

Guide d'utilisation de l'appliance virtuelle Cisco IQ v1.2.0

Introduction

Cisco IQTM propose des améliorations et des fonctionnalités conçues pour améliorer la visibilité des ressources, fournir des informations plus intelligentes sur l'ensemble de leurs environnements et rationaliser la gestion des dossiers. En outre, des fonctionnalités d'IA telles que Cisco IQ AI Assistant optimisent les résultats opérationnels et l'expérience utilisateur Cisco IQ en fournissant une compréhension contextuelle qui vous permet de prendre des décisions proactives et éclairées et de rationaliser les processus pour l'engagement et la réussite des clients.

Cisco IQ On-Prem Air-Gapped est l'un des modes de déploiement de Cisco IQ, conçu pour les clients des secteurs fortement réglementés ayant des exigences strictes en matière de conformité, de souveraineté des données et de sécurité. Dans ce mode, Cisco IQ est fourni sous la forme d'une machine virtuelle autonome (VM) appelée appliance virtuelle Cisco IQ (VA). L'appliance virtuelle fonctionne entièrement dans les locaux du client et fonctionne de manière totalement isolée des réseaux externes. Pour maintenir cette isolation, les mises à jour logicielles et les packages de maintenance sont obtenus à partir de Cisco IQ SaaS et transférés à l'appliance virtuelle par le biais d'un processus manuel approuvé.

Cisco IQ On-Prem Air-Gapped étend les fonctionnalités clés de Cisco IQ SaaS aux environnements à faible débit, ce qui permet aux équipes stratégiques de fonctionner avec une vitesse et une intelligence de diagnostic comparables à celles des entreprises connectées au cloud.

Pour accéder à l'appliance virtuelle Cisco IQ, ouvrez un navigateur pris en charge et accédez à <https://<fqdn-of-the-appliance>>. Connectez-vous à l'aide du nom d'utilisateur et du mot de passe admin définis lors du processus d'installation.

 Remarque : La solution Cisco IQ VA est actuellement limitée aux clients inscrits au programme de disponibilité contrôlée. L'accès au téléchargement pour le logiciel du système VA et les packages opérationnels supplémentaires (modules, règles et droits) à partir du portail Cisco IQ est disponible exclusivement pour certains clients. Pour plus d'informations, contactez votre représentant de compte.

Gestion des connexions (collecte de données)

Cisco IQ VA est une solution sur site de collecte de données réseau qui offre une visibilité approfondie de votre infrastructure. Il collecte des données via Catalyst Center et Direct Connection. Elle simplifie la gestion de l'authentification réseau et de la détection des périphériques. La configuration de la collecte de données comprend :

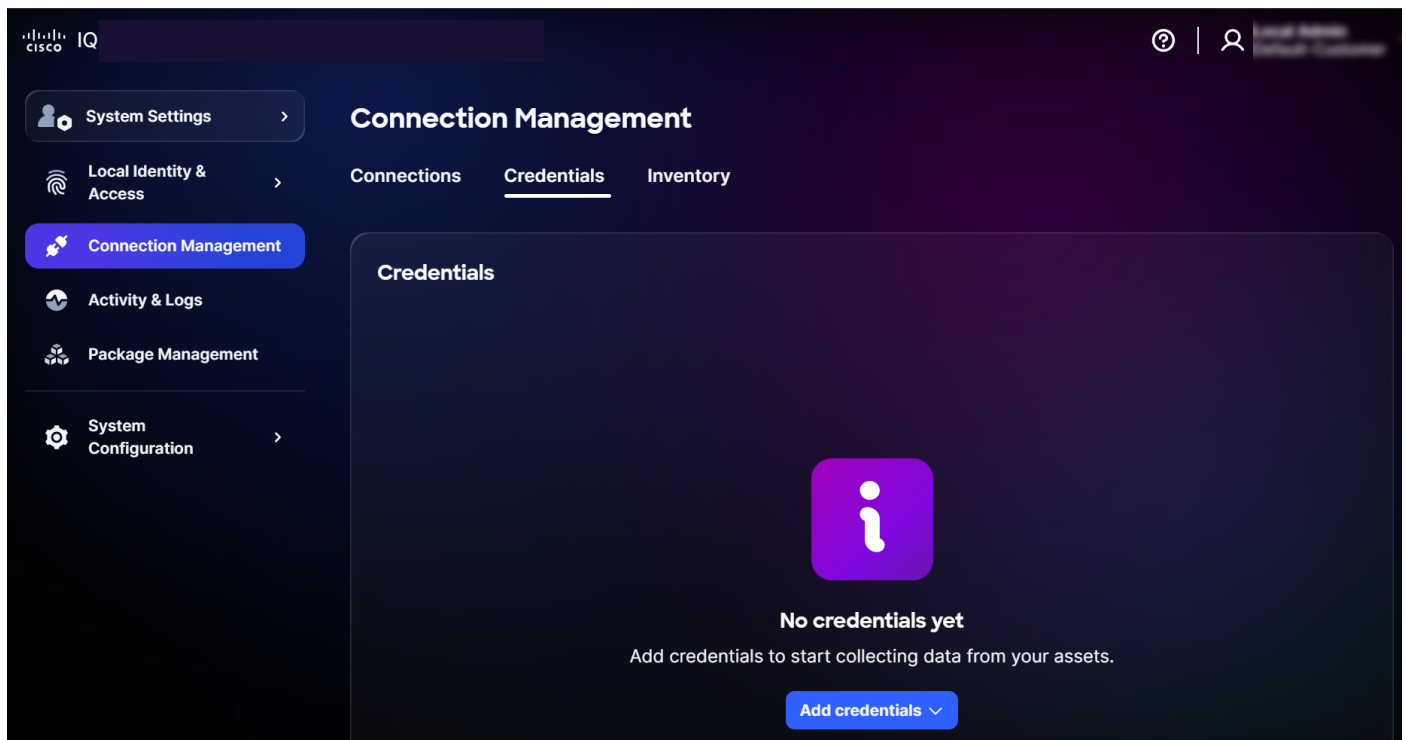
- Création de jeux d'informations d'identification : Établissez les protocoles d'authentification (par exemple, SNMP (Simple Network Management Protocol) v1/v2c/v3) pour communiquer avec vos périphériques réseau. La centralisation des informations d'identification par zone ou emplacement de sécurité (par exemple, « SanJose-SNMPv3 ») vous permet de mettre à jour les mots de passe dans un emplacement unique, les modifications étant automatiquement propagées à tous les périphériques associés.
- Mappage des informations d'identification à Inventory : Associez vos jeux d'informations d'identification à vos ressources d'inventaire pour automatiser le processus d'authentification. En créant des règles qui lient des plages IP spécifiques à des jeux d'informations d'identification définis, le système applique automatiquement l'authentification correcte lors de la collecte des données. Cela élimine les erreurs de saisie manuelle et garantit que votre configuration reste précise au fur et à mesure que votre réseau se développe.

 Remarque : Les protocoles SNMPv2c/SNMPv3 et SSH sont requis pour la détection des périphériques, et des informations d'identification HTTP/HTTPS doivent être fournies avant de configurer Catalyst Center.

Ajout de références

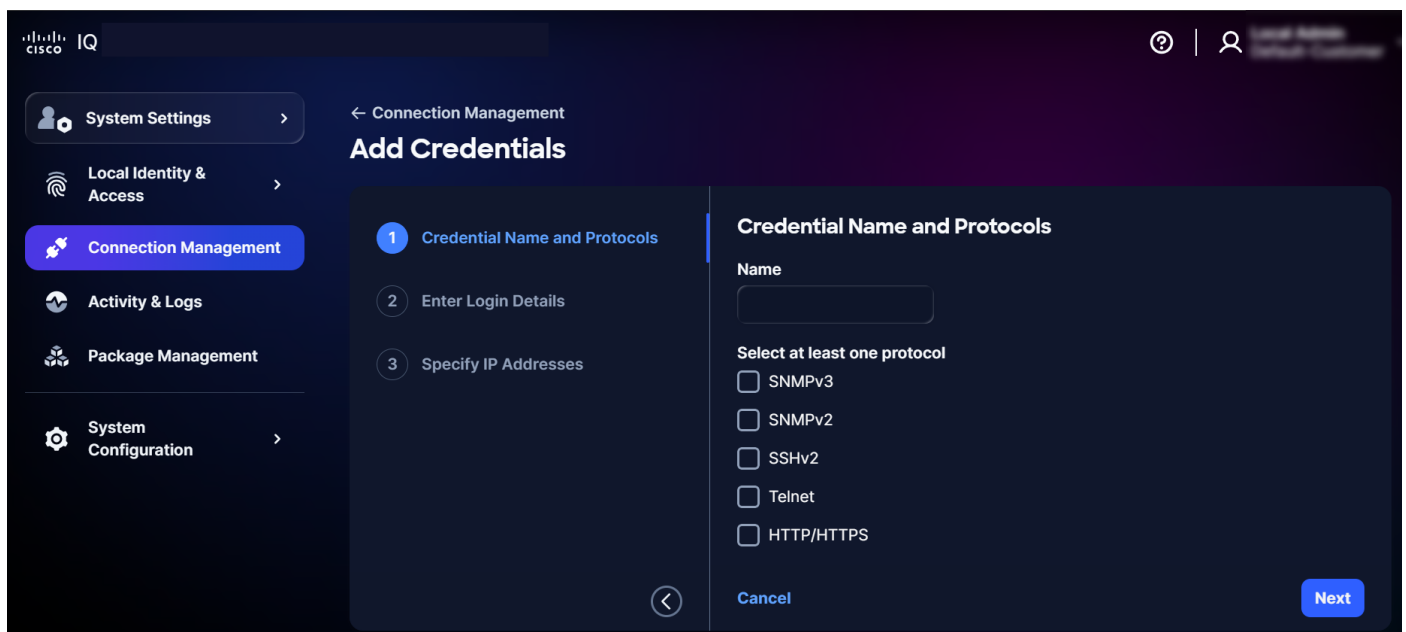
Vous devez d'abord ajouter des informations d'identification pour collecter des données. Pour ajouter des informations d'identification :

1. Dans Paramètres système, sélectionnez Gestion des connexions. La page Gestion des connexions s'affiche.
2. Cliquez sur l'onglet Informations d'identification.



Onglet Informations d'identification

3. Cliquez sur Ajouter des informations d'identification.



Ajouter des identifiants

4. Saisissez un nom.

5. Cochez toutes les cases du protocole applicable.

6. Cliquez sur Suivant.

Add Credentials

1. Credential Name and Protocols

2. Enter Login Details

3. Specify IP Addresses

SNMPv3

Username

Engine ID (optional)

Authorization algorithm

Authorization password [Show](#)

Privacy algorithm (optional)

Privacy password (optional) [Show](#)

[Back](#) [Next](#) [Cancel](#)

Ajouter des informations d'identification

 Remarque : Pour l'image ci-dessus, l'affichage de la sélection de tous les protocoles à l'étape précédente est illustré. Votre interface affiche uniquement les protocoles que vous avez choisis.

7. Saisissez les informations de connexion pour chaque protocole sélectionné.

8. Cliquez sur Suivant.

Add Credentials

1. Credential Name and Protocols

2. Enter Login Details

3. Specify IP Addresses

Specify IP Addresses

Included IPs

e.g. *-*-*, 192.168.1.0/24, 172.16.*.*

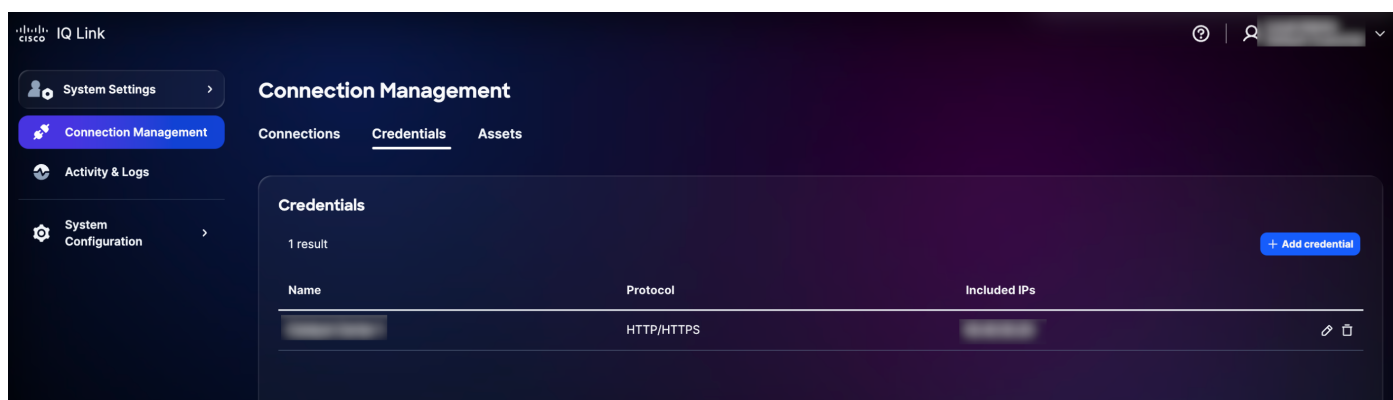
[Back](#) [Save and add another credential](#) [Save](#) [Cancel](#)

Spécifier les adresses IP

9. Saisissez les adresses IP incluses.

 Remarque : Ce champ définit les adresses IP ou les plages IP où les informations d'identification peuvent être utilisées pour établir une connexion. Il prend en charge une combinaison d'adresses IP et de masques IP (en utilisant la notation générique). Pour plus d'informations sur les formats pris en charge, consultez [Sélection des informations d'identification et logique de correspondance](#).

10. Cliquez sur Save. Une confirmation s'affiche et vous êtes redirigé vers l'onglet Informations d'identification.



Informations d'identification ajoutées

Vous pouvez modifier les informations d'identification en cliquant sur l'icône Modifier et les supprimer en cliquant sur l'icône Supprimer.

Sélection des informations d'identification et logique correspondante

Le moteur de télémétrie utilise une logique de correspondance basée sur la priorité pour déterminer quelles informations d'identification doivent être appliquées pendant la découverte et la collecte. La compréhension de cette hiérarchie permet de s'assurer que les informations d'identification correctes sont utilisées pour les périphériques prévus.

- Classement des priorités : Lorsque plusieurs jeux d'informations d'identification s'appliquent à un périphérique, Cisco IQ les évalue en fonction de leur correspondance spécifique avec le périphérique ; le système applique la priorité suivante, avec des correspondances plus spécifiques prioritaires :

- Correspondance IP exacte : Priorité la plus élevée
- Correspondance générique de fin : la priorité dépend du nombre d'étoiles de fin ; moins d'étoiles indiquent une correspondance plus spécifique et donc une priorité plus élevée
- Règles de mise en forme générique : Les caractères génériques (*) ne sont pris en charge que comme caractères de fin dans une adresse IP ; ils doivent être appliqués de droite à gauche.
 - Formats pris en charge :
 - 1.2.3.* (priorité la plus élevée)
 - 1.2.*.*
 - 1.*.*.*
 - *.*.*.* (priorité la plus basse)
 - Formats non pris en charge :
 - Caractères génériques de début (par exemple, *.1.2.3)
 - Caractères génériques entre les octets (par exemple, 10.10.*.20)
 - Utilisation de tirets ou d'autres délimiteurs non standard

Exemple de sélection des informations d'identification :

Le tableau suivant montre comment le moteur de télémétrie sélectionne l'ensemble d'informations d'identification le plus approprié lorsqu'un périphérique correspond à plusieurs modèles définis.

Tableau 1 : Exemple de sélection des informations d'identification

IP du périphérique	Jeux d'informations d'identification disponibles	Jeu d'identifiants sélectionné
10.10.1.5	10.10.1.5, 10.10.1, 10.10.1.*	10.10.1.5 (Correspondance exacte)
10.10.2.15	10.10.2, 10.10.2.*	10.10.2.* (plus spécifique)
10.10.5.50	10.10..., ...	10.10.. (Plus spécifique)

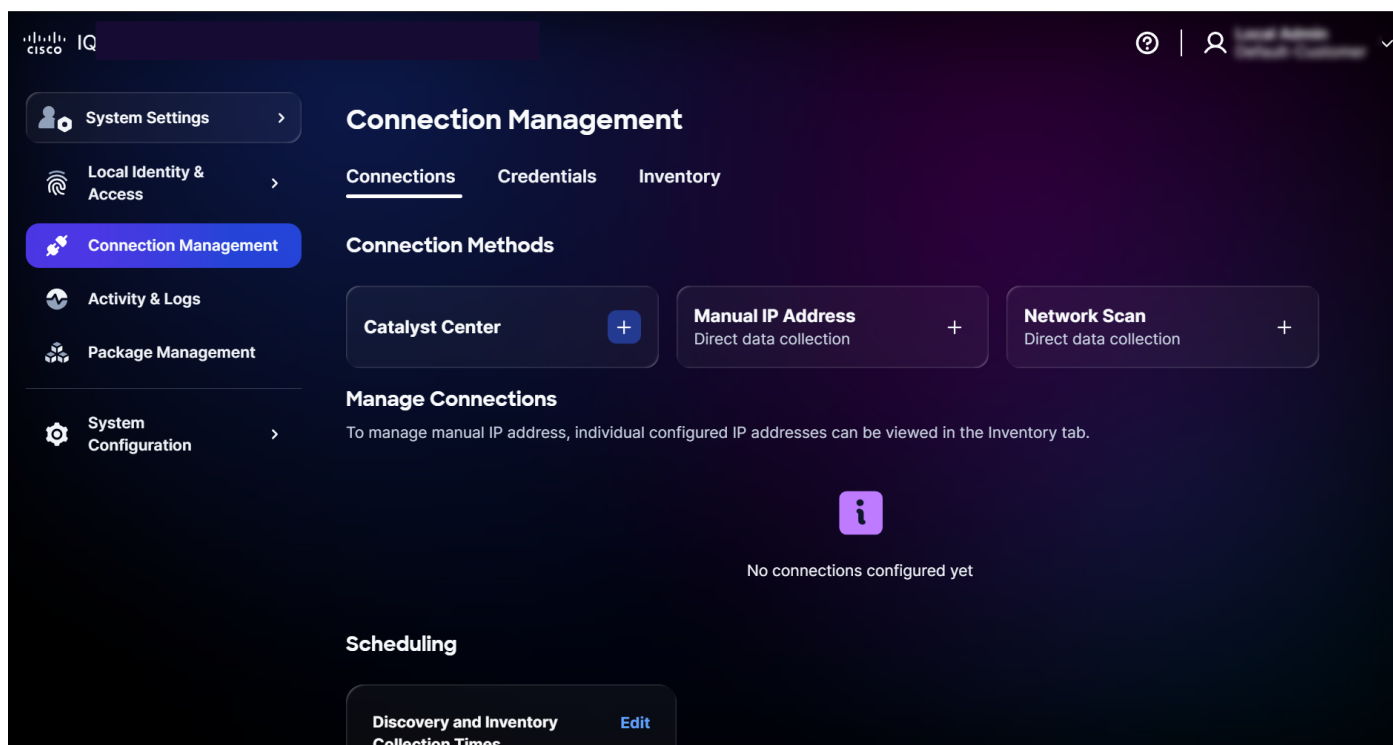
 Remarque : Si un périphérique appartient à plusieurs catégories qui se chevauchent, le système sélectionne toujours l'ensemble d'informations d'identification ayant la plus grande spécificité (en d'autres termes, le moins de caractères génériques de fin).

Collecte de données avec Catalyst Center

Vous pouvez connecter jusqu'à 20 centres Catalyst (hors cluster) pour chaque instance de Cisco IQ VA.

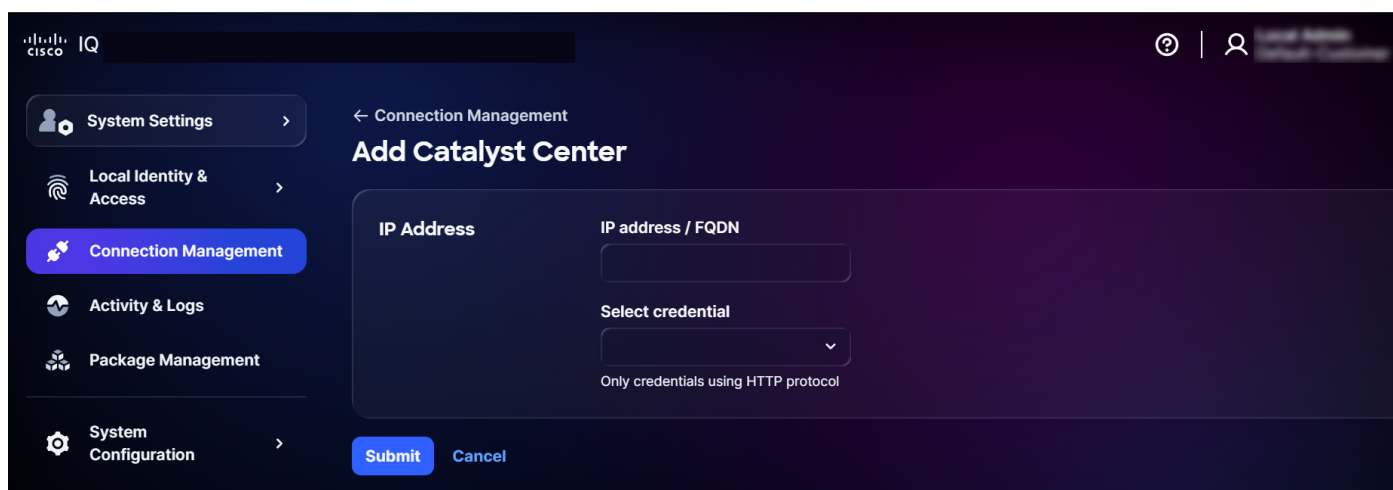
Pour la collecte de données avec Catalyst Center :

1. Dans Paramètres système, sélectionnez Gestion des connexions. La page Gestion des connexions s'affiche.



Gestion des connexions

2. Cliquez sur l'option Catalyst Center.



Ajouter Catalyst Center

3. Saisissez l'adresse IP ou le nom de domaine complet.
4. Sélectionnez une information d'identification HTTP/HTTPS configurée dans la liste

déroulante Sélectionner l'information d'identification.

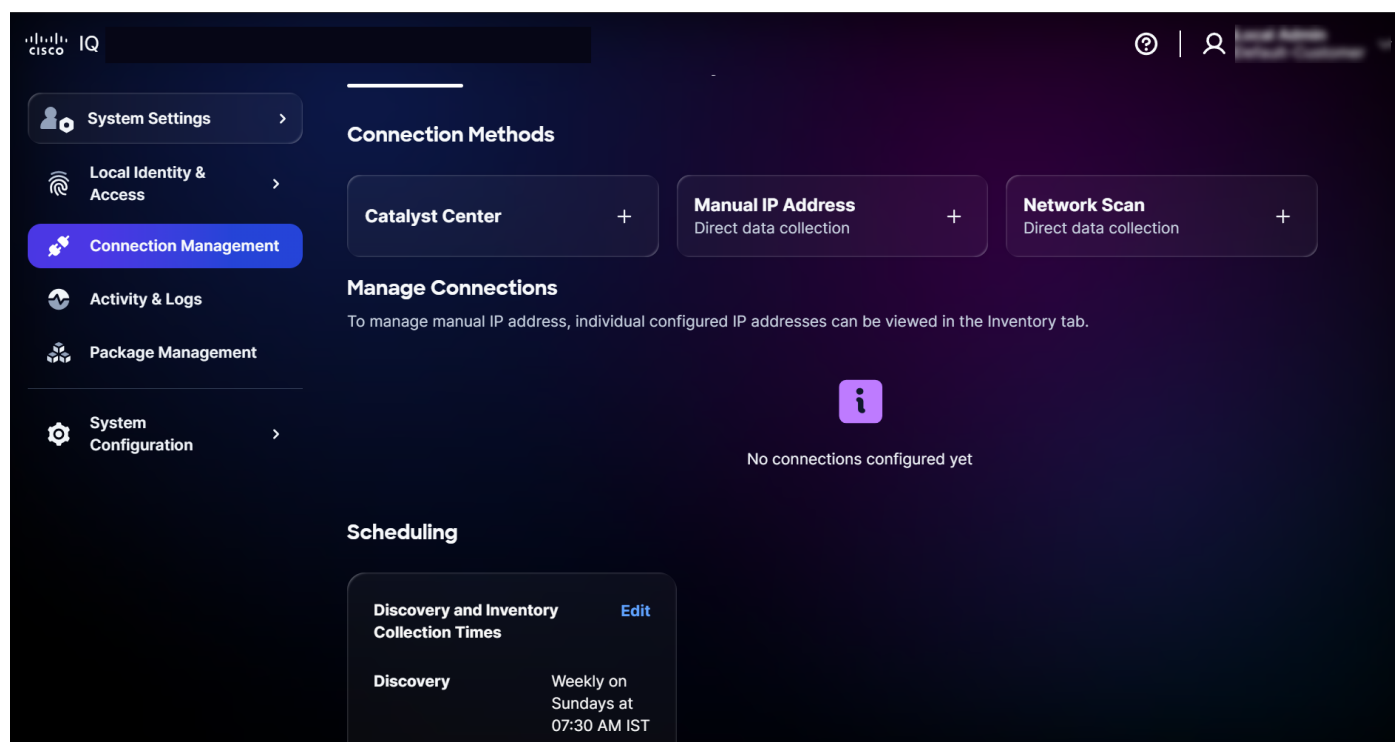
5. Cliquez sur Submit. Une confirmation s'affiche (jusqu'à 75 minutes). Vous pouvez afficher le Catalyst Center nouvellement ajouté sous Connexions configurées.
6. Planifier une collecte. Voir [Planification](#) pour plus de détails.

 Remarque : Cisco IQ VA est préconfiguré avec une configuration de planification automatique et le système lance une planification de collecte automatique par défaut. Il est vivement recommandé de modifier le planning afin de l'aligner sur les exigences de votre entreprise et les fenêtres de maintenance.

Collecte manuelle des données

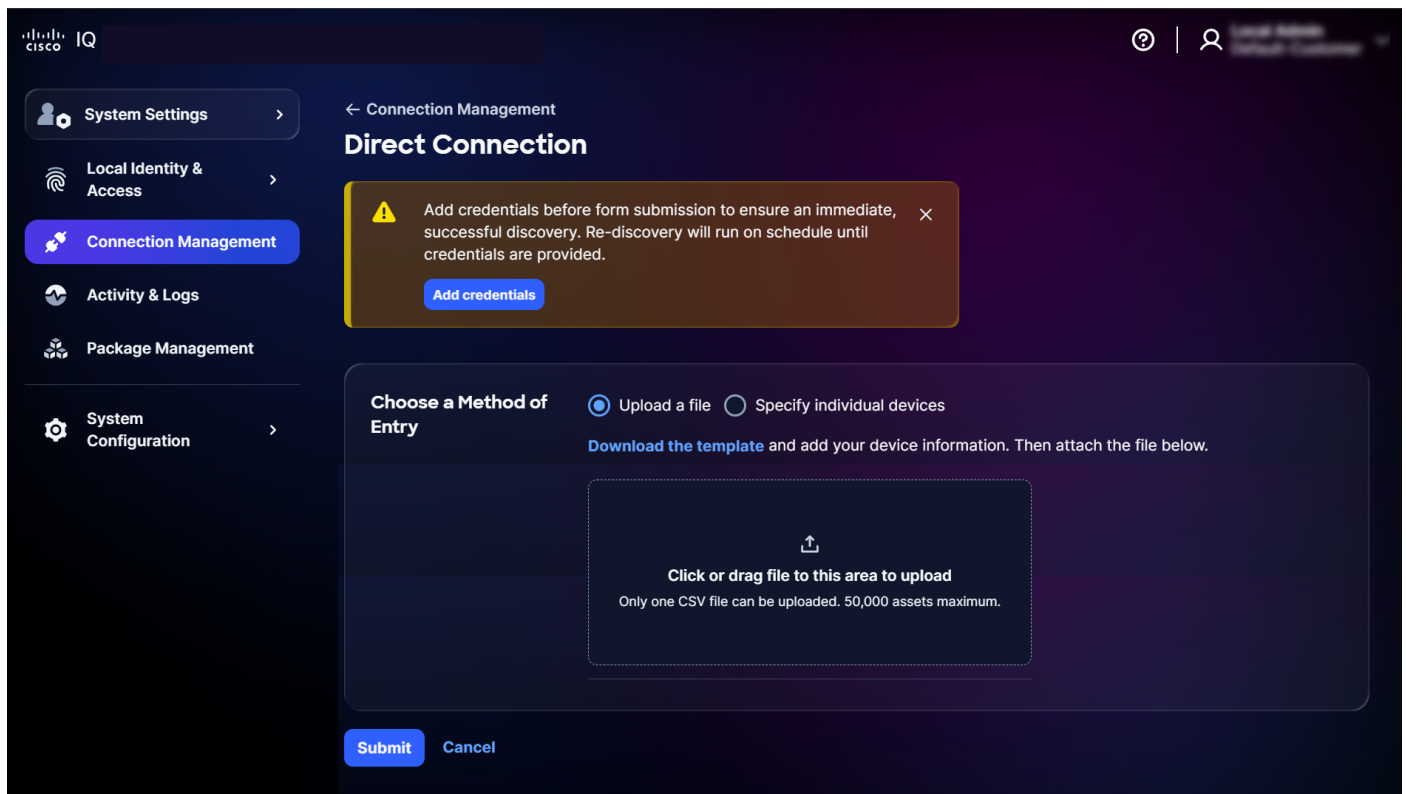
Pour ajouter des périphériques pour une connexion de données directe :

1. Dans Paramètres système, sélectionnez Gestion des connexions. La page Gestion des connexions s'affiche.



Gestion des connexions

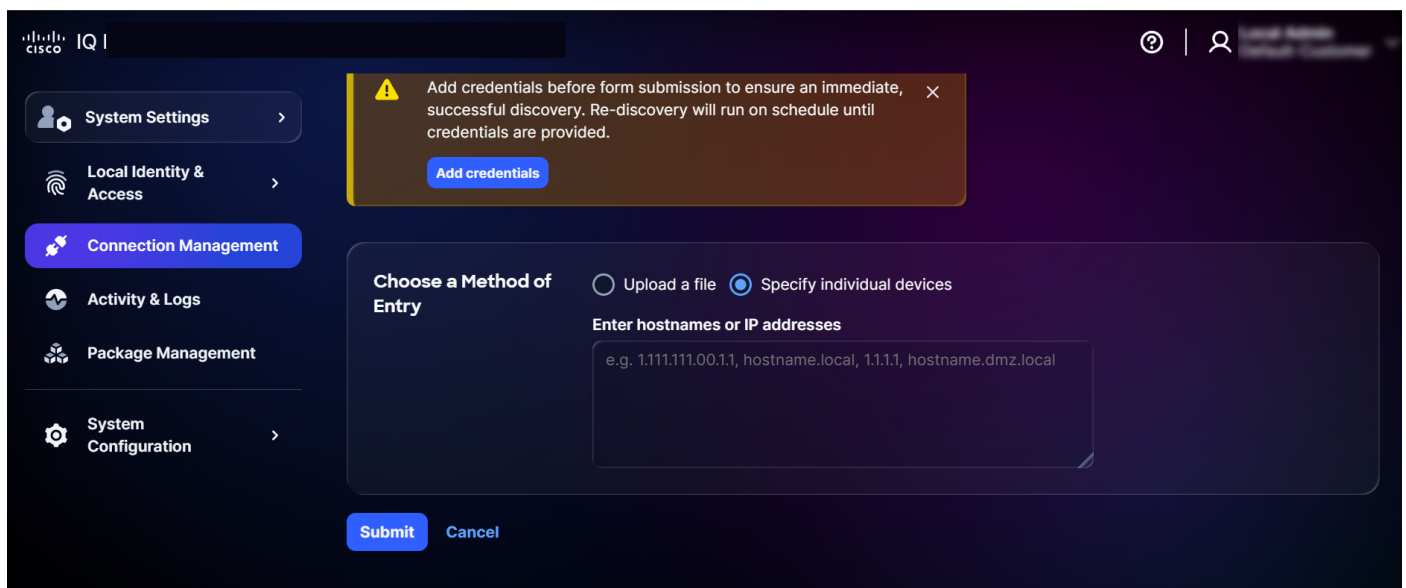
2. Cliquez sur Manual IP Address. La page Connexion directe s'affiche avec deux (2) options pour collecter des données.



Télécharger le fichier

3. Cliquez sur l'option préférée dans Choisir une méthode d'entrée et fournissez les informations sur votre périphérique en utilisant l'une des méthodes suivantes :

- Télécharger un fichier : Cliquez sur le fichier ou faites-le glisser



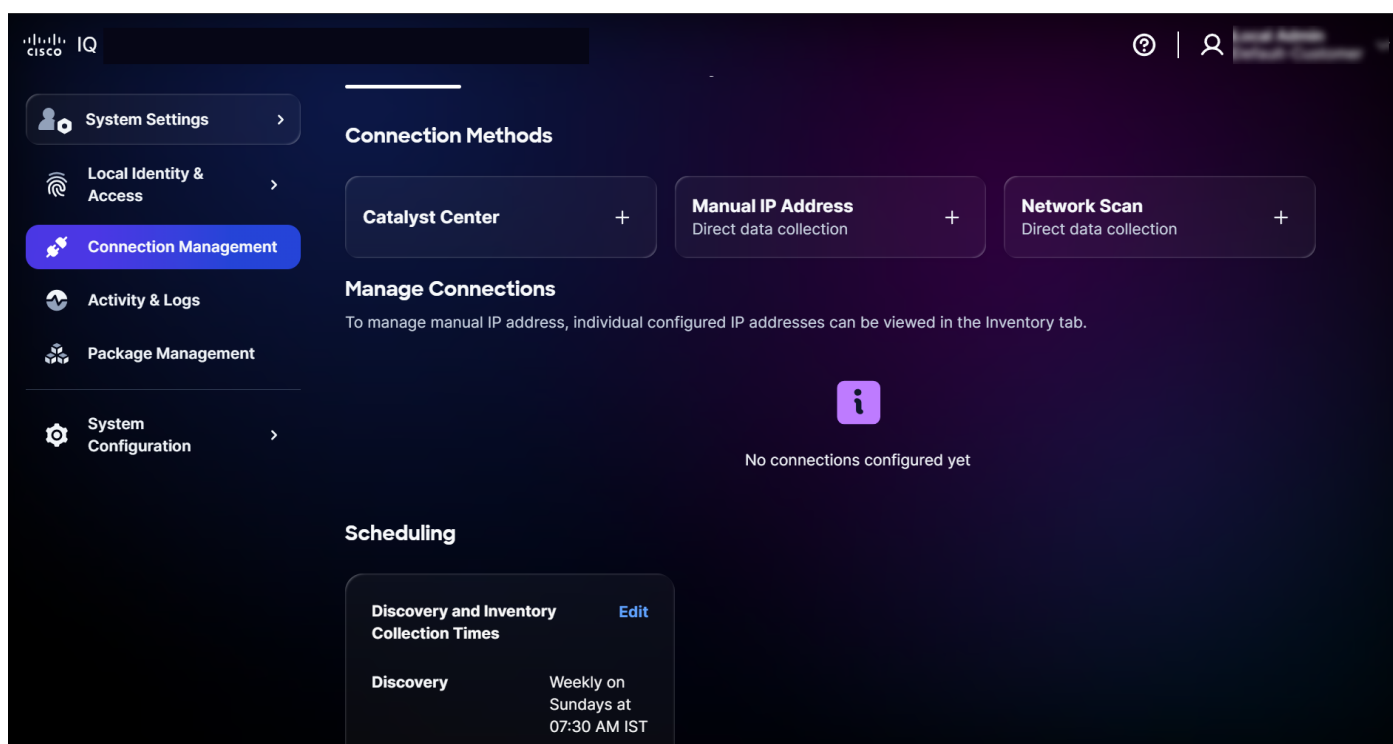
Spécifier des périphériques individuels

- Spécifier les périphériques individuels : Saisissez un nom d'hôte unique, des adresses IP ou une liste de noms d'hôtes et/ou d'adresses IP séparés par des virgules
4. Cliquez sur Submit. Vous êtes redirigé vers l'onglet Actifs après l'envoi réussi.
 5. Planifier une collecte. Voir [Planification](#) pour plus de détails.

 Remarque : Cisco IQ VA est préconfiguré avec une configuration de planification automatique et le système lance une planification de collecte automatique par défaut. Il est vivement recommandé de modifier le planning afin de l'aligner sur les exigences et les fenêtres de maintenance de votre entreprise.

Analyse du réseau

1. Dans Paramètres système, sélectionnez Gestion des connexions. La page Gestion des connexions s'affiche.



Analyse du réseau

2. Cliquez sur Network Scan. La page Connect Assets by Network Scan s'affiche avec trois (3) options.

- Spécifier la plage IP : Définir une plage d'adresses IP pour les équipements cibles dans cette plage pour les tâches de découverte ou de gestion du réseau
- Spécifier le protocole de découverte (CDP/LLDP) : Sélectionnez le protocole de détection de réseau à utiliser
- Téléchargement de fichier : Télécharger un fichier, tel que des fichiers de configuration ou des données

3. Saisissez Name.

4. Saisissez IP Start et IP End.

5. Sous Programmer le balayage, choisissez Fréquence et heure.

6. Cliquez sur Connecter les ressources.

Planification

La planification vous permet de définir le moment où Cisco IQ VA effectue la collecte automatisée des données. Pour planifier la collecte :

1. Dans la section Planification de la page Gestion des connexions, cliquez sur Modifier pour la planification que vous souhaitez modifier. La page Modifier la planification s'affiche.

The screenshot shows the Cisco IQ 'Edit Schedule' configuration page. On the left, a sidebar lists navigation items: System Settings, Local Identity & Access, Connection Management (selected), Activity & Logs, Package Management, and System Configuration. The main content area is titled 'Edit Schedule' and features two configuration sections. The 'Schedule Discovery' section includes a 'Frequency' dropdown set to 'Weekly', a 'Time' field set to '07:30', and a 'Day' dropdown set to 'Sunday'. The 'Schedule Inventory Collection' section includes a 'Frequency' dropdown set to 'Daily', a 'Time' field set to '05:30', and a clock icon with 'IST'. At the bottom of the main area are 'Submit' and 'Cancel' buttons.

Modifier la planification

2. Dans la section Schedule Discovery, choisissez votre fréquence et votre jour préférés dans les listes déroulantes et entrez l'heure de début souhaitée.
3. Dans la section Schedule Inventory Collection, choisissez votre fréquence préférée dans les listes déroulantes et entrez l'heure de début souhaitée.
4. Cliquez sur Submit.

 Remarque : Prévoyez entre 5 et 10 minutes pour que les modifications apportées aux calendriers de détection ou de collecte soient synchronisées et reflétées avec précision au sein de l'appliance virtuelle.

Installation des packages (modules, règles et droits)

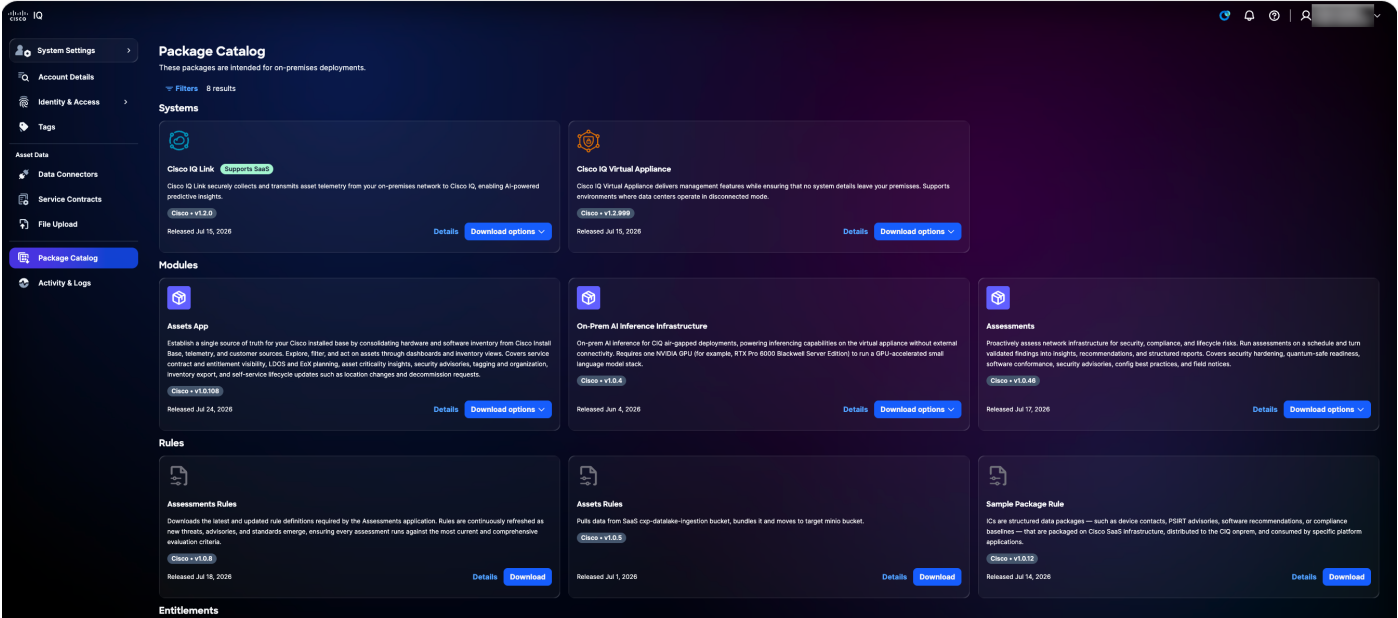
Vous pouvez gérer le cycle de vie du logiciel (c'est-à-dire l'installation et la configuration) des modules opérationnels, des règles, des droits et des fonctions IA spécialisées au sein de l'appliance virtuelle. Vous pouvez les installer en téléchargeant les dernières versions de Cisco IQ (SaaS) en naviguant vers le catalogue de packages. Le catalogue de packages affiche les instances logicielles à votre disposition. Il vous permet de surveiller et de gérer les mises à jour en toute transparence, garantissant ainsi un suivi et une gestion efficaces de vos instances système.

Ajout de modules

Un module est un progiciel autonome qui fournit des fonctionnalités de base au sein de l'appliance virtuelle. Il s'agit d'un service indépendant avec son propre cycle de vie, permettant l'installation, la maintenance et le redimensionnement. La consommation des ressources, notamment le

processeur, l'unité de traitement graphique (GPU) et la mémoire vive, est attribuée de manière dynamique en fonction de la taille de déploiement (petite, moyenne ou grande) sélectionnée lors de l'installation initiale.

- 1. Connectez-vous à [Cisco IQ](#).
- 2. Accédez à Paramètres système > Catalogue de packages.



Catalogue de packages

- 3. Dans la carte de module souhaitée, cliquez sur Options de téléchargement > Packages d'installation. La fenêtre Télécharger s'affiche.



Remarque : Le module d'évaluation est utilisé pour les exemples d'images.

Download Assessments

System version

System v1.2.0

Build type

Application version

-

Cancel

Download

Télécharger

4. Sélectionnez une version du système dans la liste déroulante.

5. Sélectionnez un type de build dans la liste déroulante.

6. Cliquez sur Download pour enregistrer le fichier localement.

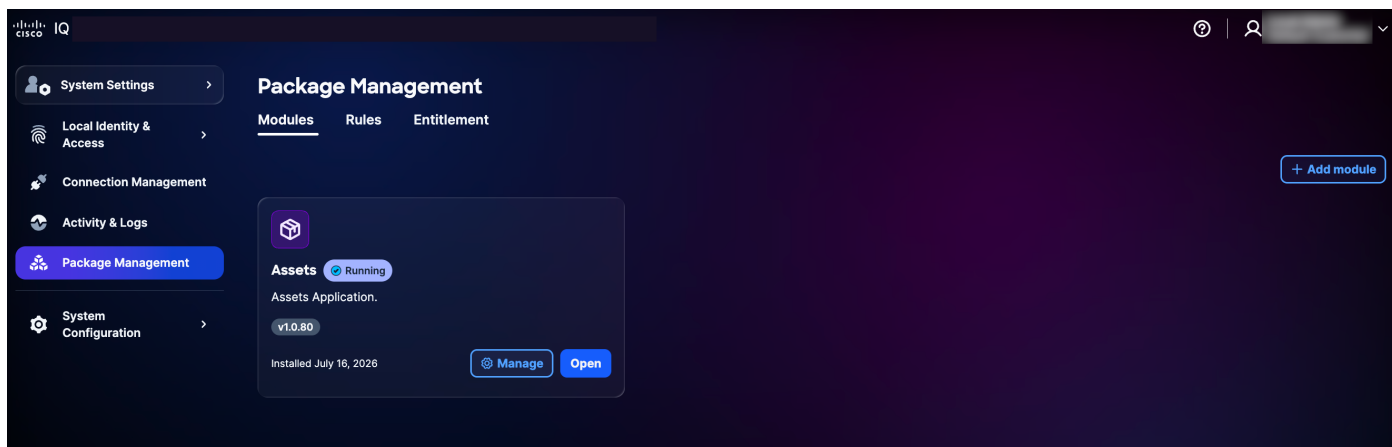


Remarque : Les fichiers d'installation sont volumineux (10-25 Go) ; assurez-vous que vous disposez d'un espace disque suffisant avant de télécharger.

7. Accédez à VA.

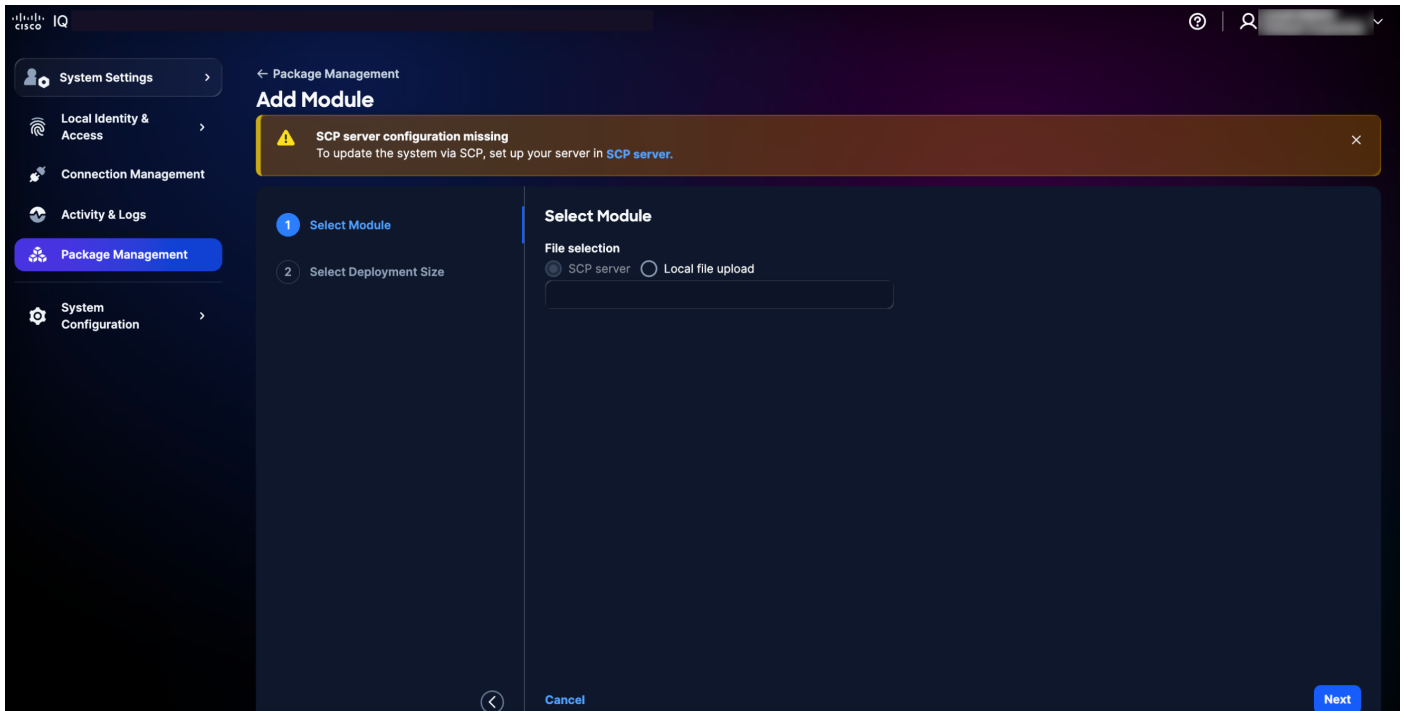
8. Accédez à Home > System Settings > Package Management. La page Gestion des packages s'affiche avec les onglets suivants :

- Modules
- Règles
- Droits



Modules

9. Cliquez sur Add module.

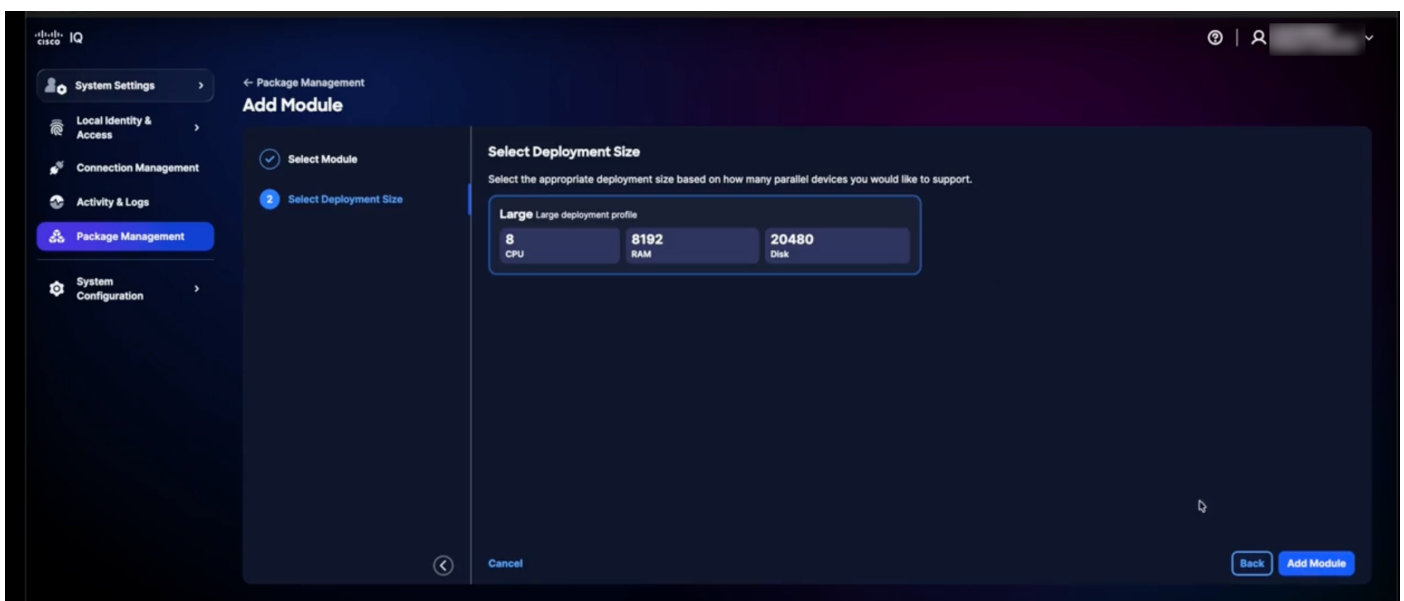


Ajouter un module

10. Choisissez votre option de sélection de fichier préférée :

- Serveur SCP : Entrez le nom exact du package d'installation (recommandé pour les fichiers volumineux)
- Téléchargement de fichier local : Glissez-déposez le fichier d'installation téléchargé (déconseillé pour les fichiers de 30 Go ou plus en raison du temps de téléchargement)

11. Cliquez sur Suivant.

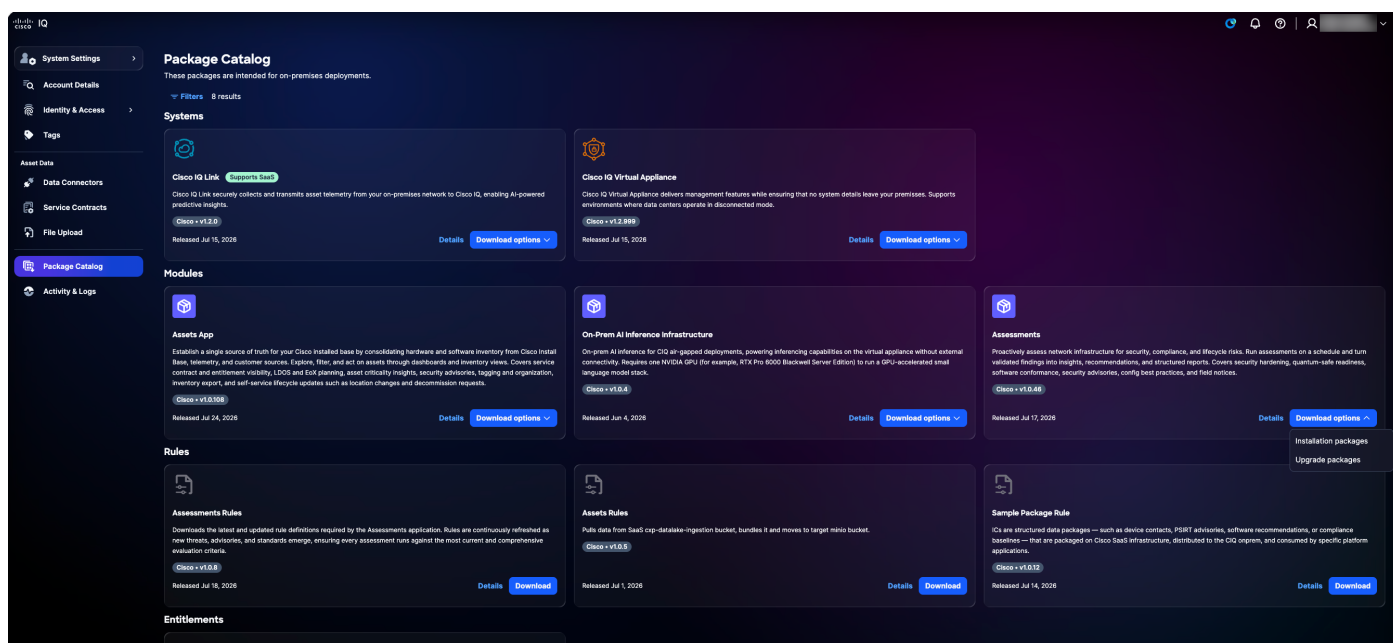


Taille du déploiement

12. Sélectionnez la taille de déploiement (par exemple, Petit, Moyen ou Grand). Ces tailles sont prédéfinies et dictent les besoins en ressources.
13. Cliquez sur Ajouter un module. Le module nouvellement installé s'affiche dans l'onglet Modules de la Gestion des packages. Une fois terminé, l'état du module passe à « En cours d'exécution » et le bouton Ouvrir devient disponible.

