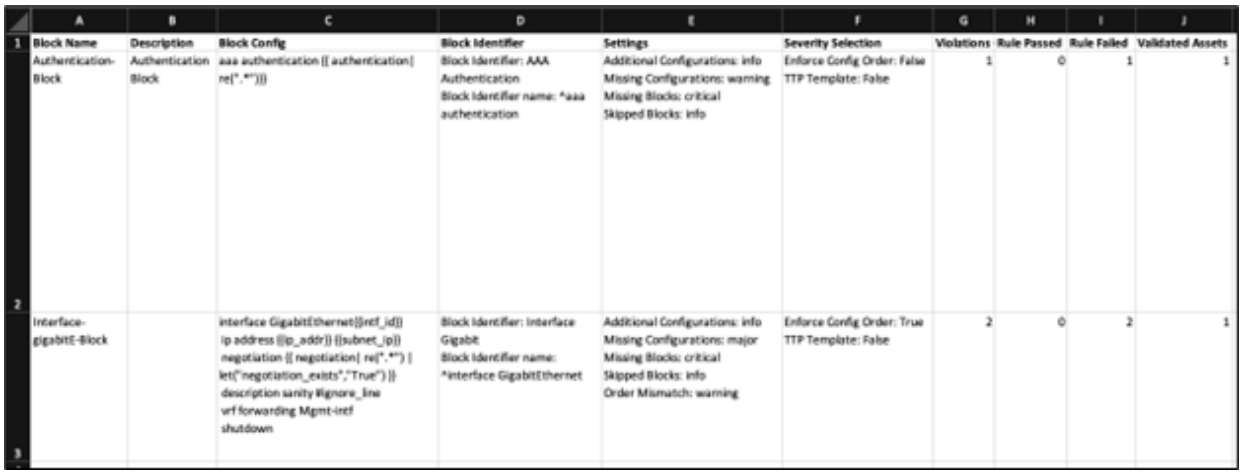
Automatic Block Generation页包含以下字段：

- 生成源:生成块的源。它有以下三个选项：
  - 设备配置备份:系统从备份使用案例中选择设备配置



设备配置备份

- 文件上传:用户可打开“文件上传”窗口上传设备配置



	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

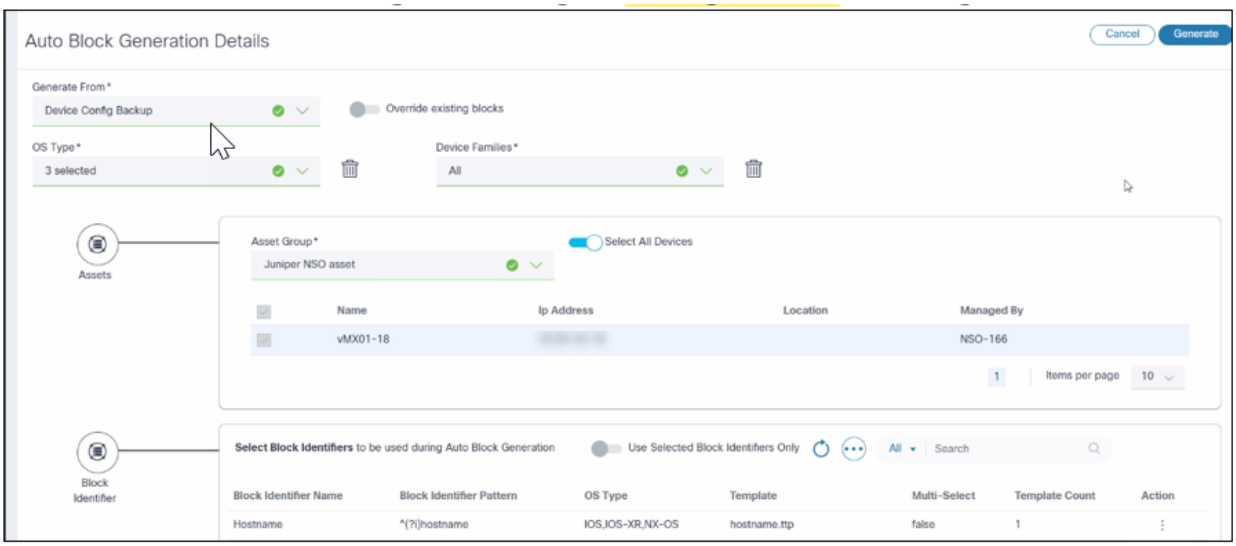
文件上传

- 当前配置:输入系统用于获取设备配置的CLI配置命令。

	A	B	C	D	E	F	G
1	Rule Name	Rule Description	Violation Name	Description	Severity	Violation Count	Affected Assets Count
2	Gigabit Rule	Rule to validate violations for 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							

当前配置

- 操作系统类型：与此块相关的操作系统类型列表。
- 设备系列:与此块相关的设备系列的列表。
- 资产:Assets功能提供了一种结构化方法，用于选择生成动态块的设备
  - 资产组选择:
    - 允许用户选择预定义的设备组（称为资产组），用于生成动态块
    - 根据特定条件（如位置、类型或功能）对设备进行分组，从而便于管理和组织设备
  - 子集设备选择:
    - 用户可以灵活选择所选资产组内的特定设备子集
    - 使用户能够专注于特定设备段，实现更有针对性的数据块生成和管理



块生成

- 块标识符:为用户提供用于选择块生成期间使用的块标识符列表的选项。它还内联提供块标识符管理功能。

块标识符

块标识符使用CiscoConfParser从整个设备配置中提取配置块。每个块标识符应与regex模式相关联。用户可以使用UI或API创建自己的块标识符或更新现有块标识符。该平台目前提供大约55-60个默认块标识符。每个标识符对于OS类型是唯一的，并且在BPA应用部署期间通过Ingester服务进行加载。TTP模板可以与每个块标识符相关联。块标识符的名称和模式都必须是唯一的。

如果为块标识符启用了Multi选项，则合规性框架会从匹配的配置生成多个配置块。否则，它会将所有匹配的配置视为一个块。

Multi option True的块标识符示例：接口、路由器bgp、vrf、l2vpn等

Multi option False的块标识符示例：日志记录、snmp-server、域等

示例：

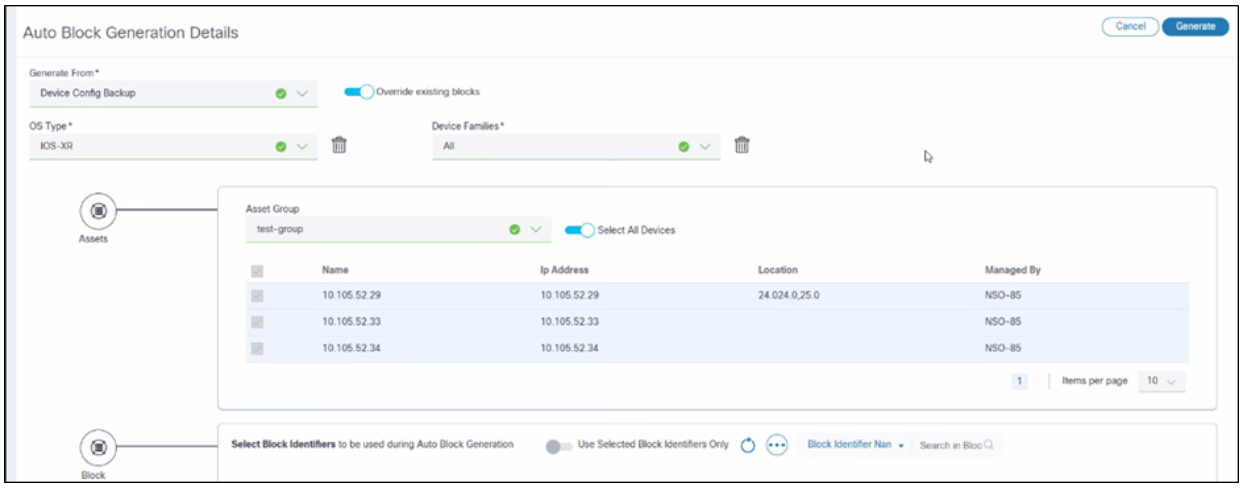
```
{
  “name”: “BundleEthernet Interface”,
  “osType”: [“IOS”, “IOS-XR”, “NX-OS”],
  “multi”: true,
  “blockIdentifier”: “^(?i)interface Bundle-Ether”,
  “templates”: [“parent_interface.ttp”]
}

{
```

