Guide de l'utilisateur BPA - Conformité et correction de la configuration v5.1

Introduction

L'application CnR (Configuration Compliance and Remediation) permet aux opérateurs réseau d'effectuer des contrôles de conformité de la configuration des périphériques pour les politiques personnalisées construites à partir de blocs de configuration. Les opérateurs créent manuellement ou génèrent automatiquement des blocs de configuration à l'aide du système à partir de configurations de périphériques sélectionnées. Les utilisateurs peuvent également établir des règles qui s'appliquent à ces blocs, avec des conditions de règle potentiellement dérivées de valeurs obtenues à partir de l'application RefD. Les opérateurs peuvent facilement exécuter des vérifications de conformité selon un calendrier ou lancer les vérifications instantanément.

L'application dispose d'un tableau de bord intuitif, présentant une vue d'ensemble complète des violations de conformité, offrant à la fois des résumés et des vues détaillées au niveau des périphériques et des blocs de configuration.

L'application comprend un cadre de correction robuste pour traiter les infractions à la conformité. Cette structure s'appuie sur des workflows et des modèles (modèles de configuration, appelés modèles de configuration standard ou modèles de processus) pour rationaliser le processus de correction. Comme pour les contrôles de conformité, les tâches de correction peuvent être programmées pour s'exécuter selon un calendrier ou déclenchées immédiatement pour traiter rapidement les violations.

Le tableau de bord de conformité et de correction du portail de nouvelle génération (nouvelle génération) comporte des fonctionnalités conçues pour améliorer la gestion de la sécurité du réseau, rationaliser les procédures de conformité et simplifier les activités de correction. Le tableau de bord fournit un résumé complet de la conformité des ressources et des politiques, ce qui permet aux opérateurs réseau d'évaluer facilement l'état de leur réseau et de s'assurer que les périphériques respectent des protocoles de sécurité stricts.

Les blocs de configuration peuvent être générés automatiquement, puis modifiés ou ajoutés manuellement, offrant un équilibre entre l'automatisation et la personnalisation. L'identification précise des blocs de configuration et des mécanismes de contrôle d'accès granulaires, notamment les paramètres détaillés des utilisateurs, des groupes et des autorisations sur les interfaces classiques et modernes, garantissent que les configurations réseau restent sécurisées et sont gérées par un personnel de confiance. Ces fonctionnalités constituent un puissant ensemble d'outils pour les entreprises cherchant à maintenir des normes élevées de conformité et de sécurité du réseau.

Nouveautés de Cisco

Les principales fonctionnalités et améliorations suivantes ont été introduites :

- Un tableau de bord complet pour générer, afficher et télécharger des rapports de conformité
- Possibilité d'effectuer des audits de conformité hors ligne en téléchargeant des configurations de périphériques sans intégrer le périphérique à l'aide d'Asset Manager
- Possibilité de configurer des modèles dans la configuration de bloc pour masquer les données de configuration des périphériques sensibles
- Possibilité d'exporter les données de la grille récapitulative de conformité des stratégies et des ressources sous forme de fichiers CSV
- Afficher et comparer les configurations de correction générées avec les configurations en cours des périphériques
- Améliorations apportées aux blocs pour prendre en charge les violations de déclenchement si la configuration existe
- Permettre à l'utilisateur connecté de créer et de modifier des pages de stratégie pour effectuer un lancement croisé dans des composants enfants tels que la page de création de bloc
- Amélioration des tâches de conformité pour créer et modifier des pages à lancer de manière croisée dans la page de modification de stratégie

Composants

La conformité et la correction prennent en charge les types de contrôleurs et de périphériques suivants :

Contrôleur	Types de SE
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. Conformité validée uniquement
FMC (7.2.5)	FX-OS (FTD). Conformité validée uniquement
Directement vers le périphérique (D2D)	IOS XE, IOS XR, JunOS

Remarque : La prise en charge de Nokia SR-OS via le contrôleur NSO s'applique uniquement à la fonctionnalité de conformité de la configuration. La correction n'est pas prise

en charge pour les périphériques Nokia.

Remarque : La fonctionnalité de conformité fonctionne avec la configuration des périphériques au format CLI (Command Line Interface) de Cisco et au format de type YAML pour les périphériques Juniper et Nokia. Actuellement, le framework ne prend pas en charge d'autres formats tels que Netconf, JSON, XML, etc.

Dans le cadre de la version 5.0, l'application classique Compliance and Remediation (CnR) a été désapprouvée. Toutes les fonctionnalités CnR sont désormais entièrement intégrées et disponibles sur le portail Next-Gen.

Hypothèses et prérequis

Les conditions préalables suivantes sont requises pour utiliser efficacement l'exemple d'utilisation CnR.

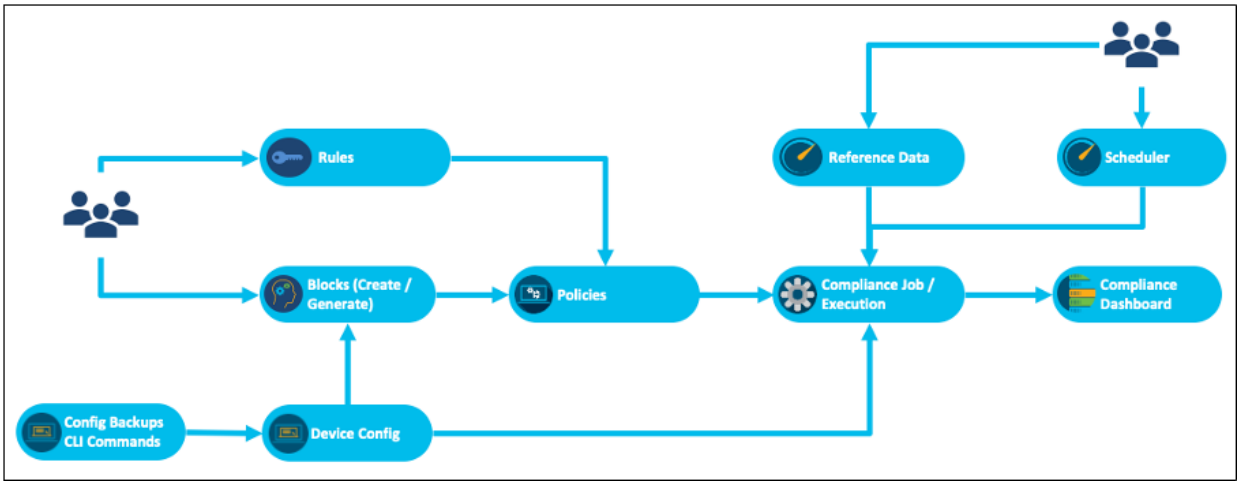
- La clé d'autorisation d'abonnement pour l'exemple d'utilisation CnR doit être téléchargée.
- Le contrôleur et les périphériques concernés doivent être intégrés et disponibles dans le cadre du gestionnaire d'actifs BPA. Reportez-vous à la section Gestionnaire d'actifs du Guide de l'utilisateur BPA pour plus de détails.
- Les ressources intégrées doivent être regroupées en fonction des besoins du client dans des groupes de ressources sur le portail Next-Gen.

Tableau de bord de conformité

Le tableau de bord de conformité fournit une vue récapitulative des violations sur tous les périphériques pour la durée sélectionnée. Les données du mois en cours s'affichent par défaut. Les utilisateurs peuvent modifier la fenêtre de temps pour afficher les données historiques sur les violations de conformité. Le mois en cours est la vue sélectionnée par défaut.

Remarque : Le tableau de bord de conformité déconseillé de l'interface utilisateur classique a été supprimé et n'est plus disponible. Le tableau de bord disponible dans le portail Nouvelle génération doit être utilisé.

Diagramme de conformité de configuration



Présentation du composant de conformité de configuration

Les violations de conformité affichées dans le tableau de bord sont renseignées lorsqu'une tâche de conformité est exécutée pour une stratégie par rapport à une liste d'actifs. La stratégie de conformité est créée en ajoutant une liste de configurations de blocs ainsi que les règles de conformité nécessaires. La règle de conformité peut avoir des vérifications avec des valeurs statiques ou des variables dynamiques pour lesquelles les données sont extraites de l'application RefD. Une tâche de conformité peut être exécutée à la demande, ponctuellement ou de façon périodique.

La conformité de la configuration inclut les fonctionnalités importantes suivantes :

- Blocage de la création : Les blocs sont créés manuellement ou générés automatiquement à l'aide du modèle TTP (Template Text Parser). Ils peuvent être statiques ou dynamiques (avec des variables).
- Création de règles : Les règles valident les variables dans les blocs. Les valeurs de règle peuvent être définies de manière statique ou extraites de manière dynamique à partir du système de données de référence (RefD) pendant le temps d'exécution.
- Création de stratégie : Les politiques sont créées en sélectionnant la liste des blocs et les règles correspondantes. Les données des règles peuvent être statiques ou extraites de manière dynamique de l'infrastructure RefD au moment de l'exécution.
- Création d'emplois de conformité : Les tâches de conformité sont créées en sélectionnant une stratégie et un groupe d'actifs (contenant une liste d'actifs) pour exécuter le contrôle de conformité. Les utilisateurs peuvent choisir de récupérer la configuration du périphérique à partir de l'infrastructure de sauvegarde ou d'exécuter des commandes en direct via des modèles de processus sur les périphériques pendant l'exécution. L'extraction de la configuration à partir de la sauvegarde permet d'effectuer un audit hors ligne des périphériques sans devoir se connecter à un périphérique actif. Les tâches peuvent être planifiées ou exécutées à la demande.
- Violations de conformité : Afficher les violations de conformité sur le tableau de bord.

Synthèse de conformité des ressources

L'onglet Asset Compliance Summary est une fonctionnalité essentielle conçue pour fournir une vue d'ensemble complète des violations de conformité sur tous les périphériques d'un réseau. Cet onglet permet aux utilisateurs d'identifier rapidement les problèmes de conformité, afin de s'assurer que tous les périphériques respectent les politiques et les normes établies. L'interface est dotée de puissantes fonctionnalités de filtrage et de recherche, qui facilitent la navigation et l'analyse des données de conformité.

Fonctionnalités principales

- Résumé des violations par périphérique : L'onglet affiche une vue récapitulative des violations de conformité pour chaque périphérique, offrant aux utilisateurs un instantané rapide de l'état de conformité global, classé par niveaux de gravité (critique, élevé, moyen et faible).
- Informations détaillées sur les violations : Pour chaque périphérique, la fenêtre contextuelle fournit des informations détaillées sur les politiques enfreintes et l'utilisateur peut approfondir la recherche dans le bloc et la ligne de configuration à l'origine de la violation.

Afficher le récapitulatif de conformité des ressources

- Options de filtrage avancées : Les filtres situés en haut et à gauche de l'onglet permettent aux utilisateurs de restreindre les données affichées dans la grille. Les utilisateurs peuvent filtrer par plage de dates, groupe d'actifs, gamme de produits, etc., ce qui permet une analyse ciblée des données de conformité.
- Fonctionnalité de recherche : Un champ de recherche est disponible pour affiner les données de la grille. Les utilisateurs peuvent rapidement localiser des périphériques spécifiques ou les gérer par contrôleur en saisissant des mots clés ou des expressions appropriés.
- Plage de dates personnalisable : Par défaut, le mois en cours est sélectionné dans le filtre de plage de dates, fournissant les données de conformité les plus récentes. Toutefois, les utilisateurs peuvent personnaliser la plage de dates pour afficher les données.
- Filtres : Plusieurs filtres sont disponibles, tels que Gamme de produits, Groupe d'équipements et Type d'audit. Appliquez le filtre pour actualiser la grille.

Synthèse de conformité des ressources

- Exporter au format CSV : Fonction permettant aux utilisateurs d'obtenir une copie locale de la conformité de la configuration des ressources à des fins d'analyse hors ligne, de création de rapports et d'archivage. Pour exporter des données en tant que fichier CSV, sélectionnez Exporter au format CSV dans l'icône Autres options. Le fichier CSV téléchargé contient les données actuellement affichées dans la grille, en respectant les filtres appliqués.

Résumé de conformité des ressources : Exporter au format CSV

Détails du fichier CSV pour la conformité des ressources

Le fichier CSV comprend toutes les colonnes visibles dans la grille Asset Compliance Summary, telles que le nom du périphérique, l'instance de contrôleur (gérée par), la famille de produits du périphérique, l'état de conformité du périphérique, le nombre de violations par gravité (par exemple, Critique, Majeur, Mineur, Avertissement, Info, Inconnu) et la date à laquelle la conformité a été vérifiée pour la dernière fois pour le périphérique.

Si la grille comporte une pagination, l'exportation inclut tous les enregistrements sur plusieurs pages, pas uniquement la page visible.

Ouverture et utilisation du fichier CSV pour la conformité des ressources

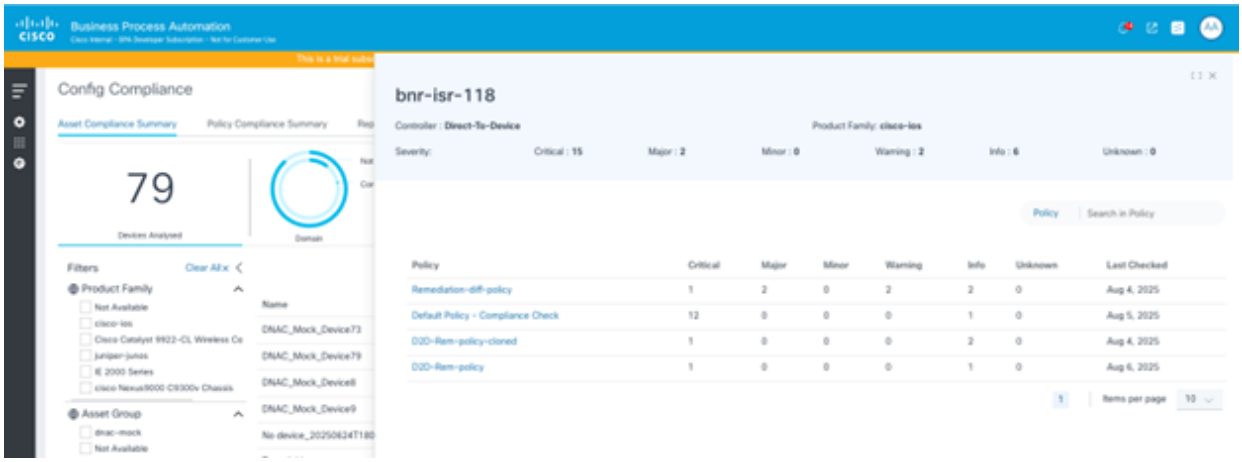
1. Ouvrez le fichier CSV téléchargé dans Excel ou toute application de feuille de calcul compatible.
2. Assurez-vous que le contenu correspond à celui affiché dans la grille Résumé de conformité des ressources, y compris les résultats filtrés.

	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											

Résumé de conformité des ressources : Fichier CSV ouvert dans l'application Excel

Afficher le récapitulatif de conformité des ressources par stratégie

En cliquant sur une ligne de la grille Récapitulatif de conformité des actifs, vous affichez les détails des violations des actifs, classées par catégories en fonction des différentes stratégies par rapport auxquelles le périphérique est validé. Les utilisateurs disposent ainsi d'une vue détaillée du nombre de violations par gravité dans chaque stratégie.



Résumé de conformité des ressources : Récapitulatif de conformité par stratégie

---

Remarque : Il convient de noter ce qui suit.
- Le lien hypertexte de la colonne Stratégie dirige les utilisateurs vers la page Détails de la

---

stratégie
- Cliquez sur une ligne pour afficher la page Détails de la violation de la stratégie sélectionnée

Afficher les détails des violations

La page Détails de la violation affiche les violations de niveau de bloc et de règle superposées sur la configuration du périphérique. En outre, les utilisateurs peuvent également afficher la configuration de bloc et les suggestions de configuration de correction.

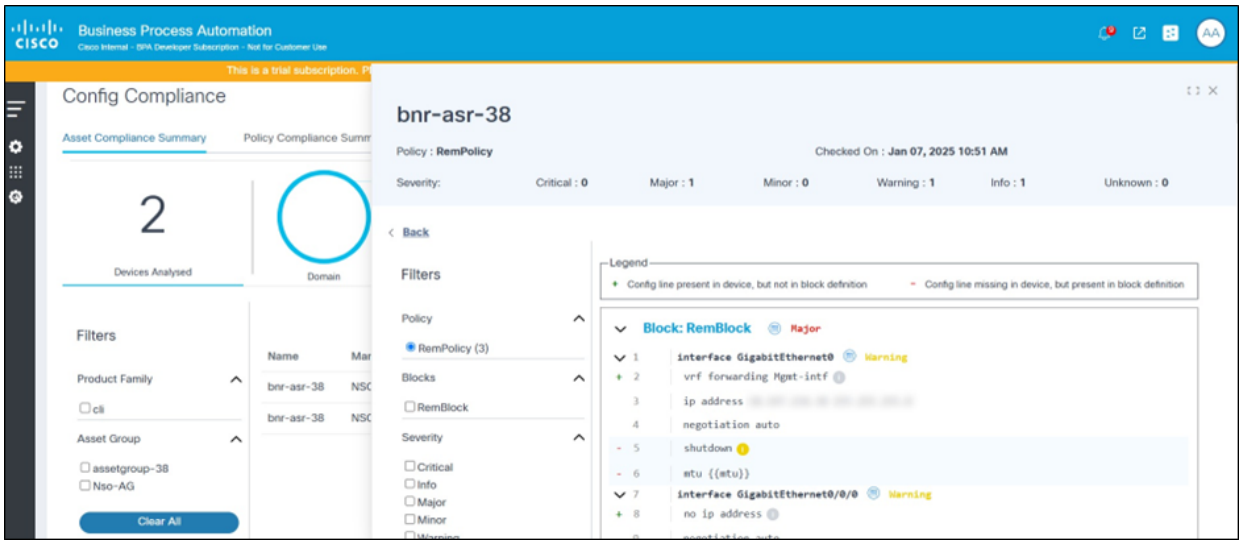
Pour visualiser la page Détails de violation à partir de la page Récapitulatif de conformité des actifs et le fractionnement au niveau de la règle :

1. Sélectionnez une ligne dans la grille Conformité des actifs. Une fenêtre contextuelle s'affiche. La grille affiche une répartition des détails de conformité par stratégie.
2. Sélectionnez une ligne dans la grille. La page Détails de la violation s'affiche.

Pour afficher la page Détails des violations à partir de la grille Synthèse de la conformité des stratégies :

1. Sélectionnez la grille de conformité aux politiques.
2. Sélectionnez une ligne **>** Grille des ressources affectées.
3. Sélectionnez une ligne. La page Détails des violations s'affiche.

La partie droite de la page Violations Details affiche les blocs de configuration de périphérique et superpose les violations sur celle-ci. Les violations sont répertoriées par rapport aux lignes de configuration correspondantes. En cas d'échec d'une condition, le ruban de violation fournit des détails sur le nom de la règle, la condition et la configuration attendue (telle que définie dans la règle) par rapport à la configuration récupérée à partir de la configuration du périphérique.



Violations de conformité des ressources

Symboles de bloc

- Le signe « + » placé contre une ligne indique que la configuration n'est pas attendue selon la configuration de bloc, mais qu'elle est également présente dans la configuration de périphérique.
- Un signe « - » en regard d'une ligne indique que la configuration est attendue selon la configuration de bloc, mais qu'elle est absente de la configuration du périphérique.

Filtres

La section Filtre située à gauche de la page permet aux utilisateurs d'effectuer les actions suivantes :

- Modifier la politique ; la page est actualisée et les violations de la stratégie nouvellement sélectionnée sont chargées
- Cochez les cases Blocks pour afficher les violations relatives aux blocs sélectionnés
- Cochez les cases Gravité pour afficher les violations avec un ou plusieurs niveaux de gravité donnés
- Cochez les cases Type de violation pour afficher les violations du type sélectionné :
  - Incompatibilité de commande : L'ordre des lignes de configuration de périphérique ne correspond pas à l'ordre défini dans la configuration de bloc
  - Config manquante : Affichez les lignes de configuration attendues selon la configuration de bloc mais manquantes dans la configuration de périphérique
  - Configuration supplémentaire : Affichez les lignes de configuration qui ne sont pas attendues selon la configuration de bloc, mais qui sont également présentes dans la configuration de périphérique
  - Échecs de règle : Défaillances d'une ou de plusieurs conditions dans les règles.
  - Blocs manquants : Le bloc de configuration de périphérique complet est manquant ou ne correspond pas à la configuration de bloc définie.

- Blocs ignorés : Ce bloc de configuration est ignoré car les conditions de filtre de bloc ne sont pas remplies.

Affichage et comparaison de la configuration de correction

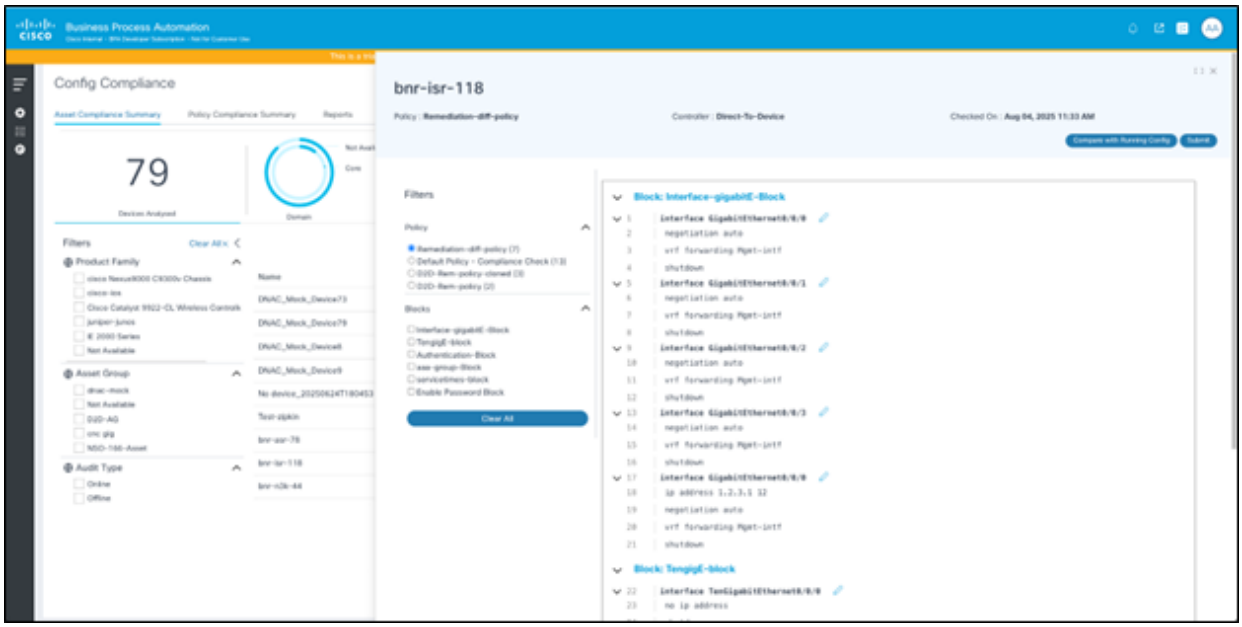
La page Remediation Config affiche la configuration générée pour le périphérique sélectionné pour chacun des blocs d'une stratégie donnée. La configuration est générée et prend en compte les détails de bloc et de règle présents dans la politique, ainsi que la configuration de périphérique récupérée lors de l'exécution de la conformité. Les utilisateurs peuvent mettre à jour la configuration dans la même page. Cette configuration générée peut être transmise au périphérique à l'aide de la fonction de tâches de conversion. En outre, cette page permet aux utilisateurs de comparer la configuration générée à la configuration en cours du périphérique. L'utilisateur peut spécifier une ou plusieurs commandes pour récupérer la configuration actuelle du périphérique.

Pour afficher la page Remediation Config depuis la grille Asset Compliance :

1. Cliquez sur l'onglet Asset Compliance Summary.
2. Dans la grille de conformité des ressources de la colonne Action , sélectionnez l'icône Autres options > Afficher la configuration de la correction. La page Remediation Config s'affiche.

Pour afficher la page Remediation Config à partir de la grille Policy Compliance :

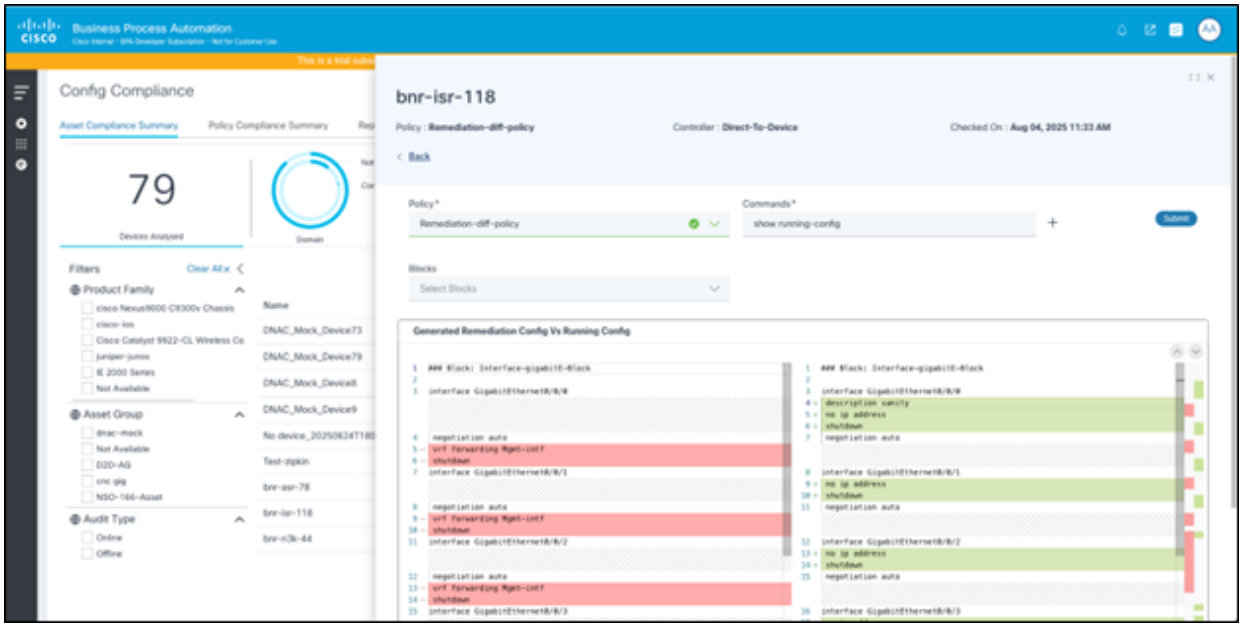
1. Cliquez sur l'onglet Résumé de la conformité des politiques.
2. Dans la grille de conformité des politiques, sélectionnez la ligne souhaitée. La grille Actifs affectés s'affiche.
3. Dans la colonne Action, sélectionnez l'icône Plus d'options > Sélectionner Afficher la configuration de la résolution. La page Remediation Config s'affiche.



Page Remediation Config

La page Remediation Config affiche les éléments suivants :

- Configuration de correction générée : La configuration générée est affichée sur le côté droit de la page, avec une option permettant aux utilisateurs de modifier les blocs de configuration et d'envoyer les modifications à enregistrer
- Filtres : Les filtres peuvent être utilisés pour sélectionner une politique, puis éventuellement sélectionner un ou plusieurs blocs pour afficher la configuration générée correspondante
- Comparer avec Configuration en cours : Cliquez sur Comparer avec configuration en cours pour afficher une page détaillée qui permet aux utilisateurs de comparer la configuration générée avec la configuration en cours du périphérique



Page Comparer avec configuration en cours

La page Comparer avec la configuration en cours affiche les éléments suivants :

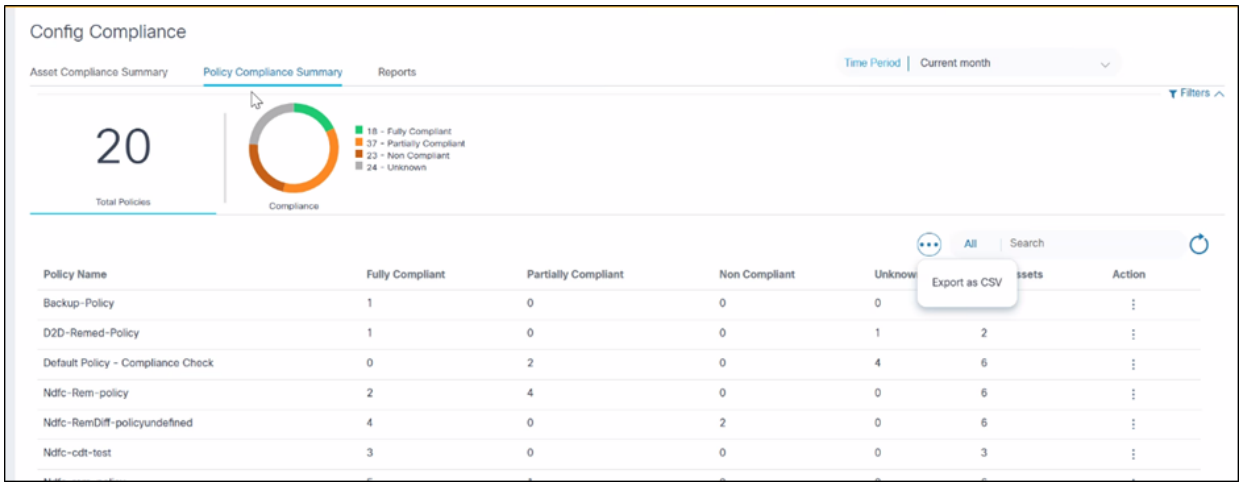
- Option de sélection d'une stratégie : La stratégie sélectionnée dans la page précédente est présélectionnée.
- Zone de texte permettant d'entrer une ou plusieurs commandes à exécuter sur le périphérique
- Un bouton Submit pour exécuter la ou les commandes sur le périphérique et récupérer la configuration
- Option d'affichage et de filtrage des blocs : Par défaut, tous les blocs de la stratégie sont affichés ; les utilisateurs peuvent sélectionner des blocs individuels selon leurs besoins
- Un visualiseur de différences de configuration affichant la configuration générée et la configuration de périphérique côte à côte, avec des surbrillances pour les différences

Résumé de conformité aux stratégies

L'onglet Policy Compliance Summary est conçu pour fournir une vue d'ensemble claire et concise de l'état de conformité des périphériques par rapport aux politiques définies. Cet onglet permet aux utilisateurs d'évaluer rapidement le paysage de la conformité et d'identifier les domaines problématiques. L'onglet classe les périphériques en fonction de leur état de conformité, ce qui facilite la compréhension et la gestion de la conformité brièvement.

États de conformité :

- Entièrement conforme : Tous les périphériques respectent toutes les règles de conformité de la stratégie correspondante.
- Partiellement conforme : Certains périphériques sont conformes aux règles, mais d'autres ne le sont pas.
- Non conforme : Aucun périphérique n'est conforme à la politique.
- Inconnu : La conformité de la stratégie ne peut pas être vérifiée en raison de problèmes de connexion réseau ou de l'indisponibilité des sauvegardes.



Récapitulatif de conformité aux politiques avec exportation CSV

Exporter au format CSV pour la conformité aux stratégies

La fonction Exporter au format CSV permet aux utilisateurs d'obtenir une copie locale de la conformité aux stratégies à des fins d'analyse, de création de rapports et d'archivage hors connexion. Pour exporter des données en tant que fichier CSV, sélectionnez Exporter au format CSV dans l'icône Autres options. Le fichier CSV téléchargé contient les données actuellement affichées dans la grille, en respectant les filtres appliqués.

Détails du fichier CSV pour la conformité aux politiques

Le fichier CSV comprend le nom de la stratégie, le nombre total d'actifs validés et la ventilation du nombre par état de conformité (c.-à-d. Entièrement conforme, Partiellement conforme, Non conforme et Inconnu). Si la grille comporte une pagination, l'exportation inclut tous les enregistrements de toutes les pages, et pas uniquement ceux affichés sur la page active.

Ouverture et utilisation du fichier CSV pour la conformité aux politiques

1. Ouvrez le fichier CSV téléchargé dans Excel ou toute application de feuille de calcul compatible.
2. Assurez-vous que le contenu correspond à ce qui est affiché dans la grille Résumé de conformité aux politiques, y compris les résultats filtrés.

	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						

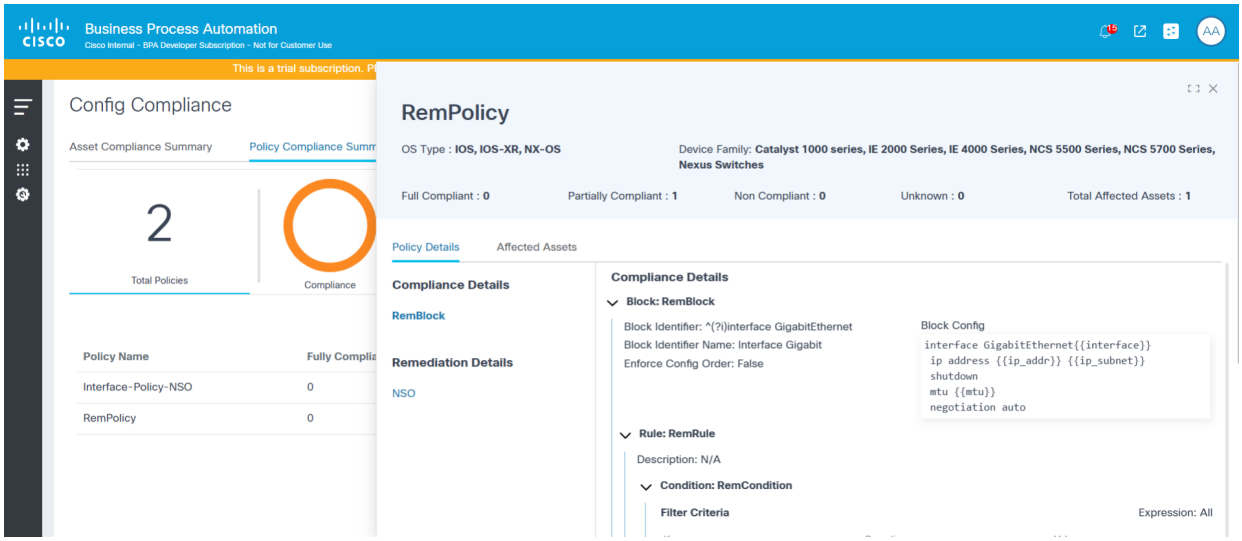
Conformité aux politiques : Détails de stratégie

Afficher les détails de stratégie

Pour afficher les détails d'une stratégie :

1. Sélectionnez une stratégie à partir de l'icône Autres options sous la colonne Action.
2. Sélectionnez Afficher les détails de stratégie. La page Détails de la stratégie s'affiche.

Remarque : La page Détails de la stratégie est une vue en lecture seule de toutes les informations de stratégie, y compris les blocs, les règles et les conditions.Les utilisateurs peuvent cliquer sur des liens hypertexte dans la page qui permet d'accéder directement au bloc concerné.



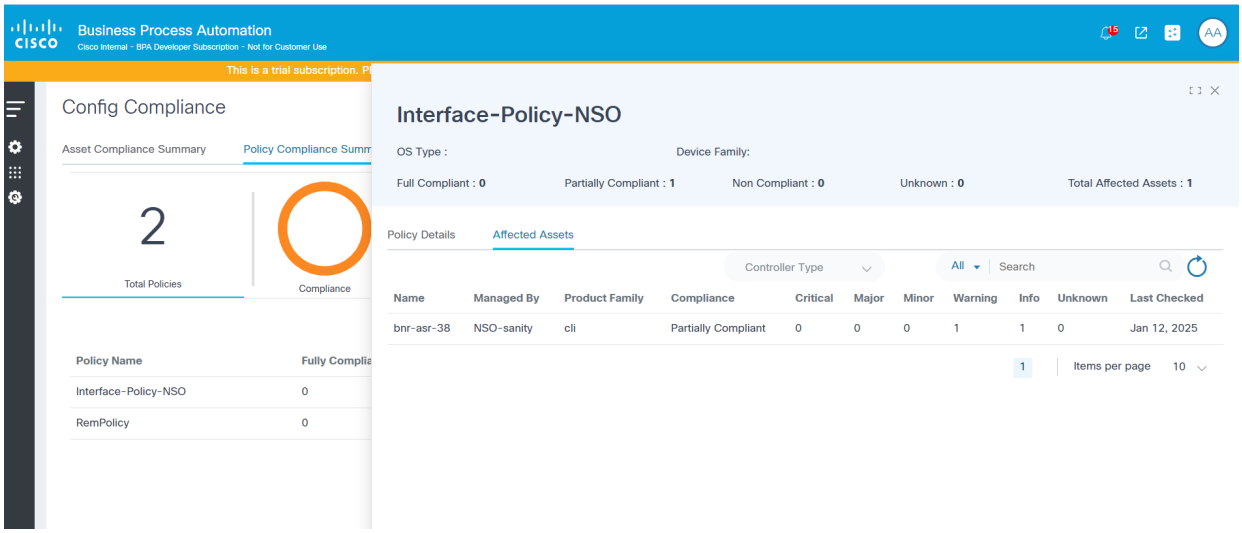
Conformité aux politiques : Détails de stratégie

Afficher les ressources affectées

L'onglet Actifs affectés affiche la liste des actifs analysés sous chaque politique et le nombre de violations divisé par gravité. Les périphériques peuvent être filtrés à l'aide de la liste déroulante Type de contrôleur et de la zone de recherche.

Pour afficher les ressources affectées à partir de l'onglet Synthèse de conformité aux stratégies :

1. Sélectionnez une ligne. La fenêtre Politique de conformité s'affiche.
2. Cliquez sur l'onglet Actifs affectés.



Conformité aux politiques : Ressources affectées

Remarque : L'onglet Actifs affectés propose des actions permettant d'ouvrir les pages Afficher les détails des violations et Afficher la configuration des mesures correctives. Référez-vous à Résumé de conformité des actifs pour plus d'informations.

Rapports

La section Rapports est conçue pour fournir des informations complètes sur la conformité des périphériques, identifier les violations et faciliter les efforts de correction. L'application offre une interface conviviale pour générer, afficher, télécharger et gérer divers types de rapports de conformité.