Mise à niveau d'un module

Les derniers Cisco modules sont continuellement mis à jour dans le catalogue de packages (dans Cisco IQ). Pour effectuer une mise à niveau vers la dernière version :



Connexion des ressources par analyse du réseau

1. Dans la carte de module souhaitée, cliquez sur Download options > Upgrade packages. La fenêtre Télécharger s'affiche.



Remarque : Le module Évaluation est utilisé comme exemple pour les images.

Upgrade Assessments

System version

System v1.2.0



Current app version



Build type



Application version

-

Cancel

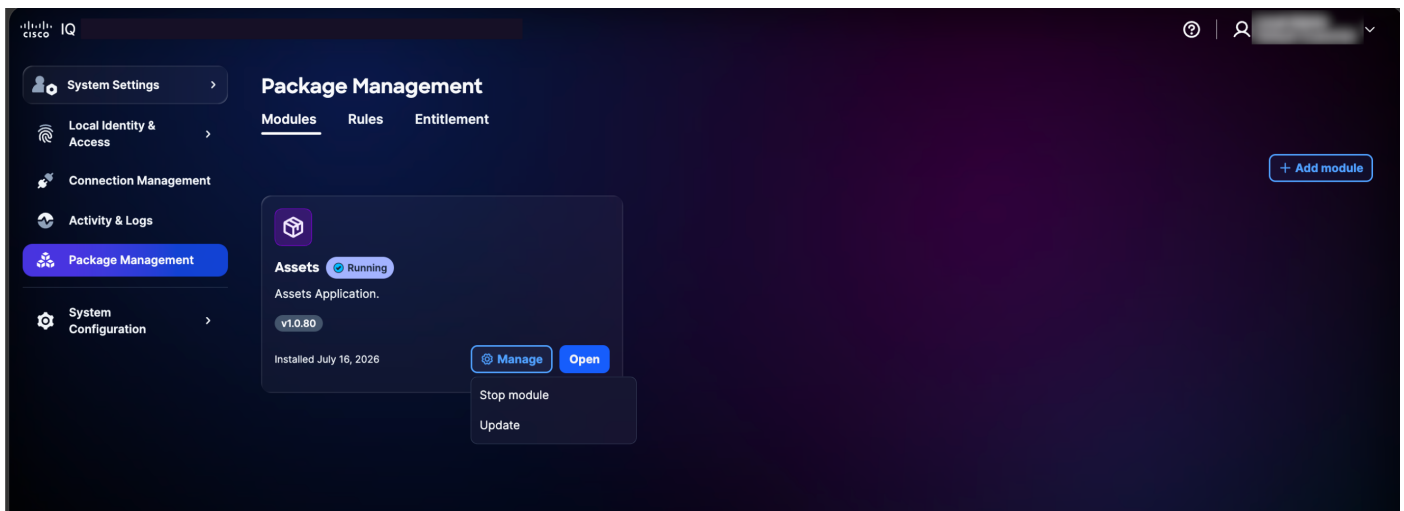
Download

Télécharger

2. Sélectionnez une version du système dans la liste déroulante.
3. Sélectionnez une version d'application actuelle dans la liste déroulante.
4. Sélectionnez un type de build dans la liste déroulante.
5. Cliquez sur Download pour enregistrer le fichier localement.
6. Accédez à VA et terminez l'installation du fichier téléchargé.

Gestion des modules

Après avoir ajouté un module, vous pouvez le modifier à partir de la page Gestion de package en cliquant sur Gérer. Les options de modification disponibles incluent le redimensionnement et la mise à niveau vers une version supérieure. Pour gérer un module :



Type de mise à jour

1. Dans la page Package Management, cliquez sur Manage > Update pour le module souhaité.
2. Sélectionnez le type de mise à jour :
 - Modifier la taille du déploiement uniquement
 - Mettre à jour version

3. Si l'option Modifier la taille de déploiement est sélectionnée, cliquez sur Suivant et choisissez la nouvelle taille de déploiement sur la page suivante.

OU

Si l'option Mettre à jour la version est sélectionnée, l'option Sélection de fichier s'affiche. Choisissez SCP Server et entrez le nom de fichier exact du package d'installation ou choisissez Local file upload et faites glisser le fichier d'installation téléchargé.

4. Cliquez sur Suivant. La page Sélectionner une planification de mise à jour s'affiche.
5. Choisissez l'une des options de case d'option suivantes pour mettre à jour la planification :
 - Mettre à jour maintenant
 - Mettre à jour ultérieurement



Remarque : Certains modules prennent en charge les mises à jour sans interruption. Si un temps d'arrêt est requis, une bannière affiche les détails.

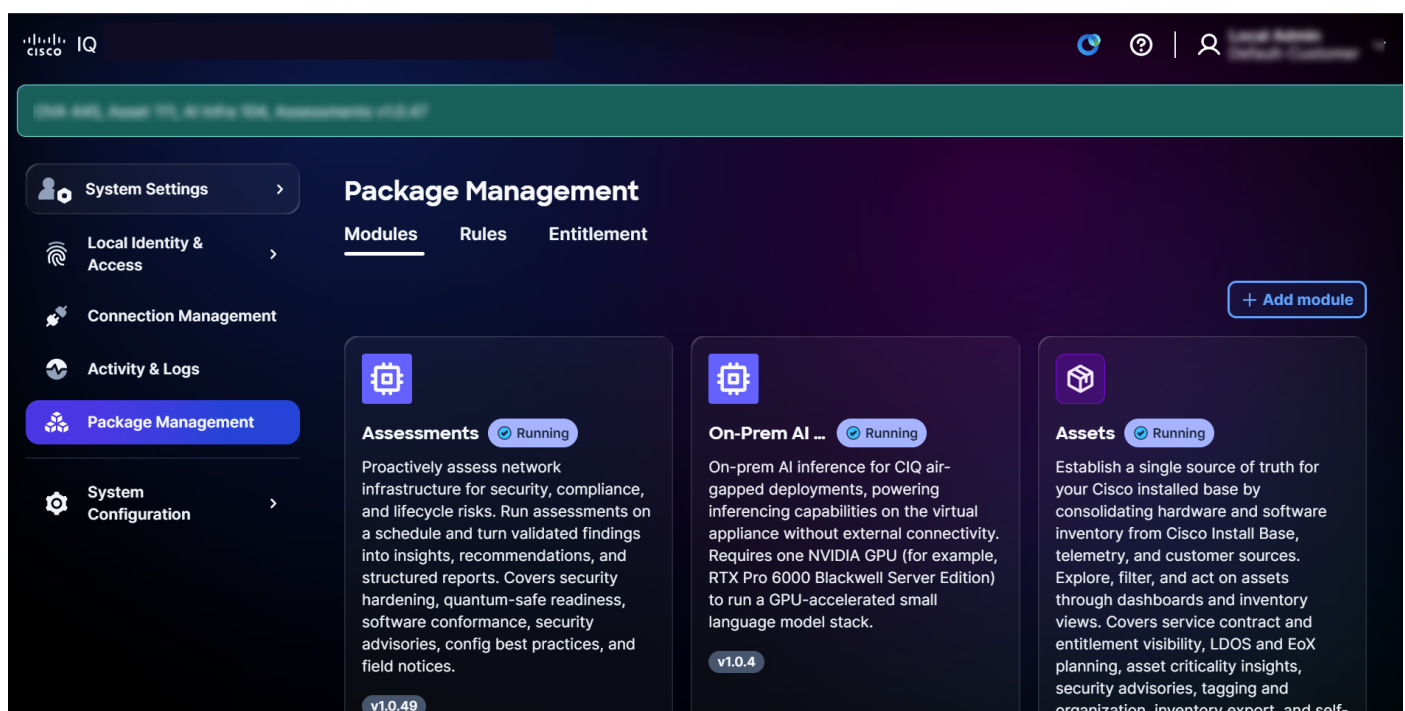
6. Si l'option Mettre à jour ultérieurement est sélectionnée, entrez la date et l'heure.
7. Cliquez sur Suivant. Le récapitulatif des mises à jour s'affiche.

 Remarque : Vous pouvez accéder aux Notes de version à partir du Résumé des mises à jour.

8. Cliquez sur Update Module et accédez à l'onglet Module. Le module affiche l'état « mise à jour planifiée ».

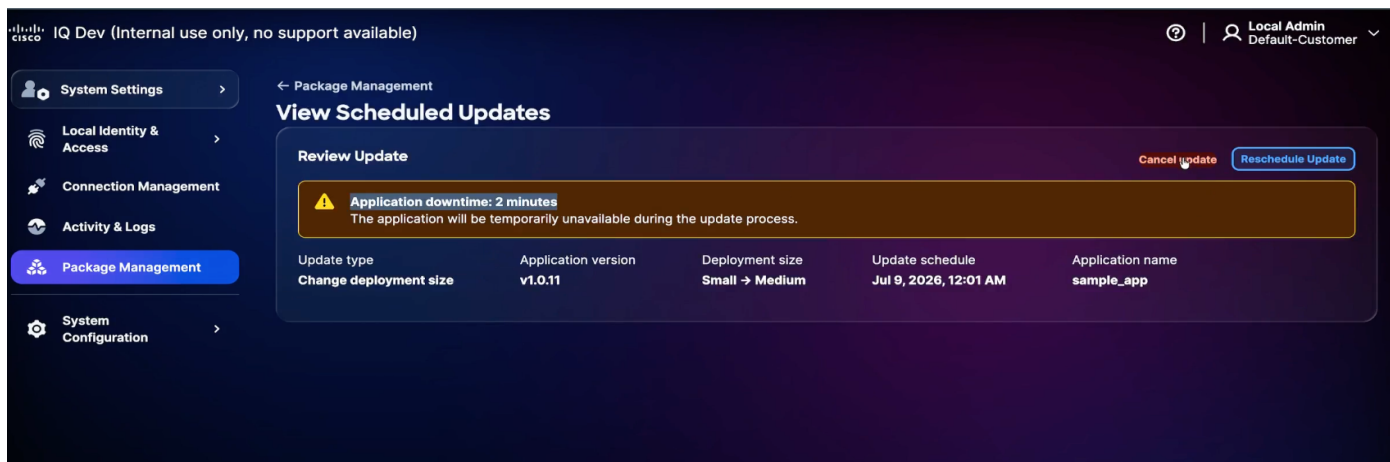
Modification des plannings

Vous pouvez également afficher, modifier ou annuler les mises à jour planifiées. Pour modifier ou annuler une mise à jour planifiée :



Modification du planning

1. Sur la page Package Management, cliquez sur Manage > View Scheduled update du module souhaité. La fenêtre Afficher les mises à jour planifiées s'affiche.



Planifier les mises à jour

2. Cliquez sur Annuler la mise à jour ou Replanifier la mise à jour si nécessaire.
3. Suivez les instructions à l'écran pour effectuer les opérations.

 Remarque : Si une opération de module (par exemple, l'installation, la mise à niveau ou le redimensionnement) échoue, choisissez l'une des options suivantes :

Réessayer : L'interface utilisateur affiche un bouton Réessayer, qui vous permet de recommencer l'opération. Journaux : Si une erreur persiste, cliquez sur Journaux pour afficher des informations de diagnostic détaillées. Il s'agit de la principale méthode permettant d'identifier la cause des échecs d'installation ou d'exécution.

Installation des règles

Une règle est un composant spécialisé ou un module complémentaire qui étend ou modifie la fonctionnalité d'un module existant. Les règles ne sont pas conçues pour s'exécuter en tant que programmes autonomes ; ils sont « branchés » à un module pour fournir des règles, une logique ou des fonctionnalités spécifiques. Les règles sont liées à des modules spécifiques. Lorsqu'une règle est installée, elle est liée au module qu'elle prend en charge. Les règles permettent de mettre à jour ou de personnaliser le système sans nécessiter une mise à niveau complète du module principal. Si un nouvel ensemble de règles ou de fonctionnalités est nécessaire, vous pouvez simplement ajouter une nouvelle règle au module existant.

Pour télécharger une règle :

1. Connectez-vous à [Cisco IQ](#).

2. Accédez à System Settings > Package Catalog.
3. Dans la fiche de règles souhaitée, cliquez sur Download.



Remarque : L'exemple d'image suivant concerne une règle Assets.

Download Assets Rules

Target app version

assets v1.0.0



Cancel

Download

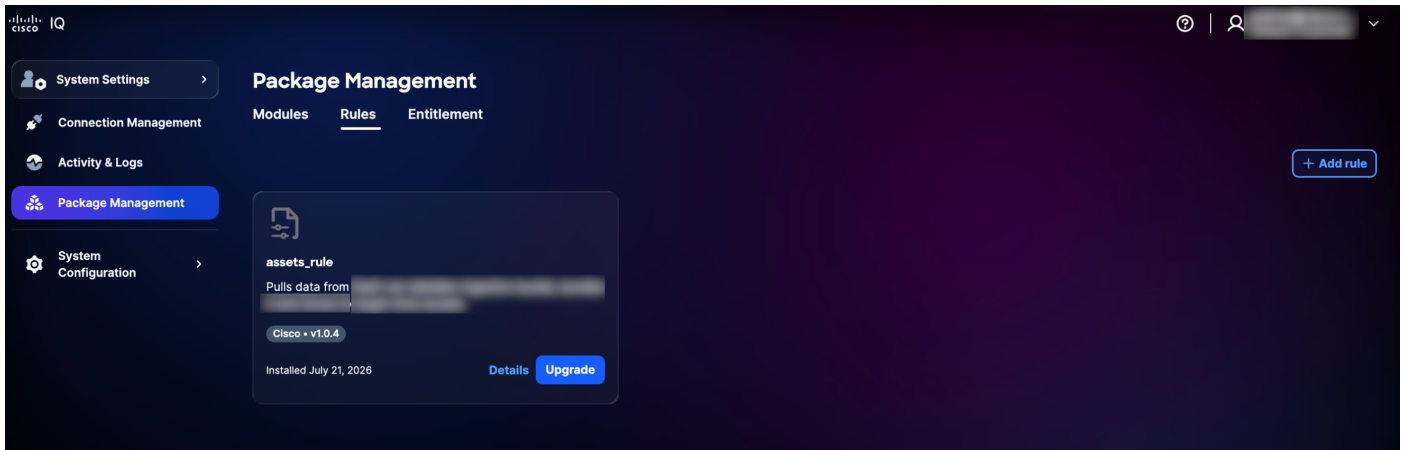
Télécharger

4. Sélectionnez une version d'application cible dans la liste déroulante.
5. Cliquez sur Download pour enregistrer le fichier localement.



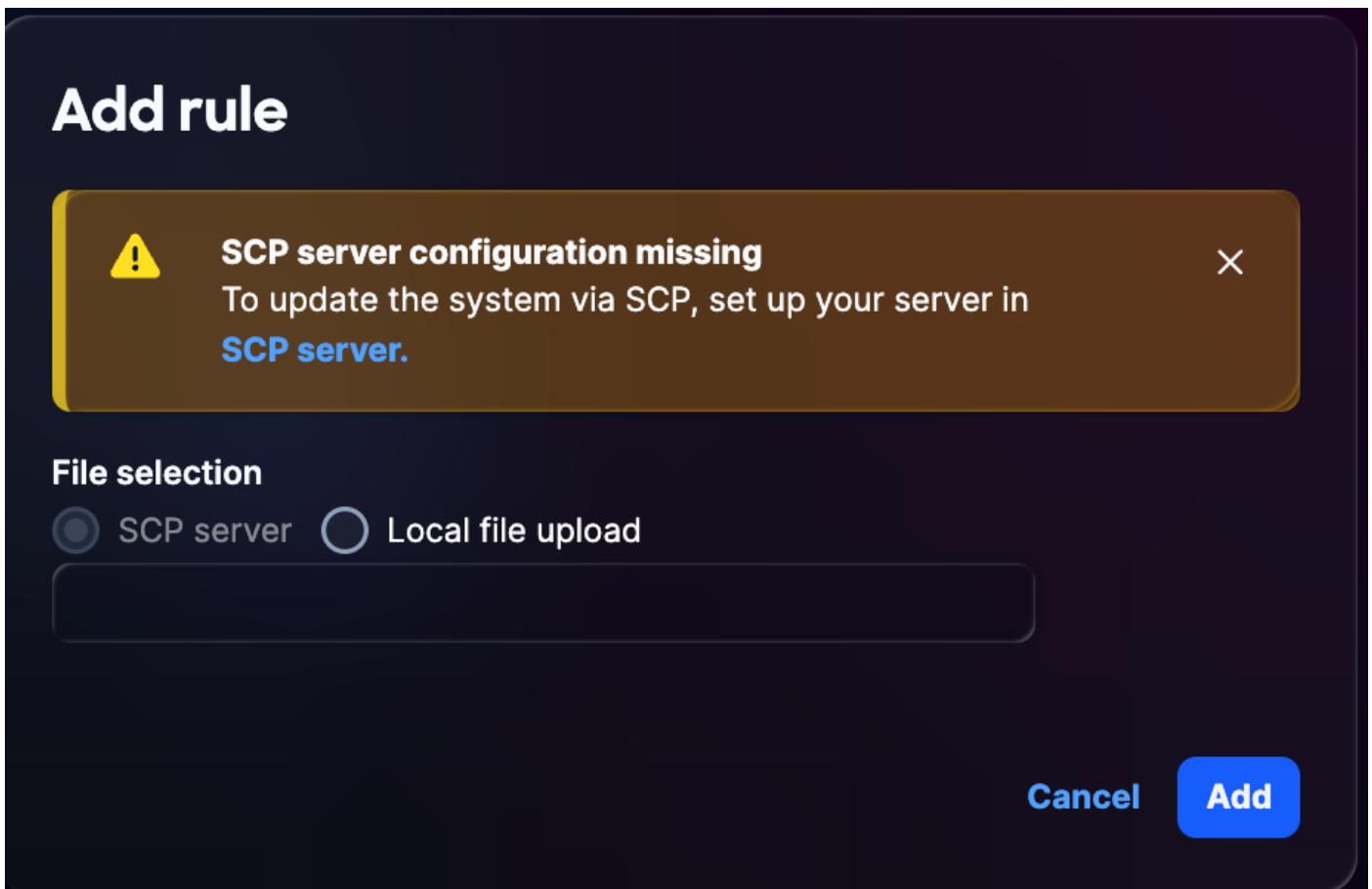
Remarque : Les fichiers d'installation sont volumineux (10-25 Go) ; assurez-vous que vous disposez d'un espace disque suffisant avant de télécharger.

6. Accédez à VA.
7. Accédez à Home > System Settings > Package Management. La page Gestion des packages s'affiche avec les onglets suivants.
 - Modules
 - Règles
 - Droits
8. Cliquez sur l'onglet Règles.



Gestion des packages

9. Cliquez sur Ajouter une règle.



Ajouter une règle

10. Choisissez votre option de sélection de fichier préférée :

- Serveur Secure Copy Protocol (SCP) : Entrez le nom de fichier exact du package

d'installation. Cette méthode est recommandée pour les fichiers volumineux.

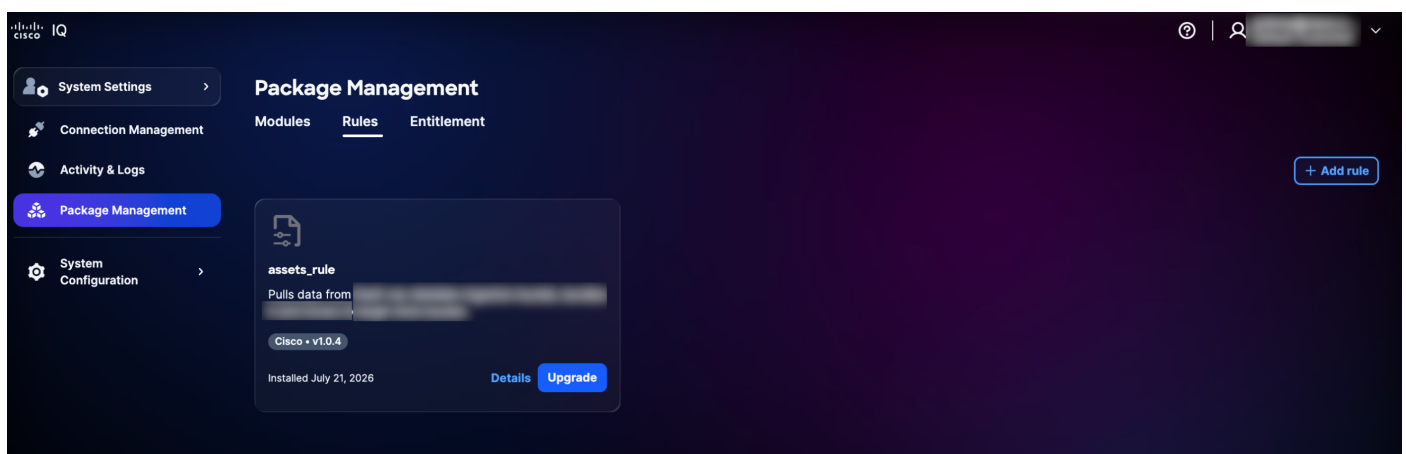
- Téléchargement de fichier local : Glissez-déposez le fichier d'installation téléchargé.

11. Cliquez sur Ajouter. La règle ajoutée s'affiche dans Gestion des packages.

Mise à niveau des règles

Pour mettre à niveau les règles :

1. Accédez à System Settings > Package Management dans VA.



Mise à niveau

2. Dans la règle souhaitée, cliquez sur Upgrade. La fenêtre Upgrade Rule s'ouvre.

Upgrade Rule

File selection

☒ SCP server ☐ Local file upload

Cancel

Add

Règle de mise à niveau

3. Choisissez votre option de sélection de fichier préférée :

- Serveur Secure Copy Protocol (SCP) : Entrez le nom de fichier exact du package d'installation. Cette méthode est recommandée pour les fichiers volumineux.
- Téléchargement de fichier local : Glissez-déposez le fichier d'installation téléchargé.

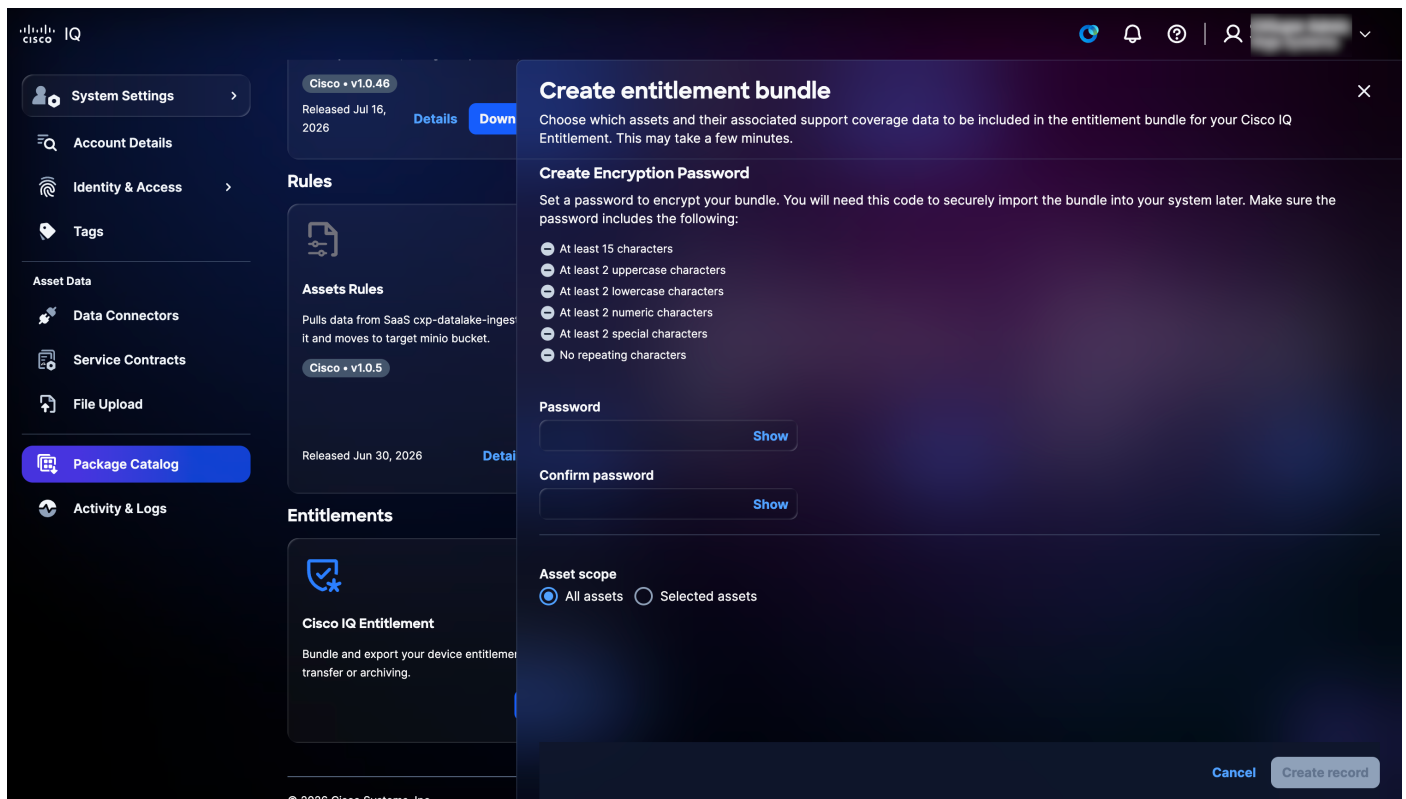
4. Cliquez sur Ajouter.

 Remarque : Ces règles sont appliquées au niveau de la collecte de télémétrie périodique planifiée des périphériques. Pour une application immédiate, vous pouvez lancer manuellement la collecte de télémétrie des périphériques.

Installation des droits

Un Justificatif permet de valider le droit de votre entreprise à utiliser des fonctionnalités logicielles, des modules ou des services spécifiques. Pour installer un droit :

1. Connectez-vous à [Cisco IQ](#).
2. Accédez à Paramètres système > Catalogue de packages.
3. Dans la carte de droits, cliquez sur Créer un enregistrement. La fenêtre Créer un lot de droits s'affiche.



Créer un bundle de droits

4. Saisissez un mot de passe. Reportez-vous aux règles de création de mot de passe qui s'affichent à l'écran.
5. Entrez à nouveau le même mot de passe dans Confirmer le mot de passe.
6. Sélectionnez la case d'option Étendue de l'actif préférée.
 - Toutes les ressources : Inclut toutes les ressources qui vous sont liées
 - Ressources sélectionnées : Vous permet de sélectionner des périphériques spécifiques en fonction de votre environnement ; si cette option est sélectionnée, cochez les cases de toutes les ressources applicables
7. Cliquez sur Créer un enregistrement pour enregistrer le fichier localement.



Remarque : Après avoir créé l'ensemble de droits, ne quittez pas l'écran actuel. Si vous accédez à une autre page, l'offre groupée est invalidée et vous devez la régénérer pour activer l'option de téléchargement.



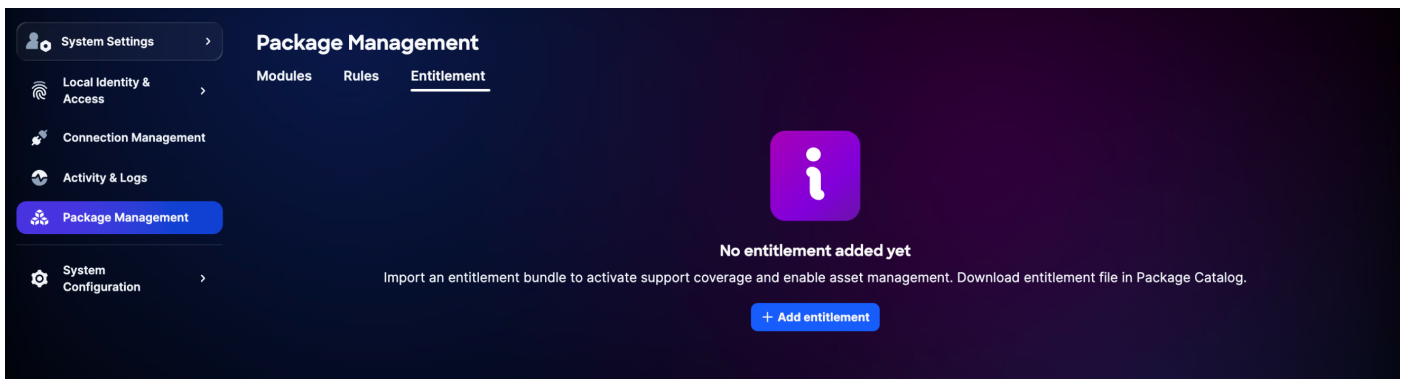
Remarque : Les fichiers d'installation sont volumineux (10-25 Go) ; assurez-vous que vous disposez d'un espace disque suffisant avant de télécharger.

8. Connectez-vous à VA.

9. Accédez à Home > System Settings > Package Management. La page Gestion des packages contient les onglets suivants :

- Modules
- Règles
- Droits

10. Cliquez sur l'onglet Droits.



Onglet Autorisation

11. Cliquez sur Ajouter un droit.

Add Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

[Show](#)[Cancel](#)[Add](#)

Ajouter un droit

12. Sélectionnez l'option de sélection de fichier que vous préférez.

- Serveur Secure Copy Protocol (SCP) : Entrez le nom de fichier exact du package d'installation ; cette méthode est recommandée pour les fichiers volumineux
- Téléchargement de fichier local : Glissez-déposez le fichier d'installation téléchargé

13. Saisissez un mot de passe.

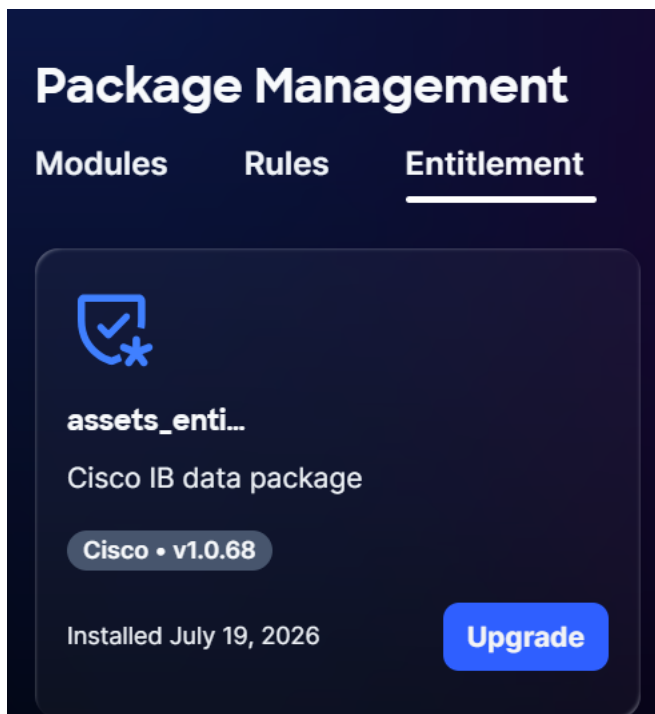
14. Cliquez sur Ajouter. Le droit nouvellement installé s'affiche dans l'onglet Droits dans Gestion des packages.

15. Pour activer les droits, attendez 5 à 10 minutes après les avoir ajoutés, puis lancez la collecte de télémétrie du périphérique.

 Remarque : L'ajout d'un contrat de service dans le processus d'autorisation ajoute tous les périphériques liés à ce contrat à l'inventaire des périphériques sur site. Vous avez la possibilité de filtrer les périphériques par numéro de série, d'utiliser plusieurs ID de compte ou de sélectionner des périphériques spécifiques pour gérer les droits.

Mise à niveau des droits

Pour mettre à niveau un droit :



Mise à niveau des droits

1. Dans le champ Entitlement, cliquez sur Upgrade.

Upgrade Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

[Show](#)[Cancel](#)[Add](#)

Droit de mise à niveau

2. Choisissez votre option de sélection de fichier préférée :

- Serveur Secure Copy Protocol (SCP) : Entrez le nom de fichier exact du package d'installation ; cette méthode est recommandée pour les fichiers volumineux
- Téléchargement de fichier local : Glissez-déposez le fichier d'installation téléchargé

3. Saisissez un mot de passe.

4. Cliquez sur Ajouter.

Fonctionnalités AI-Powered

Le module d'infrastructure d'inférence AI sur site offre des fonctionnalités IA sur site dans VA. Il exécute un modèle SLM (Small Language Model) localement, permettant au système de répondre aux invites de l'IA. Une fois installé, vous pouvez interagir directement avec lui dans l'interface VA.

Les types de requête suivants sont pris en charge :

- Ressources : Identifier les ressources à risque en raison de l'état de fin de vie, de la non-conformité ou de la mise à jour des logiciels, des failles de sécurité et des lacunes de couverture du contrat
- Stocks: Demander une analyse basée sur l'intelligence artificielle des ressources de votre inventaire

Le package d'installation On-Prem AI Inference Infrastructure est disponible dans le catalogue de packages Cisco IQ et est distribué de la même manière que d'autres modules, tels que Assets.

 Remarque : Une seule (1) infrastructure d'inférence AI locale peut être exécutée par GPU à la fois. L'installation prend environ 40 à 45 minutes. Les fichiers d'installation sont volumineux (environ 30 Go) ; assurez-vous que vous disposez d'un espace disque suffisant avant de télécharger.

Prérequis pour l'infrastructure d'inférence AI locale

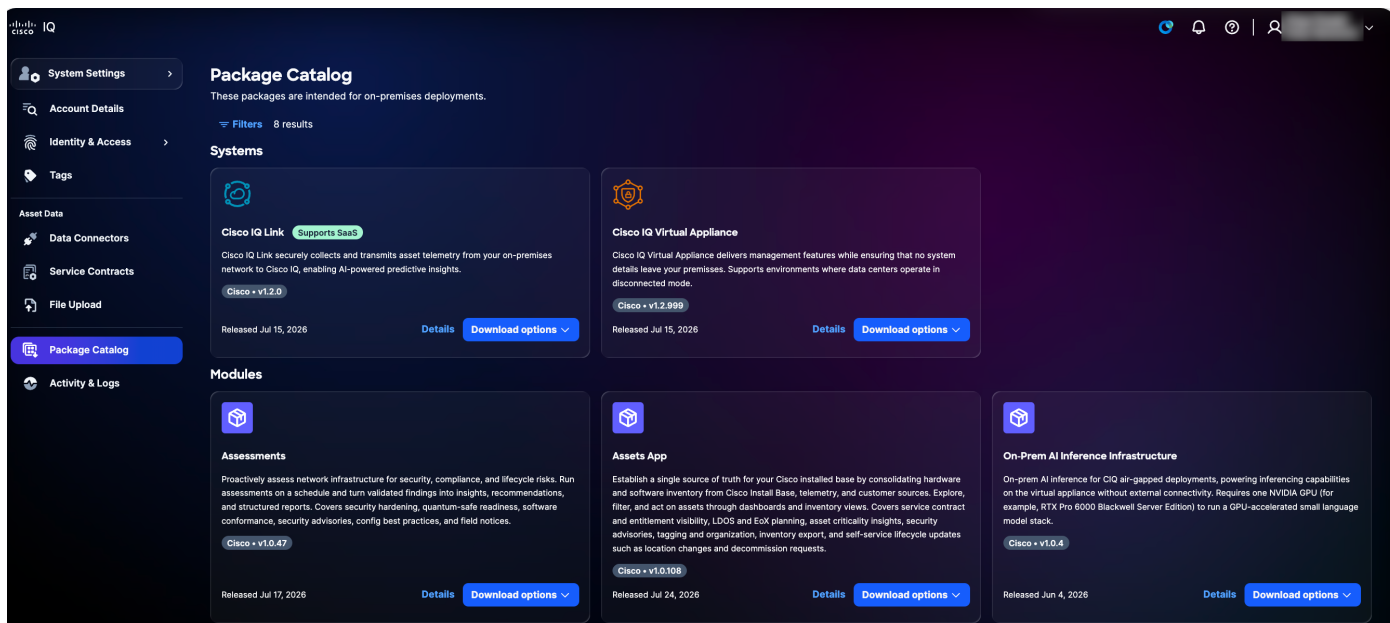
Avant d'installer l'infrastructure d'inférence AI sur site, les conditions suivantes doivent être remplies :

- L'appliance virtuelle doit inclure une machine virtuelle avec un accès GPU ; le SLM nécessite un processeur graphique et ne peut pas s'exécuter sans
- La machine virtuelle GPU doit disposer d'au moins 80 Go de mémoire VRAM GPU

Installation de l'infrastructure d'inférence AI locale

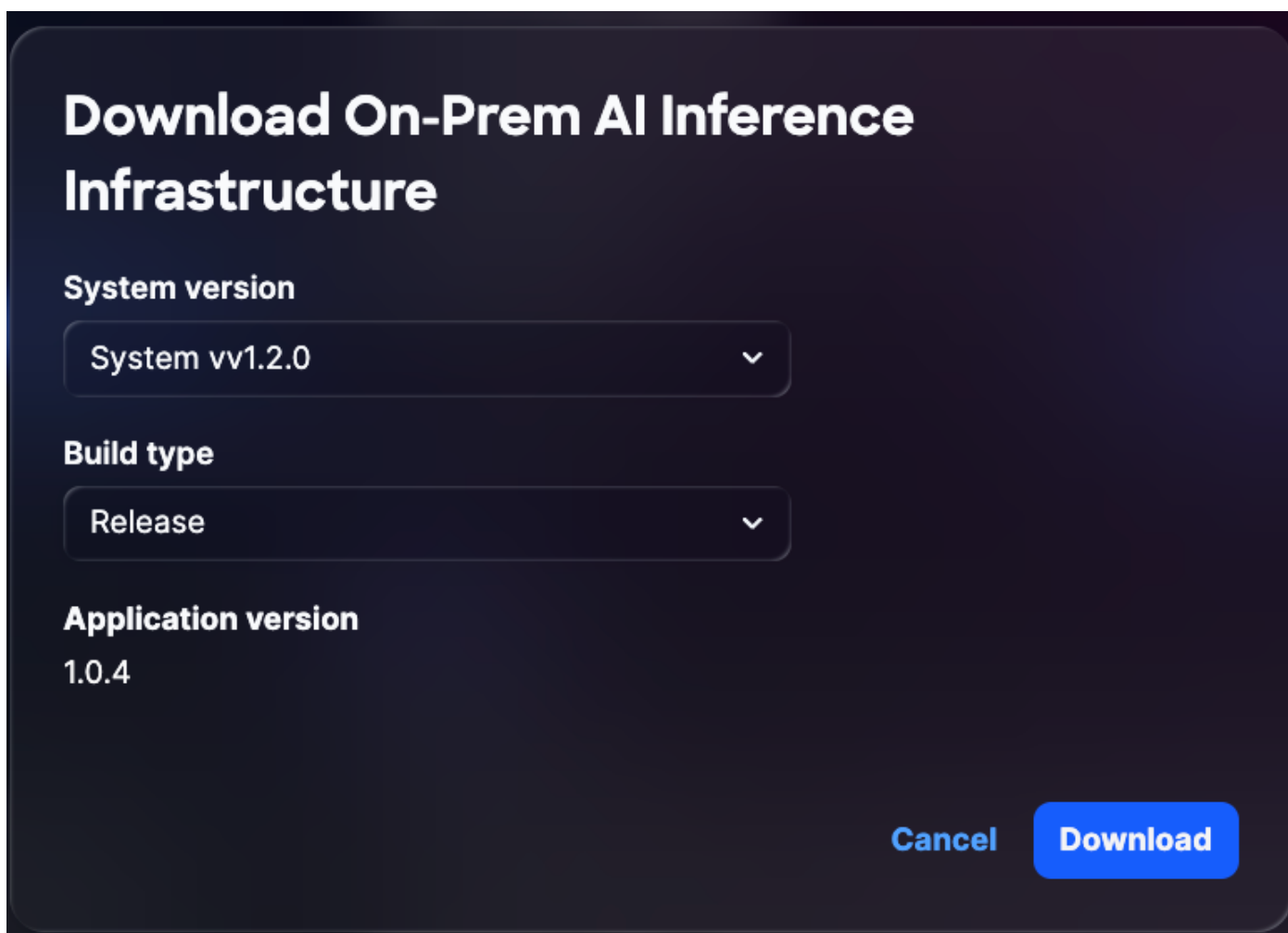
Pour installer l'infrastructure d'inférence d'IA sur l'appliance virtuelle, téléchargez le module d'infrastructure d'inférence d'IA sur site à partir de Cisco IQ SaaS :

1. Connectez-vous à [Cisco IQ](#).
2. Accédez à Paramètres système > Catalogue de packages.



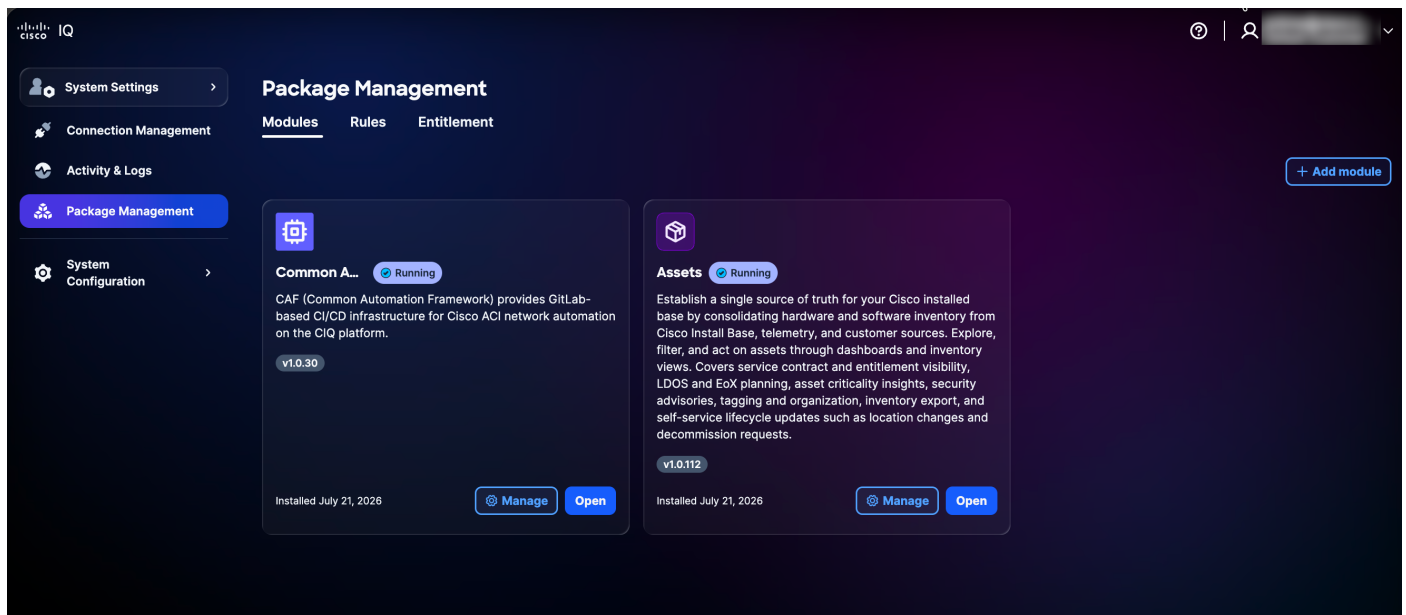
Installer le package

3. Depuis la carte On-Prem AI Inference Infrastructure, cliquez sur Download options > Installation packages. La fenêtre Télécharger l'application s'affiche.



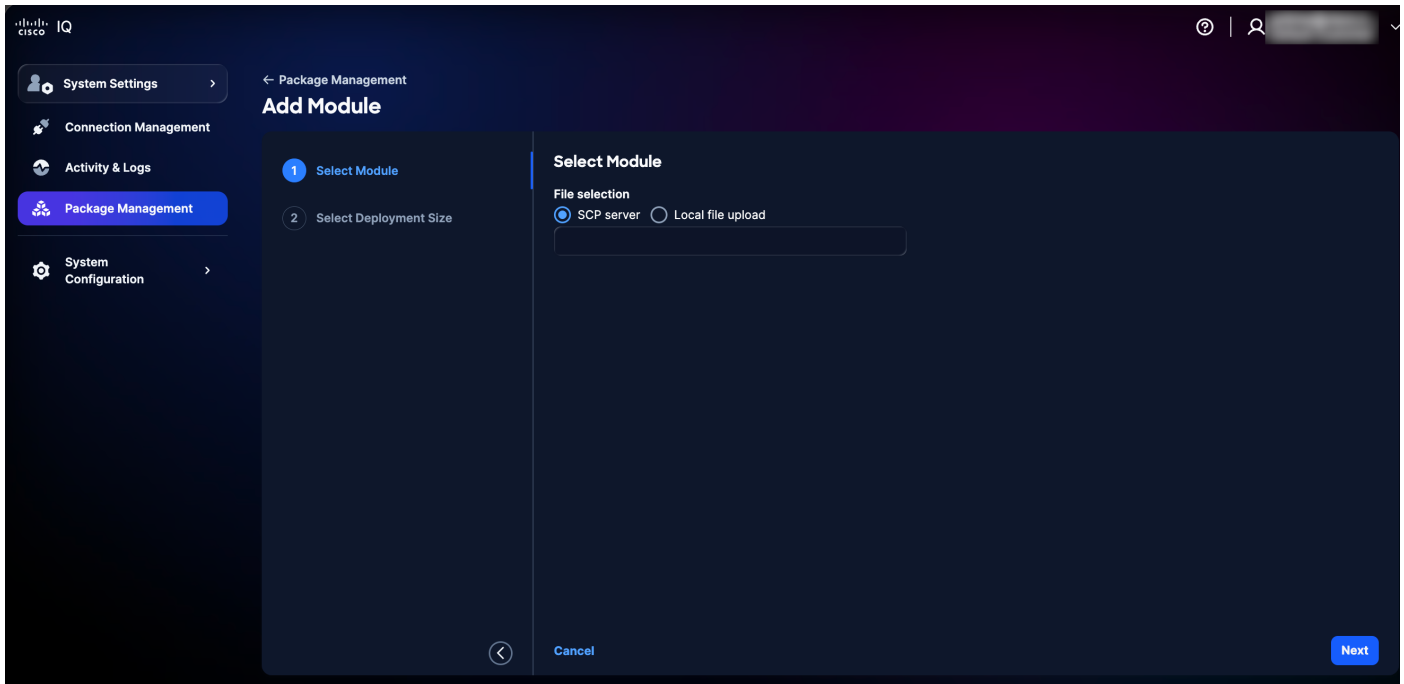
Télécharger l'infrastructure AI Inference

4. Sélectionnez une version du système dans la liste déroulante.
5. Sélectionnez un type de build dans la liste déroulante.
6. Cliquez sur Télécharger.
7. Accédez à VA.



Gestion des packages

8. Accédez à Home > System Settings > Package Management. La page Gestion des packages s'affiche avec les onglets suivants :
 - Modules
 - Règles
 - Droits
9. Dans l'onglet Modules, cliquez sur Add modules.



Sélectionner un module

10. Choisissez votre option de sélection de fichier préférée :

- Serveur SCP : Entrez le nom exact du package d'installation (recommandé pour les fichiers volumineux).
- Téléchargement de fichier local : Glissez-déposez le fichier d'installation téléchargé (déconseillé pour les fichiers de 30 Go ou plus en raison du temps de téléchargement).
Remarque : La méthode de chargement de fichier local a un seuil de 20 minutes. Si le processus de téléchargement dépasse cette durée, l'installation échoue. L'utilisation d'un serveur SCP est la méthode privilégiée pour garantir une installation stable et réussie.

11. Cliquez sur Suivant. Le système commence à télécharger le fichier.

12. Choisissez une taille de déploiement (par exemple, petite, moyenne ou grande).

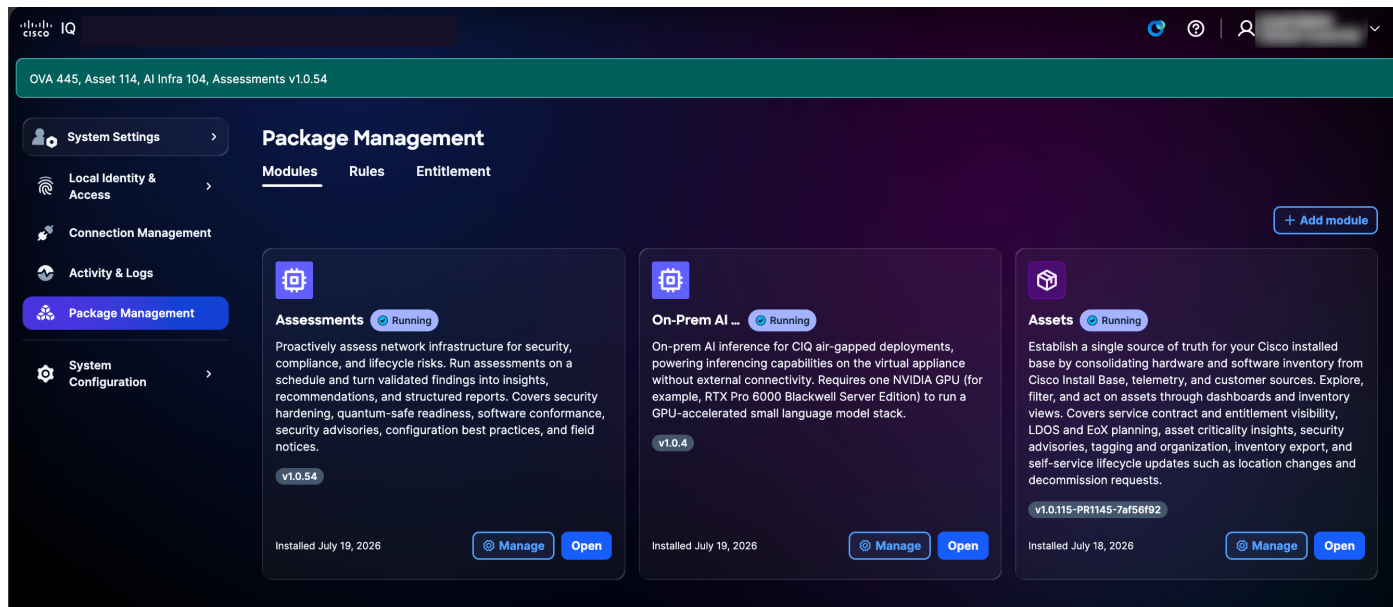
13. Cliquez sur Ajouter un module. L'installation commence et prend environ 40 à 45 minutes.

Une fois l'installation terminée, l'infrastructure d'inférence AI sur site s'affiche dans l'onglet Module de la section Gestion des packages.

 Remarque : Un seul module d'infrastructure d'inférence AI sur site peut être exécuté par GPU. Le module utilise environ 90 % de la VRAM du processeur graphique. La tentative d'installation d'une instance supplémentaire sur le même processeur graphique n'est pas prise en charge.

Gestion du module d'infrastructure d'inférence AI sur site

Une fois installé, le module d'infrastructure d'inférence AI sur site peut être géré à partir de l'onglet Applications dans Gestion de package.



Modification de l'infrastructure AI Inference

Pour gérer le module, cliquez sur Manage à côté du module On-Prem AI Inference Infrastructure. Voir [Gestion des modules](#) pour plus de détails.

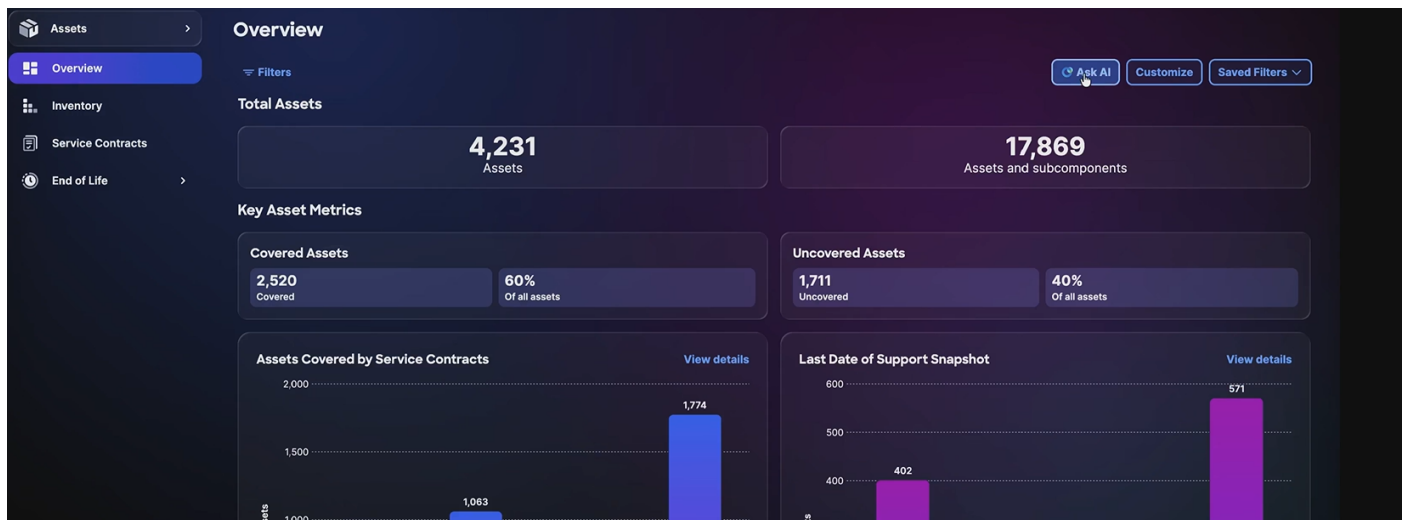
Utilisation des fonctionnalités AI

Une fois que le module d'infrastructure d'inférence AI sur site est correctement installé, le bouton Ask AI devient disponible dans l'interface VA.