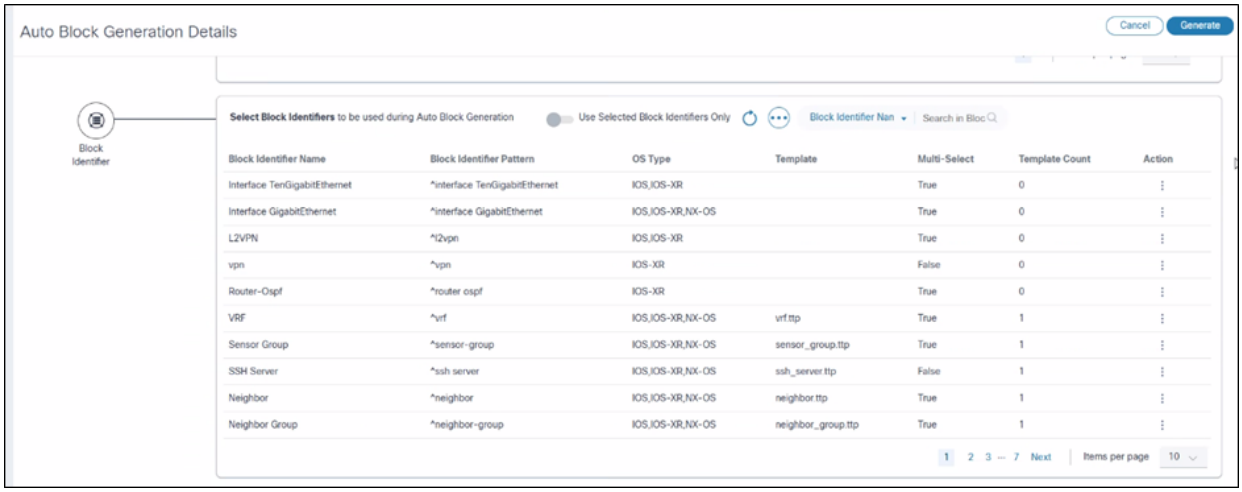
```
  “name”: “Loopback Interface”,
  “osType”: [“IOS”, “IOS-XR”, “NX-OS”],
  “multi”: true,
  “blockIdentifier”: “^(?i)interface Loopback”,
  “templates”: [“parent_interface.ttp”]
}
```