Tableau de bord

Le tableau de bord de génération de rapports sert de concentrateur central pour toutes les activités de génération de rapports de conformité. Les utilisateurs peuvent gérer efficacement leurs rapports depuis cette interface unique. Les principales fonctionnalités disponibles sur le tableau de bord Rapports sont les suivantes :

- Affichage des rapports : Les utilisateurs peuvent afficher une liste de tous les rapports générés, y compris leur nom, leur type, la stratégie associée, le format, la date de création et l'état actuel (par exemple, Initié, Terminé, Échec, Partiellement terminé)
- Téléchargement des rapports : Les rapports, une fois générés, peuvent être téléchargés à des fins d'analyse hors ligne ou d'archivage ; La colonne Action fournit des options de téléchargement
- Suppression de rapports : Les utilisateurs ont la possibilité de supprimer les rapports anciens ou inutiles du tableau de bord, ce qui contribue à maintenir un environnement de rapports propre et organisé

- Filtrage et recherche : Le tableau de bord fournit des options de filtrage étendues, permettant aux utilisateurs de localiser rapidement des rapports spécifiques en fonction de critères tels que le type de rapport (par exemple, Détails de conformité, Résumé de la conformité, Lot de mesures correctives), la politique et l'état d'initialisation (par exemple, Dernière heure, Dernières 24 heures, Dernière semaine, Plage personnalisée) ; une barre de recherche est également disponible
- Surveillance du statut des rapports : Un résumé visuel (c.-à-d. un graphique à secteurs) indique l'état des rapports, indiquant combien sont lancés, terminés, en échec ou partiellement terminés.

Le tableau de bord Création de rapports est la page de renvoi située sous l'onglet Rapports du tableau de bord Conformité et mesures correctives.

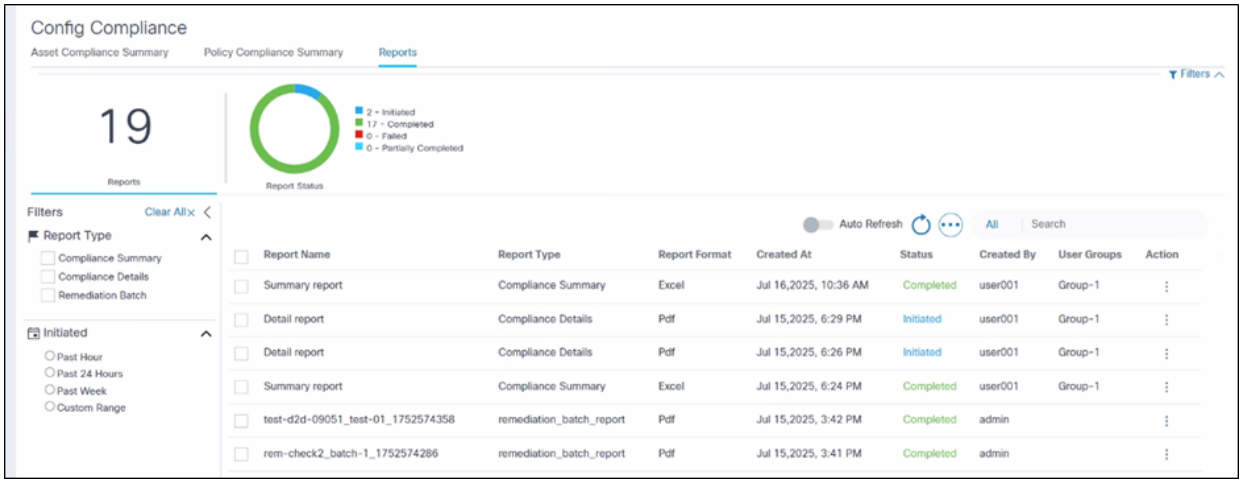


Tableau de bord Rapports

- Les types de rapports disponibles sont les suivants :
  - Rapport récapitulatif de conformité
  - Rapport détaillé de conformité
  - Rapport de lot de mesures correctives
- Utilisez des filtres pour sélectionner les éléments suivants :
  - Type de rapport
  - Policy (politique)
  - Période initiée (la liste de rapports est filtrée en fonction de la période sélectionnée)
- Option d'actualisation automatique de la liste de rapports

Configurations des rapports

Reporting Configurations permet à un administrateur de configurer des paramètres clés liés aux rapports, en fonction du déploiement et des besoins de l'entreprise. Les paramètres suivants sont disponibles pour la configuration :

- Supprimer automatiquement les rapports de plus de (jours) : Tout rapport antérieur à cette durée est supprimé du système
- Nombre maximal de blocs à sélectionner par stratégie dans un rapport récapitulatif de conformité : Aide à maintenir le nombre d'onglets dans le fichier Excel à une limite lisible
- Nombre maximal d'actifs à sélectionner dans un rapport détaillé de conformité : Aide à limiter le nombre de fichiers PDF générés pour un rapport détaillé donné

Liste des tâches de conformité

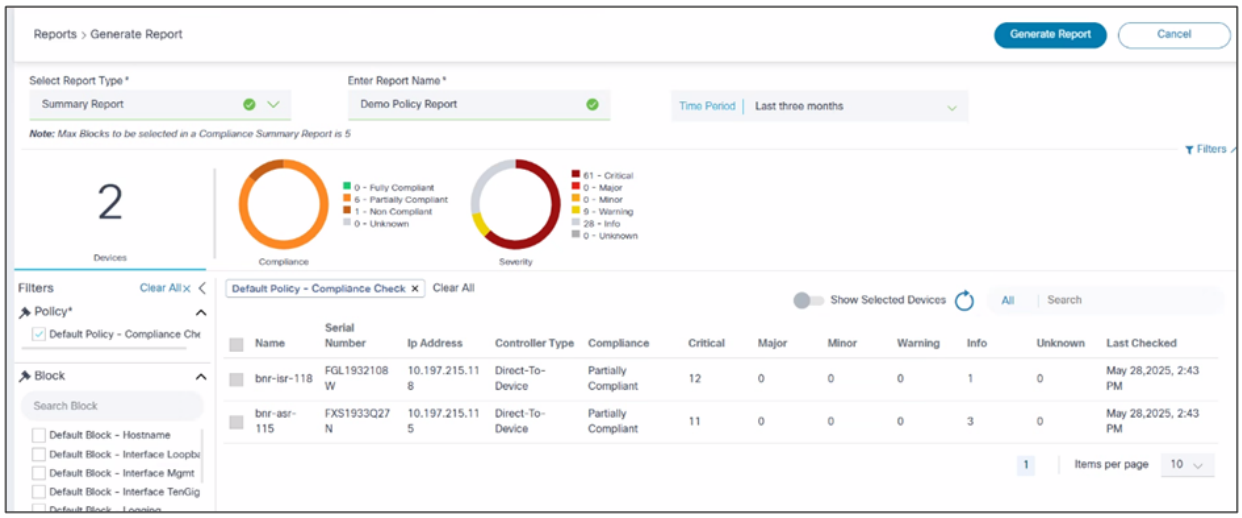
Génération de rapports

L'application fournit une interface dédiée pour générer de nouveaux rapports de conformité, permettant aux utilisateurs de sélectionner le type de rapport, de définir l'étendue et d'appliquer des filtres spécifiques. Le processus de génération de rapport est lancé à partir de l'action « Générer un rapport » sous la page Tableau de bord Création de rapports.

Les principaux aspects de la génération de rapports sont les suivants :

- Sélection du type de rapport : Les utilisateurs peuvent choisir entre les différents types de rapports suivants
    - Rapport récapitulatif : Fournit une vue d'ensemble de la conformité de tous les périphériques pour les stratégies sélectionnées
    - Rapport détaillé : Offre une vue détaillée plus précise, fournissant des informations détaillées sur les violations spécifiques de chaque périphérique
- Attribution d'un nom au rapport : Les utilisateurs doivent fournir un nom approprié pour le rapport généré
- Sélection de la période : Des rapports peuvent être générés pour des périodes spécifiques, telles que le « mois en cours » ou des plages personnalisées, afin de se concentrer sur les données de conformité récentes
- Appliquer des filtres: Des options de filtrage complètes permettent aux utilisateurs de réduire la portée du rapport
    - Policy (politique) : Sélectionnez une ou plusieurs stratégies de conformité à inclure dans le rapport. La sélection de la stratégie est obligatoire
    - Block: Dans les politiques sélectionnées, choisissez les blocs de configuration spécifiques à inclure dans le rapport. La sélection de bloc est facultative
    - Groupe d'actifs : Les utilisateurs peuvent filtrer les actifs dans l'étendue en sélectionnant un ou plusieurs groupes d'actifs
- Sélection des ressources : Ceci s'applique uniquement aux rapports détaillés
    - Les utilisateurs peuvent sélectionner des périphériques spécifiques pour lesquels le rapport doit être généré
    - La table des actifs affiche des détails tels que le nom, le numéro de série, l'adresse IP, la gestion par et l'état de conformité actuel, avec des nombres correspondant aux différents niveaux de gravité

Pour générer un rapport récapitulatif de conformité :

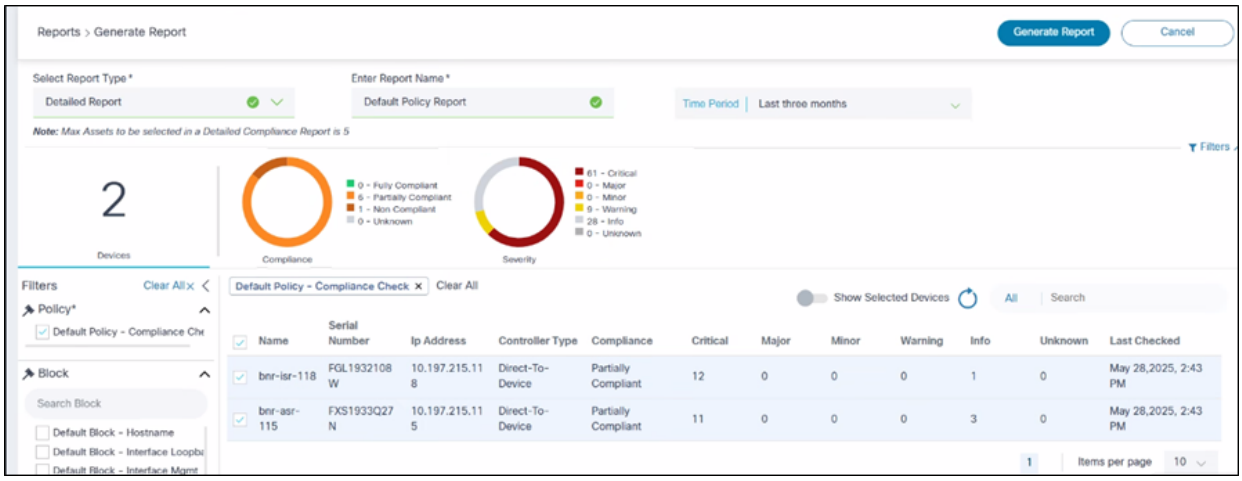


Générer un rapport récapitulatif

1. Sélectionnez Rapport de synthèse dans la liste déroulante Sélectionner le type de rapport.
2. Entrez un nom de rapport.
3. Sélectionnez une plage de temps. Les politiques et les blocs seront répertoriés en fonction de cette sélection.
4. Sélectionnez une stratégie. Vous pouvez également sélectionner d'autres stratégies.
5. Le cas échéant, sélectionnez Blocs. Si aucun n'est sélectionné, tous les blocs sont inclus.
6. Sélectionnez les groupes d'actifs, l'état de conformité et les niveaux de gravité requis.
7. Cliquez sur Générer un rapport.

- Dans la page de liste de rapports, l'état du rapport est défini sur Initié
- Une fois terminé, l'état passe à Terminé. Si certains des sous-rapports échouent, l'état passe à Partiellement terminé
- Si la génération du rapport entier échoue, une notification s'affiche et l'état passe à Échec
- Une fois terminé, l'option de téléchargement est disponible. Les utilisateurs peuvent télécharger un fichier zip contenant les rapports Excel

Pour générer un rapport détaillé de conformité :



Générer un rapport détaillé

1. Sélectionnez Rapport détaillé dans la liste déroulante Sélectionner le type de rapport.
2. Entrez un nom de rapport.
3. Sélectionnez une plage de temps. Les politiques et les blocs seront répertoriés en fonction de cette sélection.
4. Sélectionnez une stratégie. Vous pouvez également sélectionner d'autres stratégies.
5. Le cas échéant, sélectionnez Blocs. Si aucun n'est sélectionné, tous les blocs sont inclus.
6. Sélectionnez les groupes d'actifs, l'état de conformité et les niveaux de gravité requis.
7. Sélectionnez les ressources requises dans la grille. Les utilisateurs ont la possibilité de sélectionner tous les périphériques et d'afficher les périphériques sélectionnés.
8. Cliquez sur Générer un rapport.

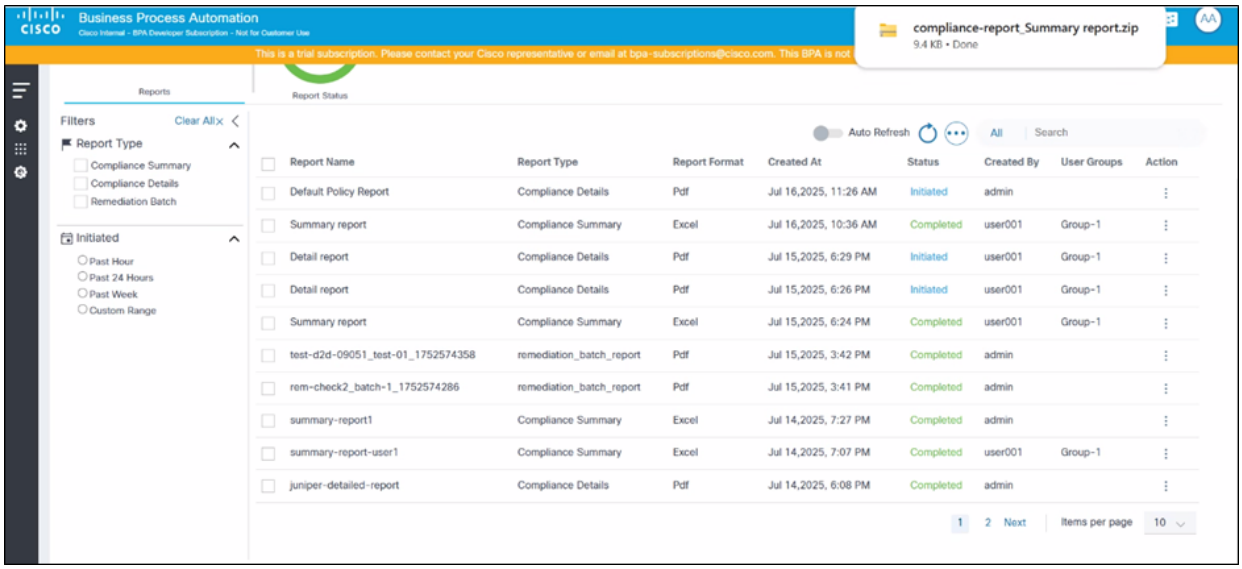
- Dans la page de liste de rapports, l'état du rapport est défini sur Initié
- Une fois terminé, l'état passe à Terminé. Si certains des sous-rapports échouent, l'état passe à Partiellement terminé
- Si la génération du rapport entier échoue, une notification s'affiche et l'état passe à Échec

Téléchargement et affichage des rapports

Les rapports terminés peuvent être téléchargés à l'aide de l'icône Télécharger située dans la ligne souhaitée de la grille Tableau de bord des rapports.

Présentation du rapport récapitulatif de conformité de la configuration

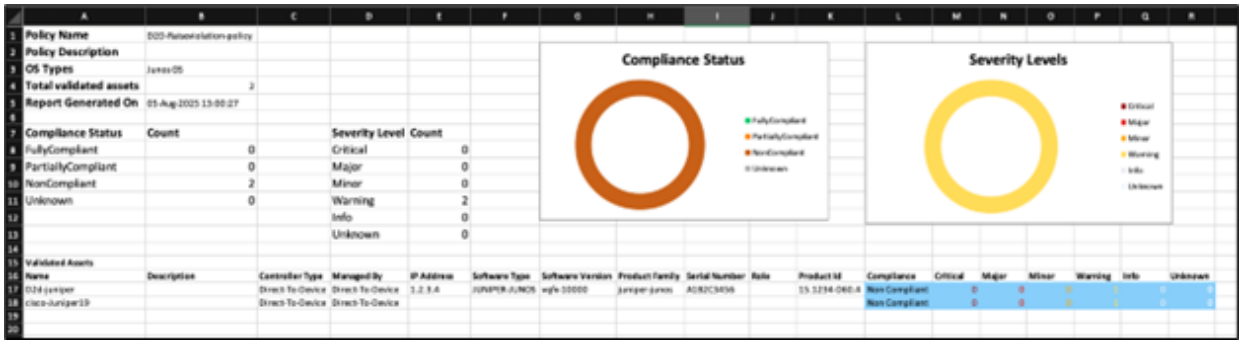
Le résumé de conformité est un fichier zip qui contient des rapports PDF individuels, avec un PDF généré par périphérique. Ce type de rapport offre une vue d'ensemble des violations de conformité par politique, ainsi que des détails sur les violations de mappage détaillé au niveau des blocs par rapport aux périphériques.



Rapport récapitulatif de conformité

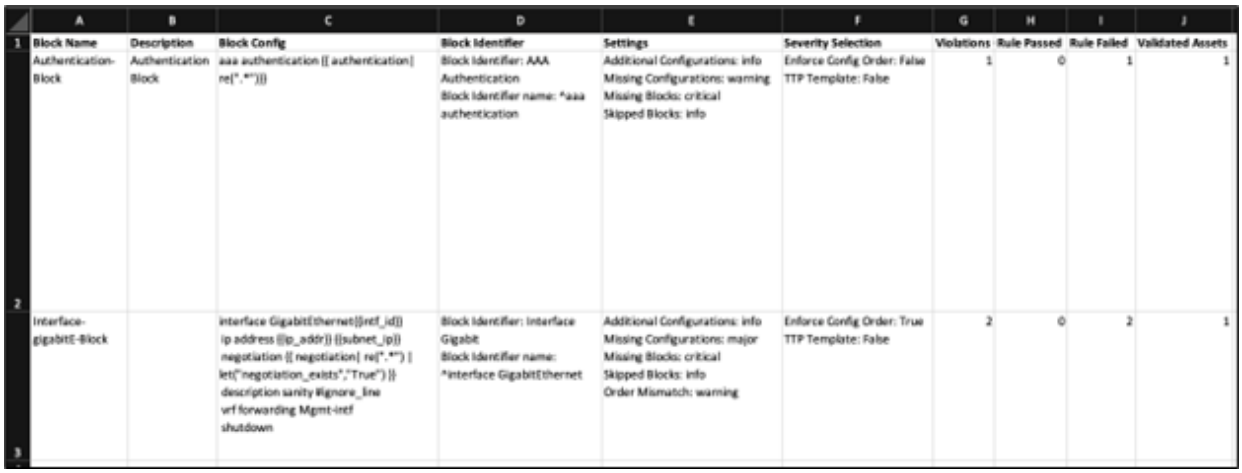
Chaque rapport Excel comprend les feuilles suivantes et fournit les informations suivantes :

- Récapitulatif des stratégies :
  - Détails de la présentation, tels que le nom de la stratégie, sa description, le ou les types de système d'exploitation et le total des ressources validées
  - Une vue de grille et de graphique du nombre d'actifs validés par état de conformité (par exemple, Entièrement conforme, Partiellement conforme, Non conforme et Inconnu)
  - Vue sous forme de grille et de graphique du nombre total de violations divisé par niveau de gravité (par exemple, Critique, Majeur, Mineur, Avertissement et Inconnu)
  - Une grille des ressources avec des détails sur les périphériques, l'état de conformité et le nombre de violations pour chaque niveau de gravité



Résumé de la politique

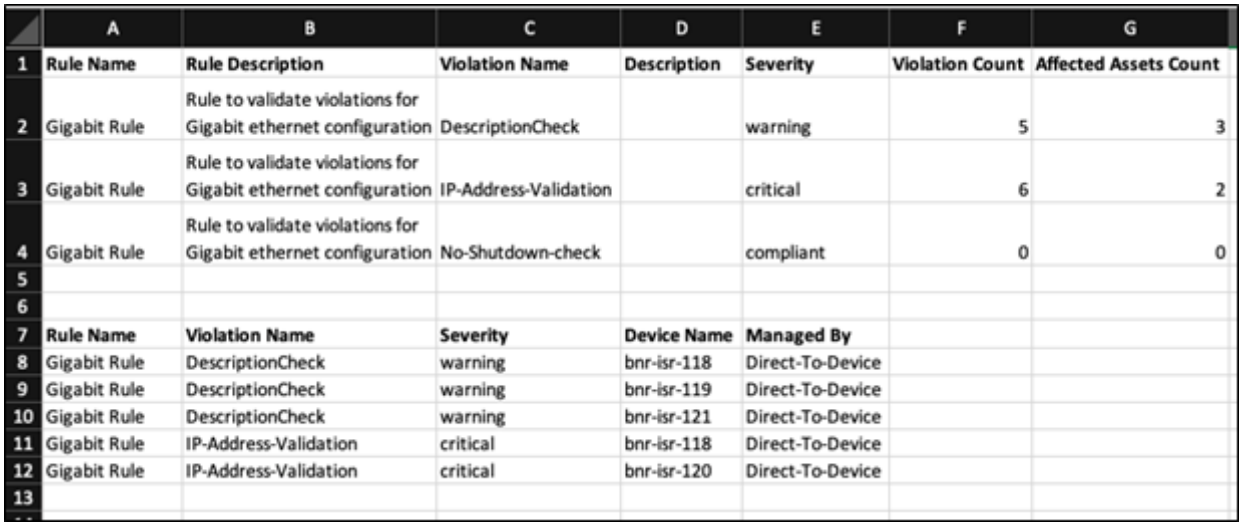
- Résumé du bloc :
  - Détails du bloc, tels que le nom du bloc, sa description, la configuration du bloc, les détails de l'identificateur de bloc et les paramètres de gravité des violations de bloc
  - Nombre de violations, de règles passées, de règles ayant échoué et de ressources validées pour le bloc donné



	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

Feuille Récapitulatif des blocs

- Détails des règles et des violations par bloc :
- La grille de niveau de violation affiche une liste de noms de règles, une description, un nom de violation, un niveau de gravité de description, le nombre de violations observées sur les ressources et le nombre de ressources affectées
- La grille au niveau du périphérique affiche le mappage entre la règle, la violation, la gravité, le nom du périphérique et le nom du contrôleur (géré par)



	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							

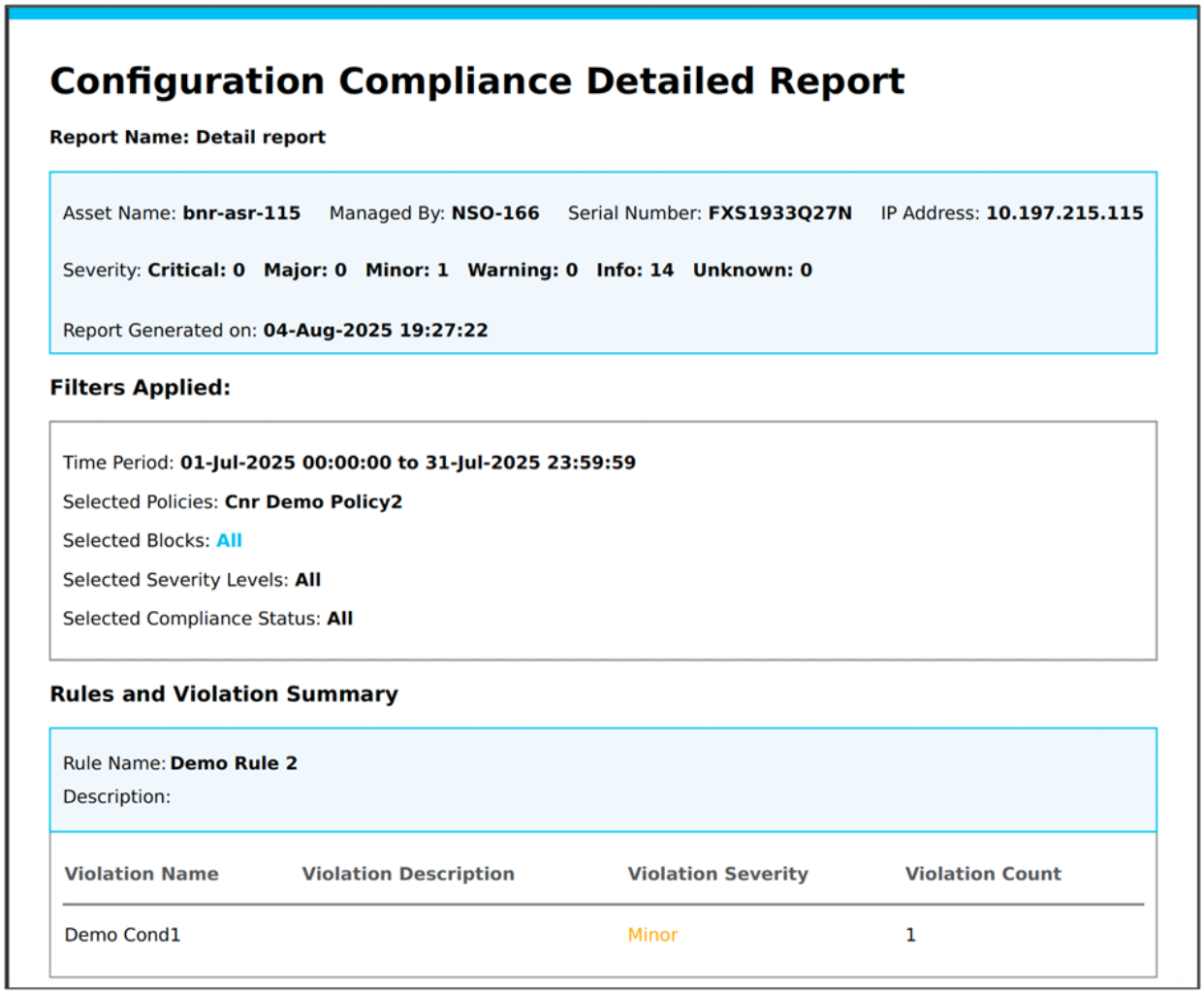
Rapport détaillé de conformité

L'état Détails de conformité contient les informations suivantes :

- Nom du rapport : Identifie le nom du rapport
  - Nom du bien : Spécifie le périphérique pour lequel la vérification de conformité a été effectuée
  - Autres détails sur les actifs : Inclut des détails tels que l'adresse IP et le numéro de série, le cas échéant
  - Gravité : Fournit un récapitulatif du nombre de violations par niveau de gravité
  - Rapport généré le : Indique l'horodatage de la création du rapport
- Filtres appliqués : Décrit en détail les critères de filtre spécifiques utilisés pour générer un

rapport spécifique, garantissant la transparence et la reproductibilité. Cela inclut la période, les politiques sélectionnées, les blocs, les niveaux de gravité et les états de conformité

- Résumé des règles et violations : Répertorie chaque règle qui a été évaluée et fournit un résumé des violations détectées pour cette règle. La grille récapitulative affiche le nom, la description, la gravité de la violation et le nombre de fois où cette violation s'est produite
- Détails de la violation : Fournit des détails explicites sur chaque ligne de configuration de périphérique pour les blocs sélectionnés, ainsi que les détails de violation pour chaque ligne



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:

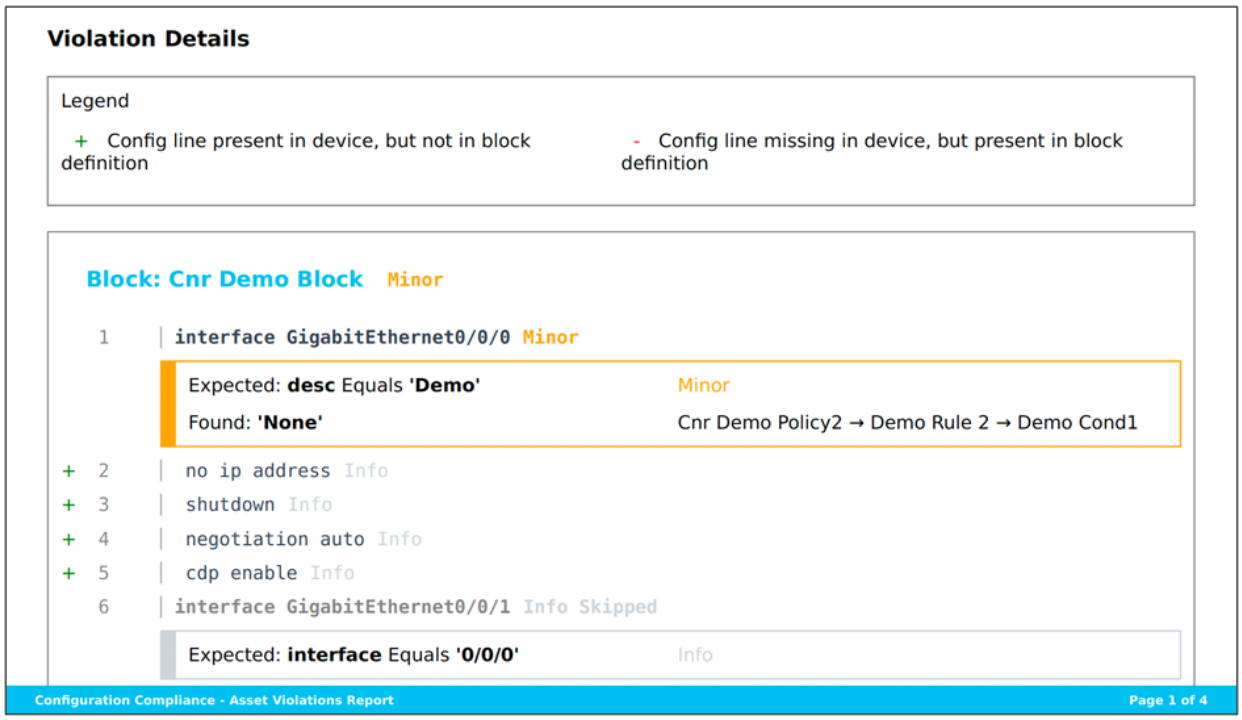
Time Period: **01-Jul-2025 00:00:00 to 31-Jul-2025 23:59:59**
Selected Policies: **Cnr Demo Policy2**
Selected Blocks: **All**
Selected Severity Levels: **All**
Selected Compliance Status: **All**

Rules and Violation Summary

Rule Name: **Demo Rule 2**
Description:

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

Rapport détaillé sur la conformité - Exemple PDF Page 1

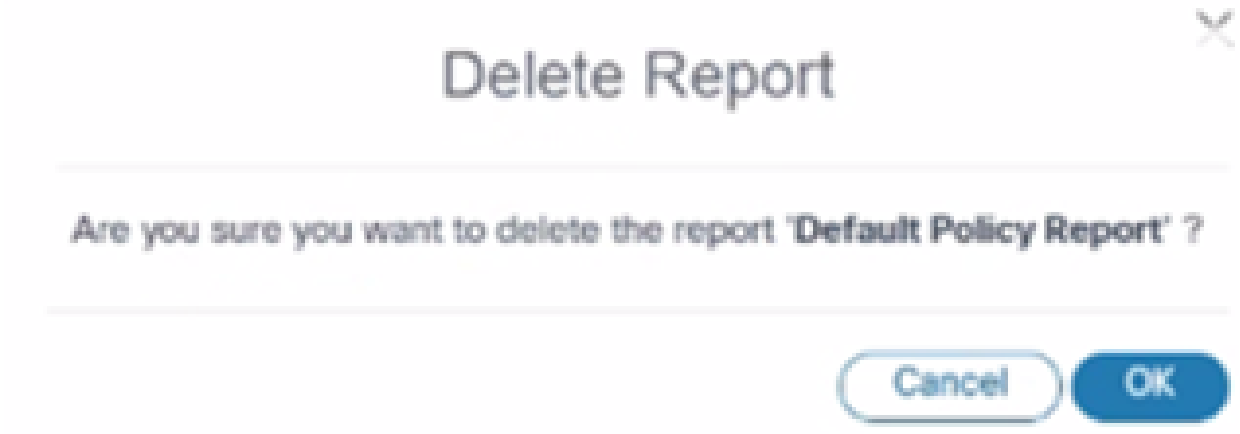


Rapport détaillé sur la conformité - Exemple PDF Page 2

Remarque : Le rapport PDF de lot de mesures correctives créé à partir de la page de lot de mesures correctives peut également être téléchargé et affiché à partir de la liste des rapports.

Supprimer les rapports

Les rapports peuvent être supprimés individuellement en sélectionnant l'icône Supprimer ou en bloc en cochant les cases des rapports et en sélectionnant l'icône Plus d'options > Supprimer.



Liste des tâches de conformité

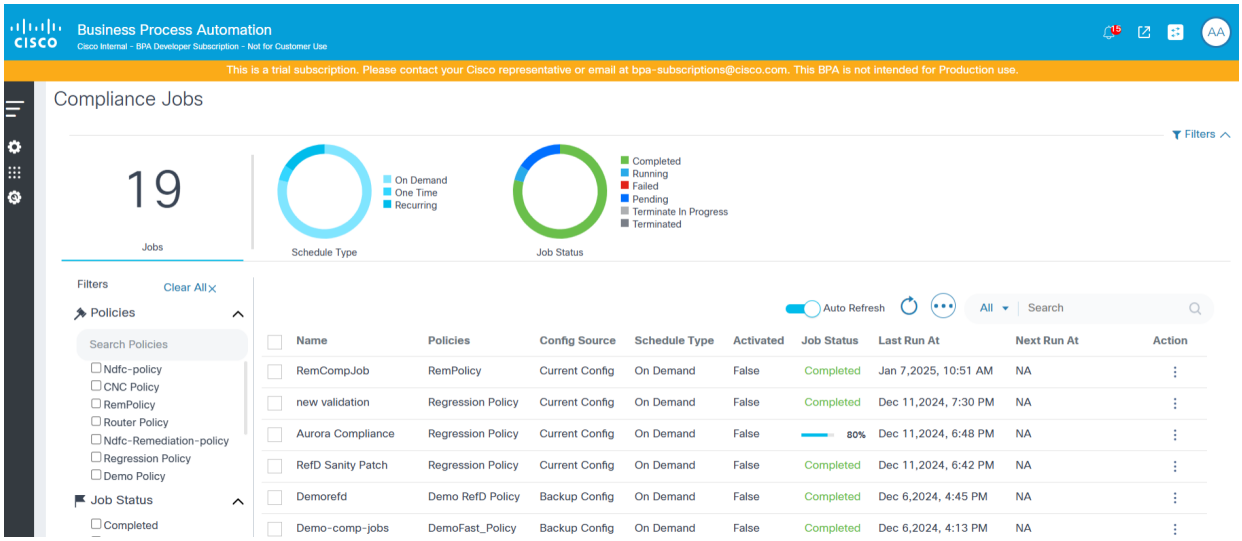
Remarque : La suppression d'un rapport supprime uniquement les fichiers et l'entrée de rapport du tableau de bord de rapport ; les détails d'exécution de conformité sous-jacents sont conservés.

Tâches de conformité

La fonction Tâches de conformité du portail Nouvelle génération est conçue pour aider les utilisateurs à créer, gérer et exécuter des tâches de conformité sur des stratégies et des groupes d'actifs sélectionnés. Ces tâches peuvent être planifiées pour s'exécuter à intervalles réguliers ou exécutées à la demande, ce qui garantit que la conformité de toutes les ressources est vérifiée de manière cohérente.

Fonctionnalités principales

- Lister les tâches de conformité : Afficher toutes les tâches de conformité définies, avec des options d'audit hors connexion, de filtrage, de création, de modification, de suppression et d'exécution des tâches.
- Tâches planifiées et à la demande : Configurez les tâches pour qu'elles s'exécutent à intervalles planifiés ou immédiatement, si nécessaire.
- Contrôle d'accès à granularité fine : L'accès aux tâches de conformité est contrôlé en fonction des autorisations utilisateur, ce qui garantit que les utilisateurs ne voient que les tâches liées aux stratégies auxquelles ils ont accès.
- Options de filtrage : Filtrez les travaux par politiques, statut de travail, type de planification et plage de dates pour faciliter la navigation et la gestion.



