Guide d'exploitation de la liaison Cisco IQ version 1.2.0

Introduction

Cisco IQTM vous propose des améliorations et des fonctionnalités conçues pour améliorer la visibilité des ressources, fournir des informations plus intelligentes sur l'ensemble de vos environnements et rationaliser la gestion des dossiers. En outre, des fonctionnalités d'IA telles que l'assistant AI 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 Link collecte et transmet en toute sécurité la télémétrie des ressources de votre réseau sur site vers Cisco IQ, ce qui permet d'obtenir des informations prédictives basées sur l'intelligence artificielle qui vous aident à améliorer la visibilité du réseau, à anticiper les problèmes et à améliorer l'efficacité opérationnelle.

Authentification locale

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

- Nom d'utilisateur par défaut : admin
- Mot de passe par défaut : mot de passe défini lors du processus d'installation de Cisco IQ Link ; pour plus d'informations, reportez-vous au guide Cisco IQ Link Getting Started Guide.
- Contexte du compte par défaut : Client par défaut

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

Définition 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).

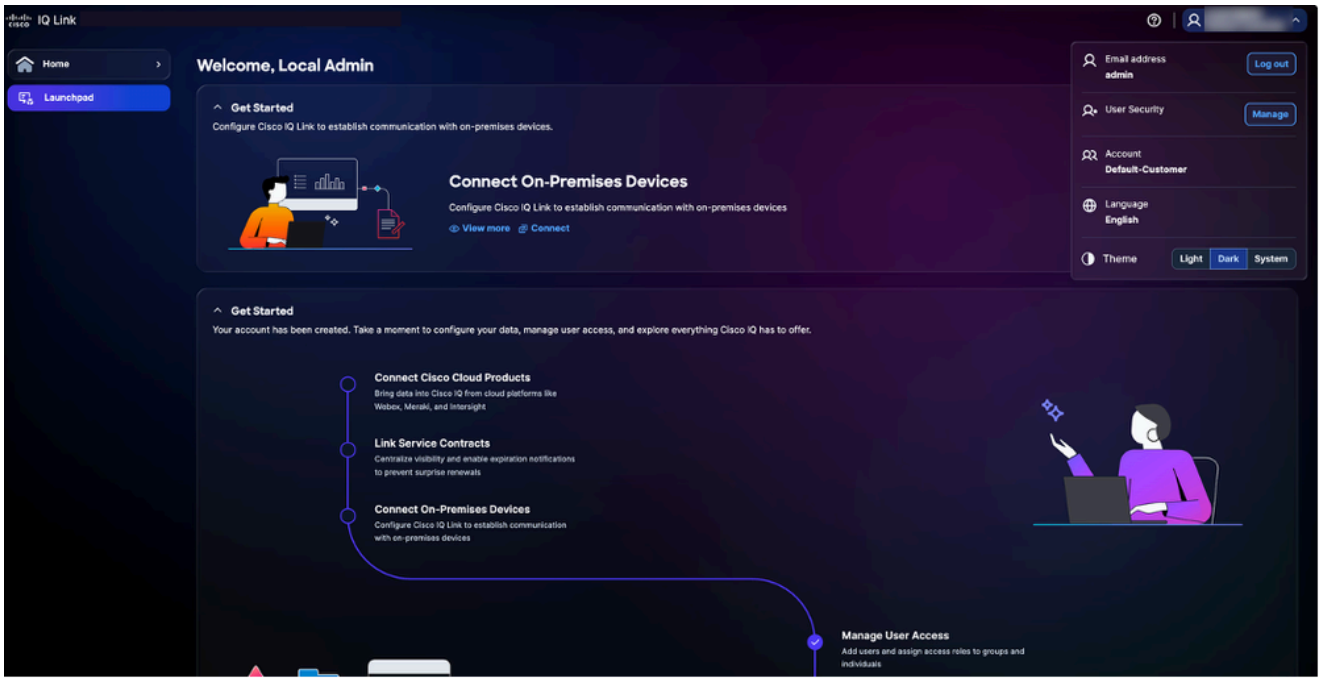
Remarque : Vous avez trois (3) tentatives de saisie du mot de passe correct dans un délai de 15 minutes. Si les trois (3) tentatives échouent, votre compte se verrouille temporairement pendant 30 minutes pour protéger votre sécurité.
Vous ne pouvez pas tenter de vous connecter pendant la période de verrouillage. Le système affiche le message suivant : "Compte verrouillé en raison d'un trop grand nombre de tentatives infructueuses. 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.