列表块标识符

列表块标识符允许用户查看块标识符列表以及搜索和排序功能。Generate Blocks页面中提供了此功能。

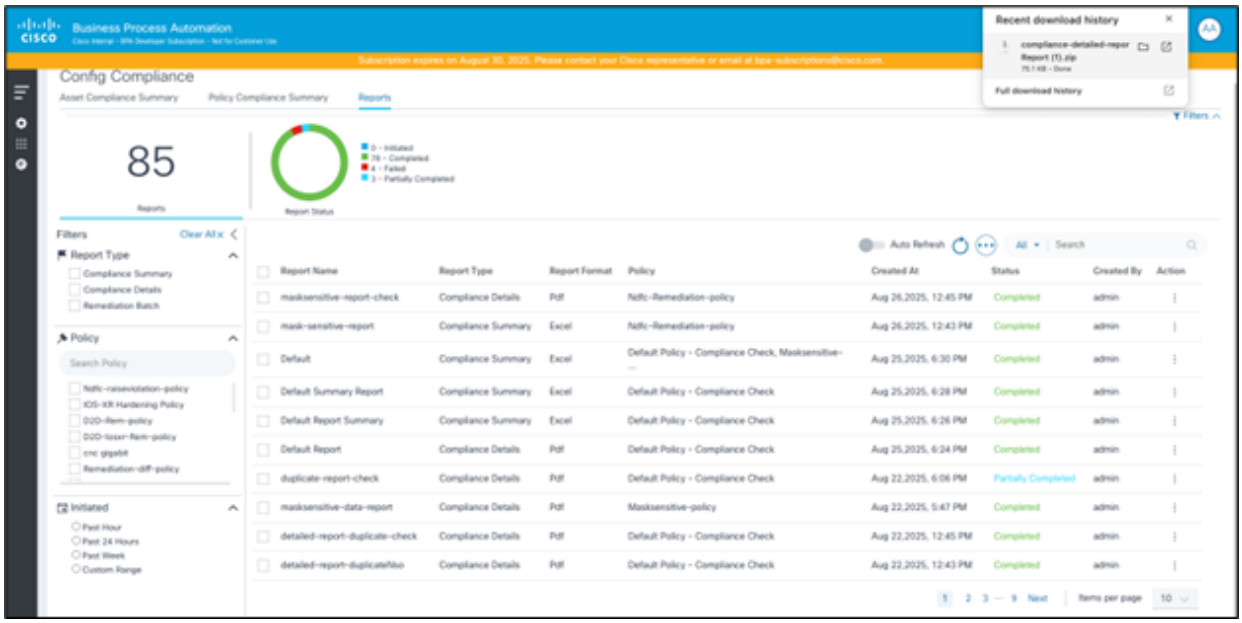


阻止标识符列表



块标识符

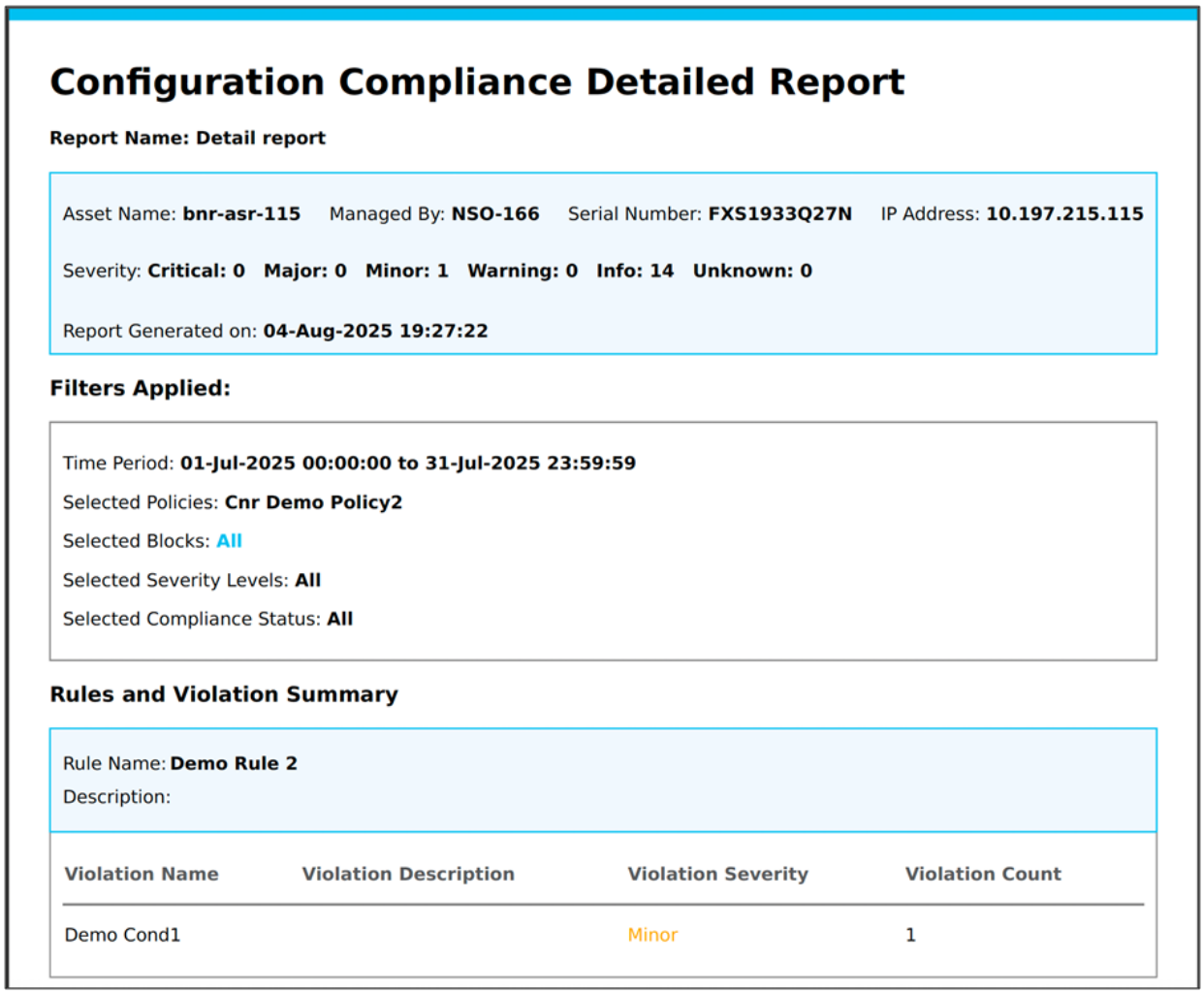
创建或编辑块标识符



编辑块标识符

Auto Block Generation页面上的Block Identifier List部分为用户提供有效管理块标识符的工具。功能如下所示：

- 创建块标识符
  - 用户可以将新的块标识符添加到列表中
  - 这允许引入可用于组织和区分块的唯一标识符
- 编辑块标识符
  - 可以修改现有的块标识符
  - 启用标识符更新或更正，确保标识符保持准确且与其代表的块相关
- 删除块标识符
  - 用户可选择从列表中删除阻止标识符
  - 通过允许删除不再需要的标识符或不再适用的标识符来简化标识符管理



Configuration Compliance Detailed Report

Report Name: Detail report

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

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

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

Filters Applied:

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

Selected Policies: **Cnr Demo Policy2**

Selected Blocks: **All**

Selected Severity Levels: **All**

Selected Compliance Status: **All**

Rules and Violation Summary

Rule Name: **Demo Rule 2**

Description:

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

删除块标识符

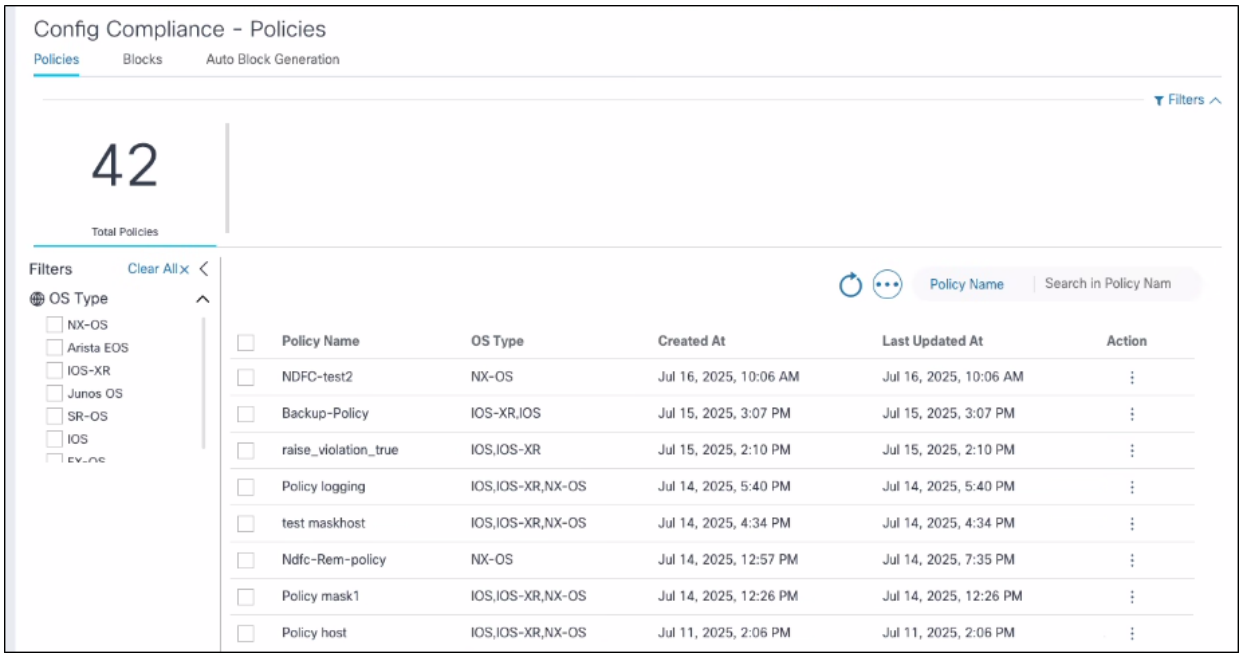
配置:策略

可以在Policies选项卡上定义一组策略、规则和块以启用合规性执行。策略是由配置块和规则组成的用户定义的模板。可以选择用于创建策略的配置块列表和每个配置块的规则列表。