Liste des tâches de conformité

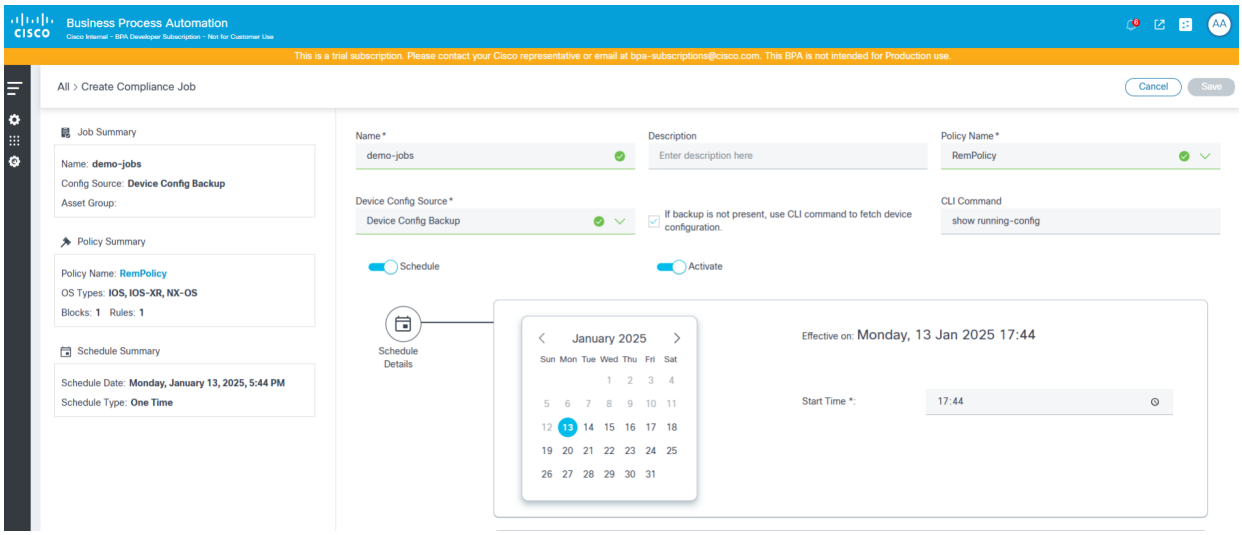
Créer des tâches de conformité

La page Création d'un travail de conformité comporte les attributs suivants :

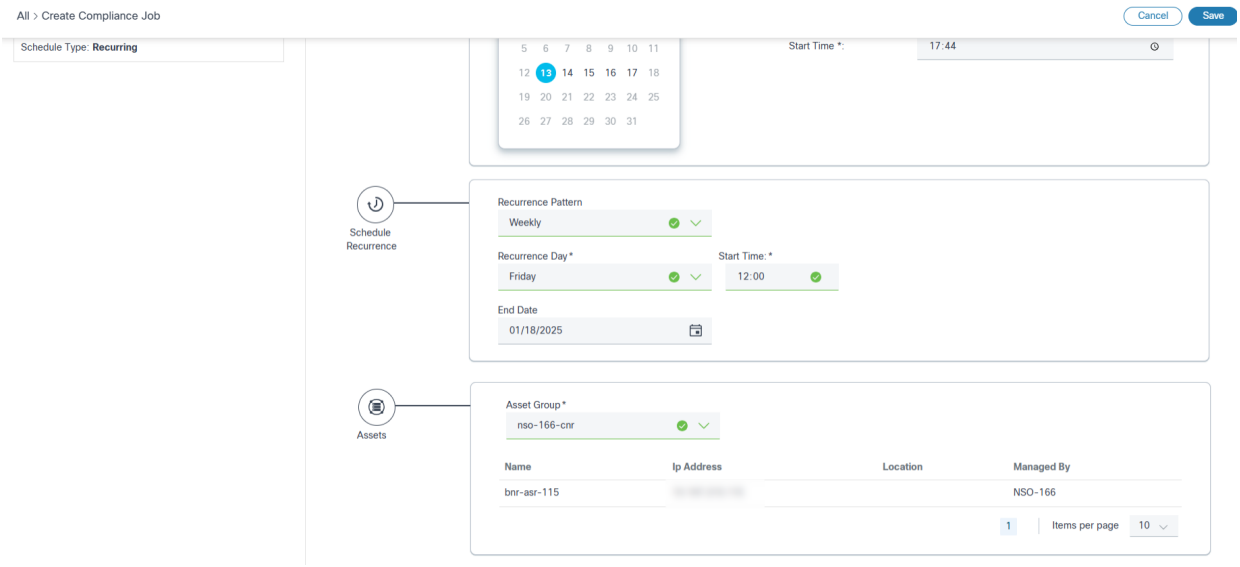
- Name : Nom de la tâche
- Description: Une description facultative
- Nom de la stratégie : Une liste déroulante pour sélectionner une stratégie à exécuter, potentiellement filtrée par les stratégies d'accès configurées pour l'utilisateur connecté
- Source de configuration du périphérique : Une liste déroulante pour sélectionner la source pour récupérer la configuration du périphérique (configuration actuelle ou sauvegarde de configuration du périphérique) pour exécuter le travail de conformité et une case à cocher pour indiquer s'il faut revenir à une commande CLI si la sauvegarde n'est pas présente.

Remarque : L'option Device Config Backup ne fonctionne que si le contrôleur sous-jacent prend en charge la fonctionnalité de sauvegarde.

- Variables définies par l'utilisateur : Zone de texte modifiable pour l'espace de noms disponible lorsque la stratégie sélectionnée comporte des variables définies par l'utilisateur
- Détails de la planification : Section permettant de sélectionner divers paramètres de planification tels que la date/heure de début et de fin, la périodicité, etc.
- Ressources : Section permettant de sélectionner un groupe d'actifs afin d'identifier la liste des périphériques pour exécuter la conformité
- Planification : Activez ou désactivez l'exécution de la tâche dans les délais prévus (ponctuelle ou récurrente). Si elle est désactivée, la tâche est exécutée immédiatement
- Est actif : Indique si la planification sélectionnée est active ou non



Créer des tâches de conformité



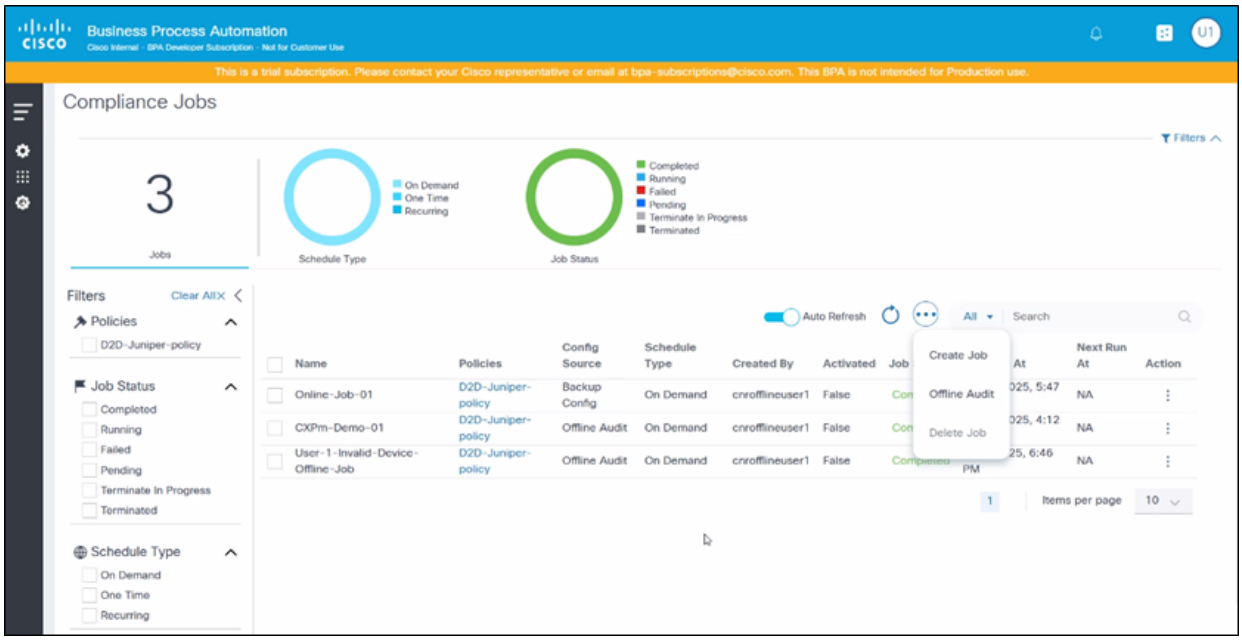
Création de travaux de conformité 2

Créer des travaux d'audit hors connexion

La fonctionnalité d'audit hors ligne des travaux de conformité permet aux utilisateurs d'effectuer des contrôles de conformité sur les configurations de périphériques sans exiger l'intégration des périphériques dans le BPA. Les utilisateurs peuvent télécharger manuellement la configuration du périphérique sous forme de fichier. Plusieurs configurations de périphériques peuvent être compressées et téléchargées ensemble sous la forme d'un fichier zip. Une fois téléchargés, ces fichiers de configuration sont analysés et des tâches de conformité peuvent être créées en utilisant le contenu de ces fichiers comme source. Les résultats des audits hors ligne sont ensuite affichés sur le tableau de bord de conformité à côté des résultats d'audit en ligne.

La page Audit hors connexion comporte les attributs suivants :

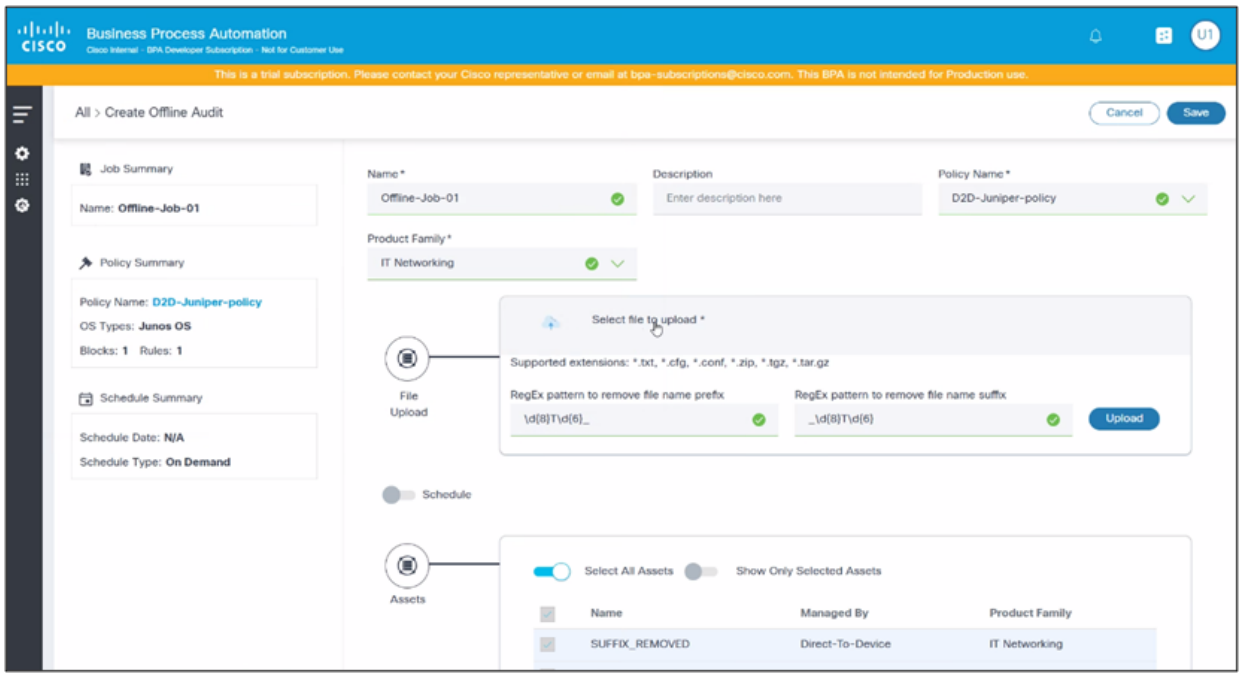
- Name : Nom de la tâche
- Description: Une description facultative
- Nom de la stratégie : Une liste déroulante pour sélectionner une stratégie à exécuter, potentiellement filtrée par les stratégies d'accès configurées pour l'utilisateur connecté
- Gamme de produits : Une liste déroulante pour sélectionner la gamme de produits
- Téléchargement de fichier : Utiliser la fonction d'audit hors ligne pour télécharger manuellement les fichiers de configuration ; Cette opération est effectuée via une interface de téléchargement dans laquelle vous sélectionnez les fichiers à partir du système local
- Planification : Activer/désactiver la planification
- Ressources : Affiche la liste des périphériques en fonction du contenu du fichier téléchargé



Sélectionner un audit hors connexion

Pour créer des tâches d'audit hors connexion :

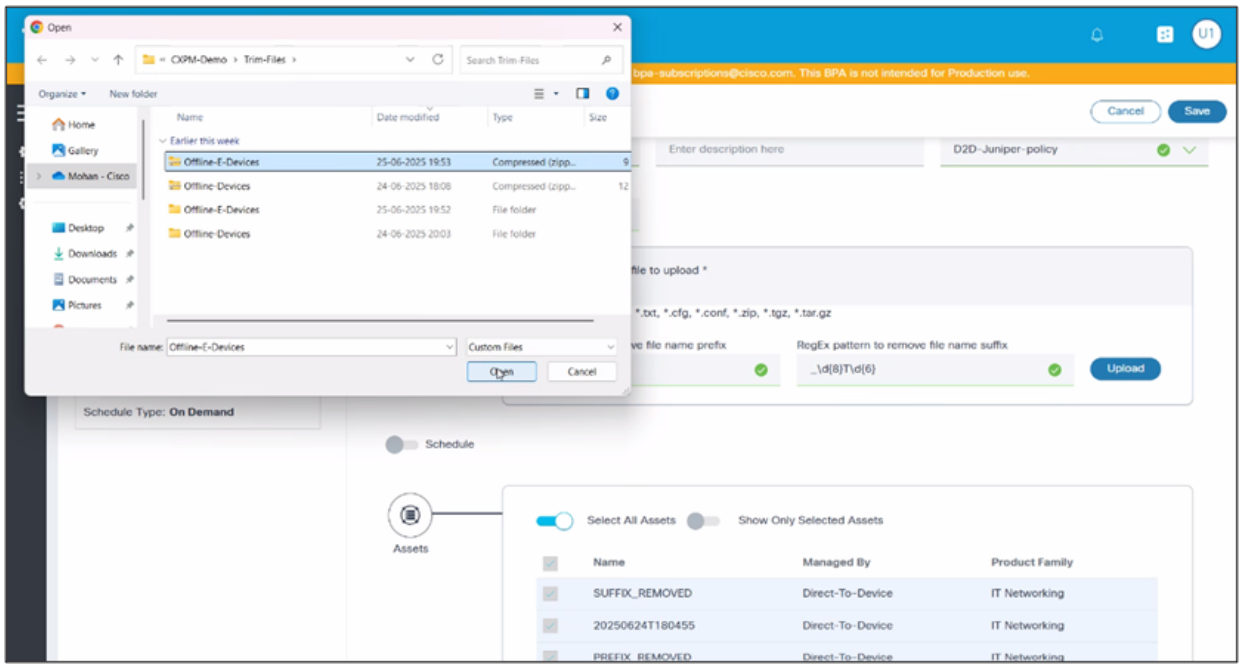
1. Sélectionnez Audit hors connexion dans l'icône Autres options.



Télécharger le fichier

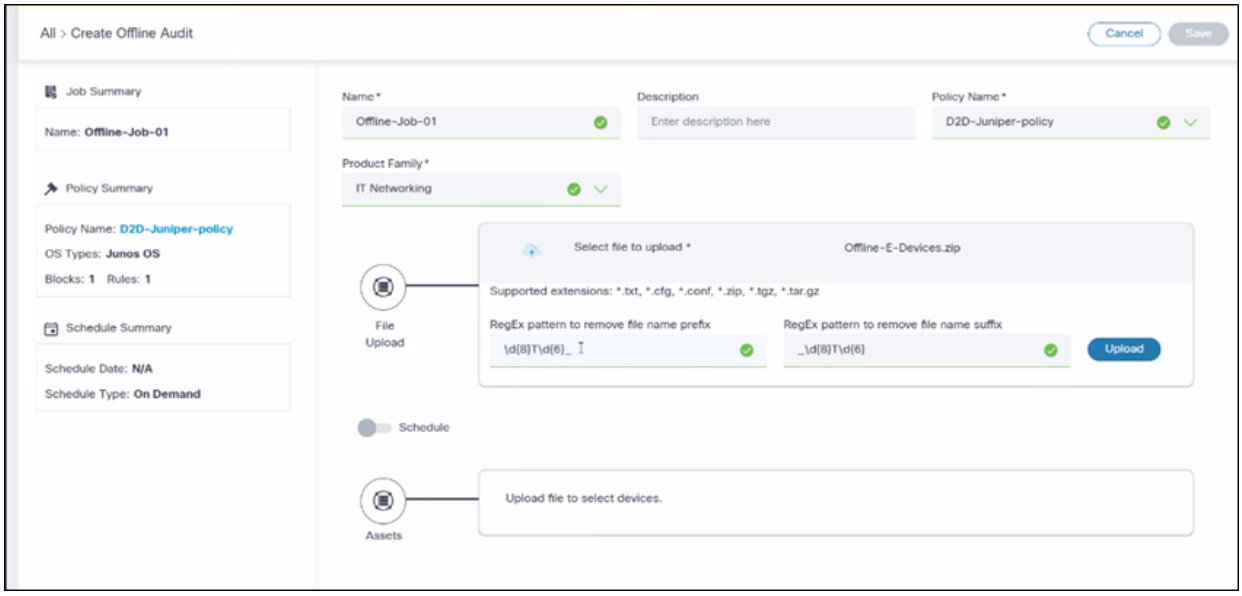
2. Cliquez sur Select file to upload pour télécharger les fichiers de configuration.

Remarque : Les types de fichiers pris en charge sont (.txt,.cfg,.conf,.zip,.tgz,.tar.gz).



Fichiers de bureau

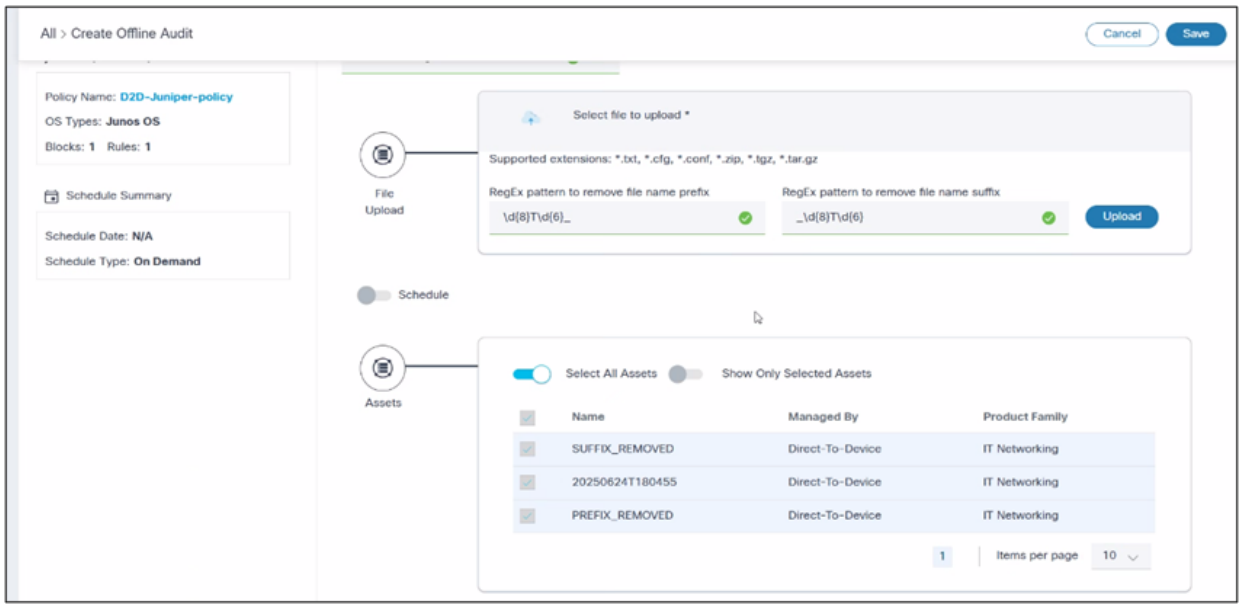
3. Si les fichiers de configuration sont compressés dans un dossier ou une archive, extrayez-les avant de les télécharger.



Modèle Regex

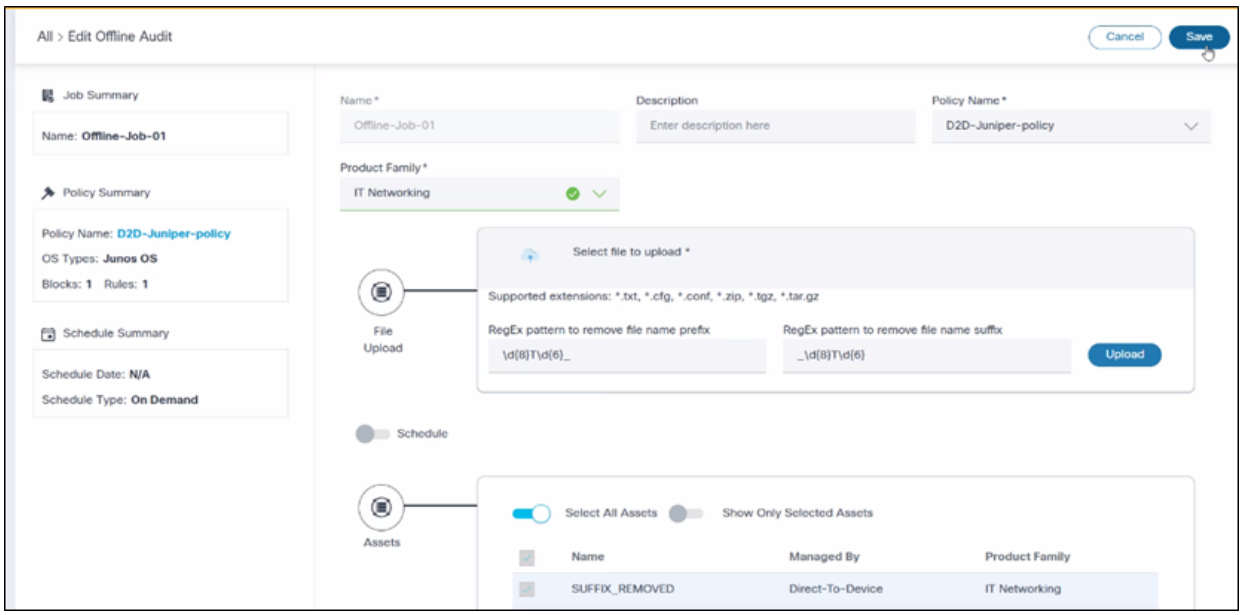
4. Appliquez le modèle Regex pour l'ajustement du nom de fichier (facultatif).

Remarque : Utilisez des modèles d'ajustement de préfixe ou de suffixe (regex) pour standardiser ou simplifier les noms de fichiers téléchargés pour un traitement plus facile.



Télécharger les fichiers

5. Cliquez sur Upload (charger). Un message de confirmation s'affiche, indiquant que les fichiers ont été enregistrés dans la base de données et téléchargés avec succès.



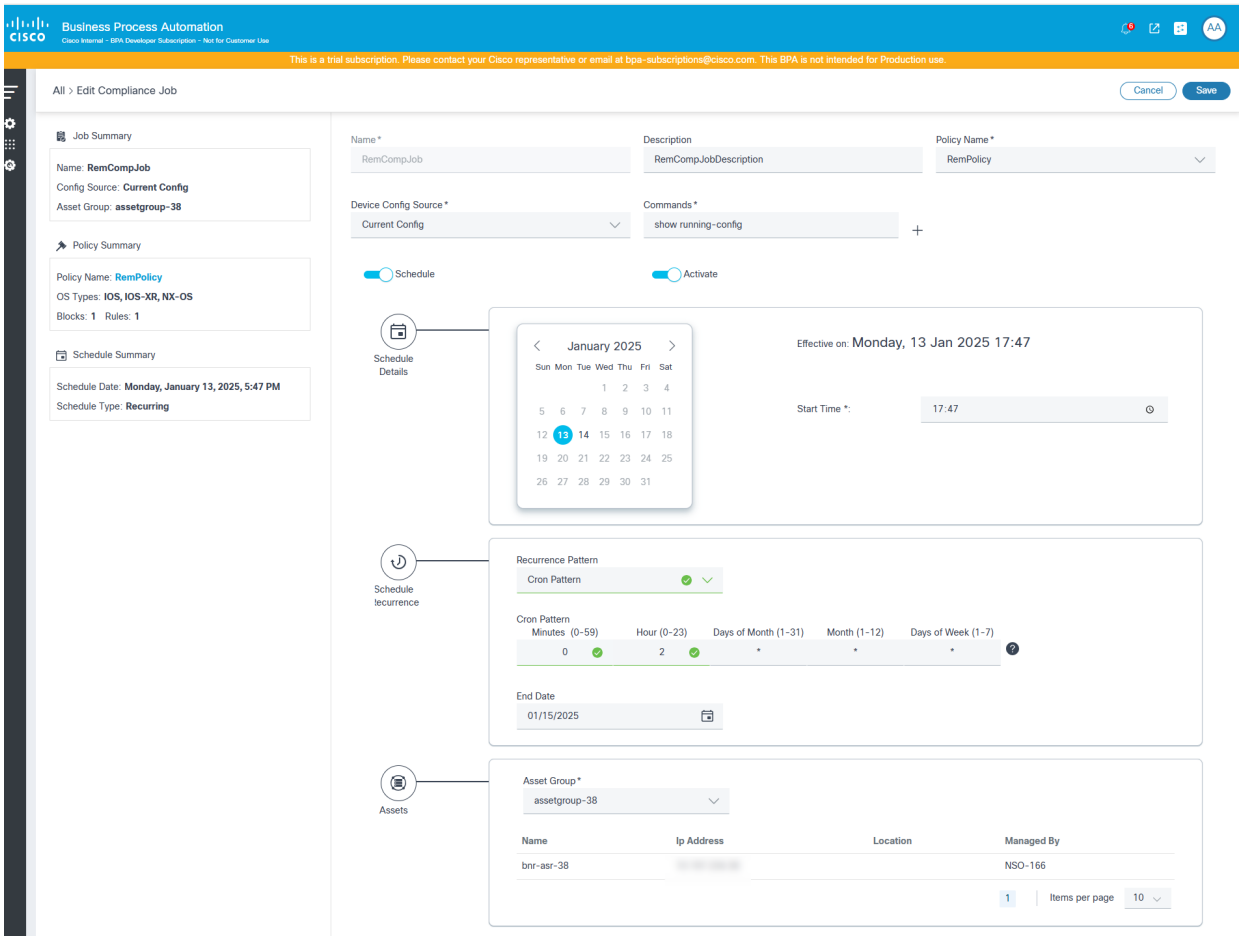
Enregistrer l'audit hors connexion

6. Cliquez sur Enregistrer pour créer la tâche d'audit hors connexion.

Modification des tâches de conformité

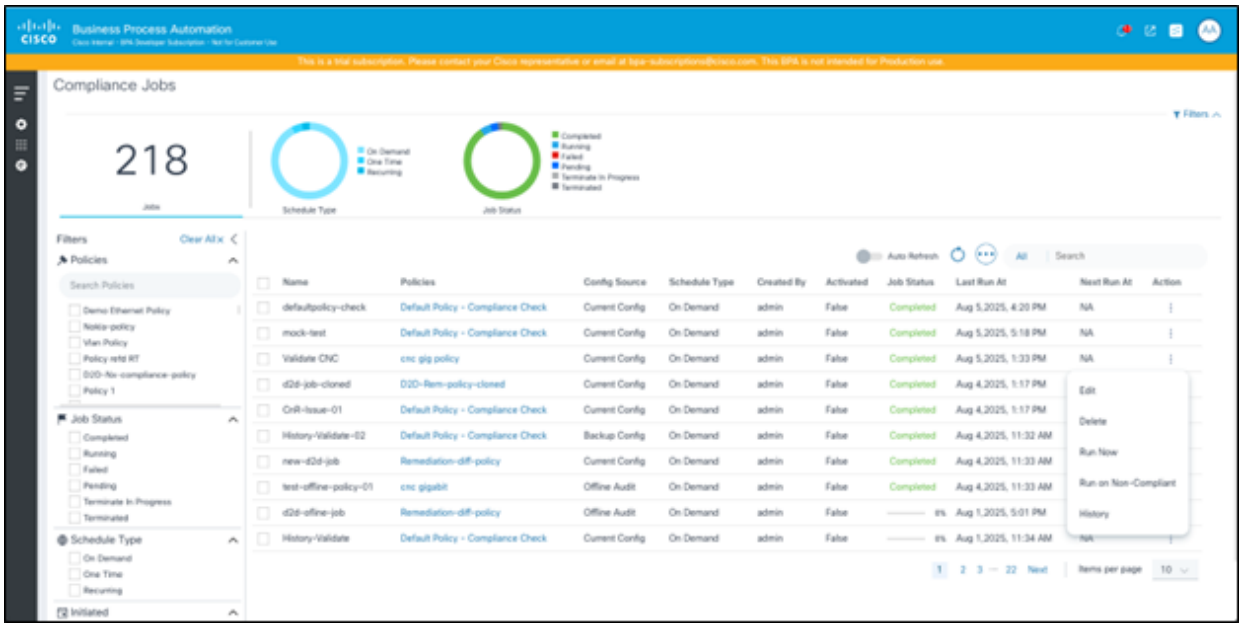
Pour modifier des travaux de conformité, suivez les étapes fournies dans Création de travaux de conformité.

Remarque : Le nom de la tâche ne peut pas être modifié.



Modifier le travail de conformité

Exécuter maintenant ou relancer les tâches de conformité



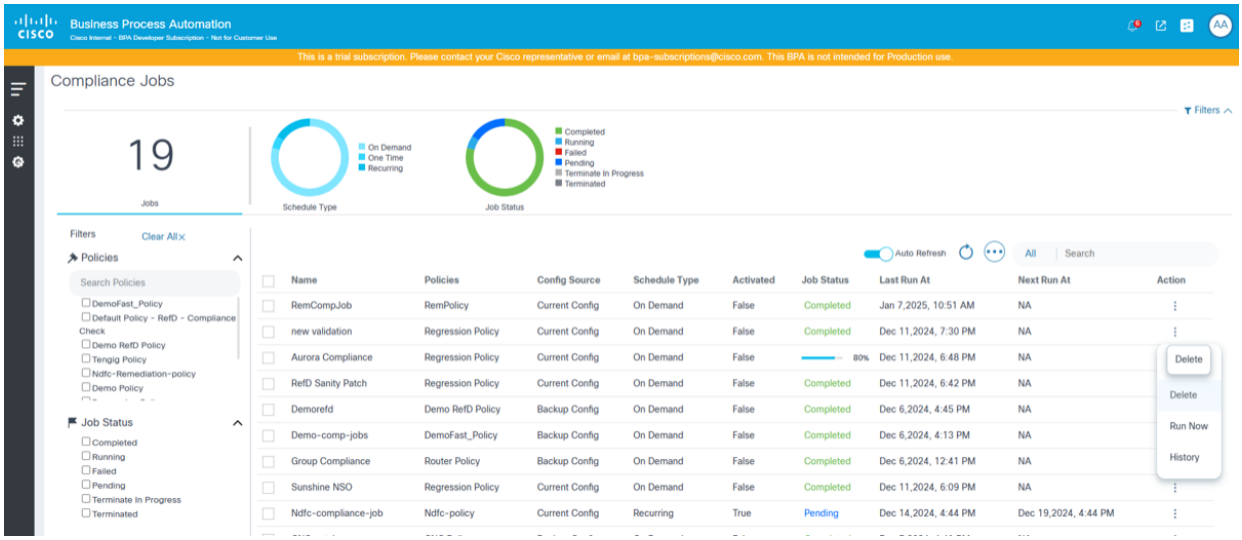
Tâche de conformité - Exécuter maintenant et Exécuter sur non conforme

La grille Tâches de conformité propose une option permettant d'exécuter une tâche à la demande en sélectionnant Exécuter maintenant dans l'icône Autres options. Si une tâche a déjà été exécutée, les utilisateurs peuvent sélectionner Exécuter sur non conforme dans l'icône Autres options. Cette action exécute la tâche de conformité uniquement sur la liste des ressources qui ne sont pas marquées comme entièrement conformes lors de l'exécution précédente.

Suppression de travaux de conformité

Le portail permet de supprimer un ou plusieurs travaux de conformité si l'utilisateur dispose du rôle RBAC (Role Based Access Control) correct. Les travaux ne peuvent pas être supprimés lorsqu'une exécution est en cours. Les utilisateurs peuvent choisir de supprimer une ou plusieurs tâches de conformité.

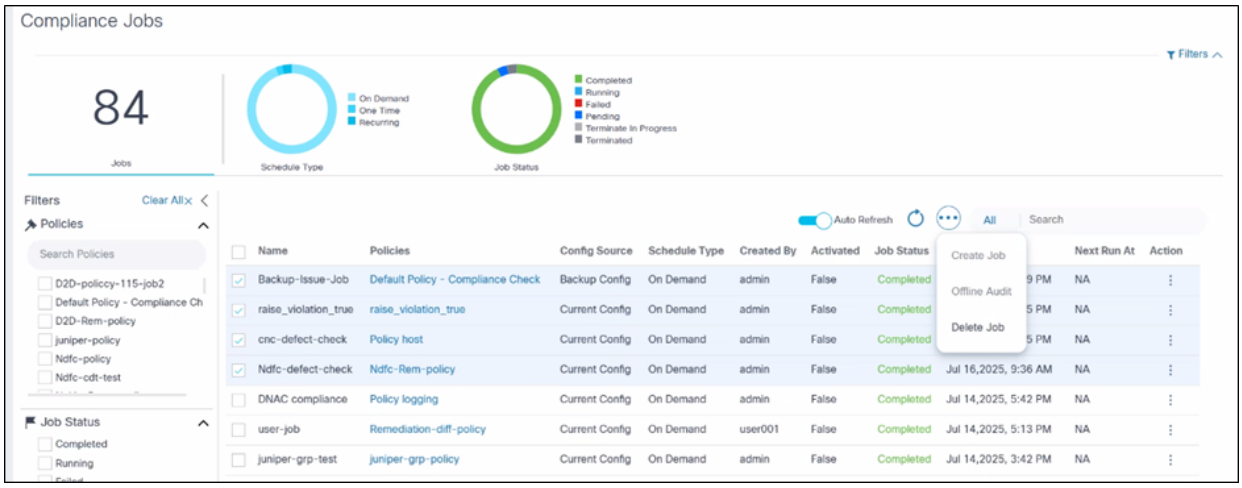
Pour supprimer une tâche de conformité :



Suppression d'une tâche de conformité unique

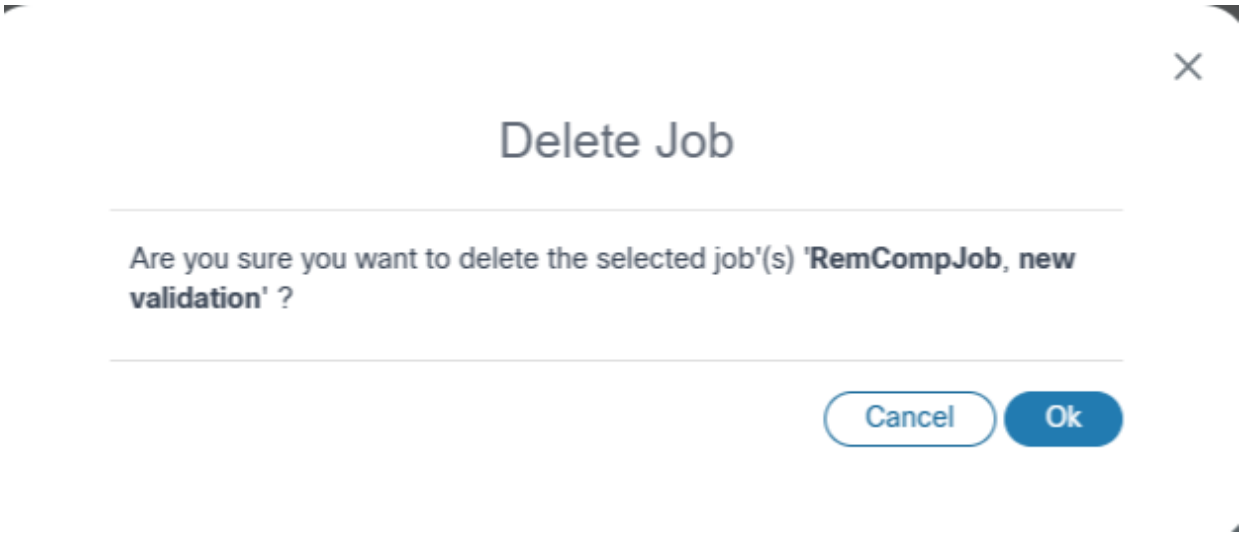
1. Dans la page Tâches de conformité, sélectionnez l'icône Autres options > Supprimer sur le travail à supprimer.

OU



Suppression de plusieurs tâches de conformité

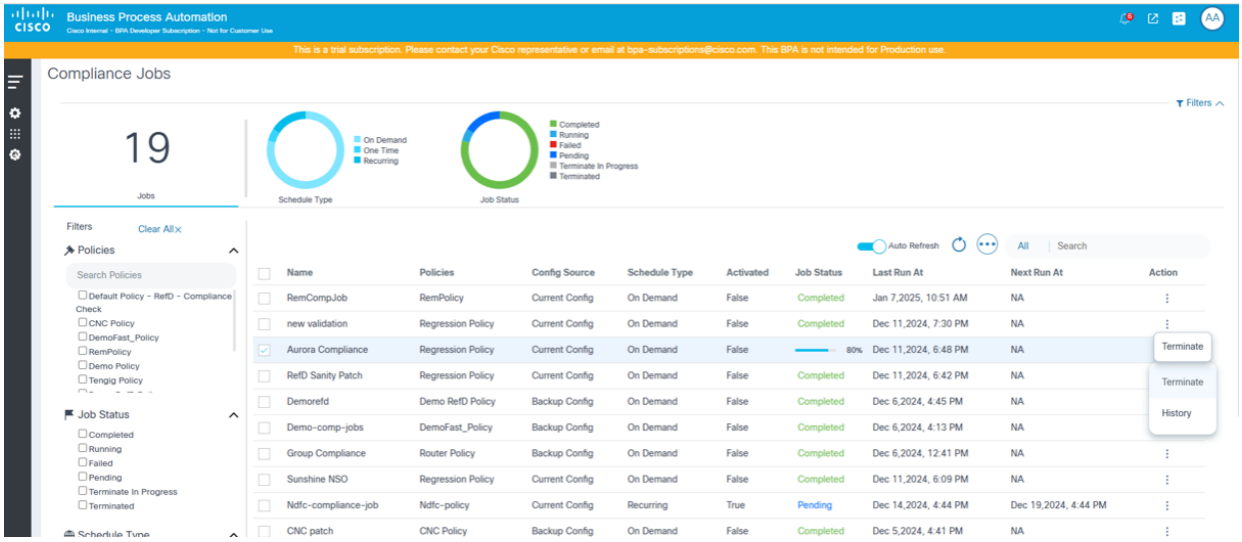
Pour supprimer plusieurs travaux de conformité, cochez les cases correspondant aux travaux à supprimer et sélectionnez Plus d'options > Supprimer le travail. Une confirmation s'affiche.



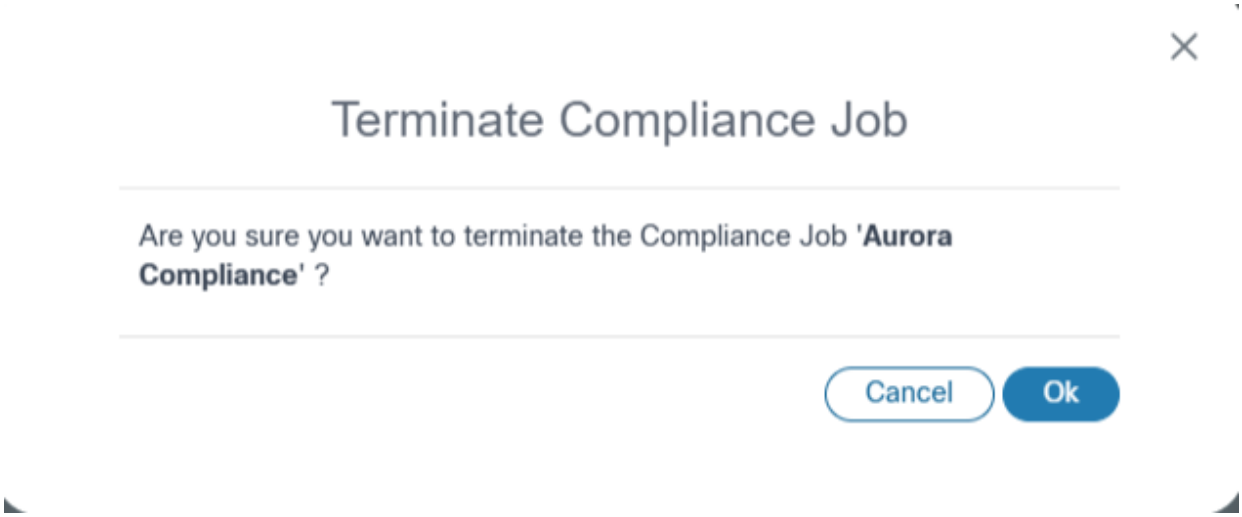
Supprimer la confirmation de tâche de conformité

Fin des travaux de conformité

Le portail offre aux utilisateurs la possibilité de mettre fin à l'exécution d'un travail donné. Lorsqu'un travail est terminé, les périphériques en cours d'exécution terminent leur exécution et annulent toutes les autres exécutions de périphériques en file d'attente.