Demander IA dans les ressources

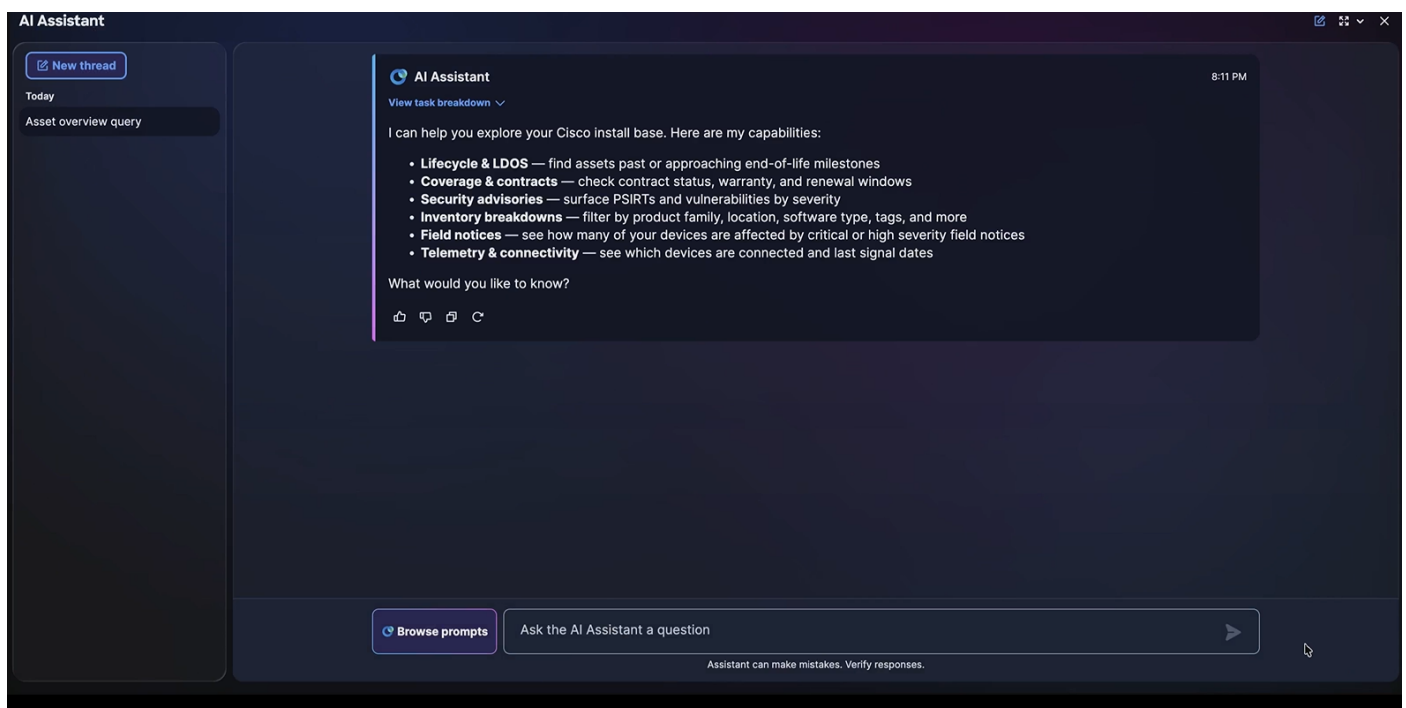
Pour utiliser l'option Demander IA dans les ressources :

1. Sélectionnez le menu Accueil > Actifs. La page Ressources s'affiche.



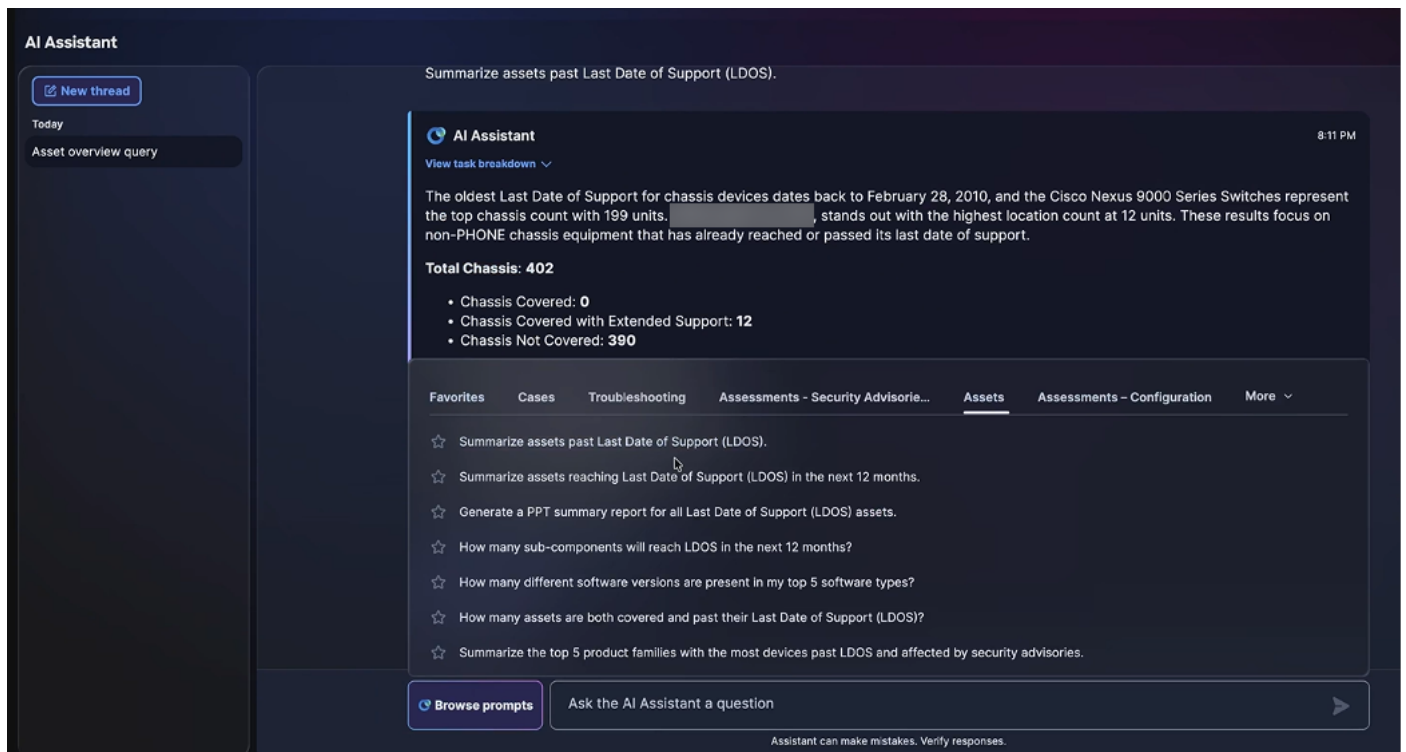
Page Ressources

2. Cliquez sur Demander IA. Lancement de l'infrastructure d'inférence AI sur site.



Parcourir les invites

3. Cliquez sur Browse invites pour afficher les invites disponibles ou entrez une question personnalisée dans le champ Ask the AI Assistant a question.



Ensemble d'invites

4. Cliquez sur l'invite souhaitée ou appuyez sur Entrée. Le SLM sur site génère une réponse.

Analyse IA dans l'inventaire

Le module Infrastructure d'inférence AI sur site fournit une analyse automatisée basée sur l'IA dans la section Inventaire. Les résultats d'analyse s'affichent automatiquement une fois les données d'inventaire renseignées.

Pour afficher l'analyse IA dans Inventory :

1. Sélectionnez le menu Accueil > Inventaire. La page Inventaire s'affiche.

Assets

Overview

Inventory

Service Contracts

End of Life

Assets

Q Search

1 Equipment type

Filters (1) 4231 results

Reset filters

Export

Saved Filters

Insights

Asset inventory analysis filtered to chassis equipment, covering lifecycle status, support coverage, telemetry enrollment, and software version diversity.

- Of the **1,711 assets with no active coverage**, 1,028 (60.1%) belong to the Cisco Nexus 9000 Series Switches product family. Within that uncovered population, 390 assets (46.0%) are already at **Last Date of Support**, meaning they no longer receive security patches or bug fixes from Cisco. Prioritize upgrade planning for Nexus 9000 assets that are both uncovered and past LDOS. [View](#)
- 1,711 assets (40.4%)** across the inventory are **not covered** by an active support contract, compared to 2,520 (59.6%) that are covered. Assets without coverage may have limited access to Cisco support resources if a failure occurs. Conduct a coverage review and prioritize renewal for business-critical chassis. [View](#)
- 295 assets (7.0%)** have an End of Service Contract Renewal date within the next 6 months, from Jul 8, 2026 through Jan 8, 2027, with the earliest deadline on Jul 25, 2026. Assets that pass this milestone without renewal may lose the ability to reinstate contracted support. Begin renewal planning now to avoid coverage lapses. [View](#)
- Among 453 assets with no active coverage, 280 (61.8%) have End of Software Maintenance as their next milestone. Once this milestone passes, software defect fixes will no longer be available from Cisco, compounding the risk of operating without a support contract. Prioritize coverage renewal or upgrade planning for these assets before the milestone is reached. [View](#)
- Assets with telemetry enabled average **5.1 affected Security Advisories**, while assets with telemetry not enabled average **0.0 affected Security Advisories**. This gap indicates that unconnected assets are not being evaluated for known vulnerabilities within Cisco IQ, not that they have none. Enroll chassis assets in telemetry to enable accurate advisory tracking. [View](#)

Full Analysis

Name	Product ID	Product Type	Equipment Type	Serial Number	Next Milestone	Next Milestone...	Contract Number	Coverage Status	Telemetry Status	Security Adviso...	
			Chassis			Jun 25, 2028	—	🔒	🔒	0	
			Chassis			—	204599980	🔒	🔒	35	
			Chassis			—	204599980	🔒	🔒	35	
			Chassis			Oct 29, 2026	—	🔒	🔒	3	
			Chassis			Apr 26, 2028	—	🔒	🔒	7	
			Chassis			Jul 31, 2027	—	🔒	🔒	7	
			Chassis			—	—	🔒	🔒	2	

Stocks

- Affichez l'analyse générée par l'IA. Les résultats s'affichent dans la vue d'inventaire une fois les données disponibles.

Remarque : Cliquez sur Analyse complète pour afficher des visualisations telles que des graphiques, des tableaux de bord et des graphiques qui fournissent des informations supplémentaires.

Fonctionnalités courantes des modules

Cette section détaille les fonctionnalités principales partagées sur tous les modules. Ces fonctionnalités offrent une expérience utilisateur homogène, optimisent les performances du système et rationalisent les workflows administratifs

Analyse des données

Le panneau Insights fournit une analyse basée sur l'IA des données de cette page, fournissant des informations exploitables pour améliorer la sécurité et la santé de votre environnement réseau.

Remarque : La fonction Analyse n'est disponible que sur certaines pages.

The screenshot shows the Cisco IQ Inventory page. The left sidebar contains navigation links: Assets, Overview, Inventory (selected), Service Contracts, and End of Life. The main content area is titled 'Assets' and includes a search bar, filters (Product family, Product ID, Location, Tags), and a 'Filters (1)' indicator showing 1716 results. An 'Export' button is also present.

The 'Insights' panel displays several key findings:

- 69 assets that are **not covered** by any support contract have already reached **Last Date of Support**, leaving them without security patches or bug fixes. Prioritize upgrades or replacements for these assets to mitigate operational risks. [View](#)
- 175 Cisco Catalyst 9300 Series Switches (49.7% of **not covered** assets) lack active support contracts, which may limit access to Cisco support resources. Align renewal planning with the channel partner for these business-critical switches. [View](#)
- 73 assets with **telemetry not enabled** are at **End of Software Maintenance**, reducing visibility within Cisco IQ for proactive alerts and lifecycle planning. Enable telemetry for these assets to restore full monitoring capabilities. [View](#)
- 75 assets (4.4%) have **coverage expiring** between **Apr 24, 2026** and **Oct 24, 2026**, with the earliest deadline on **Apr 30, 2026**. Review these contracts to avoid lapses in vendor support and potential cost increases. [View](#)
- 75 assets (4.4%) have **End of Service Contract Renewal** dates between **May 1, 2026** and **Oct 24, 2026**, starting with a deadline on **May 1, 2026**. Coordinate with the selling partner to renew these contracts before expiry. [View](#)

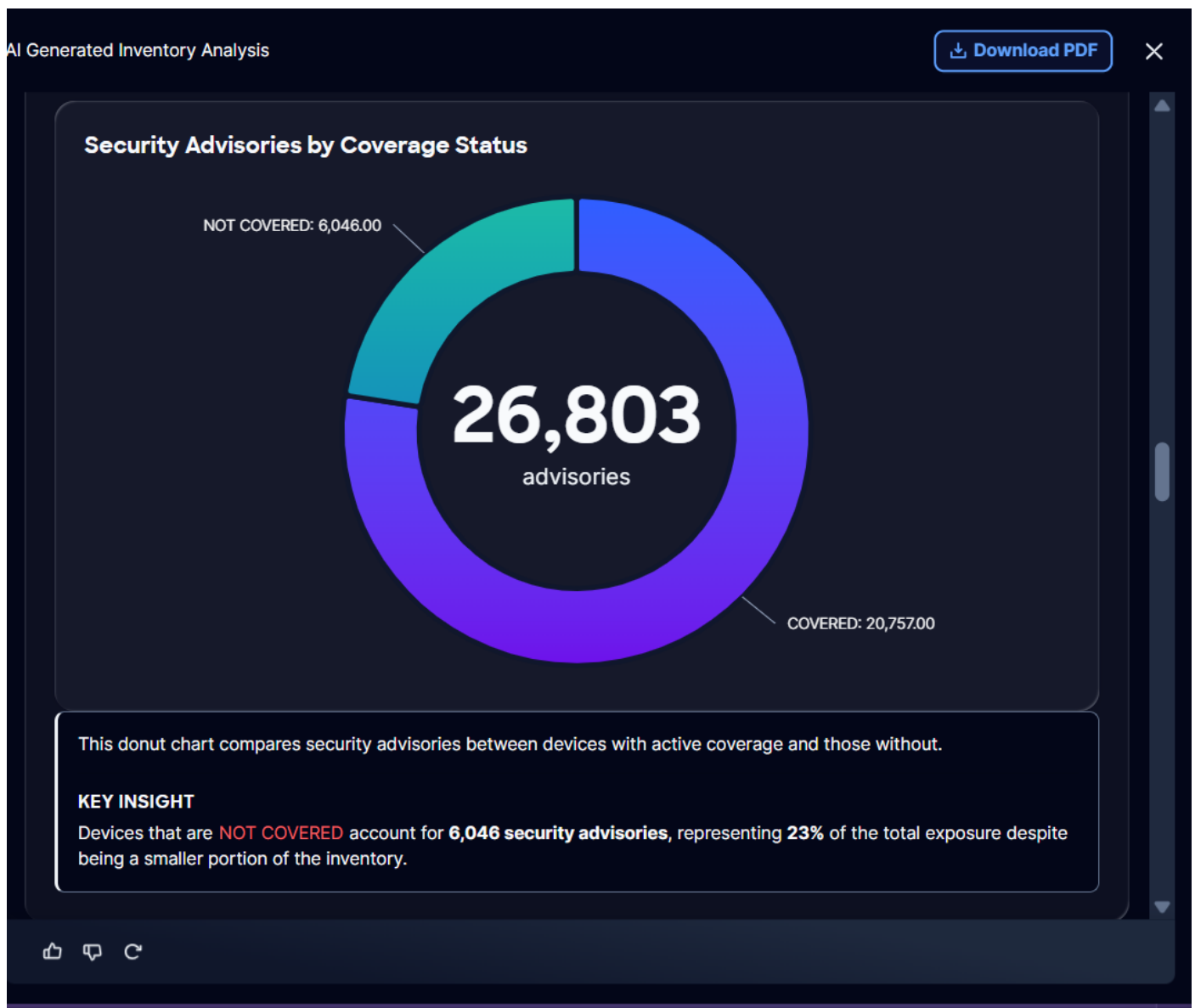
Below the insights is a table of assets:

☐	Name	Product ID	Product Type	Serial Number	Next Milestone	Next Milesto...	Contract Number	Coverage Status	Telemetry Status	Security...
☐	[Redacted]	[Redacted]	Cloud and ...	[Redacted]	End of Ser...	Jun 25, 2028	—	🔒	🟢	0
☐	[Redacted]	[Redacted]	Switches	[Redacted]	End of Ser...	Jan 29, 2027	—	🔒	🟢	4
☐	[Redacted]	[Redacted]	Switches	[Redacted]	—	—	[Redacted]	🟢	🟢	23
☐	[Redacted]	[Redacted]	Switches	[Redacted]	—	—	[Redacted]	🟢	🟢	23
☐	[Redacted]	[Redacted]	Switches	[Redacted]	—	—	[Redacted]	🟢	🟢	23

Volet Insights

Les options suivantes sont disponibles dans le panneau Insights :

- Cliquez sur l'icône Développer pour développer le panneau et afficher des informations supplémentaires
- Cliquez sur l'icône Pouces vers le haut ou Pouces vers le bas pour fournir des commentaires sur les informations générées par l'IA
- Cliquez sur Analyse complète pour afficher des informations supplémentaires, une analyse plus approfondie et des visualisations telles que des graphiques, des tableaux de bord et des graphiques



Analyse complète

Les options suivantes sont disponibles dans une analyse complète :

- Cliquez sur Download PDF pour enregistrer une copie hors ligne de l'analyse pour vos dossiers ou pour la collaboration

Exportation des informations

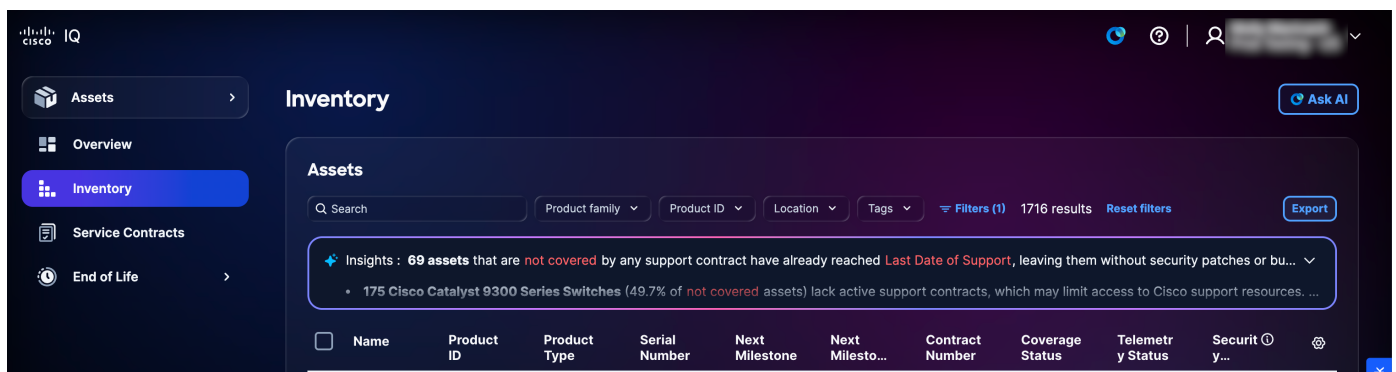
La fonction d'exportation vous permet d'exporter des vues personnalisées pour les informations sur les ressources et la sécurité au format .xls ou .csv.



Remarque : La fonction d'exportation n'est disponible que pour les pages sélectionnées.

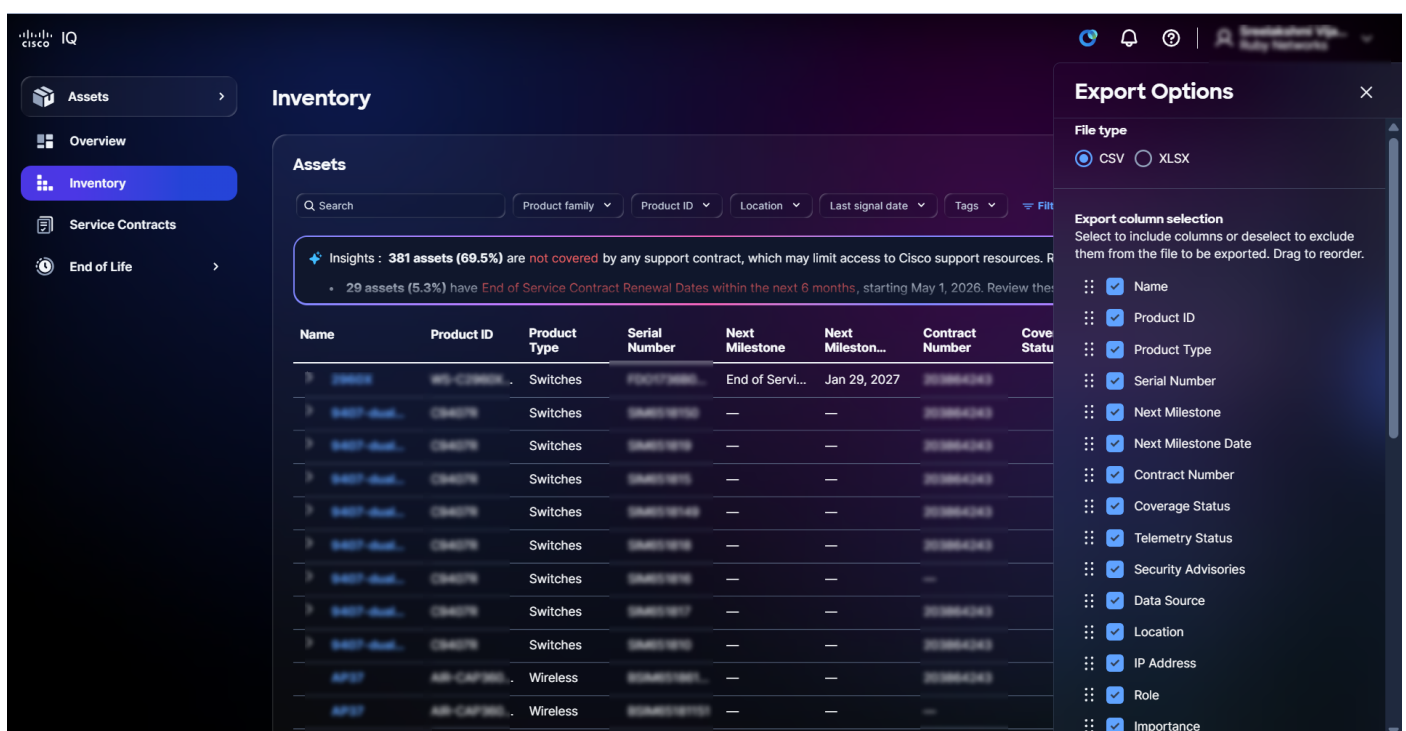
Pour exporter des informations d'une page :

1. Accédez à la page.



Exportation de l'inventaire dans le module Ressources

2. Cliquez sur Exporter. Les options d'exportation s'affichent.



Options d'exportation

3. Sélectionnez un type de fichier.

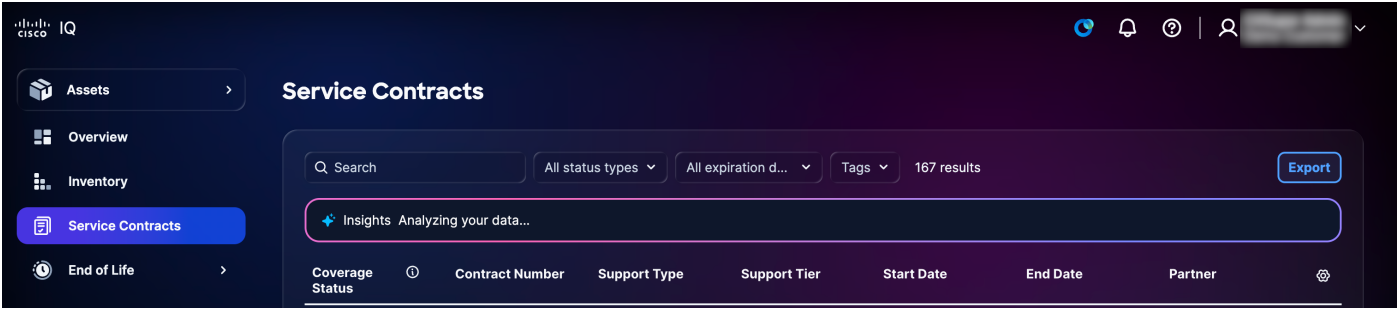
4. Cochez la ou les cases dans la ou les colonnes souhaitées.

5. Cliquez sur Exporter. Le fichier est téléchargé dans le dossier de téléchargement local du

navigateur.

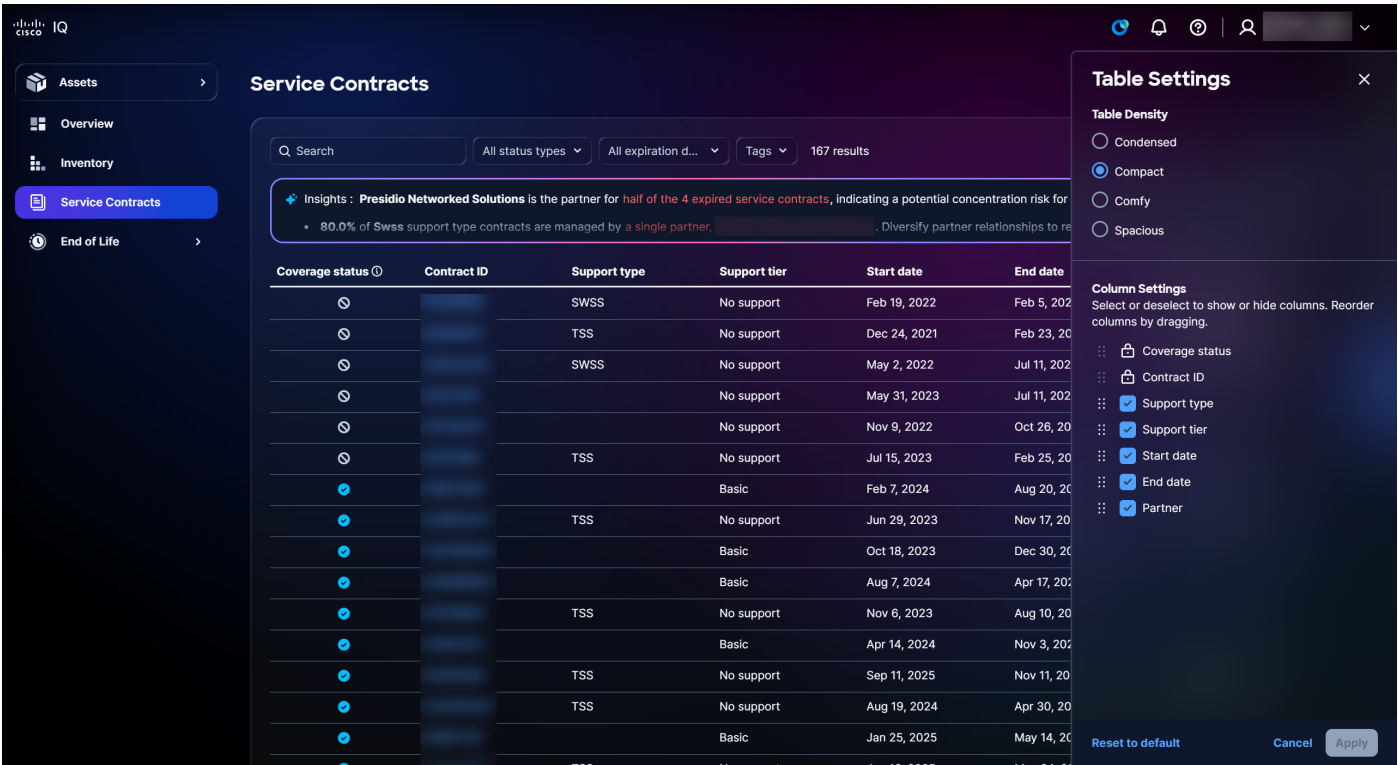
Paramètres du tableau

Vous pouvez configurer les paramètres du tableau pour créer des vues personnalisées et affinées pour différentes fonctions du module.



Paramètres du tableau

Pour modifier les colonnes qui s'affichent sur les pages sélectionnées, cliquez sur l'icône Paramètres du tableau. Les paramètres du tableau s'affichent.



Options des paramètres du tableau

Modification du tableau

Pour modifier l'affichage du tableau :

1. Sélectionnez l'une des options Densité du tableau suivantes :

- Condensé : Réduit les éléments visuels et l'espacement pour afficher plus d'informations
- Compact : Réduit l'espace blanc et resserre l'espacement entre les éléments UI
- Confortable : Utilise plus d'espaces et un espacement plus important entre les éléments
- Spacieux : Met en évidence les nombreux espaces blancs et les éléments d'interface utilisateur volumineux

2. Cliquez sur Apply.

Ajout et suppression de colonnes

Pour ajouter ou supprimer des colonnes :

1. Activez ou désactivez la ou les cases à cocher Paramètres de colonne.

2. Cliquez sur Apply.



Remarque : La colonne Name ne peut pas être supprimée de la vue de table.

Modification de l'ordre des colonnes

Pour modifier l'ordre des colonnes :

1. Faites glisser le nom de la colonne pour organiser les éléments dans l'ordre souhaité.

2. Cliquez sur Apply.

Personnalisation des tableaux de bord

La fonction Tableau de bord personnalisé vous permet de personnaliser les tableaux de bord standard grâce à une gamme d'options de personnalisation intuitives :

- Réorganiser les widgets ou les panneaux du tableau de bord à l'aide de la fonctionnalité glisser-déplacer
- Supprimez tous les composants qui ne sont pas pertinents pour votre workflow
- La disposition personnalisée de votre tableau de bord est stockée en toute sécurité dans votre profil utilisateur et automatiquement appliquée à toutes les sessions et à tous les périphériques
- Restaurer la disposition d'origine du tableau de bord avec une simple option de réinitialisation

Pour personnaliser un tableau de bord :

1. Accédez au tableau de bord.



Personnaliser

2. Cliquez sur Personnaliser.



Modifier le tableau de bord

3. Modifiez le tableau de bord comme vous le souhaitez :

- Réorganiser : Faites glisser et déposez les widgets dans la disposition souhaitée
- Supprimer : Cliquez sur l'icône Supprimer pour supprimer un widget
- Réinitialiser : Cliquez sur Rétablir les paramètres par défaut pour rétablir la disposition d'origine du tableau de bord

4. Cliquez sur Save. Un message Dashboard Saved s'affiche.

La disposition de votre tableau de bord est automatiquement appliquée à toutes les sessions et à tous les périphériques.

Personnalisation des filtres

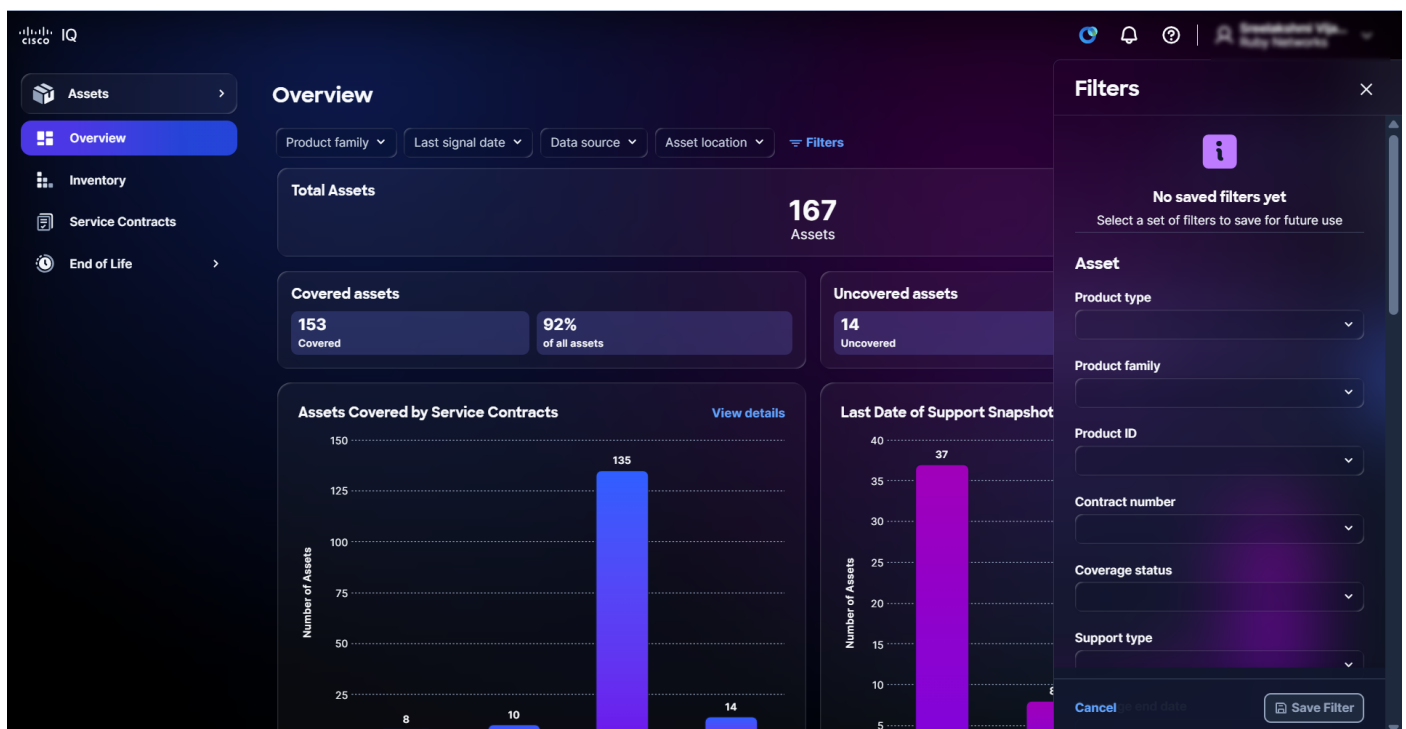
Vous pouvez enregistrer des configurations de filtres personnalisées pour n'importe quelle vue du tableau de bord, ce qui vous permet de revenir facilement à vos paramètres préférés si nécessaire. Toutes les préférences de filtrage sont stockées en toute sécurité par utilisateur et par

compte, ce qui garantit une expérience personnalisée et cohérente à chaque accès à Cisco IQ.

Création d'un filtre

Pour créer un filtre personnalisé :

1. Accédez au tableau de bord.
2. Cliquez sur Filtres.



Filtres

3. Sélectionnez les filtres souhaités dans les listes déroulantes.
4. Cliquez sur Enregistrer le filtre. La fenêtre Nom du filtre enregistré s'ouvre.

Name saved Filter

Filter name *

Custom Filter |

Cancel

Save Filter

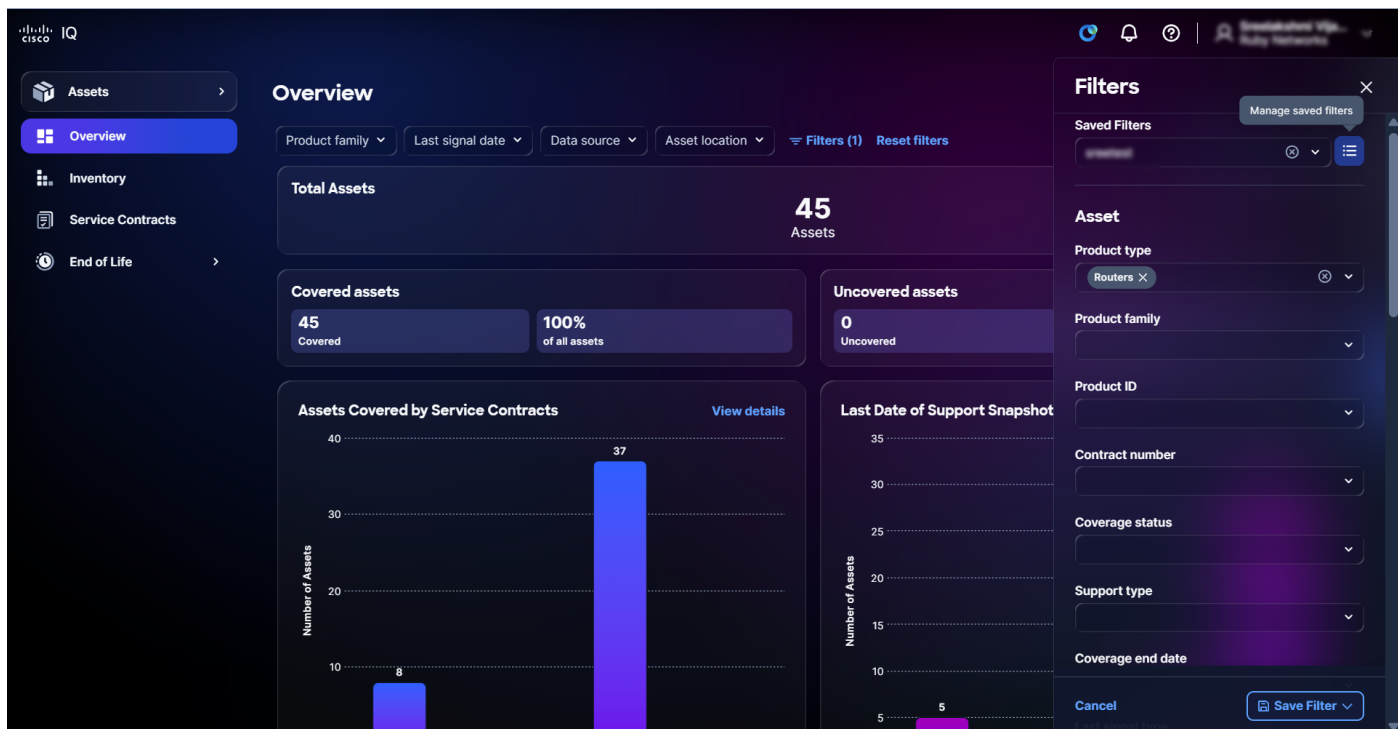
Nom du filtre

5. Entrez un nom de filtre.
6. Cliquez sur Save Filter pour confirmer.

Modification d'un nom de filtre

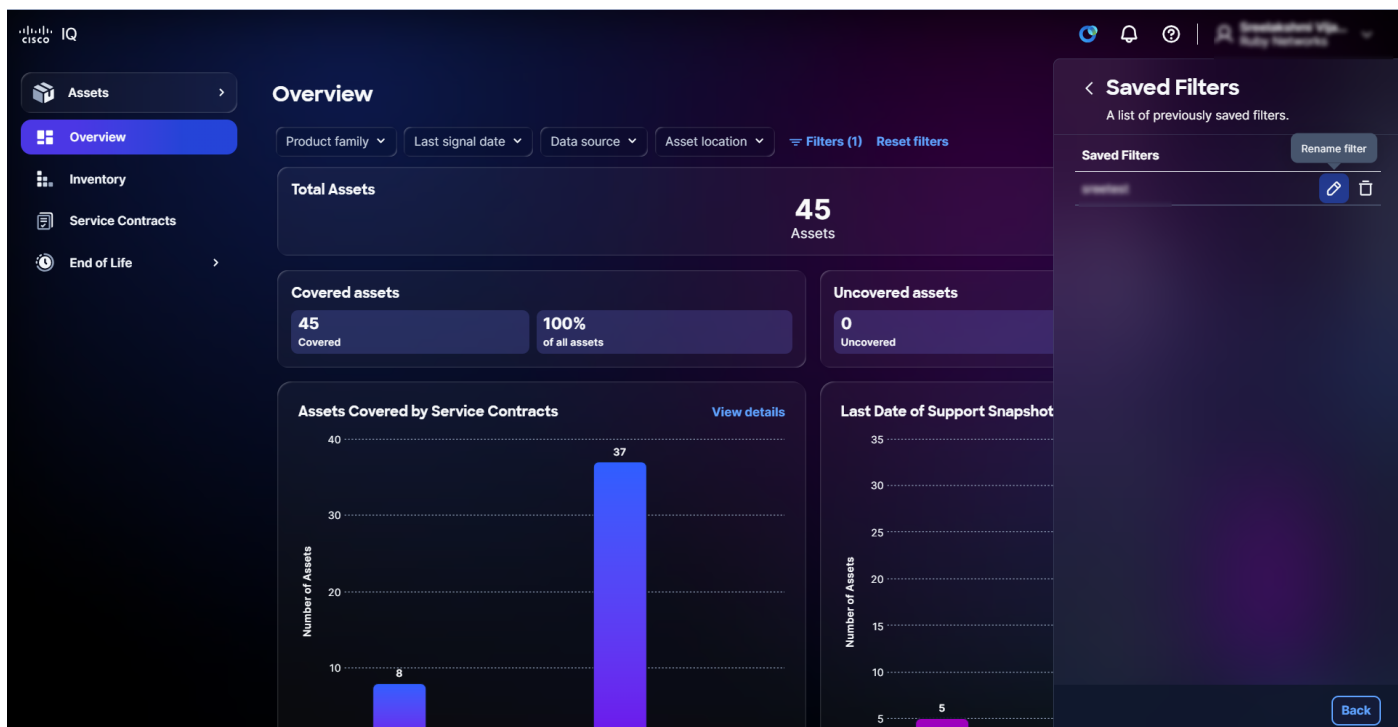
Pour modifier un filtre personnalisé :

1. Cliquez sur Filtres.



Gérer les filtres enregistrés

2. Cliquez sur l'icône Gérer les filtres enregistrés.
3. Accédez au filtre.



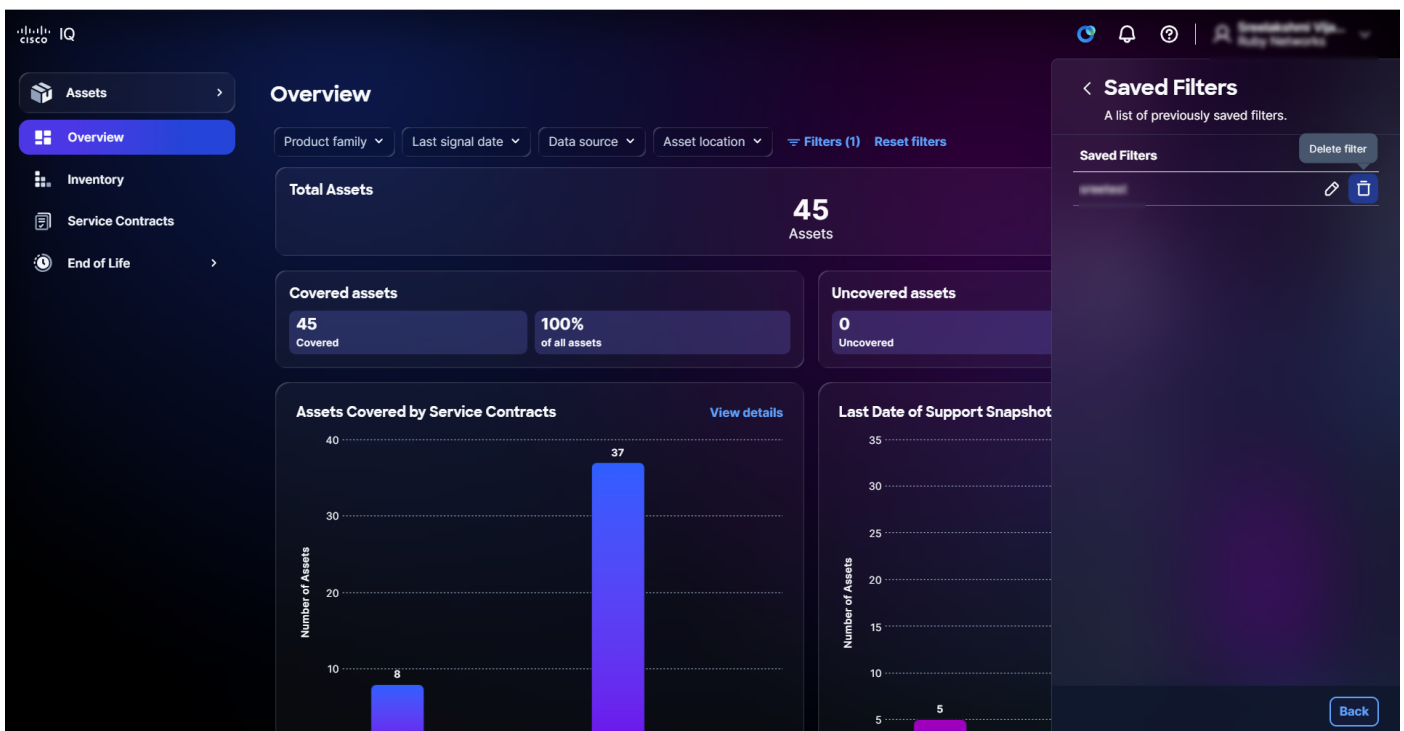
Modifier le filtre

4. Cliquez sur l'icône Modifier. La fenêtre Nom du filtre enregistré s'ouvre.
5. Modifiez le nom du filtre.
6. Cliquez sur Save Filter pour confirmer.

Suppression d'un filtre

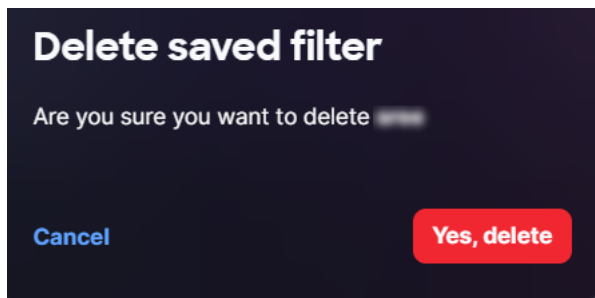
Pour supprimer un filtre personnalisé :

1. Cliquez sur Filtres.
2. Cliquez sur l'icône Filtres enregistrés gérés
3. Accédez au filtre.



Supprimer le filtre enregistré

4. Cliquez sur l'icône Supprimer. La fenêtre Supprimer le filtre enregistré s'ouvre.



Confirmation de suppression du filtre enregistré

5. Cliquez sur Yes, delete pour confirmer.

Module de ressources

Le module Assets offre une visibilité et des fonctionnalités de gestion complètes pour les ressources Cisco et sert de base à Cisco IQ, en fournissant une liste centralisée de tous les périphériques au sein d'une organisation. En collectant des informations auprès de plusieurs sources, il agit comme une source unique de vérité pour l'inventaire des périphériques. La mise à jour d'une liste complète et précise des ressources est essentielle, car d'autres modules de Cisco IQ, tels que le module d'évaluation, s'appuient sur ces données pour évaluer l'intégrité et la sécurité de vos périphériques.

Concepts de base

Le module Actifs repose sur les concepts fondamentaux suivants :

- Ressource : Tout périphérique physique, matériel ou logiciel inventorié et géré dans le cadre de la prestation de services de Cisco avec un suivi détaillé de son identité, de sa fonction, de sa couverture de service et de son cycle de vie
- Ressources sous contrat : Les ressources sont directement introduites dans l'inventaire à partir des données de contrat de service liées, plutôt que par télémétrie. Cisco IQ recueille les types d'équipements suivants à partir des données du contrat : Châssis, modules, alimentations et ventilateurs. Ces ressources sont visibles dans l'inventaire même si aucune connexion de télémétrie n'est présente
- Date de fin d'assistance (LDOS) : Suivi des étapes de fin de vie et de fin d'assistance pour les produits Cisco
- Couverture du service : Contrats d'assistance actifs, garanties et niveaux de droits associés à un matériel ou logiciel spécifique

- Étiquette de ressource : Libellé défini par l'utilisateur et affecté à une ressource pour les workflows d'organisation, de filtrage et opérationnels
- Signal du périphérique : Désigne la date à laquelle Cisco a observé un périphérique pour la dernière fois (par son numéro de série) en fonction de la télémétrie du périphérique, des dossiers d'assistance et des renouvellements de contrat ; Les données de télémétrie des ressources sont ingérées et enrichies via un pipeline de données multicouche

Module Accès aux ressources

Pour accéder aux fonctions de gestion des ressources dans Cisco IQ, choisissez le menu Accueil > Ressources ou cliquez sur Ressources dans la section Application de la page Accueil > onglet Launchpad. La page Overview s'affiche.

Présentation des ressources

La page Overview affiche un tableau de bord qui vous permet d'évaluer rapidement l'état et l'état des périphériques.

100% 400 Assets 100% 400 Assets 100% 400 Assets



Assets



Overview



Inventory



Service Contracts



End of Life



Overview

Filters

Ask AI

Customize

Saved Filters

Total Assets

199

Assets

928

Assets and subcomponents

Key Asset Metrics

Covered Assets

186

Covered

93%

Of all assets

Uncovered Assets

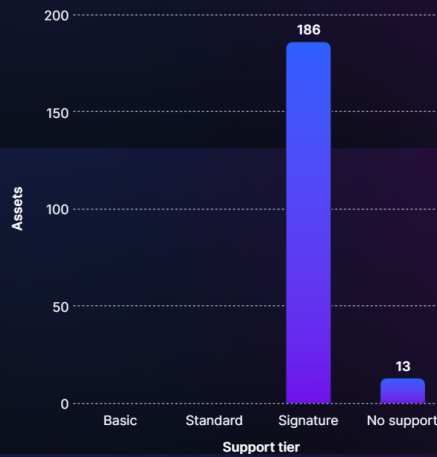
13

Uncovered

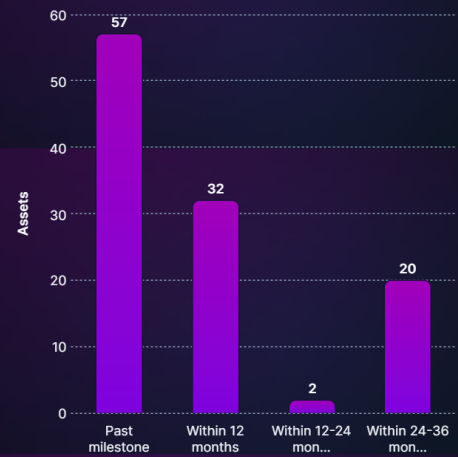
7%

Of all assets

Assets Covered by Service Contracts [View details](#)



Last Date of Support Snapshot [View details](#)



Assets With Telemetry Enabled

186

With telemetry

93%

Of all assets

Assets Without Telemetry Enabled

13

Without telemetry

7%

Of all assets

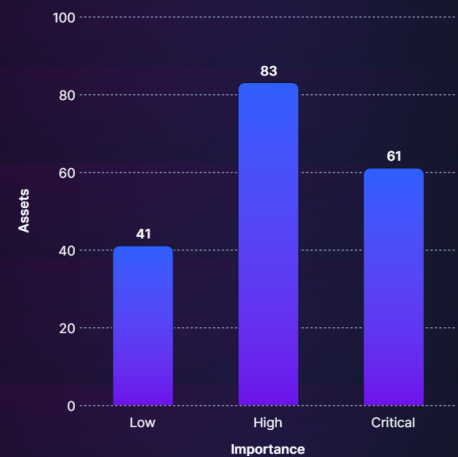
Assets With Critical or High Security Advisories [View details](#)



Of the 186 assets with telemetry enabled, 170 have critical or high Security Advisories

Assets by Importance [View details](#)

Importance can be evaluated for 185 assets.

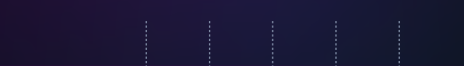


Asset Breakdown

Top 5 Product Families [View details](#)



Top 5 Install-At Locations [View details](#)



Présentation des ressources

Le tableau de bord affiche les informations suivantes :

- Total des actifs : Nombre total de ressources dans le compte Cisco IQ
- Indicateurs clés des ressources : Mesures clés supplémentaires telles que l'état de télémétrie, les avis de sécurité critiques et les informations LDOS
- Actifs couverts : Le nombre total et le pourcentage d'actifs couverts par les contrats de service
- Actifs non couverts : Le nombre total et le pourcentage d'actifs non couverts par les contrats de service
- Actifs couverts par les contrats de service : Ventilation du nombre d'actifs (matériels ou logiciels) couverts par les contrats de service, classés par niveau de droit
- Date de la dernière prise en charge : Ventilation du nombre d'actifs ayant dépassé la DDOS ou ayant atteint la DDOS
- Ressources avec télémétrie activée : Nombre total et pourcentage de ressources avec la télémétrie activée
- Ressources sans télémétrie activée : Nombre total et pourcentage de ressources sans télémétrie activée
- Ressources avec avis de sécurité critique ou élevé : Pourcentage du total des ressources pour lesquelles la télémétrie est activée et pour lesquelles des conseils de sécurité critiques ou élevés sont disponibles
- Actifs par importance : Décomposition de la priorité attribuée à un périphérique par rapport aux autres périphériques du réseau.
- Ventilation des actifs : Affichage détaillé des informations sur les ressources, telles que les gammes de produits, les emplacements d'installation, les versions logicielles et les rôles des ressources

Filtrage des vues pour les ressources

Vous pouvez filtrer la vue du tableau de bord en choisissant un filtre dans les listes déroulantes ou en cliquant sur Filtres et en choisissant une option dans la liste des filtres disponibles.

 Remarque : Certains filtres peuvent être masqués en fonction des paramètres de zoom de l'écran. Différents filtres sont disponibles en fonction de vos rôles et autorisations.

Voir les détails des immobilisations

Lorsque vous cliquez sur Afficher les détails, la page redirige vers la page Inventaire. Voir [Inventaire](#) pour plus d'informations.

Informations sur la criticité des ressources

Cisco IQ inclut Asset Criticality Insights, une nouvelle fonctionnalité du module Assets qui prédit le rôle fonctionnel et l'importance commerciale des périphériques réseau. En analysant les configurations des périphériques et les fonctionnalités activées, Asset Criticality Insights vous aide à identifier les ressources qui ont le plus d'impact sur votre réseau, afin que vous puissiez les hiérarchiser pour la correction des problèmes de sécurité, les mises à niveau logicielles, la planification de fin de vie et les décisions de couverture.

 Remarque : Les informations sur la criticité des ressources sont disponibles uniquement pour les ressources avec niveaux Standard ou Signature qui ont des connexions de télémétrie actives. Assurez-vous que vos ressources répondent aux exigences de configuration pour renseigner ces informations dans le tableau de bord.

Les informations sur la criticité des ressources sont disponibles dans l'application Ressources dans les domaines suivants :

- Présentation des ressources : Filtrer et afficher les ventilations récapitulatives par attributs
Aperçu de la criticité des actifs
- Inventaire des ressources : Afficher, rechercher, filtrer et trier les périphériques par rôle et importance
- Détails des ressources : Afficher le rôle et l'importance pour chaque périphérique, avec des info-bulles expliquant chaque valeur

Substitution des classifications de rôle et d'importance

Cisco IQ prédit automatiquement le rôle et l'importance de chaque ressource en fonction des données de télémétrie. Les administrateurs de compte peuvent corriger manuellement ces classifications lorsque la prédiction automatisée ne reflète pas avec précision la fonction ou la criticité de la ressource sur le réseau.



Remarque : Les contrôles de remplacement ne sont disponibles que pour les administrateurs de compte. Les valeurs Rôle et Importance sont en lecture seule pour tous les autres rôles d'utilisateur.

Remplacer les classifications de la table d'inventaire

Pour remplacer le rôle ou l'importance d'une ou de plusieurs ressources :

1. Accédez à Immobilisations > Inventaire.
2. Cochez la case de la ligne d'actif souhaitée. Pour mettre à jour plusieurs ressources simultanément, cochez plusieurs cases.

The screenshot shows the Cisco IQ Inventory page. The left sidebar has a menu with 'Assets', 'Overview', 'Inventory' (selected), 'Service Contracts', and 'End of Life'. The main content area is titled 'Inventory' and shows a table of assets. The table has columns: Name, Product ID, Product Name, Equipment Name, Serial Number, Next Mile, Next Mile, Contract, Coverage, Telemetry, and a selection column. The table shows 4 items selected. The 'Coverage' column has a visual indicator (blue checkmark) for the selected item.

	Name	Product ID	Product Name	Equipment Name	Serial Number	Next Mile	Next Mile	Contract	Coverage	Telemetry	
☐			Modules	Module		—	—		✓	✓	0
☐			Modules	Module		—	—		✗	✓	0
☒			Unified ...	Chassis		—	—		✓	✓	1
☐			Storage...	Chassis		—	—		✓	✓	0

Rôle et importance

3. Dans la colonne Role ou Importance, choisissez la valeur correcte dans la liste déroulante de la ligne d'actif.
4. Cliquez sur Apply pour confirmer le remplacement.