列出策略

策略列表可以显示在Policies选项卡上，该选项卡还提供用于添加、编辑、删除、导入和导出策略的操作。

注意：策略会与相关的块和规则一起导入或导出。



列出策略

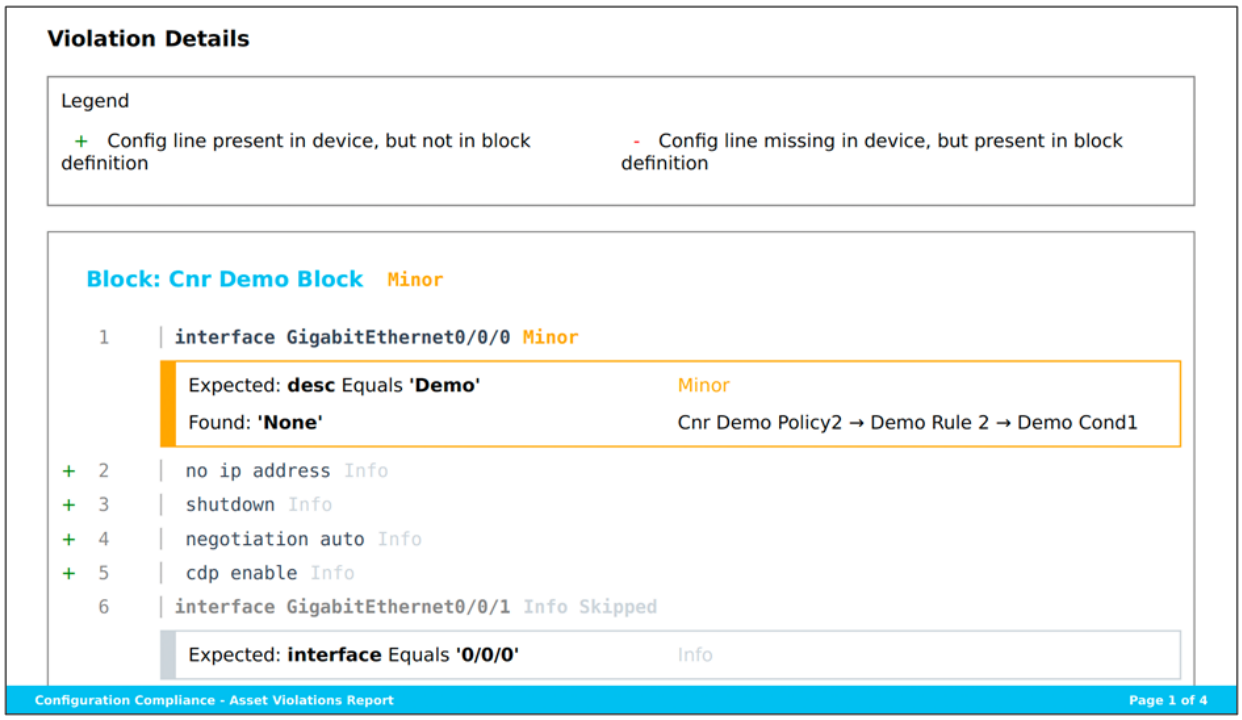
添加和编辑策略

本节概述了Add Policy和Edit Policy页：

策略详细信息

- 策略名称：策略名称
- 操作系统类型：此策略支持的操作系统类型列表
- 设备系列:此策略支持的设备系列列表
- 策略说明（可选）:使用简短描述描述策略

OS Type和Device Family字段会根据下一部分中的选定块自动填充。

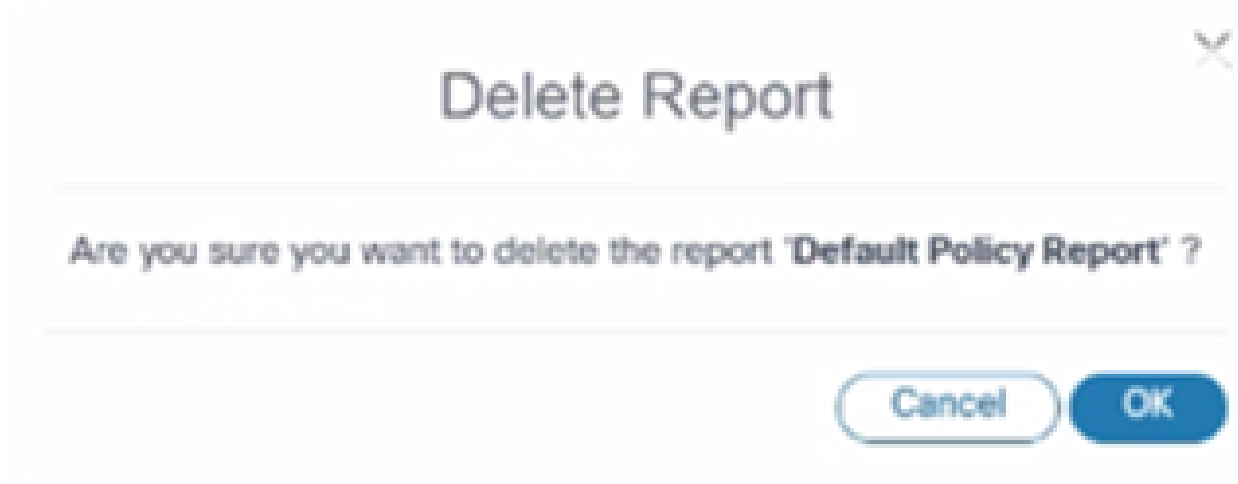


配置策略：策略详细信息

“选择块”对话框

“选择块”(Select Blocks)功能是一个用户友好的界面，旨在帮助用户选择包含在策略中的配置块。其功能在本节中列出：

- 弹出对话框
  - 目的:为用户提供一个专用空间，用户无需离开当前页面即可选择配置块
  - 用户交互:通过在单独的重点对话框中演示选项，确保直观的选择流程
- 添加和选择选项
  - 多个选择:用户可以选择一个或多个要包含在策略中的配置块
  - 灵活性:支持根据用户的特定策略要求包含各种块
- 导航功能
  - 过滤器:允许用户根据特定条件缩小可用块列表，从而更轻松地查找相关块
  - 分页:将块组织成可管理的页面，从而改善通过大量数据的导航
  - 搜索功能:支持按名称或其他标识符快速定位块，简化选择过程



块选择

用户可以通过点击“块选择”部分中的创建来创建新块。新的浏览器选项卡会交叉启动，用户可创建新块。提交后，用户可以返回到原始选项卡，并选择新创建的块以将其添加到策略。

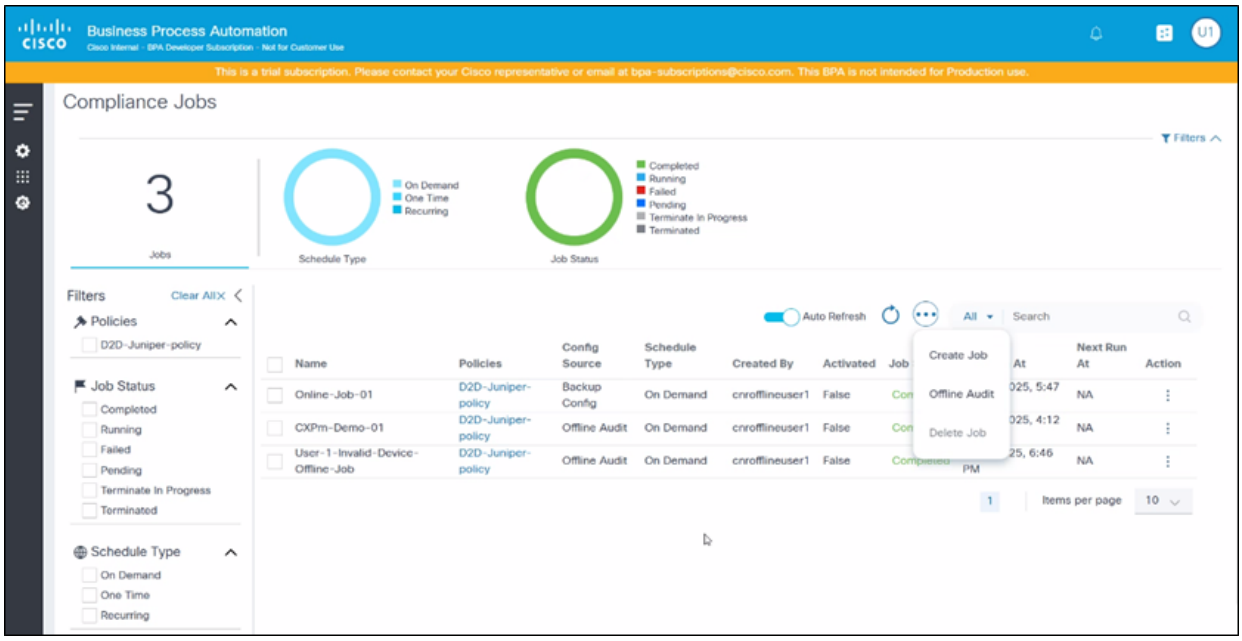
条件过滤器

Conditional Filters功能是一种高级工具，允许用户将特定条件应用于配置块，从而确保精确且有针对性的合规性检查。

- 允许用户根据预定义条件应用配置或对所选配置块运行合规性检查
- 通过过滤掉不符合指定标准的资源块，将资源和工作集中在相关块上
- 用户可以定义配置块必须满足的条件，以便包括在合规性检查或其他流程中
- 仅执行符合这些条件的块，而忽略其他块，从而允许更精确的控制

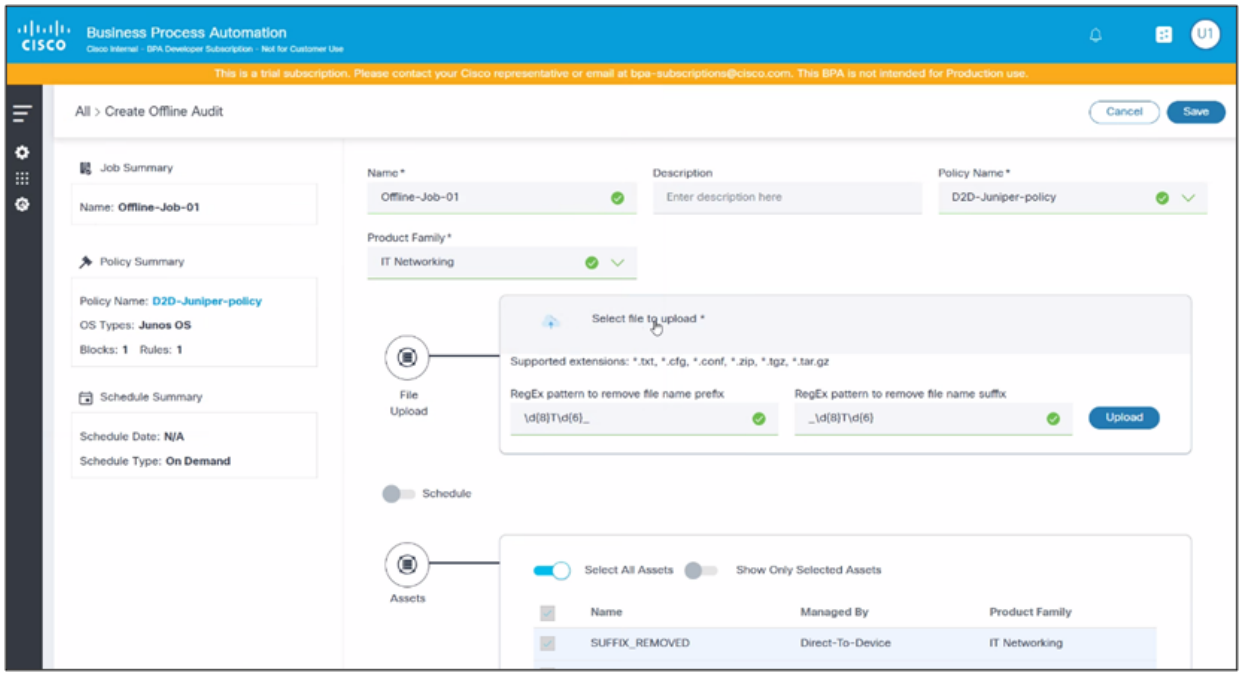
使用案例示例:

- 选择性合规性检查：如果策略旨在检查可用的20个接口中的两个特定接口上的配置，则用户可以设置条件以将合规性检查限制为仅检查这两个接口。



条件过滤器

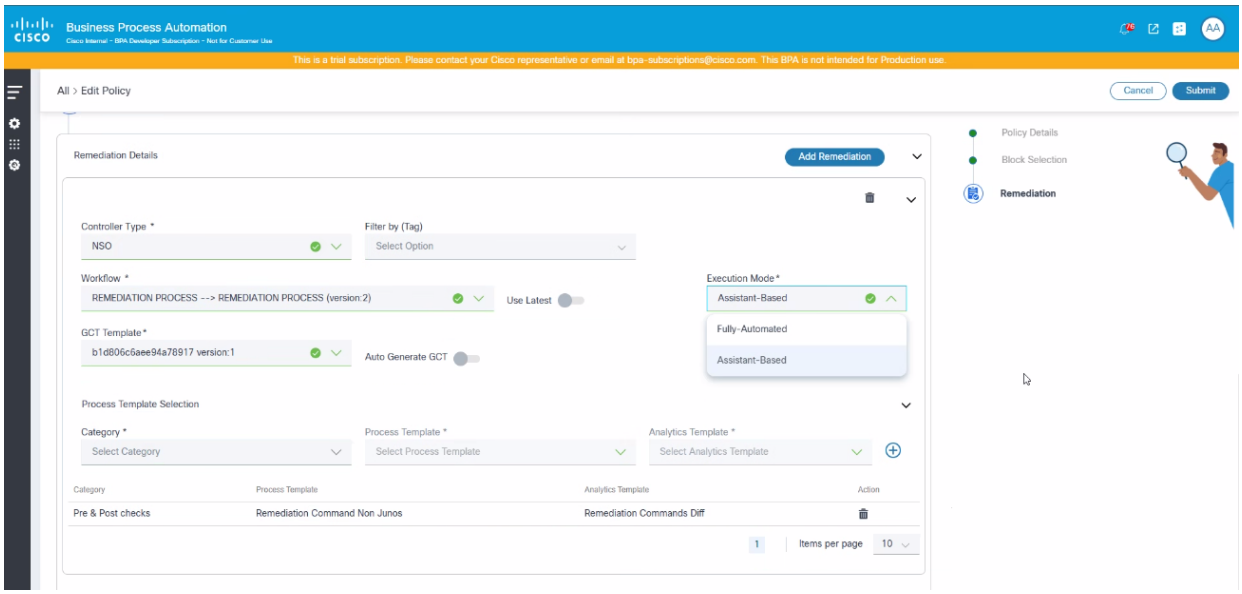
- 选择规则:用于为给定配置块选择一个或多个规则的选项。



选择规则

Remediation部分

Policies页面提供了一个可选部分，用于按控制器类型定义补救详细信息。



配置策略：补救详细信息

- 控制器类型:支持补救的控制器类型列表
- 补救工作流程:为所选控制器类型的设备执行的工作流程
- GCT模板:要应用的一个或多个GCT模板
- 流程模板：要作为预检查和后检查的一部分执行的一个或多个流程模板以及相应的分析模板。
- 预检查模板:可选的流程模板列表，仅用于预检查
- 后检查模板:可选的流程模板列表，仅对后检查执行
- 执行模式:
  - 完全自动:补救过程自动运行，无需手动干预或用户任务
  - 基于助理:系统在补救过程中创建需要手动协助的用户任务

自动生成GCT功能

自动生成GCT功能旨在简化创建补救所需的GCT模板的流程。具体工作如下：

- 根据合规性执行的结果和详细信息自动生成GCT模板
- 自动化模板创建流程
- 生成的模板经过定制，可解决在合规性检查过程中发现的问题，确保补救措施与合规性需求保持一致

角色和访问控制

静态权限列表

下一代门户中的配置合规性控制面板支持BPA的RBAC功能，具有以下权限，这些权限表示如何在GUI表示中显示配置动态文本块，以处理规则和条件：

组	操作	描述
ui-app	complianceDashboard.show	显示/隐藏合规性控制面板应用
ui-app	remediationDashboard.show	显示补救作业应用
ui-app	complianceJobs.show	显示合规性作业应用
ui-app	complianceConfigurations.show	显示合规性配置应用
合规性控制面板	资产合规性摘要	查看资产合规性摘要
合规性控制面板	策略合规性摘要	查看策略合规性摘要
合规性控制面板	viewViolations	查看违规详细信息
合规性控制面板	policyComplianceAssetsSummary	查看受影响的资产
合规性控制面板	查看报告	查看报告控制面板、报告设置和下载报告
合规性控制面板	管理报告	创建和删除报告
合规性控制面板	manageReportSettings	修改报告设置
remediation控制面板	viewRemediationJobs	查看补救作业
remediation控制面板	viewRemediationMilestones	查看补救里程碑
remediation控制面板	manageRemediationJob	管理补救作业，例如创建、删除、存档和处理用户任务
合规性作业	viewComplianceJob	查看合规性作业和执行
合规性作业	manageComplianceJob	管理合规性作业
合规性配置	viewCompliance配置	查看合规性配置，如策略、块、规则、块生成、块标识符和TTP模板
合规性配置	管理合规性策略	管理合规性策略
合规性配置	manageComplianceBlock	管理合规性块和规则以及块标识符
合规性配置	manageComplianceBlockGeneration	管理合规性块生成和TTP模板

预定义角色

配置合规性和补救使用案例具有下表中列出的预定义角色：

注意：管理员可以根据客户要求创建或更新角色。

角色	描述	权限
合规性管理员	具有所有合规性相关权限的管理员角色	UI应用: 显示资产管理器 — 显示资产组 — 查看合规性控制面板 — 显示合规性作业 — 显示合规性配置 资产: 查看资产列表 — 查看资产的备份配置 — 备份配置 — 执行启用控制器的设备操作 资产组: — 查看资产组 — 管理资产组 — 创建动态资产组 备份配置:查看、比较和下载设备配置备份 备份还原策略:查看备份还原策略 合规性控制面板： — 查看资产的合规性摘要 — 查看策略的合规性摘要 — 查看违规 — 查看受影响的资产 创建和删除报告 查看报告控制面板、报告设置和下载报告 修改报告设置： 合规性作业

角色	描述	权限
合规操作员	操作员角色具有除配置管理之外的所有合规性权限	查看合规性作业和执行 — 管理合规性作业 合规性配置: — 查看合规性配置，如策略、阻止和规则 — 管理合规性策略 — 管理合规性块、规则和块标识符 — 管理合规性块生成和TTP模板 UI应用: — 显示资产经理 — 显示资产组 — 查看合规性控制面板 — 显示合规性作业 — 显示合规性配置 资产: 查看资产列表 — 查看资产的备份配置 — 备份配置 — 执行启用控制器的设备操作 资产组: — 查看资产组 — 管理资产组 — 创建动态资产组 备份配置:查看、比较和下载设备配置备份 备份还原策略:查看备份还原策略 合规性控制面板： — 查看资产合规性摘要 — 查看策略合规性摘要 — 查看违规