Fin des travaux de conformité

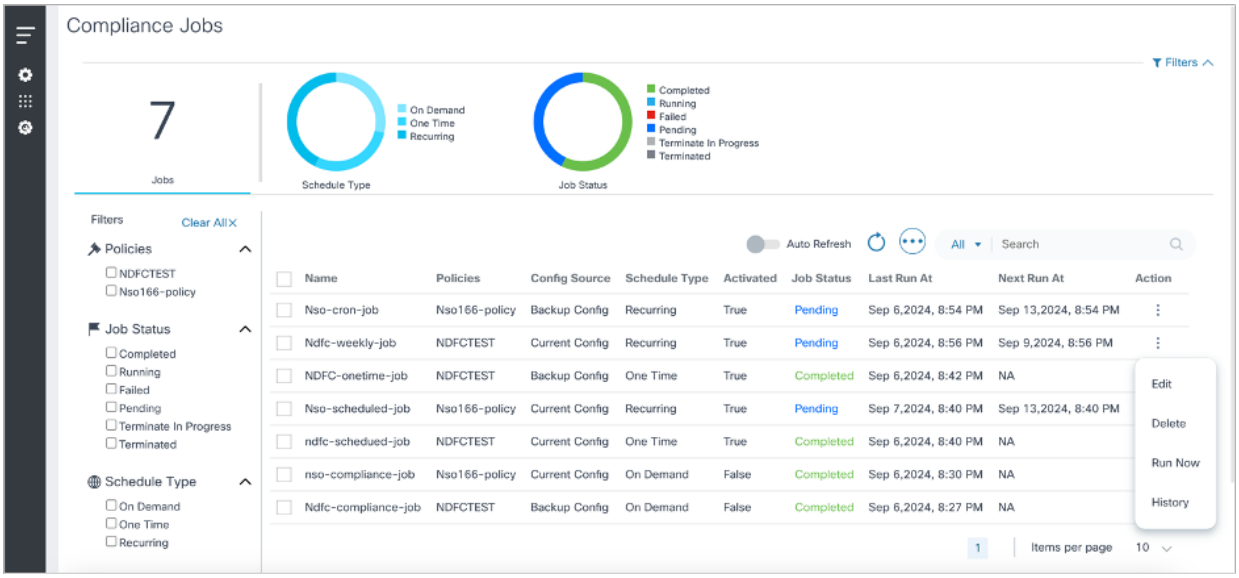


Résilier la confirmation de tâche de conformité

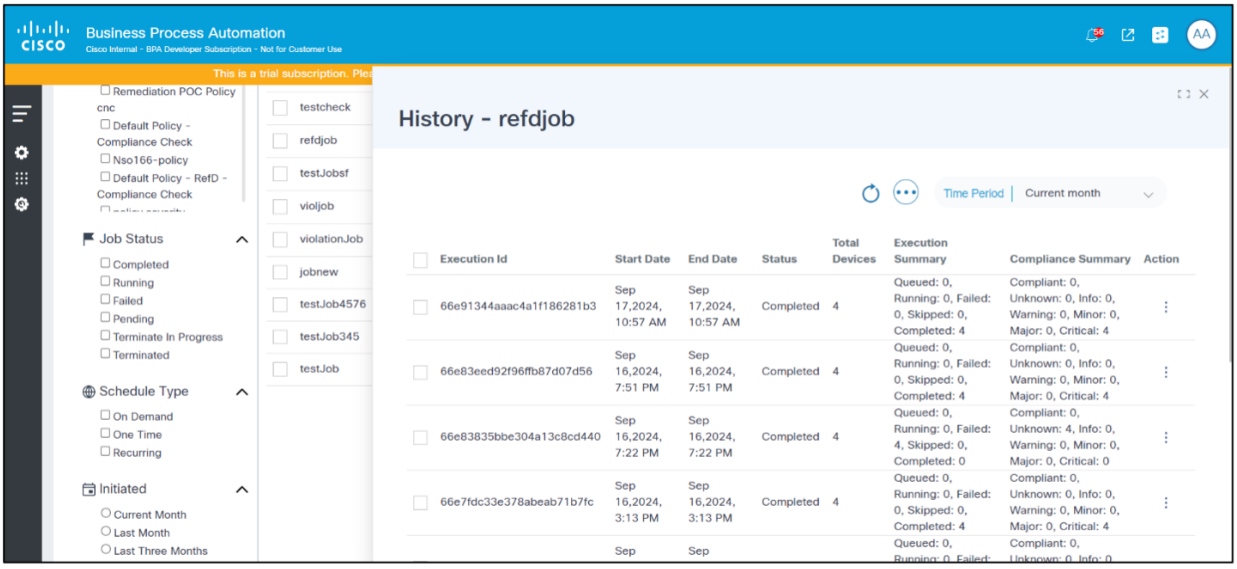
Historique des tâches de conformité

L'option Historique de la tâche de conformité affiche la liste des exécutions pour la tâche sélectionnée, filtrée par la plage de dates programmée.

Pour afficher l'historique d'un travail de conformité, dans la page Tâches de conformité, sélectionnez l'icône Autres options > Historique. La page Historique s'affiche.



Historique des tâches de conformité

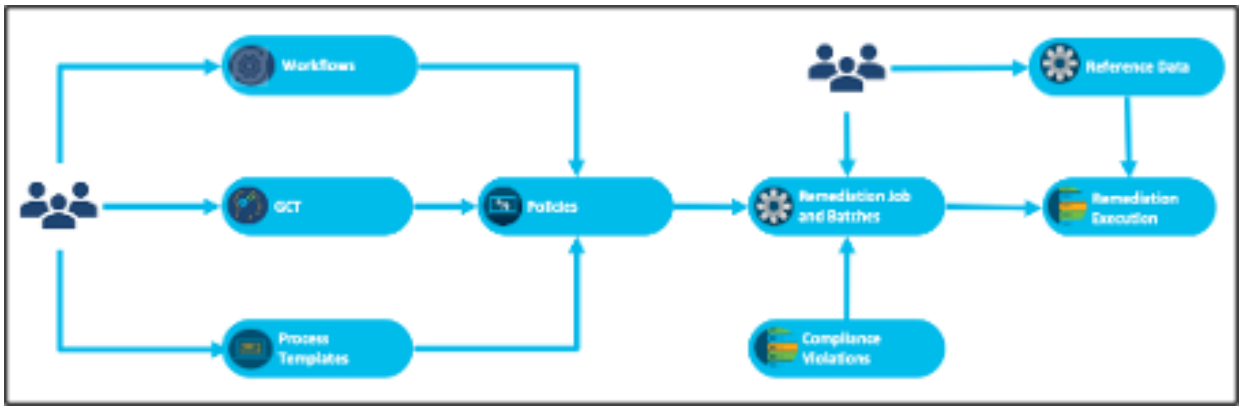


Page Historique

Tâches de correction

L'infrastructure de correction permet aux opérateurs de corriger les violations de conformité répertoriées dans le tableau de bord de conformité. Ce cadre utilise des workflows, des GCT et des modèles de processus.

Diagramme de flux de résolution de configuration



Présentation de la correction de configuration

L'exemple d'utilisation Correction de la configuration permet aux opérateurs de corriger les violations de configuration sur les périphériques à l'aide des travaux de résolution. La stratégie de conformité est d'abord configurée avec le workflow approprié, les modèles GCT et les modèles de processus par type de contrôleur. Une tâche de correction est exécutée pour une stratégie sur une liste de ressources affectées. Pendant la conversion, les valeurs à appliquer sur un périphérique peuvent être extraites à partir de diverses sources de données, y compris le résultat de l'exécution de la conformité, l'application RefD et la configuration de périphérique existante. Le workflow peut être personnalisé en fonction des besoins spécifiques du client afin de prendre en charge des étapes supplémentaires lors de la correction.

Les étapes les plus importantes de la fonction de conversion sont expliquées ci-dessous :

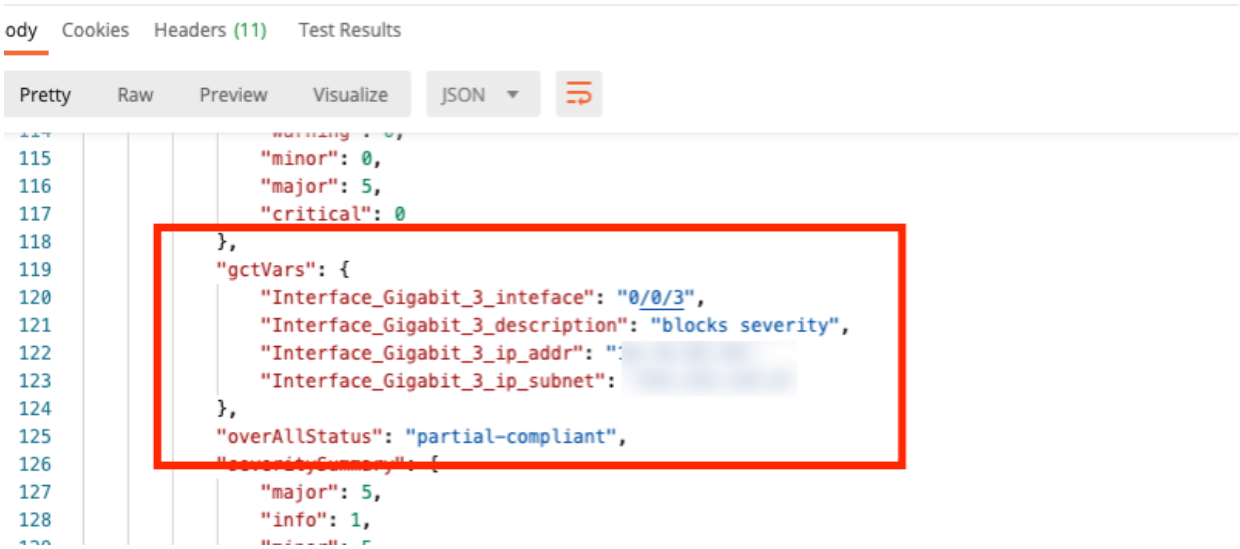
Modèle GCT

Les GCT sont une fonctionnalité de base BPA utilisée pour appliquer des modifications de configuration sur les périphériques à l'aide de modèles spécifiques au contrôleur.

- Création d'un modèle GCT qui met à jour les configurations des périphériques et résout les violations de conformité
- La structure prend en charge le mappage automatique des variables si les variables du modèle GCT respectent la syntaxe suivante :
  - Pour les blocs de configuration à un seul périphérique : **<>_<>**. Exemple : adr_ipv4_interface_gestion, sous-réseau_ipv4_interface_gestion
  - Plusieurs blocs de configuration de périphériques sont prévus pour une prochaine version
- Si les champs « Nom de l'identificateur de bloc » et « Nom de la variable du bloc » contiennent des espaces, ces espaces doivent être remplacés par des traits de soulignement (« _ ») (par exemple, si « Nom de l'identificateur de bloc » est « Interface de gestion » et que « Nom de la variable » est « IPV4_ADDR », le nom de la variable dans le GCT doit être « Interface de gestion_IPV4_ADDR »)
- Les utilisateurs peuvent vérifier la sortie « gctVars » de l'exécution du dispositif de conformité pour voir si la syntaxe et les mappages des variables GCT sont corrects ; Pour

obtenir l'exécution du périphérique de conformité, utilisez les API REST suivantes :

- Obtenir les exécutions pour trouver l'ID d'exécution
  - URL: /api/v1.0/compliance-remediation/compliance-executions
  - Méthode : GET
- Obtenir les exécutions de périphériques en utilisant l'ID d'exécution
  - URL: https://<>/bpa/api/v1.0/compliance-remédiation/compliance-device-exécutions?executionId=<>
  - Méthode : GET



Variables GCT - gctVars

- Pour récupérer les variables du bloc, utilisez l'API REST suivante :
  - URL: https://<>/bpa/api/v1.0/compliance-remédiation/utils/schema
  - Méthode : POST
  - Body (Corps) : {«blockName» : « << nom du bloc >> » }
- Validez les modèles GCT en appliquant les modèles aux périphériques pour l'exécution à

sec et la validation
- Configurez les modèles GCT ci-dessus dans la stratégie de conformité

Workflows

L'infrastructure de correction fournit les workflows de référence prêts à l'emploi suivants :

- PROCESSUS DE CORRECTION : Ce workflow présente l'ensemble commun des étapes impliquées dans l'exécution de la conversion.
- SOUS-PROCESSUS DE CORRECTION : Ce workflow contient des tâches d'affectation de variables, d'exécution à sec GCT et de validation GCT qui peuvent être personnalisées par d'autres équipes en fonction des besoins.

Les deux workflows peuvent être utilisés tels quels, mis à jour ou remplacés en fonction des besoins du client.

Modèles de processus

Les modèles de processus et les modèles d'analyse peuvent être configurés par rapport à la stratégie pour exécuter des vérifications avant et après et comparer les résultats.

Politiques

La stratégie CnR relie les workflows, les modèles GCT et les modèles de processus par type de périphérique, qui peuvent être utilisés pour corriger la configuration à l'aide de tâches.

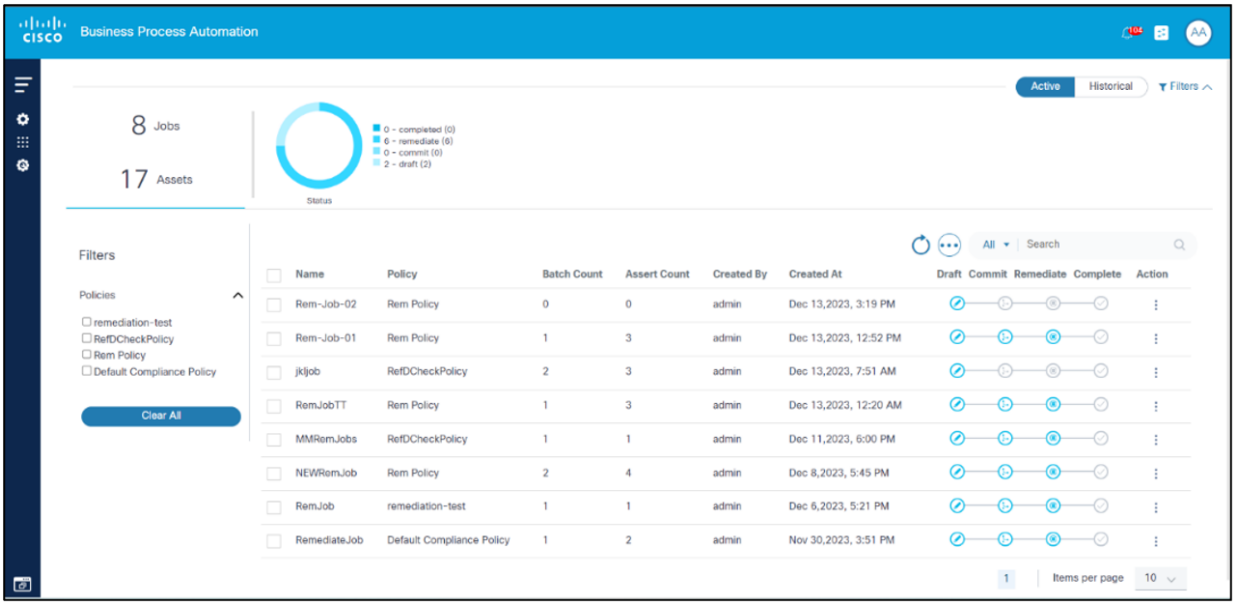
Tâches de correction

Les tâches de conversion aident les opérateurs à appliquer des stratégies de conversion à une liste sélectionnée d'actifs affectés. Le travail de résolution peut être exécuté à la demande ou selon les prévisions. Au moment de l'exécution, le workflow de conversion peut extraire des données de diverses sources, notamment les détails du périphérique, les détails de l'exécution de la conformité et l'infrastructure RefD.

Liste des travaux de résolution

Les utilisateurs peuvent filtrer, trier et afficher les travaux de résolution créés dans le tableau de bord comme suit :

- Tâches : Affiche le nombre total de tâches créées
- Ressources : Affiche le total des ressources créées
- État : Affiche les tâches par statut
- Actif et historique : Affiche les tâches actives ou historiques (inactives), en fonction de la sélection
- Stratégies : Filtre les tâches de résolution par stratégies
- Grille principale : Affiche la liste par défaut des travaux qui peuvent être triés en cliquant sur l'en-tête et inclut une recherche par nom et politique avec paginations
- Actions: Les tâches peuvent être archivées ou supprimées lorsqu'elles sont à l'état Brouillon ou Terminé ; impossible d'archiver ou de supprimer un travail en cours d'exécution

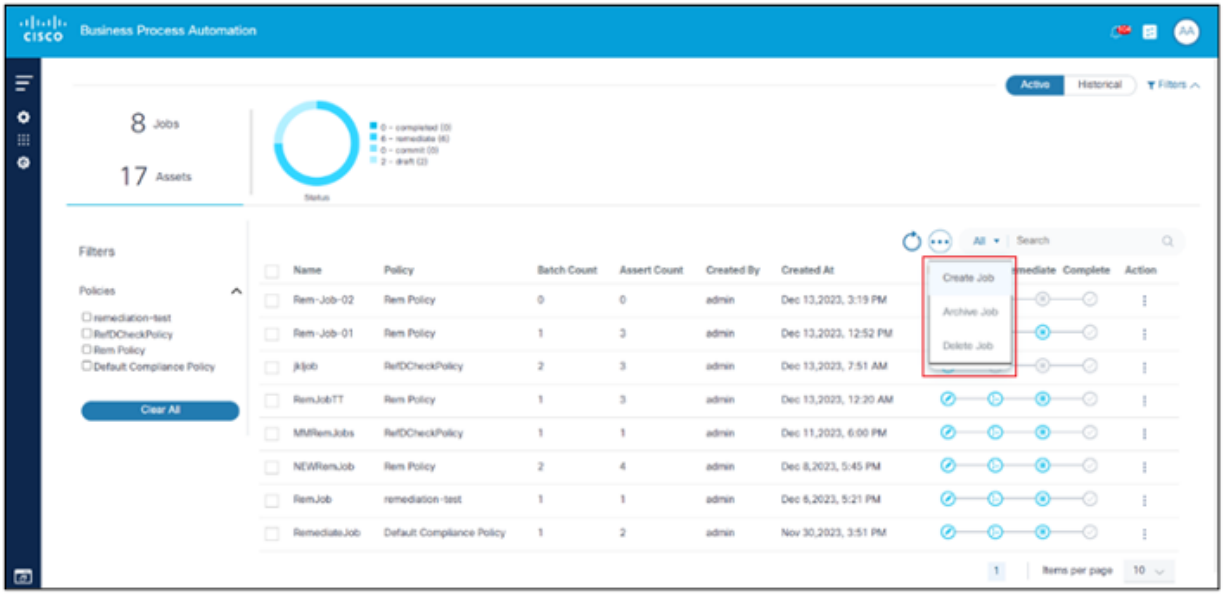


Liste des travaux de résolution

Création et modification de travaux de résolution

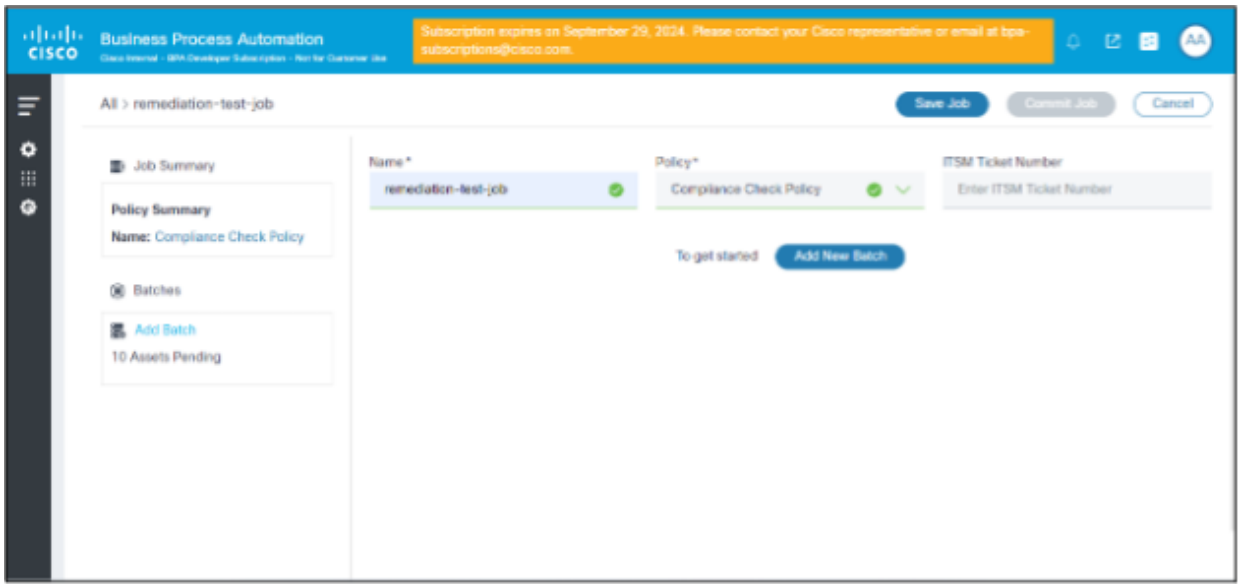
Les travaux de résolution sont créés à partir de la page Liste des travaux et peuvent être créés en procédant comme suit :

1. Cliquez sur l'icône Autres options > Créer un travail. La page Créer un travail s'affiche.



Options des travaux de résolution

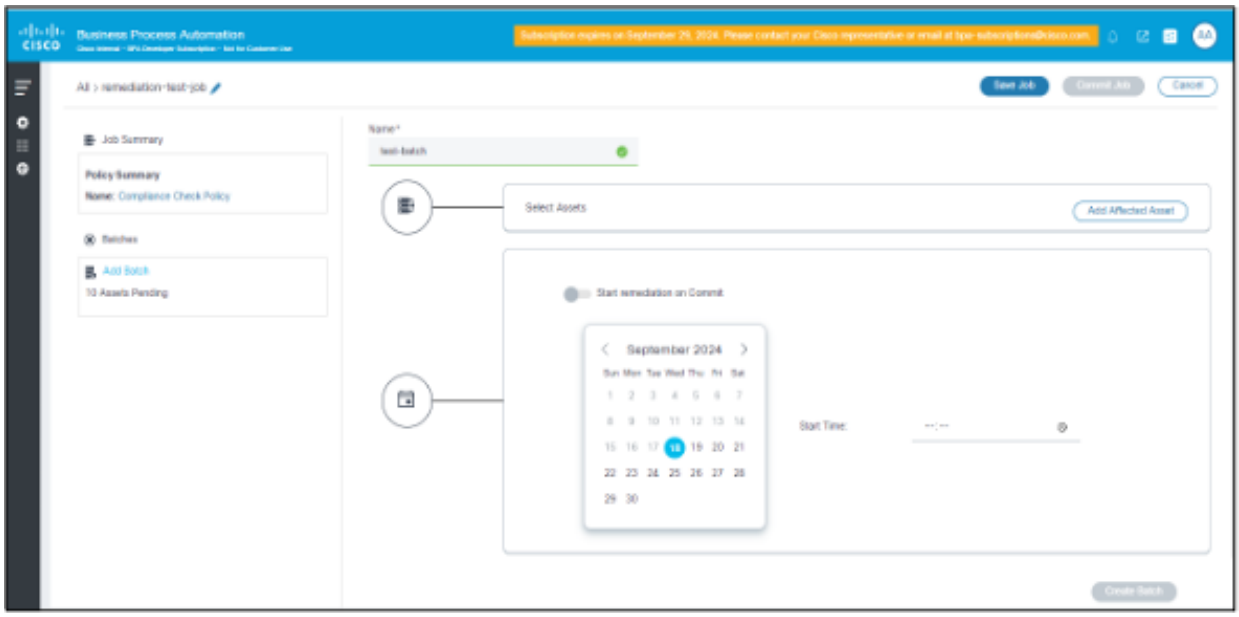
2. Complétez ou modifiez les détails.



Tâches de correction : Détails

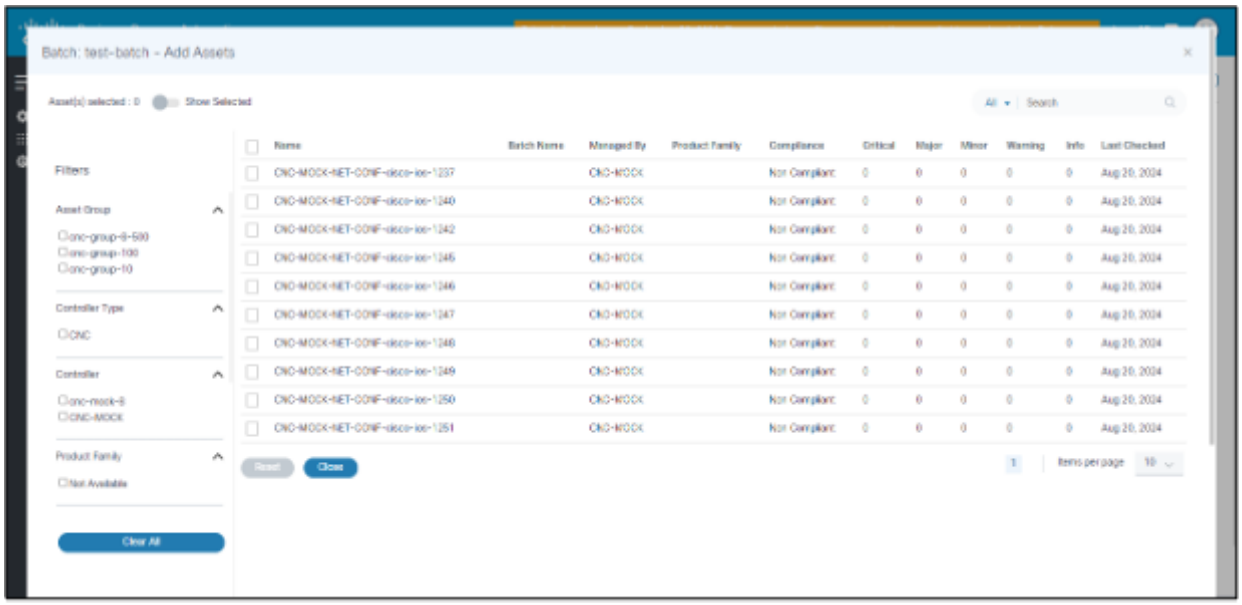
3. Cliquez sur Enregistrer le travail.

Pour ajouter des lots à des travaux à partir de la page Créer un travail :



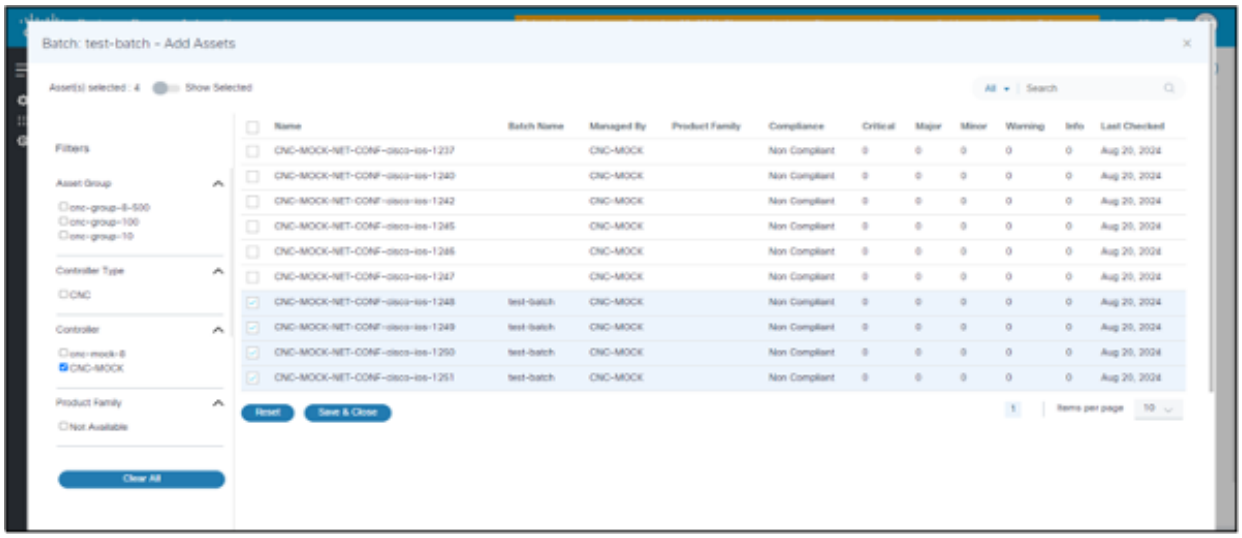
Tâches de correction : Ajouter des lots

1. Cliquez sur Ajouter un nouveau lot.
2. Saisissez le nom, les détails de l'immobilisation affectée et les détails du programme.
3. Cliquez sur Ajouter les ressources affectées.
4. Dans la page Détails des ressources, sélectionnez la liste des ressources affectées et cliquez sur Enregistrer le travail.
5. Filtrez les ressources en fonction du type de contrôleur, du contrôleur, du groupe d'actifs et de la gamme de produits.
6. Une fois les ressources sélectionnées, cliquez sur Save & Close pour revenir à la page précédente.



Tâches de correction : Ajouter les ressources affectées

Remarque : Les utilisateurs peuvent appliquer des filtres dans la page Actifs affectés



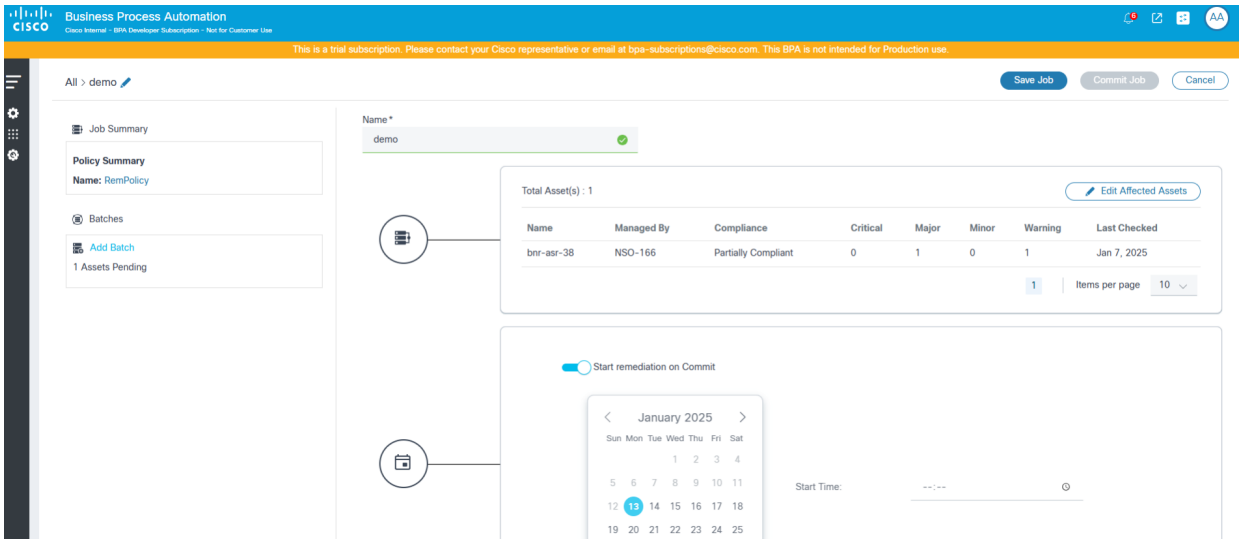
Tâches de correction : Ajouter les filtres affectés

Une fois les immobilisations affectées ajoutées, le lot peut être exécuté une seule fois, soit lors d'une sauvegarde, soit à une date ultérieure planifiée.

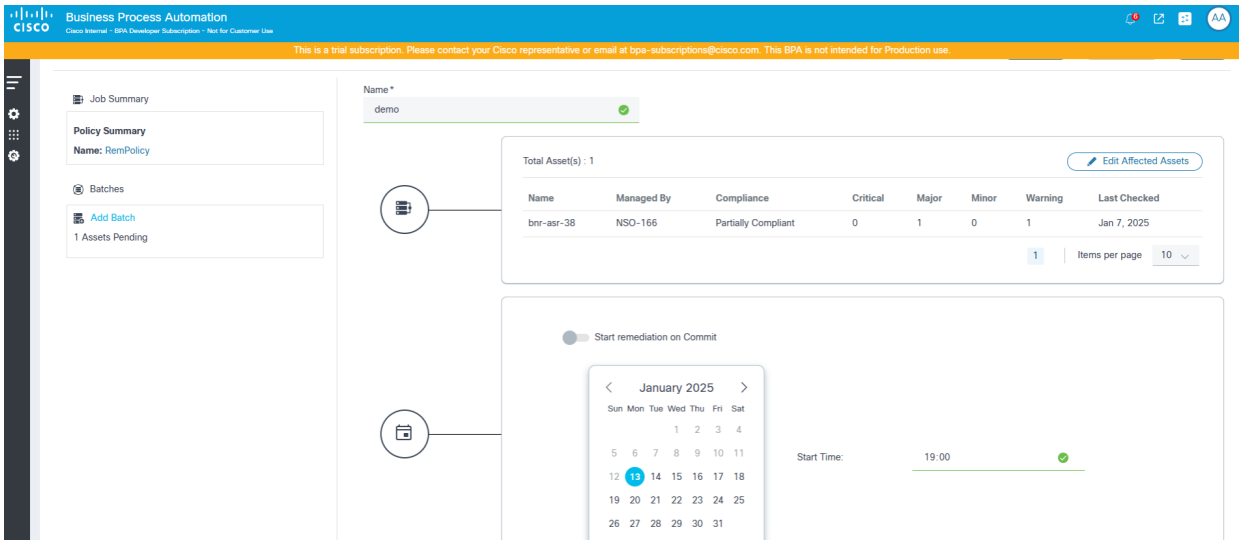
Remarque : Pour exécuter le travail à la demande, activez la bascule Lancer la conversion lors de la validation. Si un utilisateur sélectionne cette option, la date et l'heure ne sont pas nécessaires. Si l'utilisateur sélectionne l'option One-Time, la date et l'heure doivent être fournies pour exécuter le travail.

Un même travail de résolution comporte plusieurs lots. Chaque lot peut être démarré lors de la validation ou à une date et une heure planifiées.

Un lot de résolutions en cours de validation peut être exécuté à la demande ou planifié.



Tâches de correction : À la demande

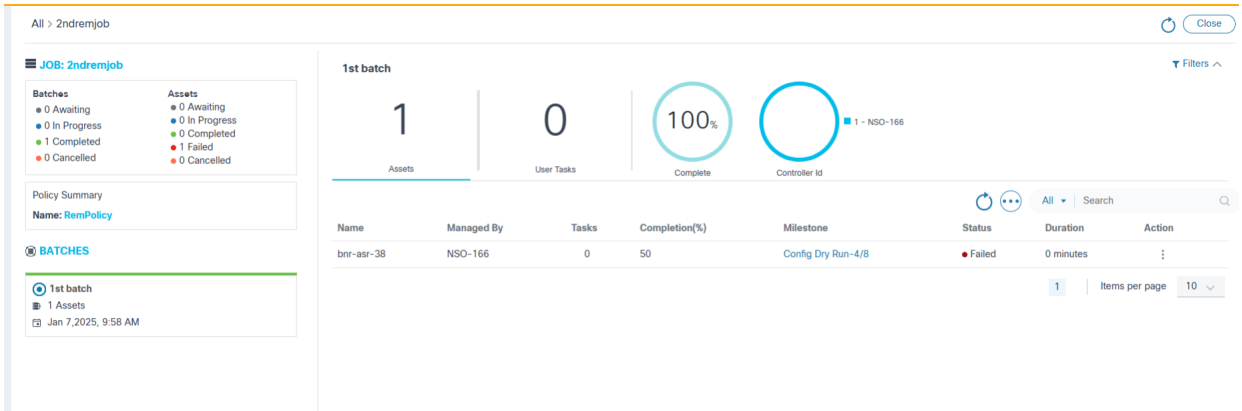


Tâches de correction : Une seule fois/planifié

Exécution de la correction : Liste des périphériques

Une fois le travail de résolution validé, son exécution est déclenchée et son état s'affiche dans la page Lister les périphériques sous Travaux de résolution. Les utilisateurs peuvent appliquer des filtres par ID de contrôleur, Nom, Géré par, Gamme de produits.

- TÂCHE : affiche les détails de l'état des lots et des actifs, ainsi que le nom de la stratégie sélectionnée pour exécuter le travail de résolution
- LOTS : affiche la liste des batches dans le cadre de la tâche de conversion en cours
- Actualisation automatique : affiche les options permettant d'actualiser automatiquement la page toutes les 30 secondes si le travail est en cours d'exécution, d'actualiser la page ou d'annuler pour revenir à la page précédente
- Détails de niveau lot : affiche les détails de synthèse au niveau du lot, notamment le nombre total d'actifs, le nombre de tâches utilisateur, le pourcentage d'achèvement et les détails du contrôleur
- Grille de ressources : affiche la vue de la grille des ressources, y compris la tâche utilisateur, le pourcentage de réalisation et le jalon en cours pour chaque ressource



Exécution de la correction : Liste des périphériques

Exécution de la correction : Détails des tâches utilisateur en ligne

Dans la liste des périphériques, la colonne Tâches indique si un utilisateur a des tâches à effectuer.