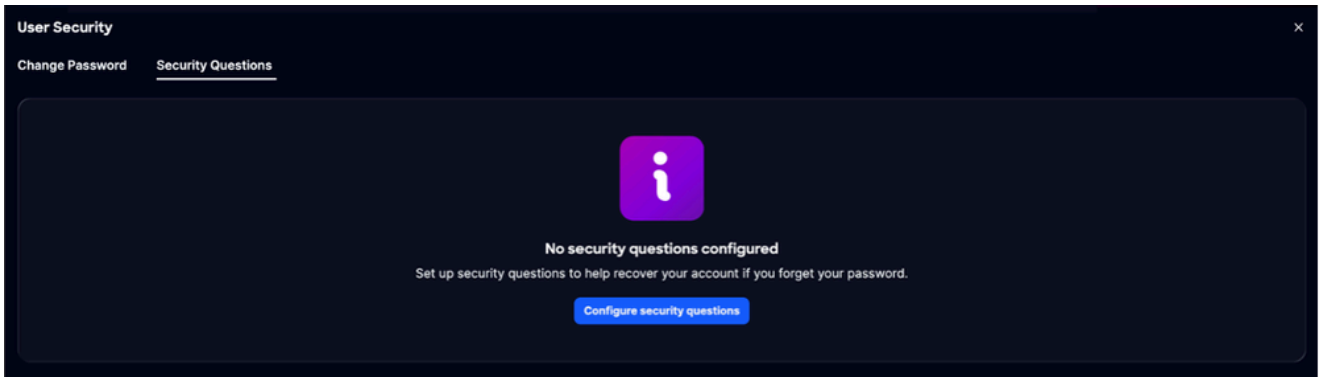


Menu Profil utilisateur

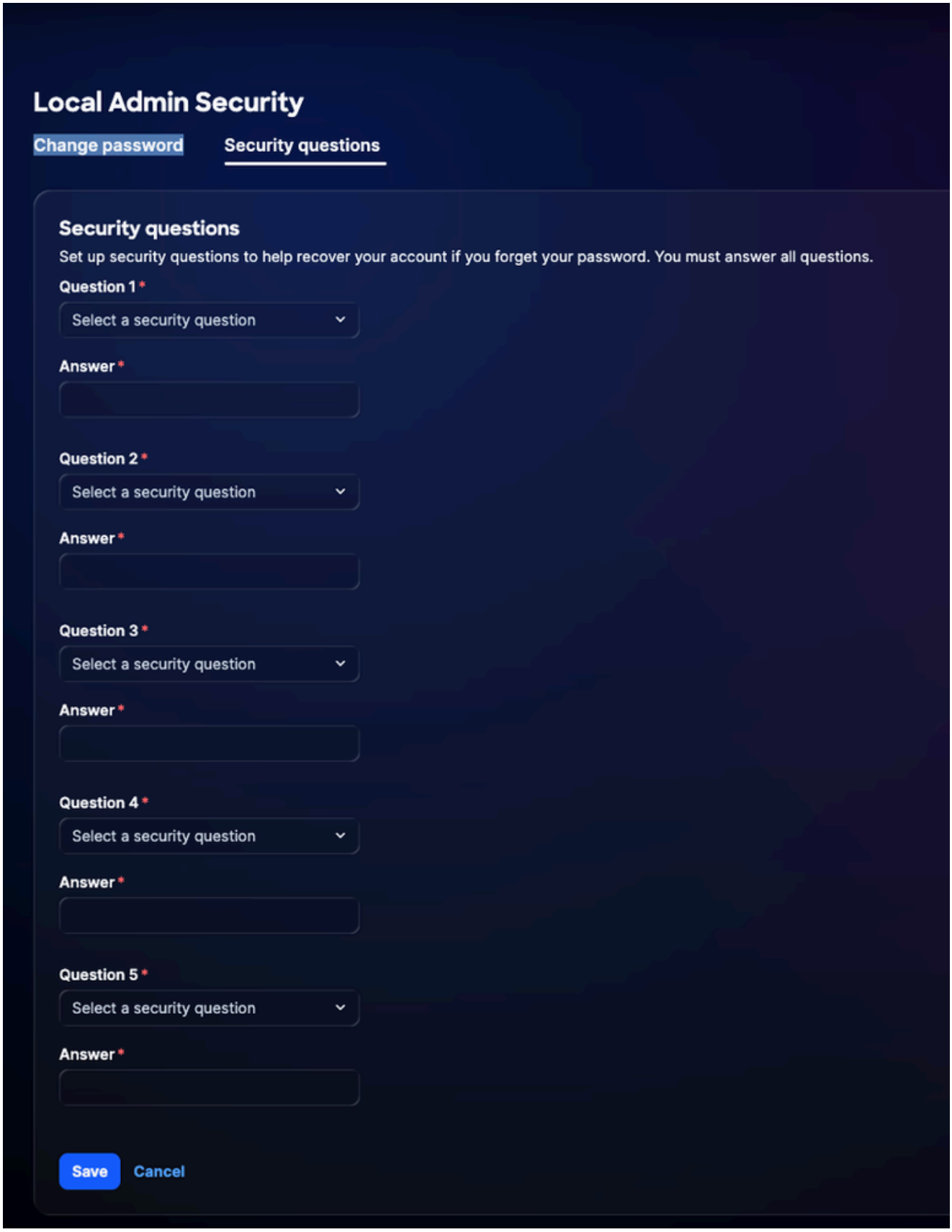
2. Cliquez sur Gérer dans Sécurité utilisateur. La page Sécurité utilisateur s'affiche.

Modifier le mot de passe

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



4. Cliquez sur 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, par exemple, " Smith" et "smith" sont considérés comme identiques.

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 les mots de passe pour 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 après 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

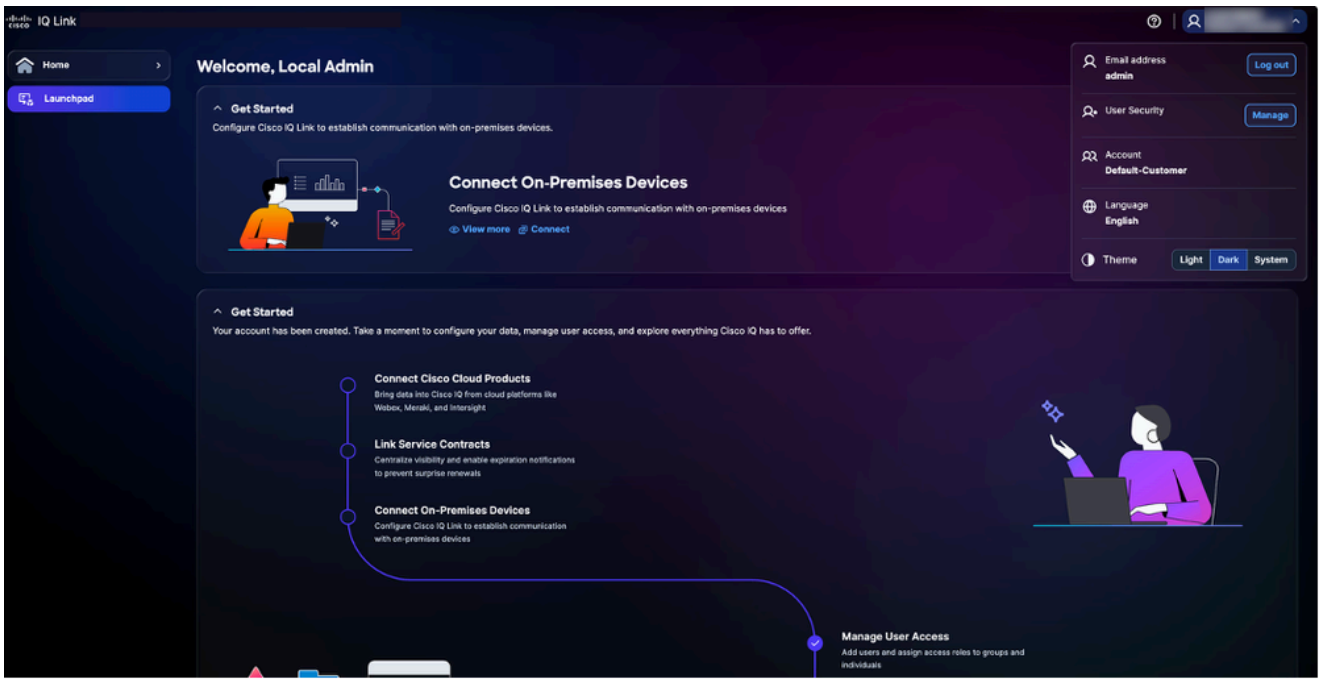
Pour gérer les mots de passe, les conditions suivantes doivent être remplies :

- 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 Link
- Vous connaissez le mot de passe actuel

Modification des mots de passe

Pour modifier un mot de passe :

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



Menu Profil 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.