角色	描述	权限
		— 查看受影响的资产 创建和删除报告 查看报告控制面板、报告设置和下载报告 合规性工作: 查看合规性作业和执行 — 管理合规性作业 合规性配置: 查看合规性配置，如策略、阻止和规则 UI应用: — 显示资产经理 — 显示资产组 — 查看合规性控制面板 — 显示合规性作业 — 显示合规性配置 资产: 查看资产列表 — 查看资产的备份配置 — 执行启用控制器的设备操作
合规性只读	提供与合规性使用案例相关的所有只读权限	资产组: — 查看资产组 备份配置:查看、比较和下载设备配置备份 备份还原策略:查看备份还原策略 合规性控制面板： 查看资产合规性摘要 — 查看策略合规性摘要 — 查看违规 — 查看受影响的资产 查看报告控制面板、报告设置和下载报

角色	描述	权限
补救管理员/补救操作员	具有所有补救相关权限的操作员角色	告 合规性工作: 查看合规性作业和执行 合规性配置: 查看合规性配置，如策略、阻止和规则 UI应用: — 显示资产经理 — 显示资产组 — 查看补救控制面板 资产: — 查看资产列表 资产组: — 查看资产组 管理资产组 — 创建动态资产组 补救控制面板: — 查看补救作业 — 查看补救里程碑 — 查看资产合规性摘要 — 管理补救作业，例如创建、删除、存档和处理用户任务 — 查看受影响的资产
补救只读	提供与补救使用案例相关的所有只读权限	UI应用: — 显示资产经理 — 显示资产组 — 查看补救控制面板 资产: — 查看资产列表

角色	描述	权限
		资产组: — 查看资产组 创建动态资产组 补救控制面板: — 查看补救作业 — 查看补救里程碑 — 查看资产合规性摘要 — 查看受影响的资产

访问策略

访问策略功能可确保用户具有对特定合规性策略和资产组的适当访问权限。此功能允许管理员根据用户角色和责任定义和实施访问控制，从而提高安全性和运营效率。访问策略通过“访问策略”(Access Policy)页面进行管理，管理员可以在其中创建、编辑策略并将其分配给用户或组。管理员可以定义精细权限，指定每个用户或组可以查看、编辑或管理的合规性策略和资产组。这一级别的详细信息有助于保持对敏感信息和关键操作的严格控制。

定义访问策略后，根据当前用户有权访问的CnR策略和资产列表，在下一代UI中的所有合规性和补救页面上限制数据。

要提供用户访问权限，请执行以下操作：

注意：权限只能由管理员提供。

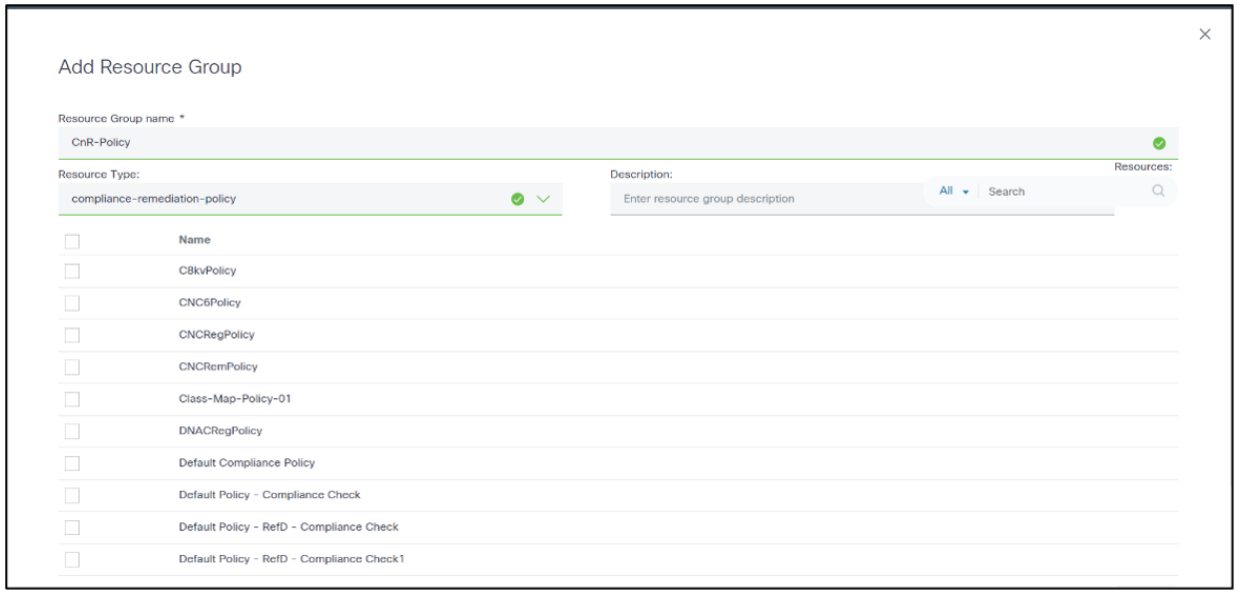
---

1. 创建用户并将他们分配到用户组。
2. 创建用户角色并将其分配到创建的用户组。
3. 将资产添加到资产组。
4. 创建资源组以分配合规性策略资源。
5. 创建访问策略并选择相关用户组、资产组和资源组。

创建资源组

使用Resource Type下拉列表中的compliance remediation-policy创建资源组，并选择需要授予相应

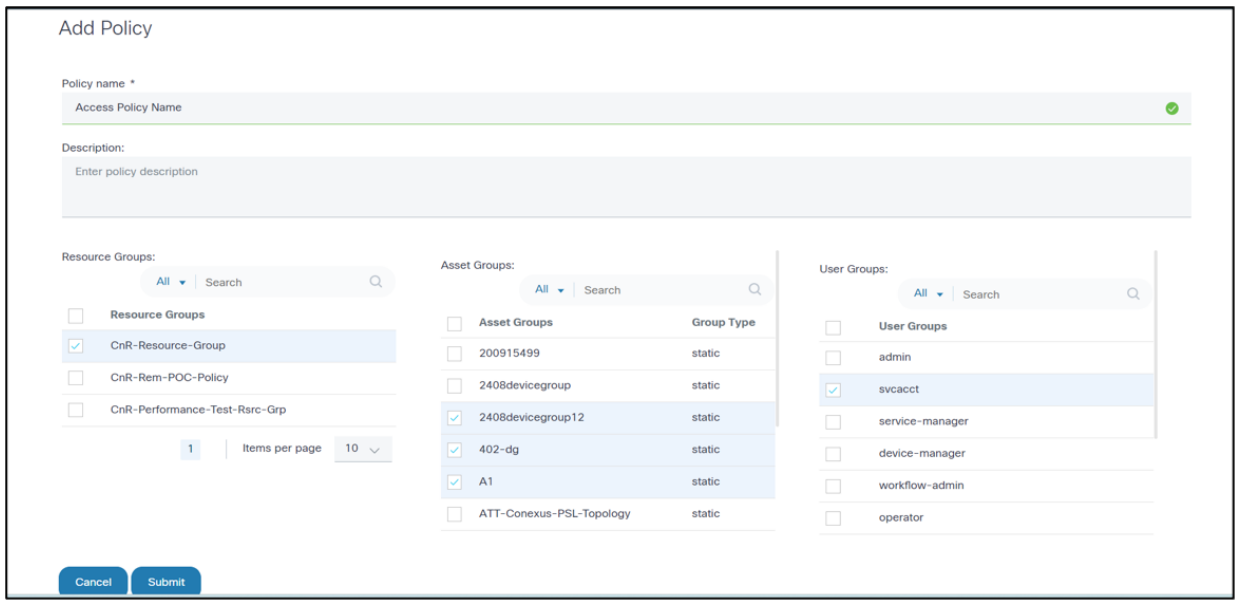
用户组访问权限的合规性策略。



创建资源组

创建访问策略

创建需要授予用户组权限的资源组和资产组的访问策略。



创建访问策略

脱机合规性

离线合规性功能使用户可以对资产资产清单中的活动设备不可用的设备配置运行合规性检查。

用户可以使用设备备份配置或通过在合规性作业中创建脱机审核来运行脱机合规性。可以在“合规性”控制面板上查看执行结果。

使用设备备份配置

管理员可以手动上传包含所需设备集的运行配置的zip文件。此功能在备份和还原应用程序中的“设备配置 — 上传”部分下可用。上传设备配置后，可以通过选择Device Backup Config作为设备配置源来创建所需设备的合规性作业。在执行期间，将从备份应用程序检索已上传的设备配置，并对其执行合规性检查。