Les immobilisations dont les valeurs sont remplacées manuellement affichent un indicateur visuel dans la colonne Rôle ou Importance.



Remarque : Pour supprimer un remplacement précédemment configuré et revenir à la prédiction automatisée, sélectionnez l'option tiret (—) dans la liste déroulante Rôle ou Importance.

Remplacer les classifications des détails d'immobilisation

Pour remplacer le rôle ou l'importance dans la vue détaillée des immobilisations :

1. Accédez à Actifs > Inventaire et cliquez sur une immobilisation.
2. Dans le panneau Détails de l'actif, localisez les champs Rôle et Importance.
3. Cliquez sur la liste déroulante du champ que vous souhaitez mettre à jour et sélectionnez la valeur correcte.
4. Cliquez sur Apply pour confirmer.

La vue détaillée d'une ressource affiche également une explication des attributs de télémétrie qui ont servi de base à la prédiction automatisée initiale, afin de déterminer si un remplacement est approprié.

Afficher la piste d'audit de remplacement

Tous les remplacements de rôle et d'importance sont enregistrés dans une piste d'audit au niveau du compte. Pour accéder à la piste d'audit :

1. Sélectionnez Accueil > Paramètres système > Exercice et journaux.
2. Choisissez Filters > Action Type > override pour afficher uniquement les événements de remplacement.

La piste d'audit affiche le nom de l'actif, les valeurs précédente et nouvelle, l'utilisateur qui a effectué la modification, ainsi que la date et l'heure de la modification. La piste d'audit peut être exportée à l'aide de l'option Export.



Remarque : La piste d'audit peut être filtrée par plage de dates, par utilisateur et par nom d'actif.

Stocks

La page Inventaire fournit une liste de toutes les ressources Cisco dans le compte Cisco IQ.

Assets

Overview

Inventory

Service Contracts

End of Life

Inventory

Ask AI

Assets

Search

1 Equipment type

Filters (1) Reset filters

Export

Saved Filters

Insights: Among the 13 assets with Telemetry Status **Not Connected**, Support Tier **NO SUPPORT** is the most frequen...

With a Partition Key of " (empty)", 10 of the 13 assets have the Next Milestone as **End Of Sale** (40.0%). As these produc...

	Name	Produ ct ID	Produ ct...	Equip men...	Serial Nu...	Next Mile...	Next Mile...	Contr act...	Cover age...	Telem etry...	
☐			Cloud a...	Chassis		End of ...	Jun 25, ...	204107...			0
☐			Wireless	Chassis		—	—	204107...			0
☐			Wireless	Chassis		—	—	204107...			0
☐			Routers	Chassis		—	—	204107...			8
☐			Routers	Chassis		End of ...	Feb 19, ...	204107...			0
☐			Switches	Chassis		—	—	204107...			10

Stocks

Rechercher et filtrer des vues pour l'inventaire des ressources

Vous pouvez filtrer l'affichage de liste en choisissant un filtre dans les listes déroulantes ou en cliquant sur Filtres et en choisissant une option dans la liste des filtres disponibles. Vous pouvez également rechercher des ressources en saisissant leur nom dans le champ Rechercher.

 Remarque :

- Certains filtres peuvent être masqués en fonction des paramètres de zoom de l'écran.
- Différents filtres sont disponibles en fonction de vos rôles et autorisations.

Analyse des stocks

Le volet Insights de la page Inventory affiche une analyse basée sur l'intelligence artificielle qui fournit un résumé des ressources en mettant l'accent sur la couverture de l'assistance, la connectivité et les étapes clés. Cliquez sur Analyse complète pour afficher des visualisations telles que des graphiques, des tableaux de bord et des graphiques qui fournissent des informations supplémentaires. Voir [Analyser les données](#) dans les caractéristiques communes du module pour

plus de détails.

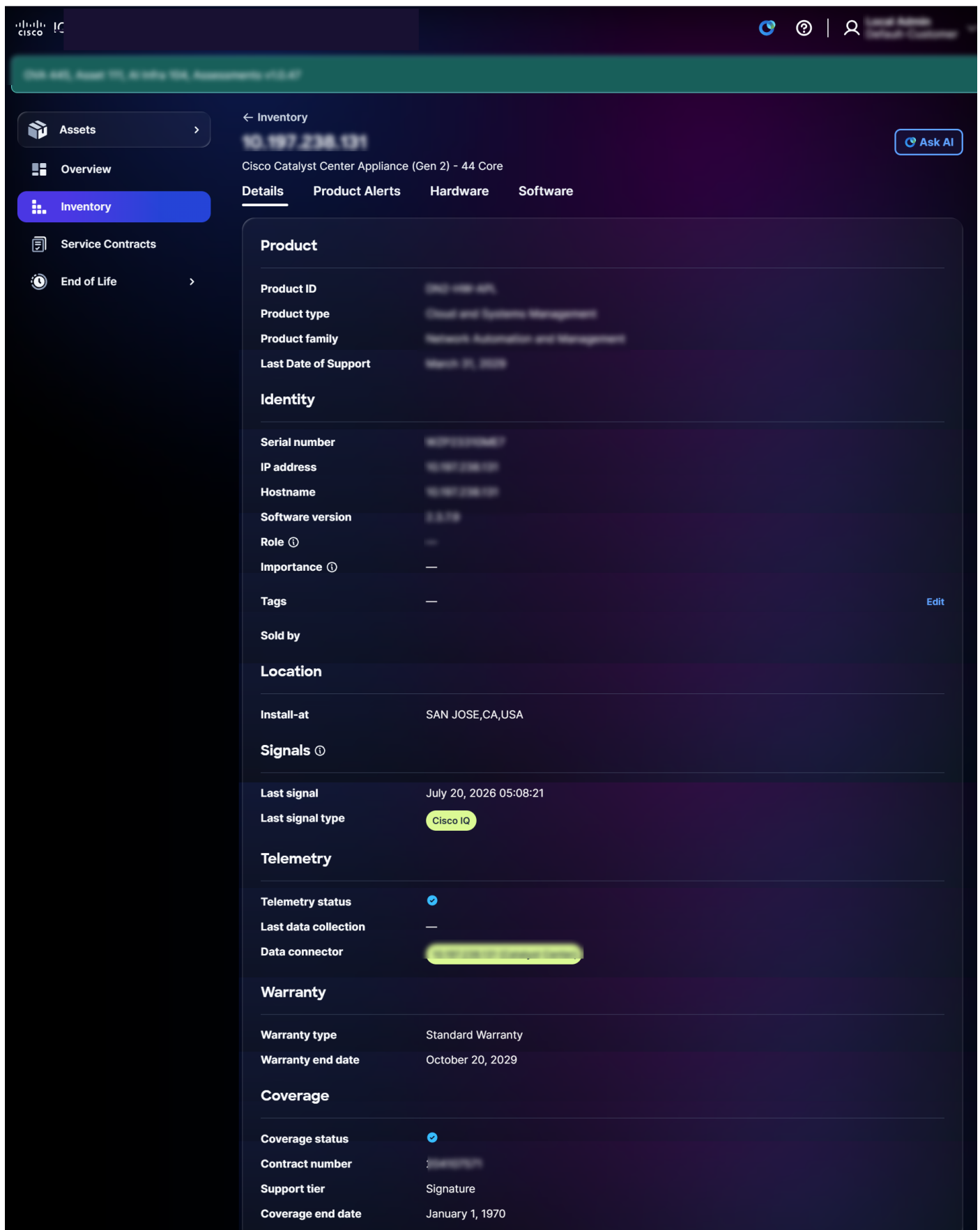
Exportation de stock

Cliquez sur Export pour enregistrer une liste d'inventaire filtrée au format .xls ou .csv. Pour plus d'informations, consultez [Exportation d'informations](#) dans Fonctionnalités du module commun.

Voir les détails des équipements

Cliquez sur une ressource pour en afficher les détails. La vue détaillée d'une ressource s'affiche avec les onglets suivants :

- Détails: Affiche des informations sur les ressources telles que le produit, les données de signal, l'identité, l'emplacement, la garantie et la couverture



Détails des ressources

- **Alertes de produits:** Affiche les alertes produit associées, telles que les avis de sécurité et

les notices de champ

- Matériel : Fournit une vue chronologique détaillée de la fin de vie du matériel (par exemple, les dates de fin de vente, de dernière livraison et de dernière date d'assistance)
- le logiciel Cisco IOS: Fournit une vue chronologique détaillée de la fin de vie du logiciel

Étiquettes de ressources

Les étiquettes d'inventaire sont des étiquettes personnalisées que vous attribuez aux ressources d'inventaire dans Cisco IQ. Une balise est une paire clé/valeur que vous définissez (par exemple, Environnement : Produit ou Étiquette : Campus). Vous pouvez affecter des étiquettes à des ressources individuelles ou à plusieurs ressources à la fois, et vous pouvez filtrer votre inventaire par étiquette pour trouver rapidement les ressources qui vous intéressent.

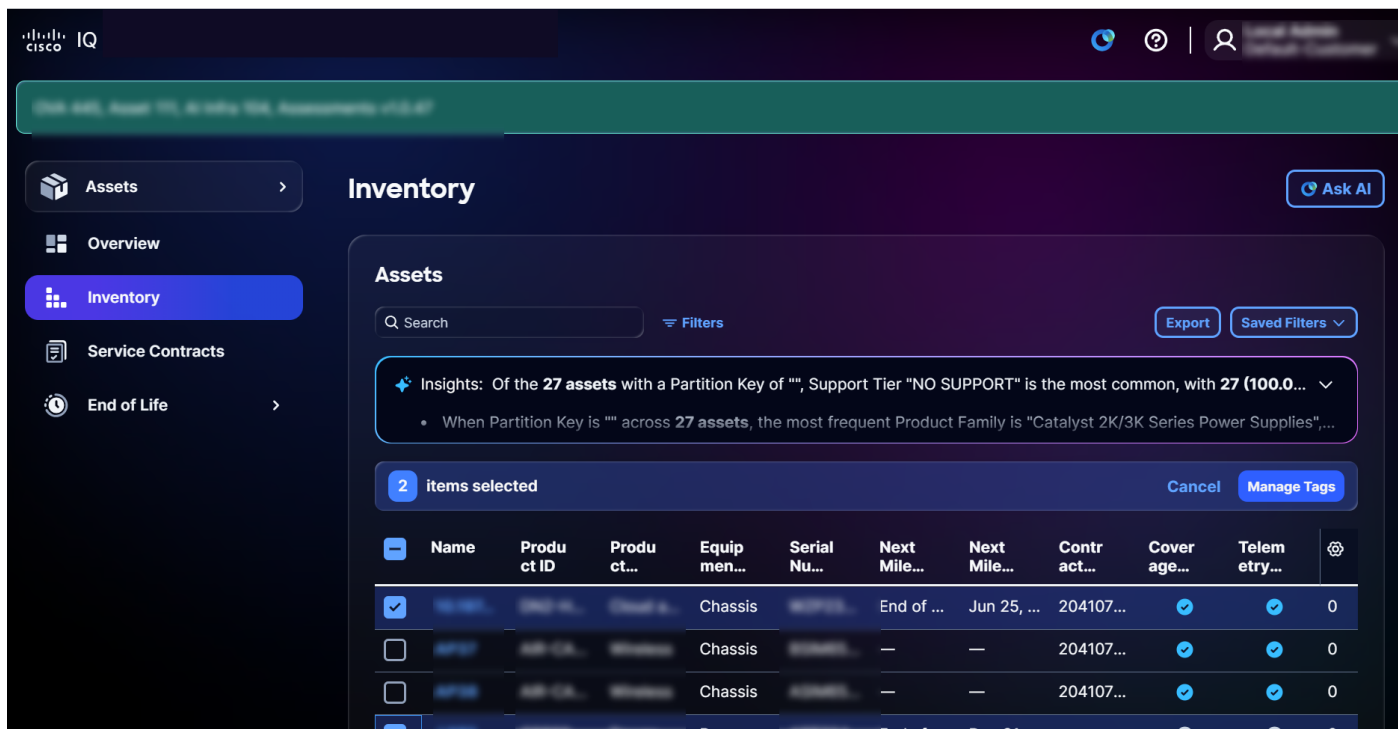
 Remarque : Après la création d'une balise par un administrateur de compte, les utilisateurs peuvent affecter une balise à une ressource.

Affectation de balises

L'affectation de balises à des ressources sélectionnées dans la vue Inventaire permet d'organiser et de classer les ressources pour un filtrage, des rapports et une gestion améliorés.

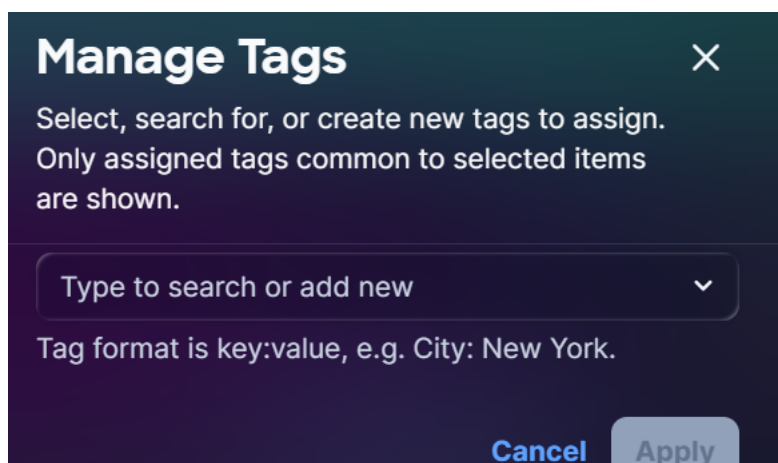
Pour affecter une balise à une ressource :

1. Accédez à Immobilisations > Inventaire.



Étiquetage des ressources

2. Activez les cases à cocher des ressources souhaitées.
3. Cliquez sur Gérer les balises. La fenêtre Gérer les balises s'ouvre.



Affectation de balises

4. Dans le champ de texte, entrez ou sélectionnez le nom de la balise dans les options existantes et appuyez sur Entrée.



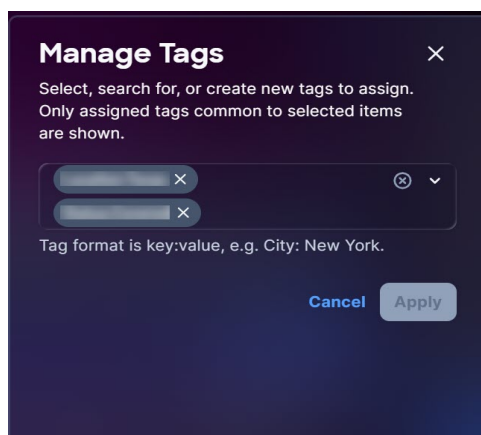
Remarque : Les balises sont au format clé:valeur (par exemple, City:NYC).

5. Cliquez sur Apply.

Suppression des étiquettes de ressources

Pour supprimer une balise d'un ou de plusieurs éléments :

1. Accédez à Immobilisations > Inventaire.
2. Cochez la case en regard d'une ou de plusieurs ressources.
3. Cliquez sur Gérer les balises. La fenêtre Gérer les balises s'ouvre.



Suppression de balises

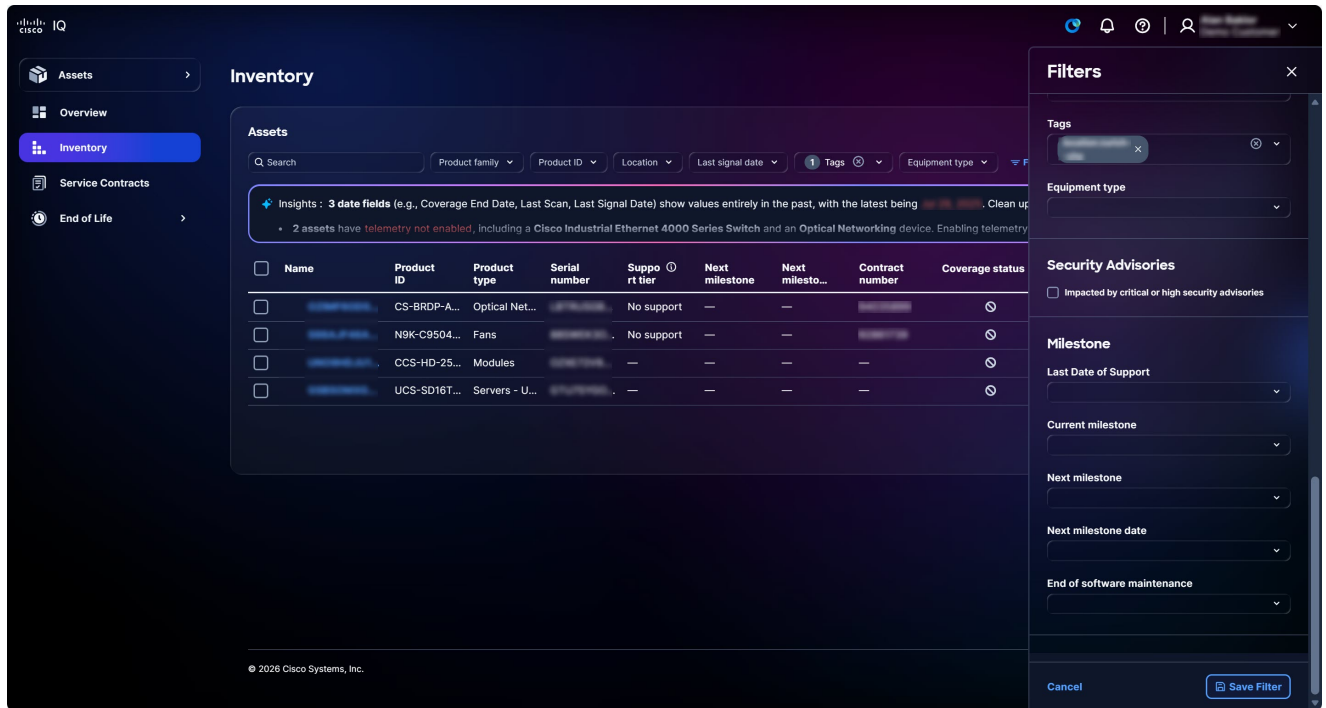
4. Cliquez sur le X sur n'importe quelle balise pour le supprimer de la sélection.
5. Cliquez sur Apply.

Utilisation des étiquettes d'équipement comme filtres

Après avoir créé une balise, vous pouvez l'utiliser comme filtre.

Pour utiliser une balise comme filtre :

1. Accédez à la page Inventaire.
2. Cliquez sur Filtres. La fenêtre Filtres s'ouvre.

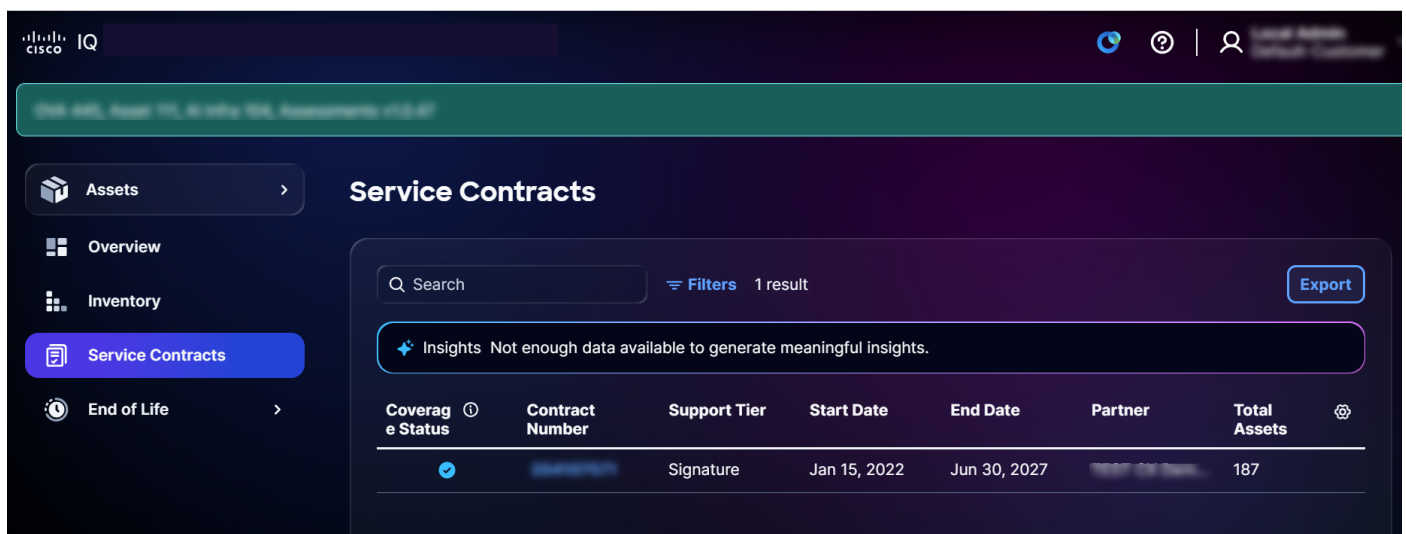


Utilisation de la balise comme filtre

3. Dans la liste déroulante Tags, cochez les cases des balises souhaitées. Après avoir sélectionné la balise, l'affichage de la page Inventaire se met à jour vers l'affichage filtré.

Contrats de service

La page Contrats de service simplifie la supervision des contrats de support en fournissant des résumés et des informations détaillées sur les contrats, ce qui permet une planification efficace du renouvellement et des stratégies de couverture.



Contrats de service

Rechercher et filtrer des vues pour les contrats de service

Vous pouvez filtrer l'affichage de la liste en sélectionnant un filtre dans les listes déroulantes. Vous pouvez également rechercher des contrats de service en saisissant le numéro de contrat dans le champ Rechercher.

Exporter des contrats de service

Cliquez sur Export pour enregistrer une liste filtrée de contrats au format .xls ou .csv. Pour plus d'informations, consultez [Exportation d'informations](#) dans Fonctionnalités du module commun.

Récapitulatif EA des services

La page Récapitulatif des contrats de services d'entreprise fournit une vue consolidée de la croissance de la base installée dans votre portefeuille d'actifs. Les données proviennent directement des dossiers de la base installée de Cisco, ce qui vous permet, ainsi qu'aux équipes chargées des comptes, d'avoir une vue cohérente des changements de portefeuille au fil du temps.

La page Récapitulatif EA des services affiche les informations suivantes :

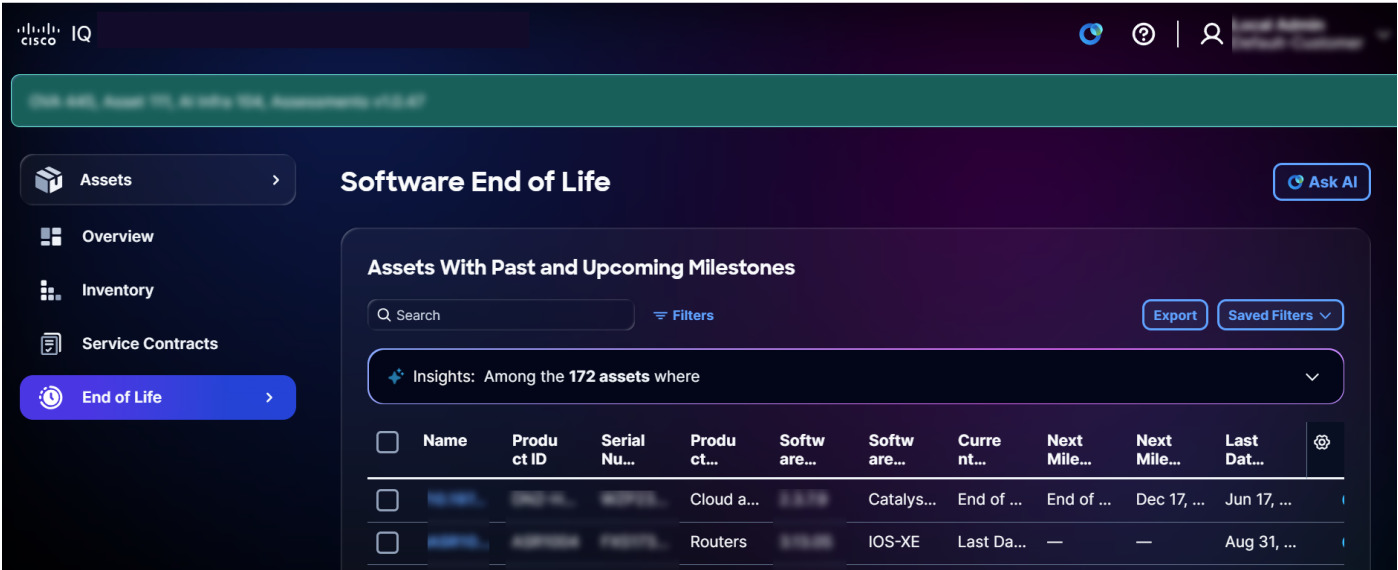
- Ressources ajoutées : Nouvelles ressources ajoutées à la base installée au cours de la période de reporting
- Changement net : Modification globale de la taille de la base installée pour la période de rapport

 Remarque : L'accès à la page Récapitulatif de l'évaluation environnementale des services peut être soumis à des exigences de rôle et d'autorisation. Contactez votre administrateur de compte si cette page n'est pas visible dans votre navigation.

Fin de vie

Les pages Hardware End of Life et Software End of Life fournissent des informations détaillées sur la fin de vie des produits, ce qui fournit aux utilisateurs l'assistance nécessaire pour gérer de manière proactive les cycles d'actualisation des produits et la couverture de l'assistance. Si vous cliquez sur une ressource dans les pages de fin de vie, vous êtes redirigé vers la ressource

appropriée dans la page Inventaire.



Fin de vie du logiciel

Analyse de fin de vie

Le panneau Insights de la page End of Life affiche une présentation basée sur l'IA des ressources avec un dernier jour d'assistance défini. Cliquez sur Analyse complète pour afficher des visualisations telles que des graphiques, des tableaux de bord et des graphiques qui fournissent des informations supplémentaires. Voir [Analyser les données](#) dans les caractéristiques communes du module pour plus de détails.

Exportation de fin de vie

Cliquez sur Export pour enregistrer une liste filtrée d'actifs en fin de vie au format .xls ou .csv. Pour plus d'informations, consultez [Exportation d'informations](#) dans Fonctionnalités du module commun.

Module Évaluations

Le module Assessments fournit un cadre d'évaluation qui vous permet d'examiner et de limiter de manière proactive les risques liés à la sécurité, à la stabilité, à la capacité, à la conformité et au vieillissement, tout en préservant la sécurité, la stabilité et la fiabilité des réseaux.

Concepts de base

Le module Évaluations repose sur les concepts fondamentaux suivants :

- **Évaluation** : une évaluation systématique des entités de l'infrastructure par rapport à des critères prédéfinis pour mesurer les performances, la conformité, la sécurité ou la capacité opérationnelle ; Les évaluations sont déclenchées à la demande, selon un planning ou par un événement
- **Exécution de l'évaluation** : Une instance ou une exécution unique d'une évaluation ; Chaque exécution crée un nouvel enregistrement d'exécution qui suit l'étendue, le mécanisme de déclenchement, l'horodatage et les données résultantes produites par l'évaluation
- **Recherche** : Observation validée et exploitable identifiant une lacune, un risque, un problème ou un état remarquable. Les résultats représentent les données au niveau du sol au cours d'une évaluation
- **Insight** : Une conclusion analytique de niveau supérieur dérivée de modèles ou de tendances à travers plusieurs résultats. Les informations permettent d'interpréter les résultats dans un contexte commercial ou opérationnel plus large
- **Recommandation** : une prescription spécifique et exploitable liée à des conclusions ou à des idées ; Les recommandations fournissent une orientation claire sur les étapes nécessaires pour résoudre les problèmes identifiés ou tirer parti des opportunités
- **Rapport** : Un document structuré qui regroupe les conclusions, les points de vue et les recommandations pour un public cible ; Les rapports constituent le principal élément livrable pour communiquer les résultats des évaluations aux clients, aux cadres et aux équipes techniques

Accès au module Évaluations

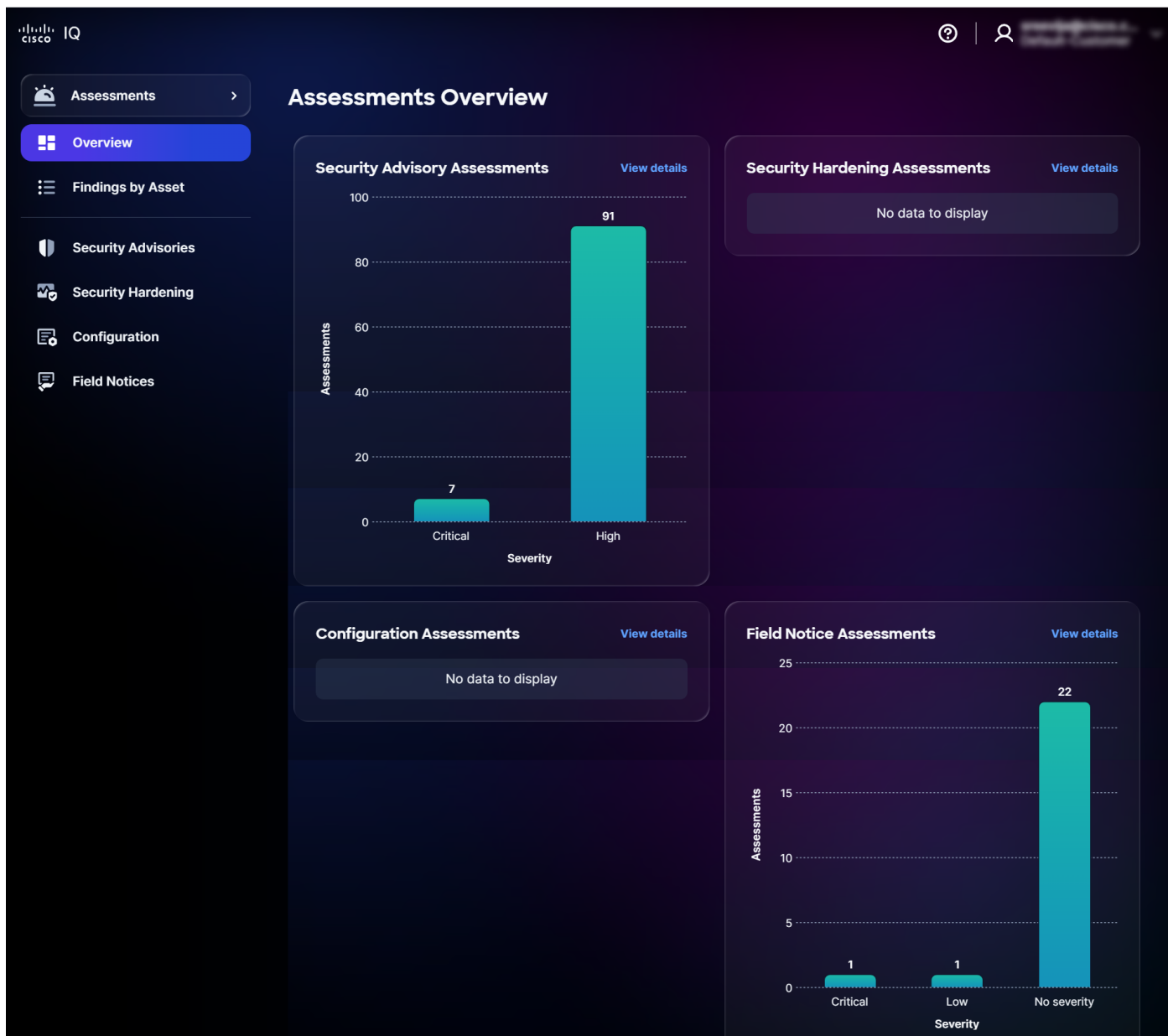
Pour accéder aux fonctions de sécurité et d'évaluation de l'appliance virtuelle, choisissez le menu Accueil > Évaluations ou cliquez sur Évaluations dans la section Application de la page d'accueil > onglet Launchpad. La page Aperçu des évaluations s'affiche.



Remarque : Le module d'évaluation peut également être lancé à partir de Configuration système > Gestion des packages.

Présentation des évaluations

La page Aperçu des évaluations affiche le tableau de bord suivant :



Présentation des évaluations

Le tableau de bord affiche les informations suivantes :

- Évaluations des conseils de sécurité : Affiche les évaluations des avis de sécurité, classées par gravité Critique et Élevée
- Évaluations du renforcement de la sécurité : Affiche les ressources qui ne respectent pas les règles de sécurisation renforcée, classées par gravité Élevée, Moyenne, Faible et Informationnelle
- Évaluations de la configuration : Affiche les ressources ne respectant pas les règles de conformité de configuration, classées par gravité critique, élevée, moyenne, faible et informationnelle

- Évaluations des avis de terrain : Affiche les évaluations des notices de champ, classées par gravité Critique, Élevée et Sans objet



Remarque : Vous ne pouvez afficher que les ressources auxquelles vous êtes autorisé à accéder.

Résultats par actif

La page Résultats de la recherche par actif fournit la liste des actifs qui ont été évalués à l'aide d'au moins une des évaluations suivantes : Avis de sécurité, renforcement de la sécurité, configuration et notices de terrain.

Name	Importance	IP Address	Serial Number	Security Advisory	Security Hardening	Configuration	Field Notice	Signature
Security A	Low	10.10.10.10	10000000	5	11	32	1	Signature
Security A	Low	10.10.10.10	10000000	5	11	32	1	Signature
Security A	Low	10.10.10.10	10000000	5	11	32	1	Signature
Security A	Low	10.10.10.10	10000000	5	11	32	1	Signature
Security A	Low	10.10.10.10	10000000	5	11	32	1	Signature

Constatations Par Actif

Rechercher et filtrer des vues pour les résultats par ressource

Vous pouvez filtrer l'affichage de liste en choisissant un filtre dans les listes déroulantes ou en cliquant sur Filtres et en choisissant une option dans la liste des filtres disponibles. Vous pouvez également rechercher des résultats par actif dans le champ Rechercher.



Remarque :

- Certains filtres peuvent être masqués en fonction des paramètres de zoom de l'écran.
- Différents filtres sont disponibles en fonction de vos rôles et autorisations.

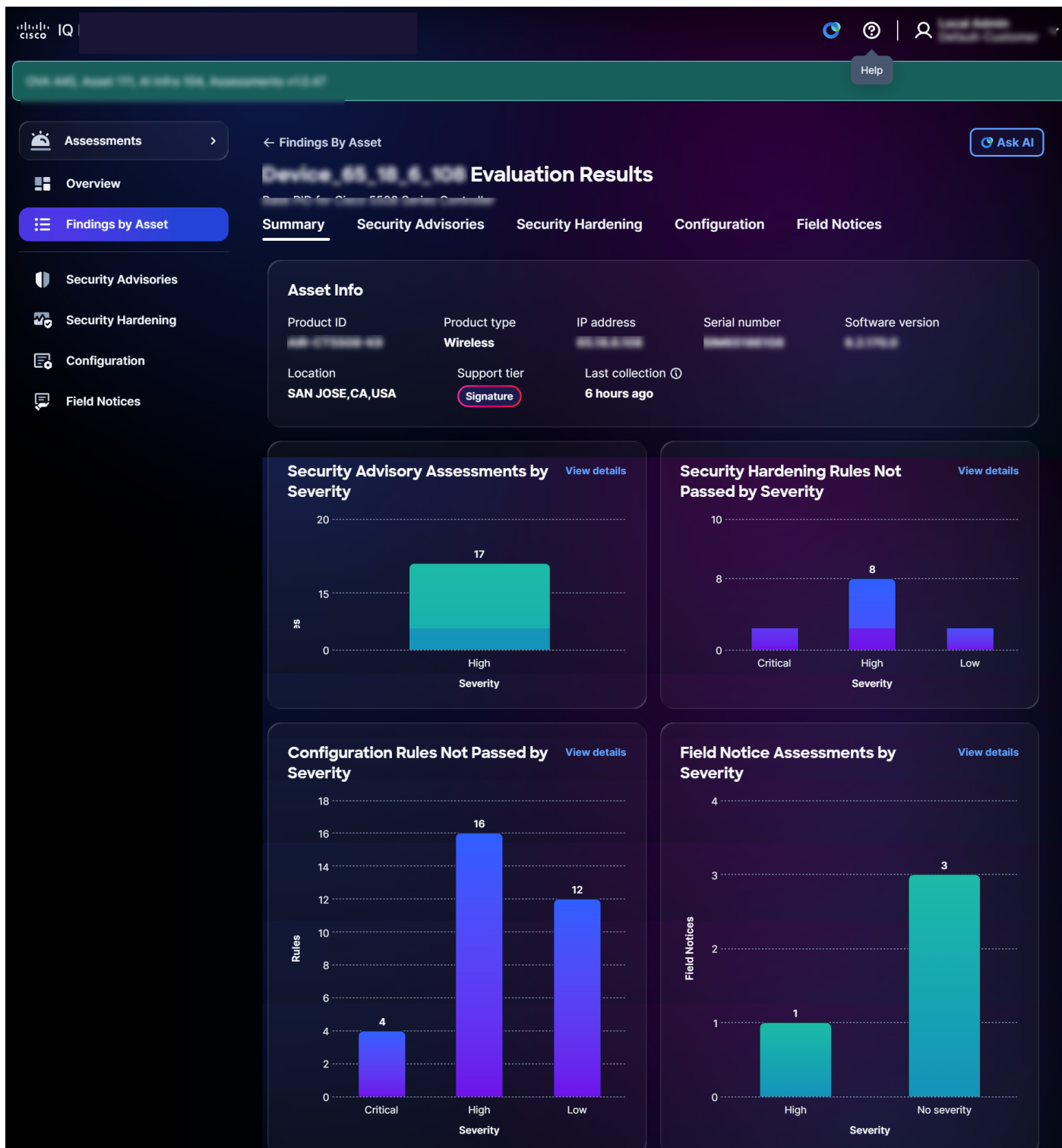
Exportation des conclusions par actif

Pour exporter la vue de liste Résultats de la recherche par actif, cliquez sur Exporter. Consultez [Exportation d'informations](#) pour plus d'informations.

Voir les résultats par détail d'immobilisation

Pour afficher les détails des résultats par actif, cliquez sur un actif. Les onglets suivants affichent les détails de l'immobilisation sélectionnée :

- **Résumé:** Fournit des informations détaillées sur les ressources, notamment le nombre d'avis de sécurité, de renforcement de la sécurité, de configuration et d'avis sur site
- **Avis de sécurité :** Fournit une liste des évaluations de conseils de sécurité associées
- **Renforcement de la sécurité :** Fournit une liste des ressources dont les règles de renforcement de la sécurité échouent
- **Configuration:** Fournit une liste des ressources qui échouent aux règles des meilleures pratiques de configuration
- **Notes de champ :** Fournit une liste des évaluations d'avis de terrain associées



Résultats par détail d'actif

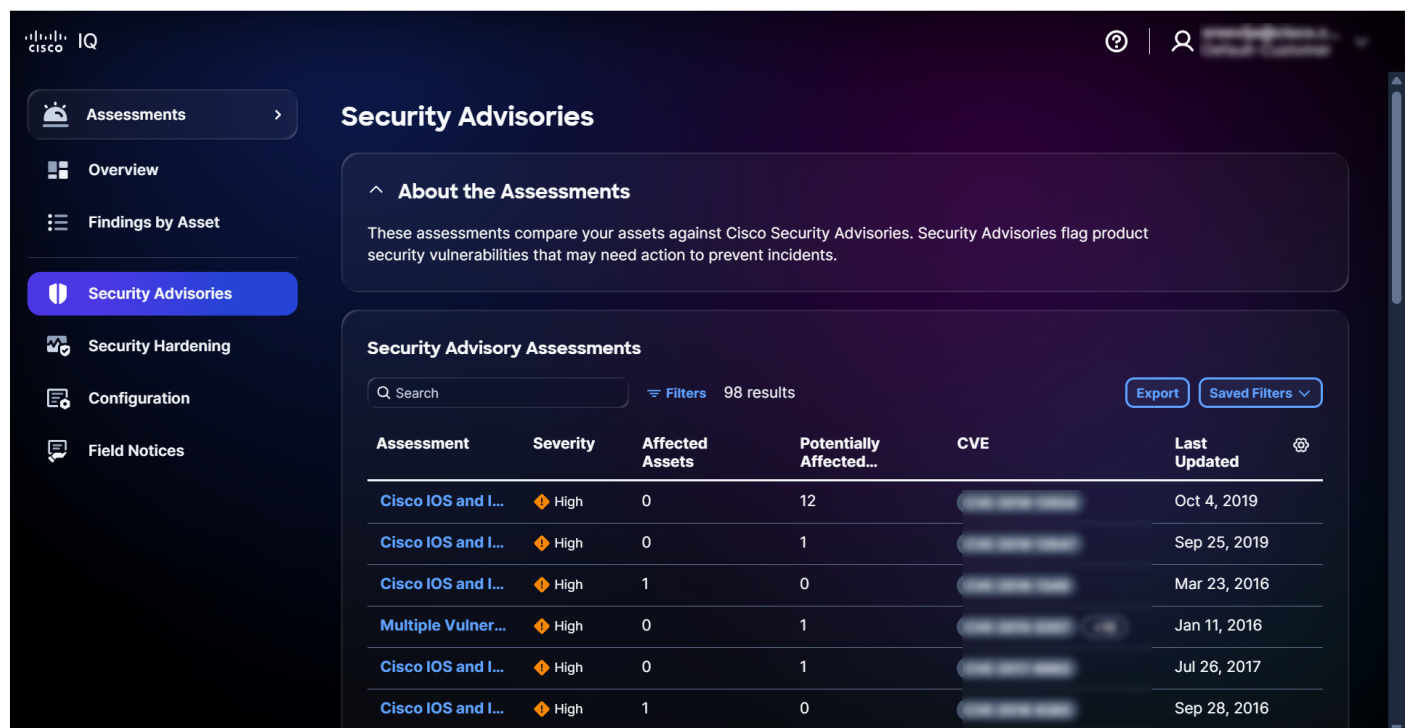
Lorsque vous cliquez sur Afficher les détails sur une vignette, la page est redirigée vers la page appropriée dans le module.

Lorsque vous cliquez sur Afficher les détails complets de l'équipement, la page de vue des détails de l'équipement s'affiche.

Bulletins de renseignements de sécurité

Les évaluations des conseils de sécurité identifient les vulnérabilités et les classent par ordre de priorité en fonction de leur risque, de leur gravité et de leur degré de criticité, améliorant ainsi les capacités de gestion des risques de l'entreprise. Les avis de sécurité fournissent des informations précises sur les vulnérabilités, permettent d'accélérer la réduction des menaces critiques et garantissent l'alignement avec les objectifs de conformité et commerciaux. Cela renforce la sécurité, optimise l'allocation des ressources et favorise la résilience face aux menaces en constante évolution dans l'entreprise. Les avis de sécurité sont automatiquement mis à jour dans Cisco IQ dès qu'ils sont publiés.

La page Avis de sécurité fournit une liste de tous les avis de sécurité comportant des vulnérabilités détectées au sein de l'organisation. Cliquez sur un avis dans la liste des évaluations de conseils de sécurité pour accéder à la vue détaillée correspondante.



Assessment	Severity	Affected Assets	Potentially Affected...	CVE	Last Updated
Cisco IOS and I...	High	0	12	CVE-2019-11961	Oct 4, 2019
Cisco IOS and I...	High	0	1	CVE-2019-11961	Sep 25, 2019
Cisco IOS and I...	High	1	0	CVE-2019-11961	Mar 23, 2016
Multiple Vulner...	High	0	1	CVE-2016-0728, CVE-2016-0729	Jan 11, 2016
Cisco IOS and I...	High	0	1	CVE-2017-15587	Jul 26, 2017
Cisco IOS and I...	High	1	0	CVE-2016-0728	Sep 28, 2016

Bulletins de renseignements de sécurité

Recherche et filtrage des vues pour les avis de sécurité

Vous pouvez filtrer l'affichage de la liste en sélectionnant un filtre dans la liste déroulante. Vous pouvez également rechercher des évaluations de conseil de sécurité en saisissant le nom de l'évaluation dans le champ Rechercher.

 Remarque : certains filtres peuvent être masqués en fonction des paramètres de zoom de l'écran. Certains filtres peuvent être masqués en fonction des paramètres de zoom de l'écran. Différents filtres sont disponibles en fonction de vos rôles et autorisations. Les valeurs de gravité manquantes s'affichent sous la forme « - » avec une info-bulle descriptive.

Exportation des avis de sécurité

Pour exporter des évaluations de conseils de sécurité, cliquez sur Exporter. Consultez [Exportation d'informations](#) pour plus d'informations.

Afficher les détails de l'évaluation Security Advisory

Cliquez sur une évaluation pour afficher des détails supplémentaires à son sujet. La page de détails fournit des informations telles que le score CVSS (Common Vulnerability Scoring System), le score CVE (Common Vulnerabilities and Exposures), la gravité, et un lien vers l'avis de sécurité Cisco référencé.

Vous pouvez afficher les types de résultats suivants dans le tableau des résultats de l'évaluation :

- **Affecté** : Indique que l'actif ou le composant présente une vulnérabilité confirmée qui peut être exploitée par un pirate, nécessitant une correction
- **Potentiellement affecté** : indique que l'actif ou le composant présente des signes susceptibles d'entraîner une vulnérabilité, mais qu'il n'est pas définitivement confirmé ; une enquête plus approfondie peut être nécessaire

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

← Security Advisories

Cisco IOS and IOS XE Software Session Initiation Protocol Denial of Service Vulnerability

About the Assessment

A vulnerability in the common Session Initiation Protocol (SIP) library of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient sanity checks on an internal data structure....

Show more

Severity

High

CVE

CVSS score

8.8

Version

1.1

First published

Sep 25, 2019

Last updated

Oct 4, 2019

References

[Security Advisory](#)

Asset Results

Q Search

Filters 12 results

Export

Saved Filters

Asset	Result	Product ID	IP Address	Serial Number	Support Tier
ISR44...	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature
Isr4431	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature

Détails des avis de sécurité

Rechercher et filtrer des vues pour les résultats d'évaluation des ressources

Vous pouvez filtrer l'affichage de liste en choisissant un filtre dans les listes déroulantes ou en cliquant sur Filtres et en choisissant une option dans la liste des filtres disponibles. Vous pouvez également rechercher des ressources en saisissant leur nom dans le champ Rechercher.

 Remarque : Certains filtres peuvent être masqués en fonction des paramètres de zoom de l'écran. Différents filtres sont disponibles en fonction de vos rôles et de vos autorisations.

Afficher les résultats d'évaluation

Pour afficher les détails d'un résultat d'évaluation, cliquez sur une ressource dans le tableau Résultat de l'évaluation. La page de détails des résultats de l'évaluation de l'actif s'affiche.

Security Advisories > Cisco Secure Boot Hardware Tampering Vulnerability

Device: 65, 10, 4, 106 Result [Ask AI](#)

Assessment: Cisco Secure Boot Hardware Tampering Vulnerability

Result Details Potentially affected

Evidence

- ✓ Matched on software type
- ✓ Matched on chassis product ID
- ✓ Matched on module product ID

Additional Verification Needed

1) Software Releases are not checked for the automation of this Security Advisory. You must manually check your software release against the information in the advisory. 2) Module/Chassis PID level Automation is not done for the following product families. Please refer to the Security Advisory for the impacted PIDs and determine the Vulnerability of the device Cisco 4000 Series Integrated Services Routers Cisco Catalyst 6800 Series Switches Cisco Network Convergence System 5500 Series Routers

About the Assessment

A vulnerability in the logic that handles access control to one of the hardware components in Cisco's proprietary Secure Boot implementation could allow an authenticated, local attacker to write a modified firmware image to the component. This vulnerability affects multiple Cisco products that support hardware...

[Show more](#)

Severity	CVE	CVSS score
High		6.7
First published	Last updated	
May 13, 2019	Nov 20, 2019	
References		
Security Advisory		

About the Asset [View evaluated asset](#)

Product ID	Product type	IP Address
	Switches	
Serial Number	Software version	Location
		SAN JOSE,CA,USA
Support tier		
Signature		

Détails du résultat

Exporter les résultats des ressources pour les avis de sécurité

Pour exporter les résultats des ressources, cliquez sur Exporter. Consultez [Exportation d'informations](#) pour plus d'informations.

Renforcement de la sécurité

Le renforcement de la sécurité offre une visibilité automatisée, quasiment en temps réel, sur la position de sécurité de votre infrastructure réseau en évaluant en permanence les routeurs, les commutateurs et les pare-feu par rapport aux tests de référence standard. Il identifie les failles de configuration et fournit des conseils de correction exploitables, permettant aux administrateurs de compte de réduire efficacement la surface d'attaque et de maintenir un alignement cohérent avec les meilleures pratiques de sécurité rigoureuses de

Cisco. En centralisant la surveillance de la conformité et en simplifiant le processus de renforcement, le module transforme la gestion de la sécurité d'une tâche réactive en une stratégie proactive axée sur les données, garantissant un réseau d'entreprise résilient et sécurisé.

 Remarque : Les évaluations du renforcement de la sécurité sont disponibles exclusivement pour les ressources avec niveaux d'assistance standard.

Affichage des évaluations de renforcement de la sécurité

La page Évaluation du renforcement de la sécurité affiche les informations suivantes :

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Security Hardening Assessment

This assessment only applies to assets with Standard or Signature support. Learn about your coverage details in [Cisco Support Tiers](#).

About the Assessment

This assessment evaluates your assets against Cisco OS Hardening Guides. It detects configuration deviations across your infrastructure that may affect security posture, or risk exposure. Each security hardening rule is evaluated across your covered assets, with findings prioritized by severity to help you...
[Show more](#)

Execution Outcome for Jul 20, 2026, 5:40 AM

Summary

Rule evaluations

179

Assets included

146

Rule evaluations

The number of assets evaluated by a rule may differ based on its pre-checks.

Q Search

Filters

179 results

Export

Saved Filters

Rule	Severity	Assets Evaluated	Did Not Pass	Passed	Inconclusi ve	Not Appli...	Soft war...
Console M...	Medium	6	0	0	6	0	IOS
IGP MD5 A...	High	6	0	0	6	0	IOS
Minimum P...	High	31	31	0	0	0	AireOS

Renforcement de la sécurité

- À propos de l'évaluation : Fournit des détails supplémentaires en résumant l'objectif de l'évaluation
- Résultat de l'exécution : Fournit un résumé des résultats de l'évaluation des ressources, y compris le nombre total d'évaluations de règles et de ressources incluses
- Évaluations des règles : Fournit des informations détaillées sur la règle, y compris la gravité, les ressources évaluées, les échecs, les réussites, les non concluantes, les

non applicables et le type de logiciel

- **Gravité** : Indique le niveau d'importance ou d'impact de l'évaluation des règles
- **Ressources évaluées** : Indique le nombre total d'actifs évalués par rapport aux critères de la règle
- **Échec de l'opération** : Fournit les ressources qui n'ont pas satisfait aux critères de la règle pendant l'évaluation
- **Réussite** : Fournit les ressources qui répondent aux critères de la règle au cours de l'évaluation
- **Non concluant** : Fournit les ressources pour lesquelles l'évaluation n'a pas pu déterminer l'échec
- **Sans objet** : Indique les actifs ou les scénarios pour lesquels la règle ne s'applique pas ou n'est pas pertinente
- **Type de logiciel** : Fournit le type de logiciel des ressources

Recherche et filtrage des vues pour les règles

Vous pouvez filtrer l'affichage de liste en choisissant un filtre dans les listes déroulantes ou en cliquant sur Filtres et en choisissant une option dans la liste des filtres disponibles. Vous pouvez également rechercher une règle en entrant son nom dans le champ Rechercher.



Remarque : certains filtres peuvent être masqués en fonction des paramètres de zoom de l'écran. Différents filtres sont disponibles en fonction de vos rôles et autorisations.

Affichage des détails d'évaluation

Pour afficher des détails supplémentaires sur l'évaluation d'une règle, cliquez sur une règle. La page Détails de l'évaluation de la règle s'affiche avec les informations suivantes :

The screenshot shows the Cisco IQ interface for a Security Hardening Assessment. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening (highlighted), Configuration, and Field Notices. The main content area is titled 'Minimum Password Length Policy' and shows it was evaluated on Jul 20, 2026, at 5:39 AM. An 'Ask AI' button is in the top right.

About the Rule

Check 'Min. Password length' in show switch config, and warn if it is lower than 8. Proper security configuration protects the wireless infrastructure from unauthorized access, data interception, and compliance violations.

Severity: **High** (High icon) | Software type: **AireOS** | Assets evaluated: **31**

Results Summary 31 assets

0 Passed ✓	31 Didn't pass ✖	0 Inconclusive ⚠	0 Not applicable ⚙
----------------------	----------------------------	----------------------------	------------------------------

Asset Results

Search: [] Filters: 31 results [Export] [Saved Filters]

Asset	Result	Product ID	Serial Number	IP Address	Support Tier
Device_...	✖ Didn't pass	...	...	...	Signature
Device_...	✖ Didn't pass	...	...	...	Signature
Device_...	✖ Didn't pass	...	...	...	Signature
Device_...	✖ Didn't pass	...	...	...	Signature
Device_...	✖ Didn't pass	...	...	...	Signature

Affichage des règles

- À propos de la règle : Fournit des détails sur la règle, tels que la gravité, le type de logiciel, la version et les ressources évaluées, et inclut des liens descriptifs libellés vers la documentation source appropriée
- Résumé des résultats : Fournit un résumé des résultats de ressources associés à la règle, tels que Passed, Has not pass, Inconclusive, and Not applicable
- Résultats des ressources : Fournit une liste de ressources avec des détails tels que l'actif, le résultat, l'ID de produit, le numéro de série, l'adresse IP et le niveau de support



Remarque : Cisco IQ fournit une orientation claire lorsqu'une conclusion d'évaluation est « non concluante », expliquant la cause (par exemple, absence de télémétrie ou système d'exploitation non pris en charge) et recommandant des étapes comme la vérification de la collecte des données, la mise à jour des informations d'identification ou l'actualisation des données. Des liens vers la documentation appropriée sont également fournis pour vous aider à résoudre les problèmes.

Rechercher et filtrer des vues pour les règles d'équipement

Vous pouvez filtrer l'affichage de liste en choisissant un filtre dans les listes déroulantes ou en cliquant sur Filtres et en choisissant une option dans la liste des filtres disponibles. Vous pouvez également rechercher les résultats de l'évaluation des ressources en saisissant le nom de l'actif dans le champ Rechercher.



Remarque : certains filtres peuvent être masqués en fonction des paramètres de zoom de l'écran. Différents filtres sont disponibles en fonction de vos rôles et autorisations.

Exporter les résultats des ressources

Pour exporter les résultats d'évaluation des règles, cliquez sur Exporter. Consultez [Exportation d'informations](#) pour plus d'informations.