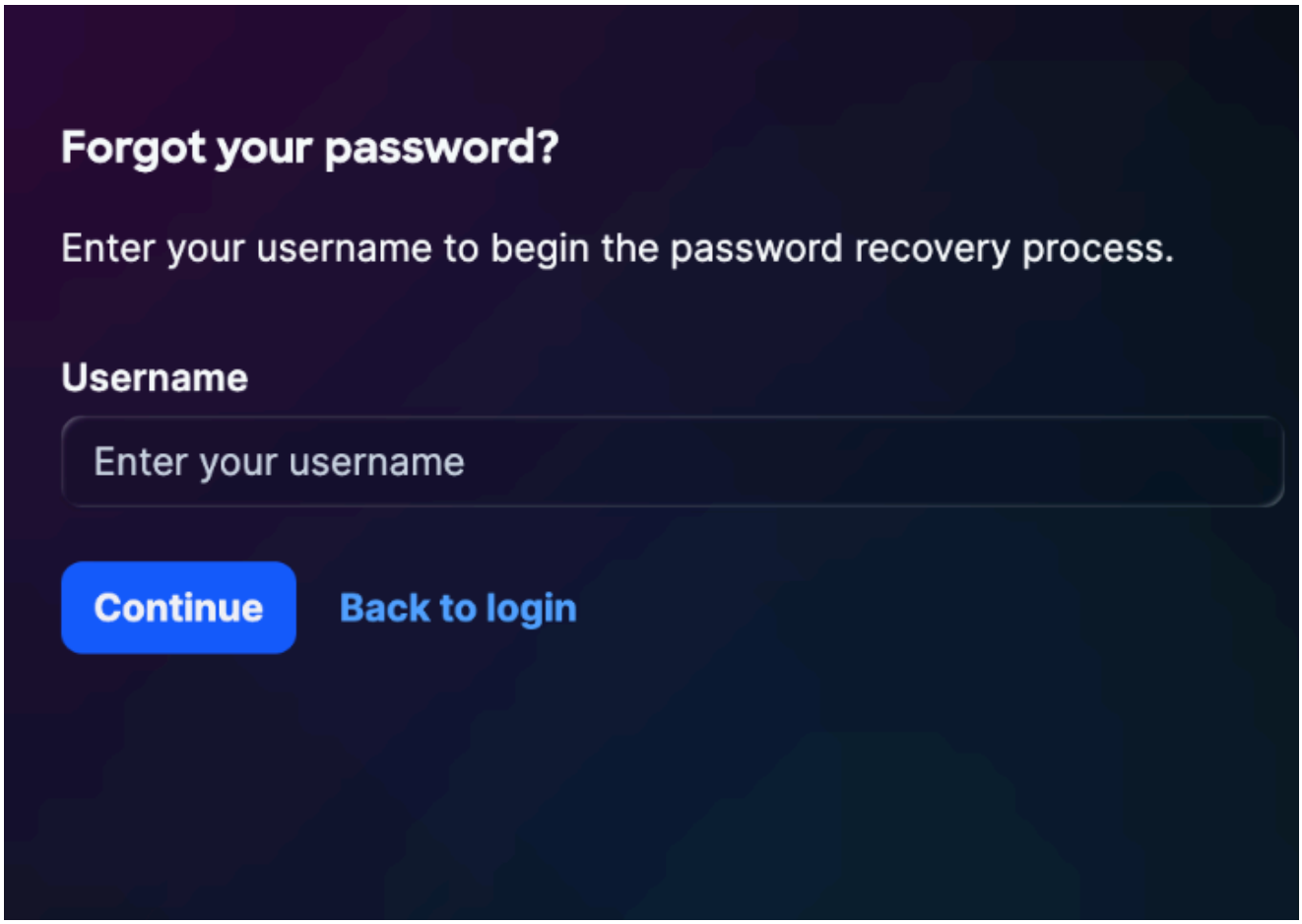
Le mot de passe est mis à jour dans le système Cisco IQ, y compris la machine virtuelle Cisco IQ.

Réinitialisation d'un mot de passe oublié

Vous pouvez réinitialiser un mot de passe oublié à l'aide du processus de vérification des questions de sécurité, si vous avez configuré les questions de sécurité précédemment. Consultez Configuration des questions et réponses de sécurité pour plus de détails.