Pour afficher les détails des tâches utilisateur en ligne :

1. Sélectionnez le nombre de tâches. La fenêtre de liste Tâches utilisateur s'affiche.
2. Sélectionnez une tâche. La fenêtre Détails des tâches utilisateur s'affiche.

Les actions suivantes peuvent être entreprises à partir de la ligne :

- Terminer
- Réessayer
- Annuler

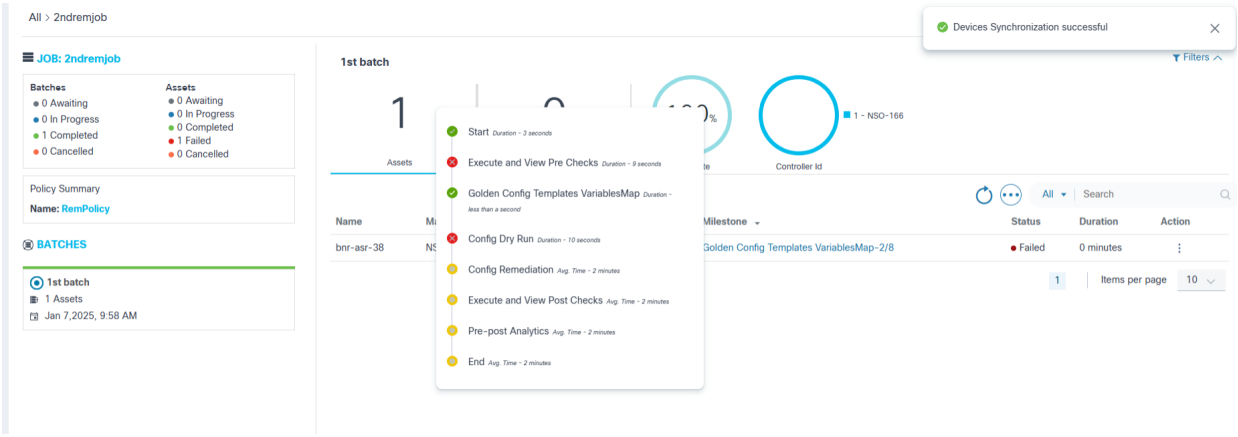
Exécution de la correction : Détails du jalon en ligne

Dans la liste des périphériques, la colonne Jalon indique le jalon actuel lié à la correction du périphérique donné.

Pour afficher les détails des jalons en ligne, sélectionnez la colonne. La fenêtre Détails du jalon s'ouvre.

Les états suivants sont disponibles pour les jalons :

- Non démarré
- Marche
- Terminé
- Échec



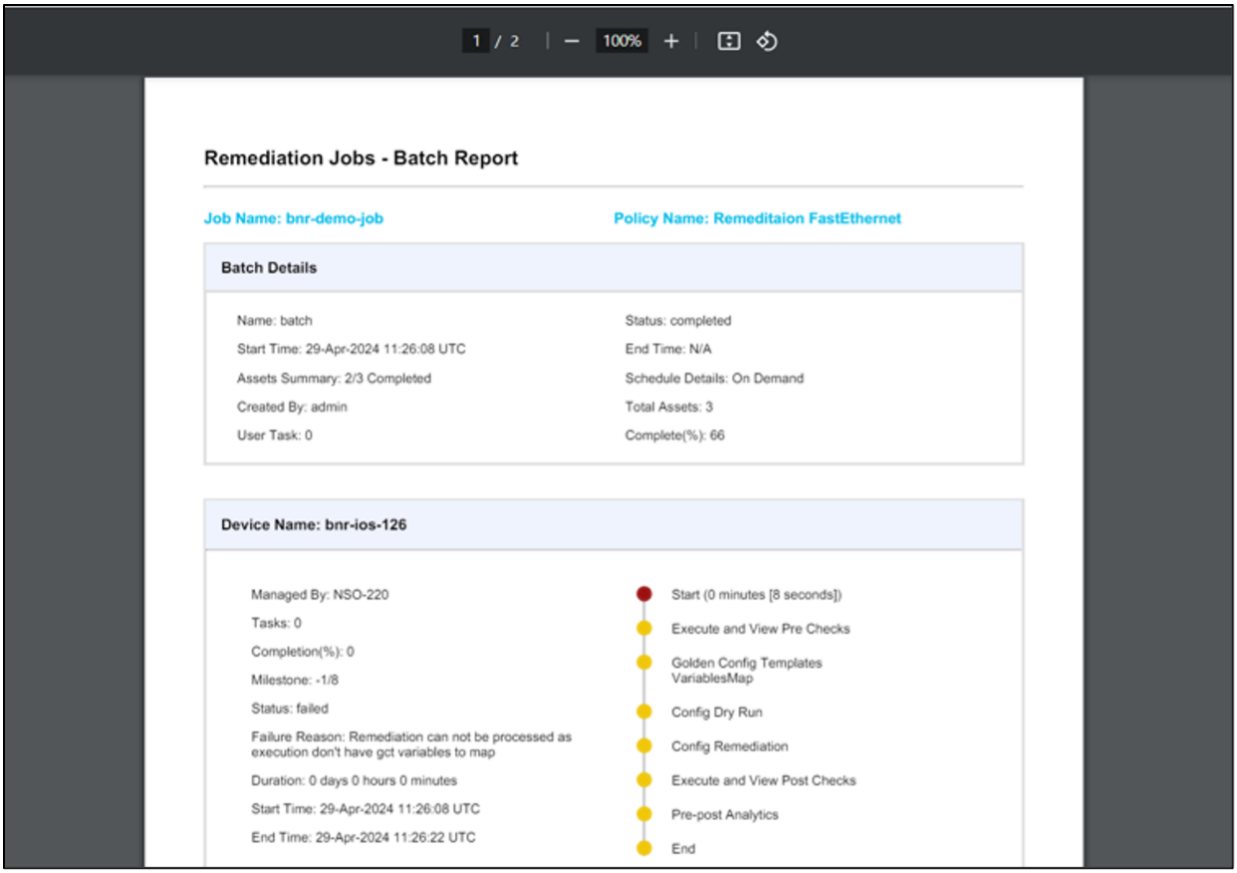
Exécution de la correction : Détails du jalon en ligne

Exécution de la correction : Génération et téléchargement de rapports PDF récapitulatifs sur les lots

Des résumés de lots peuvent être générés et téléchargés.

Pour télécharger le rapport de synthèse au format PDF par lot :

1. Cliquez sur l'icône Autres options > Générer un rapport. Le système vérifie en interne si le rapport est prêt. Lorsque le rapport est prêt, l'option Télécharger le rapport est activée.
2. Cliquez sur l'icône Autres options > Télécharger le rapport. Le PDF est téléchargé.



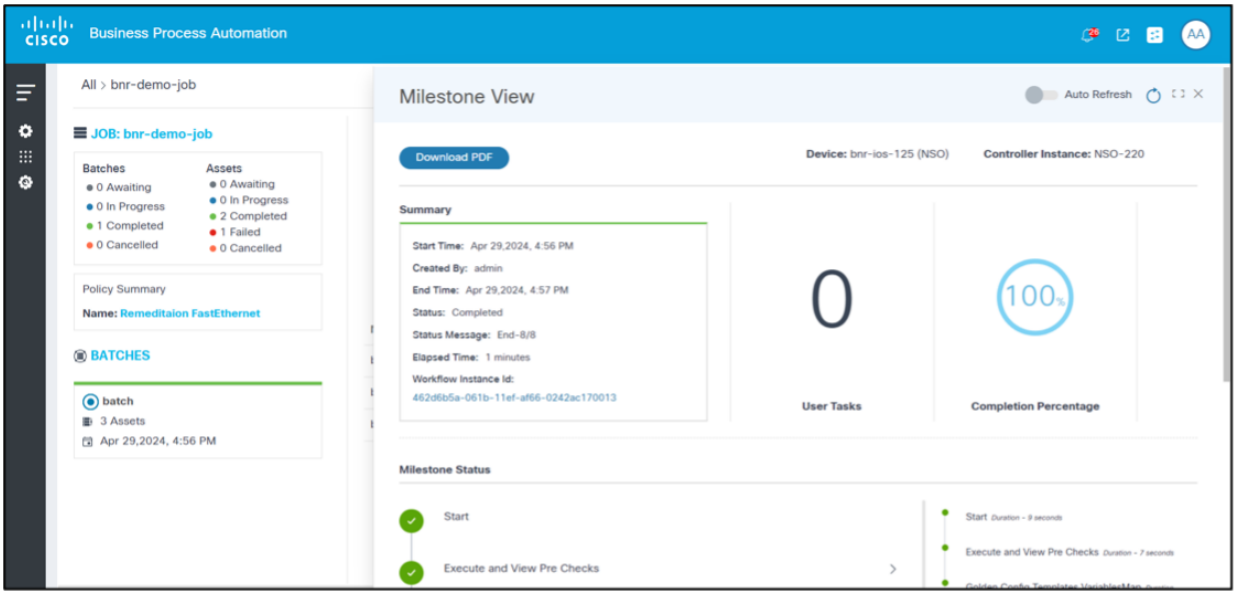
Résumé du lot PDF

Le rapport sur les lots de travaux de résolution contient une section Détails du lot, qui fournit une synthèse du lot de résolution, comme le nom du lot, le nom du lot, les heures de début et de fin, le total des immobilisations et le statut global. Elle est suivie d'une section Device Detail (une section par périphérique) qui inclut le nom du périphérique, l'état de correction spécifique au périphérique, le calendrier, la durée et la liste des jalons, ainsi que l'état.

Exécution de la correction : Détails du périphérique

Pour afficher les détails du périphérique pour les jalons, sélectionnez la page Détails du périphérique. La page Milestone View s'affiche.

Un résumé de la correction pour le périphérique donné avec un état de jalon détaillé s'affiche, y compris le résultat de la commande des jalons clés terminés. Par exemple, les sorties de commande du modèle de processus, les sorties de tirage à sec GCT et le contenu de sortie de différence analytique peuvent être affichés.



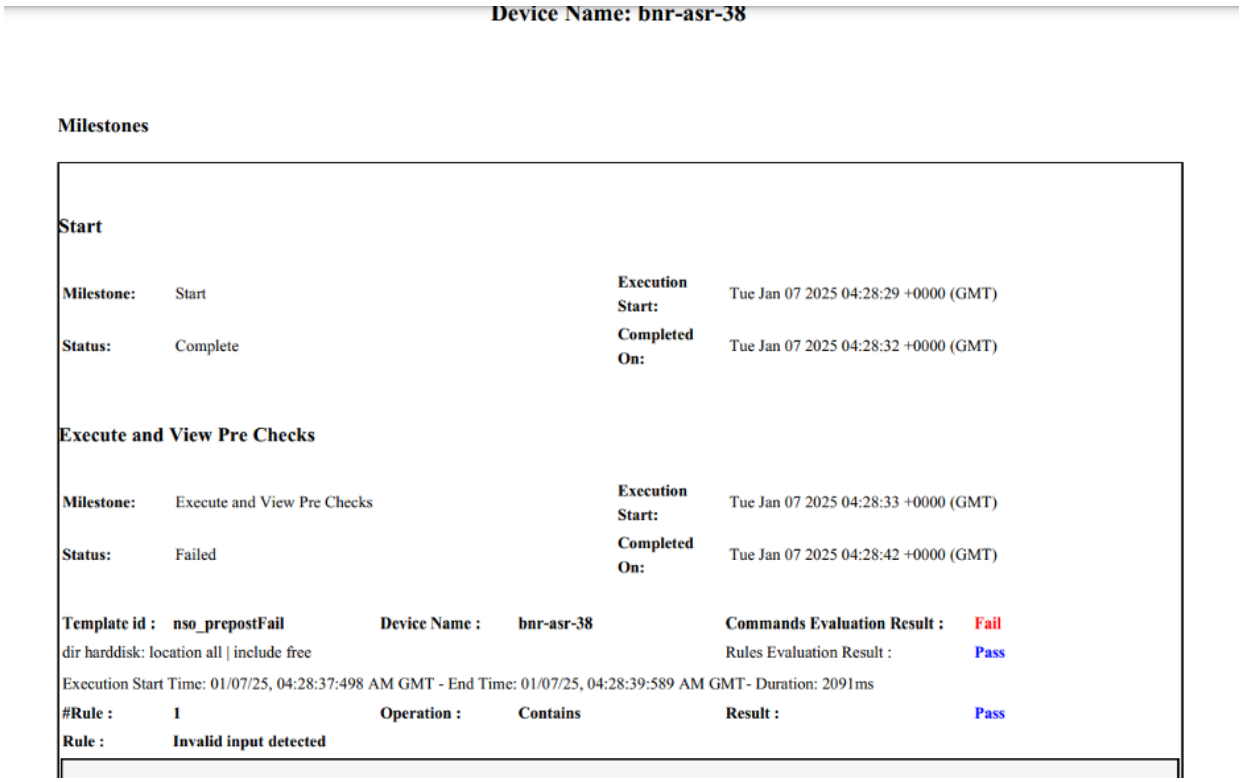
Exécution de la correction : Vue Jalon

Exécution de la correction : Détails du périphérique - Rapport d'étape

Pour afficher le rapport de jalons :

1. Sélectionnez la page Détails du périphérique. La page Milestone View s'affiche.
2. Cliquez sur Download PDF. Le rapport d'affichage des jalons est généré et téléchargé comme indiqué ci-dessous.

Ce rapport fournit des détails plus détaillés sur les étapes et le contenu correspondant pour la correction du périphérique sélectionné.



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**				

Exécution de la correction : Détails du périphérique - Jalon Voir le rapport PDF

Configuration: Blocs et règles

Fonctionnalité des blocs

Les blocs de configuration sont des éléments essentiels pour créer et appliquer des politiques de conformité dans les systèmes de gestion de réseau. Ils représentent les configurations CLI des périphériques, telles que celles des interfaces, du protocole BGP (Border Gateway Protocol) du routeur, etc. Les principales caractéristiques des blocs de configuration sont les suivantes :

- Modularité : Les blocs de configuration permettent la création de politiques modulaires, ce qui permet aux administrateurs de définir et de gérer des sections distinctes de configurations de périphériques de manière indépendante. Cette modularité simplifie le processus de mise à jour et de maintenance des politiques de conformité.
- Granularité : En divisant les configurations des périphériques en parties plus petites et plus faciles à gérer, les administrateurs peuvent effectuer des contrôles de conformité précis et appliquer des normes spécifiques. Cela garantit que chaque partie de la configuration du périphérique suit les politiques requises.
- Réutilisabilité : Une fois définis, les blocs de configuration peuvent être réutilisés sur plusieurs politiques et périphériques de conformité. Cette réutilisation réduit la redondance et

garantit la cohérence de la gestion de la configuration.

- Bloc de configuration statique : Un bloc de configuration statique représente la configuration brute du périphérique sans variables.

  Exemple : Le bloc suivant peut être utilisé pour exécuter un contrôle de conformité sur l'interface TwentyFiveGigE0/0/0/31

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

- Bloc de configuration dynamique : Un bloc de configuration dynamique représente la configuration du périphérique qui inclut des variables permettant une plus grande adaptabilité et réutilisation. Ces blocs fonctionnent comme un modèle TTP, s'appliquent aux configurations des périphériques et récupèrent les valeurs des variables. Des conditions peuvent être ajoutées aux règles pour valider ces variables. Référez-vous à https://ttp.readthedocs.io/en/latest/Overview.html pour plus de détails sur le protocole TCP.

  Exemple : Le bloc suivant peut être utilisé pour exécuter un contrôle de conformité sur toutes les interfaces TwentyFiveGigE

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

Bloc de configuration dynamique avec sous-hiérarchies : Ce bloc fonctionne comme un bloc de configuration dynamique et est utilisé pour récupérer des valeurs à partir de configurations de périphériques qui ont plusieurs hiérarchies.

Exemple : L'exemple suivant illustre la configuration d'un périphérique et le bloc dynamique correspondant utilisé pour extraire des valeurs d'une structure hiérarchique.

Configuration du périphérique avec une structure hiérarchique :

```
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 pour analyser la configuration ci-dessus.