Rechercher et filtrer des vues pour les résultats des équipements

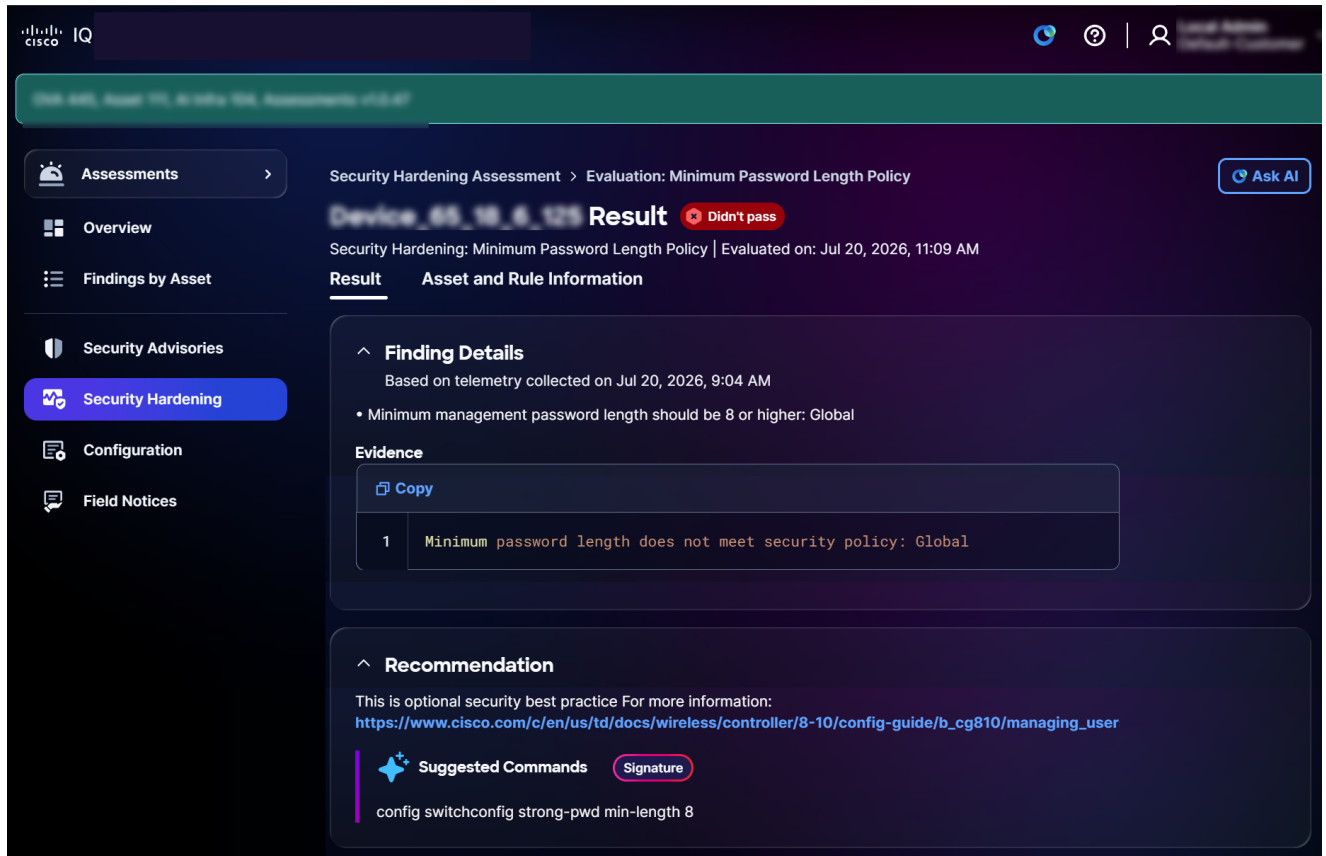
Vous pouvez filtrer l'affichage de liste en choisissant un filtre dans les listes déroulantes ou en cliquant sur Filtres et en choisissant une option dans la liste des filtres disponibles. Vous pouvez également rechercher des résultats d'actifs en saisissant le nom de l'actif dans le champ Rechercher.



Remarque : Certains filtres peuvent être masqués en fonction des paramètres de zoom de l'écran. Différents filtres sont disponibles en fonction de vos rôles et autorisations.

Afficher les résultats des ressources pour le renforcement de la sécurité

Cliquez sur un actif dans Résultats de l'actif pour afficher ses détails. La page des détails des résultats de l'actif affiche des informations en fonction de votre niveau de droit ou de votre niveau.



Niveau standard de renforcement de la sécurité

- Niveau standard
- Recherche de détails : Fournit des informations sur les écarts de configuration identifiés au cours de l'évaluation, ainsi que des journaux de preuves
- Recommandations: Fournit des conseils pour traiter les résultats et assurer la cohérence de la configuration

Afficher les informations sur les ressources et les règles pour renforcer la sécurité

Pour afficher les détails d'un actif et de ses règles, cliquez sur l'onglet Infos sur l'actif et la règle. La page Infos sur les ressources et les règles s'affiche.

À propos de l'actif : Fournit les détails de l'actif tels que l'ID de produit, le type de produit, l'adresse IP, le numéro de série, la version du logiciel, l'emplacement et le niveau de support

- À propos de la règle : Fournit des détails sur les règles (y compris la gravité et le type de logiciel) et l'importance de ce contrôle de durcissement particulier

Configuration

Les évaluations de la configuration évaluent vos ressources par rapport aux meilleures pratiques recommandées en fonction de l'expertise éprouvée de Cisco pour détecter les écarts de configuration susceptibles d'affecter la disponibilité, la sécurité ou les

performances de votre infrastructure. Chaque règle de meilleures pratiques est évaluée pour l'ensemble des ressources couvertes et les conclusions sont classées par ordre de gravité afin de garantir la cohérence de la configuration, une résilience améliorée et une réduction du risque opérationnel.

 Remarque : Les évaluations de configuration sont disponibles uniquement pour les ressources avec des niveaux d'assistance standard.

Affichage des évaluations de configuration

La page Évaluation de la configuration affiche les informations suivantes :

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Configuration Assessment

This assessment only applies to assets with Standard and Signature support. Learn about your coverage details in [Cisco Support Tiers](#).

About the Assessment

This assessment evaluates your assets against recommended best practices based on Cisco's proven expertise. It detects configuration deviations across your infrastructure that may affect availability, security, or performance. Each best practice rule is evaluated across your covered assets, with findings prioritized b...
[Show more](#)

Execution Outcome for Jul 20, 2026, 05:40 AM

Summary

Rule evaluations

729

Assets included

146

Rule Evaluations

The number of assets evaluated by a rule may differ based on its pre-checks.

Q Search

Filters

729 results

Export

Saved Filters

Rule	Severity	Assets	Did Not...	Passed	Inconclus...	Not...	Category
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless
Console Memory Reservation	Medium	6	0	0	6	0	Platform
SSH Server Logging	Medium	10	9	0	0	1	Logging

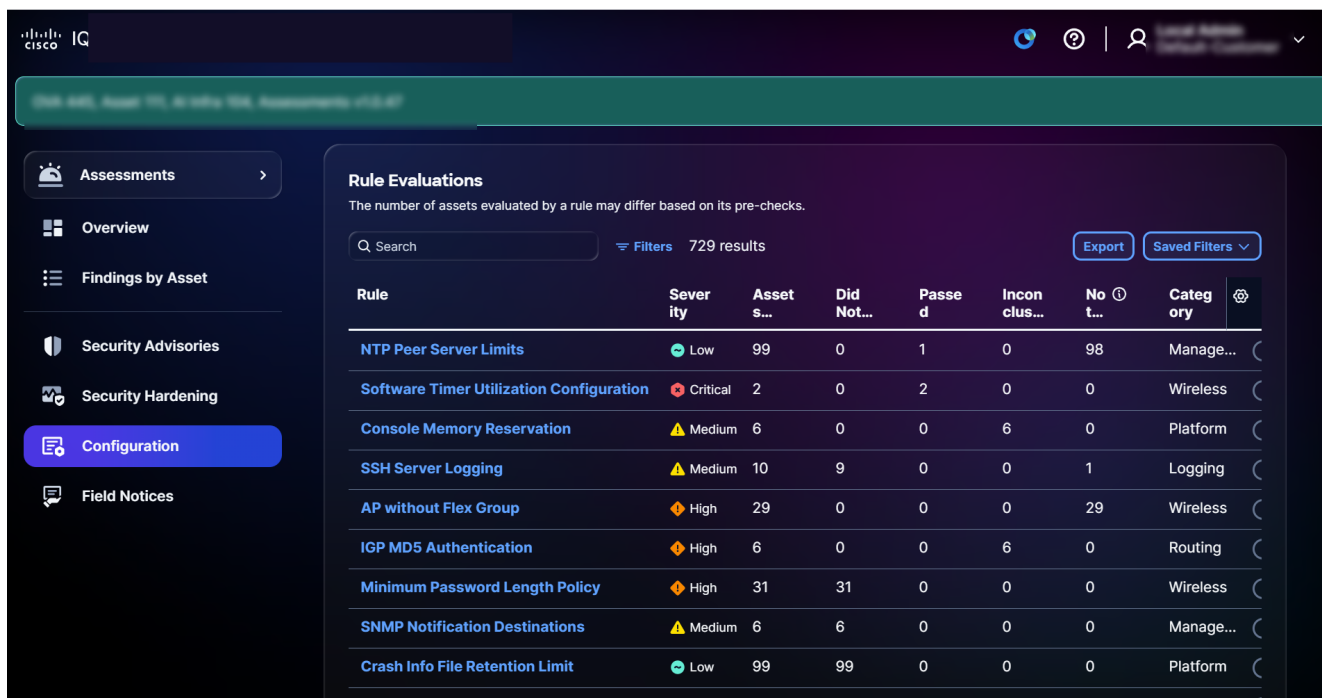
Évaluation de la configuration

- À propos de l'évaluation : Fournit des détails supplémentaires en résumant l'objectif de l'évaluation
- Résumé: Fournit un résumé de l'exécution de la configuration comme Règles évaluées et Ressources évaluées
- Points clés : Fournit des informations sur les lacunes de configuration identifiées générées par l'analyse des modèles et une corrélation des résultats ; elles sont

affichées sous forme de cartes-clés regroupées de manière intelligente pour mettre en évidence les zones les plus critiques qui nécessitent une attention particulière

- Évaluations des règles : Fournit des informations détaillées sur la règle, notamment la gravité, les ressources évaluées, les succès, les échecs, les questions non concluantes, les questions sans objet, la catégorie et le type de logiciel
- Gravité : Indique le niveau d'importance ou d'impact de l'évaluation des règles
- Ressources évaluées : Indique le nombre total d'actifs évalués par rapport aux critères de la règle
- Échec de l'opération : Indique le nombre total d'actifs qui n'ont pas satisfait aux critères de la règle au cours de l'évaluation
- Non concluant : Indique le nombre total de ressources pour lesquelles l'évaluation n'a pas pu s'exécuter
- Réussite : Fournit les ressources qui répondent aux critères de la règle au cours de l'évaluation
- Sans objet : Indique les actifs ou les scénarios pour lesquels la règle ne s'applique pas ou n'est pas pertinente
- Catégorie : Fournit la zone de domaine à laquelle la règle appartient
- Type de logiciel : Indique le type de ressources logicielles auquel la règle s'applique

Recherche et filtrage des vues pour les règles



Rule Evaluations
The number of assets evaluated by a rule may differ based on its pre-checks.

Search: Filters: 729 results Export Saved Filters

Rule	Severity	Asset s...	Did Not...	Passe d	Incon clus...	No t...	Categ ory
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless
Console Memory Reservation	Medium	6	0	0	6	0	Platform
SSH Server Logging	Medium	10	9	0	0	1	Logging
AP without Flex Group	High	29	0	0	0	29	Wireless
IGP MD5 Authentication	High	6	0	0	6	0	Routing
Minimum Password Length Policy	High	31	31	0	0	0	Wireless
SNMP Notification Destinations	Medium	6	6	0	0	0	Manage...
Crash Info File Retention Limit	Low	99	99	0	0	0	Platform

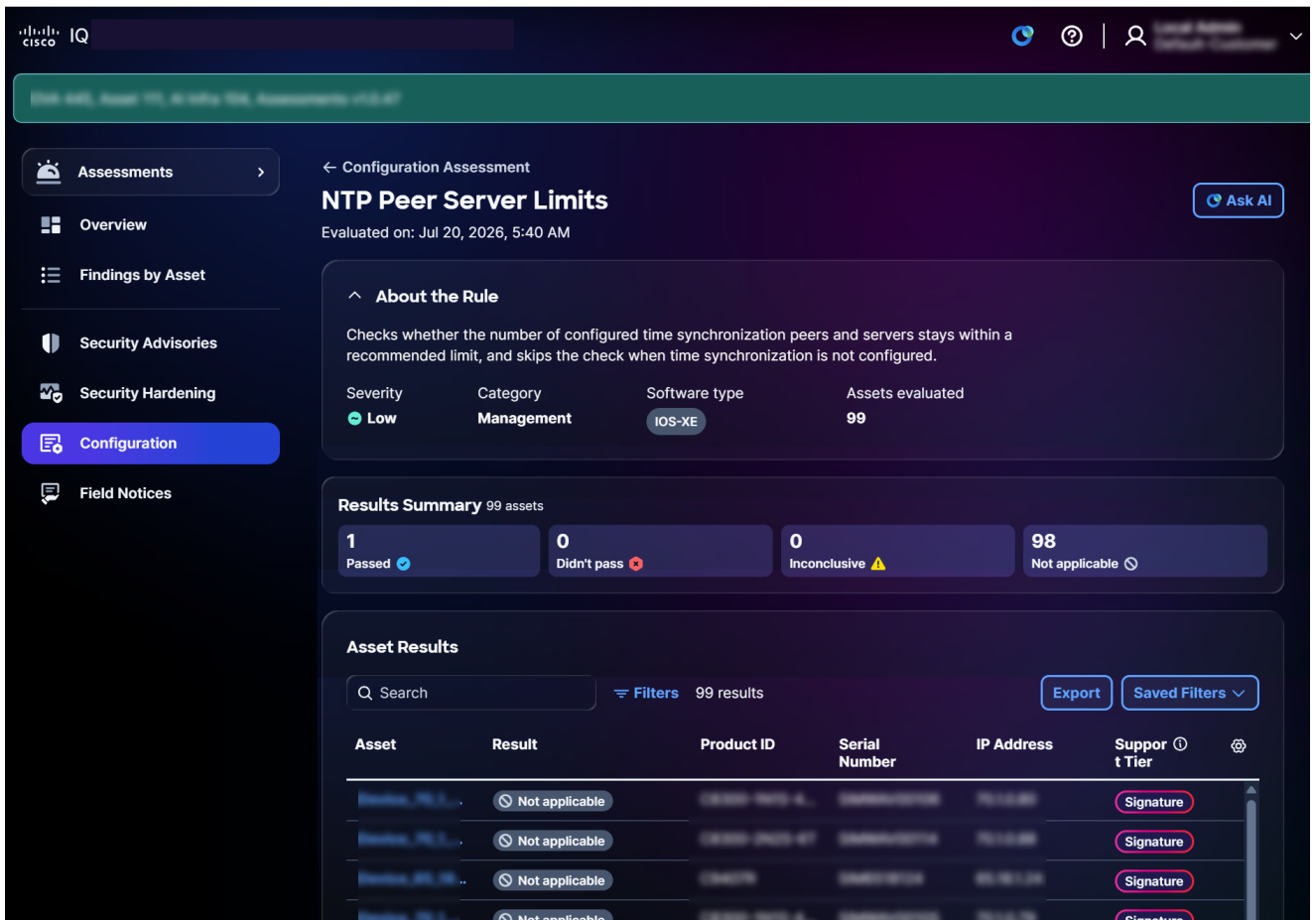
Évaluations des règles

Vous pouvez filtrer l'affichage de liste en choisissant un filtre dans les listes déroulantes ou en cliquant sur Filtres et en choisissant une option dans la liste des filtres disponibles. Vous pouvez également rechercher une règle en entrant son nom dans le champ Rechercher.

 Remarque : Certains filtres peuvent être masqués en fonction des paramètres de zoom de l'écran. Différents filtres sont disponibles en fonction de vos rôles et autorisations.

Affichage des détails d'évaluation

Pour afficher des détails supplémentaires sur l'évaluation d'une règle, cliquez sur une règle. La page Détails de l'évaluation de la règle s'affiche avec les informations suivantes :



The screenshot shows the Cisco IQ interface for a Configuration Assessment. The main heading is 'NTP Peer Server Limits', evaluated on Jul 20, 2026, at 5:40 AM. The assessment is categorized as 'Low' severity, 'Management' category, and 'IOS-XE' software type, with 99 assets evaluated. The 'Results Summary' shows 1 Passed, 0 Didn't pass, 0 Inconclusive, and 98 Not applicable. The 'Asset Results' table lists individual assets with their results, product IDs, serial numbers, IP addresses, and support tiers.

Asset	Result	Product ID	Serial Number	IP Address	Support Tier
ios-xe-10.1.1.1	Not applicable	CISCO IOS-XE	1000000000	10.1.1.1	Signature
ios-xe-10.1.1.2	Not applicable	CISCO IOS-XE	1000000001	10.1.1.2	Signature
ios-xe-10.1.1.3	Not applicable	CISCO IOS-XE	1000000002	10.1.1.3	Signature
ios-xe-10.1.1.4	Not applicable	CISCO IOS-XE	1000000003	10.1.1.4	Signature

Évaluation

- À propos de la règle : Fournit des détails sur une règle telle que la gravité, la catégorie, le type de logiciel et les ressources évaluées et inclut des liens descriptifs libellés vers la documentation source appropriée
- Résumé des résultats : Fournit les résultats globaux des ressources en affichant le nombre d'actifs dans les états Passed, Not pass, Inconclusive et Not applicable
- Résultats des ressources : Fournit une liste des ressources affectées par la règle sélectionnée avec l'état du résultat

 Remarque : Cisco IQ fournit une orientation claire lorsqu'une conclusion d'évaluation est « non concluante », en expliquant la cause (par exemple, absence de télémétrie ou système d'exploitation non pris en charge) et en recommandant des étapes telles que la vérification de la collecte des données, la mise à jour des informations d'identification ou l'actualisation des données. Des liens vers la documentation appropriée sont également fournis pour vous aider à résoudre les problèmes. Le module d'évaluation prend en charge la sélection de plusieurs catégories de règles, ce qui permet un traitement et une évaluation simultanés de plusieurs catégories de règles.

Exporter les résultats des ressources

Pour exporter les résultats des ressources pour les règles, cliquez sur Exporter. Consultez [Exportation d'informations](#) pour plus d'informations.

Rechercher et filtrer des vues pour les résultats des équipements

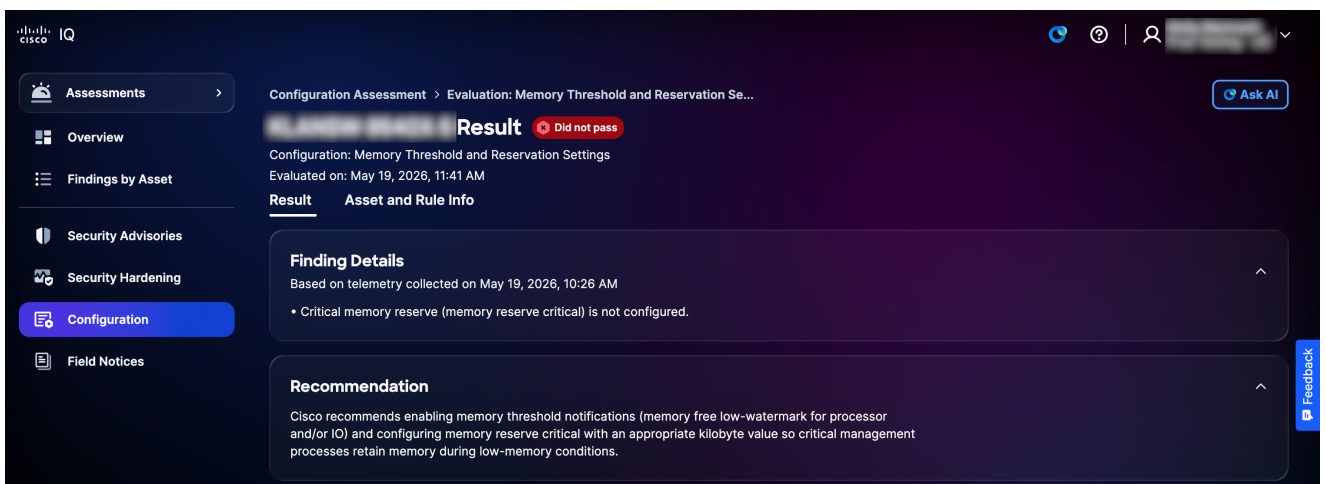
Vous pouvez filtrer l'affichage de liste en choisissant un filtre dans les listes déroulantes ou en cliquant sur Filtres et en choisissant une option dans la liste des filtres disponibles. Vous pouvez également rechercher des résultats d'actifs en saisissant le nom de l'actif dans le champ Rechercher.

 Remarque : Certains filtres peuvent être masqués en fonction des paramètres de zoom de l'écran. Différents filtres sont disponibles en fonction de vos rôles et autorisations.

Afficher les résultats des ressources pour les évaluations de configuration

Pour afficher les détails des résultats d'immobilisation, cliquez sur une immobilisation dans les résultats d'immobilisation.

La page des détails des résultats de l'actif affiche des informations en fonction de votre niveau de droit ou de votre niveau.



The screenshot displays the Cisco IQ interface for a Configuration Assessment. The left sidebar contains navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (highlighted), and Field Notices. The main content area shows the 'Configuration Assessment' details for 'Evaluation: Memory Threshold and Reservation Settings'. A 'Result' card indicates 'Did not pass' with a red status. Below this, the 'Finding Details' section states: 'Based on telemetry collected on May 19, 2026, 10:26 AM' and 'Critical memory reserve (memory reserve critical) is not configured.' The 'Recommendation' section provides guidance: 'Cisco recommends enabling memory threshold notifications (memory free low-watermark for processor and/or IO) and configuring memory reserve critical with an appropriate kilobyte value so critical management processes retain memory during low-memory conditions.' A 'Feedback' button is visible on the right side of the interface.

Niveau standard de configuration

- Niveau standard
- Recherche de détails : Fournit des informations sur les écarts de configuration identifiés au cours de l'évaluation, ainsi que des journaux de preuves
- Recommandations: Fournit des conseils pour traiter les résultats et assurer la cohérence de la configuration

Afficher les informations sur les ressources et les règles pour les évaluations de configuration

Pour afficher les informations détaillées sur les ressources et les règles, cliquez sur l'onglet Infos sur les ressources et les règles.

The screenshot displays the Cisco IQ Configuration Assessment interface. The left sidebar contains navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (highlighted), and Field Notices. The main content area shows the 'Configuration Assessment > Evaluation: NTP Peer Server Limits' page. The top right has an 'Ask AI' button. The page title is 'Device_70_1.0.0.00 Result' with a 'Not applicable' status. Below this, it states 'Configuration: NTP Peer Server Limits' and 'Evaluated on: Jul 20, 2026, 11:10 AM'. The 'Result' tab is active, showing 'Asset and Rule Info'. The 'About the Asset' section includes a table with the following data:

Product ID	Product type	IP address	Serial number	Software version
10000000000000000000	Routers	70.1.0.00	10000000000000000000	15.0.0

Below the table, the 'Location' is 'SAN JOSE, CA, USA' and the 'Support tier' is 'Signature'. A 'View evaluated asset' link is in the top right of this section. The 'About the Rule' section explains the rule: 'Checks whether the number of configured time synchronization peers and servers stays within a recommended limit, and skips the check when time synchronization is not configured.' It also shows the rule details: Severity is 'Low', Category is 'Management', and Software type is 'IOS-XE'.

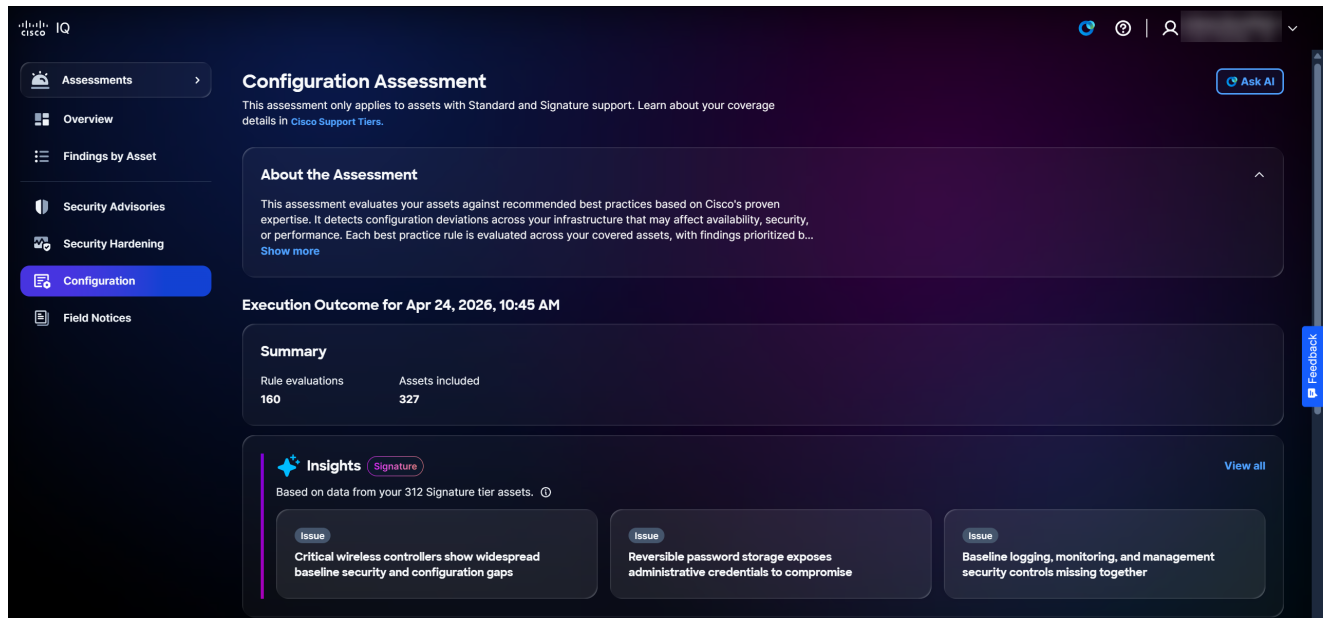
Informations sur les ressources et les règles

La page Infos sur les ressources et les règles s'affiche avec les informations suivantes :

- À propos de l'actif : Fournit les détails d'une ressource, tels que l'ID de produit, le type de produit, l'adresse IP, le numéro de série, la version du logiciel, l'emplacement et le niveau de support
- À propos de la règle : Fournit les détails d'une règle telle que la gravité, la catégorie et le type de logiciel

Afficher les informations

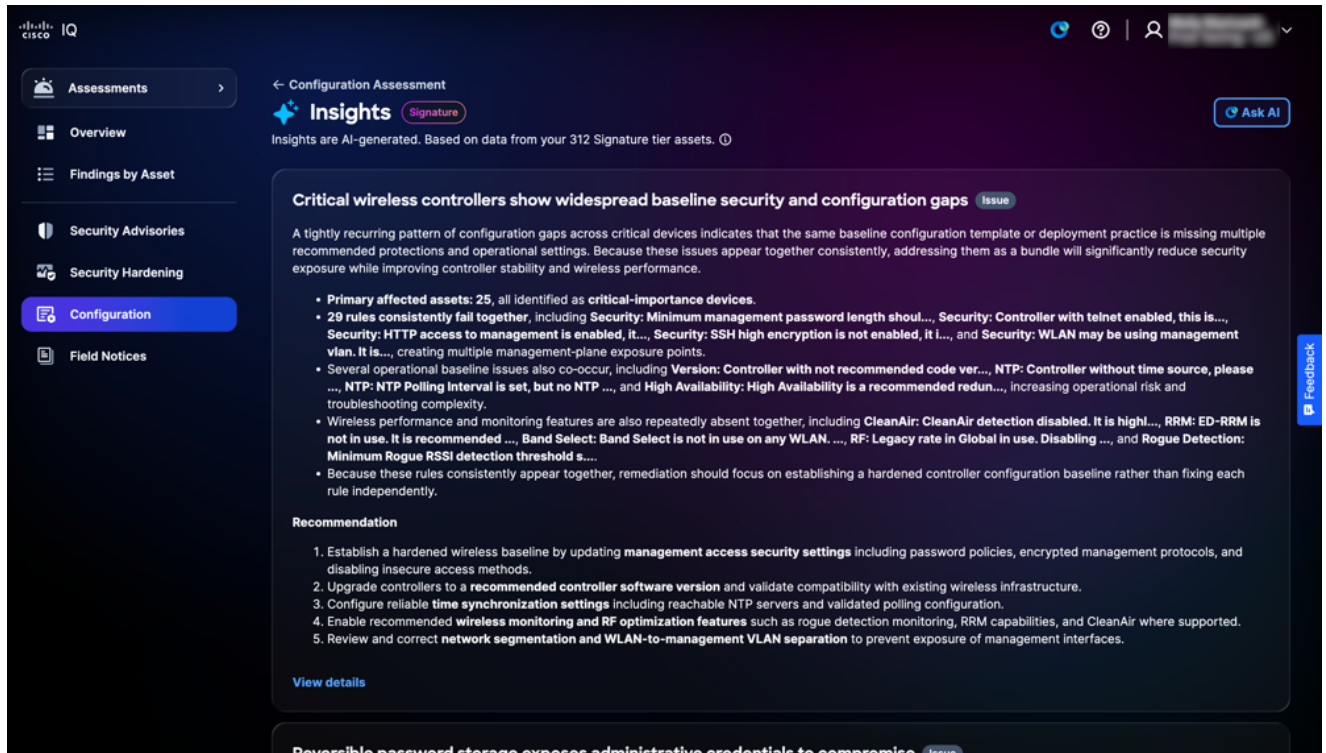
Les informations sont générées par l'intelligence artificielle et servent de tableau de bord intelligent qui synthétise les données d'évaluation en cartes clés hiérarchisées, mettant en évidence les disparités de configuration critiques entre plusieurs résultats. Il vous permet de traiter efficacement les risques d'infrastructure les plus importants en vous concentrant sur ces domaines urgents. Il met également en évidence les points forts en identifiant les domaines dans lesquels votre infrastructure est performante, conformément aux meilleures pratiques.



Idées

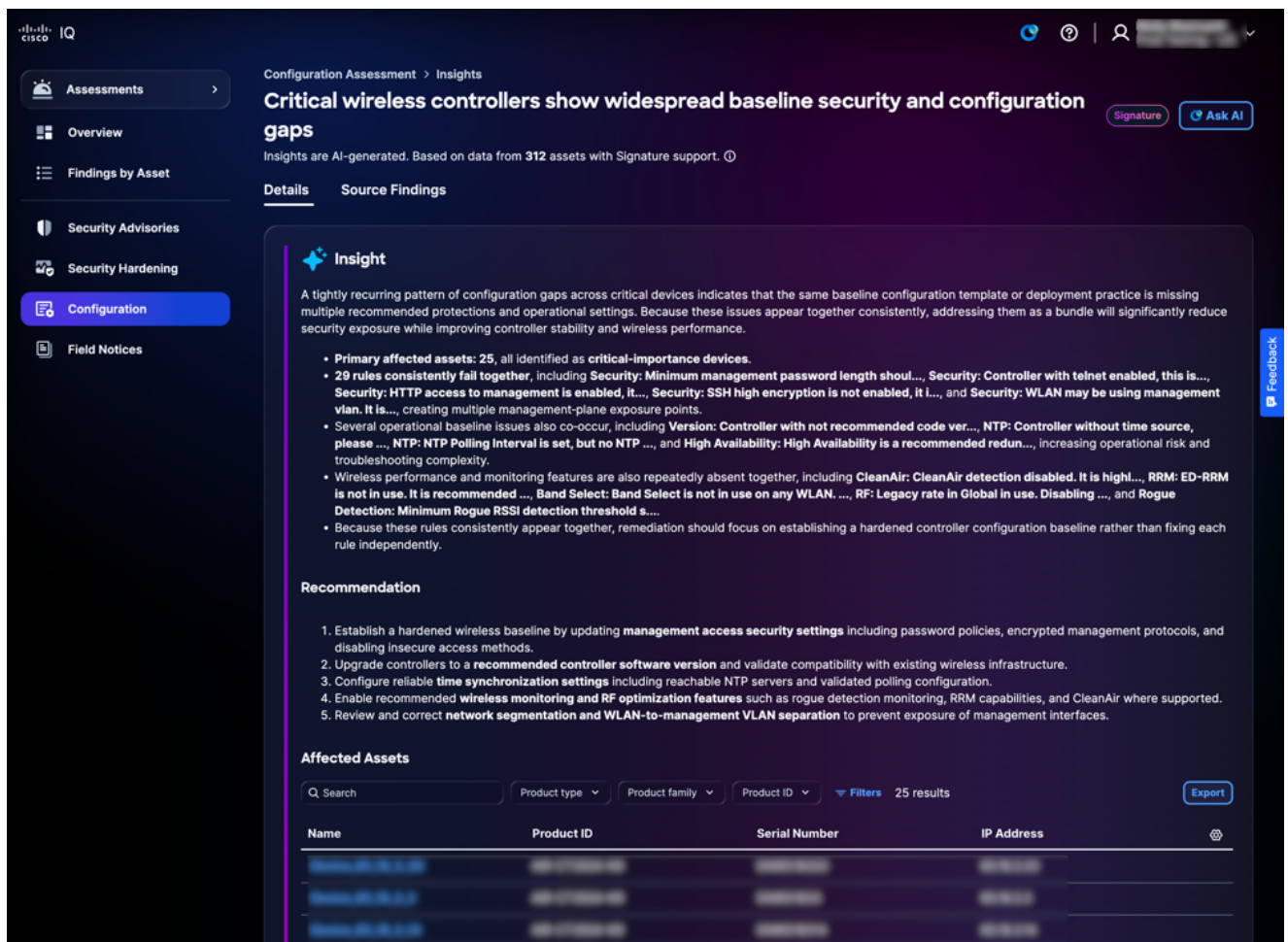
Pour afficher les détails Insights :

1. Dans le panneau Insights, cliquez sur View all. La page Insights affiche toutes les informations.



Page Insights

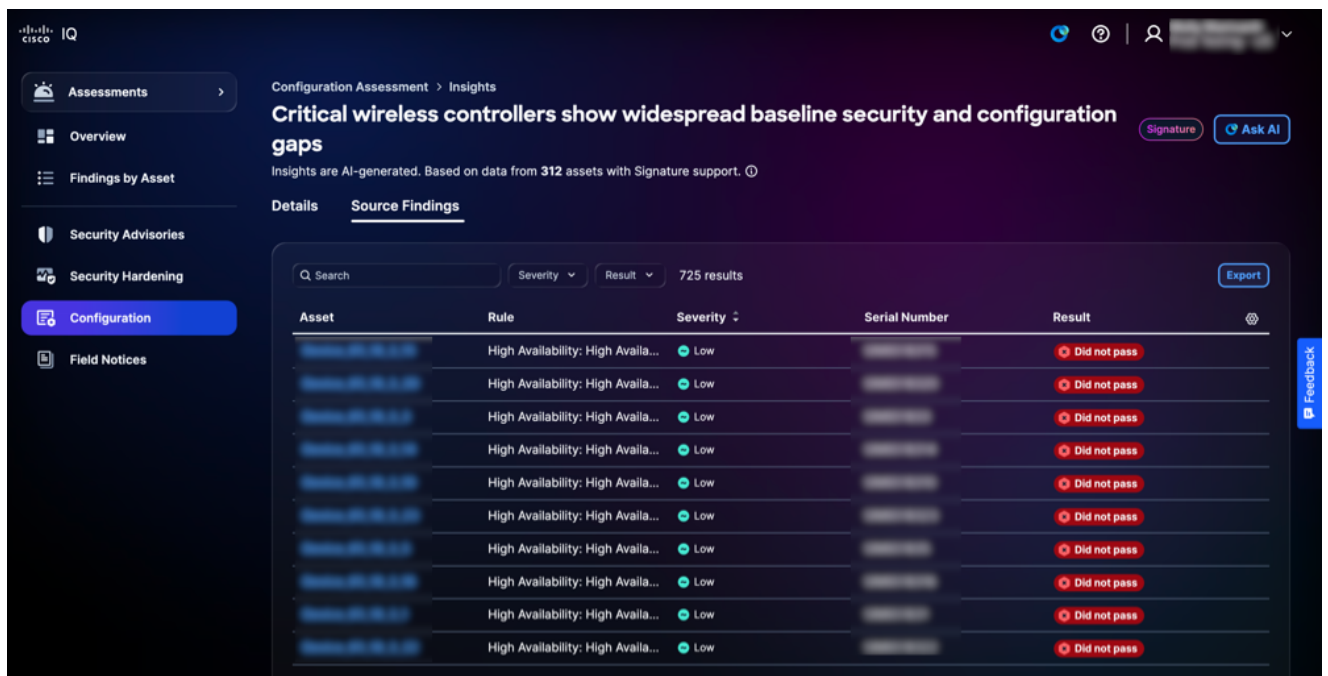
2. Cliquez sur Afficher les détails ou cliquez sur une carte. La page de détails Insights s'affiche avec les informations suivantes :



Détail Insights

- **Insight** : Fournit un résumé qui met en évidence les modèles récurrents d'écarts de configuration identifiés par le biais d'une analyse complète de plusieurs résultats, ainsi que les domaines d'excellence de votre infrastructure dans lesquels les configurations sont conformes aux meilleures pratiques.
- **Recommandation** : Fournit des étapes exploitables pour remédier aux failles de configuration identifiées
- **Ressources affectées** : Fournit une liste de périphériques spécifiques où l'écart de configuration a été identifié comme défini dans la section Insight

3. Cliquez sur Source Findings. La page Résultats de la recherche source affiche les résultats individuels détaillés qui étayent vos informations.



The screenshot displays the Cisco IQ Configuration Assessment Insights page. The main heading is "Critical wireless controllers show widespread baseline security and configuration gaps". Below this, it states "Insights are AI-generated. Based on data from 312 assets with Signature support." The page is divided into two tabs: "Details" and "Source Findings". The "Source Findings" tab is active, showing a table of results. The table has five columns: "Asset", "Rule", "Severity", "Serial Number", and "Result". There are 725 results in total, all with a severity of "Low" and a result of "Did not pass".

Asset	Rule	Severity	Serial Number	Result
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass

Résultats source

Vous pouvez filtrer la vue de tableau en choisissant un filtre dans les listes déroulantes Severity et Result.

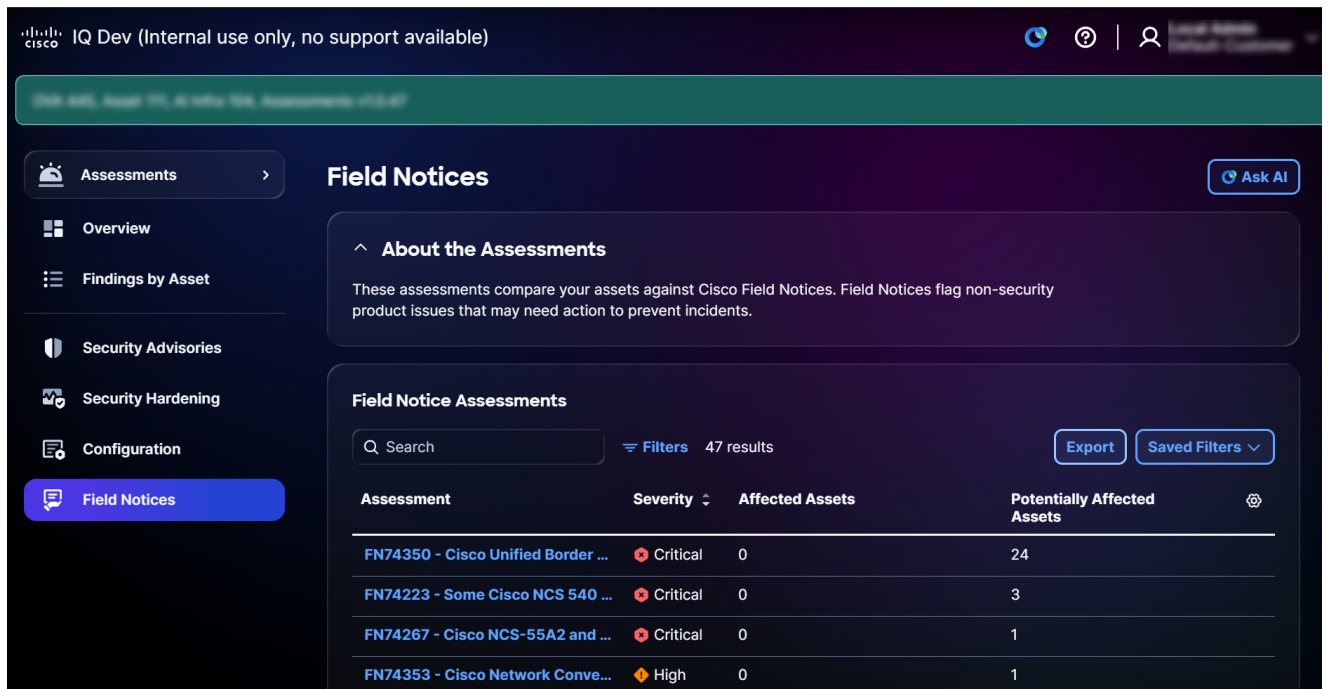


Remarque : Les recommandations et les ressources concernées sont facultatives en fonction des résultats de chaque analyse.

Notes de terrain

Les avis sur site identifient les problèmes importants liés aux produits non liés à la sécurité et les organisent en fonction de leur gravité et de leur criticité, améliorant ainsi la capacité de l'entreprise à gérer les risques liés aux produits. Les notices de terrain fournissent des informations exploitables sur les défauts des produits, accélèrent la réduction des risques

grâce aux mises à niveau recommandées ou aux solutions de contournement, et garantissent l'alignement avec les objectifs opérationnels et commerciaux. Cela renforce la fiabilité des produits, optimise l'allocation des ressources et favorise la résilience face à l'évolution des défis liés aux produits dans toute l'entreprise.



The screenshot shows the Cisco IQ Dev interface. The top bar indicates 'Internal use only, no support available'. The sidebar on the left contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, and Configuration. The 'Field Notices' section is active, showing an 'Ask AI' button. Below this is an 'About the Assessments' section explaining that assessments compare assets against Cisco Field Notices. The main part of the interface is a table titled 'Field Notice Assessments' with a search bar and a filter button. The table has four columns: Assessment, Severity, Affected Assets, and Potentially Affected Assets. It displays four rows of data:

Assessment	Severity	Affected Assets	Potentially Affected Assets
FN74350 - Cisco Unified Border ...	Critical	0	24
FN74223 - Some Cisco NCS 540 ...	Critical	0	3
FN74267 - Cisco NCS-55A2 and ...	Critical	0	1
FN74353 - Cisco Network Conve...	High	0	1

Notes de terrain

Rechercher et filtrer des vues pour des avis de champ

Vous pouvez filtrer l'affichage de la liste en sélectionnant un filtre dans les listes déroulantes. Vous pouvez également rechercher des évaluations d'avis de champ en saisissant le nom de l'évaluation dans le champ Rechercher.

Afficher les évaluations pour les notices de champ

Pour afficher des détails supplémentaires sur une note de champ, cliquez sur une évaluation. Les détails d'évaluation suivants s'affichent :

- À propos des évaluations : Fournit des détails supplémentaires en résumant l'objectif de l'évaluation
- Évaluations des avis de terrain : Affiche la liste des ressources affectées par la notification de champ sélectionnée, y compris les ressources présentant des vulnérabilités détectées

Field Notices

FN74223 - Some Cisco NCS 540 Series Medium Density Routers May Become Unresponsive After Upgrade to Cisco IOS XR Software Release 7.11.1 or Later - Workaround Provided

About the assessment

Some medium density Cisco Network Convergence System (NCS) 540 Series Routers may not boot when subjected to a field programmable device (FPD) upgrade during installation of Cisco IOS XR Software Release 7.11.1 or later.

Severity: **Critical** | Last updated: **Dec 11, 2024** | Bugs: [Redacted]

References: [Field Notice](#)

Asset Results

Search: [Input] | Filters: 3 results | Export | Saved Filters

Asset	Result	Product ID	Serial Number	Product Type	Product Family	Sup po...
Device_70_1...	Potentially affected	[Redacted]	[Redacted]	Routers	Cisco Network...	Signature
Device_70_1...	Potentially affected	[Redacted]	[Redacted]	Routers	Cisco Network...	Signature
Device_70_1...	Potentially affected	[Redacted]	[Redacted]	Routers	Cisco Network...	Signature

Afficher les évaluations pour les notices de champ

Rechercher et filtrer des vues pour les résultats d'immobilisations pour les avis de champ

Vous pouvez filtrer l'affichage de liste en choisissant un filtre dans les listes déroulantes ou en cliquant sur Filtres et en choisissant une option dans la liste des filtres disponibles. Vous pouvez également rechercher des résultats d'actifs en saisissant le nom de l'actif dans le champ Rechercher.



Remarque : Certains filtres peuvent être masqués en fonction des paramètres de zoom de l'écran. Différents filtres sont disponibles en fonction de vos rôles et autorisations.

Exporter les résultats d'immobilisations pour les notifications de champ

Pour exporter les résultats des ressources d'évaluation pour les notices de champ, cliquez sur Exporter. Consultez [Exportation d'informations](#) pour plus d'informations.

Voir les résultats d'évaluation des équipements pour les notices de champ

Pour afficher les détails des résultats de l'évaluation d'une ressource, cliquez sur une ressource dans Résultats de l'évaluation des ressources. La page Détails des résultats de l'évaluation de l'actif s'affiche.

Vous pouvez afficher les types de résultats suivants :

- Affecté : Indique les ressources qui répondent à tous les critères automatiquement vérifiés pour un avis sur site et qui ne nécessitent aucune vérification manuelle supplémentaire pour confirmer qu'elles sont affectées
- Potentiellement affecté : Indique les ressources qui répondent à tous les critères vérifiés automatiquement pour un avis sur site, mais qui nécessitent une vérification manuelle supplémentaire pour confirmer si elles sont réellement affectées

Les invites suivantes sont disponibles sous l'onglet Évaluations - Renforcement de la sécurité :

- Quelles sont les meilleures pratiques de renforcement de la sécurité Cisco pour les périphériques réseau ?
- Comment renforcer mes périphériques Cisco IOS XE ?
- Énumérez les principales étapes de renforcement de la sécurité pour les routeurs et les commutateurs.
- Quels sont les paramètres de durcissement de base recommandés pour les périphériques Cisco ?
- Combien de ressources enseignent les meilleures pratiques de renforcement de la sécurité ?

Authentification locale

Les administrateurs de compte doivent utiliser les informations d'identification suivantes pour se connecter à VA :

- Nom d'utilisateur par défaut : admin
- Mot de passe par défaut : mot de passe défini lors du processus d'installation de VA ; reportez-vous au Guide de démarrage pour plus d'informations
- Contexte du compte par défaut : Client par défaut

Lors de la connexion, l'utilisateur par défaut, « admin », et le nom de compte, « Default-Customer » s'affichent sur la page d'accueil.

Configuration de la sécurité administrateur local

Vous pouvez modifier votre mot de passe et définir des questions de sécurité via le menu Profil utilisateur de la page d'accueil.

Paramètres de verrouillage

Les paramètres de verrouillage de compte suivants peuvent être configurés pendant le

déploiement :

- Lockout Status : active ou désactive la fonctionnalité de verrouillage du compte.
- Maximum Login Attempts : définit le nombre maximal de tentatives infructueuses consécutives autorisées avant le verrouillage d'un compte (valeur par défaut : 3; Plage: 0–10).
- Rolling Time Window : définit la période de temps pour le suivi des tentatives infructueuses (par défaut : 15 minutes ; Plage: 0-60 minutes).
- Duration : définit la durée pendant laquelle un compte reste verrouillé une fois le nombre maximal de tentatives atteint (valeur par défaut : 30 minutes ; Plage: 0-60 minutes).



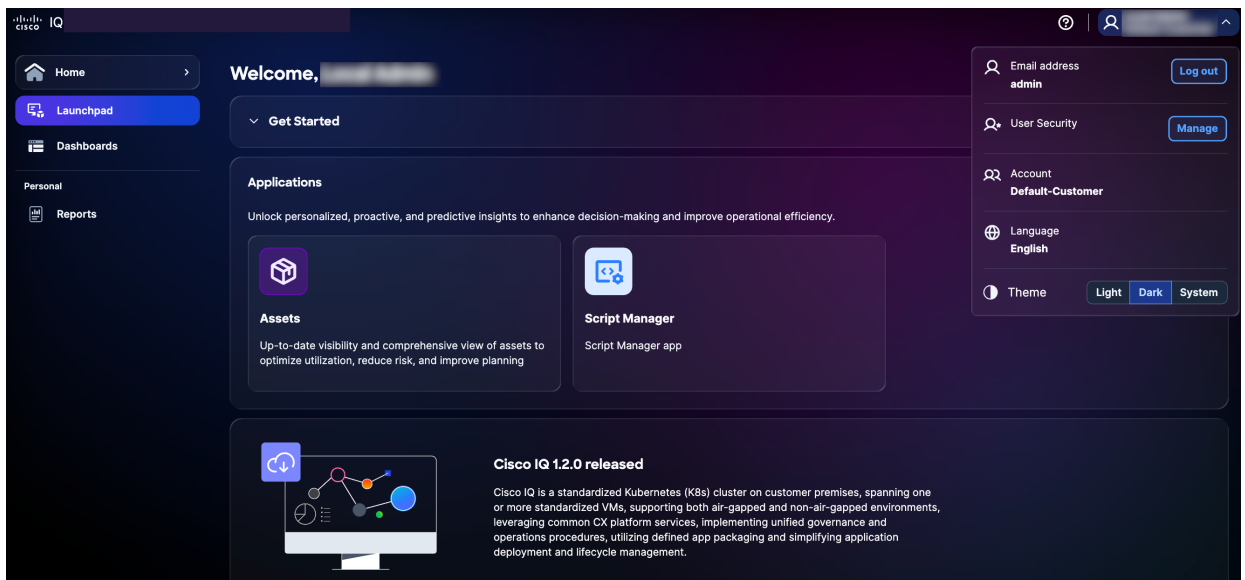
Remarque : Vous avez trois (3) tentatives de saisie du mot de passe correct dans un délai de 15 minutes. Si les trois (3) tentatives échouent, votre compte se verrouille temporairement pendant 30 minutes pour protéger votre sécurité. Vous ne pouvez pas tenter de vous connecter pendant la période de verrouillage. Le système affiche le message suivant : «Compte verrouillé en raison d'un trop grand nombre de tentatives ayant échoué. Veuillez réessayer ultérieurement. », y compris la date d'expiration du verrouillage. Votre compte se déverrouille automatiquement au bout de 30 minutes. Vous pouvez alors tenter de vous connecter ou de réinitialiser votre mot de passe.

Configuration des questions de sécurité et des réponses

Les questions de sécurité vous aident à vérifier votre identité si vous oubliez votre mot de passe. Les administrateurs de compte doivent configurer les réponses à cinq (5) questions de sécurité pour activer la fonction de réinitialisation du mot de passe. Il s'agit d'une configuration unique.

Pour configurer les questions de sécurité :

1. Sur la page d'accueil, cliquez sur l'icône Profil utilisateur. Le menu déroulant s'ouvre.



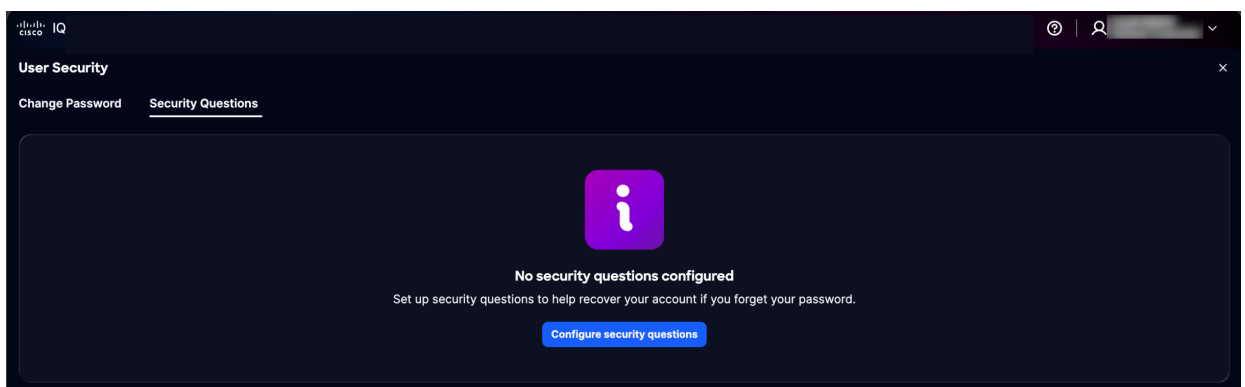
Utiliser la sécurité

2. Cliquez sur Gérer dans Sécurité utilisateur. La page Sécurité utilisateur s'affiche.



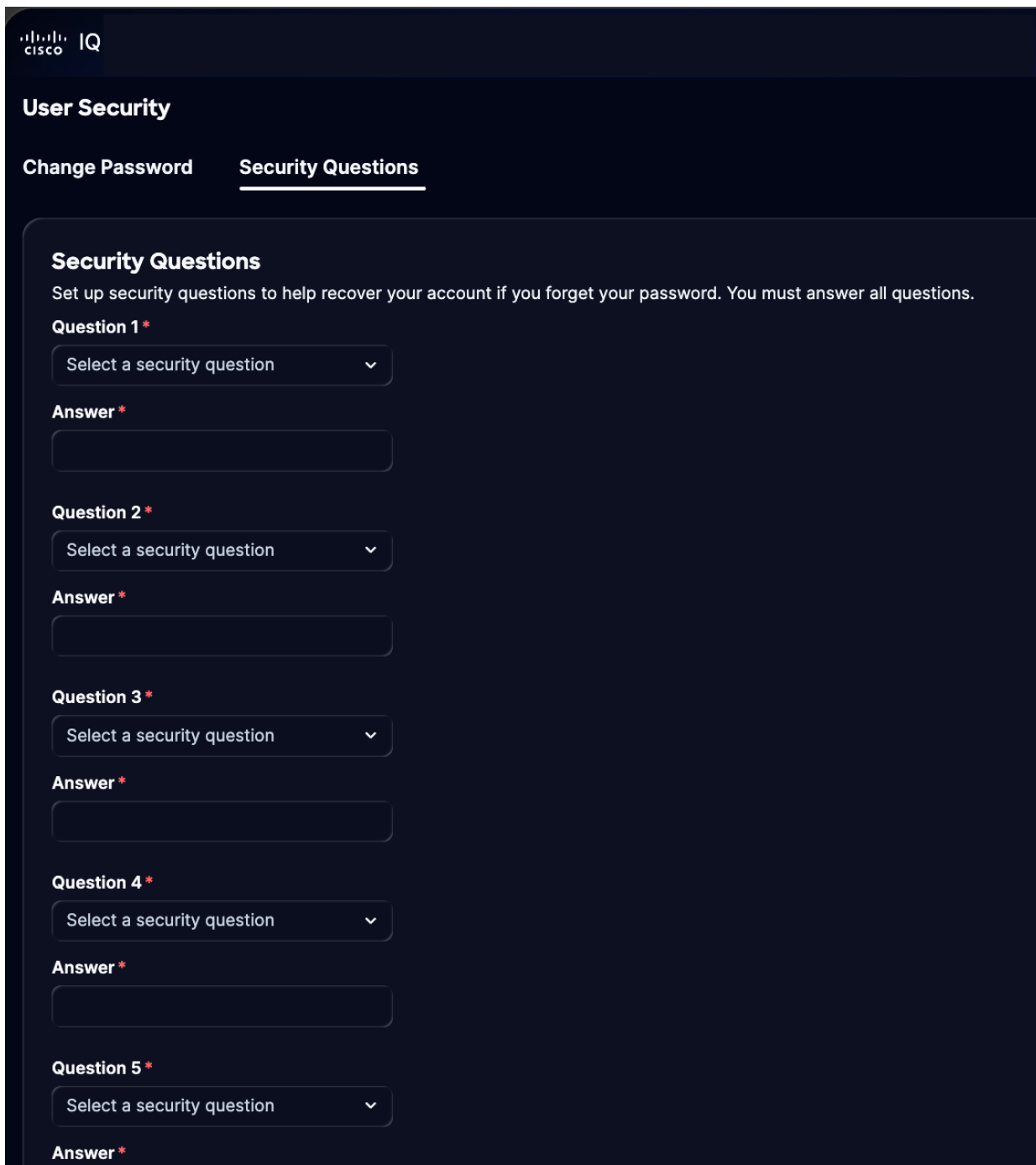
Questions de sécurité

3. Cliquez sur Security Questions pour ouvrir l'onglet.



Onglet Questions de sécurité

4. Cliquez sur Configurer les questions de sécurité.



The screenshot shows the Cisco IQ User Security page. The 'Security Questions' tab is selected. The page title is 'Security Questions'. Below the title, there is a instruction: 'Set up security questions to help recover your account if you forget your password. You must answer all questions.' There are five questions, each with a dropdown menu to select a security question and a text input field for the answer. The questions are labeled 'Question 1 *', 'Question 2 *', 'Question 3 *', 'Question 4 *', and 'Question 5 *'. The dropdown menus are labeled 'Select a security question' and the answer fields are labeled 'Answer *'.