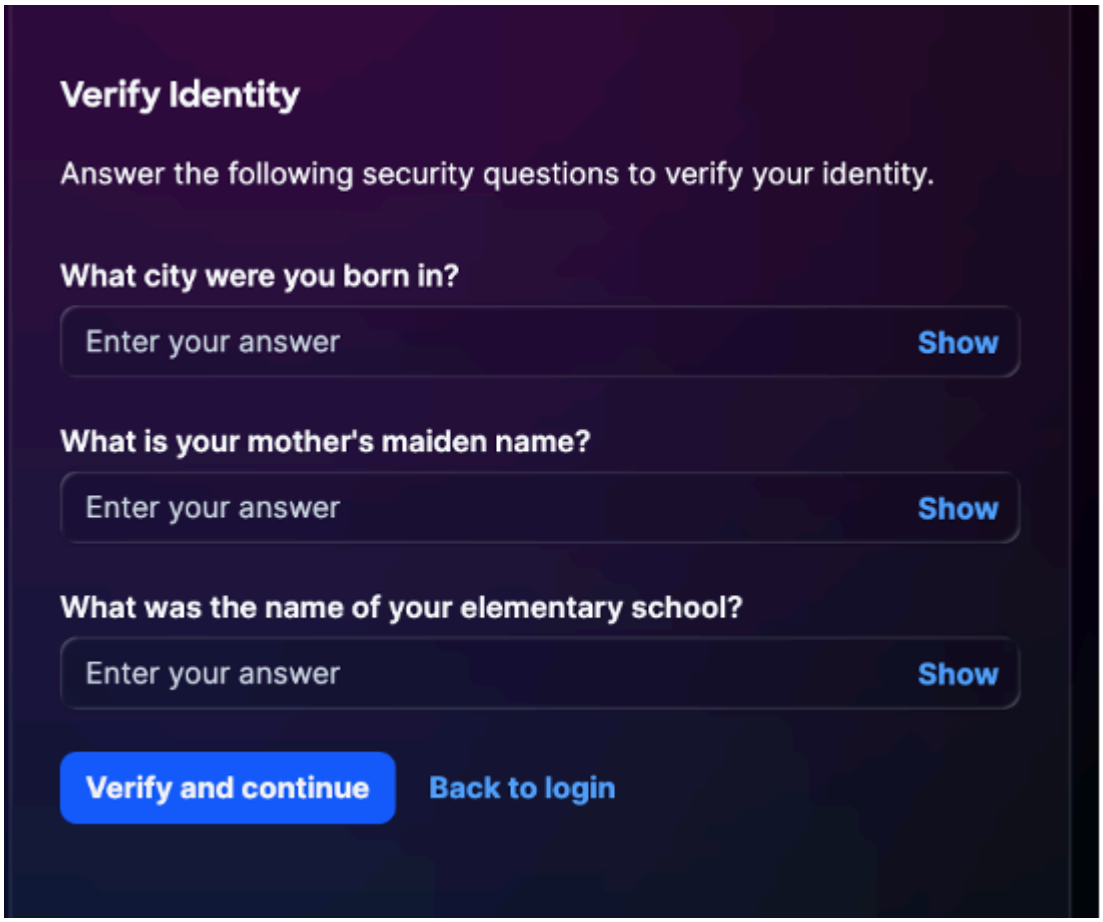
Pour réinitialiser un mot de passe oublié :

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



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.



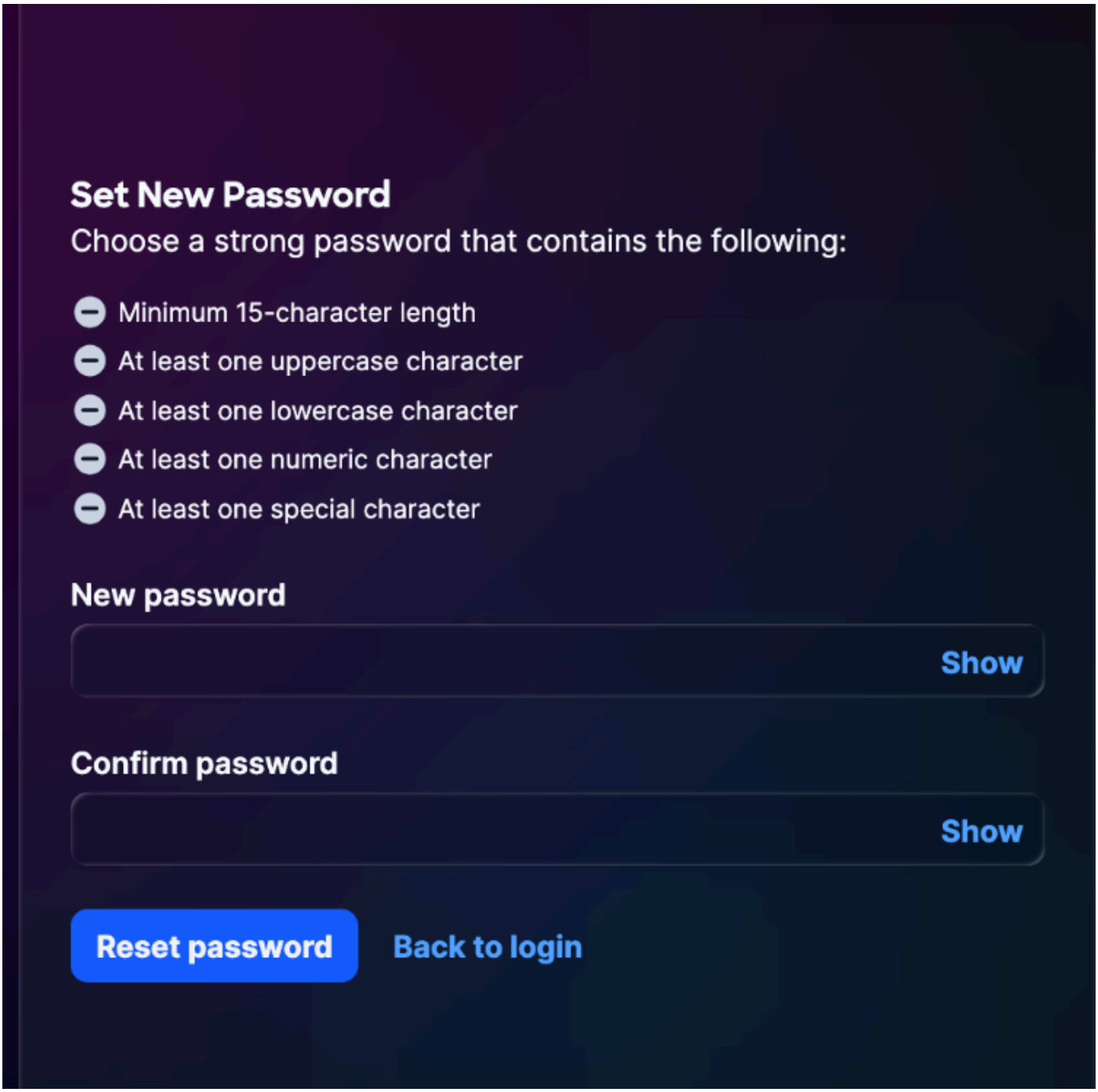
Vérifier l'identité

Remarque : Les questions de sécurité affichées ci-dessus sont spécifiques à l'utilisateur et varient en conséquence.

---

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.



Réinitialiser le mot de passe

Vous avez trois (3) tentatives pour répondre correctement aux questions de sécurité 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 réinitialiser votre mot de passe pendant la période de verrouillage.
Le système affiche le message suivant : "Compte verrouillé en raison d'un trop grand nombre de tentatives de vérification infructueuses. 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.