在合规性作业中使用创建脱机审核功能

要脱机运行设备配置的合规性，用户可从合规性作业页面上的更多选项图标中选择脱机审核。这允许用户直接在合规性应用程序中手动上传包含运行配置的zip文件。在执行期间，将解析上传的设备配置，并执行合规性检查。

通过Ingester部署配置

合规性配置项目的加载可以使用Ingester框架自动完成。一旦开发工件，就可以使用以下步骤将其导出、打包并部署到目标环境中。

- 使用以下命令创建NPM软件包：

```
mkdir <


      >
cd  <


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

- 从BPA门户导出配置（传统UI）
  - 导航至BPA Classic UI > Configuration Compliance & Remediation > Configurations
  - 导出“TTP模板/块标识符/块/规则/策略”(TTP Templates/Block

Identifiers/Blocks/Rules/Policies)

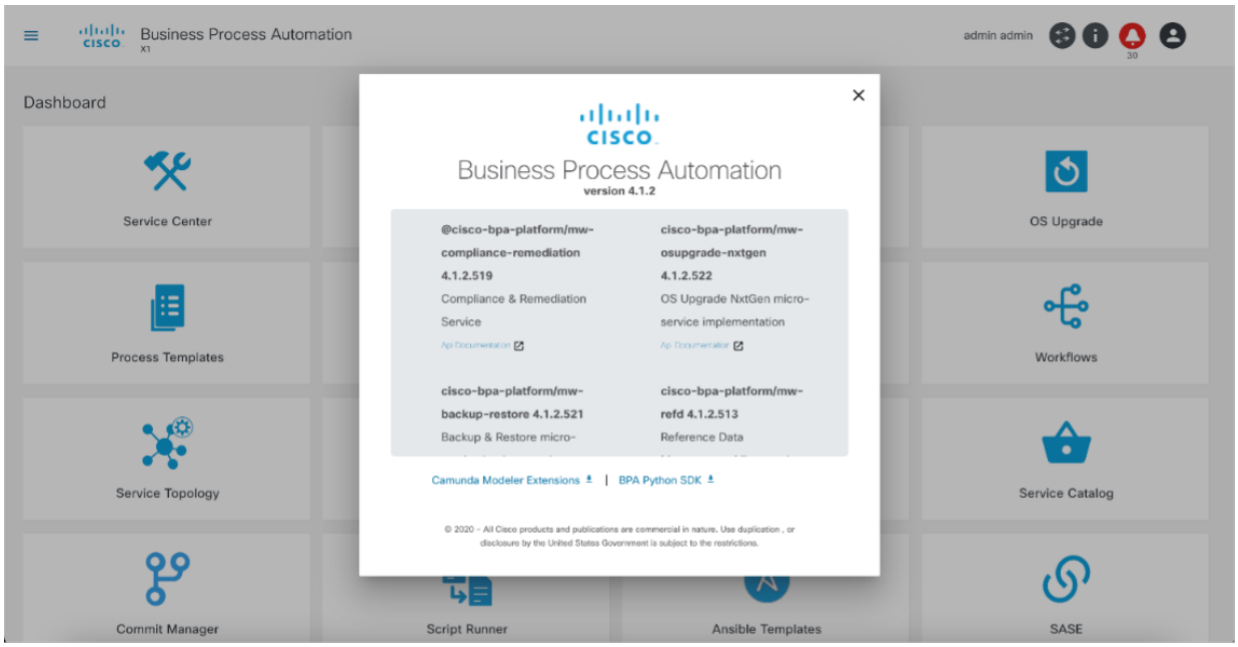
- 按如下方式重命名导出的文件：
  - TTP模板：<<filename>>.cnrttptemplate.json
  - 阻止标识符：<<文件名>>.cnrblockidentifier.json
  - 块：<<filename>>.cnrblock.json
  - 规则：<<filename>>.cnrrule.json
  - 策略：<<filename>>.cnrpolicy.json
- 包入口数据(.tgz)
  - 将所有导出文件复制到“步骤1”中创建的npm软件包中
  - 在npm软件包中运行`npm pack`命令以创建“.tgz”文件
- 将ingester数据(.tgz)部署到BPA单节点环境
  - 将.tgz文件复制到部署BPA捆绑包的服务器中的<<BPA core bundle>>/packages/data文件夹中
  - 重新启动Ingester服务器(docker restart ingester-service)
- 将Ingester数据(.tgz)部署到BPA多节点环境
  - 将.tgz文件复制到部署舵表的服务器中的/opt/bpa/packages/data文件夹中
  - 重新部署Ingester pod(`kubectl rollout restart deployment ingester-service -n bpa-ns`)

参考

名称	描述
TTP	配置块中使用的模板文本解析器
会议解析器	用于分析CLI设备配置的配置字段解析器

API 文档

有关合规性和补救的API文档详细信息可在传统UI“关于”(About)弹出窗口中找到：



BPA关于（传统UI）

故障排除

控制面板

不显示最近的合规性作业结果

观察:最近的合规性作业结果不会显示在下一代门户控制面板中。

潜在原因1:控制面板有一个日期范围选择，默认为“当前月份”。如果最近开始了一个新月（例如，今天是一个月的第一天），则不会显示昨天（上个月的最后一天）之前执行的执行。

分析:确认在控制面板中选择了正确的日期范围（如果需要，包括上个月的日期），以显示正确的违规数据。

潜在原因2:不同的用户可能已在同一策略和/或资产组合上运行了合规性作业。控制面板显示所选日期范围内的最新运行期间发现的违规。

分析:以管理员（或有权访问所有符合性作业的用户）身份，查看符合性作业的列表及其历史记录，以确定执行哪些策略或资产组组合。