Configurer les questions de sécurité

5. Choisissez l'une des cinq (5) questions de sécurité dans les listes déroulantes.
6. Saisissez votre réponse pour chaque question.
7. Cliquez sur Save.



Remarque : Les réponses ne sont pas sensibles à la casse. Par exemple, « SMITH » et « smith » sont considérés comme identiques. Les espaces supplémentaires sont ignorés, ce qui signifie que « Smith » et « Smith »

 sont traités de la même manière. N'oubliez pas la façon dont vous avez entré votre réponse (par exemple, noms complets ou surnoms). Utilisez des réponses simples dont vous vous souviendrez des années plus tard. Choisissez des questions avec des réponses qui ne changeront pas au fil du temps.

 Remarque : Vous pouvez mettre à jour vos réponses ultérieurement si nécessaire. Lorsque vous mettez à jour vos réponses, toutes les réponses précédentes sont remplacées. Vous devez donc fournir à nouveau les réponses aux cinq (5) questions et pas seulement celles que vous souhaitez modifier.

Gestion des mots de passe

Les administrateurs de compte et les utilisateurs locaux peuvent gérer le mot de passe de Cisco IQ.

Pour garantir la sécurité de votre compte, les stratégies de mot de passe suivantes sont appliquées :

- Restriction de réutilisation : votre nouveau mot de passe ne correspond à aucun de vos cinq (5) mots de passe précédents. Cette stratégie s'applique aux flux Inscription, Mot de passe oublié et Modifier le mot de passe.
- Variation de caractères : lorsque vous modifiez votre mot de passe lors de l'authentification, au moins huit (8) caractères de votre mot de passe actuel doivent être différents dans votre nouveau mot de passe.
- Intervalle de modification minimum : par défaut, vous devez attendre 24 heures avant de modifier à nouveau votre mot de passe. Si un intervalle différent est configuré, vous ne pourrez pas mettre à jour votre mot de passe tant que ce délai ne sera pas écoulé.
- Expiration du mot de passe : Les mots de passe expirent tous les 60 jours. Lors de votre première connexion suivant la date d'expiration, vous devrez définir un nouveau mot de passe avant de pouvoir accéder au système (si la valeur 0 est configurée, l'expiration du mot de passe est désactivée).

Conditions préalables

Pour gérer les mots de passe, les conditions suivantes doivent être remplies :

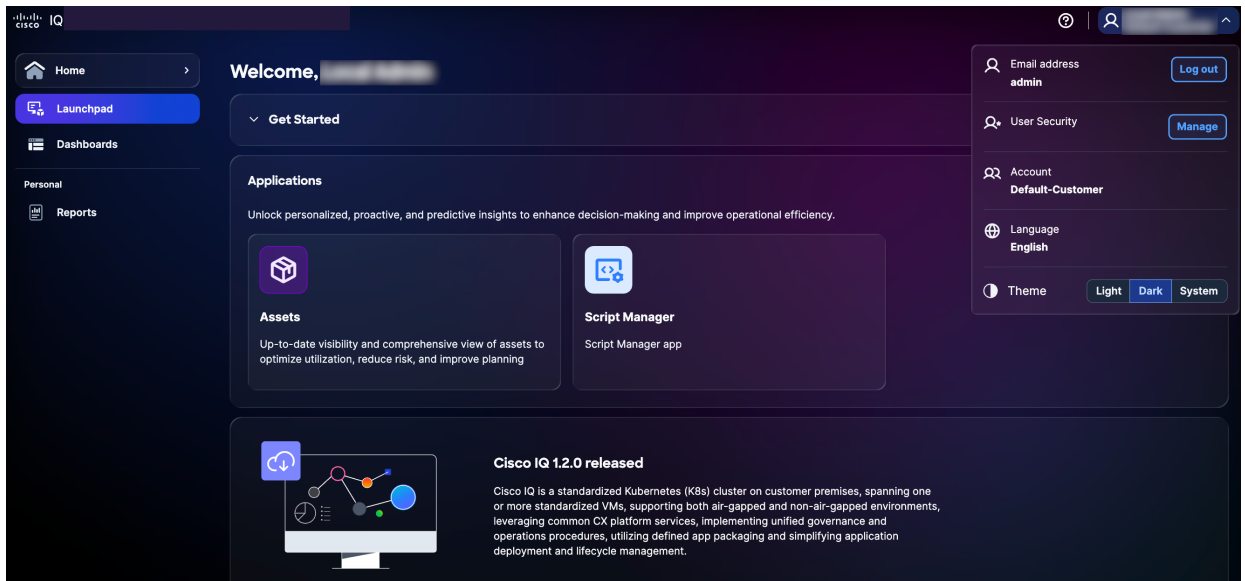
- Vous êtes un administrateur de compte ou un utilisateur local
- Vous utilisez un compte local (et non une authentification unique (SSO) ou externe)

- Vous êtes connecté à Cisco IQ
- Vous connaissez le mot de passe actuel

Modification des mots de passe

Pour modifier le mot de passe :

1. Sur la page d'accueil, cliquez sur l'icône Profil utilisateur. Le menu déroulant s'ouvre.



Gérer la sécurité utilisateur

2. Cliquez sur Gérer dans Sécurité utilisateur. La page Sécurité utilisateur s'affiche.



Modifier le mot de passe

3. Saisissez le mot de passe actuel.
4. Saisissez le nouveau mot de passe.

5. Saisissez à nouveau le nouveau mot de passe pour le confirmer.

6. Cliquez sur Save.

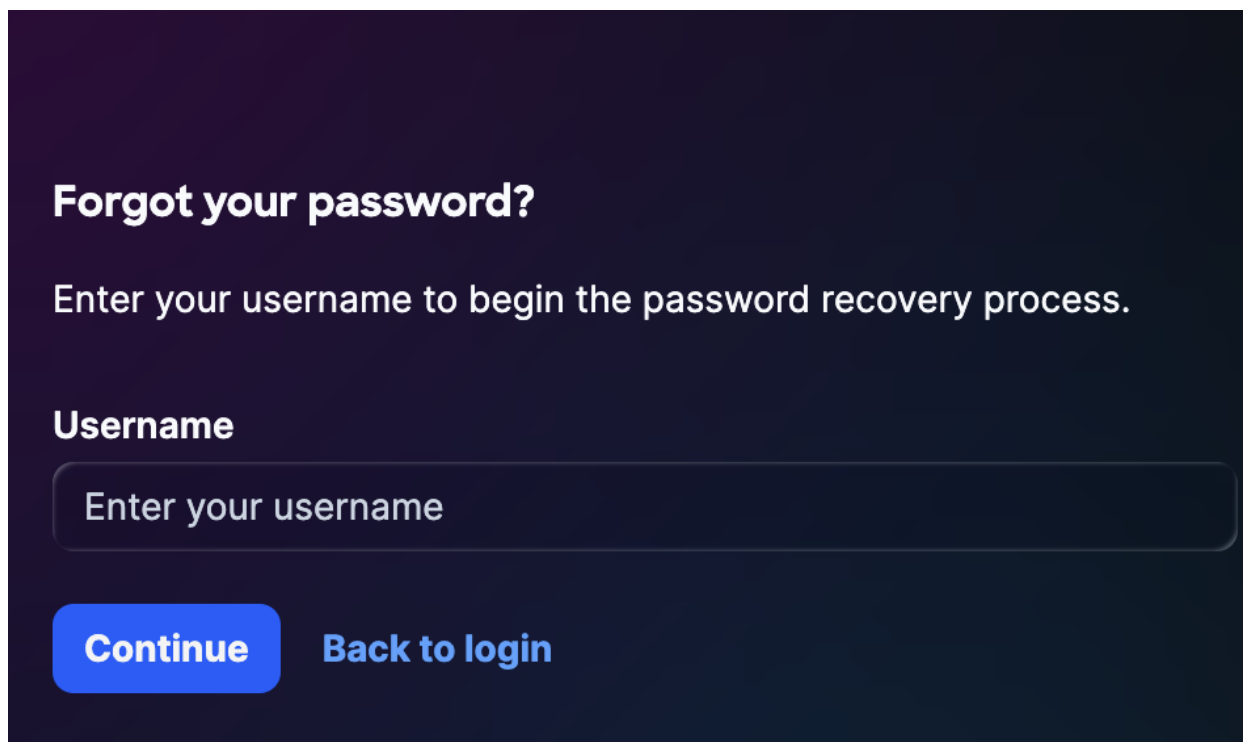
Le mot de passe est mis à jour dans le système Cisco IQ, y compris la machine virtuelle Cisco IQ.

Réinitialisation d'un mot de passe oublié

Vous pouvez réinitialiser un mot de passe en utilisant le processus de vérification des questions de sécurité.

Pour réinitialiser un mot de passe oublié :

1. Accédez à la page de connexion Cisco IQ VA.
2. Cliquez sur Mot de passe oublié.



Forgot your password?

Enter your username to begin the password recovery process.

Username

Continue **Back to login**

Mot de passe oublié

3. Saisissez le nom d'utilisateur.
4. Cliquez sur Continuer. La page Vérifier l'identité affiche trois (3) questions de sécurité aléatoires sur les cinq (5) questions précédemment configurées.

Verify Identity

Answer the following security questions to verify your identity.

What city were you born in?

[Show](#)

What is your mother's maiden name?

[Show](#)

What was the name of your elementary school?

[Show](#)[Verify and continue](#)[Back to login](#)

Vérifier l'identité

5. Saisissez les réponses aux trois (3) questions affichées.
6. Cliquez sur Vérifier et continuez. Si la réponse envoyée correspond à vos réponses précédemment enregistrées, vous êtes invité à saisir un nouveau mot de passe.

Set New Password

Choose a strong password that contains the following:

- At least 15 characters
- At least 2 uppercase characters
- At least 2 lowercase characters
- At least 2 numeric characters
- At least 2 special characters
- No repeating characters

New password

Show

Confirm password

Show

Reset password

Back to login

Réinitialiser le mot de passe

 Remarque : Vous avez trois (3) tentatives de saisie du mot de passe correct dans un délai de 15 minutes. Si les trois (3) tentatives échouent, votre compte se verrouille temporairement pendant 30 minutes pour protéger votre sécurité. Vous ne pouvez pas tenter de vous connecter pendant la période de verrouillage. Le système affiche le message suivant : «Compte verrouillé en raison d'un trop grand nombre de tentatives ayant échoué. Veuillez réessayer ultérieurement. », y compris la date d'expiration du verrouillage. Votre compte se déverrouille automatiquement au bout de 30 minutes. Vous pouvez alors tenter de vous connecter ou de réinitialiser votre mot de passe.

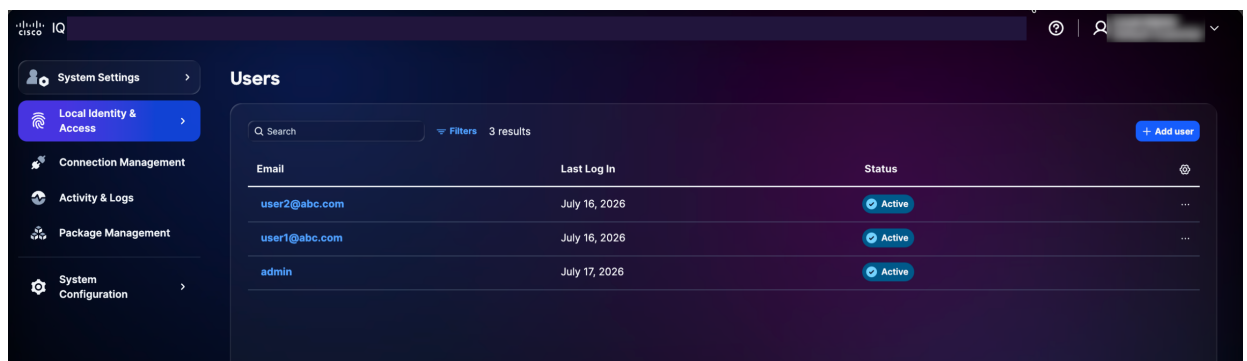
- Saisissez le nouveau mot de passe.
- Entrez à nouveau le mot de passe pour le confirmer.
- Cliquez sur Submit.

Ajout d'utilisateurs locaux

Les administrateurs de compte peuvent ajouter des utilisateurs au compte Cisco IQ.

Pour ajouter un nouvel utilisateur :

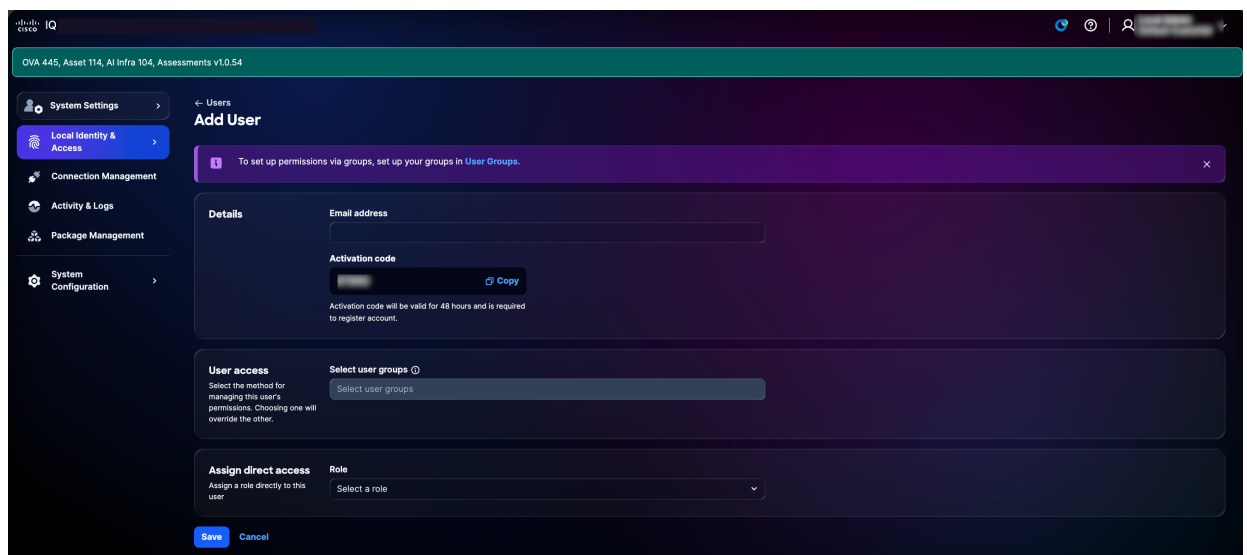
1. Accédez à Paramètres système > Identité et accès locaux > > Utilisateurs. La page Utilisateurs s'affiche. Elle répertorie tous les utilisateurs locaux existants, ainsi que leur état.



Page Utilisateurs

 Remarque : Ne partagez pas le code d'activation sur des canaux non sécurisés. Si le code est perdu ou compromis, utilisez l'icône Menu pour régénérer un nouveau code d'activation, ce qui invalide le précédent. Les codes d'activation sont valides pendant 48 heures. Si votre code expire, veuillez contacter votre administrateur de compte pour en demander un nouveau.

- Cliquez sur Ajouter des utilisateurs. La page Ajouter un utilisateur s'affiche.



Ajouter un utilisateur

3. Saisissez l'adresse e-mail.
4. Saisissez le code d'activation.

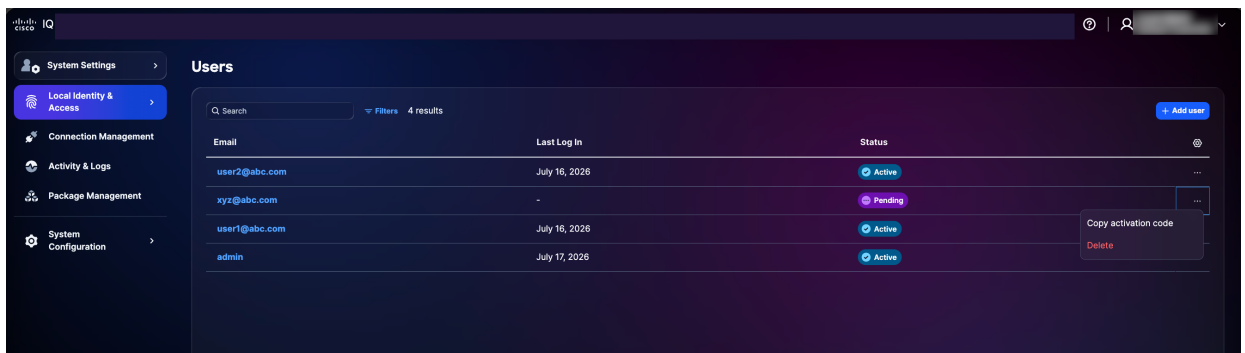
 Remarque : Le code d'activation est affiché par défaut. Partagez le code

 d'activation affiché avec l'utilisateur, tel qu'il est requis pour l'inscription.

5. Dans Accès utilisateur, sélectionnez le groupe d'utilisateurs dans la liste déroulante Sélectionner les groupes d'utilisateurs.

 Remarque : Les utilisateurs héritent de l'accès du groupe sélectionné.

6. Dans Affecter un accès direct, sélectionnez un rôle dans la liste déroulante Rôle. Deux (2) rôles sont disponibles :
 - Visionneuse : Afficher et accéder aux applications
 - Administrateur de compte : Accédez aux modules et gérez les paramètres système, sauf System Management et Identity Provider (IDP)
7. Cliquez sur Save. Le nouvel utilisateur est créé et s'affiche dans la liste des utilisateurs à l'état En attente. En attente indique que l'utilisateur n'a pas encore terminé l'auto-activation.
8. Localisez le nouvel utilisateur dans la liste et vérifiez que la colonne Status (État) affiche Pending (En attente).
9. Cliquez sur l'icône Plus d'options en regard du nouvel utilisateur.



Copier le code d'activation

10. Sélectionnez Copier le code d'activation dans la liste déroulante. Le code d'activation est copié dans le Presse-papiers.
11. Partagez ce code avec l'utilisateur en toute sécurité (par exemple, via un canal interne sécurisé). Le code d'activation est destiné à une utilisation unique et est requis pour terminer l'inscription.

 Remarque : Ne partagez pas le code d'activation sur des canaux non sécurisés. Si le code est perdu ou compromis, utilisez l'icône Menu pour régénérer un nouveau code d'activation, ce qui invalide le précédent. Les codes d'activation sont valides pendant 48 heures. Si votre code expire, veuillez contacter votre

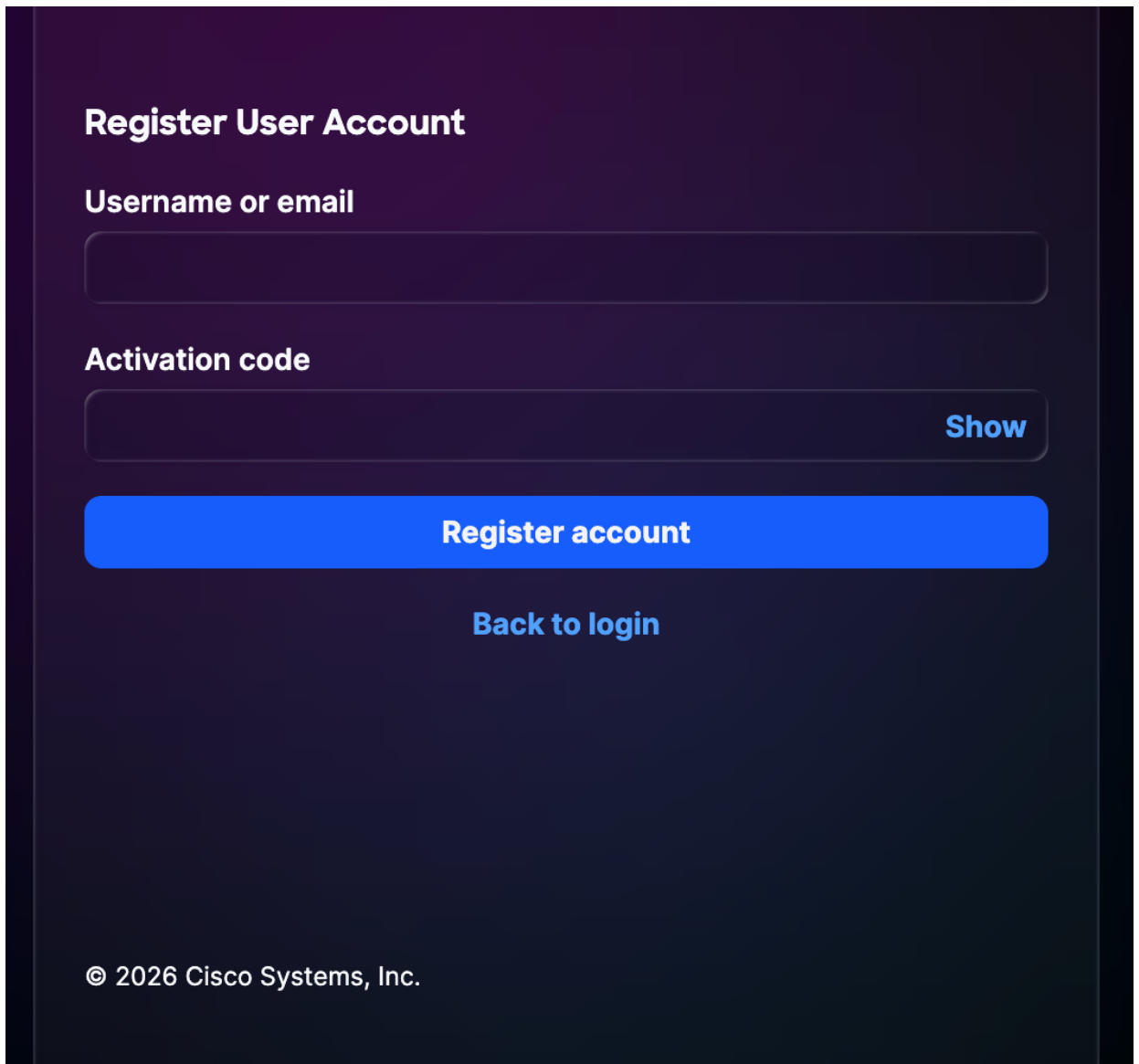
 administrateur de compte pour en demander un nouveau.

12. Pour vous déconnecter, cliquez sur l'icône Profil utilisateur dans l'angle supérieur droit et sélectionnez Déconnexion. Vous revenez à la page de connexion de Cisco IQ.

Inscription de nouveaux comptes utilisateur

Pour enregistrer le nouveau compte d'utilisateur :

1. Sur la page de connexion, cliquez sur le lien Register a new user account.



Register User Account

Username or email

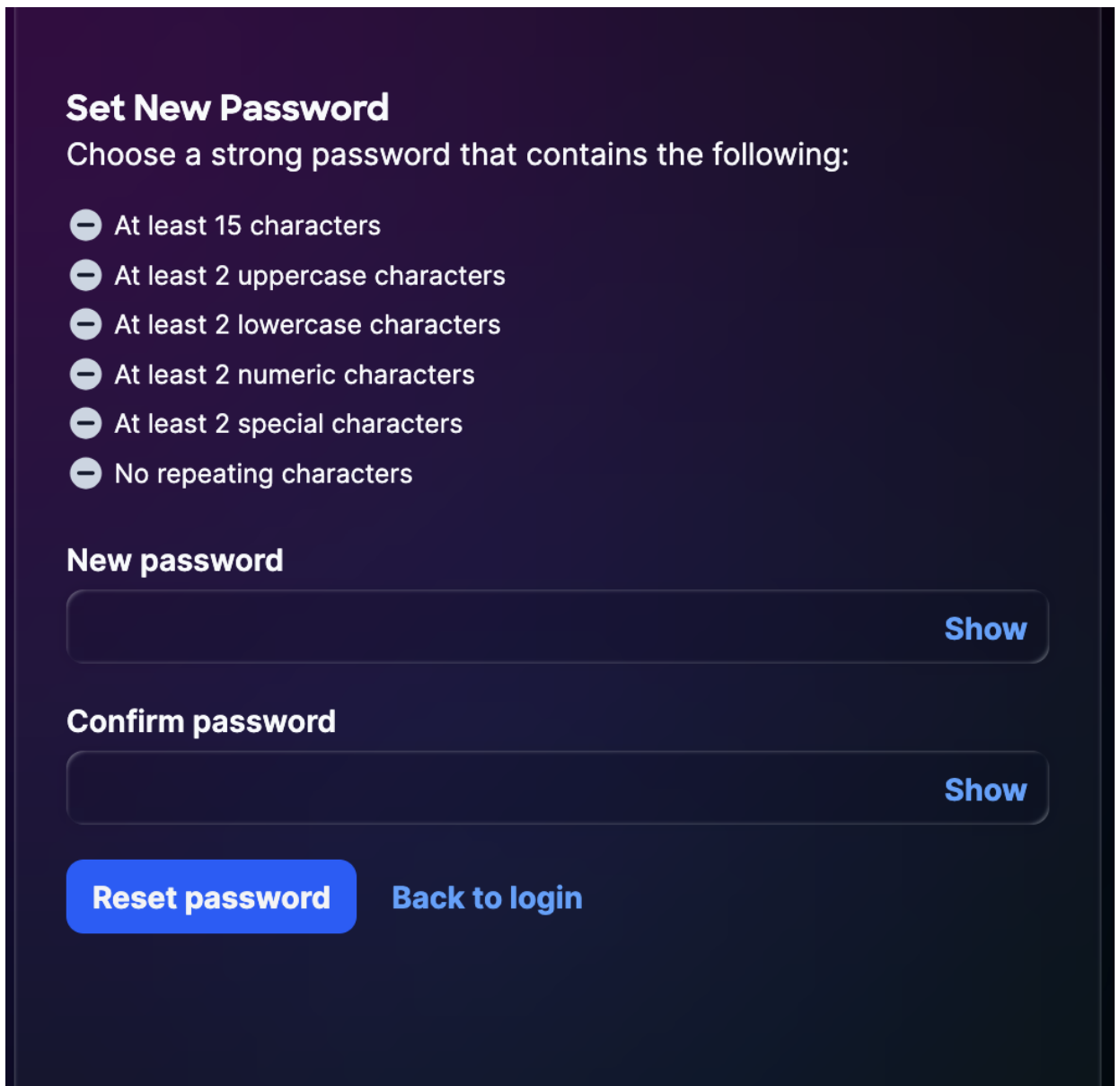
Activation code

 Show

Nouveau compte d'utilisateur

2. Saisissez le nom d'utilisateur ou l'adresse e-mail utilisés lors de la création de l'utilisateur (par exemple, user1@abc.com)
3. Saisissez le code d'activation partagé par l'administrateur de compte.

4. Cliquez sur Register account. La fenêtre Définir un nouveau mot de passe s'affiche.



Set New Password

Choose a strong password that contains the following:

- At least 15 characters
- At least 2 uppercase characters
- At least 2 lowercase characters
- At least 2 numeric characters
- At least 2 special characters
- No repeating characters

New password

Confirm password

Reset password **Back to login**

Nouveau mot de passe de compte utilisateur

5. Saisissez un nouveau mot de passe.
6. Entrez à nouveau le mot de passe dans Confirmer le mot de passe.
7. Lors de la première connexion réussie, l'utilisateur est invité à configurer cinq (5) questions de sécurité. (Voir [Configuration des questions de sécurité](#)).

Gestion des groupes d'utilisateurs locaux

Les groupes d'utilisateurs permettent à l'administrateur de comptes de gérer les rôles de plusieurs utilisateurs locaux à la fois. Au lieu d'attribuer un rôle à chaque utilisateur individuellement, vous pouvez créer un groupe, lui associer un rôle et un ensemble d'utilisateurs et mettre à jour le rôle ou l'appartenance à un seul emplacement. La

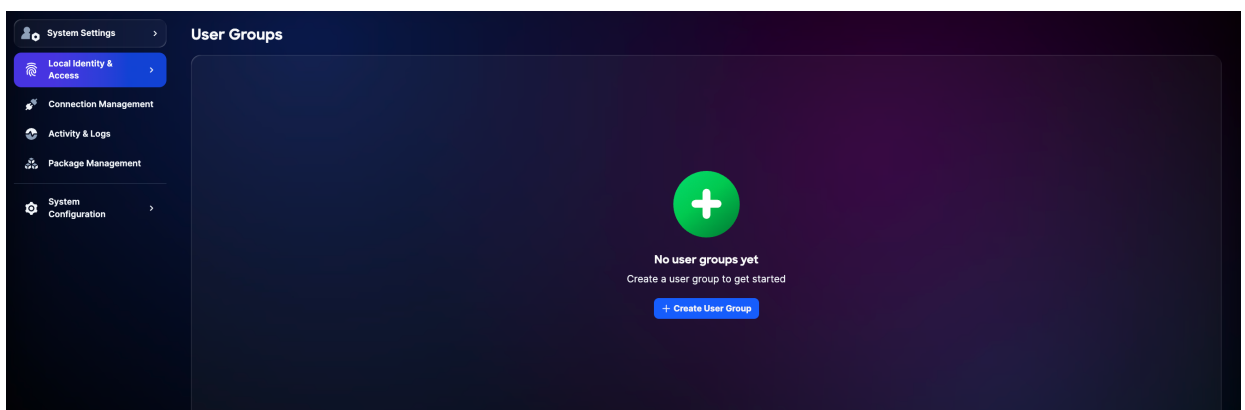
gestion de tous les groupes d'utilisateurs est effectuée à partir de la page Identité locale et accès.

 Remarque : Seul un administrateur de compte peut créer, modifier ou supprimer des groupes d'utilisateurs. Les groupes sont composés d'utilisateurs locaux existants ; les utilisateurs doivent être créés avant de pouvoir être ajoutés à un groupe. Référez-vous à [Ajout d'utilisateurs locaux](#) pour plus d'informations.

Création d'un groupe d'utilisateurs

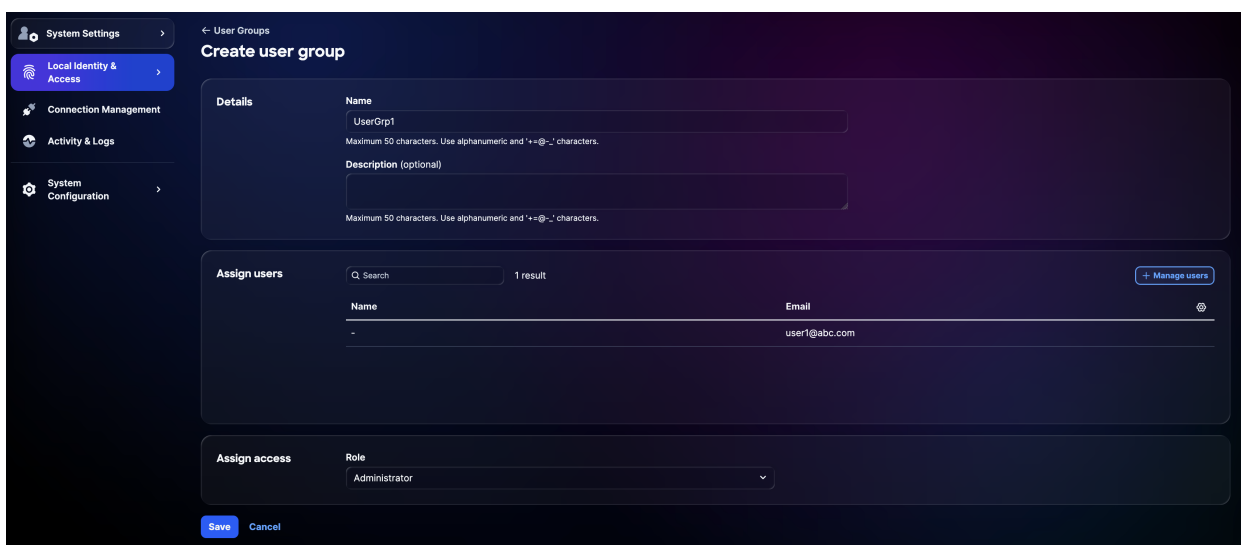
Pour créer un groupe d'utilisateurs :

1. Dans Paramètres système, choisissez Identité et accès locaux > Groupes d'utilisateurs. La page Groupes d'utilisateurs s'affiche.



Groupes d'utilisateurs

2. Cliquez sur Créer un groupe d'utilisateurs. La page Créer un groupe d'utilisateurs s'affiche.



Créer un groupe d'utilisateurs

3. Renseignez les sections suivantes :

- Détails
- Name : Entrez un nom unique pour le groupe (par exemple, Opérateurs en lecture seule)
- Description (Facultatif) : Une brève description du groupe (50 caractères maximum ; alphanumérique et + = @ - _ caractères autorisés)
- Affecter des utilisateurs : Recherchez et sélectionnez un ou plusieurs utilisateurs locaux existants à ajouter au groupe. Remarque : Pour ajouter des utilisateurs qui ne figurent pas encore dans la liste, cliquez sur Gérer les utilisateurs.
- Attribuer un accès
- Rôle : Sélectionnez le rôle système à attribuer à tous les membres de ce groupe. Les rôles suivants sont disponibles :
- Visionneuse : Modules d'affichage et d'accès (lecture seule)
- Administrateur : Accès aux modules et gestion des paramètres système

4. Cliquez sur Save.

Le nouveau groupe d'utilisateurs s'affiche dans la liste Groupes d'utilisateurs avec le rôle qui lui a été attribué et le nombre de membres.

Modification d'un groupe d'utilisateurs

Pour modifier un groupe d'utilisateurs :

1. Dans la liste Groupes d'utilisateurs, localisez le groupe que vous souhaitez modifier.
2. Cliquez sur l'icône Plus d'options > Modifier du groupe souhaité. La page Modifier un groupe d'utilisateurs s'affiche.

← User Groups

Edit user group

Details

Name
UserGrp1
Maximum 50 characters. Use alphanumeric and '+','=','_' characters.

Description (optional)

Maximum 50 characters. Use alphanumeric and '+','=','_' characters.

Assign users

Q Search 1 result + Manage users

Name	Email
—	user1@abc.com

Assign access

Role
Administrator

Save Cancel

Modifier le groupe d'utilisateurs

3. Effectuez les modifications souhaitées.

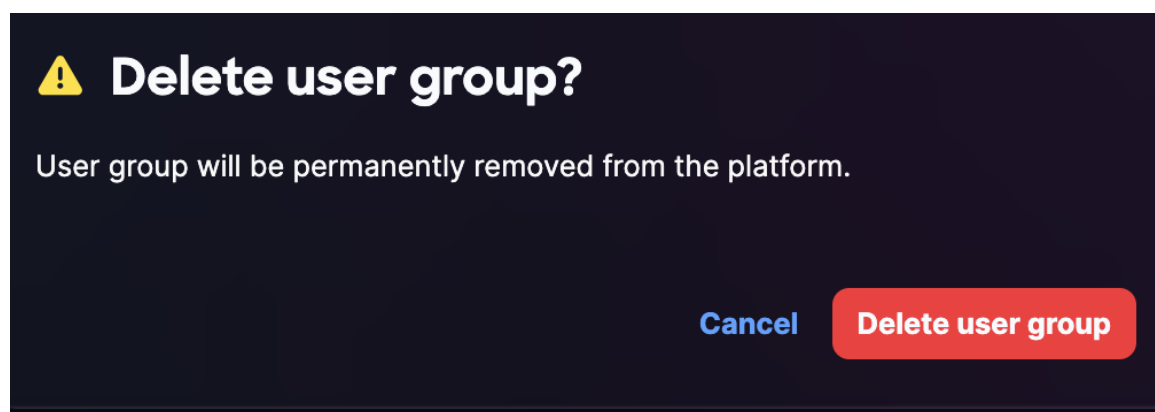
4. Cliquez sur Save.

Le groupe mis à jour s'affiche dans la liste Groupes d'utilisateurs. Le nouveau rôle prend effet pour tous les membres du groupe.

Suppression d'un groupe d'utilisateurs

Pour supprimer un groupe d'utilisateurs :

1. Dans la liste Groupes d'utilisateurs, localisez le groupe que vous souhaitez supprimer.
2. Cliquez sur l'icône Plus d'options en regard du groupe et sélectionnez Supprimer.



Supprimer le groupe d'utilisateurs

3. Confirmez la suppression lorsque vous y êtes invité.

Le groupe est supprimé de la liste Groupes d'utilisateurs.



Remarque : La suppression d'un groupe d'utilisateurs supprime l'affectation de rôle basée sur le groupe de tous les membres. Les comptes utilisateur individuels ne sont pas supprimés.

Configuration du fournisseur d'identité

Une fois connectés à VA, les administrateurs de compte peuvent configurer divers paramètres. Les administrateurs de compte peuvent se connecter en utilisant l'administration locale ou la configuration IDP.

Configuration SAML d'Okta IDP pour SSO

Conditions requises pour configurer IDP SAML

- Accès administrateur local à Cisco IQ
- Accès au portail IDP

Configuration SAML IDP pour SSO

Pour configurer le langage SAML (IDP Security Assertion Markup Language) pour SSO :

1. Accédez à votre portail IDP.

Tableau 2 : Attributs Cisco IQ

Champ	Valeur
Nom de l'application	<Nom de l'application>
Environnement	Application professionnelle ESP
Groupes de propriétaires d'applications	Propriétaire des paramètres IDP
Expéditeur d'équipe	Mailer pour l'équipe
Public	Non-employés
Catégorie d'intégration	Sélectionnez « Nouvelle intégration ».

Tableau 3 : Paramètres de configuration SAML

Paramètre	Configuration	Exemple
Public (ID d'entité)	Nom de domaine complet (FQDN)	mymanagementhost.mydomain.com
URL d'authentification unique	Point de terminaison SAML Assertion Customer Service (ACS)	https://mymanagementhost.mydomain.com/saml/acs
Format ID nom	Adresse électronique	S. O.
Nom d'utilisateur	Nom d'utilisateur	S. O.

5. Configurez les instructions d'attribut.



Remarque : Les modifications des attributs IDP dépendent du fournisseur et de la configuration spécifiques. Cisco IDP et ses attributs sont partagés ci-dessous à titre d'exemple.

- Première entrée
 - Name : Nom d'utilisateur
 - Valeur: user.login
- Deuxième entrée

- Name : E-mail principal
- Valeur: user.email
- Instructions d'attribut de groupe
 - Name : groupes
 - Filtre : REGEX
 - Valeur: .*

6. Configurez les paramètres de déconnexion unique (SLO) dans l'application.

Tableau 4 : Paramètres de configuration SLO

Champ	Valeur
Certificat de signature	Pour Okta, ce certificat n'est requis que si vous choisissez d'activer SLO. Téléchargez le certificat de signature à l'aide de Télécharger le certificat SP dans Fournisseurs d'identité. Enregistrez le fichier sous le nom sp-public-key.crt. Voir Configuration de déconnexion unique pour plus de détails.
Métadonnées SP	Les métadonnées du fournisseur de services (SP) sont requises pour le IDP ADFS uniquement (et non pour Okta).
Voulez-vous activer la déconnexion unique ?	Oui ou Non
URL de déconnexion unique	https://mymanagementhost.mydomain.com/saml/logout
Émetteur SP (ID d'entité/d'audience ou URL ACS)	https://mymanagementhost.mydomain.com

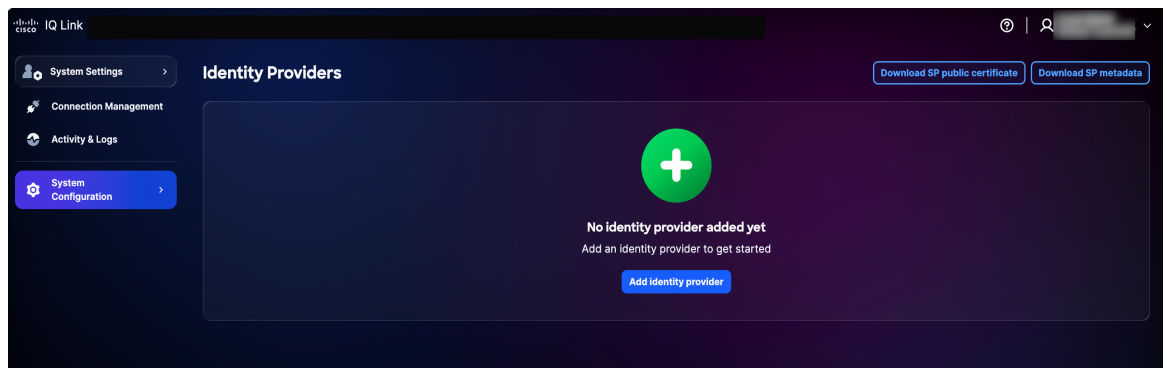
8. Cliquez sur l'icône Download pour télécharger le fichier « IDP Metadata XML ».

9. Provisionnez ou créez l'application selon les besoins du fournisseur.

Ajout du PDI Okta

Pour ajouter un IDP dans Cisco IQ :

1. Dans Paramètres système, choisissez Configuration système > Fournisseurs d'identités. La page Fournisseurs d'identités s'affiche.



Page d'accueil IDP



Remarque : Vous ne pouvez ajouter qu'un (1) PDI à la fois.

2. Cliquez sur Ajouter un fournisseur d'identité. La page Ajouter un fournisseur d'identité s'affiche.

Add Identity Provider

Identity provider name *

Enter identity provider name

Domains

Enter domain names **Add**

Organization IDP metadata *

Select or drag file to this area to upload

Only one file can be uploaded at 5 MB or less

☐ Enable single log out (SLO)

Save **Cancel**

Ajouter un fournisseur d'identité

3. Saisissez le nom du fournisseur d'identités.
4. Cliquez sur Add pour ajouter un nom de domaine configuré Cisco IQ au champ Domain(s).
5. Faites glisser et déposez ou téléchargez le fichier de métadonnées SAML obtenu à partir de l'application IDP dans le champ de métadonnées IDP de l'organisation. Ce fichier contient les détails du certificat et de l'entité SP.
6. (Facultatif) activez le bouton bascule Activer la déconnexion unique. Vous pouvez également activer le SLO ultérieurement.
7. Cliquez sur Save.

Configuration du mappage des rôles

1. Dans l'IDP ajouté, choisissez l'icône Plus d'options > Mapper les rôles. La page Mapper les rôles utilisateur s'affiche.

×

Map identity provider roles to system roles to assign permissions.

Map User Roles

IDP Role	System Role
iq-demo-user ×	General Account... × ▼ 🗑
	▼ 🗑
	▼ 🗑
	▼ 🗑
	▼ 🗑

+ Add identity provider role

Save

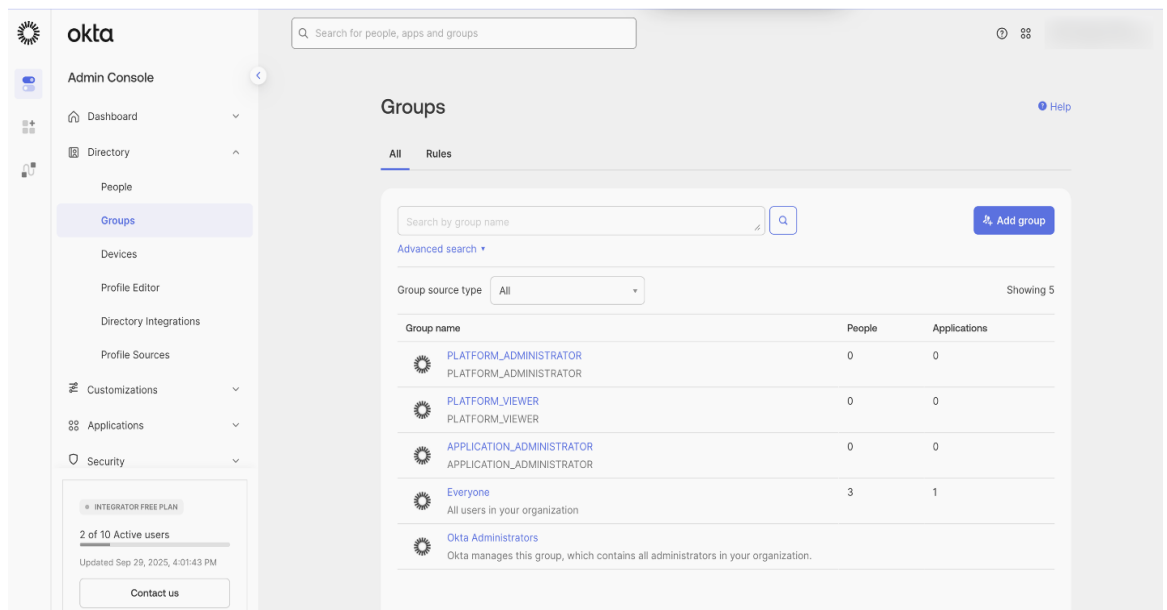
Mapper les rôles utilisateur

- Entrez un rôle IDP pour le rôle système sélectionné. Les rôles système suivants sont pris en charge :

- Administrateur de compte général : L'administrateur général du compte dispose des autorisations complètes pour effectuer toutes les actions du produit
- Observateur général de comptes : La visionneuse de comptes générale a un accès en lecture seule



Remarque : Le rôle IDP est un champ de texte ouvert. Il doit correspondre exactement au nom du groupe ou du rôle configuré dans le PID de votre entreprise. Un exemple de groupes Okta est présenté ci-dessous.



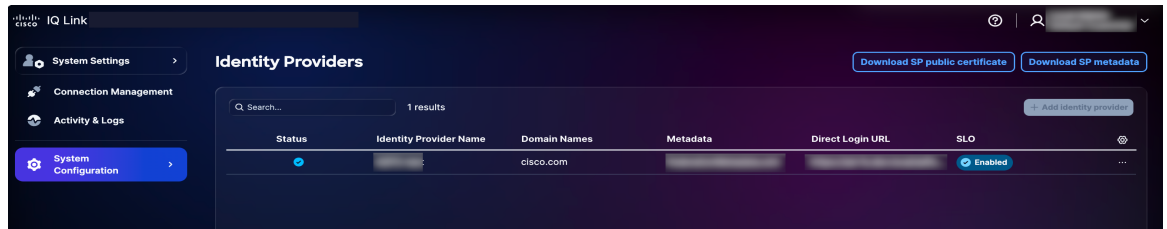
Référence de mappage de rôle

3. Mappez des rôles supplémentaires si nécessaire en cliquant sur Ajouter un rôle de fournisseur d'identité.
4. Cliquez sur Save. Une fois configurée, la page de connexion affiche une option permettant de se connecter avec SSO (via IDP).

Configuration de déconnexion unique

Si vous choisissez d'activer le SLO, vous devez télécharger les métadonnées qui incluent l'URL du SLO. Vous pouvez configurer cela en modifiant les paramètres de votre fournisseur d'identité et en activant l'option Activer la déconnexion unique. Pour terminer la configuration SLO :

1. Sur la page d'accueil Identity Providers, cliquez sur Download SP public certificate.



Certificat public SP

2. Enregistrez le fichier téléchargé sous le nom sp-public-key.crt.
3. Accédez à votre portail IDP.
4. Téléchargez le fichier de certificat de signature généré dans [Configuration SAML IDP pour SSO](#).
5. Saisissez l'URL du SLO (par exemple, https://ciq-xxx-xxx-37-160.cx-hub-rtt.cisco.com/saml/logout).
6. Saisissez l'émetteur du SP (par exemple, ciq-xxx-xxx-37-160.cx-hub-rtt.cisco.com).
7. Cliquez sur Submit.
8. Téléchargez à nouveau le fichier de métadonnées IDP.
9. Sur la page Fournisseurs d'identités, sélectionnez l'icône Autres options du IDP ajouté > Modifier.
10. Activez le bouton bascule Activer la déconnexion unique (SLO).
11. Téléchargez le fichier de métadonnées nouvellement téléchargé.
12. Utilisez la liste de contrôle suivante pour vérifier la fonctionnalité SSO et SLO :

Liste de vérification :

- La connexion de l'administrateur local a réussi
- Le portail IDP est configuré et provisionné
- IDP est ajouté à Cisco IQ avec un statut « Réussite »
- Les mappages de rôles sont configurés et testés
- Les métadonnées SP sont téléchargées et le certificat est extrait
- Si SLO est activé, la configuration de SLO est terminée avec le certificat de signature réelle
- Le flux SSO et SLO de bout en bout a été testé avec succès

Dépannage des problèmes IDP

Les tableaux suivants répertorient les problèmes courants et les solutions possibles pour identifier et résoudre rapidement les problèmes liés à l'état IDP, aux erreurs de certificat, aux échecs de connexion SSO et à la configuration SLO :

Tableau 5 : Dépannage

Problème	Solution
L'état IDP indique « Incomplete »	Vérifier les configurations de mappage des rôles
Erreurs de certificat	Vérifier le format et la validité du certificat
Échecs de connexion SSO	Valider le mappage d'attributs et les affectations de groupes
Le SLO ne fonctionne pas comme prévu	Vérifiez que le certificat est correctement chargé et que les URL SLO sont configurées

Configuration SAML ADFS IDP pour SSO

Cette section fournit des conseils pour configurer Microsoft Active Directory (AD) Federation Services (FS) en tant qu'IDP SAML pour Cisco IQ, en prenant en charge l'authentification basée sur mot de passe et PKI (Public Key Infrastructure) ou sur certificat.

Conditions requises pour configurer ADFS IDP SAML pour SSO

- ADFS 6.0+ est recommandé
- Windows Server 2016 + (recommandé en 2019)
- Intégration AD configurée avec les comptes d'utilisateurs
- Certificats SSL/TLS sur le serveur ADFS
- Accès administrateur à Cisco IQ
- Accès administratif au serveur ADFS (Windows Server)
- Accès PowerShell sur le serveur ADFS
- Connectivité réseau entre ADFS et Cisco IQ
- Autorité de certification d'entreprise (CA) (installée ou accessible)
- Privilèges d'administrateur de domaine ou d'administrateur d'entreprise (requis pour PKI uniquement)

- Détails de la configuration du serveur ADFS (comme indiqué dans le tableau ci-dessous)

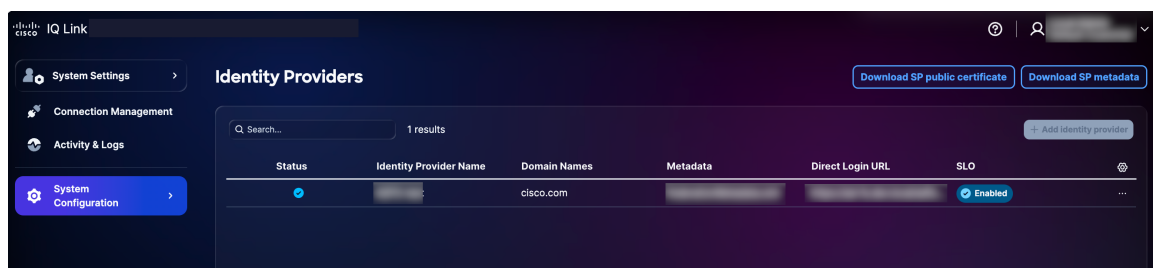
Tableau 6 : Présentation du flux d'authentification

Élément	Description	Exemple
FQDN Cisco IQ	Nom d'hôte du déploiement utilisateur	<Your-CIQ-FQDN> Par exemple, dev35-23.cx-xxx-xxx.cisco.com
URL du serveur ADFS	Adresse du serveur ADFS utilisateur	https://<Your-ADFS-HOSTNAME> Par exemple, https://adfs.dev.local
Domaine de la société	Domaine de messagerie	<Votre-domaine>
Groupe AD	Nom de domaine (DN) du groupe Active Directory	CXIQ OU=Groupes, DC=dev, DC=local
Nom de l'AC (PKI)	Nom de CA d'entreprise	<Nom-Autorité-de-certification>
Port d'authentification de certification (PKI)	Port TLS alternatif ADFS	49443
Empreinte numérique du certificat SSL	Certificat SSL du serveur ADFS	<Your-SSL-CERT-THUMBPRINT>

Configuration du SAML ADFS de base

Pour configurer ADFS :

1. Dans Paramètres système, choisissez Configuration système > Fournisseurs d'identités. La page Fournisseurs d'identités s'affiche.



Options de téléchargement

2. Cliquez sur Télécharger le certificat public SP et sur Télécharger les métadonnées SP pour télécharger ces fichiers.
3. Copiez et enregistrez les fichiers service-provider-metadata.xml et service-provider-certificate.crt sur le serveur ADFS (par exemple, C:\).