7. Entrez le nouveau mot de passe.

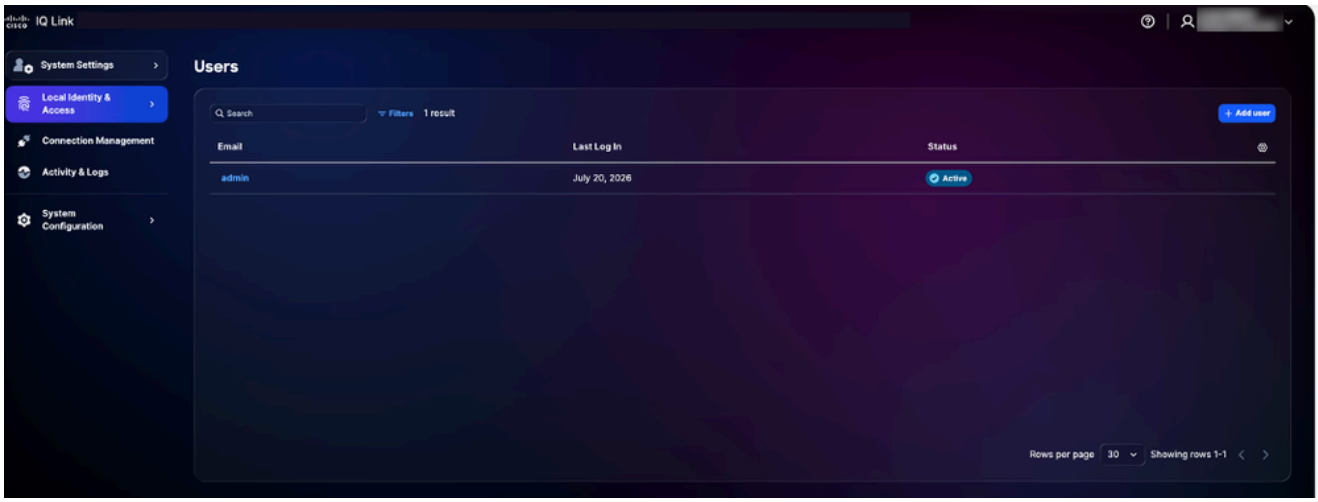
8. Entrez à nouveau le mot de passe pour le confirmer.

9. Cliquez sur Soumettre.

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.

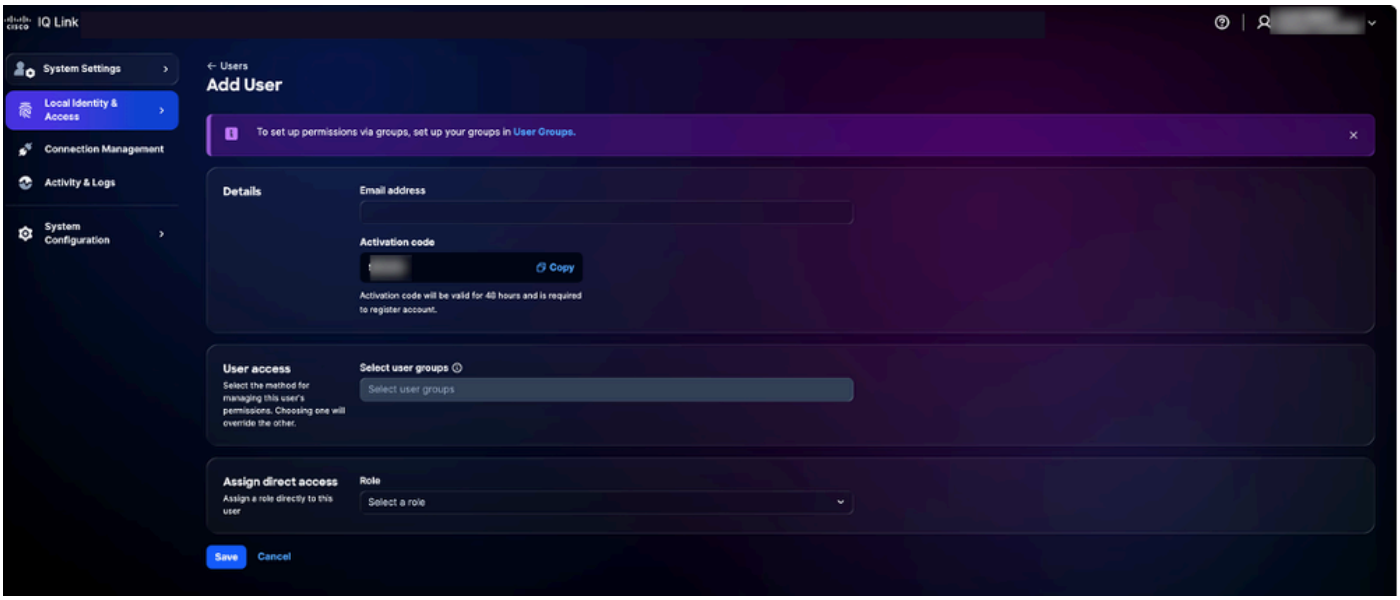


Page Utilisateurs

Remarque : L'icône Plus d'options ne s'affiche pas pour les administrateurs de compte (comme illustré dans l'image ci-dessus).

---

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



Ajouter un utilisateur

3. Saisissez l'adresse e-mail.

4. Entrez le code d'activation.

Remarque : Le code d'activation est affiché par défaut. Partagez-le avec l'utilisateur, car il est nécessaire pour terminer l'inscription.