```
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
```

Fonctionnalité des règles

Les règles permettent aux utilisateurs de définir des conditions à valider par rapport aux variables présentes dans un bloc de configuration. Dans le cadre d'une exécution, le moteur de conformité analyse la configuration du dispositif, trouve des instances correspondantes d'instances de bloc de dispositif, lit des valeurs sur les lignes et exécute des conditions définies dans les règles par rapport aux valeurs. Le résultat, qu'il y ait ou non une violation dans les lignes de configuration, est stocké pour être affiché dans le tableau de bord.

Les règles de configuration font désormais partie du cycle de création des blocs. Par conséquent, il n'y a pas de page séparée pour afficher les règles. Les règles peuvent être répertoriées, créées et mises à jour sous la page correspondante de création ou de mise à jour de bloc.

Dans le cadre CnR, les règles jouent un rôle crucial dans la validation des configurations par rapport à des conditions spécifiées. Cette section fournit une vue d'ensemble de la manière dont les règles sont intégrées et gérées dans le système.

- Objectif: Les règles permettent aux utilisateurs de définir les conditions utilisées pour valider les variables présentes dans un bloc de configuration
- Processus d'exécution :
    - Le moteur de conformité analyse la configuration du périphérique
    - Identifie les instances correspondantes des instances de bloc de périphérique
    - Extrait les valeurs des lignes de configuration
    - Applique les conditions définies dans les règles à ces valeurs

    - Les résultats indiquant les violations sont stockés et affichés dans le tableau de bord

Intégration au cycle de vie des blocs

- Intégration du cycle de vie : Les règles de configuration font désormais partie intégrante du cycle de création des blocs
- Gestion :
    - Les règles sont répertoriées, créées et mises à jour directement dans les pages utilisées pour la création ou les mises à jour de blocs
    - Il n'existe pas de page dédiée à l'affichage des règles, ce qui permet de rationaliser leur gestion dans le cycle de vie des blocs

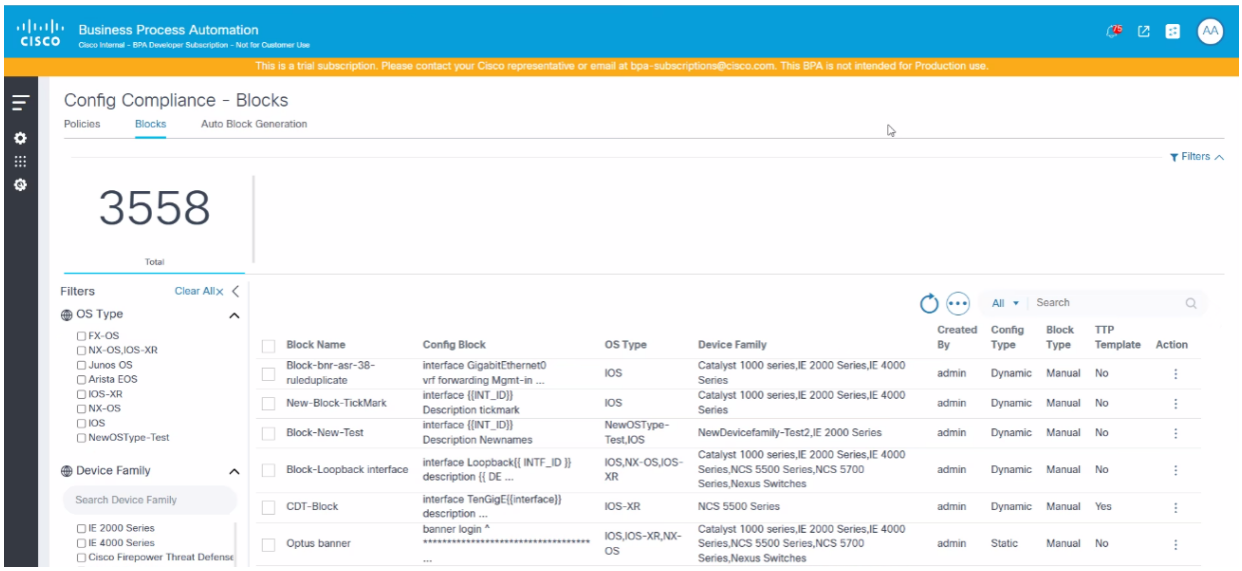
Cette intégration garantit que les contrôles de conformité sont intégrés de manière transparente dans le processus de gestion de la configuration, ce qui permet une surveillance et une gestion efficaces des configurations des périphériques par rapport à des règles prédéfinies.

Blocs de liste

La page Blocks répertorie tous les blocs de configuration et fournit des actions pour générer, ajouter, modifier, supprimer, importer et exporter des blocs. Les utilisateurs peuvent filtrer, trier et afficher les détails des blocs.

Détails du bloc de fonctionnalités

- Nombre total : Affiche le nombre total de blocs créés
- Options de filtre :
    - Types de système d'exploitation et famille de périphériques : Permet aux utilisateurs de filtrer les blocs en fonction de critères sélectionnés
- Grille principale :
    - Affiche une liste de blocs par défaut
    - Les utilisateurs peuvent trier la liste en cliquant sur les en-têtes de colonne
    - Inclut une fonction de recherche permettant aux utilisateurs de rechercher par tous les attributs ou spécifiquement par nom de bloc
    - Prise en charge de la pagination pour une navigation aisée dans la liste
- Actions:
    - Modifier : Les utilisateurs peuvent modifier les blocs existants
    - DELETE : Les utilisateurs peuvent supprimer des blocs de la liste



Liste des blocs de configuration

Ajout ou modification de blocs et de règles

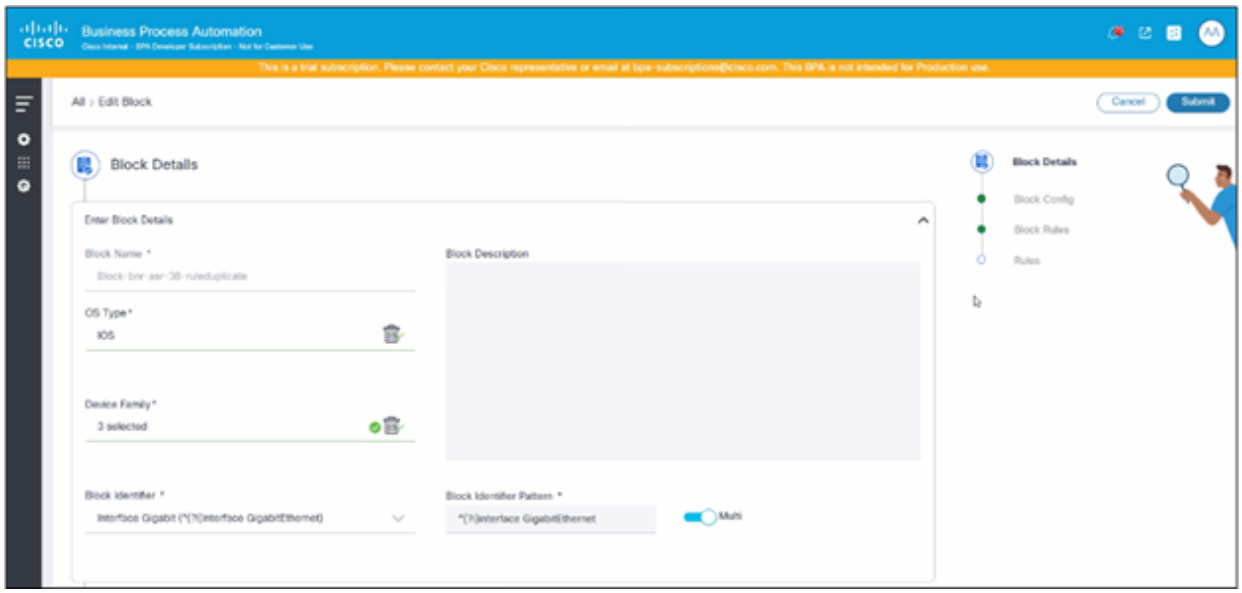
La page Ajouter ou Modifier un bloc est conçue pour capturer et gérer des informations essentielles concernant les blocs. Cette page présente les sections suivantes :

- Détails du bloc de base :

  La section Détails de base comprend :

  - Nom du bloc : Nom désigné pour le bloc
  - Description: Brève présentation ou explication de l'objectif ou de la fonctionnalité du bloc
  - Type de système d'exploitation : Type de système d'exploitation associé au bloc
  - Famille de périphériques : Catégorie ou groupe de périphériques compatibles avec le bloc
  - Sélection de l'identificateur de bloc : Options de sélection d'un identificateur unique pour le bloc
  - Ajouter ou modifier les détails d'identificateur de bloc : Si aucun identificateur de bloc approprié n'est présent, les utilisateurs peuvent utiliser les mêmes champs pour ajouter ou modifier les détails suivants de l'identificateur de bloc :

    - Nom d'identificateur de bloc : Nom spécifique donné à l'identificateur de bloc
    - Modèle : Modèle ou format suivi par l'identificateur de bloc
    - Multiples : Permet d'indiquer si le bloc de configuration doit être traité comme une configuration multiligne

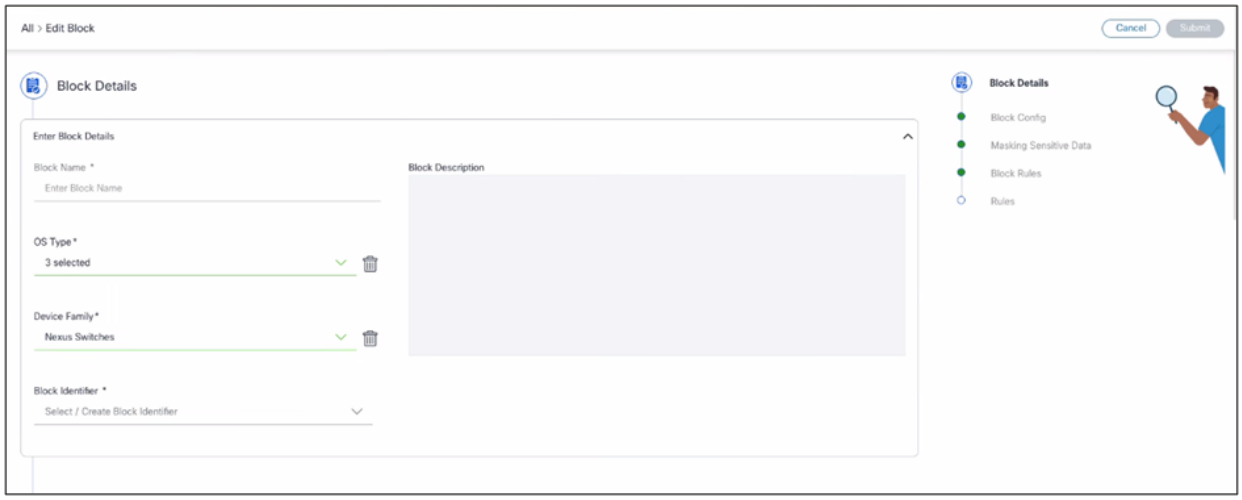


Ajouter ou modifier des blocs - Détails du bloc

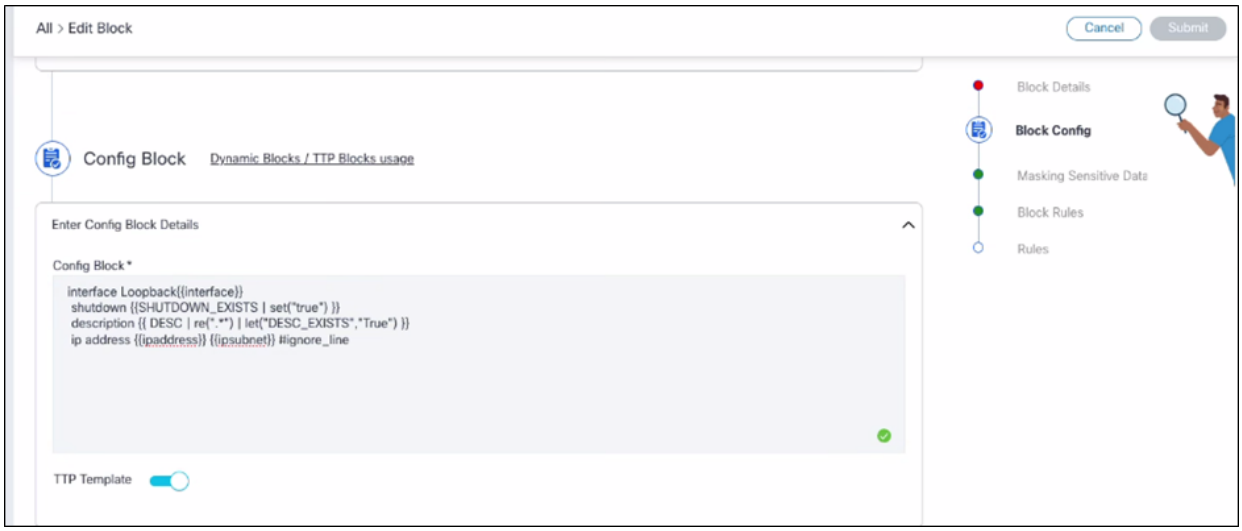
- Bloquer la configuration :

La section Block Config comprend :

- Bloc de configuration : Représente la configuration d'un périphérique, en incorporant différentes variables. Cette configuration décrit la manière dont le périphérique doit être configuré et géré dans le système.
- Modèle TTP : Indique si le bloc est désigné comme modèle de protocole de transformation de modèle (TTP), ce qui permet d'identifier les blocs utilisés comme modèles pour la transformation ou la normalisation des configurations entre les périphériques.



Détails du bloc



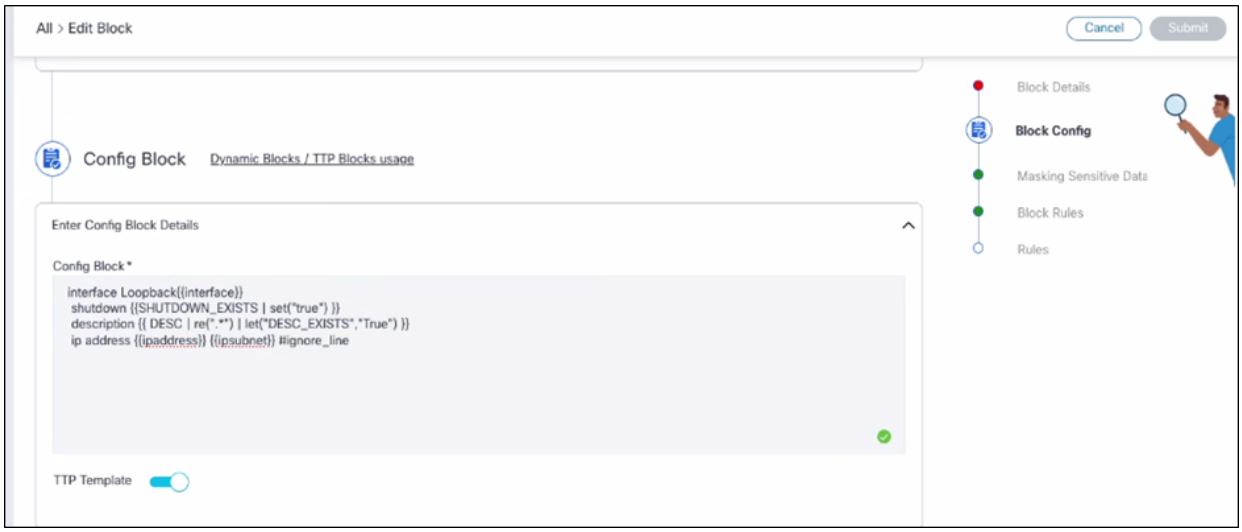
Bloquer la configuration

Utilisation de la syntaxe de ligne Ignore

La syntaxe de ligne Ignorer permet aux utilisateurs d'ajouter un commentaire à la fin d'une ligne de configuration spécifique dans un bloc pour indiquer au système d'ignorer les contrôles de conformité ou les violations sur cette ligne. Cela empêche la ligne d'apparaître comme une violation dans les rapports ou le tableau de bord.

Procédez comme suit pour utiliser Ignorer la syntaxe de ligne :

1. Localisez la ligne de configuration à exclure des contrôles de conformité (par exemple, adresse IP).



Ignorer la syntaxe de ligne

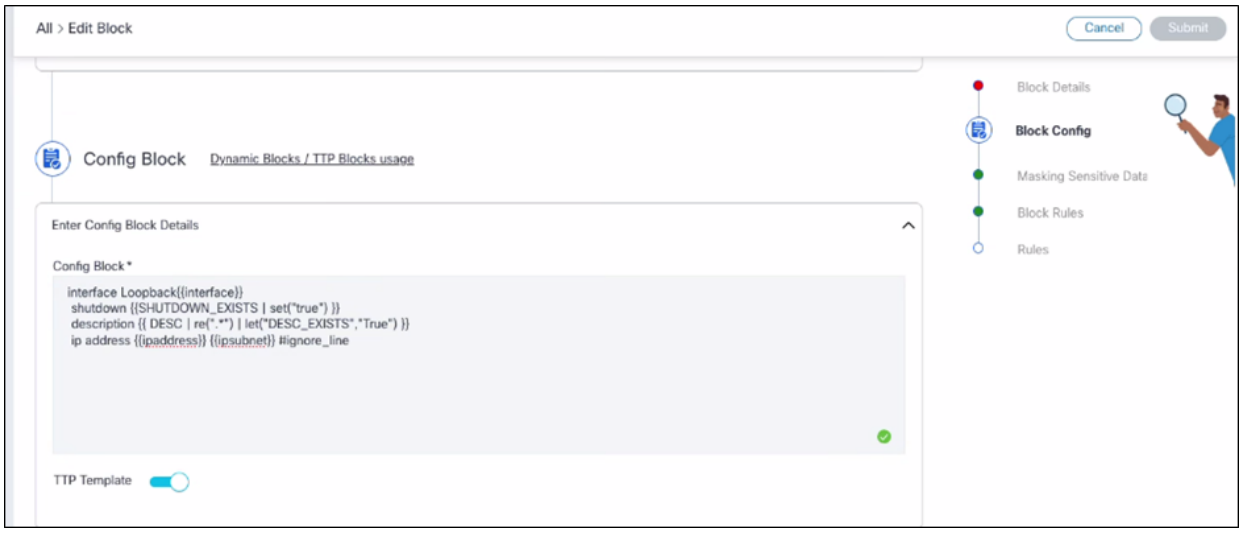
2. Ajoutez la ligne en utilisant la syntaxe de commentaire « #ignore_line » à la fin de cette ligne. Exemple : ip address {{ipAddress}} {{ipSubnet}} #ignore_line

Déclenchement D'Une Violation

Cette fonctionnalité d'analyseur de texte modèle (TTP) dans la configuration de bloc peut être utilisée pour indiquer si une violation doit être déclenchée si une ligne particulière existe.

Procédez comme suit pour utiliser la fonctionnalité TTP :

1. Dans la section Block Config de la page de création ou de modification de bloc, recherchez la ligne de configuration à contrôler.
2. Définissez une variable TCP à l'aide de la commande set ou let comme suit :
   - Si la ligne de configuration shutdown existe, utilisez la commande set pour définir une variable comme suit :
     shutdown | {{INDICATEUR_ARRÊT | set(« true »)}} »
   - Si les utilisateurs ont une variable existante dans la ligne de configuration comme description {{DESC}}, utilisez la commande let comme suit :
     description {{ DESC | re(«.*«) | let(»DESC_EXISTS», «True») }}
3. Utilisez ces variables (SHUTDOWN_FLAG ou DESC_EXISTS dans l'exemple ci-dessus) dans une règle pour déclencher des violations.



Susciter des violations

Effet :

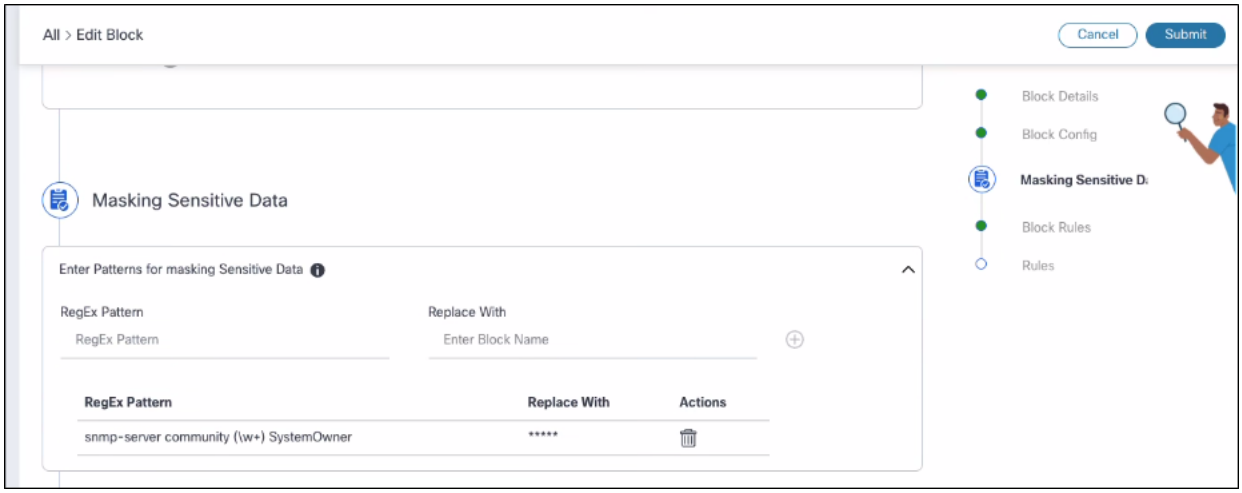
Une violation est affichée sur la page du tableau de bord si les lignes « shutdown » ou « description config » sont disponibles dans la configuration du périphérique. La gravité de la violation dépend de la sélection effectuée lors de la création de la règle.

- Masquer les données sensibles :

Les données sensibles au masque sont une fonctionnalité qui permet aux utilisateurs de définir des modèles à l'aide d'expressions régulières pour identifier et masquer des informations sensibles (telles que des mots de passe ou des clés) dans les configurations de périphériques. Cela empêche l'affichage de données sensibles dans des vues de violation ou des différences de configuration de correction en remplaçant les données correspondantes par un masque spécifié (par exemple, « *** »).

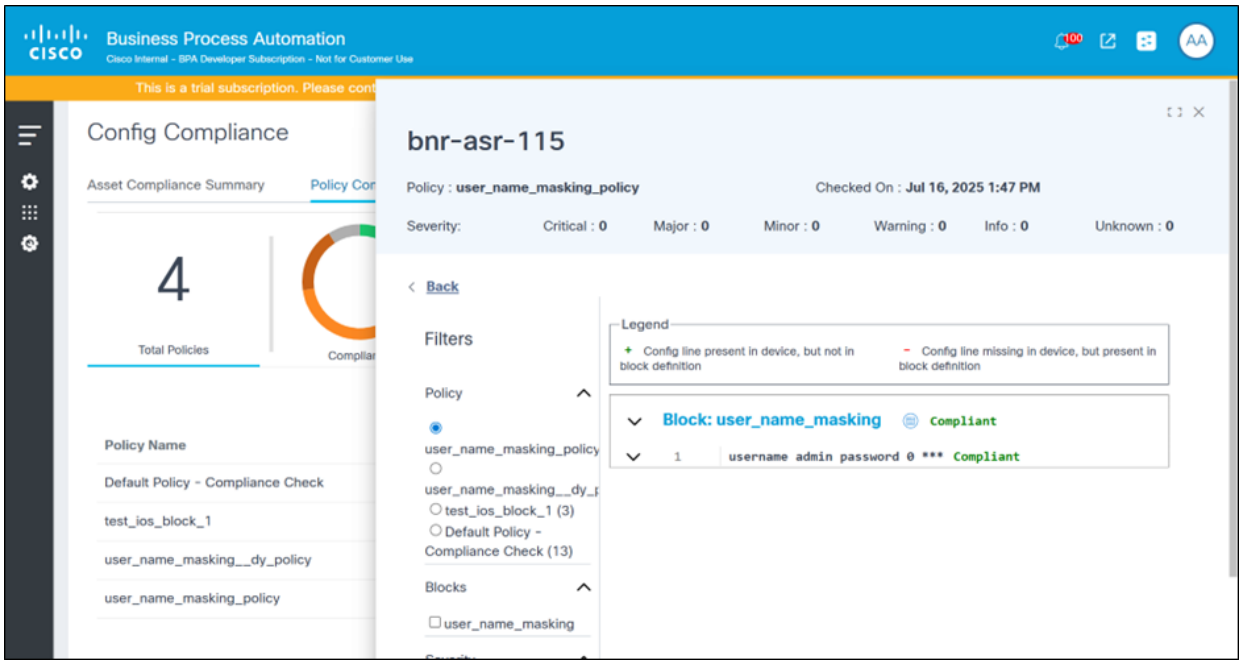
Pour masquer les données sensibles, procédez comme suit :

1. Dans la section Masquer les données sensibles :
    - Ajoutez plusieurs modèles d'expressions régulières (regex) pour identifier les données sensibles
    - Spécifiez la chaîne de remplacement pour masquer les données correspondantes (par exemple, ««) Par exemple, le modèle Regex peut être rempli avec un mot de passe (pour correspondre à tout texte commençant par « mot de passe » suivi d'un mot) et le remplacement doit être .
2. Ajoutez autant de modèles d'expressions rationnelles que nécessaire ; ils sont affichés sous forme de grille



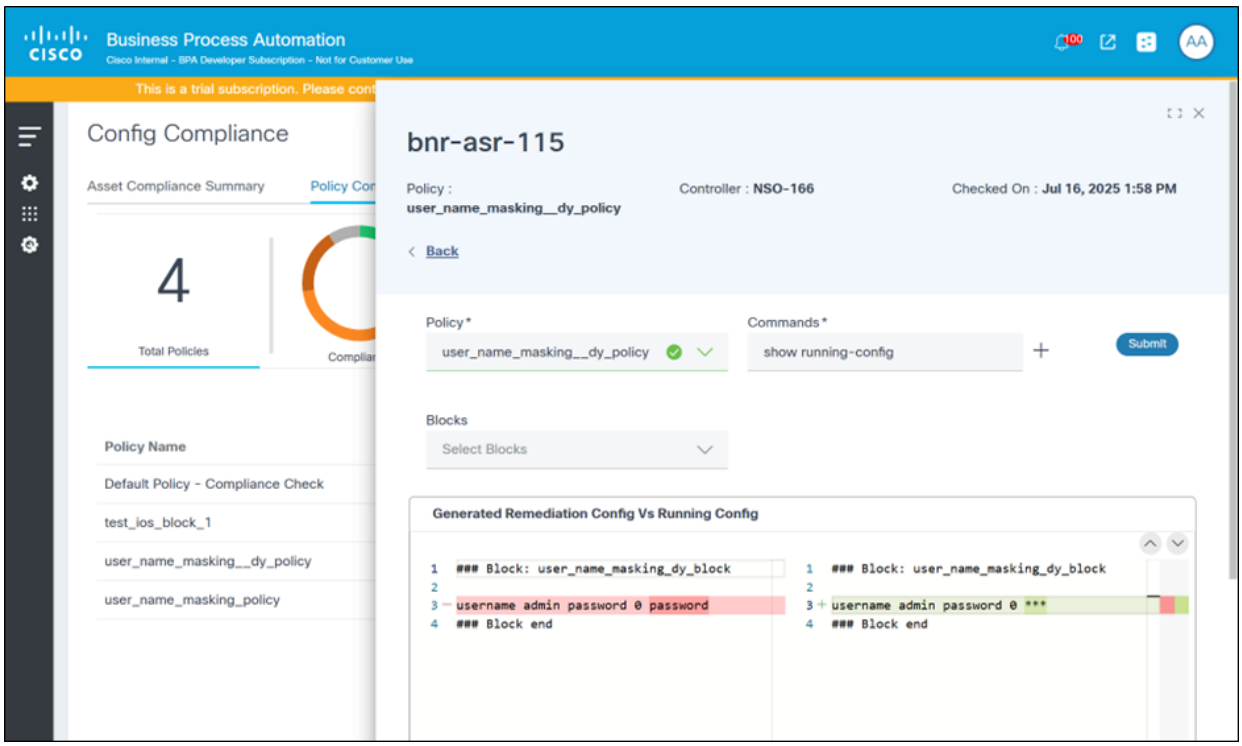
Masquer les données sensibles

3. Supprimez tout modèle de la liste s'il n'est plus nécessaire.
4. Le système utilise les expressions régulières pour rechercher les données de configuration sensibles correspondantes et les remplacer par le masque spécifié (par exemple, « *** »). Ce masquage est utilisé dans les pages suivantes :
    - Tableau de bord Conformité > Immobilisations affectées > Page Visualiser les violations : Les données de configuration affichées dans l'interface utilisateur ainsi que le rapport de conformité des ressources généré en fonction de ces détails de violation



Masquer les données sensibles dans la page Afficher les violations

- Tableau de bord Conformité > Afficher la configuration de la résolution > Page Afficher la différence de résolution : Les données de configuration du périphérique affichent les données sensibles masquées en fonction des paramètres de masque du bloc

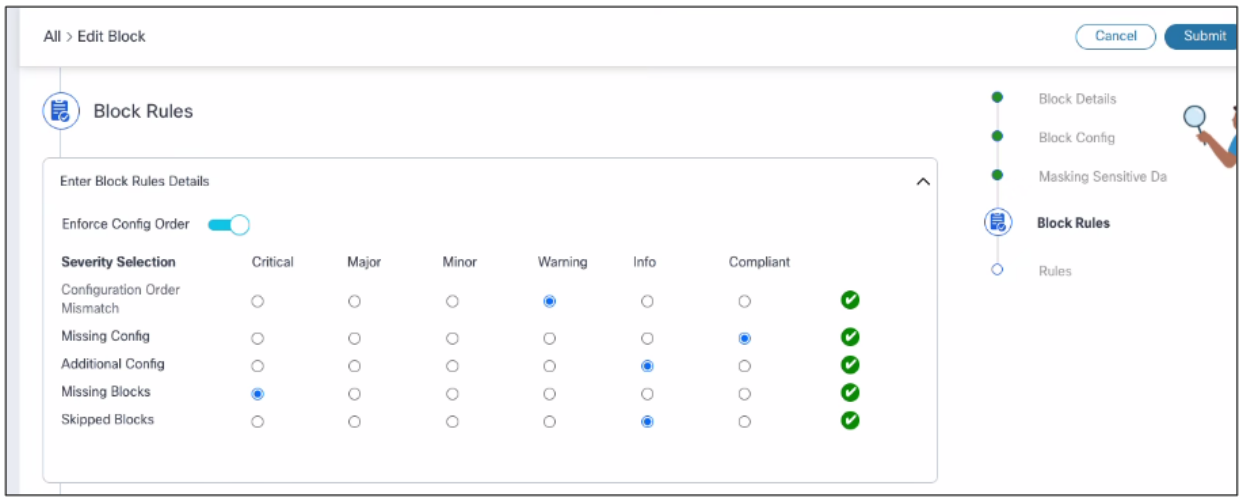


Masquer les données sensibles dans la page de différences de conversion

- Règles de blocage (sélection de la gravité) :

  La section Règles de blocage comprend :

- Appliquer l'ordre de configuration : S'assure que les lignes de configuration s'affichent dans le bon ordre lors des contrôles de conformité. Le moteur de conformité vérifie la séquence des lignes de configuration par rapport à l'ordre attendu.
- Sélection de la gravité : Permet aux utilisateurs d'attribuer un niveau de gravité aux violations au sein d'un bloc. Les niveaux de gravité permettent de hiérarchiser et de gérer efficacement les problèmes de conformité.
- Non-concordance des ordres de configuration : Identifie les écarts dans l'ordre des lignes de configuration et émet des alertes lorsque la séquence des lignes de configuration des périphériques ne correspond pas à l'ordre attendu.
- Config manquante :
  - Détecte les lignes de configuration manquantes
  - Met en évidence les lignes de configuration attendues qui sont absentes de la configuration du périphérique
  - Vérifie si le bloc de configuration de périphérique complet est manquant ou ne correspond pas à la configuration de bloc définie
- Configuration supplémentaire :
  - Identifie les lignes de configuration inattendues
  - Affiche les lignes de configuration présentes dans la configuration du périphérique mais non attendues selon la configuration de bloc
- Blocs ignorés :
  - Indique les blocs de configuration non vérifiés
  - Le bloc est ignoré s'il ne remplit pas les conditions de filtre spécifiées



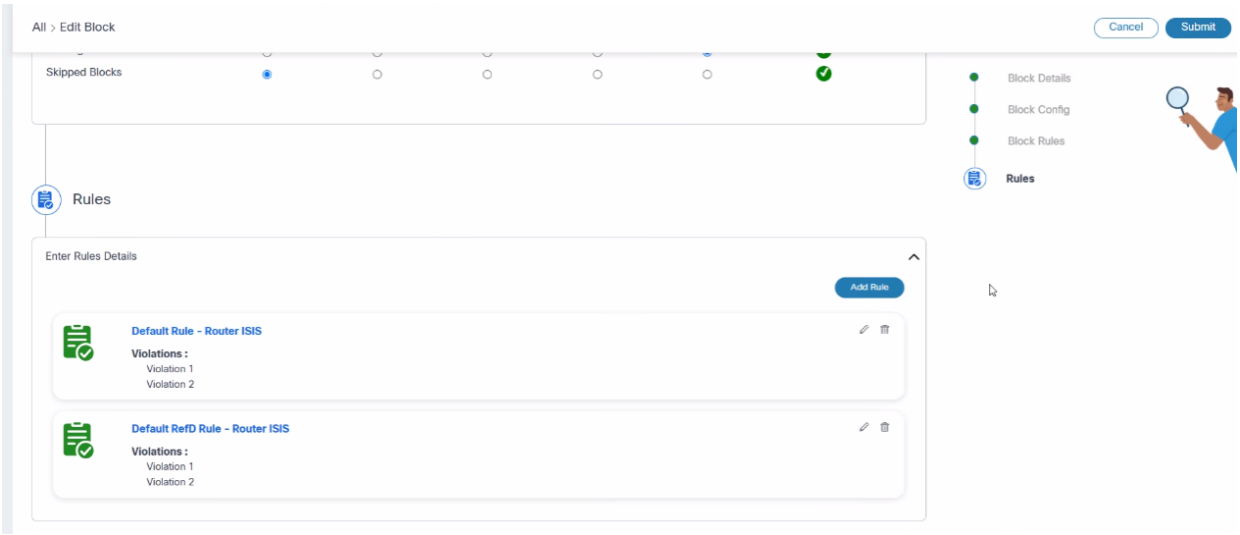
Ajouter ou modifier des blocs-Règles de bloc

Gestion des règles

Dans l'infrastructure CnR, les utilisateurs peuvent gérer les règles de blocage via l'interface « Ajouter ou modifier des blocs ». Cette fonctionnalité est structurée comme indiqué dans la section ci-dessous :

Remarque : Si un utilisateur ne souhaite pas déclencher une violation de niveau de bloc spécifique, le niveau de gravité « Conforme » peut être sélectionné.

- Configuration des règles :
  - Les utilisateurs peuvent configurer et gérer des règles que le moteur de conformité utilise pour valider les configurations
  - Les utilisateurs peuvent créer, modifier ou supprimer des règles selon leurs besoins
- Liste des règles :
  - Fournit une liste complète de toutes les règles créées, offrant une visibilité sur leurs détails
  - Les utilisateurs peuvent modifier des règles existantes ou supprimer les règles qui ne sont plus nécessaires



Ajout et modification de blocs de configuration

Ajouter ou modifier des détails de règle

- Nom de la règle :
  - Attribuer un nom unique à la règle pour l'identification
  - Ce champ est obligatoire pour garantir que chaque règle peut être reconnue distinctement
- Règle par défaut :
  - Spécifier si la règle doit être définie comme règle par défaut
  - Les utilisateurs peuvent activer ce paramètre pour que la règle devienne une valeur par défaut dans l'infrastructure de conformité
- Description:
  - Fournit un contexte ou des informations supplémentaires sur la règle
  - Ce champ est facultatif, mais peut s'avérer utile pour la documentation et la clarté
- Violations :
  - Gérer la liste des violations associées à la règle

- Les utilisateurs peuvent ajouter, modifier ou supprimer des violations selon leurs besoins

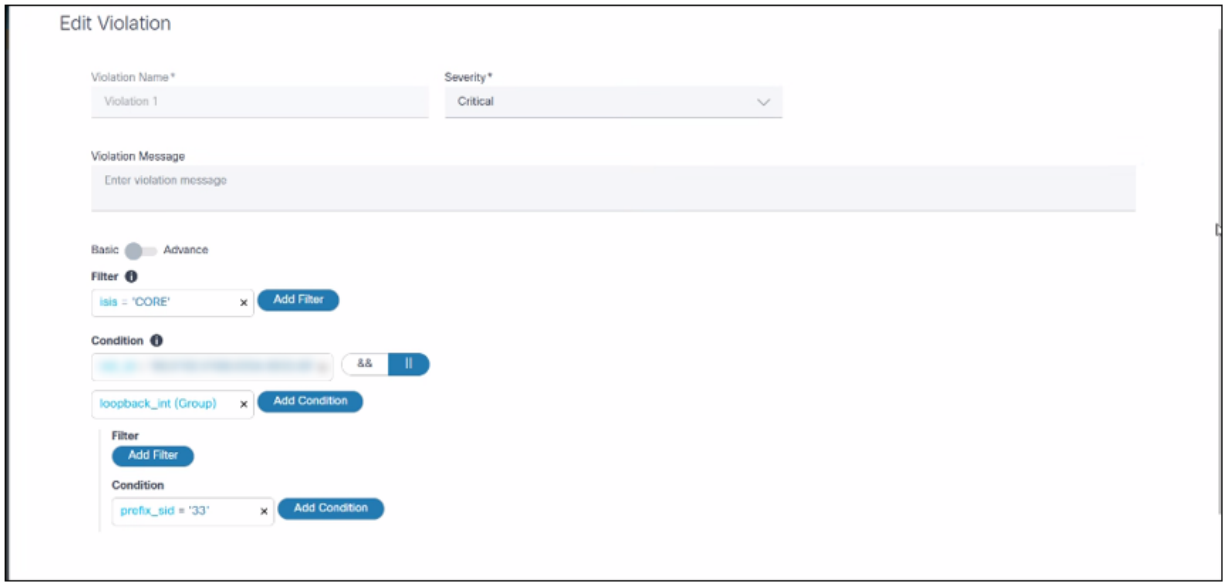
	A	B	C	D	E	F	G	H	I	J	K
1	Device Name	Managed By	Product Family	Compliance	Critical	Major	Minor	Warning	Info	Unknown	Last Checked
2	CNC-bnr-asr-78	Direct-To-Device	IE 2000 Series	Non Compliant	1	0	0	0	0	0	04-Aug-25
3	D2d-118	Direct-To-Device	IE 2000 Series	Partially Compliant	0	1	0	1	1	0	04-Aug-25
4	D2d-juniper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

Ajouter ou modifier des blocs-règles : Ajouter ou modifier une règle

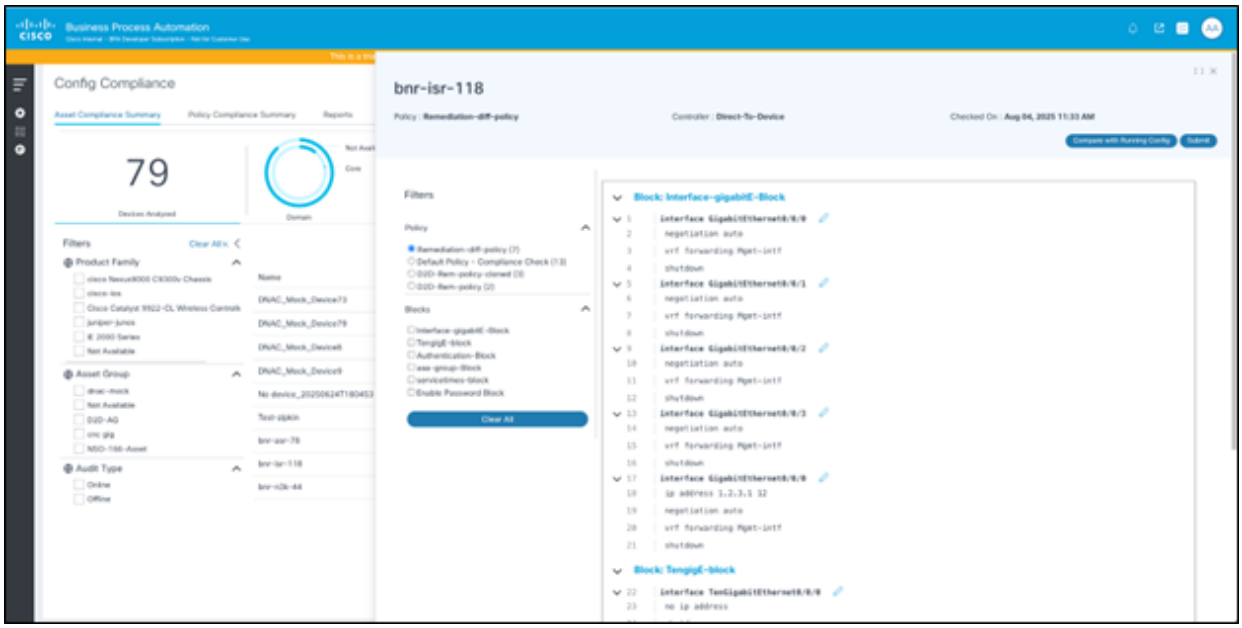
Ajout ou modification de violations de règle

Les violations de règle sont un composant critique de l'exécution de la conformité. Elles détaillent les contrôles spécifiques à effectuer. Vous trouverez ci-dessous un aperçu de la manière dont les violations de règles peuvent être créées et gérées :

- Mode de base :
  - Éléments de l'interface utilisateur : Ce mode permet aux utilisateurs de créer des violations de règle à l'aide d'une interface utilisateur graphique (GUI). Cette approche est généralement plus conviviale et plus accessible pour ceux qui préfèrent ne pas s'engager dans le codage.
  - Conseils étape par étape : Les utilisateurs sont guidés tout au long du processus de définition des vérifications à l'aide d'éléments d'interface utilisateur prédéfinis.
- Mode avancé :
  - Format de code de type JSON : Pour les utilisateurs qui sont à l'aise avec le codage, ce mode permet la création de violations de règles en les tapant dans un format structuré, semblable à JSON.
  - Flexibilité et précision : Cette méthode offre plus de souplesse et de précision pour définir des contrôles de règles complexes.



Créer ou modifier des violations de règle - Mode de base



Créer ou modifier des violations de règle - Mode avancé

Les violations de règle sont décrites dans les sections suivantes :

- Nom de la violation : Nom de la violation
- Gravité : Définit la gravité de conformité si cette violation échoue pendant une exécution
- Message de violation : Le message s'affiche lorsqu'une vérification de violation échoue
- Critères de filtre de violation : Applique les conditions de violation dans lesquelles des variables de schéma autres que des groupes peuvent être utilisées
  - Utilisé dans les critères de filtre pour définir des conditions basées sur des éléments de données individuels qui ne font pas partie d'un groupe
  - Permet aux utilisateurs de sélectionner des critères en fonction de la hiérarchie et de la structure des données, assurant ainsi un filtrage précis et pertinent

- Conditions des règles : Conditions réelles de vérification de la conformité dans lesquelles les variables de schéma de groupe et non-groupe peuvent être utilisées
  - Les deux types de variables sont utilisés dans les règles pour créer des conditions globales
  - Variables de groupe : Autoriser l'application de conditions aux collectes de données connexes, en assurant des contrôles approfondis au sein des groupes structurés
  - Variables non-groupe : Autoriser l'application de conditions aux éléments de données indépendants, ce qui offre une certaine souplesse dans l'application des règles

Blocs définis par l'utilisateur dynamiques - Meilleures pratiques

- Assurez-vous que les noms de variable sont uniques dans chaque bloc.
- Évitez d'utiliser des variables dans les noms de groupe.
- Pour les configurations de sous-hiérarchie, utilisez « **<group>** » dans les blocs.

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

- Pour capturer des valeurs pour des lignes de configuration similaires dans une seule variable, utilisez la variable comme suit : `{{ <<nom_var>> ligne | | jointmatches(',') }}`. Placez la ligne de configuration entre `{{ start }}` et `{{ end }}` comme indiqué dans l'exemple suivant :

Configuration du périphérique	Bloquer la configuration
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 {{ domaines | _ligne_ | joinmatches(‘,’) }} {{ _end_ }} ip domain list vrf {{ vrf_name }} {{ vrf_domain }}

- Pour capturer une valeur qui contient des espaces à partir d'une ligne de configuration, utilisez la variable du bloc comme indiqué dans le tableau ci-dessous : `{{ <<nom_var>> | re(".*") }}`

Configuration du périphérique	Bloquer la configuration
interface HundredGigE0/0/1/31	interface {{ INTF_ID }}

Configuration du périphérique	Bloquer la configuration
description Interface : 12ylaa01 Hg0/0/1/31 mtu 9216	description {{ INTF_DESC | re(«.*«) }} mtu 9216

Présentation de la hiérarchie des règles et de l'intégration RefD dans les règles et les règles non RefD

Le protocole TTP de bloc dynamique comporte deux schémas distincts qui déterminent la manière dont les configurations sont structurées et validées.

- Schéma basé sur les groupes :
  - Ce schéma organise les configurations de manière hiérarchique, en établissant une relation parent-enfant entre les éléments
  - Idéal pour les configurations complexes où les éléments sont logiquement imbriqués et interconnectés
  - Des règles peuvent être définies pour valider les relations hiérarchiques et les dépendances entre les différents éléments de configuration
- Schéma non basé sur un groupe :
  - Les configurations sont structurées de manière linéaire, tous les éléments existant au même niveau sans relation hiérarchique
  - Convient pour des configurations plus simples où la hiérarchie n'est pas nécessaire
  - Des règles peuvent être définies pour garantir que chaque élément de configuration répond à des critères spécifiques

Intégration RefD

- Objectif de la référence :
  - Rôle : Sert d'outil de gestion des variables locales et externes dans le cadre BPA
  - Fonctionnalité :
    - Récupération dynamique : Facilite la récupération et la gestion dynamiques des données variables, ce qui permet aux contrôles de conformité de s'adapter aux modifications des données en temps réel
    - Interaction API : Propose des API pour les cas d'utilisation BPA afin d'accéder et de gérer ces variables et valeurs dynamiques, garantissant une intégration en douceur dans les workflows de conformité

Syntaxe des valeurs de règle de conformité

L'exemple d'utilisation CnR s'intègre à l'infrastructure RefD pour utiliser dynamiquement les données dans les processus de vérification de la conformité et de correction. Une description

détaillée du fonctionnement de cette intégration, notamment en ce qui concerne la syntaxe et les types de variables utilisés, est présentée ci-dessous :

- Mot clé: La syntaxe doit commencer par « RefD »
- Paramètres : Le paramètre « key » est obligatoire dans la syntaxe
- Exemple :

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

Types de variables

- Variables définies par l'utilisateur :
  - Configuré lors de la création des tâches de conformité.
  - Étendue : Applicable à toutes les exécutions pour le travail spécifié
  - Syntaxe: `{$VarName}`
  - Exemple : `{$SITE}`
- Variables système
  - Prédéfini par le framework en fonction des données contextuelles disponibles lors de l'exécution
  - Actuellement, le cadre fournit un accès à l'objet périphérique
  - Syntaxe: `{#VarName}}`
  - Exemples:
    - `{{#device.deviceIdentifier}}` - Représente l'identificateur de périphérique
    - `{{#device.additionalAttributes.serialNumber}}` - Représente le numéro de série du périphérique
- Variables TTP
  - Présente dans la configuration de bloc
  - Syntaxe: `{{ NomVar }}`
  - Exemple : `{{ INT_ID }}`

Règles non-RefD

- Ces règles sont semblables aux règles RefD, mais ne commencent pas par le mot clé « RefD »
- Exemple :

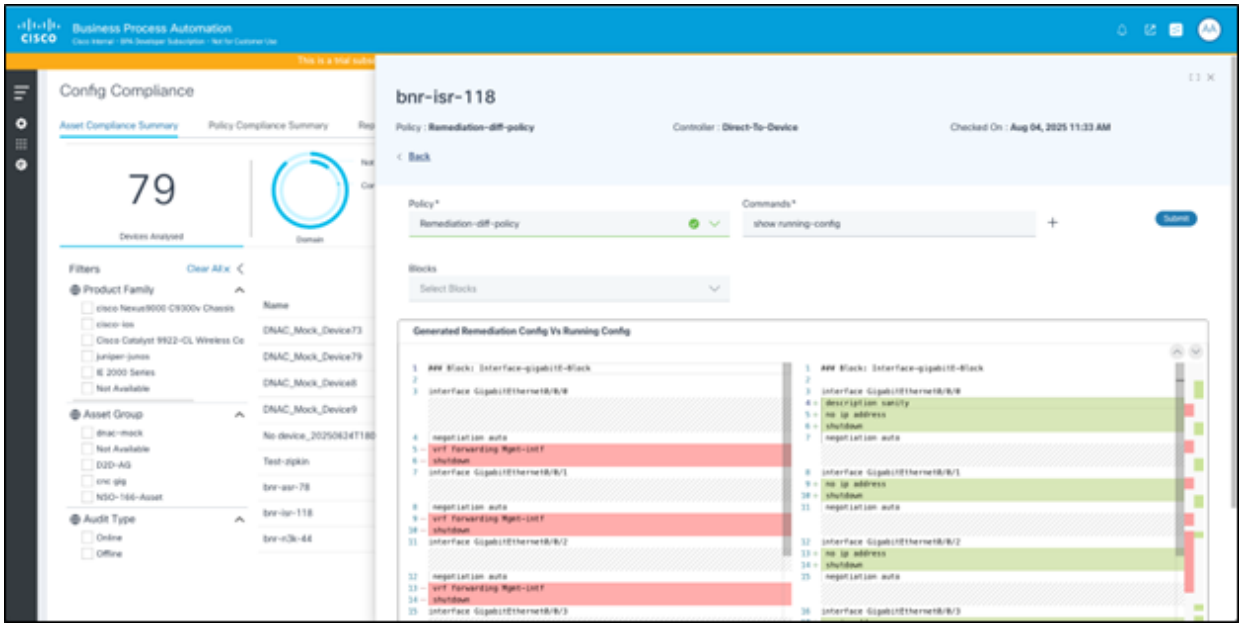
```
plaintext
Copy Code
{$int_id}.{{#device}}.{{ mtu_val }}
```

Utilisation variable

- Variables définies par l'utilisateur : Représenté par `{$Var}`
- Variables système : Représenté sous la forme `{{#Var}}`, exposant des attributs tels que deviceIdentifier, controllerId, controllerType, etc.
- Variables TTP : Représenté entre doubles accolades par `{{var}}`

Exécution

- Lors de la création d'une tâche, leurs valeurs peuvent être définies si des variables $ sont spécifiées
- Les valeurs combinées des variables sont comparées à la configuration de dispositif extraite pour assurer la conformité



Configuration de périphériques

	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						

Règles de configuration : RéfD

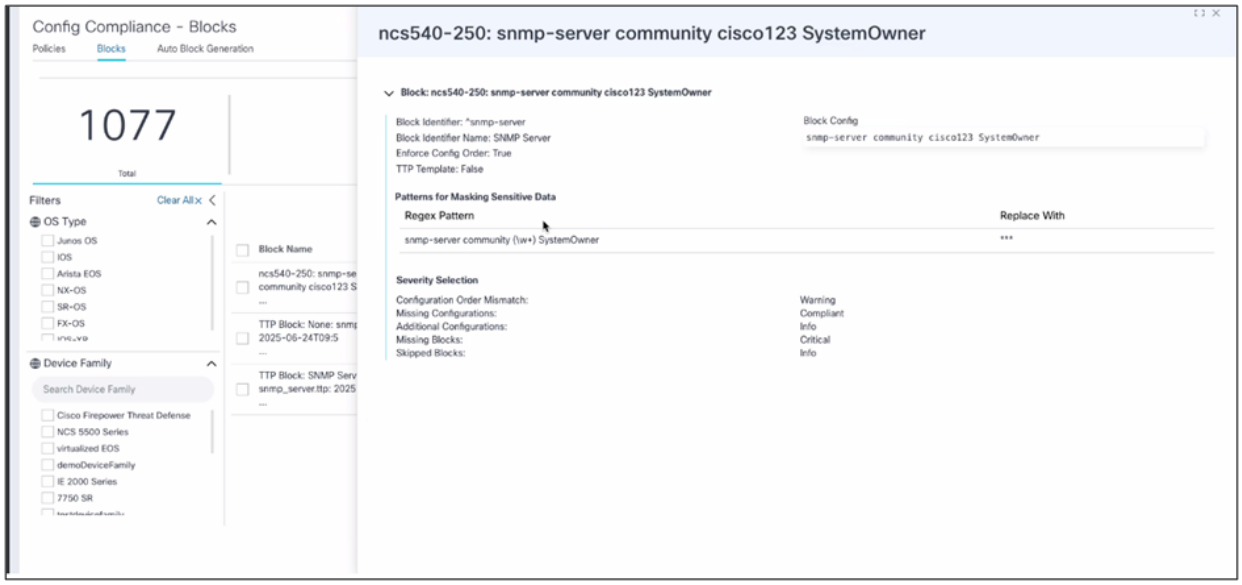
Afficher les détails du bloc

Pour accéder aux détails du bloc :

1. Accédez à la page Blocks.
2. Sélectionnez ou cliquez sur la ligne dans la grille pour afficher les détails du bloc spécifique.La page Détails du bloc s'affiche sur le côté droit de l'écran.

Remarque : Cette page fournit une vue en lecture seule de toutes les informations relatives au bloc, y compris les blocs associés, les règles et les violations éventuelles.

Si vous cliquez sur des liens hypertexte dans les détails, les utilisateurs sont redirigés vers le bloc approprié ou vers des informations connexes.



Vue Détails du bloc

Suppression de blocs

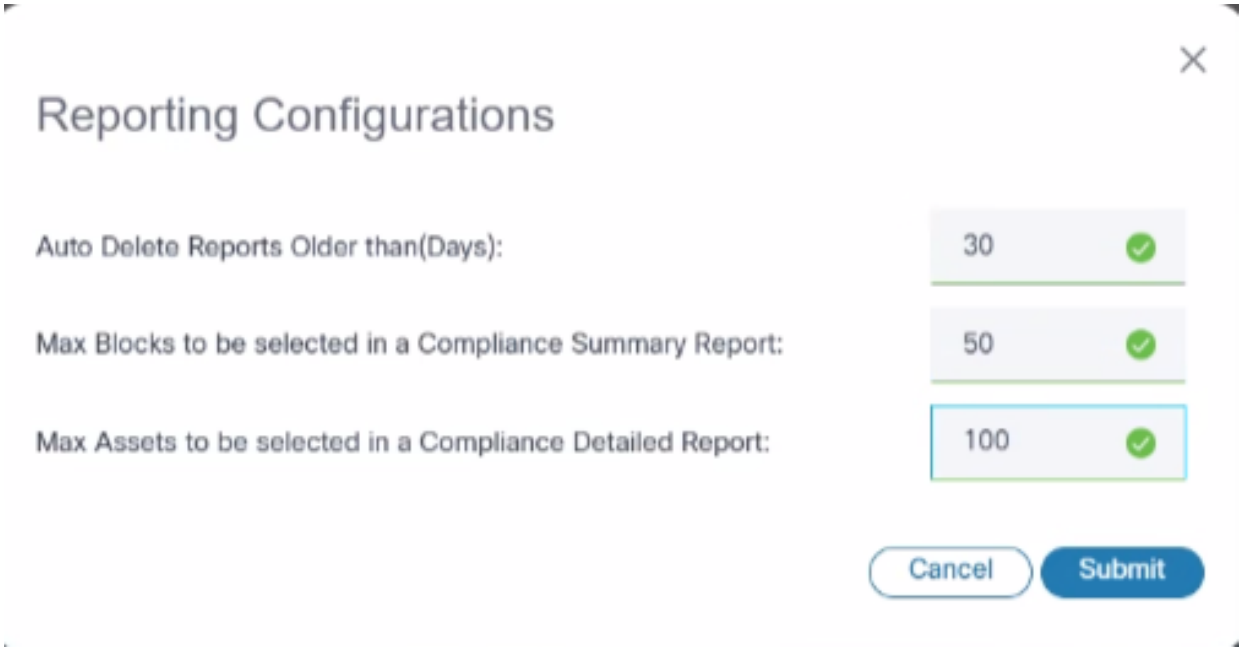
Le portail permet aux utilisateurs de supprimer un ou plusieurs blocs, à condition qu'ils disposent des autorisations RBAC appropriées. Les utilisateurs peuvent effectuer ces actions en procédant comme suit :

Pour la suppression d'un seul bloc :

1. Accédez à la page Blocks.
2. Cliquez sur l'icône Plus d'options en regard du bloc à supprimer.
3. Sélectionnez l'option Supprimer. Un message de confirmation s'affiche.

Pour la suppression de blocs multiples :

1. Accédez à la page Blocks.
2. Cochez les cases en regard de chaque bloc à supprimer.
3. Cliquez sur l'icône Autres options et sélectionnez Supprimer. Un message de confirmation.

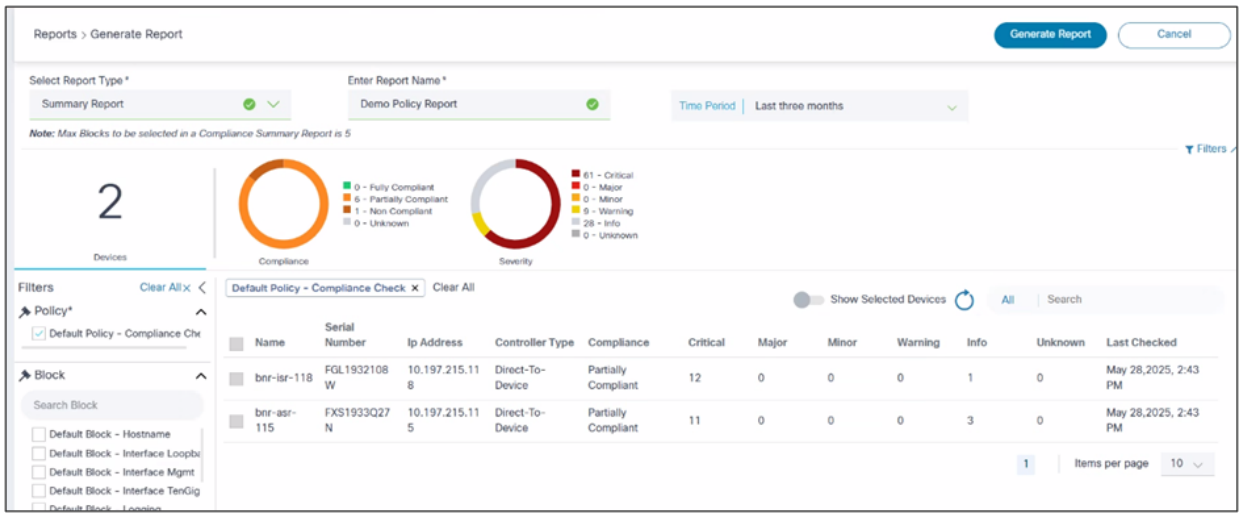


Supprimer le bloc

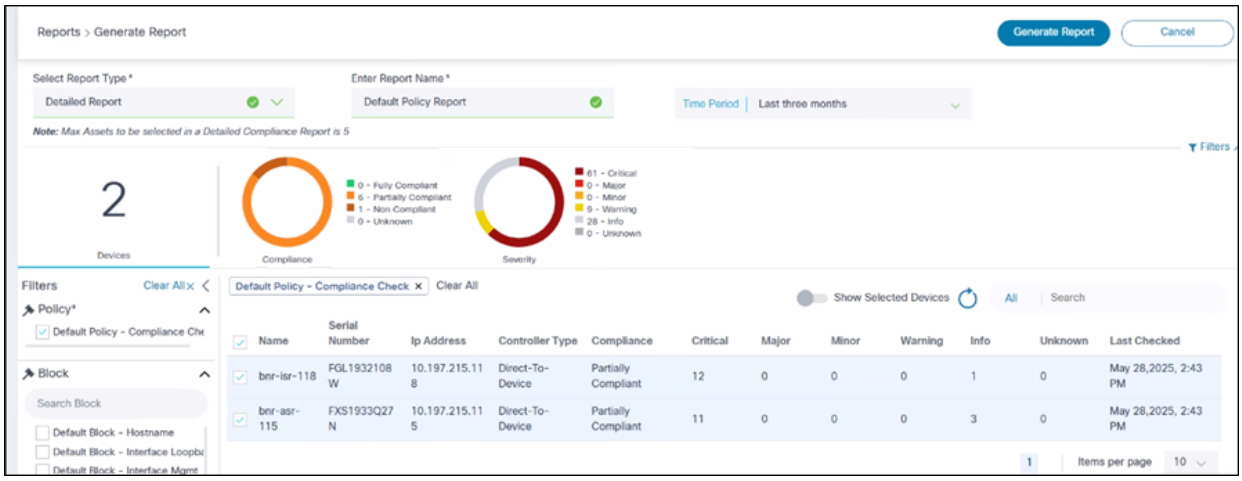
Configuration: Génération automatique de blocs

La génération de blocs permet aux utilisateurs de créer automatiquement des blocs en fonction de la configuration d'un périphérique. Cette automatisation réduit le temps et les efforts nécessaires à la création manuelle et permet aux utilisateurs de modifier plus facilement les blocs en ajoutant ou en supprimant des variables, plutôt qu'en repartant de zéro.

Cliquez sur une ligne pour afficher les détails de la génération de blocs.

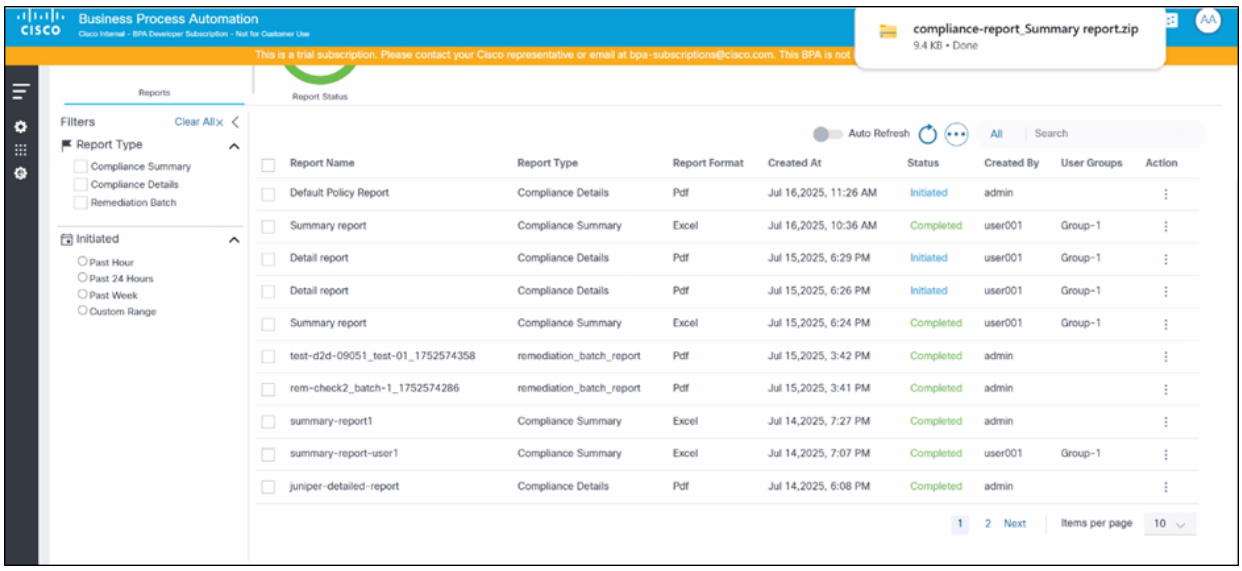


Liste de génération automatique de blocs - Affichage



Génération automatique de blocs - Détails

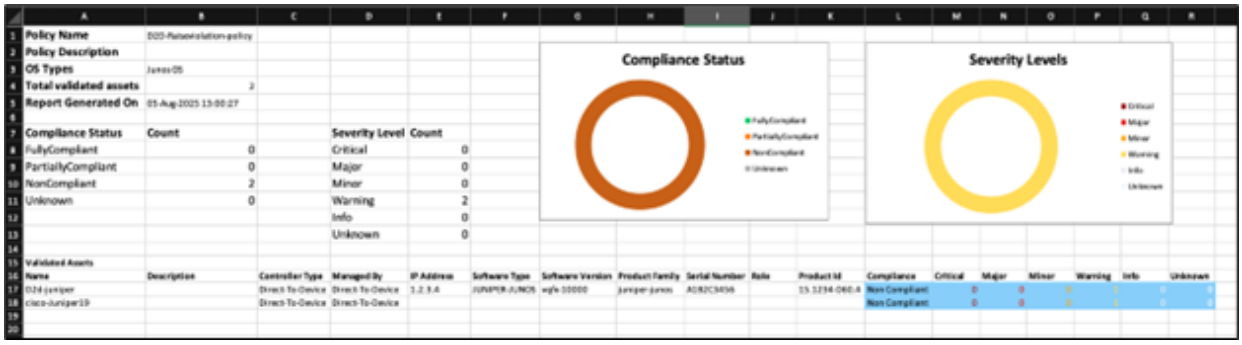
Génération automatique de blocs



Liste de génération de bloc automatique

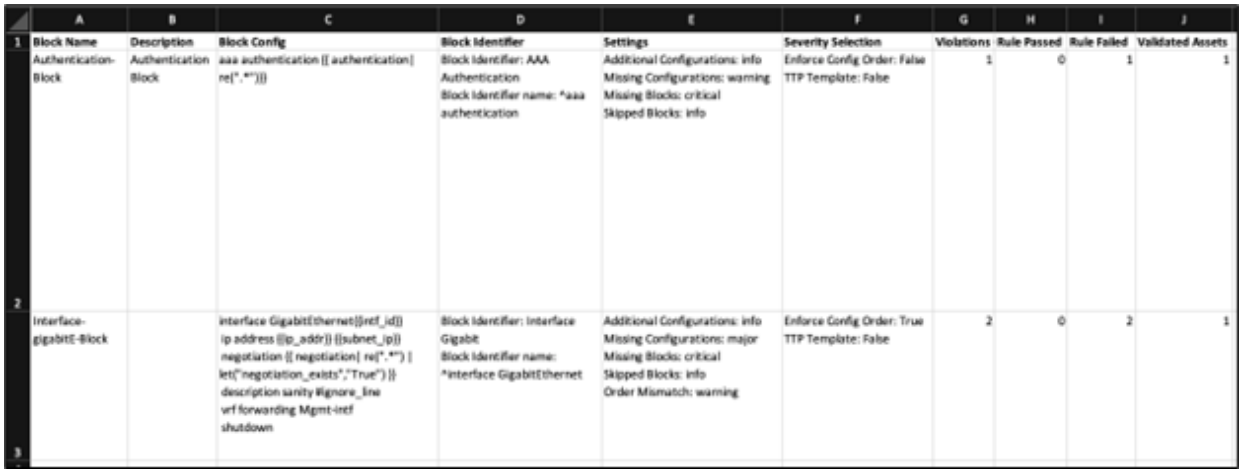
La page Génération automatique de blocs comporte les champs suivants :

- Générer à partir de : Source à partir de laquelle les blocs sont générés. Il propose les trois options suivantes :
    - Sauvegarde de configuration de périphérique : Le système choisit une configuration de périphérique dans l'exemple d'utilisation de sauvegarde



Sauvegarde de configuration de périphérique

- Téléchargement de fichier : Une fenêtre Téléchargement de fichier s'ouvre pour que les utilisateurs téléchargent la configuration du périphérique



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

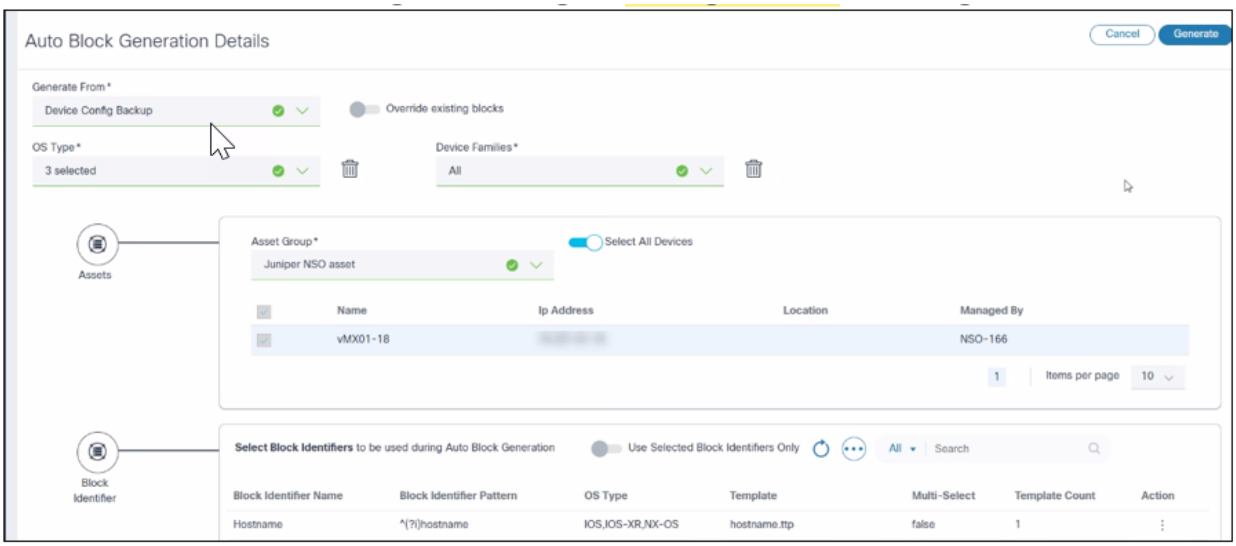
Téléchargement de fichier

- Configuration actuelle : Entrez la commande de configuration CLI que le système utilise pour récupérer la configuration du périphérique.

	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							

Configuration actuelle

- Type de système d'exploitation : Liste des types de système d'exploitation pour lesquels ce bloc est pertinent.
- Famille de périphériques : Liste des familles de périphériques pour lesquelles ce bloc est pertinent.
- Ressources : La fonction Actifs offre une approche structurée de la sélection des périphériques pour la génération de blocs dynamiques
    - Sélection du groupe d'équipements :
        - Permet aux utilisateurs de choisir un groupe prédéfini de périphériques, appelé groupe d'actifs, qui est utilisé pour générer des blocs dynamiques
        - Facilite la gestion et l'organisation des périphériques en les regroupant en fonction de critères spécifiques, tels que l'emplacement, le type ou la fonction
    - Sélection du périphérique de sous-ensemble :
        - Les utilisateurs ont la possibilité de sélectionner un sous-ensemble spécifique de périphériques au sein du groupe de ressources choisi
        - Permet aux utilisateurs de se concentrer sur un segment particulier de périphériques, ce qui permet une génération et une gestion de blocs plus ciblées



Génération de blocs

- Identificateur de bloc : Permet aux utilisateurs de sélectionner la liste des identificateurs de bloc utilisés lors de la génération de bloc. Il fournit également des fonctionnalités de gestion des identificateurs de bloc en ligne.

Identificateur de bloc

Un identificateur de bloc utilise CiscoConfParser pour extraire un bloc de configuration de la configuration complète du périphérique. Chaque identificateur de bloc doit être associé à un modèle d'expression régulière. Les utilisateurs peuvent créer leurs propres identificateurs de bloc ou mettre à jour les identificateurs de bloc existants à l'aide de l'interface utilisateur ou de l'API. La plate-forme fournit actuellement entre 55 et 60 identificateurs de bloc par défaut. Chaque identificateur est unique à un type de système d'exploitation et est chargé pendant le déploiement de l'application BPA via le service Ingester. Un modèle TCP peut être associé à chaque identificateur de bloc. Le nom et le modèle d'un identificateur de bloc doivent être uniques.

Si l'option Multi est activée pour l'identificateur de bloc, le cadre de conformité génère plusieurs blocs de configuration à partir des configurations correspondantes. Sinon, il traite toutes les configurations correspondantes comme un seul bloc.

Exemples d'identificateurs de bloc avec l'option Multi True : interface, routeur bgp, vrf, l2vpn, etc.

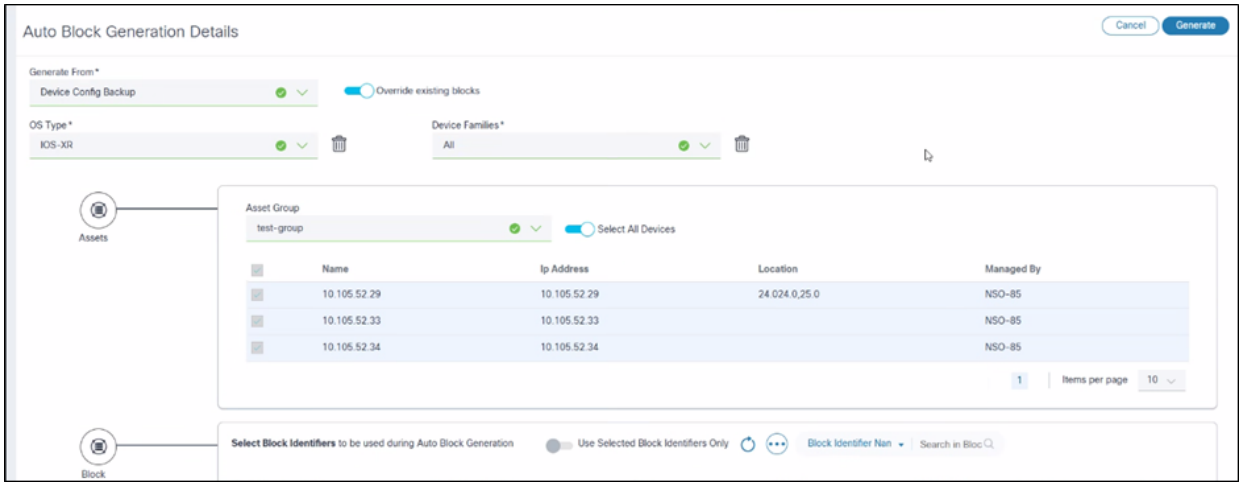
Exemples d'identificateurs de bloc avec l'option Multi False : logging, snmp-server, domain, etc.

Exemples:

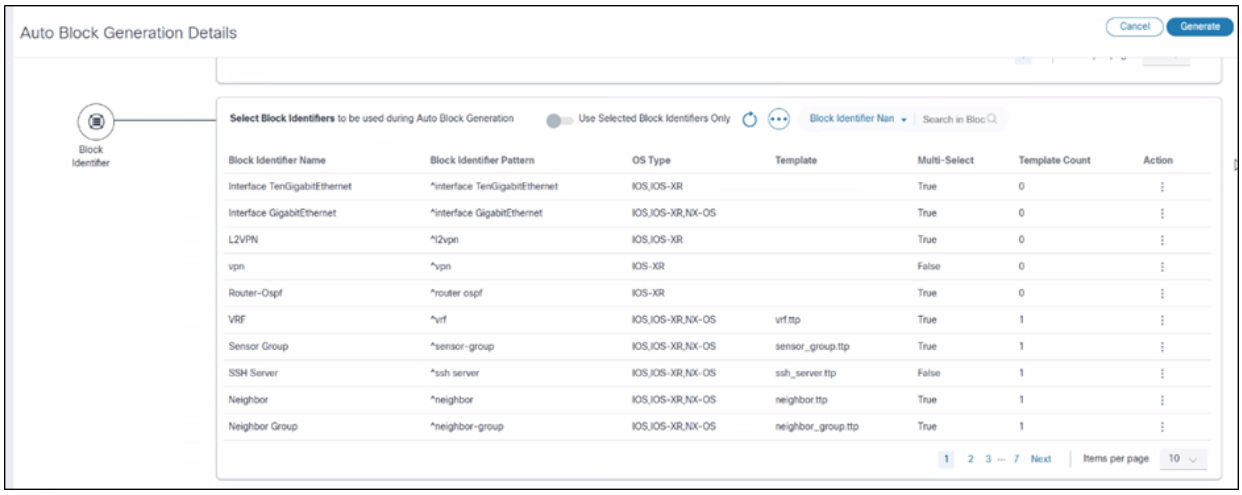
```
{
  “name”: “BundleEthernet Interface”,
  “osType”: [“IOS”, “IOS-XR”, “NX-OS”],
  “multi”: true,
  “blockIdentifier”: “^(?i)interface Bundle-Ether”,
  “templates”: [“parent_interface.ttp”]
}