4. Connectez-vous au serveur ADFS.
5. Dans le menu Gestion ADFS, cliquez sur Approbations de partie de confiance.
6. Dans le menu Approbations de partie de confiance, cliquez sur Ajouter des approbations de partie de confiance. Le nouvel assistant s'ouvre.
7. Cliquez sur la case d'option Claims Aware.
8. Cliquez sur Start pour poursuivre la configuration.
9. Cliquez sur Importer des données sur la partie de confiance à partir d'un fichier pour obtenir des détails à partir du fichier qui est enregistré dans le cadre de l'étape 3.
10. Cliquez sur Parcourir pour sélectionner le fichier de métadonnées du fournisseur de services et terminer le téléchargement du fichier.
11. Cliquez sur Suivant.
12. Saisissez un nom d'affichage (par exemple, « Cisco IQ »), ajoutez les remarques appropriées, puis cliquez sur Next.
13. Sur la page Choisir une politique de contrôle d'accès, cliquez sur Autoriser tout le monde (ou sur la politique requise par la configuration de la sécurité de votre organisation).
14. Cliquez sur Next dans les autres écrans.
15. Cliquez sur Fermer pour terminer la configuration de l'approbation de la partie de confiance.



Remarque : Ne sélectionnez pas « Autoriser tout le monde avec MFA » sauf si votre serveur ADFS dispose d'un adaptateur MFA (Multi-Factor Authentication) enregistré (par exemple, Azure MFA, Mot de passe unique basé sur l'heure (TOTP) configuré).

Si cette stratégie est activée sans fournisseur MFA configuré, ADFS authentifie l'utilisateur mais refuse finalement la demande avec l'état `urn:oasis:names:tc:SAML:2.0:status:RequestDenied`. Comme la réponse SAML ne contient aucune assertion, le plug-in échoue et signale une erreur « message manquant ».

Problème : « Permit Everyone with MFA » (Autoriser tout le monde avec AMF) est sélectionné.

Solution de contournement: Dans PowerShell, vérifiez la stratégie actuelle en exécutant la commande suivante.

```
Get-AdfsRelyingPartyTrust -Name  
“
```

```
”).AccessControlPolicyName
```

To set “Permit everyone” (no MFA requirement), run the following command:
Set-AdfsRelyingPartyTrust -TargetName “

```
”
```

```
-AccessControlPolicyName “Permit everyone”
```

You can also create the trust through PowerShell:

```
-Add-AdfsRelyingPartyTrust `
```

```
=Name “
```

```
” `
```

```
-Identifier “
```

```
” `
```

```
-SamlEndpoint (New-AdfsSamlEndpoint -Binding POST -Protocol  
SAMLAssertionConsumer -Uri “
```

```
”) `
```

```
-AccessControlPolicyName “Permit everyone” `
```

```
-IssuanceAuthorizationRules '=> issue(Type =
```

```
“http://schemas.microsoft.com/authorization/claims/permit”, Value =  
“true”);
```

Configuration des règles de revendication ADFS

Pour configurer les règles de revendication ADFS, effectuez les étapes répertoriées dans les sections suivantes.

Demandes requises

Reportez-vous au tableau suivant pour connaître les demandes requises.

Tableau 7 : Demandes requises

Demande	Objectif	Source
Courriel	Identifiant utilisateur	Courrier AD
Nom d'affichage	Nom complet de l'utilisateur	Nom d'affichage AD
UPN	Authentification PKI/certificat	ADFS mappe le certificat client à un utilisateur AD via UPN
NomID	sujet SAML	Transformé à partir des e-mails
Groupes	Accès basé sur les rôles	Appartenance au groupe AD (memberOf)

Application des règles de réclamation

1. Définissez le nom de votre tiers de confiance (par exemple, « Cisco IQ - Production »).

```
$relyingPartyName = "Your-RP-Name"
```

2. Définissez des règles de revendication pour envoyer des informations utilisateur et l'appartenance à un groupe à Cisco IQ.

```
$claimRules = @'
@RuleTemplate = "LdapClaims"
@RuleName = "Send Email and Name"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"),
@RuleTemplate = "LdapClaims"
@RuleName = "Send UPN"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"),
query = ";userPrincipalName;{0}", param = c.Value);
@RuleName = "Transform Email to NameID"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "email");
@RuleName = "Send Group Membership"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/claims/Group"),
query = ";memberOf;{0}", param = c.Value);
'@
```

3. Appliquez les règles de revendication en exécutant la commande suivante :

```
Set-AdfsRelyingPartyTrust -TargetName $relyingPartyName
-IssuanceTransformRules $claimRules
```

Write-Host « Règles de revendication configurées avec succès ! » -
ForegroundColor Vert

Avertissement : L'attribut de messagerie doit être renseigné pour chaque compte d'utilisateur AD. Si cet attribut est manquant, l'assertion SAML ne contient pas de revendication d'e-mail, ce qui entraîne un rejet de l'authentification.

Pour mettre à jour l'adresse e-mail d'un utilisateur, exécutez la commande PowerShell suivante :

```
Set-ADUser -Identity “  
  
” -EmailAddress  
“  
  
”
```

Vérification des groupes d'utilisateurs

1. Définissez le nom d'utilisateur pour vérifier l'appartenance de l'utilisateur au groupe en exécutant la commande suivante :

```
$username = “username”
```

2. Exécutez les commandes suivantes pour rechercher le compte de l'utilisateur :

```
$searcher = [adsisearcher]“(samaccountname=$username)”  
$user = $searcher.FindOne()
```

3. Affichez les groupes auxquels l'utilisateur appartient à l'aide de la commande suivante :

```
$user.Properties.memberof
```

Exemple de rapport :

CN=Rôle - Développeurs CXIQ,OU=Groupes de rôles,DC=dev,DC=local

Configuration d'ADFS pour approuver le certificat de signature SP

1. Dans le serveur ADFS, importez le certificat SP dans le magasin TrustedPeople :

```
Import-Certificate -FilePath "C:-provider-certificate.crt"  
-CertStoreLocation "Cert:"
```

2. Choisissez l'une des options suivantes :



Remarque : Le certificat SP est émis par une autorité de certification interne qu'ADFS ne peut pas valider via la chaîne de confiance standard.

- Désactiver la validation de la chaîne globalement pour cette partie de confiance

```
Set-AdfsRelyingPartyTrust `  
-TargetIdentifier "
```

```
" `
```

```
-SigningCertificateRevocationCheck None `  
-EncryptionCertificateRevocationCheck None
```

- Si le certificat SP est émis par une autorité de certification (non auto-signé), importez le certificat de l'autorité de certification émettrice dans le magasin de certificats racine

```
Import-Certificate -FilePath "C:-ca.cer" -CertStoreLocation  
"Cert:"
```

3. Appliquez les modifications en redémarrant le service ADFS.

```
Restart-Service adfssrv
```

Configuration de l'authentification PKI/Certificate

Cette section décrit comment ajouter une authentification basée sur un certificat (c'est-à-dire une carte à puce ou un certificat logiciel) aux mots de passe. Cette section peut être ignorée si l'authentification par mot de passe uniquement est suffisante.

Installation du rôle AC AD CS

Pour installer le rôle d'autorité de certification AD Certificate Services (CS) :

1. Vérifiez si une autorité de certification d'entreprise existe déjà dans votre domaine en exécutant la commande suivante :

```
certutil -config - -ping
```

Si la commande renvoie une réponse valide, vous pouvez ignorer le reste de cette section. Votre environnement est déjà configuré. Si la commande indique qu'aucune autorité de certification n'a été trouvée, passez à l'étape 2.

2. Installez le rôle AC en exécutant la commande suivante :

```
install-WindowsFeature AD-Certificate -IncludeManagementTools
```

3. Configurez le rôle AC en exécutant la commande suivante :

```
install-AdcsCertificationAuthority `
-CAType EnterpriseRootCA `
-CACommonName "
    " `
-KeyLength 2048 `
-HashAlgorithmName SHA256 `
-CryptoProviderName "RSA#Microsoft Software Key Storage Provider" `
-ValidityPeriod Years `
-ValidityPeriodUnits 10 `
-Force
```

4. Vérifiez l'installation en exécutant la commande suivante :

```
certutil -ca
```

5. Vérifiez que le service est actif et accessible en exécutant la commande suivante :

```
certutil -config - -ping
```

Configuration d'un modèle de certificat

Pour configurer un modèle de certificat avec l'utilisation améliorée de la clé d'authentification du client :

1. Ouvrez certsrv.msc et développez le noeud AC.
2. Cliquez avec le bouton droit sur Modèles de certificats > Gérer.
3. Dupliquez le modèle Utilisateur.



Remarque : Le modèle utilisateur intégré est fonctionnel ou valide uniquement si le certificat émis à partir de celui-ci inclut l'EKU d'authentification du client.

4. Configurez les paramètres dans les onglets suivants :
 - Généralités: Saisissez « CIQ User Authentication » dans le champ Name avec une période de validité d'un (1) an
 - Traitement des demandes : Sélectionnez Signature and encryption dans la liste déroulante Purpose et cochez la case Allow private key to be export
 - Nom du sujet : Sélectionnez Générer à partir des informations Active Directory et incluez un e-mail dans les champs Objet et SAN

Avertissement : Les champs Subject et SAN doivent contenir le nom d'utilisateur principal (UPN) d'un utilisateur ou un e-mail qui correspond à un compte AD. ADFS mappe le certificat à un utilisateur AD à l'aide de ces champs.

- Extensions : Assurez-vous que les politiques d'application incluent « Authentification du client (1.3.6.1.5.5.7.3.2) »
- Sécurité: Ajouter des utilisateurs de domaine et leur accorder des autorisations Lecture et Inscription

5. Publiez le modèle à l'aide de la commande suivante :

```
Add-CATemplate -Name "CIQUserAuthentication" -Force
```

Inscription d'un certificat utilisateur

1. Connectez-vous en tant qu'utilisateur cible.
2. Inscrivez le certificat en exécutant la commande suivante :

```
certreq -enroll -user "CIQUserAuthentication"
```

3. Vérifiez l'installation du certificat en exécutant la commande suivante :

```
Get-ChildItem Cert:| Where-Object {  
$_.EnhancedKeyUsageList.ObjectId -contains "1.3.6.1.5.5.7.3.2"} | Format-Table Subject,
```

Exportation d'un certificat utilisateur à partir de Windows et installation sur le client (Mac)

Pour exporter un certificat utilisateur de Windows vers Mac :

1. Exportez le certificat de Windows en tant que fichier PFX en exécutant les commandes suivantes :

```
$cert = Get-ChildItem Cert:| Where-Object { $_.Subject -like "*  
  
*" }  
$password = ConvertTo-SecureString -String "  
  
" -Force -AsPlainText  
Export-PfxCertificate -Cert $cert -FilePath "C:-cert.pfx" -Password $password
```

2. Transférez le fichier user-cert.pfx sur votre périphérique Mac.
3. Importez le certificat dans la chaîne de clés Mac en exécutant la commande suivante :


```
security import user-cert.pfx -k ~/Library/Keychains/login.keychain-db -P “  
”
```



Remarque : Après l'importation du certificat, votre navigateur doit être fermé et rouvert pour qu'il soit reconnu.

4. Faites confiance à l'autorité de certification sur Mac en exécutant :

```
sudo security add-trusted-cert -d -r trustRoot \  
-k /Library/Keychains/System.keychain ca-certificate.cer
```

Activation des terminaux d'authentification de certificat ADFS

Pour activer les points de terminaison d'authentification de certificat ADFS :

1. Activez les points de terminaison de certificat ADFS requis en exécutant les commandes suivantes :

```
EEnable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificate  
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificatetransport  
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificate  
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificatetransport
```

2. Vérifiez que tous les terminaux sont activés en exécutant la commande suivante :

```
Get-AdfsEndpoint | Where-Object { $_.AddressPath -like “*cert*” } | Format-Table Address
```

Activation de l'authentification du certificat comme principal

Pour activer l'authentification du certificat en tant que certificat principal :

1. Configurez les principaux fournisseurs d'authentification pour l'accès intranet et extranet à l'aide de la commande suivante :

```
Set-AdfsGlobalAuthenticationPolicy `\  
-PrimaryIntranetAuthenticationProvider @(“CertificateAuthentication”, “WindowsAuthentic
```

```
-PrimaryExtranetAuthenticationProvider @"CertificateAuthentication", "FormsAuthentication"
```

2. Vérifiez que les deux listes incluent CertificateAuthentication et FormsAuthentication à l'aide des commandes suivantes :

```
(Get-AdfsGlobalAuthenticationPolicy).PrimaryIntranetAuthenticationProvider  
(Get-AdfsGlobalAuthenticationPolicy).PrimaryExtranetAuthenticationProvider
```

3. Vérifiez la configuration actuelle du port client TLS à l'aide de la commande suivante :

```
Get-AdfsProperties | Select-Object HostName, HttpsPort, TlsClientPort
```

4. Si le TlsClientPort n'est pas 49443, mettez à jour le port et redémarrez le service ADFS à l'aide des commandes suivantes :

```
Set-AdfsProperties -TlsClientPort 49443  
Restart-Service adfssrv
```

Correctifs SChannel/TLS (CRITIQUES pour PKI)

Les étapes des sections suivantes résolvent les erreurs CERT_E_UNTRUSTEDROOT (0x800B0109) qui empêchent l'authentification de certificat de fonctionner.

Liaison de certificats SSL sur le port 49443

Pour lier des certificats SSL sur le port 49443 :

1. Supprimez toutes les liaisons de certificat SSL existantes sur le port 49443 à l'aide de la commande suivante :

```
>netsh http delete sslcert  
hostnameport=
```

:49443

2. Créez une nouvelle liaison avec la négociation de certificat client activée à l'aide de la commande suivante :

```
netsh http add sslcert hostnameport=
```

```
          :49443 `
certhash=
```

```

appid="{5d89a20c-beab-4389-9447-324788eb944a}" `
certstorename=MY `
clientcertnegotiation=enable `
verifyclientcertrevocation=disable
```

3. Vérifiez que la négociation de certificat client est activée à l'aide de la commande suivante :

```
http show sslcert
hostnameport=
```

```
          :49443
```

Nettoyage du magasin de certificats (CRITIQUE)

Pour nettoyer le magasin de certificats :

Avertissement : Windows SChannel rejette tous les certificats clients si des certificats non auto-signés sont présents dans le magasin racine de confiance. Il s'agit de la principale cause des défaillances PKI.

1. Identifiez les certificats non auto-signés dans le magasin racine de confiance en exécutant la commande suivante :

```
$bad = Get-ChildItem Cert:| Where-Object { $_.Issuer -ne $_.Subject }
$bad | ForEach-Object { Write-Host "PROBLEM: $(($_.Subject) | Issuer: $(($_.Issuer))" -For
```

2. Déplacez ces certificats vers le magasin d'autorité de certification intermédiaire en exécutant la commande suivante :

```
$bad | Move-Item -Destination Cert:\IntermediateCA
Write-Host "Moved $($bad.Count) cert(s) from Root to Intermediate CA store" -ForegroundColor
```

3. Vérifiez qu'aucun certificat non auto-signé ne reste dans le magasin racine de confiance en exécutant la commande suivante :

```
Get-ChildItem Cert:| Where-Object { $_.Issuer -ne $_.Subject }
```

Correctifs du registre SChannel (CRITIQUE)

Pour configurer les paramètres du registre SChannel afin de garantir une authentification de certificat appropriée :

1. Définissez la variable de chemin d'accès du Registre à l'aide de la commande suivante :

```
$regPath = "HKLM:"
```

2. Appliquez les paramètres de registre définis dans le tableau ci-dessous à l'aide des commandes suivantes :

```
Set-ItemProperty -Path $regPath -Name "ClientAuthTrustMode" -Value 2 -Type DWord
Set-ItemProperty -Path $regPath -Name "SendTrustedIssuerList" -Value 0 -Type DWord
```

Tableau 8 : Paramètres du registre SChannel

Réglage	Valeur	Objectif
ModeConfianceAuthClient	2	Active l'approbation CA exclusive pour corriger le chemin de validation par défaut.
EnvoyerListeÉmetteursDeConfiance	0	Empêche le serveur d'envoyer la liste complète des émetteurs approuvés pendant la connexion TLS.

Vérification du magasin de certificats CA

Pour vérifier le magasin de certificats CA :



Remarque : Le certificat de l'autorité de certification qui émet les certificats



utilisateur doit se trouver dans SystemCertificatesstore pour s'assurer qu'il est correctement reconnu.

1. Définissez l'empreinte numérique de votre certificat CA à l'aide de la commande suivante :

```
$caThumbprint = “
```

```
”
```

2. Vérifiez que le certificat CA est déjà présent dans le LocalMachinestore* à l'aide de la commande suivante :

```
$exists = Test-Path “HKLM:\caThumbprint”
```

Si le certificat est introuvable, importez-le dans le magasin LocalMachine :

```
if (-not $exists) {  
    Import-Certificate -FilePath “C:\YOUR-CA-CERT>.cer” `  
    -CertStoreLocation “Cert:”  
}
```

Redémarrage du serveur ADFS (OBLIGATOIRE)

Redémarrez le serveur ADFS à l'aide de la commande suivante :

```
Restart-Computer -Force
```



Remarque : La modification de registre ClientAuthTrustMode prend effet uniquement après le redémarrage du serveur.

Exportation des métadonnées ADFS

Vous pouvez télécharger vos métadonnées ADFS à l'aide de PowerShell ou de votre navigateur Web.

PowerShell

Pour exporter des métadonnées ADFS à l'aide de PowerShell :

1. Ouvrez PowerShell sur votre serveur ADFS.
2. Exécutez les commandes suivantes pour télécharger le fichier de métadonnées.

```
$metadataUrl = (Get-AdfsEndpoint | Where-Object {$_.Protocol -eq "Federation Meta  
Invoke-WebRequest -Uri $metadataUrl.AbsoluteUri -OutFile "C:-metadata.xml"  
Write-Host "ADFS metadata exported to C:-metadata.xml" -ForegroundColor Green
```

Une fois les commandes exécutées, le fichier de métadonnées est enregistré dans C :-metadata.xml.

Navigateur Web

Pour exporter des métadonnées ADFS à l'aide d'un navigateur Web :

1. Accédez à <https://<votre-serveur-adfs>/FederationMetadata/2007-06/FederationMetadata.xml>, en remplaçant « <votre-serveur-adfs> » par le nom d'hôte de votre serveur ADFS.
2. Enregistrez le fichier XML de métadonnées sur votre ordinateur lorsque vous y êtes invité.

Configuration sur Cisco IQ

Pour configurer sur Cisco IQ :

1. Transférez adfs-metadata.xml vers votre station de travail.
2. Dans Cisco IQ, accédez à System Settings > System Configuration > Identity Providers.
3. Téléchargez le fichier de métadonnées ADFS pour extraire automatiquement le certificat IDP, l'ID d'entité et l'URL SSO.
4. Enregistrez la configuration.



Remarque : Si ADFS effectue un transfert automatique de certificat de signature de jeton, vous devez réexporter le fichier de métadonnées et le télécharger vers Cisco IQ pour garantir la continuité de l'authentification.

Ajout du IDP ADFS

1. Sur la page Fournisseurs d'identité, cliquez sur Ajouter un fournisseur d'identité.
2. Saisissez le nom du fournisseur d'identités.
3. Entrez le ou les domaines (par exemple, company.com).
4. (Facultatif) activez le bouton bascule Activer la déconnexion unique, si nécessaire.
5. Faites glisser ou téléchargez le fichier de métadonnées SAML obtenu à partir de l'application IDP dans le champ Upload IDP Metadata.
6. Cliquez sur Save.



Remarque : L'état est « Incomplet » jusqu'à ce que le mappage des rôles soit terminé ; c'est un comportement attendu.

Configuration du mappage des rôles

Avant de configurer le mappage de rôles, assurez-vous que vous pouvez trouver des groupes d'Active Directory à utiliser pour le mappage. Pour rechercher des groupes à partir d'Active Directory, exécutez la commande PowerShell suivante :

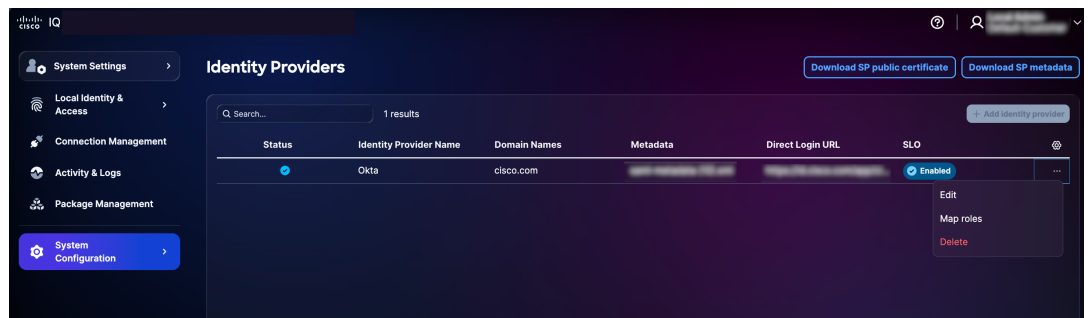
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = "(&(objectClass=group)(cn=Role - CXIQ*))"
$searcher.PropertiesToLoad.Add("distinguishedName") | Out-Null
$searcher.PropertiesToLoad.Add("cn") | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties["distinguishedname"] }
```

Le système interroge AD directement via le protocole LDAP (Lightweight Directory Access Protocol), sans nécessiter de modules supplémentaires. Les informations de groupe sont renvoyées dans le format complet du nom unique, par exemple :

```
CN=Role - CXIQ Developers, OU=Groups, DC=dev, DC=example,
DC=com
CN=Role - CXIQ Viewers, OU=Groups, DC=dev, DC=example,
DC=com
```

Si les groupes requis ne sont pas répertoriés, ils doivent être créés dans Active Directory par un administrateur de compte avant que vous puissiez effectuer le mappage de rôle ADFS.

Pour configurer le mappage des rôles :



Mappage des rôles

1. Dans l'IDP ajouté, choisissez l'icône Plus d'options > Mapper les rôles. La page Mapper les rôles utilisateur s'affiche.

Cisco IQ Link_IDP

X

Map identity provider roles to system roles to assign permissions.

Map user roles

IDP role	System role
	General Account...
	General Account...
	Select option
	Select option
	Select option

+ Add identity provider role

Save

Mappage des rôles

2. Entrez un rôle IDP pour le rôle système sélectionné. Les rôles système suivants sont pris en charge :

- Administrateur de compte général : L'administrateur général du compte dispose des autorisations complètes pour effectuer toutes les actions du produit. Le rôle IDP (nom analysé) est CXIQ Admins.
- Observateur général de comptes : La Visionneuse de comptes générale dispose d'un accès en lecture seule. Le rôle IDP (nom analysé) est Développeurs et visualiseurs CXIQ.



Remarque : Utilisez des noms analysés (par exemple, Développeurs CXIQ) et non des noms distinctifs complets.

3. Cliquez sur Save. L'état est mis à jour en Réussite.

Test de certification client SChannel

Pour vérifier que SChannel est correctement configuré pour accepter les certificats clients, ouvrez une nouvelle fenêtre PowerShell et exécutez la commande suivante :

```
curl.exe -insecure `
-cert "CurrentUser\YOUR-USER-CERT-THUMBPRINT>" `
-v "https://
```

```
:49443/adfs/ls/"
```

La sortie attendue est une réponse HTTP (par exemple, une redirection ou la page ADFS). Si une erreur de connexion TLS se produit, la connexion a échoué.

Test de bout en bout du navigateur pour le flux PKI

Avant de commencer le test de bout en bout du navigateur pour le flux PKI, assurez-vous que le certificat utilisateur est installé dans MacOS Keychain (voir [Importation du certificat utilisateur sur un ordinateur client \(MacOS\)](#)).

Pour tester :

1. Accédez à l'URL de connexion SAML de l'application. ADFS présente les options de certificat et de mot de passe.
2. Sélectionnez Authentification par certificat. Le navigateur demande un certificat.
3. Téléchargez le certificat. Le système ADFS authentifie l'utilisateur, redirige la requête avec une réponse SAML et établit une nouvelle session.

Test de bout en bout du navigateur pour le flux de mots de passe

Avant de commencer le test de bout en bout du navigateur pour le flux de

mots de passe :

1. Accédez à l'URL de connexion SAML de l'application. ADFS présente les options de certificat et de mot de passe.
2. Sélectionnez Mot de passe/Authentification par formulaire.
3. Saisissez Username.
4. Saisissez Password.
5. Vérifiez que la connexion a réussi.



Remarque : Les deux flux doivent fonctionner simultanément.

Dépannage des problèmes ADFS

La liste suivante présente les problèmes courants et les solutions possibles pour identifier et résoudre rapidement les problèmes liés à l'état ADFS, aux erreurs de certificat, aux échecs de connexion SSO et à la configuration SLO.

Tableau 9 : Problèmes ADFS

Problème	Symptômes / Description	Causes / Contrôles / Contournements et solutions
Groupes non extraits	Aucun rôle après la connexion	◦ Règle de revendication manquante : Réexécutez les instructions de la section Configuration des règles de revendication ADFS
Échec du décodage	« Impossible de déchiffrer l'assertion » dans les journaux	Vérifier la configuration du certificat ADFS
Boucle de connexion	Blocage dans une boucle d'authentification ou de connexion	◦ URL ACS non valide : Vérifier : https://your-fqdn/saml/acs ◦ Incompatibilité de cookies : Vérifier les cookies du navigateur pour le

Problème	Symptômes / Description	Causes / Contrôles / Contournements et solutions
		domaine correct

Commandes de diagnostic à dépanner

Pour garantir une intégration réussie entre votre environnement ADFS et Cisco IQ, utilisez les commandes de diagnostic suivantes. Ces commandes permettent de vérifier l'accessibilité des métadonnées, les configurations de certificats et les paramètres des points de terminaison.

- Vérifiez l'accessibilité des métadonnées ADFS : confirmez que les métadonnées de la fédération ADFS sont accessibles et accessibles au public ; il s'agit d'une étape essentielle pour établir la confiance initiale

```
curl -k https://
```

```
/FederationMetadata/2007-06/FederationMetadata.xml
```

- Validez le certificat de chiffrement : S'assurez que le certificat de cryptage correct est associé à l'approbation de la partie de confiance Cisco IQ

```
Get-AdfsRelyingPartyTrust -Name "Cisco IQ - Production" |  
Select-Object EncryptionCertificate | Format-List
```

- Vérifier la configuration des terminaux SAML : Vérifiez que les points de terminaison SAML pour la confiance Cisco IQ sont correctement configurés et que les demandes et assertions d'authentification sont routées vers les URL attendues

```
Get-AdfsRelyingPartyTrust -Name "Cisco IQ - Production" |  
Select-Object SamlEndpoints
```

Configuration SAML de Microsoft Entra ID pour SSO

Cette section fournit des conseils pour configurer Microsoft Entra ID (Entra ID) en tant qu'IDP SAML pour Cisco IQ, prenant en charge à la fois

l'authentification basée sur mot de passe et l'PKI ou l'authentification basée sur certificat (CBA).

Conditions requises pour configurer l'ID supplémentaire SAML pour SSO

- Entra ID tenant (par exemple, « ciqtestdev.onmicrosoft.com »)
- Accès au rôle Administrateur général ou Administrateur d'applications à Cisco IQ
- Connectivité entre Entra ID (cloud) et Cisco IQ
- AC d'entreprise installée ou accessible (requis pour PKI uniquement)
- Point de distribution de la liste de révocation de certificats (CRL) accessible depuis Internet (requis pour PKI uniquement)

Tableau 10 : Configuration du serveur d'ID supplémentaire

Élément	Description	Exemple
ID du locataire	Identifiant du locataire ID supplémentaire	37352d8f-0ebe-4762-8161-8775ffe897cb
FQDN Cisco IQ	Nom d'hôte de déploiement	<YOUR-CIQ-FQDN>
ID d'entité IDP	Entrer l'URL du fournisseur	https://sts.windows.net/<ID-LOCATAIRE>/
URL SSO IDP	Point de terminaison de connexion SAML	https://login.microsoftonline.com/<ID-LOCATAIRE>/saml2
Domaine de la société	Domaine de messagerie pour les utilisateurs	<VOTRE-DOMAINES>

Configuration de l'application SAML ID entrée

Création d'une application d'entreprise

1. Connectez-vous au [centre d'administration Microsoft Entra](#).
2. Accédez à Identity > Applications > Enterprise applications.
3. Cliquez sur Nouvelle application > Créer votre propre application.
4. Entrez le nom (par exemple, « Cisco IQ »).
5. Sélectionnez Intégrer toute autre application que vous ne trouvez pas

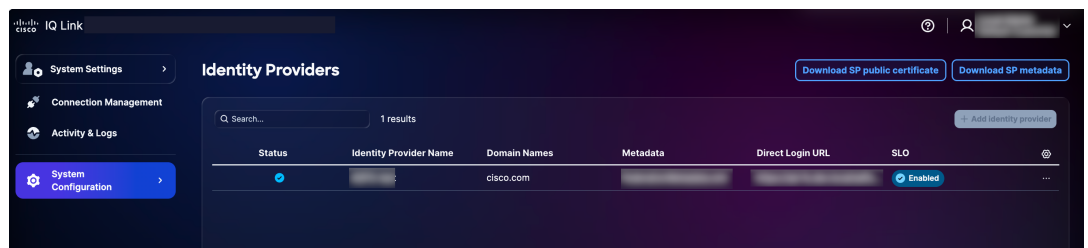
dans la galerie (hors galerie).

6. Cliquez sur Créer.

Configuration de l'authentification unique SAML

Pour configurer l'authentification unique SAML, vous devez télécharger le fichier de métadonnées SP. Vous pouvez l'obtenir en effectuant les étapes suivantes à partir de VA :

1. Dans Paramètres système, choisissez Configuration système > Fournisseurs d'identités. La page Fournisseurs d'identités s'affiche.



Options de téléchargement

2. Cliquez sur Download SP metadata pour télécharger. Ce fichier de métadonnées SP téléchargé est téléchargé pour terminer la configuration de l'authentification unique SAML.
3. Cliquez sur le bouton Upload Metadata file pour télécharger le fichier de métadonnées SP. Les données du fichier de métadonnées SP sont automatiquement renseignées dans l'écran d'authentification unique SAML après le téléchargement réussi.

Vous pouvez également choisir d'entrer manuellement ces détails pour configurer les paramètres d'authentification unique. Pour configurer manuellement l'authentification unique SAML :

4. Dans l'application d'entreprise, accédez à Authentification unique et sélectionnez SAML.
5. Dans la section Configuration SAML de base, cliquez sur Modifier et entrez les éléments suivants :
 - Identificateur (ID d'entité) : <YOUR-CIQ-FQDN>
 - URL de réponse (URL ACS) : https://<YOUR-CIQ-FQDN>/saml/acs
 - URL de connexion : https://<YOUR-CIQ-FQDN>/saml/login
 - URL de déconnexion : https://<YOUR-CIQ-FQDN>/saml/logout

6. Cliquez sur Save.



Remarque : L'ID d'entité doit correspondre exactement à ce que Cisco IQ utilise comme ID d'entité SP. Il s'agit généralement du nom de domaine complet du déploiement.

7. Pour configurer les attributs et les revendications SAML, cliquez sur Modifier dans la section Attributs et revendications.

8. Configurez les revendications suivantes :

Tableau 11 : Allégations SAML requises

Demande Attribut source		Espace de noms
Identifiant utilisateur unique (NameID)	user.userprincipalname	(par défaut)
adresse e-mail	user.mail	http://schemas.xmlsoap.org/ws/2005/05/identity
prénom	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity
nom de famille	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity
nom	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity
groupes	utilisateur.assignerdroles	(VIDE — effacer l'espace de noms)



Remarque : Pour les groupes revendiquent :

- Utilisez user.assignedroles comme source, et non user.groups
- Le champ Namespace doit être vide. Cela garantit que le nom d'attribut dans l'assertion SAML est simplement des groupes au lieu d'un URI (Uniform Resource Identifier) complet
- N'ajoutez pas de revendication de groupe dupliquée avec user.groups car cela entraîne des conflits

Configuration des rôles des applications

Les rôles d'application sont configurés dans l'enregistrement d'application (et non dans l'application d'entreprise) ; pour configurer les rôles d'application :

1. Accédez à Identity > Applications > App registrations.
2. Recherchez et sélectionnez votre application.

3. Accédez à Rôles d'application > Créer un rôle d'application.
4. Pour chaque rôle requis, configurez les éléments suivants :
 - Nom d'affichage : Par exemple, les administrateurs Cisco IQ
 - Types de membres autorisés : Utilisateurs/groupes
 - Valeur: Par exemple, les administrateurs Cisco IQ
 - Description: Par exemple, les administrateurs Cisco IQ
5. Cliquez sur Apply.



Remarque : Créez des rôles correspondant à vos exigences de mappage de rôles Cisco IQ (par exemple, Administrateurs CXIQ, Développeurs CXIQ ou Visionneuses CXIQ).

Les rôles d'application sont utilisés à la place des revendications de groupe pour les raisons suivantes :

- Les locataires cloud uniquement ne peuvent pas envoyer de noms d'affichage de groupe sans licence P1 ou P2
- sAMAccountName fonctionne uniquement pour les groupes synchronisés à partir d'Active Directory sur site
- La source d'ID de groupe envoie des identifiants uniques universels (UUID) difficiles à mapper
- Les rôles d'application envoient des valeurs de chaîne exactes correspondant aux attentes des rôles Cisco IQ

Affectation d'utilisateurs à des rôles d'application

Pour affecter des utilisateurs à des rôles d'application :

1. Revenez à l'application d'entreprise > Utilisateurs et groupes.
2. Cliquez sur Ajouter un utilisateur/groupe.
3. Sélectionnez le ou les utilisateurs et attribuez le rôle d'application approprié.
4. Cliquez sur Attribuer. Les valeurs de rôle s'affichent sous forme de chaînes lisibles dans l'attribut des groupes d'assertions SAML.

Téléchargement des métadonnées et du certificat IDP

Pour télécharger les métadonnées et le certificat IDP :

1. Dans l'application d'entreprise, choisissez Single Sign-On > SAML Signing Certificate.
2. Téléchargez le fichier XML des métadonnées de fédération (enregistrez-le sous entra-id-metadata.xml).

OU

Téléchargez le certificat (Base64) pour la saisie manuelle des certificats.

3. Notez les valeurs suivantes dans la section Configuration :
 - URL de connexion (IDP SSO URL)
 - Identificateur Azure AD (ID d'entité IDP)
 - URL de déconnexion (IDP SLO URL)



Remarque : Comme l'ID d'entrée effectue une rotation périodique des certificats de signature, vous devez télécharger à nouveau les métadonnées et les télécharger sur VA chaque fois que le certificat actif change pour garantir un service SSO ininterrompu.

Ajout d'un ID supplémentaire IDP



Remarque : Les routes APISIX pour SAML sont automatiquement créées lorsqu'un IDP est ajouté dans Cisco IQ, éliminant ainsi la nécessité d'une configuration de route manuelle.

Pour ajouter un ID supplémentaire IDP :

1. Connectez-vous à VA en tant qu'administrateur de compte.
2. Accédez à Paramètres système > Configuration système > Fournisseurs d'identités.
3. Cliquez sur Ajouter un fournisseur d'identité.
4. Saisissez le nom de l'ID interne (par exemple, « ID d'entrée »).
5. Entrez le ou les domaines (par exemple, « ciqtestdev.onmicrosoft.com » ou le domaine de votre entreprise).
6. (Facultatif) activez le bouton bascule Activer la déconnexion unique, si nécessaire.

7. Faites glisser et déposez ou téléchargez le fichier entra-id-metadata.xml obtenu à partir de Entra ID dans le champ Upload IDP Metadata.

8. Cliquez sur Save.



Remarque : L'état reste « Incomplet » jusqu'à ce que le mappage des rôles soit terminé ; c'est le comportement attendu.

Configuration du mappage des rôles

Pour configurer le mappage de rôle :

1. Dans l'IDP ajouté, choisissez l'icône Plus d'options > Mapper les rôles. La page Mapper les rôles utilisateur s'affiche.
2. Entrez un rôle IDP pour chaque rôle système. Les rôles système suivants sont pris en charge :

Tableau 12 : Rôles système

Rôle système	Rôle IDP (Valeur du rôle d'application)	Description
administrateur_compte_général	Administrateurs CXIQ	Autorisations complètes pour toutes les actions
visualiseur_compte_général	Développeurs CXIQ	Accès en lecture seule
visualiseur_compte_général	Visionneuses CXIQ	Accès en lecture seule



Remarque : Utilisez les chaînes de valeur du rôle d'application exactement comme configurées dans ID supplémentaire (voir [Configuration des rôles d'application](#) pour plus de détails)

4. Cliquez sur Save. L'état est mis à jour en Réussite.

Vérification du flux SAML (authentification par mot de passe)

Pour vérifier le flux SAML :

1. Ouvrez un navigateur en mode Incognito ou Privé.
2. Accédez à <https://<YOUR-CIQ-FQDN>/saml/login>.

3. Vérifiez que vous êtes redirigé vers la page de connexion Microsoft.
4. Authentifiez-vous avec vos identifiants (et MFA si configuré).
5. Après l'authentification, vérifiez que vous êtes redirigé vers /saml/acs et que l'application Cisco IQ s'affiche.
6. Vérifiez l'extraction du groupe en exécutant la commande suivante :

```
kubect1 -ncxue logs deployment/apisix -since=5m | grep -E "authentication success
```

Résultats attendus

Authentification conforme à SAML 2.0 réussie pour l'utilisateur :
user@domain.com avec le nom complet : N/A et 1 groupes

Groupe extrait : Administrateurs CXIQ (original : Administrateurs CXIQ)

Nombre total de groupes extraits : 1

Configuration de l'authentification basée sur certificat

Cette section décrit comment ajouter CBA aux mots de passe. Cette section peut être ignorée si l'authentification par mot de passe uniquement est suffisante.

Conditions préalables pour CBA

- Windows Server avec AD CS avec Enterprise CA configuré (par exemple, « DEV-ADCS-CA »)
- Accès administrateur PowerShell sur le serveur AC
- Le certificat UPN doit correspondre à l'ID supplémentaire userPrincipalName
- Le point de distribution CRL doit être accessible à partir d'Internet

Création d'un modèle de certificat sur AD CS

1. Ouvrez certtmpl.msc sur le serveur AC.
2. Dupliquez le modèle Utilisateur et nommez-le « EntraUserCert ».
3. Configurez le modèle :
 - Généralités: Nom complet EntraUserCert, validité 1-2 ans

- Traitement des demandes : Objectif = Signature et cryptage
- Nom du sujet : Sélectionnez Approvisionnement dans la demande
- Extensions : Les stratégies d'application doivent inclure l'authentification client (1.3.6.1.5.5.7.3.2)
- Sécurité: Accorder des autorisations Lecture et Inscription aux utilisateurs authentifiés

4. Publiez le modèle à l'aide de la commande suivante :

```
Add-CATemplate -Name "EntraUserCert" -Force
```

Demande et émission d'un certificat utilisateur

1. Créez un fichier de configuration de certificat (INF) (par exemple, C:-cert.inf) en utilisant le script PowerShell suivant :

```
@"
[Version]
Signature = "`$Windows NT`$"
[NewRequest]
Subject = "CN=

"

KeyLength = 2048
KeySpec = 1
KeyUsage = 0xa0
MachineKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
RequestType = PKCS10
[RequestAttributes]
CertificateTemplate = EntraUserCert
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.2
OID = 1.3.6.1.4.1.311.20.2.2
[Extensions]
2.5.29.17 = "{text}"
_continue_ = "upn=

&"
_continue_ = "email=

"
```

```
"@ | Out-File -FilePath C:-cert.inf -Encoding ASCII
```

2. Remplacez <USER-UPN> par votre ID supplémentaire UPN (par exemple, user@ciqtestdev.onmicrosoft.com).

3. Pour générer le certificat, exécutez les commandes suivantes :

```
certreq -new C:-cert.inf C:-cert.csr
```

4. Pour envoyer la demande à l'autorité de certification, exécutez la commande suivante :

```
certreq -submit -config "
```

```
\CA-NAME>" C:-cert.csr C:-cert.cer
```

5. Pour installer le certificat sur l'autorité de certification, exécutez la commande suivante :

```
certreq -accept C:-cert.cer
```

Exportation de certificats

Pour exporter le certificat utilisateur en tant que fichier PFX (pour le client), exécutez le script suivant :

```
$cert = Get-ChildItem Cert: | Where-Object { $_.Subject -like "*" }
```

```
*" }
```

```
$password = ConvertTo-SecureString -String "
```

```
” -Force -AsPlainText  
Export-PfxCertificate -Cert $cert -FilePath C:-cert.pfx -Password $password
```

Pour exporter le certificat racine de l'autorité de certification (pour l'ID d'entrée), exécutez le script suivant :

```
Get-ChildItem Cert: | Where-Object { $_.Subject -like “*  
*” } |  
Select-Object -First 1 | Export-Certificate -FilePath C:-root.cer -Type CERT
```

Importation du certificat utilisateur sur l'ordinateur client (MacOS)

Pour importer le certificat utilisateur (PFX), exécutez la commande suivante :

```
security import /path/to/entra-cert.pfx -k ~/Library/Keychains/login.keychain-db
```

”

Pour importer le certificat racine de l'autorité de certification, exécutez la commande suivante :

```
security import /path/to/ca-root.cer -k ~/Library/Keychains/login.keychain-db
```

Pour définir le certificat CA sur Toujours faire confiance à l'accès par chaîne de clés :

1. Ouvrez Keychain Access.
2. Recherchez le certificat CA et cliquez sur Get Info.

3. Sous Trust, sélectionnez « Always Trust ».



Remarque : Après l'importation, quittez et rouvrez votre navigateur pour que le certificat soit reconnu.

Téléchargement du certificat racine CA vers l'ID d'entrée

1. Connectez-vous au [centre d'administration Microsoft Entra](#).
2. Accédez à Protection > Security > Certificate Authorities.
3. Cliquez sur Upload et sélectionnez le fichier ca-root.cer.
4. Marquez-le comme certificat CA racine.
5. Saisissez l'URL du point de distribution CRL (doit être accessible publiquement).

Activation de CBA dans les méthodes d'authentification Entra ID

1. Accédez à Protection > Authentication methods > Policies.
2. Cliquez sur Certificate-based authentication pour configurer.
3. Activez CBA et ajoutez les utilisateurs ou groupes cibles.
4. Sous Configure, définissez le niveau de protection sur Single-factor authentication.

Configuration de la liaison de nom utilisateur

Dans la configuration CBA, accédez à l'onglet Username binding et définissez la liaison suivante :

- Champ Certificat : NomPrincipal
- Attribut utilisateur : NomPrincipalUtilisateur

Cela permet de mapper le nom UPN dans le nom alternatif de sujet (SAN) du certificat à l'utilisateur Entra ID.

Vérification du flux CBA

1. Ouvrez un navigateur en mode Incognito ou Privé.
2. Accédez à <https://<YOUR-CIQ-FQDN>/saml/login>.
3. Dans la page de connexion de Microsoft, saisissez l'adresse e-mail de l'utilisateur et cliquez sur Suivant.

4. Choisissez Utiliser un certificat ou une carte à puce (ou il peut afficher une invite automatique).
5. Sélectionnez le certificat utilisateur applicable lorsque le navigateur vous invite à sélectionner un certificat.
6. Vérifiez que Entra ID valide le certificat, redirige avec une réponse SAML et crée une session.



Remarque : Assurez-vous de sélectionner le certificat client correct. La sélection d'un certificat incorrect (par exemple, un certificat d'un autre utilisateur ou un certificat expiré) entraîne l'échec de l'authentification.

Dépannage des problèmes d'ID supplémentaire

La liste suivante présente les problèmes courants et les solutions possibles pour vous aider à identifier et résoudre rapidement les problèmes liés à la configuration SAML d'ID supplémentaire.

Tableau 13 : Dépannage

Problème	Motif	Régler
Réponse SAML non valide - e-mail manquant	L'assertion SAML n'a pas d'attribut NameID ou email	Vérifiez la configuration des revendications d'ID supplémentaire (voir Configuration de l'authentification unique SAML pour plus de détails). Vérifiez que l'attribut de messagerie de l'utilisateur est renseigné.
Nombre total de groupes extraits : 0	Revendication de groupe non configurée ou source incorrecte	Utilisez user.assignedroles comme source. Assurez-vous que l'utilisateur est affecté à un rôle d'application (voir Affectation d'utilisateurs à des rôles d'application pour plus de détails).
Revendications de groupes dupliquées	user.groups et user.assignedroles actifs	Supprimez la revendication user.groups. Ne conserver que user.assignedroles.
Groupes affichés comme UUID	L'attribut source est « ID de groupe »	Utilisez l'approche Rôles d'application (voir Configuration des rôles d'application pour plus de détails).

Problème	Motif	Régler
Le nom d'attribut indique un URI long	Le champ Espace de noms n'est pas vide	Effacez le champ Namespace dans les paramètres de revendication de groupe.
Signature SAML non valide	Certificat IdP pivoté ou non conforme	Téléchargez à nouveau les métadonnées à partir de l'ID d'entrée et téléchargez à nouveau vers Cisco IQ. Publiez la liste de révocation de certificats sur une URL accessible au public ou utilisez l'approche d'autorité de certification auto-signée (voir Contournement des listes de révocation de certificats pour les problèmes d'accessibilité pour plus de détails).
AADSTS500191	CRL inaccessible depuis Internet	Vérifiez que le certificat utilisateur est importé dans MacOS Keychain Access (voir Importation du certificat utilisateur sur l'ordinateur client (MacOS) pour plus de détails), CBA est activé dans Entra ID avec les paramètres requis (voir Activation de CBA dans Entra ID Authentication Methods pour plus de détails), et Chrome est redémarré pour appliquer les modifications.
Certificat non demandé	Certificat non inclus dans la chaîne de clés, CA non approuvé sur le client ou CBA non activé	Augmenter clock_skew_seconds dans la configuration du plugin (la valeur par défaut est 300 ; utilisez 30000 pour les travaux pratiques).
Assertion SAML expirée	Inversion d'horloge entre les systèmes	Mappage complet des rôles (voir Configuration du mappage des rôles pour plus de détails).
État « Incomplet » dans l'appliance virtuelle	Mappage des rôles non encore configuré	

Solution de contournement CRL pour les problèmes d'accessibilité

Si le point de distribution CRL de votre autorité de certification n'est pas accessible depuis Internet (comme c'est souvent le cas dans les travaux pratiques), utilisez une autorité de certification auto-signée sans exigence CRL :

```

powershell
# Create self-signed CA
$rootCA = New-SelfSignedCertificate `
-Subject "CN=CIQ-Test-CA" `
-CertStoreLocation "Cert:" `
-KeyUsage CertSign, CRLSign `
-KeyLength 2048 `
-NotAfter (Get-Date).AddYears(5) `
-TextExtension @("2.5.29.19={text}ca=TRUE")
# Create user cert signed by the CA
$userCert = New-SelfSignedCertificate `
-Subject "CN=

" `
-CertStoreLocation "Cert:" `
-Signer $rootCA `
-KeyUsage DigitalSignature `
-KeyLength 2048 `
-NotAfter (Get-Date).AddYears(2) `
-TextExtension @(
"2.5.29.37={text}1.3.6.1.5.5.7.3.2",
"2.5.29.17={text}upn=