---

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

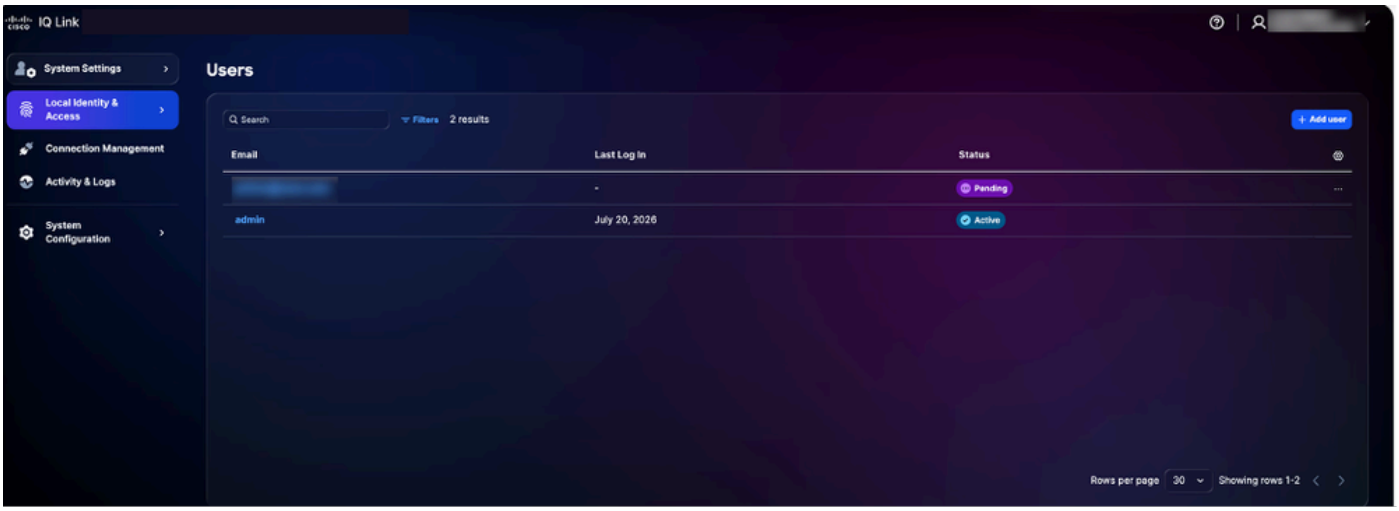
Remarque : Les utilisateurs héritent de l'accès du groupe sélectionné.

---

6. Dans Affecter un accès direct, sélectionnez un rôle dans la liste déroulante Rôle. Deux (2) rôles sont disponibles :

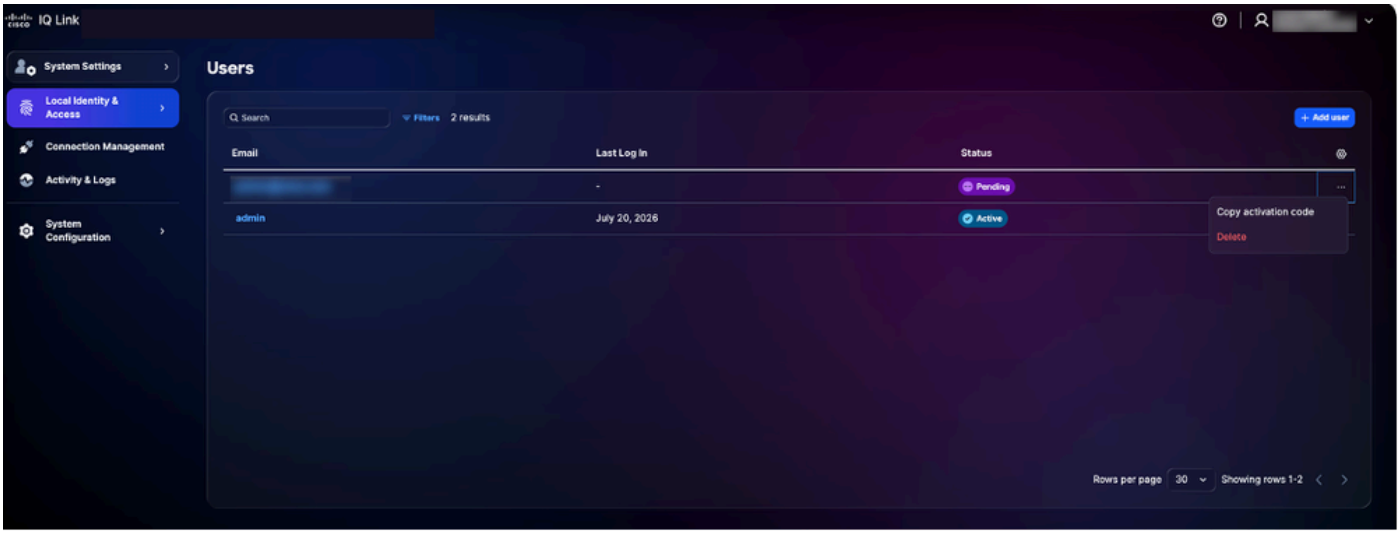
- Visionneuse : Afficher et accéder aux applications
- Administrateur : Accédez aux applications et gérez les paramètres système, à l'exception de System Management et IDP

7. Cliquez sur Enregistrer. 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.



Utilisateur nouvellement ajouté

8. Localisez le nouvel utilisateur dans la liste et vérifiez que la colonne Statut affiche En attente.



Copier le code d'activation

9. Cliquez sur l'icône Autres options > Copier le code d'activation en regard du nouvel utilisateur. Le code d'activation est copié dans le Presse-papiers.

10. 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, qui invalide le précédent