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

Identificateur de bloc de liste

List Block Identifier permet aux utilisateurs d'afficher la liste des identificateurs de bloc ainsi que les fonctions de recherche et de tri. Cette fonction est disponible dans la page Générer des blocs.

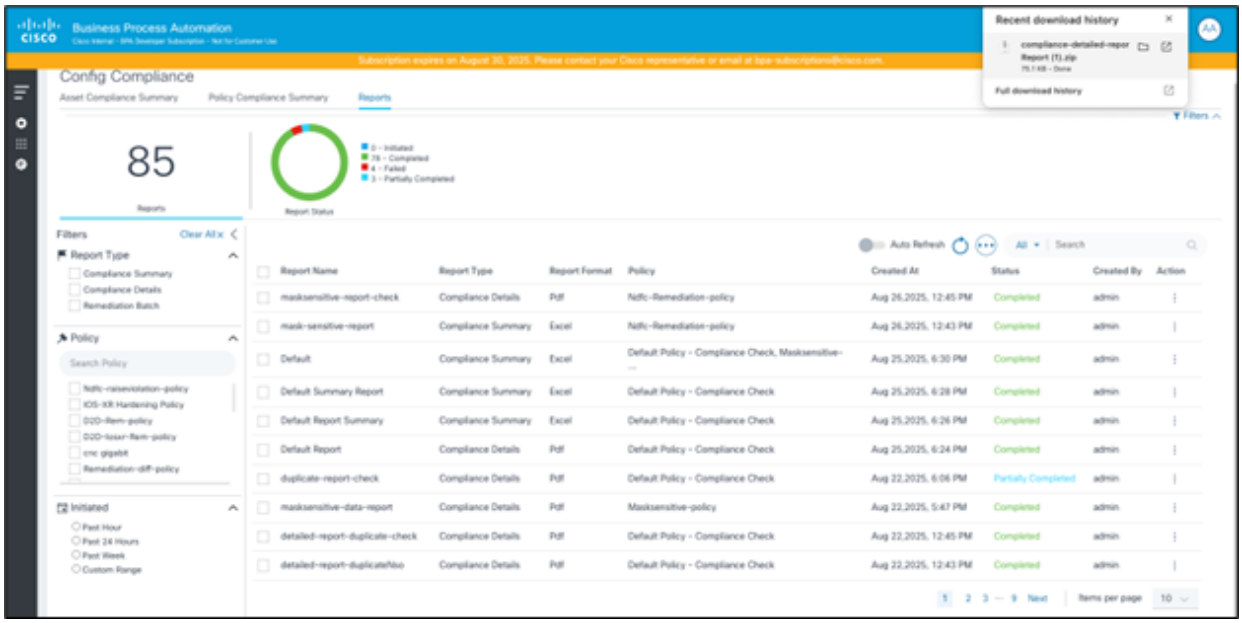


Liste des identificateurs de bloc



Identificateur de bloc

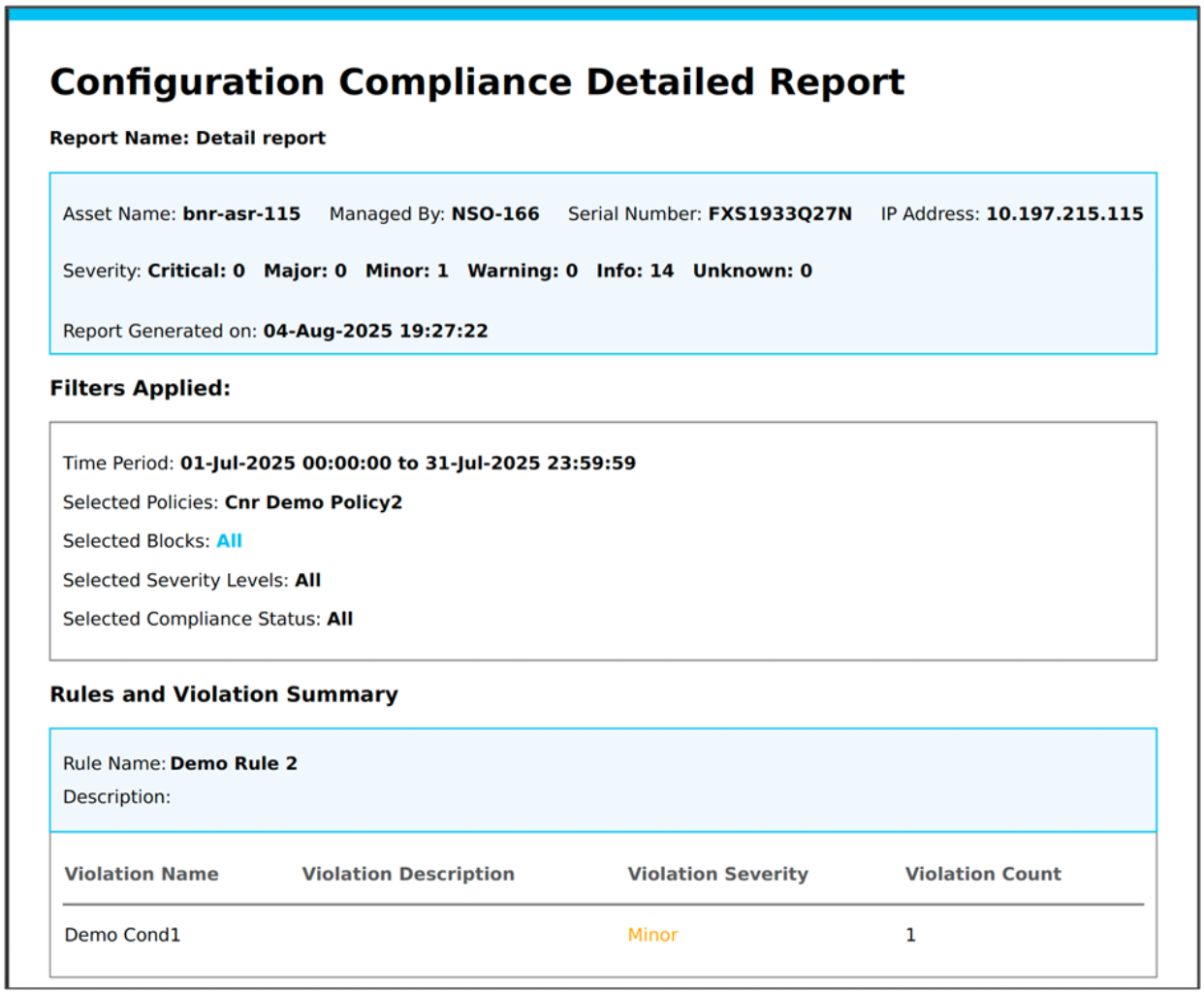
Créer ou modifier un identificateur de bloc



Modifier l'identificateur de bloc

La section Liste d'identificateurs de bloc de la page Génération automatique de blocs fournit aux utilisateurs les outils nécessaires pour gérer efficacement les identificateurs de bloc. Les fonctionnalités sont répertoriées ci-dessous :

- Créer des identificateurs de bloc
  - Les utilisateurs peuvent ajouter de nouveaux identificateurs de bloc à la liste
  - Cela permet l'introduction d'identificateurs uniques qui peuvent être utilisés pour organiser et différencier les blocs
- Modifier les identificateurs de bloc
  - Les identificateurs de bloc existants peuvent être modifiés
  - Permet des mises à jour ou des corrections des identificateurs, en s'assurant qu'ils restent précis et pertinents pour les blocs qu'ils représentent
- Supprimer l'identificateur de bloc
  - Les utilisateurs ont la possibilité de supprimer les identificateurs de bloc de la liste
  - Facilite la gestion des identificateurs en permettant la suppression de ceux qui ne sont plus nécessaires ou applicables



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

Supprimer l'identificateur de bloc

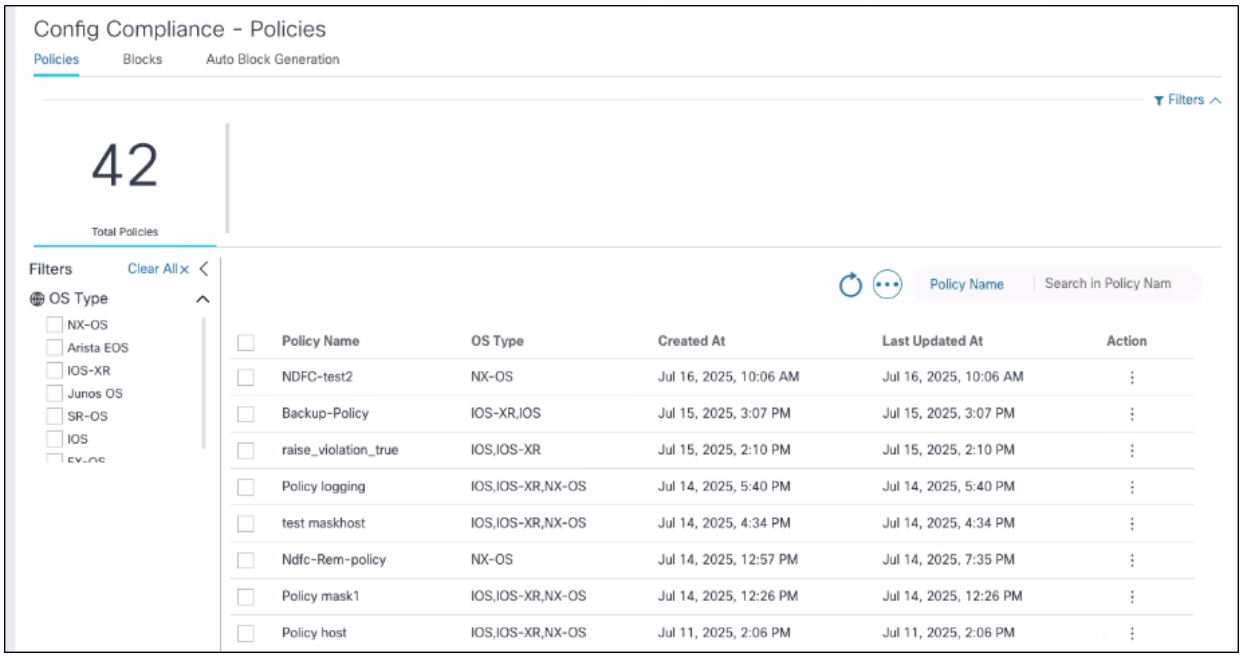
Configuration: Politiques

Un ensemble de stratégies, de règles et de blocs permettant l'exécution de la conformité peut être défini dans l'onglet Stratégies. Une stratégie est un modèle défini par l'utilisateur, composé de blocs de configuration et de règles. Vous pouvez sélectionner une liste de blocs de configuration et une liste de règles pour chaque bloc de configuration afin de créer une stratégie.

Politiques de liste

Une liste de stratégies peut être affichée sur l'onglet Stratégies qui fournit également des actions pour ajouter, modifier, supprimer, importer et exporter des stratégies.

Remarque : Les stratégies sont importées ou exportées avec les blocs et les règles associés.



Politiques de liste

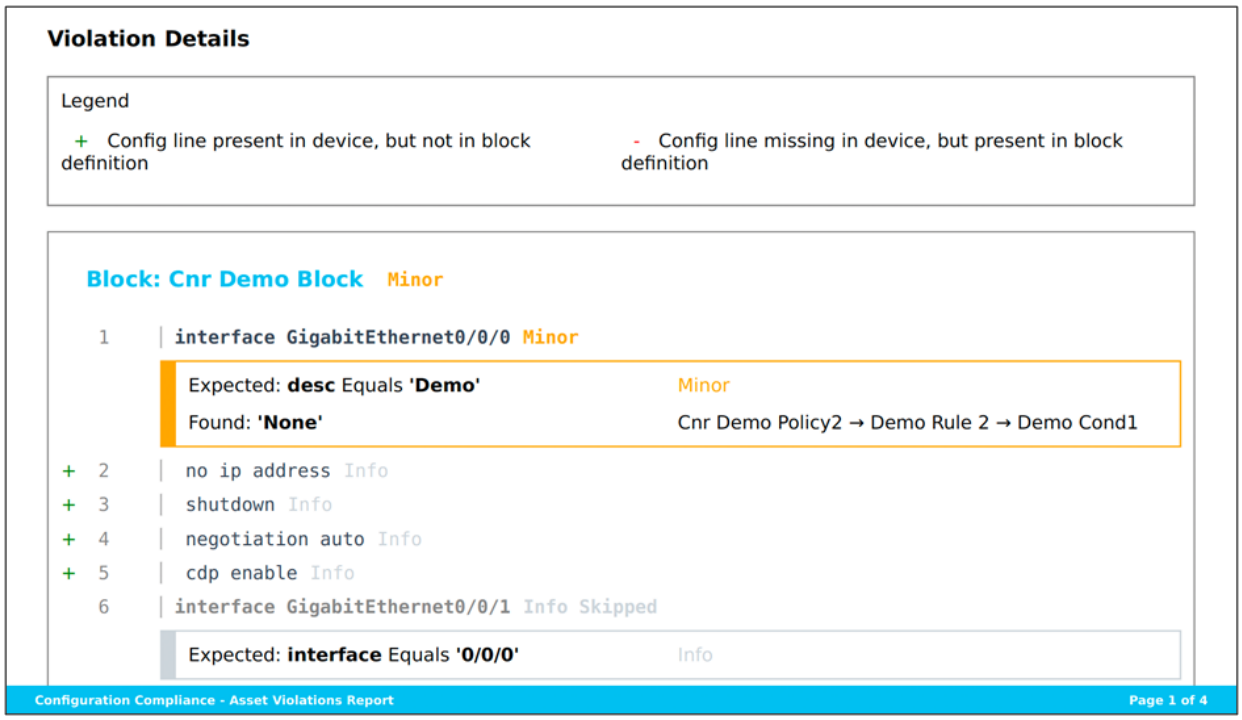
Ajout et modification de stratégies

Cette section décrit la page Ajouter une stratégie et Modifier une stratégie :

Détails de stratégie

- Nom de la stratégie : Nom de la stratégie
- Type de système d'exploitation : Liste des types de système d'exploitation pris en charge pour cette stratégie
- Famille de périphériques : Liste des familles de périphériques prises en charge pour cette stratégie
- Description de la stratégie (facultatif) : Décrit la stratégie avec une brève description

Les champs OS Type et Device Family sont remplis automatiquement en fonction des blocs sélectionnés dans la section suivante.

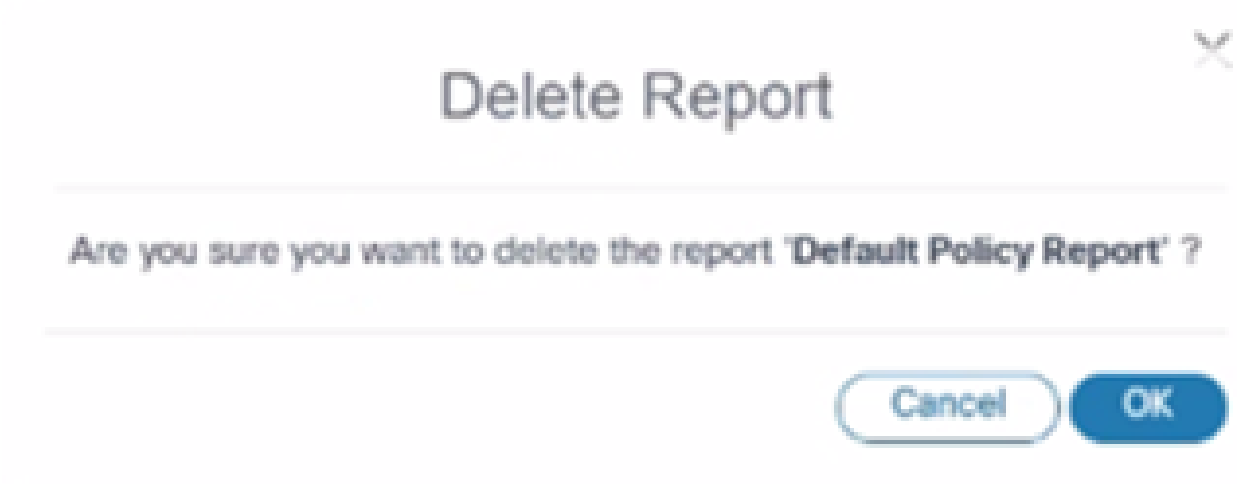


Stratégies de configuration : Détails de stratégie

Boîte de dialogue Sélectionner des blocs

La fonction « Sélectionner des blocs » est une interface conviviale conçue pour aider les utilisateurs à choisir les blocs de configuration à inclure dans une stratégie. Ses fonctionnalités sont répertoriées dans cette section :

- Boîte de dialogue contextuel
  - Objectif: Offre un espace dédié permettant aux utilisateurs de sélectionner des blocs de configuration sans quitter la page en cours
  - Interaction utilisateur : Assure un processus de sélection intuitif en présentant les options dans une boîte de dialogue distincte et ciblée
- Ajouter et sélectionner des options
  - Sélections multiples : Les utilisateurs peuvent choisir un ou plusieurs blocs de configuration à inclure dans une stratégie
  - Flexibilité : Prend en charge l'inclusion de divers blocs en fonction des exigences spécifiques de la politique de l'utilisateur
- Fonctions de navigation
  - Filtres : Permet aux utilisateurs de restreindre la liste des blocs disponibles en fonction de critères spécifiques, ce qui facilite la recherche des blocs pertinents
  - Pagination : Organise les blocs en pages faciles à gérer, ce qui améliore la navigation dans de grands ensembles de données
  - Fonctionnalités de recherche : Permet de localiser rapidement les blocs par nom ou par d'autres identificateurs, ce qui simplifie le processus de sélection



Bloquer la sélection

Les utilisateurs peuvent créer de nouveaux blocs en cliquant sur Créer dans la section Sélection de bloc. Un nouvel onglet de navigateur s'affiche et les utilisateurs peuvent créer un nouveau bloc. Une fois soumis, les utilisateurs peuvent revenir à l'onglet d'origine et sélectionner le bloc nouvellement créé pour l'ajouter à la stratégie.

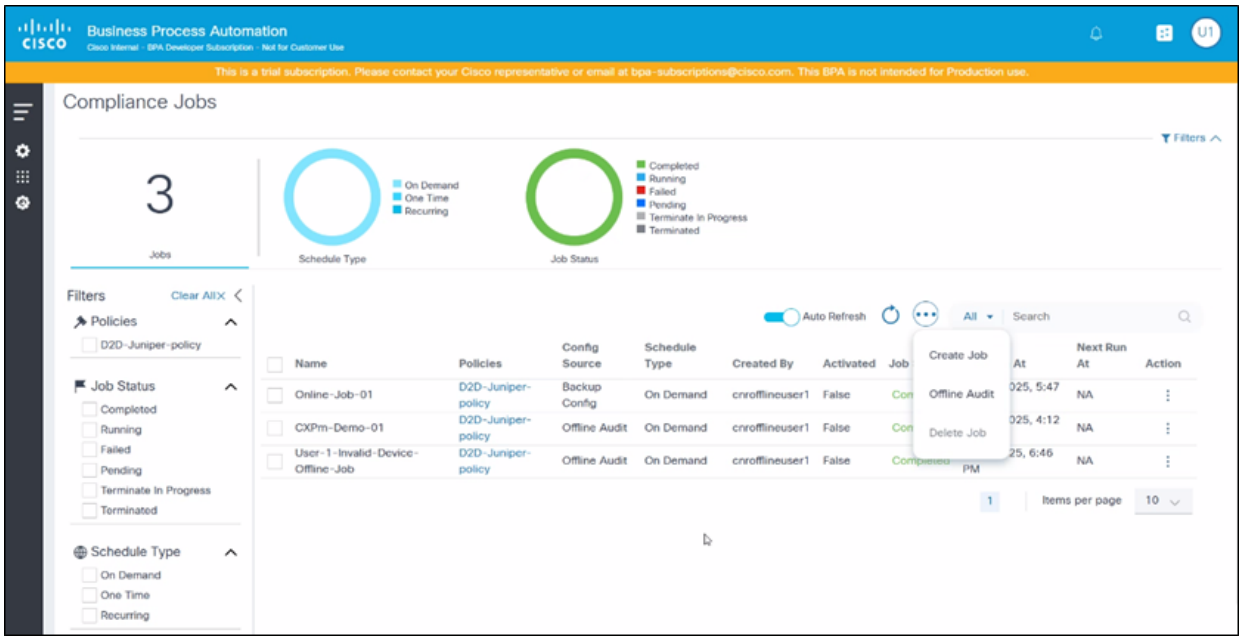
Filtres conditionnels

La fonction Filtres conditionnels est un outil avancé qui permet aux utilisateurs d'appliquer des critères spécifiques aux blocs de configuration, garantissant ainsi des contrôles de conformité précis et ciblés.

- Permet aux utilisateurs d'appliquer des configurations ou d'exécuter des contrôles de conformité sur des blocs de configuration sélectionnés en fonction de conditions prédéfinies
- Concentre les ressources et les efforts sur les blocs pertinents en filtrant ceux qui ne répondent pas aux critères spécifiés
- Les utilisateurs peuvent définir les conditions que les blocs de configuration doivent remplir pour être inclus dans les contrôles de conformité ou d'autres processus
- Seuls les blocs correspondant à ces conditions sont exécutés, tandis que d'autres sont ignorés, permettant un contrôle plus précis

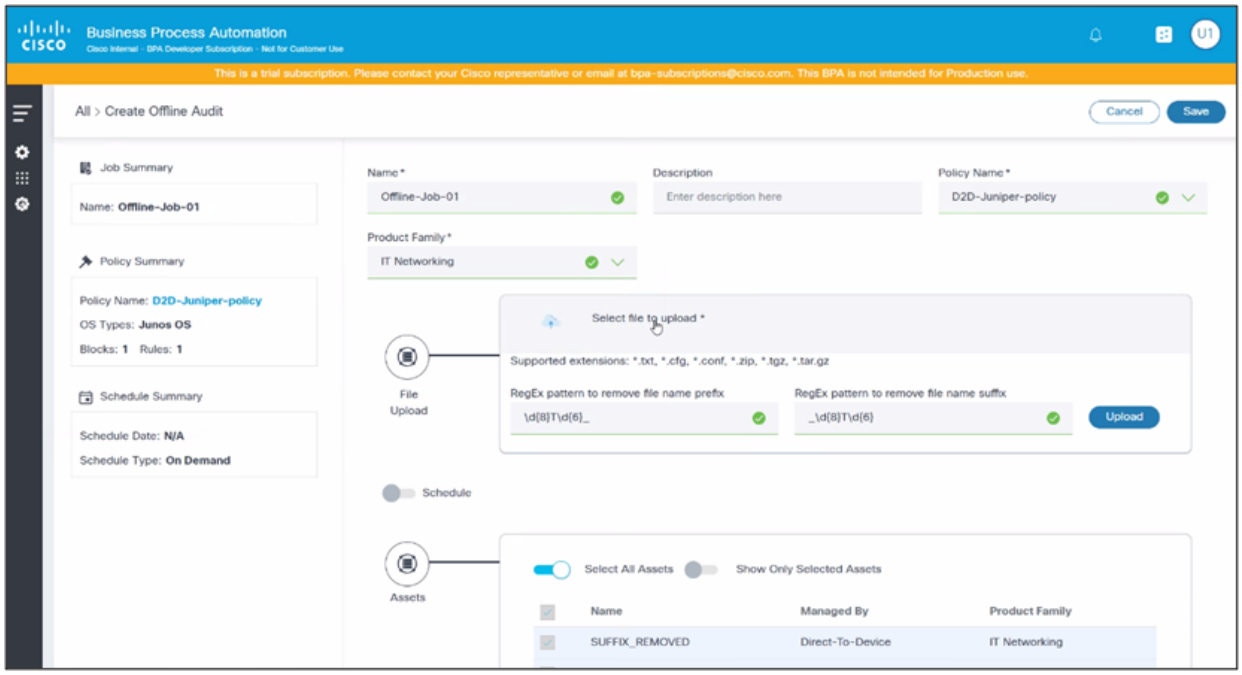
Exemple d'utilisation :

- Contrôles de conformité sélectifs : Si une stratégie est destinée à vérifier les configurations sur seulement deux interfaces spécifiques sur les 20 disponibles, les utilisateurs peuvent définir des conditions pour limiter les vérifications de conformité à seulement ces deux interfaces.