&email=

"
)

```

Téléchargez uniquement le certificat CA racine vers l'ID d'entrée. Étant donné qu'il est auto-signé sans CDP (Cisco Discovery Protocol), Entra ID ne tente pas de valider la liste de révocation de certificats.

Liste de contrôle de configuration

Cette section décrit une liste de contrôle de configuration complète pour la configuration de VA avec l'application SAML Microsoft Entra ID et le CBA facultatif.

Configuration de l'application SAML ID supplémentaire

- Créer une application d'entreprise (hors galerie) dans l'ID d'entrée
- Configurez une configuration SAML de base en entrant manuellement les métadonnées SP
- Configurer les attributs et les revendications (y compris l'e-mail, le nom et les groupes avec user.assignedroles)
- Créer des rôles d'application dans App Registration
- Affecter des utilisateurs à des rôles d'application
- Télécharger le fichier XML des métadonnées de fédération

Configuration de Cisco IQ

- Ajouter un IDP dans Cisco IQ en téléchargeant les métadonnées Entra ID
- Configurez le mappage des rôles pour mapper les valeurs de rôle d'application aux rôles système Cisco IQ
- Vérifier que la connexion par mot de passe fonctionne de bout en bout
- Vérifier que les groupes sont correctement extraits dans les journaux

Authentification basée sur certificat (facultatif)

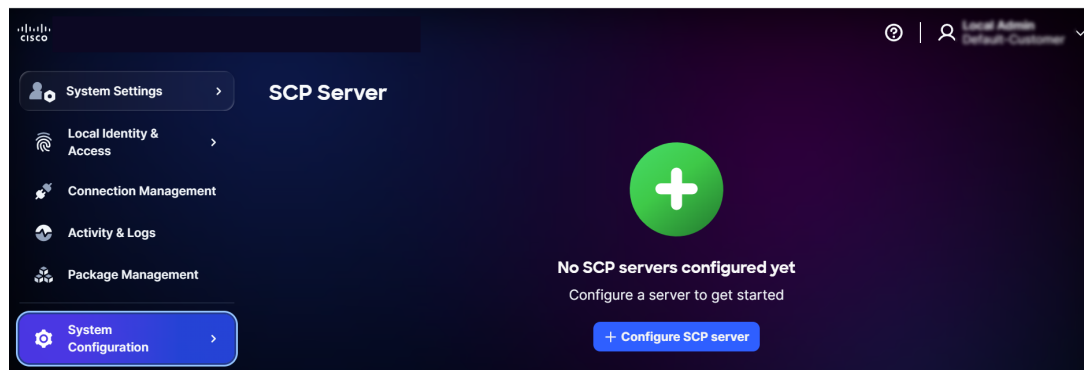
- Créer un modèle de certificat sur AD CS avec l'EKU d'authentification client
- Émettez un certificat utilisateur avec un UPN correspondant à l'utilisateur Entra ID
- Exporter un certificat utilisateur en tant que fichier PFX et l'installer sur l'ordinateur client
- Approuver le certificat CA sur l'ordinateur client
- Téléchargez le certificat racine CA vers l'ID d'entrée sous Protection > Autorités de certification
- Activer le CBA dans les méthodes d'authentification
- Configurer la liaison de nom d'utilisateur (PrincipalName et userPrincipalName)
- Vérifier que la connexion CBA fonctionne de bout en bout

Ajout du serveur SCP

Un serveur SCP est une condition préalable à l'importation de fichiers de mise à niveau essentiels pour l'ajout, la mise à niveau ou la réparation de l'installation Cisco IQ.

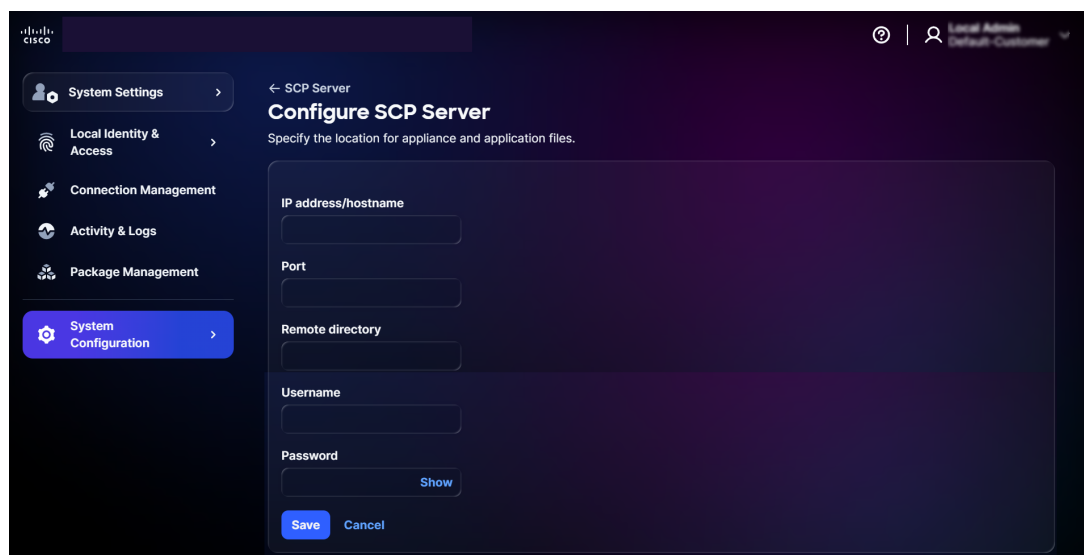
Pour ajouter un serveur SCP :

1. Dans Paramètres système, choisissez Configuration système > Serveur SCP. La page SCP Server s'affiche.



Page d'accueil du serveur SCP

2. Cliquez sur Configurer le serveur SCP. La page Configure SCP Server s'affiche.



Configurer le serveur SCP

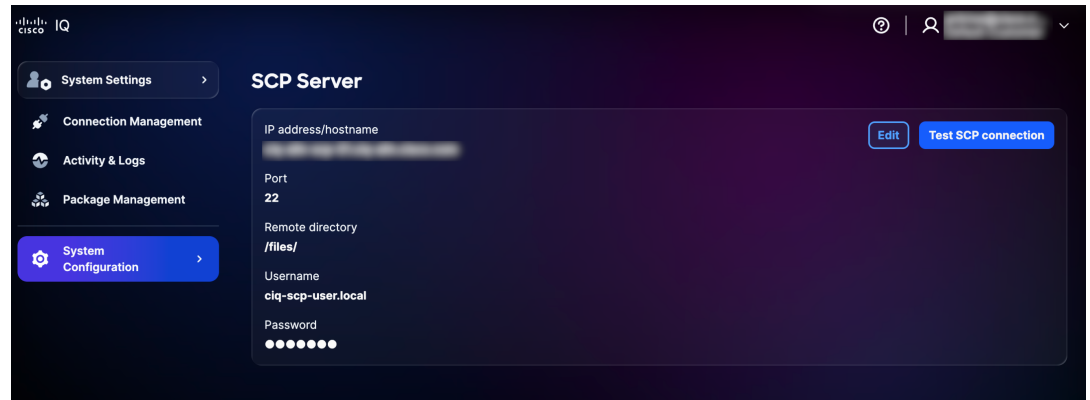
3. Saisissez une adresse IP/un nom d'hôte.
4. Saisissez un port.
5. Entrez un répertoire distant.

6. Saisissez un nom d'utilisateur.
7. Saisissez un mot de passe.
8. Cliquez sur Save. Une confirmation s'affiche.

Modifier un serveur SCP existant

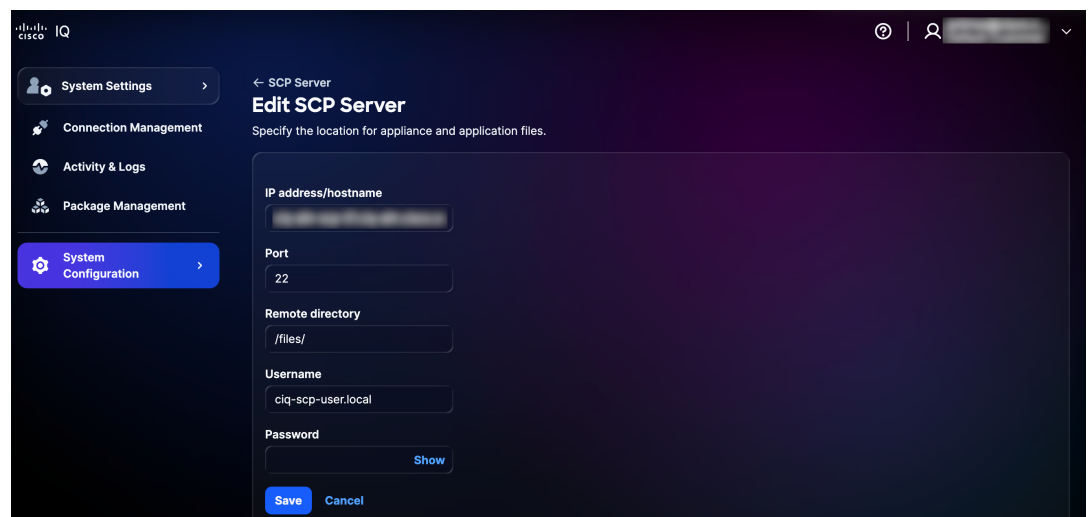
Pour modifier un serveur SCP existant :

1. Accédez à la page SCP Server.



Serveur SCP ajouté

2. Cliquez sur Edit du serveur SCP existant souhaité.



Modification du serveur SCP

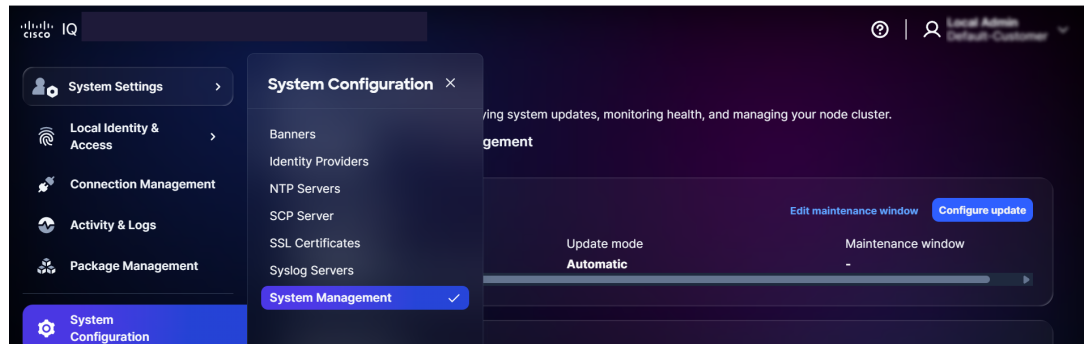
3. Modifiez les détails selon vos besoins.
4. Cliquez sur Save.

Gestion du système

Vous pouvez effectuer une mise à niveau vers la dernière version de Cisco IQ VA via l'interface utilisateur. Vous pouvez également vérifier à partir de la page Cisco IQ Data Connectors.

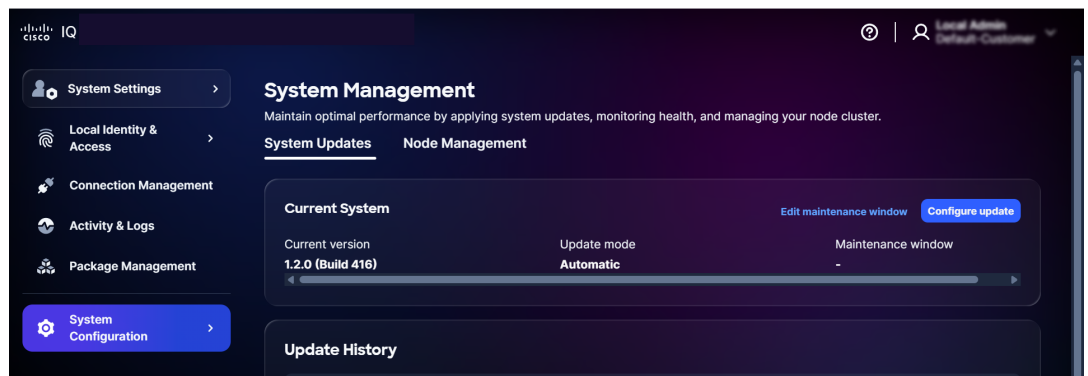
Replanifier la mise à jour système

Pour replanifier la mise à jour du système :



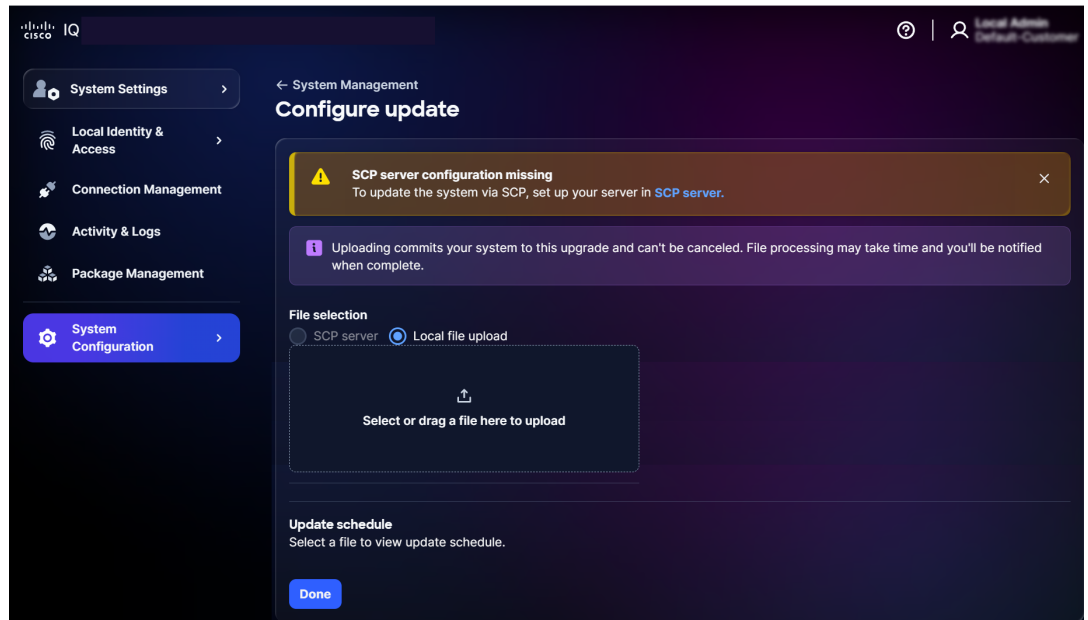
Gestion du système

1. Dans Paramètres système, choisissez Configuration système > Gestion du système. La page Gestion du système s'affiche. Cette page affiche la version du système en cours d'exécution ; si aucune mise à jour n'a été configurée, la section Historique des mises à jour est vide.



Mise à niveau du système

2. Cliquez sur Configurer la mise à jour. La page Configurer la mise à jour s'affiche.



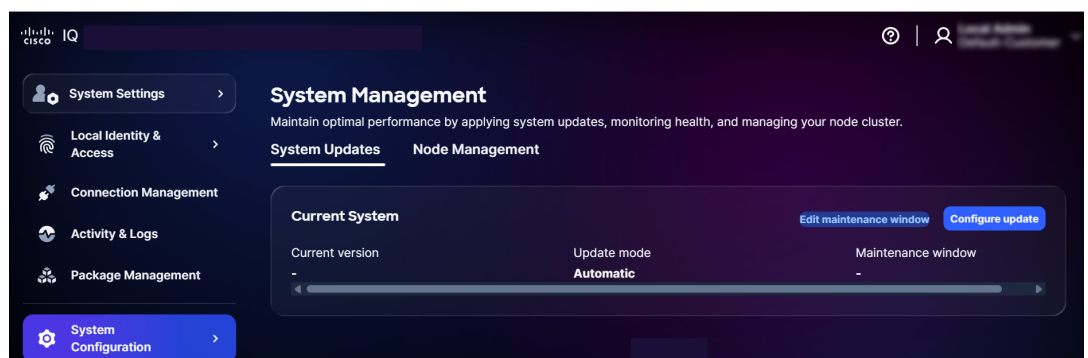
Configurer la mise à niveau

3. Sélectionnez la planification Mettre à jour pour planifier une autre heure.
4. Attendez la fin du téléchargement du fichier ; la durée dépend de la taille du bundle et de la vitesse du réseau.

Confirmez la mise à jour en vérifiant l'icône de coche affichée sous la colonne Update Status.

Modification des planifications de mise à niveau système

Vous pouvez créer une planification personnalisée pour les mises à niveau du système. Si une planification personnalisée est configurée, les mises à niveau ont lieu à des dates définies par l'utilisateur, à condition qu'elles restent dans le délai de grâce maximal. Pour créer une planification de mise à niveau du système :



Modifier la maintenance

1. Dans la section Système actuel de la page Gestion du système, cliquez sur Modifier la fenêtre de maintenance.

Edit maintenance window

Select the day and time to reserve for future updates. If an update can't be completed during the maintenance window, it will occur on the last day of the grace period.

Day

Time

hh:mm

⌚

IST

Cancel

Save

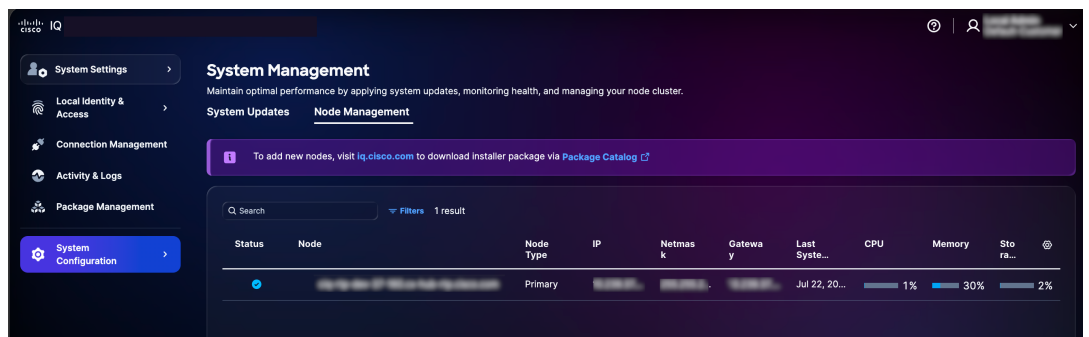
Modifier la fenêtre de maintenance

2. Choisissez une option dans les listes déroulantes Jour et Heure.
3. Cliquez sur Enregistrer. La fenêtre de maintenance a été planifiée avec succès. La mise à jour est déclenchée en fonction du calendrier affiché.

 Remarque : Si aucun calendrier de mise à niveau n'est configuré, le système utilise par défaut des périodes de grâce de deux (2) semaines pour les mises à niveau sans redémarrage et de quatre (4) semaines pour les mises à niveau nécessitant un redémarrage. Après ces périodes de grâce, les mises à jour doivent être effectuées manuellement. En cas d'échec de la mise à niveau, le système effectue jusqu'à deux (2) tentatives automatiques. Une troisième tentative est planifiée, mais elle nécessite un lancement manuel.

Gestion des noeuds

1. Accédez à System Configuration > System Management > Node Management pour afficher et gérer les noeuds dans votre cluster.



The screenshot shows the 'System Management' page in Cisco IQ. The left sidebar contains navigation links: System Settings, Local Identity & Access, Connection Management, Activity & Logs, Package Management, and System Configuration (highlighted). The main content area is titled 'System Management' and includes a sub-header 'Node Management'. A message bar states: 'To add new nodes, visit [iq.cisco.com](https://www.cisco.com) to download installer package via Package Catalog'. Below this is a table with columns: Status, Node, Node Type, IP, Netmask, Gateway, Last System Update, CPU, Memory, and Storage. The table shows one node with a status of 'Online' and a node type of 'Primary'.

Status	Node	Node Type	IP	Netmask	Gateway	Last System Update	CPU	Memory	Storage
Online	10.10.10.10	Primary	10.10.10.10	255.255.255.0	10.10.10.1	Jul 22, 2023	1%	30%	2%

Gestion des noeuds

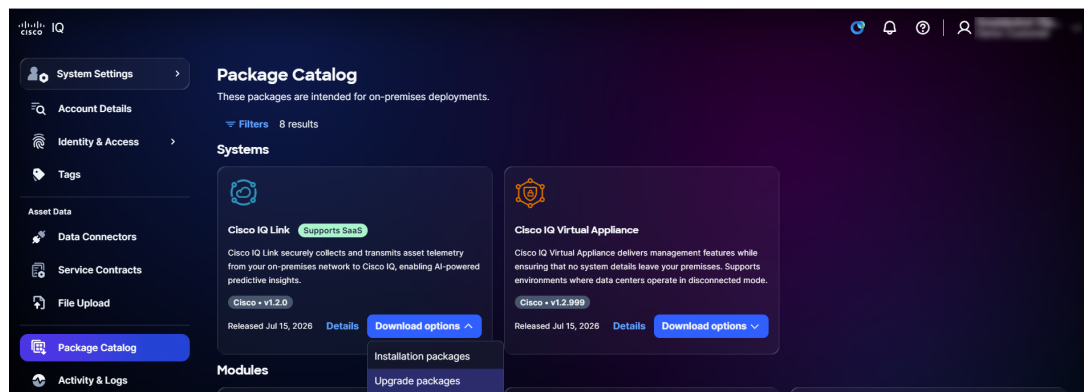
2. La liste des noeuds affiche l'état, le nom d'hôte, le type de noeud, l'adresse IP, le masque de réseau, la passerelle et l'heure de la dernière synchronisation de chaque noeud.

 Remarque : Une coche bleue dans la colonne Status indique que le noeud est actif.

Mise à niveau manuelle du système

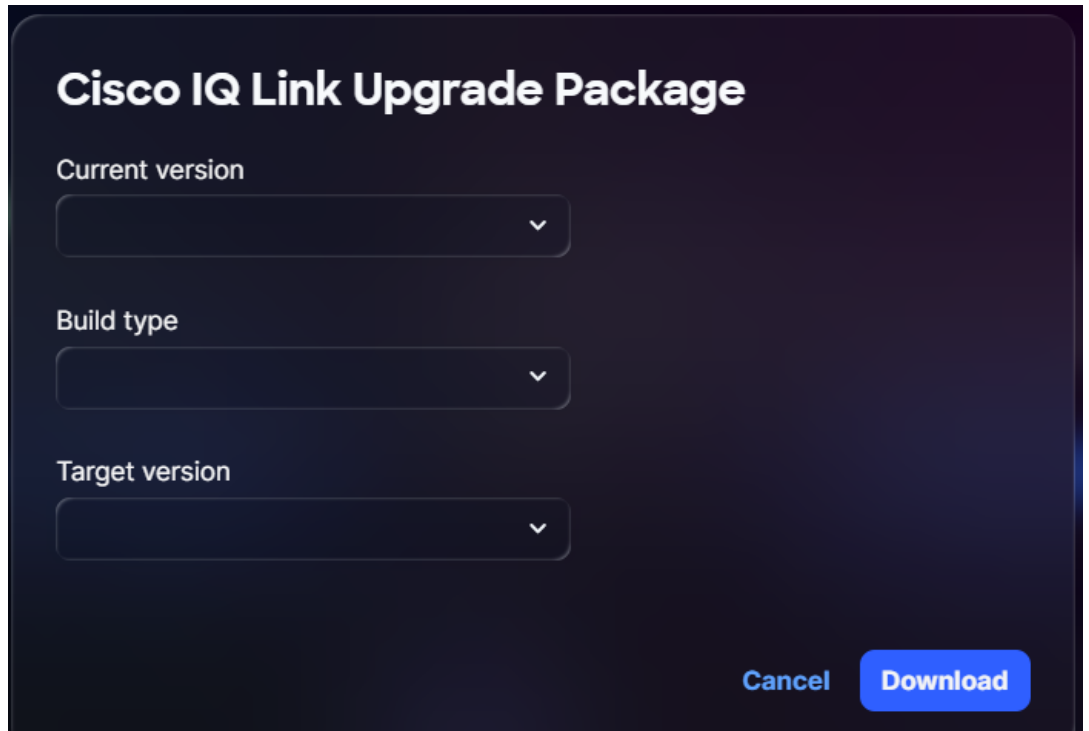
Dans les cas où la distribution automatique à partir de Cisco IQ SaaS n'est pas disponible ou est retardée, vous pouvez effectuer manuellement une mise à niveau du système en téléchargeant le bundle de mise à niveau directement à partir de Cisco IQ SaaS. Pour mettre à niveau manuellement le système :

1. Connectez-vous à [Cisco IQ SaaS](#).
2. Accédez à Accueil > Paramètres système > Catalogue de packages.



Catalogue de logiciels

3. Dans la carte Cisco IQ Virtual Appliance, cliquez sur Download options > Upgrade packages.

A dark-themed dialog box titled "Cisco IQ Link Upgrade Package". It contains three dropdown menus: "Current version", "Build type", and "Target version". At the bottom right, there are two buttons: "Cancel" and "Download".

Cisco IQ Link Upgrade Package

Current version

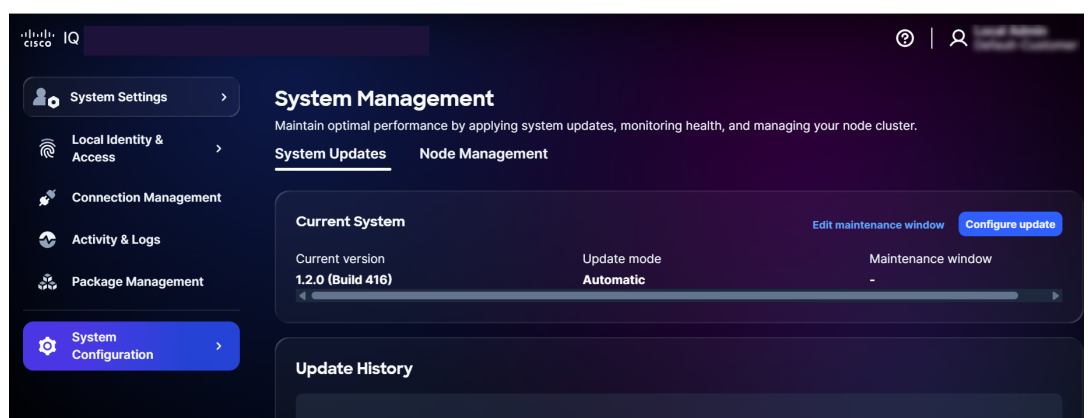
Build type

Target version

Cancel Download

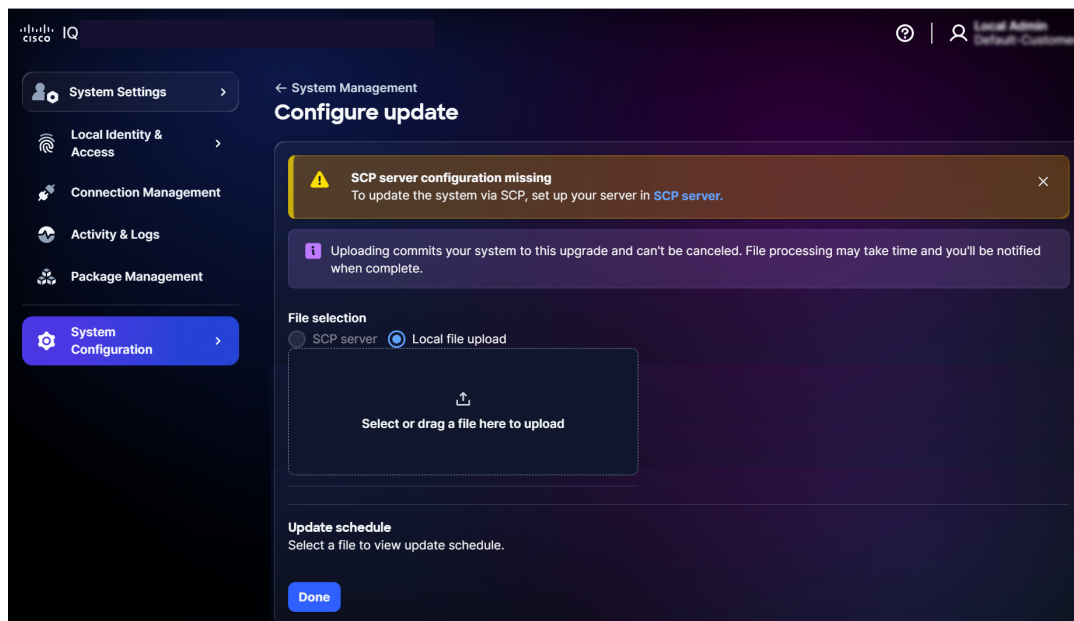
Package de mise à niveau

4. Sélectionnez la version actuelle dans la liste déroulante.
5. Sélectionnez le type de build dans la liste déroulante.
6. Sélectionnez la version cible dans la liste déroulante.
7. Cliquez sur Télécharger. Le bundle de mise à niveau est téléchargé.
8. Accédez à Cisco IQ VA.
9. Dans Paramètres système, choisissez Configuration système > Gestion du système.



Configurer la mise à jour

10. Cliquez sur Configurer la mise à jour.



Téléchargement de fichier local

11. Activez la case d'option Téléchargement de fichier local.
12. Sélectionnez ou faites glisser le fichier de bundle de mise à niveau téléchargé dans le champ de téléchargement.
13. Attendez la fin du téléchargement du fichier ; la durée dépend de la taille du bundle et de la vitesse du réseau.

Configuration des certificats SSL

Un certificat auto-signé par défaut est préinstallé et activé dans Cisco IQ, mais vous pouvez éventuellement télécharger des certificats SSL personnalisés. Lorsqu'un certificat SSL personnalisé est activé, il est utilisé pour les connexions HTTPS ; si le certificat est désactivé ou supprimé, le système revient automatiquement au certificat par défaut. Le certificat SSL par défaut ne peut pas être modifié ou supprimé.

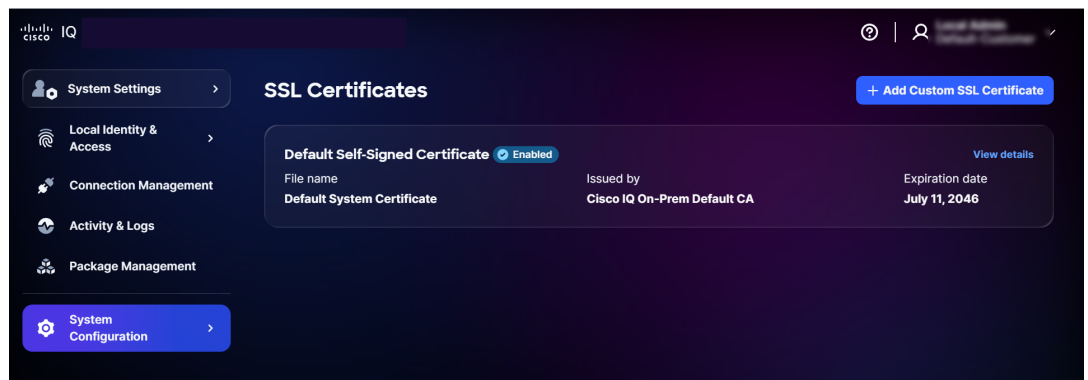


Remarque : Le certificat doit avoir au moins 90 jours de validité restants. Un certificat est considéré comme « proche de l'expiration » lorsqu'il lui reste moins de 90 jours avant son expiration. Après avoir ajouté, modifié ou supprimé un certificat SSL, vous devez télécharger le nouveau certificat SSL comme indiqué dans [Completing SLO Configuration](#) for the Okta IDP or the ADFS IDP.

Ajout d'un certificat SSL personnalisé

Pour ajouter un certificat SSL personnalisé :

1. Dans Paramètres système, choisissez Configuration système > Certificats SSL. La page SSL Certificates s'affiche et répertorie tous les certificats SSL de votre système.

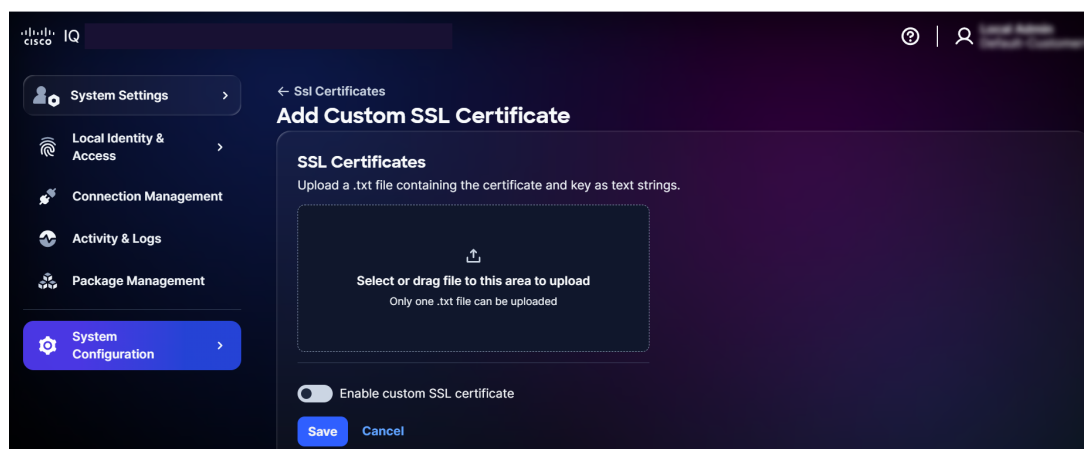


Ajout du certificat SSL

2. Cliquez sur Ajouter un certificat SSL personnalisé.



Remarque : Téléchargez un fichier .txt qui inclut le certificat et la clé codés par messagerie Privacy-Enhanced sous forme de chaînes de texte. Un seul fichier .txt peut être téléchargé à la fois. Le fichier doit contenir à la fois le certificat et la clé privée.



Télécharger le certificat SSL

3. Faites glisser et déposez ou téléchargez le certificat SSL personnalisé sous la section Certificat SSL.
4. Activez le bouton bascule Activer le certificat SSL personnalisé.

Enable Certificate?

Enabling custom SSL certificate will disable the default self-signed certificate.

Cancel

Enable certificate

Activer le certificat



Remarque : Maintenez la touche OFF désactivée si vous souhaitez télécharger le certificat sans l'activer immédiatement.

5. Cliquez sur Activer le certificat.

6. Cliquez sur Save.

Le certificat SSL personnalisé est activé et actif. Le certificat système par défaut est automatiquement désactivé.

Modification du certificat SSL personnalisé

Vous pouvez modifier le certificat SSL personnalisé pour télécharger un nouveau certificat ou désactiver le certificat actuellement activé. Pour modifier :

1. Accédez au certificat SSL personnalisé souhaité.

2. Cliquez sur l'icône Autres options > Modifier. La page Edit SSL Certificate s'affiche.

3. Modifiez les détails du certificat selon les besoins.

4. Cliquez sur Save.

Suppression du certificat SSL personnalisé

Avertissement : Un certificat SSL personnalisé peut être supprimé à tout moment, mais il s'agit d'une action irréversible ; vous pouvez télécharger un nouveau certificat personnalisé à tout moment après la suppression.

Pour supprimer :

1. Accédez au certificat SSL personnel souhaité.

2. Cliquez sur l'icône Autres options > Supprimer.
3. Cliquez sur Supprimer le certificat. Le certificat personnalisé est supprimé et le certificat par défaut est automatiquement réactivé.

Configuration du serveur Syslog

Les utilisateurs dotés du rôle Administrateur de compte peuvent configurer des serveurs syslog externes pour exporter les journaux système. Vous pouvez configurer jusqu'à deux (2) serveurs syslog.

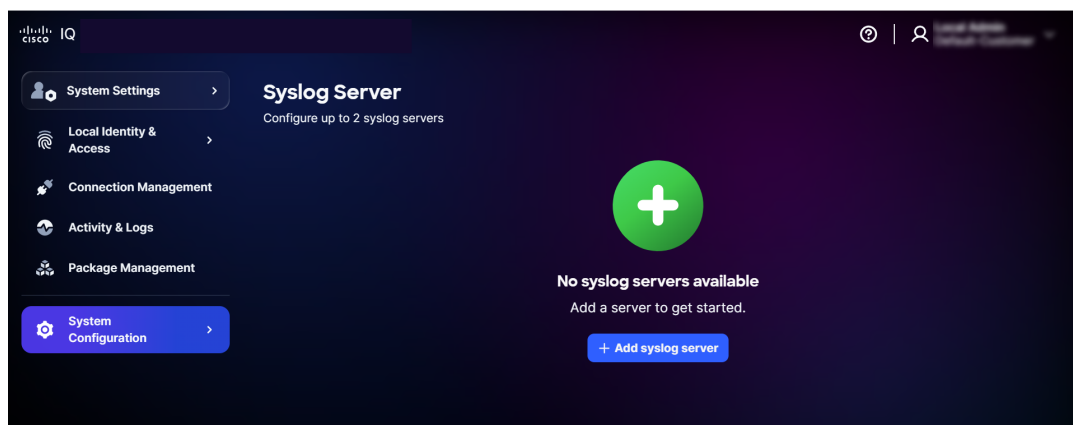


Remarque : Le serveur Syslog doit être spécifié en tant qu'adresse IP et non en tant que nom de domaine complet (FQDN).

Ajout du serveur Syslog

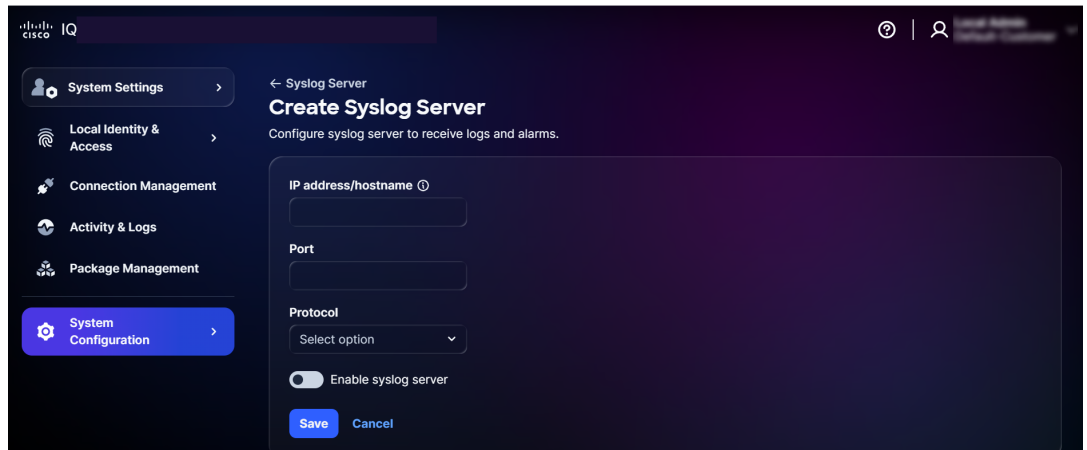
Pour ajouter un serveur Syslog :

1. Dans Paramètres système, choisissez Configuration système > Serveur Syslog. La page Syslog Server s'affiche.



Ajouter un serveur Syslog

2. Cliquez sur Add syslog server. La page Créer un serveur Syslog s'affiche.



Créer un serveur Syslog

3. Saisissez l'adresse IP/le nom d'hôte.
4. Saisissez Port.
5. Sélectionnez le protocole applicable dans la liste déroulante Protocol (par exemple, UDP, TCP).
6. Activez le bouton bascule Activer le serveur Syslog.
7. Cliquez sur Save. Une confirmation s'affiche et le nouveau serveur Syslog ajouté s'affiche sur la page d'accueil du serveur Syslog.

Modification du serveur Syslog configuré

Pour modifier un serveur syslog configuré :

1. Accédez au serveur Syslog souhaité.
2. Cliquez sur l'icône Autres options > Modifier. La page Edit Syslog Server s'affiche.
3. Modifiez les détails ou désactivez le bouton Enable syslog server, selon les besoins.
4. Cliquez sur Save.

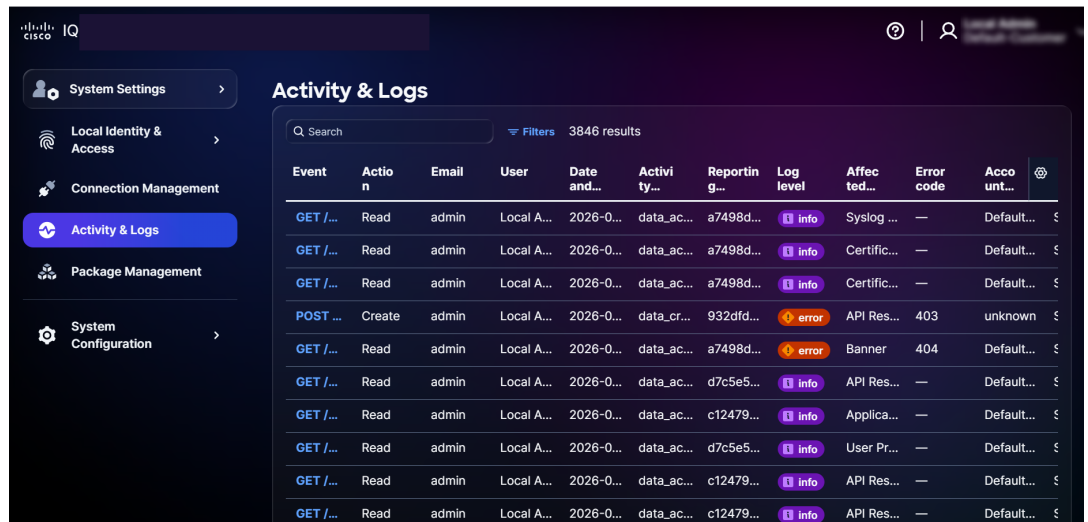
Suppression du serveur Syslog configuré

Pour supprimer un serveur syslog configuré :

1. Accédez au serveur Syslog souhaité.
2. Cliquez sur l'icône Autres options > Supprimer. Une confirmation s'affiche.
3. Cliquez sur Delete syslog server.

Activité et journaux

Les activités et les journaux fournissent un enregistrement détaillé des actions et des modifications des utilisateurs dans Cisco IQ, permettant aux administrateurs de comptes de suivre les activités des utilisateurs et de maintenir la transparence.



Event	Action	Email	User	Date and time	Activity type	Reporting	Log level	Affected resource	Error code	Account
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Syslog ...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Certific...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Certific...	—	Default...
POST ...	Create	admin	Local A...	2026-0...	data_cr...	932dfd...	error	API Res...	403	unknown
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	error	Banner	404	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	d7c5e5...	info	API Res...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	Applica...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	d7c5e5...	info	User Pr...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	API Res...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	API Res...	—	Default...

Activité et journaux

Pour afficher l'activité et les journaux, sélectionnez Activité et journaux dans le menu Paramètres système.

Exercice et journaux :

- Enregistre toutes les opérations API au niveau de la passerelle
- Prise en charge des filtres, de la pagination et des fonctions de recherche pour faciliter la recherche et la gestion des informations

Les options de filtre suivantes sont disponibles :

- Dernière date de consignation : Filtre les journaux dans une plage de temps spécifique
- Niveau de journalisation : Filtre les journaux par gravité (par exemple, erreur, avertissement et informations)
- Type d'activité : Filtre les journaux par type d'activité du système
- Code d'erreur : Filtres pour un code d'erreur spécifique

Bannières

Les administrateurs de comptes peuvent configurer des bannières à

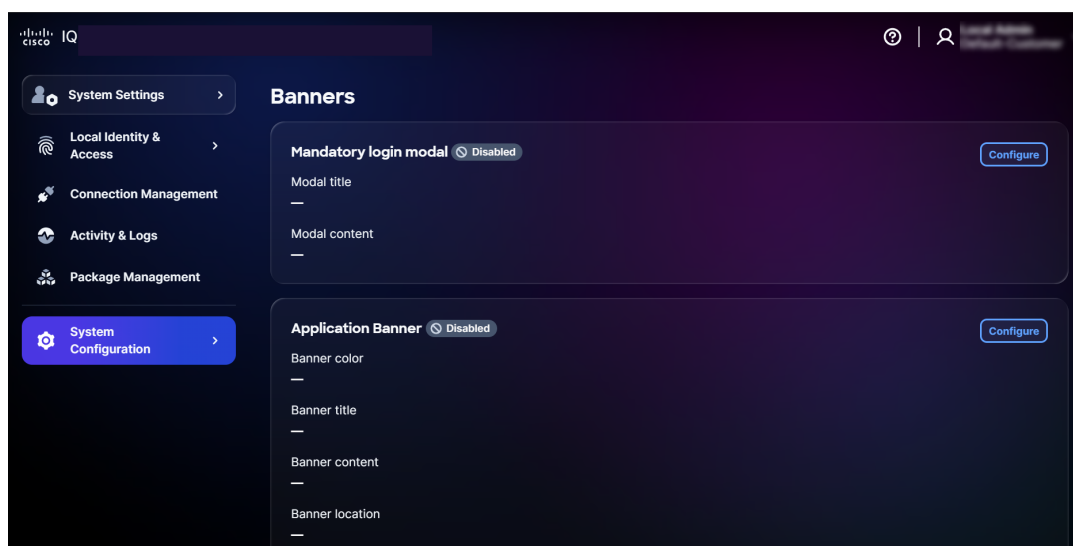
l'échelle du système pour répondre aux normes de sécurité et de conformité.

- Connexion modale obligatoire : Vous devez accuser réception de la bannière obligatoire avant de passer à l'écran de connexion.
- Bannière Application : Il s'agit de bannières personnalisées qui s'affichent dans l'application après une authentification réussie.

Configuration des bannières modales de connexion obligatoire

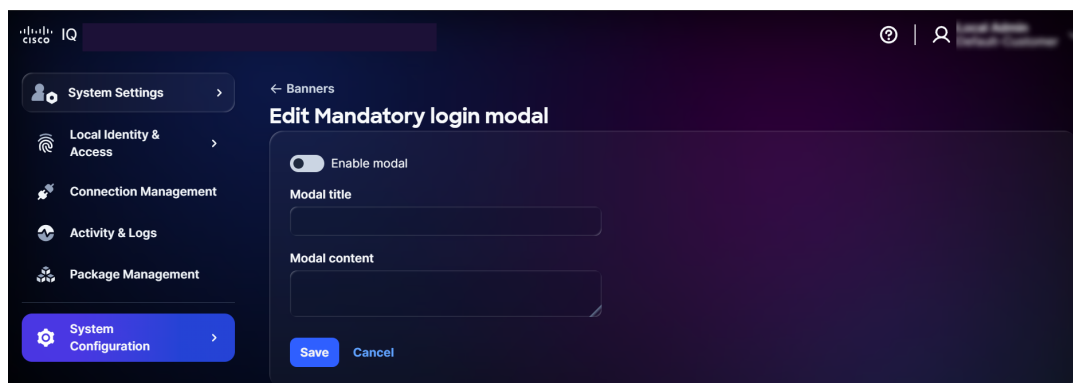
Pour configurer une bannière obligatoire :

1. Dans Paramètres système, sélectionnez Configuration système > Bannières. La page Bannières s'affiche.



Configurer la bannière obligatoire

2. Cliquez sur Configure dans le mode Connexion obligatoire. La page Edit Mandatory login modal s'affiche.



Modifier la bannière modale de connexion obligatoire

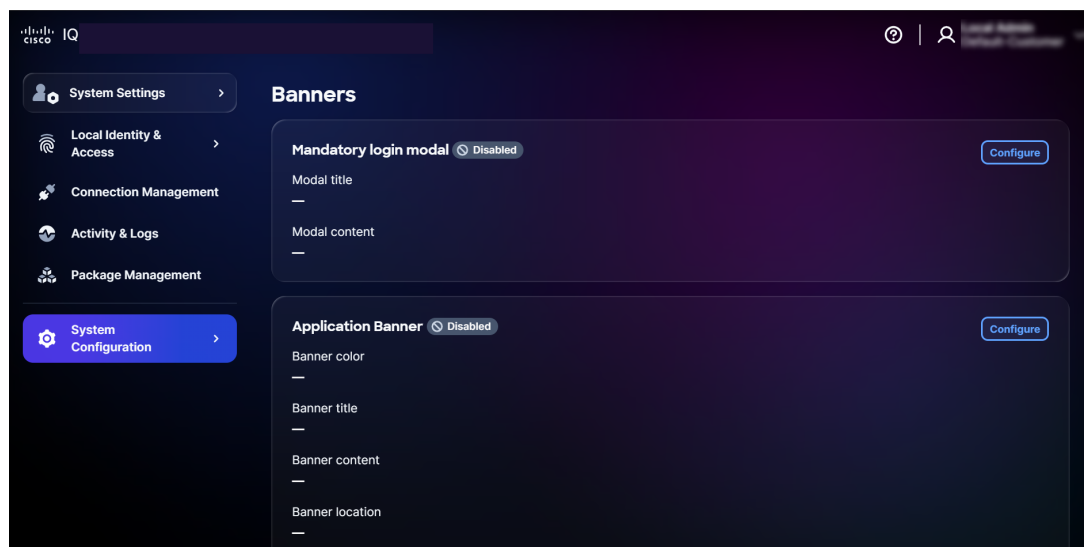
3. Cliquez sur le bouton bascule pour activer ou désactiver la bannière.

4. Saisissez le titre Modal.
5. Saisissez le contenu modal.
6. Cliquez sur Save. Le mode de connexion obligatoire est enregistré.

Configuration des bannières des applications

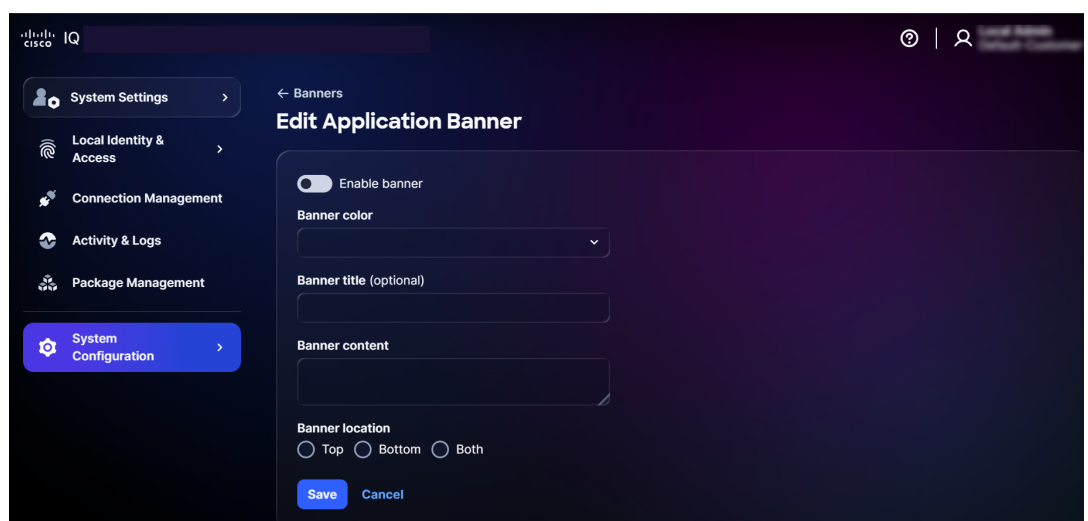
Pour configurer une bannière d'application :

1. Dans Paramètres système, sélectionnez Configuration système > Bannières. La page Bannières s'affiche.



Configurer la bannière

2. Cliquez sur Configurer dans la bannière d'application. La page Modifier la bannière d'application s'affiche.



Modifier la bannière d'application

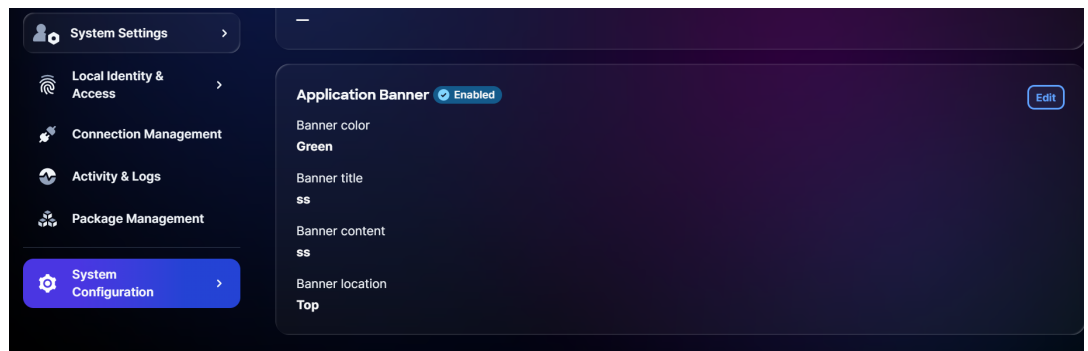
3. Cliquez sur le bouton bascule pour activer ou désactiver la bannière.

4. Choisissez une couleur de bannière.
5. Saisissez le titre de la bannière.
6. Saisissez le contenu de la bannière.
7. Choisissez un emplacement de bannière.
8. Cliquez sur Save. La bannière s'affiche dans l'application.

Modification des bannières

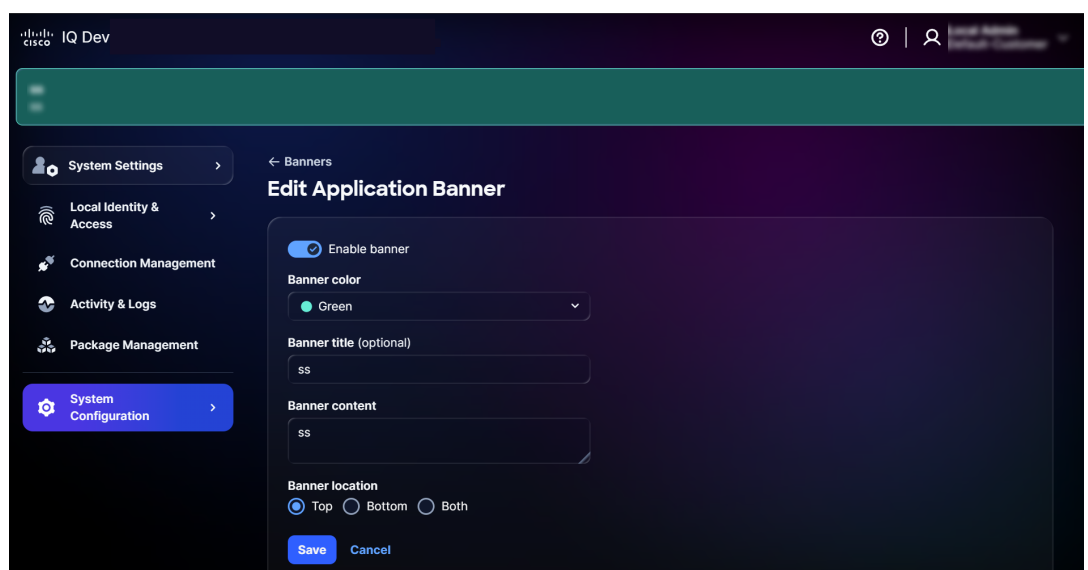
Pour modifier une bannière :

1. Dans Paramètres système, sélectionnez Configuration système > Bannières. La page Bannières s'affiche.



Modifier les bannières

2. Cliquez sur Modifier. La page Modifier la bannière d'application s'affiche.



Modifier la bannière d'application

3. Modifiez les détails souhaités.

4. Cliquez sur le bouton bascule pour activer ou désactiver la bannière.
5. Cliquez sur Save.

Dépannage

Vous pouvez collecter des fichiers de diagnostic et de journalisation à partir du système Cisco IQ et les transférer en toute sécurité vers un serveur SCP. Ces fichiers peuvent être partagés avec l'équipe d'assistance lors du signalement de problèmes afin de fournir un contexte utile et d'aider au dépannage.

Pour collecter les fichiers de diagnostic et les fichiers journaux :

1. Connectez-vous à Cisco IQ.



```

Cisco IQ

Navigation Main Menu

SYSTEM STATUS
Cisco IQ On-Prem   Installed

CONFIGURATION SETTINGS
IP Address/Mask
Gateway IP
DNS List
Search Domain
NTP List
Hostname

MAIN MENU
[1] Configure Network Settings DISABLED because the platform is installed
[2] Configure System Orchestrator DISABLED because the platform is installed
[3] System Diagnostics
[4] Help
[5] About
[q] Quit
```

Menu principal

2. Dans le menu principal de Cisco IQ, saisissez « 3 » et appuyez sur Entrée pour sélectionner System Diagnostics.

```
Navigation Main Menu > System Diagnostics

Please provide the following server connection details:

Enter SCP/SFTP Server Address: 
Valid IP address ✓
Enter SCP/SFTP Server Port (e.g. 22): 
Valid port ✓
Enter SCP/SFTP Server Path (e.g. /var/log/support/): 
Valid server path ✓

PROTOCOL SELECTION
[1] SCP (Secure Copy Protocol) - Default
[2] SFTP (SSH File Transfer Protocol)

Select protocol [1]/[2] (default: SCP): 1
scp
✓ Selected protocol: SCP
Enter Username: 
Valid username ✓
Enter Password:

Continue with System Diagnostics? ([c]ontinue/[B]ack):
```

Diagnostics du système

3. Saisissez l'adresse du serveur SCP/SFTP.
4. Saisissez le port du serveur SCP/SFTP.
5. Saisissez le chemin du serveur SCP/SFTP.
6. Sélectionnez un protocole.
7. Saisissez le nom d'utilisateur.
8. Entrez le mot de passe.
9. Entrez « C » et appuyez sur Entrée pour poursuivre les diagnostics du système.



Navigation `Main Menu` > `System Diagnostics`

```
Checking Reachability ..... ✓
Collecting System Info ..... ✓
Collecting Kubernetes Info ..... ✓
Collecting Logs ..... ✓
Preparing System Diagnostics Bundle ..... ✓
Uploading System Diagnostics Bundle ..... ✓
System Diagnostics Bundle is 'CIQ_Diagnostics_XXXXXX.tar.gz'
System Diagnostics operation completed successfully!
```

Press Enter to return to main menu...

Opération de diagnostic système terminée

Le système lance le processus de diagnostic et exécute les actions suivantes :

- Vérification de l'accessibilité
- Collecte des informations système
- Collecte des informations Kubernetes
- Collecte des journaux
- Préparation du bundle de diagnostics système
- Téléchargement du bundle de diagnostics système

Une fois terminé, un message de confirmation s'affiche pour indiquer le nom de l'offre générée.

Module de support

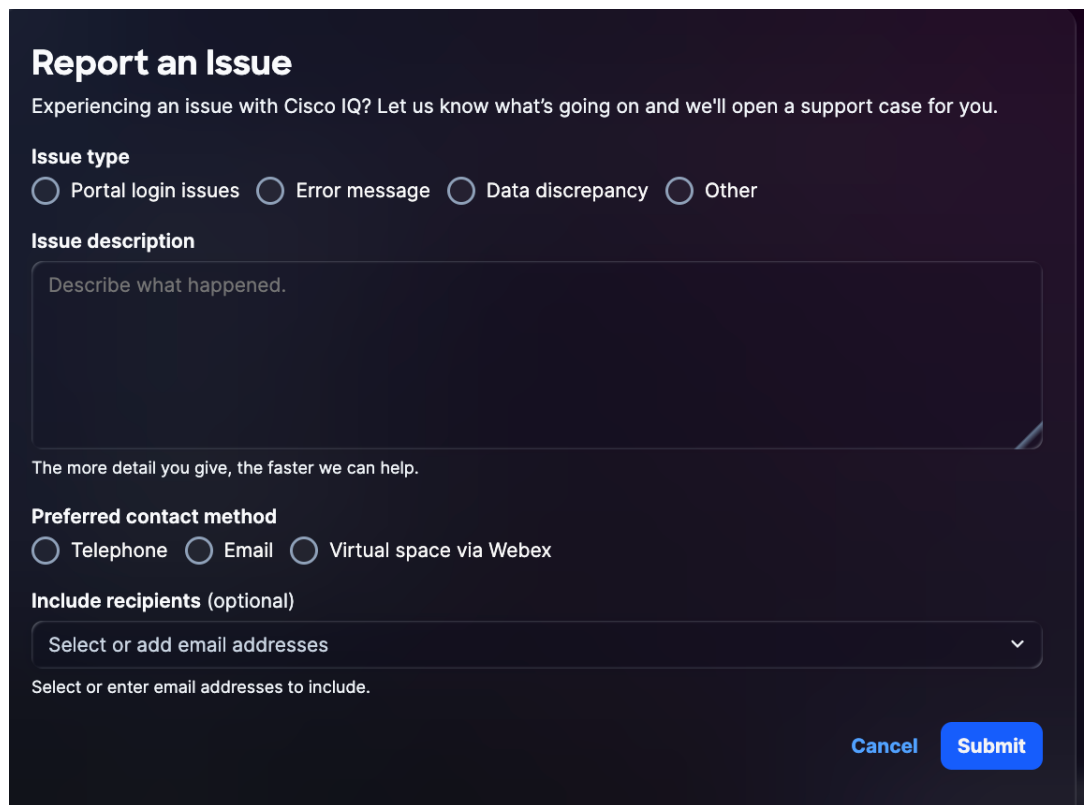
Vous pouvez créer des dossiers d'assistance spécifiques à la VA et aux modules à partir de Cisco IQ SaaS. Le module d'assistance est disponible dans Cisco IQ SaaS et offre une vue consolidée de vos dossiers d'assistance. Il vous permet de filtrer, trier et personnaliser l'affichage de la liste des dossiers, offrant ainsi une visibilité sur les dossiers ouverts et fermés auxquels vous avez droit. Pour plus d'informations sur le module Support dans Cisco IQ SaaS, consultez le [Guide de démarrage de Cisco IQ SaaS](#).

 Remarque : Les clients Cisco IQ VA peuvent accéder à la plupart des fonctionnalités du module d'assistance Cisco IQ SaaS, notamment l'ouverture de dossiers TAC (Technical Assistance Center) relatifs à Cisco IQ VA et à ses modules, ainsi que la création et la gestion de dossiers produits.

Création d'un dossier d'assistance

Vous pouvez créer des cas VA et spécifiques aux modules dans Cisco IQ SaaS. Pour créer un dossier :

1. Connectez-vous à [Cisco IQ \(SaaS\)](#).
2. Cliquez sur l'icône Aide > Signaler un problème. La fenêtre Signaler un problème s'affiche.



Report an Issue

Experiencing an issue with Cisco IQ? Let us know what's going on and we'll open a support case for you.

Issue type

☐ Portal login issues ☐ Error message ☐ Data discrepancy ☐ Other

Issue description

Describe what happened.

The more detail you give, the faster we can help.

Preferred contact method

☐ Telephone ☐ Email ☐ Virtual space via Webex

Include recipients (optional)

Select or add email addresses

Select or enter email addresses to include.

Cancel Submit

Signaler un problème

3. Fournissez les détails requis.
4. Cliquez sur Submit.

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.