---

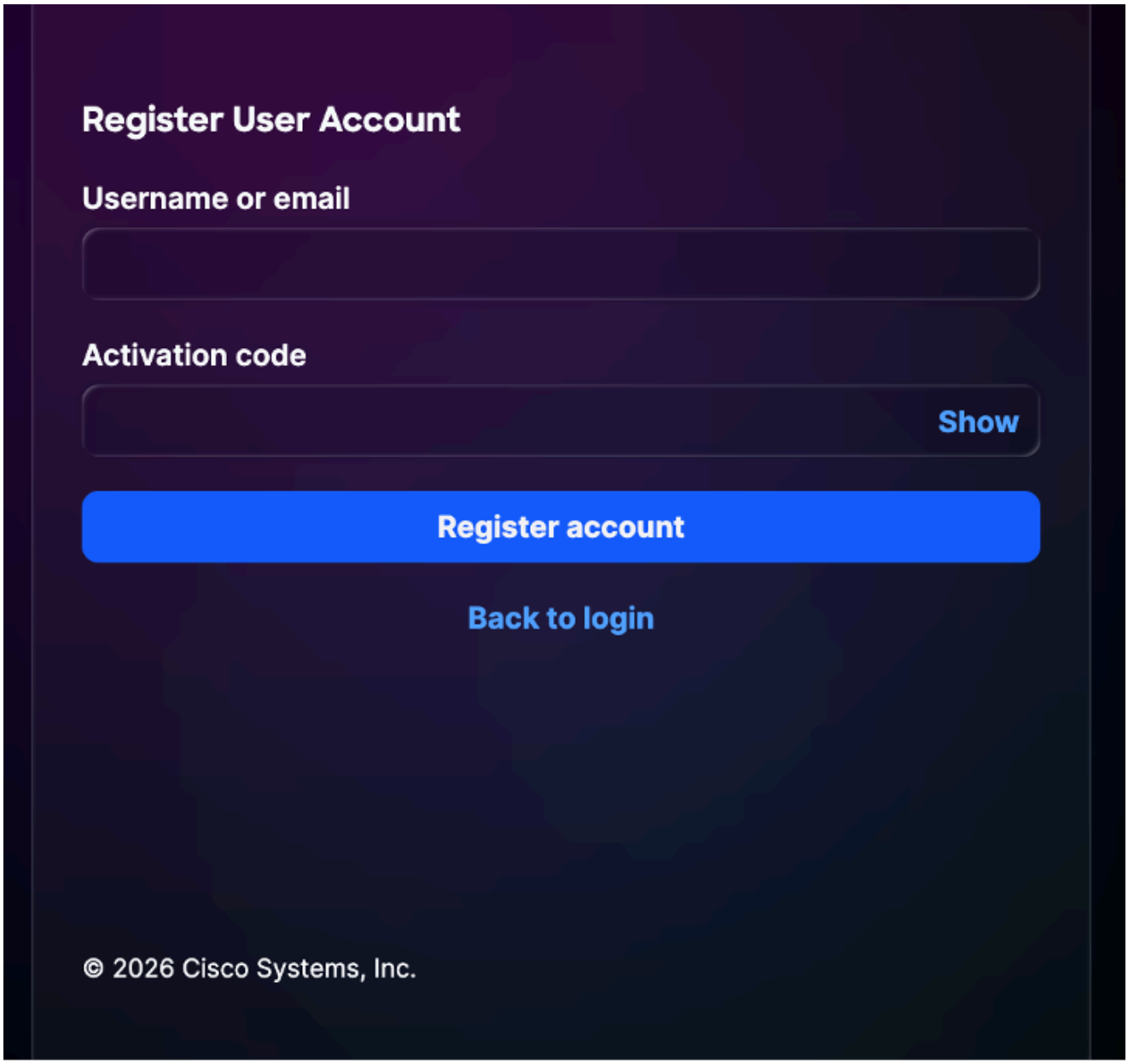
Remarque : les codes d'activation sont valides pendant 48 heures. Si votre code expire, veuillez contacter votre administrateur de compte pour en demander un nouveau.

11. Pour vous déconnecter, cliquez sur l'icône Utilisateur dans le coin supérieur droit et sélectionnez Déconnexion. Vous revenez à la page de connexion de Cisco IQ.

Inscription du nouveau compte utilisateur

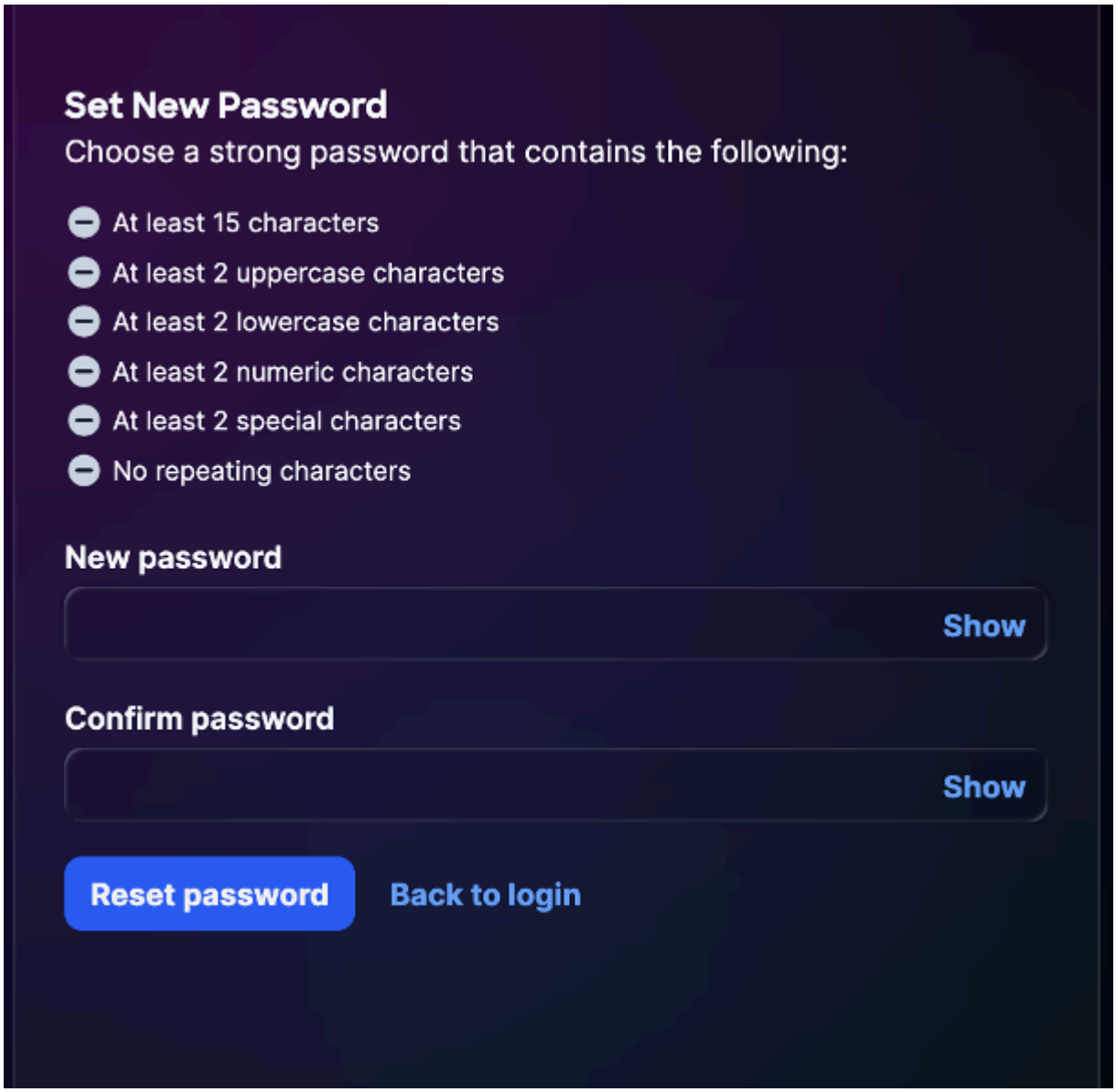
Pour enregistrer le nouveau compte d'utilisateur :

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



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.