Filtres conditionnels

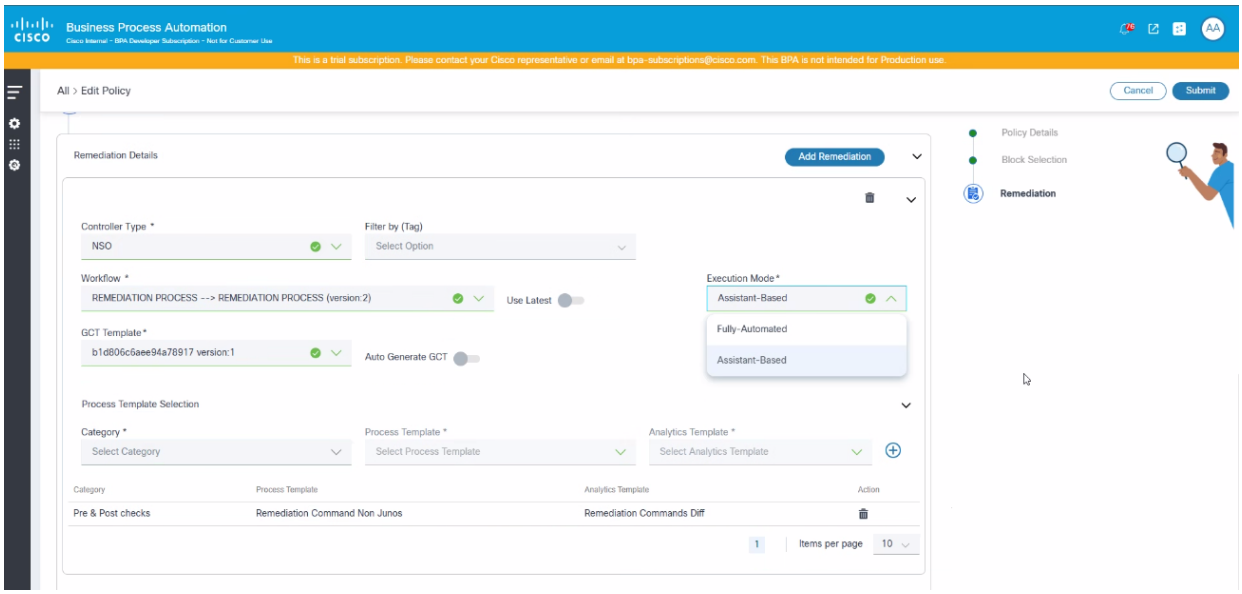
- Sélectionner des règles : Option permettant de sélectionner une ou plusieurs règles pour un bloc de configuration donné.



Sélectionner des règles

Section Correction

La page Policies fournit une section facultative pour définir les détails de la conversion par type de contrôleur.



Stratégies de configuration : Détails de correction

- Type de contrôleur : Liste des types de contrôleurs avec prise en charge de la correction
- Workflow de résolution : Workflow à exécuter pour les périphériques du type de contrôleur sélectionné
- Modèle GCT : Un ou plusieurs modèles GCT à appliquer
- Modèle de processus : Un ou plusieurs modèles de processus à exécuter dans le cadre de la pré-vérification et de la post-vérification, ainsi que le modèle analytique correspondant.
- Modèle de pré-vérification : Liste facultative de modèles de processus à exécuter uniquement pour la pré-vérification
- Modèle de post-contrôle : Liste facultative de modèles de processus à exécuter uniquement pour la vérification postérieure
- Mode d'exécution :
  - Entièrement automatique : Le processus de conversion s'exécute automatiquement sans intervention manuelle ni tâche utilisateur
  - Basé sur assistant : Le système crée des tâches utilisateur qui nécessitent une assistance manuelle pendant le processus de conversion

Génération automatique de la fonctionnalité GCT

La fonction de génération automatique de GCT est conçue pour rationaliser le processus de création des modèles GCT nécessaires à la correction. Il fonctionne comme détaillé ci-dessous :

- Génère automatiquement des modèles GCT en fonction des résultats et des détails de l'exécution de la conformité
- Automatise le processus de création du modèle
- Les modèles générés sont conçus pour résoudre les problèmes identifiés lors des vérifications de conformité, garantissant que les actions correctives s'alignent sur les besoins de conformité

Rôles et contrôle d'accès

Liste des autorisations statiques

Le tableau de bord Conformité de la configuration du portail de nouvelle génération prend en charge la fonctionnalité RBAC de BPA avec les autorisations suivantes qui indiquent comment un bloc de texte dynamique de configuration est affiché dans une représentation d'interface utilisateur graphique pour la gestion des règles et des conditions :

Groupe	Action	Description
ui-app	complianceDashboard.show	Afficher/masquer l'application Tableau de bord de conformité
ui-app	remédiationDashboard.show	Afficher l'application Tâches de résolution
ui-app	complianceJobs.show	Afficher l'application Tâches de conformité
ui-app	complianceConfigurations.show	Afficher l'application de configuration de conformité
tableau de bord	RessourcesSynthèseConformité	Afficher le récapitulatif de conformité des ressources
tableau de bord	PolicyComplianceSummary	Afficher le récapitulatif de conformité des stratégies
tableau de bord	affichageViolations	Afficher les détails des violations
tableau de bord	StratégieRessourcesConformitéRécapitulatif	Afficher les ressources affectées

Groupe	Action	Description
tableau de bord	afficherRapports	Afficher le tableau de bord des rapports, les paramètres des rapports et télécharger les rapports
tableau de bord	gérerRapports	Créer et supprimer des rapports
tableau de bord	manageReportSettings	Modifier les paramètres du rapport
Tableau de bord	affichageTâchesCorrection	Afficher les travaux de résolution
Tableau de bord	affichageÉtapesCorrection	Afficher les jalons de résolution
Tableau de bord	manageRemediationJobs	Gérer les tâches de résolution telles que créer, supprimer, archiver et gérer les tâches utilisateur
travauxConformité	afficherTâchesConformité	Afficher les travaux et les exécutions de conformité
travauxConformité	manageComplianceJobs	Gérer les tâches de conformité
ConformitéConfigurations	affichageConfigurationsConformité	Affichez les configurations de conformité telles que les stratégies, les blocs, les règles, la génération de blocs, les identificateurs de blocs et les modèles TCP
ConformitéConfigurations	manageCompliancePolicies	Gérer les

Groupe	Action	Description
		stratégies de conformité
Conformité	Configurations manageComplianceBlocks	Gérer les blocs et les règles de conformité et les identificateurs de bloc
Conformité	Configurations manageComplianceBlockGeneration	Gérer la génération de blocs de conformité et les modèles TCP

Rôles prédéfinis

L'exemple d'utilisation Conformité et correction de la configuration comporte les rôles prédéfinis répertoriés dans le tableau ci-dessous :

Remarque : Les administrateurs peuvent créer ou mettre à jour des rôles en fonction des exigences du client.

Rôle	Description	Autorisations
Administrateur de conformité	Rôle Administrateur avec toutes les autorisations liées à la conformité	Applications d'interface utilisateur : Afficher Asset Manager - Afficher le groupe d'actifs - Afficher le tableau de bord de conformité - Afficher les tâches de conformité - Afficher la configuration de conformité Ressource : Afficher la liste des ressources - Afficher la configuration de sauvegarde des ressources - Configuration de sauvegarde

Rôle	Description	Autorisations
		- Effectuer des actions de périphérique activées par le contrôleur Groupe d'actifs : - Afficher les groupes d'actifs - Gérer les groupes de ressources - Créer des groupes d'actifs dynamiques Configuration de sauvegarde : Afficher, comparer et télécharger les sauvegardes de configuration des périphériques Stratégie de sauvegarde et de restauration : Afficher les politiques de sauvegarde et de restauration Tableau de bord de conformité : - Afficher les résumés de conformité des ressources - Afficher les résumés de conformité des stratégies - Afficher les violations - Afficher les ressources affectées Créer et supprimer des rapports Afficher le tableau de bord des rapports, les paramètres des rapports et télécharger les rapports Modifier les paramètres du rapport : Tâches de conformité Afficher les travaux et les exécutions de conformité - Gérer les tâches de conformité Configurations de conformité : - Affichez les configurations de conformité telles que les stratégies,

Rôle	Description	Autorisations
		les blocs et les règles - Gérer les stratégies de conformité - Gérez les blocs de conformité, les règles et les identificateurs de bloc - Gérez la génération de blocs de conformité et les modèles TCP
Opérateur de conformité	Rôle opérateur avec toutes les autorisations de conformité, à l'exception de la gestion de la configuration	Applications d'interface utilisateur : - Afficher le gestionnaire d'actifs - Afficher le groupe d'actifs - Afficher le tableau de bord de conformité - Afficher les tâches de conformité - Afficher la configuration de conformité Ressource : Afficher la liste des ressources - Afficher la configuration de sauvegarde des ressources - Configuration de sauvegarde - Effectuer des actions de périphérique activées par le contrôleur Groupe d'actifs : - Afficher les groupes d'actifs - Gérer les groupes de ressources - Créer des groupes d'actifs dynamiques Configuration de sauvegarde : Afficher, comparer et télécharger les sauvegardes de configuration des périphériques Stratégie de sauvegarde et de restauration : Afficher les politiques de sauvegarde et de restauration Tableau de bord de conformité :

Rôle	Description	Autorisations
		- Afficher le récapitulatif de conformité des ressources - Afficher le récapitulatif de conformité aux stratégies - Afficher les violations - Afficher les ressources affectées Créer et supprimer des rapports Afficher le tableau de bord des rapports, les paramètres des rapports et télécharger les rapports Tâches de conformité : Afficher les travaux et les exécutions de conformité - Gérer les tâches de conformité Configurations de conformité : Afficher les configurations de conformité telles que les stratégies, les blocs et les règles Applications d'interface utilisateur : - Afficher le gestionnaire d'actifs - Afficher le groupe d'actifs - Afficher le tableau de bord de conformité - Afficher les tâches de conformité - Afficher la configuration de conformité
Conformité en lecture seule	Fournit toutes les autorisations en lecture seule liées à l'exemple d'utilisation de conformité	Ressource : Afficher la liste des ressources - Afficher la configuration de sauvegarde des ressources - Effectuer des actions de périphérique activées par le contrôleur Groupe d'actifs : - Afficher les groupes d'actifs

Rôle	Description	Autorisations
Administrateur de mesures correctives/Opérateur de mesures correctives	Rôle d'opérateur avec toutes les autorisations liées à la résolution	Configuration de sauvegarde : Afficher, comparer et télécharger les sauvegardes de configuration des périphériques Stratégie de sauvegarde et de restauration : Afficher les politiques de sauvegarde et de restauration Tableau de bord de conformité : Afficher le récapitulatif de conformité des ressources - Afficher le récapitulatif de conformité aux stratégies - Afficher les violations - Afficher les ressources affectées Afficher le tableau de bord des rapports, les paramètres des rapports et télécharger les rapports Tâches de conformité : Afficher les travaux et les exécutions de conformité Configurations de conformité : Afficher les configurations de conformité telles que les stratégies, les blocs et les règles Applications d'interface utilisateur : - Afficher le gestionnaire d'actifs - Afficher le groupe d'actifs - Afficher le tableau de bord de résolution Ressource : - Afficher la liste des ressources Groupe d'actifs :

Rôle	Description	Autorisations
Résolution en lecture seule	Fournit toutes les autorisations en lecture seule liées à l'exemple d'utilisation de conversion	- Afficher les groupes d'actifs Gérer les groupes de ressources - Créer des groupes d'actifs dynamiques Tableau de bord de résolution : - Afficher les travaux de résolution - Afficher les jalons de résolution - Afficher le récapitulatif de conformité des ressources - Gérez les tâches de conversion telles que la création, la suppression, l'archivage et le traitement des tâches utilisateur - Afficher les ressources affectées Applications d'interface utilisateur : - Afficher le gestionnaire d'actifs - Afficher le groupe d'actifs - Afficher le tableau de bord de résolution Ressource : - Afficher la liste des ressources Groupe d'actifs : - Afficher les groupes d'actifs Créer des groupes d'actifs dynamiques Tableau de bord de résolution : - Afficher les travaux de résolution - Afficher les jalons de résolution - Afficher le récapitulatif de conformité des ressources - Afficher les ressources affectées

Politiques d'accès

La fonction Stratégies d'accès garantit aux utilisateurs un accès approprié à des stratégies de conformité et à des groupes de ressources spécifiques. Cette fonctionnalité renforce la sécurité et l'efficacité opérationnelle en permettant aux administrateurs de définir et d'appliquer des contrôles d'accès basés sur les rôles et responsabilités des utilisateurs. Les stratégies d'accès sont gérées via la page Stratégie d'accès, où les administrateurs peuvent créer, modifier et attribuer des stratégies aux utilisateurs ou aux groupes. Les administrateurs peuvent définir des autorisations granulaires, en spécifiant les stratégies de conformité et les groupes d'actifs que chaque utilisateur ou groupe peut afficher, modifier ou gérer. Ce niveau de détail permet de maintenir un contrôle strict sur les informations sensibles et les opérations critiques.

Une fois la stratégie d'accès définie, les données sont restreintes sur toutes les pages de conformité et de correction de l'interface utilisateur de nouvelle génération, en fonction de la liste des stratégies et des ressources CnR auxquelles l'utilisateur actuel a accès.

Pour fournir un accès utilisateur :

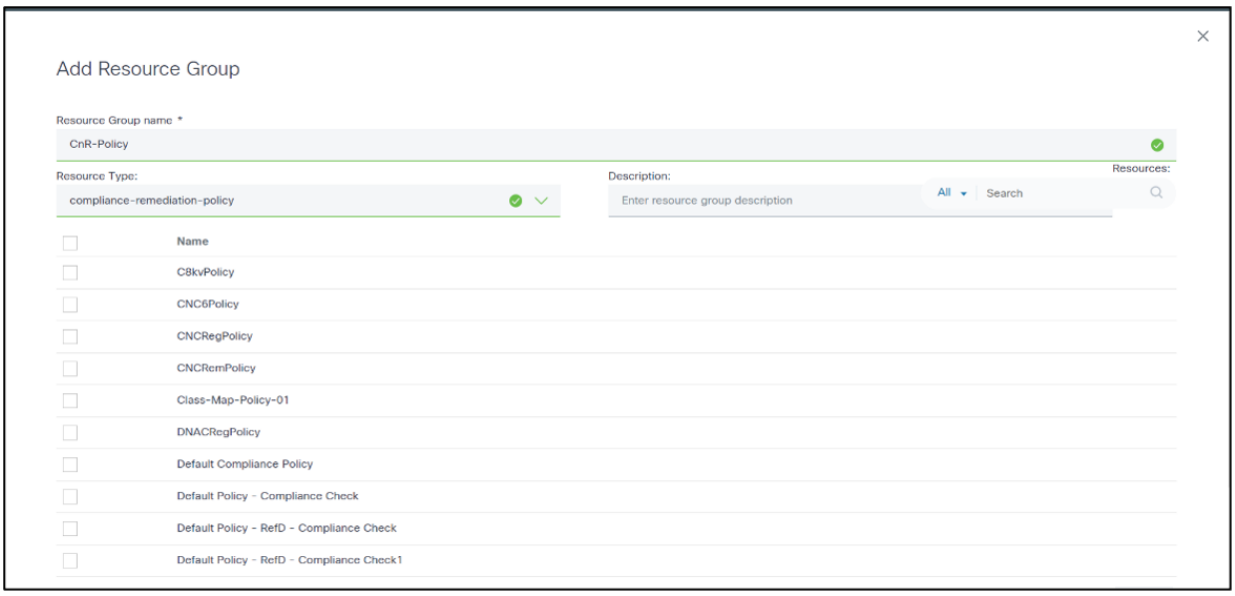
Remarque : Les autorisations ne peuvent être fournies que par les administrateurs.

---

1. Créez des utilisateurs et attribuez-leur un nom à un ou plusieurs groupes d'utilisateurs.
2. Créez des rôles d'utilisateur et attribuez-les aux groupes d'utilisateurs créés.
3. Ajouter une ou plusieurs immobilisations à un ou plusieurs groupes d'immobilisations.
4. Créez des groupes de ressources pour attribuer des ressources de stratégie de conformité.
5. Créez une stratégie d'accès et sélectionnez le ou les groupes d'utilisateurs, les groupes d'actifs et les groupes de ressources appropriés.

Créer un groupe de ressources

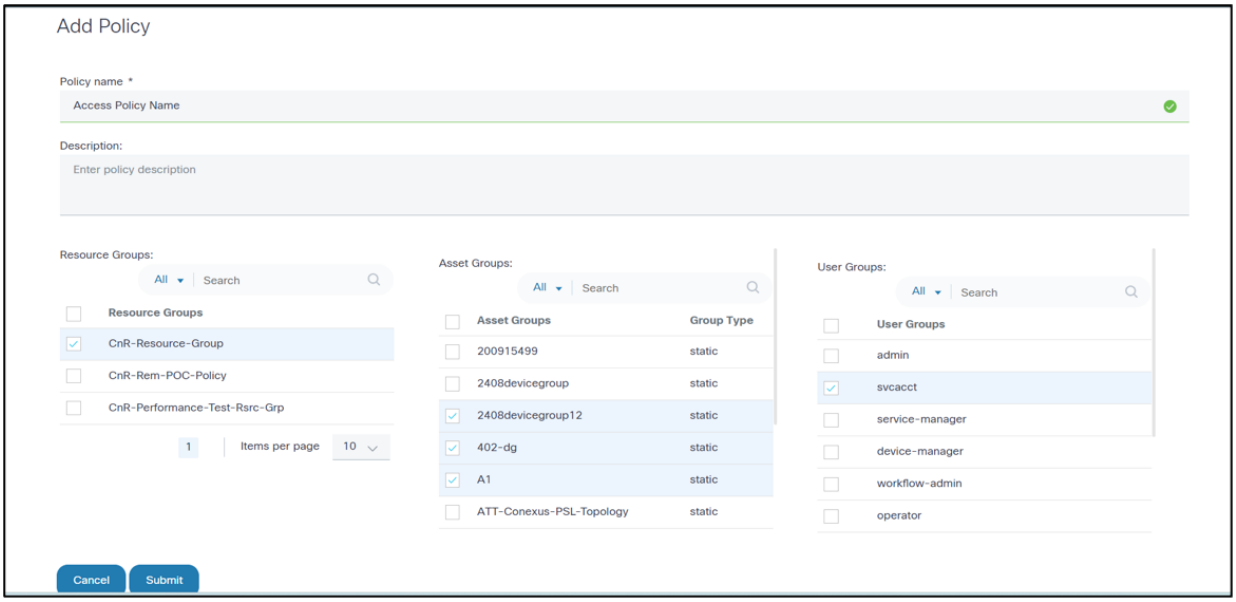
Créez un groupe de ressources à l'aide de la stratégie de conversion de conformité de la liste déroulante Type de ressource et sélectionnez les stratégies de conformité qui doivent avoir accès au groupe d'utilisateurs respectif.



Créer un groupe de ressources

Créer une stratégie d'accès

Créez une stratégie d'accès avec des groupes de ressources et des groupes d'actifs qui doivent accorder des autorisations aux groupes d'utilisateurs.



Créer une stratégie d'accès

Conformité hors ligne

La fonction de conformité hors ligne permet aux utilisateurs d'exécuter des vérifications de conformité par rapport aux configurations de périphériques qui ne sont pas disponibles via les périphériques actifs dans l'inventaire des ressources.

Les utilisateurs peuvent exécuter la conformité hors connexion en utilisant la configuration de sauvegarde du périphérique ou en créant un audit hors connexion dans les travaux de conformité. Les résultats des exécutions peuvent être affichés dans le tableau de bord Conformité.

Utilisation de Device Backup Config

Les administrateurs peuvent télécharger manuellement un fichier zip contenant la configuration en cours pour un ensemble de périphériques souhaité. Cette fonction est disponible dans la section Device Config - Upload de l'application Backup & Restore. Une fois les configurations de périphériques téléchargées, une tâche de conformité pour les périphériques souhaités peut être créée en sélectionnant Device Backup Config comme source de la configuration de périphériques. Pendant l'exécution, la configuration de périphérique téléchargée est récupérée à partir de l'application de sauvegarde et un contrôle de conformité est exécuté sur celle-ci.

Utilisation de la fonction Créer un audit hors connexion dans les travaux de conformité

Pour exécuter la conformité sur une configuration de périphérique hors connexion, les utilisateurs peuvent sélectionner Offline Audit à partir de l'icône More Options sur la page Compliance Jobs. Cela permet aux utilisateurs de télécharger manuellement un fichier zip contenant la configuration en cours directement dans l'application Conformité. Pendant l'exécution, la configuration de périphérique téléchargée est analysée et la vérification de conformité est exécutée.

Déploiement de configurations via Ingester

Le chargement des artefacts de configuration de conformité peut être automatisé à l'aide de l'infrastructure Ingester. Une fois les artefacts développés, ils peuvent être exportés, empaquetés et déployés dans l'environnement cible en procédant comme suit.

- Créez le package NPM à l'aide des commandes suivantes :

```
mkdir <

      >
cd  <

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

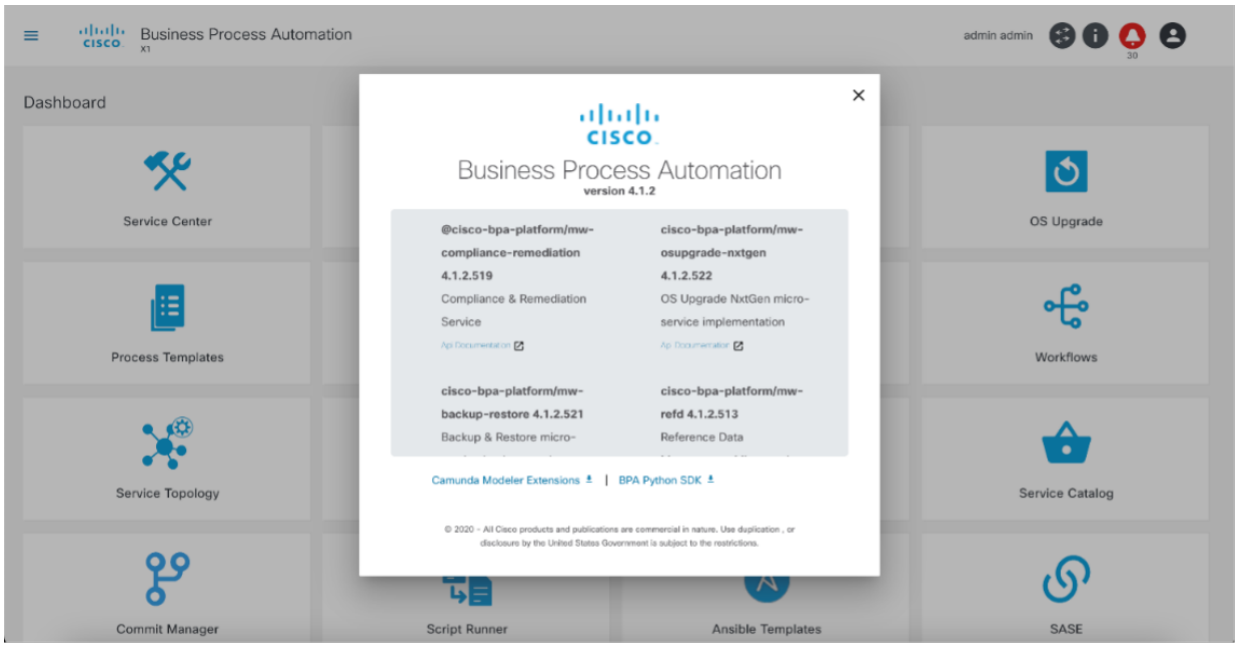
- Exporter les configurations à partir du portail BPA (interface utilisateur classique)
    - Accédez à BPA Classic UI > Configuration Compliance & Remediation > Configurations
    - Exporter « Modèles TCP/Identificateurs de bloc/Blocs/Règles/Stratégies »
- Renommez les fichiers exportés comme suit :
    - Modèles TTP : <<nom du fichier>>.cnrttptemplate.json
    - Identificateurs de bloc : <<nom de fichier>>.cnrblockidentifier.json
    - Blocs : <<nom de fichier>>.cnrblock.json
    - Règles : <<nom de fichier>>.cnrrule.json
    - Politiques : <<nom de fichier>>.cnrpolicy.json
- Données d'ingester du package (.tgz)
    - Copiez tous les fichiers exportés dans le package npm créé à l'« étape-1 »
    - Exécutez la commande `npm pack` dans le package npm pour créer le fichier « .tgz »
- Déploiement de données ingester (.tgz) dans BPA Single Node env
    - Copiez le fichier .tgz dans le dossier <<Offre groupée principale BPA>>/packages/data du serveur sur lequel l'offre groupée BPA a été déployée
    - Redémarrez le serveur Ingester (docker restart ingester-service)
- Déploiement de données Ingester (.tgz) dans BPA Multi Node env
    - Copiez le fichier .tgz dans le dossier /opt/bpa/packages/data du serveur sur lequel les graphiques de barre sont déployés
    - Redéploiement du pod Ingester (`déploiement kubectl, redémarrage du déploiement ingester-service -n bpa-ns`)

Références

Nom	Description
TP	Analyseur de texte de modèle utilisé dans les blocs de configuration
Analyseur Conf	Analyseur de champ de configuration utilisé pour analyser la configuration des périphériques CLI

Documentation API

Les détails de la documentation de l'API pour la conformité et la correction se trouvent dans la fenêtre contextuelle classique À propos de :



BPA À propos de (interface utilisateur classique)

Dépannage

Tableau De Bord

Les résultats des travaux de conformité récents ne s'affichent pas

Observation : Les résultats des travaux de conformité récents ne s'affichent pas dans le tableau de bord du portail de nouvelle génération.

Cause potentielle 1 : Le tableau de bord comporte une sélection de plage de dates, qui prend par défaut la valeur « Mois en cours ». Si un nouveau mois a récemment commencé (par exemple, aujourd'hui est le premier du mois), les exécutions effectuées avant hier (dernier jour du mois précédent) ne s'affichent pas.

Analyse: Vérifiez que la plage de dates correcte est sélectionnée dans le tableau de bord, y compris les jours du mois précédent, si nécessaire, pour afficher les données de violations appropriées.

Cause potentielle 2 : Un utilisateur différent peut avoir exécuté une tâche de conformité sur la même stratégie et/ou combinaison d'actifs. Le tableau de bord affiche les violations détectées lors de la dernière exécution dans la plage de dates sélectionnée.

Analyse: En tant qu'administrateur (ou utilisateur ayant accès à tous les travaux de conformité), passez en revue la liste des travaux de conformité et leur historique pour déterminer les

combinaisons de stratégies ou de groupes d'actifs à exécuter.

Tâches de conformité

État d'exécution complet défini comme « Ignoré »

Observation : Lors de l'exécution des travaux de conformité, un état d'exécution complet est marqué comme « Ignoré ». Aucune violation n'est signalée.

Cause potentielle : Une exécution existante pour le même travail est toujours en cours d'exécution.

Analyse: Une tâche de conformité ne peut avoir qu'une seule exécution en cours à un moment donné. Vérifiez si une exécution antérieure est toujours en cours. Les exécutions bloquées ou en cours pendant une période prolongée peuvent être terminées/

État du périphérique défini comme « Ignoré »

Observation : Dans une exécution de tâche de conformité, l'état de certains périphériques est marqué comme « Ignoré ».

Cause potentielle : La fonctionnalité de conformité n'est pas activée pour le type de contrôleur auquel ce périphérique appartient.

Analyse: La stratégie de conformité s'applique uniquement aux périphériques du groupe de ressources dont la fonctionnalité est activée.

État du périphérique défini sur « Failed »

Observation : Dans une exécution de tâche de conformité, l'état de certains périphériques est marqué comme « Échec ».

Cause potentielle : Erreurs d'exécution qui se sont produites pendant le processus d'exécution de conformité. Ces erreurs peuvent être des erreurs de code ou des configurations incorrectes dans des stratégies, des blocs, des règles, des identificateurs de bloc, etc.

Analyse:

API permettant de localiser la raison des erreurs d'exécution :

1. Obtenir les exécutions pour trouver l'ID d'exécution

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

   compliance-exécutions

   Méthode : GET

2. Obtenir les exécutions de périphériques en utilisant l'ID d'exécution

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

   compliance-device-exécutions ?

   executionId=<< id_exécution >>

   Méthode : GET

Règles de conformité

Les règles affichent une valeur vide

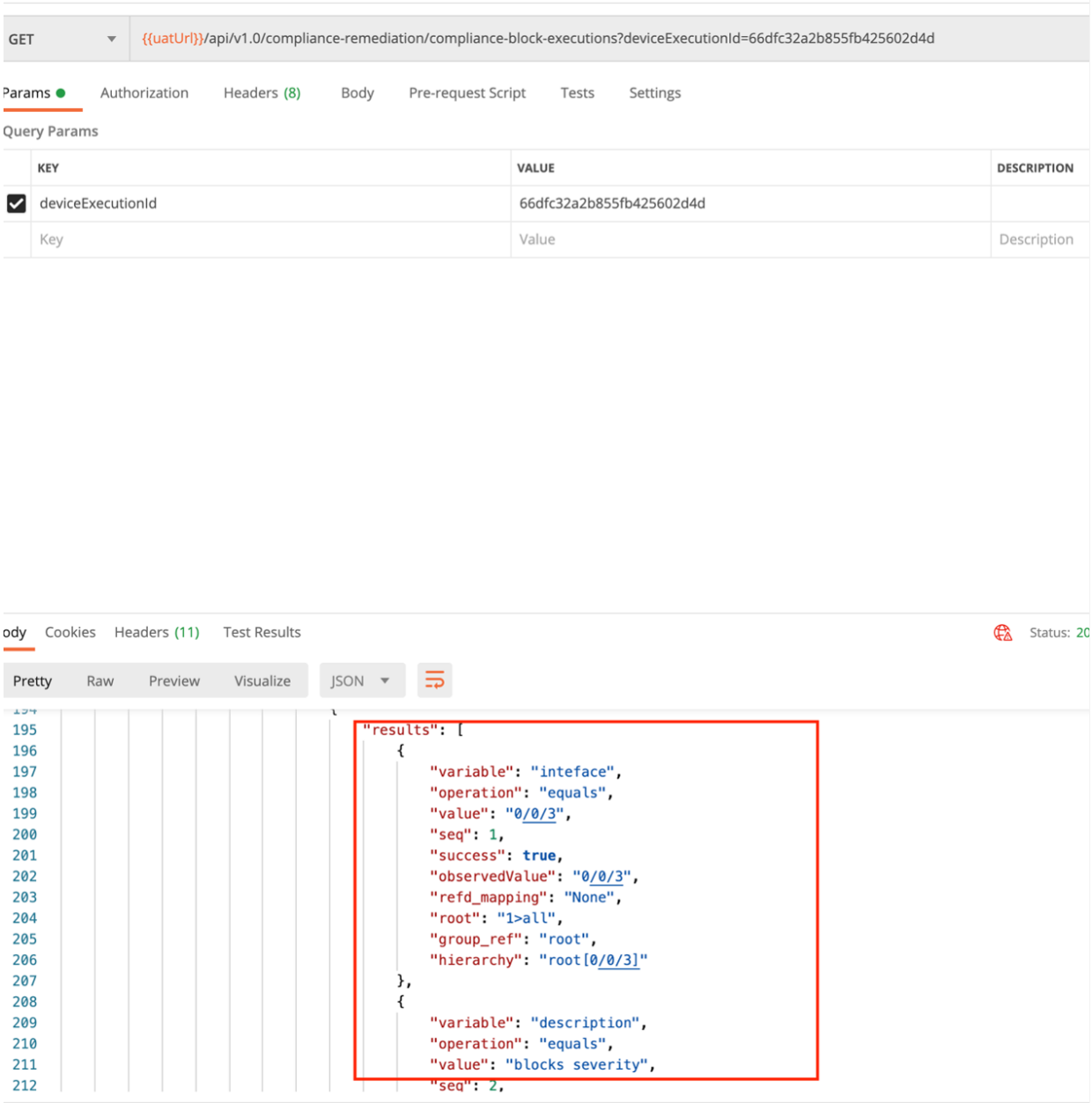
Observation : Lors de l'exécution d'un travail de conformité, les variables de règle affichent des valeurs vides.

Analyse:

1. Si des données sont extraites de l'application RefD, vérifiez que les clés RefD sont au format correct. Si c'est le cas, vérifiez que l'application RefD contient des données pour la clé liée à la variable de conformité dans les règles. Vérifiez également que la clé RefD correcte est envoyée à partir de l'application de conformité en consultant les journaux du service de conformité. Reportez-vous à Présentation de la hiérarchie des règles et de l'intégration RefD dans les règles et les règles non-RefD.
2. Vérifiez le résultat de l'exécution du bloc de conformité en utilisant l'API suivante :

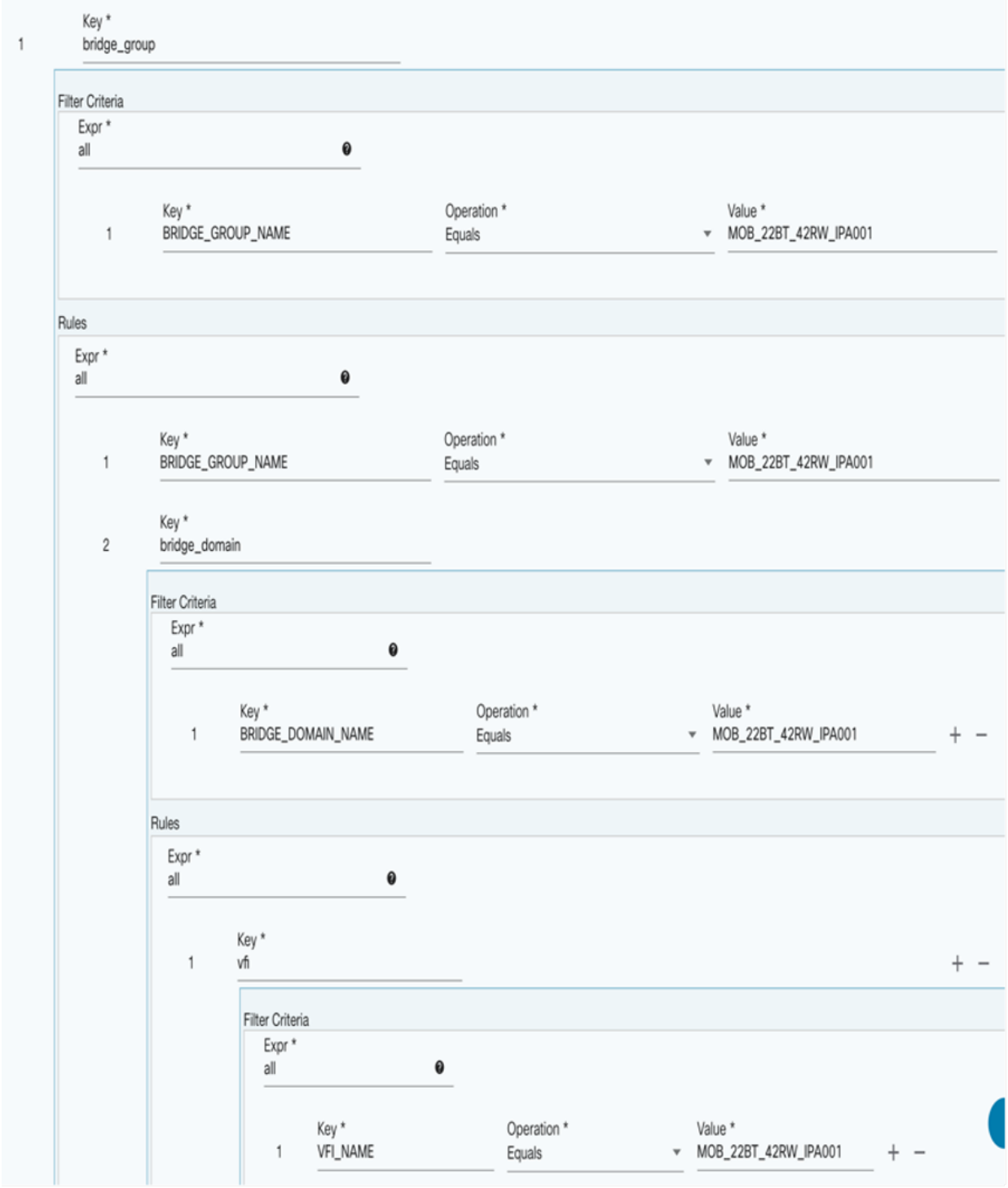
   URL: /api/v1.0/compliance-remédiation/compliance-block-exécutions?deviceExecutionId=<>

   Méthode : GET



Résultats de l'exécution du bloc de conformité

3. Vérifiez si le bloc possède des sous-hiérarchies ou une hiérarchie unique et assurez-vous que les règles sont configurées en fonction de la hiérarchie.



Résultats de l'exécution du bloc de conformité

4. Vérifiez que l'analyseur HTTP extrait la valeur de la configuration du périphérique en exécutant le script python suivant :

```
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)
```

Surveillance des journaux de conformité

Env. noeud unique :

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

Env Kubernetes multinoeud :

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

Surveillance des journaux Kibana :

```
https://<< HÔTE BPA >>:30401
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.