合规性作业

整个执行状态设置为“已跳过”

观察:运行合规性作业时，整个执行状态标记为“已跳过”。未报告任何违规事件。

潜在原因:同一作业的现有执行仍在运行。

分析:合规性作业在任何给定时间点只能有一个处于运行状态的执行。验证早期执行是否仍在运行。可以终止停滞或长时间运行的执行/

设备状态设置为“已跳过”

观察:在合规性作业执行中，某些设备的状态标记为“已跳过”。

潜在原因:未为该设备所属的控制器类型启用合规性功能。

分析:合规性策略仅适用于资产组中已启用功能的设备。

设备状态设置为“失败”

观察:在合规性作业执行中，某些设备的状态标记为“失败”。

潜在原因:合规性执行过程中发生的运行时错误。这些错误可能是代码错误或策略、块、规则、块标识符等中的错误配置。

分析:

用于查找运行时错误原因的API:

1. 获取执行以查找执行ID

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

   合规性执行

   方法：GET

2. 使用执行ID获取设备执行

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

   合规性设备执行？

executionId=<<< execution-id >>

方法：GET

合规性规则

规则显示空值

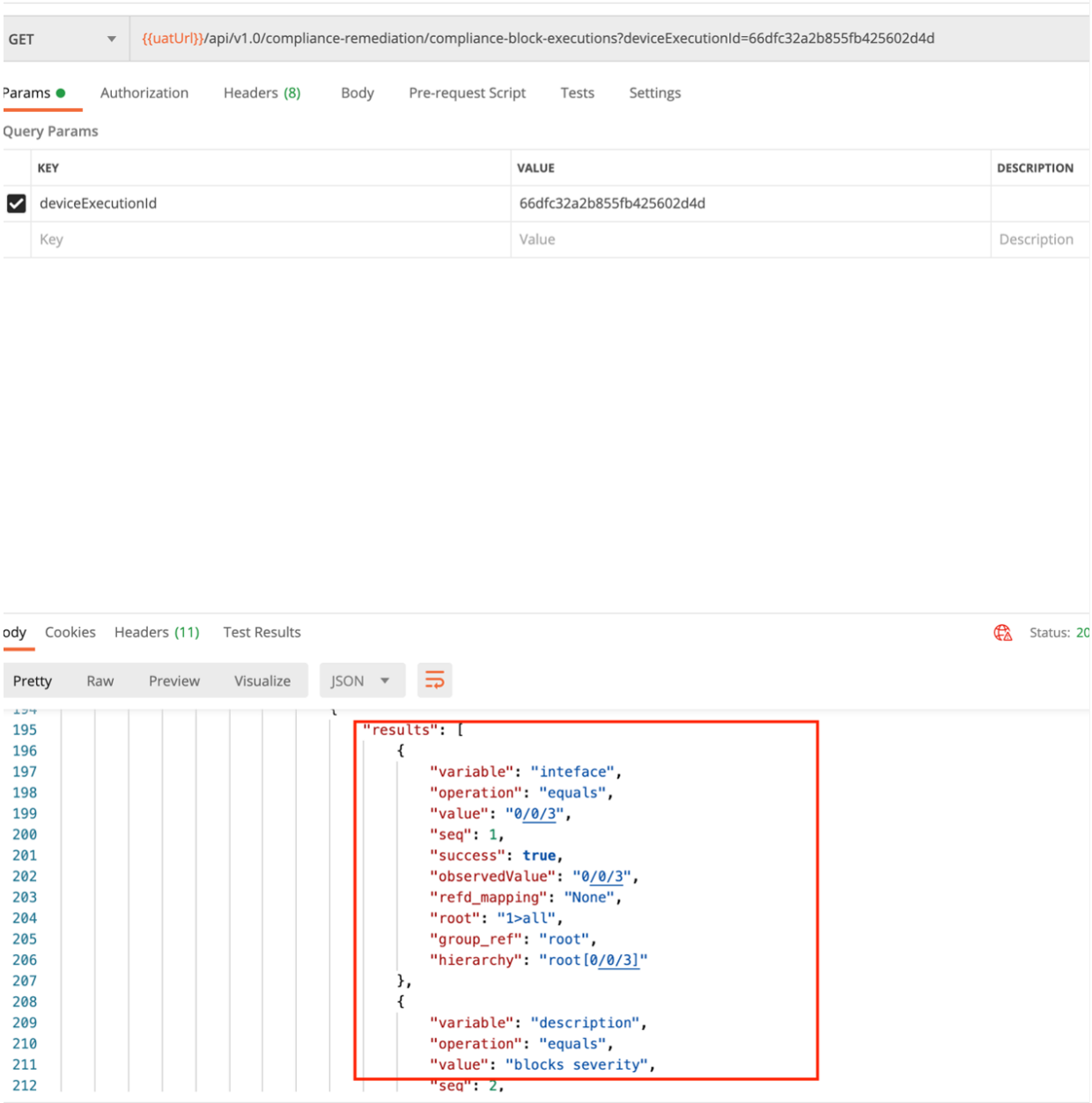
观察:在执行合规性作业期间，规则变量显示空值。

分析:

1. 如果正在从RefD应用检索数据，请确认RefD键的格式正确。如果是，请确认RefD应用程序具有链接到规则中合规性变量的密钥的数据。此外，通过检查合规性服务日志，验证是否从合规性应用发送了正确的RefD密钥。请参阅了解规则层次结构和RefD在规则和非RefD规则中的集成。
2. 使用以下API检查合规性块执行结果：

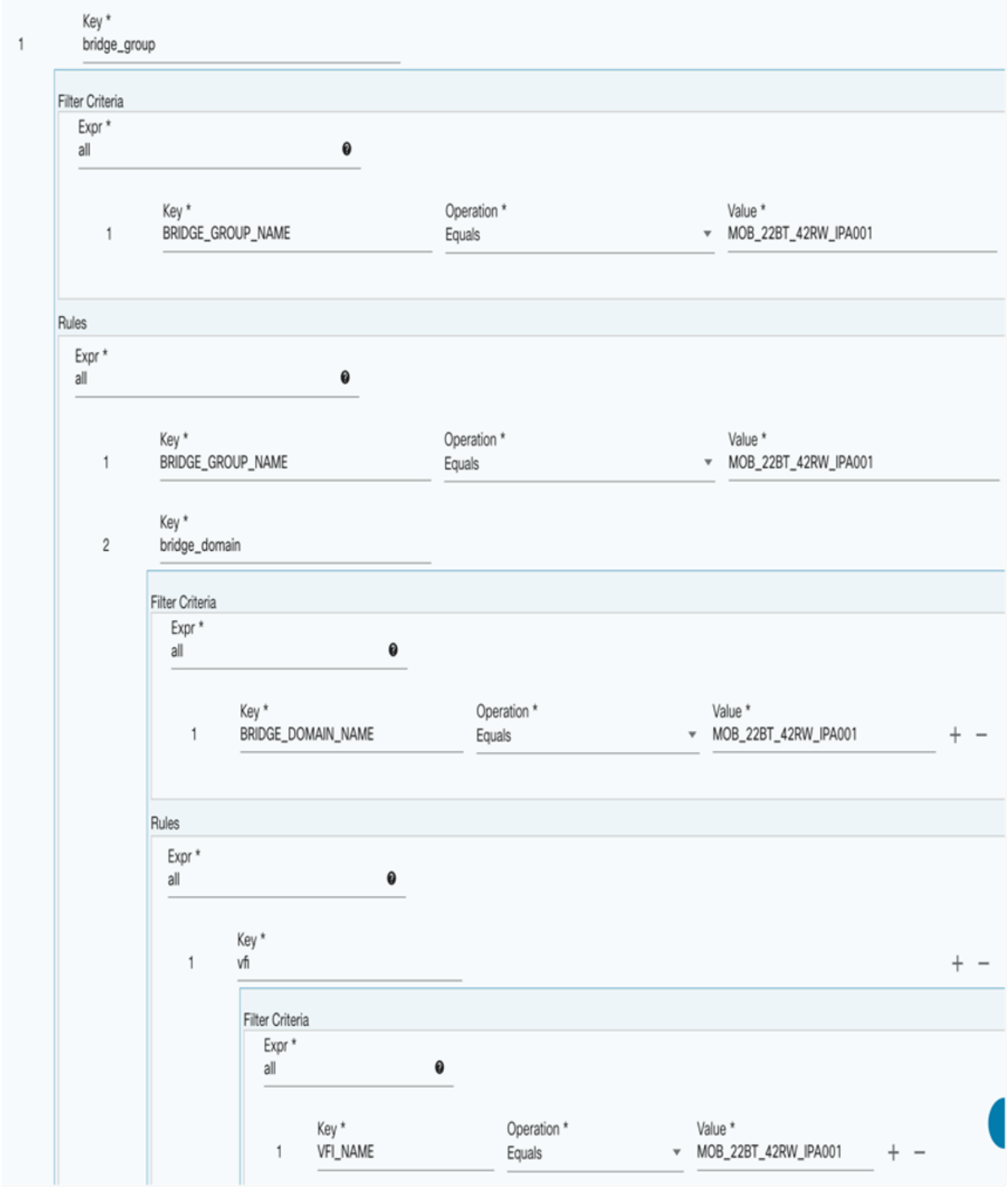
   URL:/api/v1.0/compliance-remediation/compliance-block-executions?deviceExecutionId=<>

   方法：GET



合规性块执行的结果

3. 验证块是否具有子层次结构或单个层次结构，并确保规则是根据层次结构配置的。



合规性块执行的结果

4. 通过运行以下python脚本，验证TTP解析器是否正在从设备配置中提取值：

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

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

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

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

监控合规性日志

单节点环境:

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

多节点Kubernetes环境:

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

Kibana日志监控:

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。