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 et réponses de sécurité pour plus d'informations).

Gestion des groupes d'utilisateurs locaux

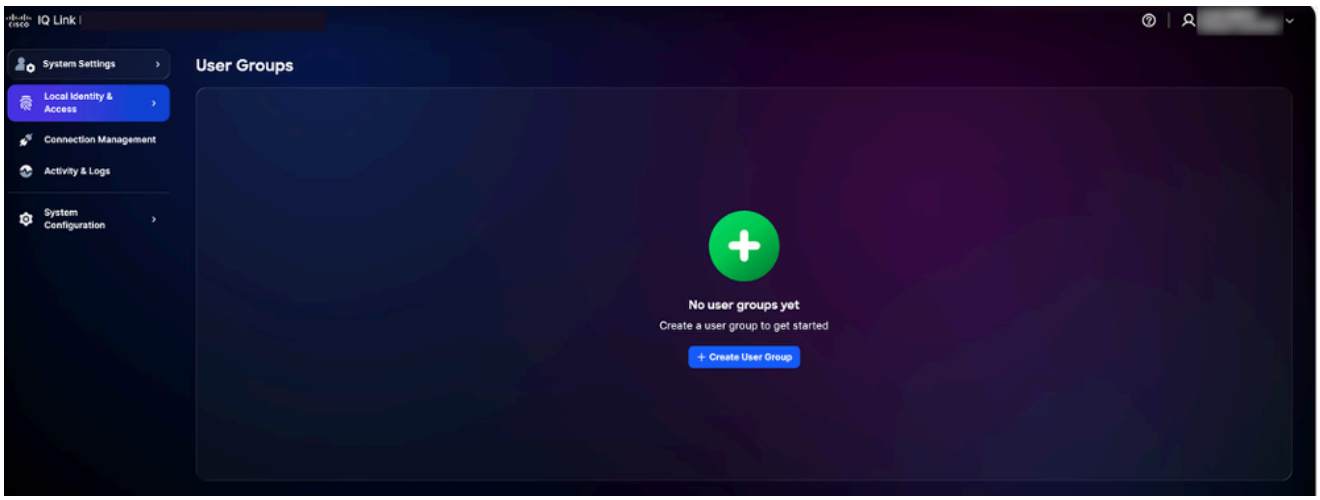
Les groupes d'utilisateurs permettent aux administrateurs de comptes de gérer ensemble les rôles de plusieurs utilisateurs locaux. Au lieu d'attribuer un rôle à chaque utilisateur individuellement, un administrateur de compte peut créer un groupe, y associer un rôle et un ensemble d'utilisateurs et mettre 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.

Création d'un groupe d'utilisateurs

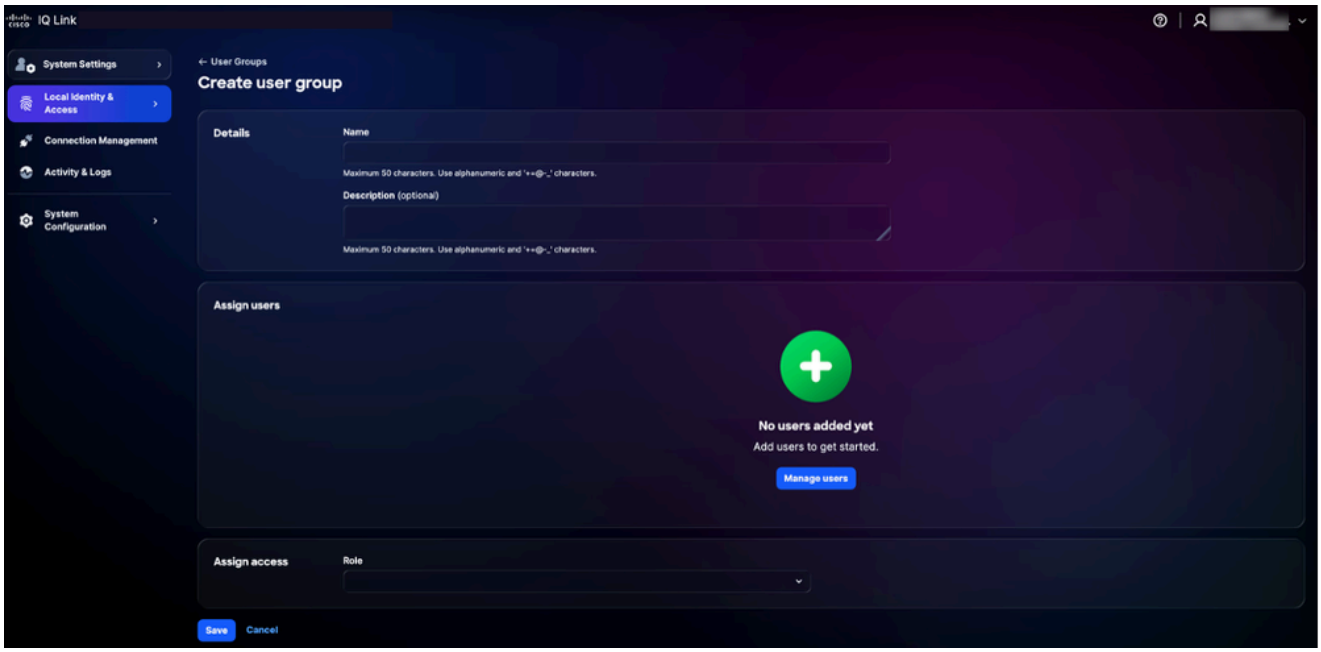
Pour créer un groupe d'utilisateurs :

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 : Afficher et accéder aux applications (lecture seule)
    - Administrateur : Accéder aux applications et gérer les paramètres système

4. Cliquez sur Enregistrer.

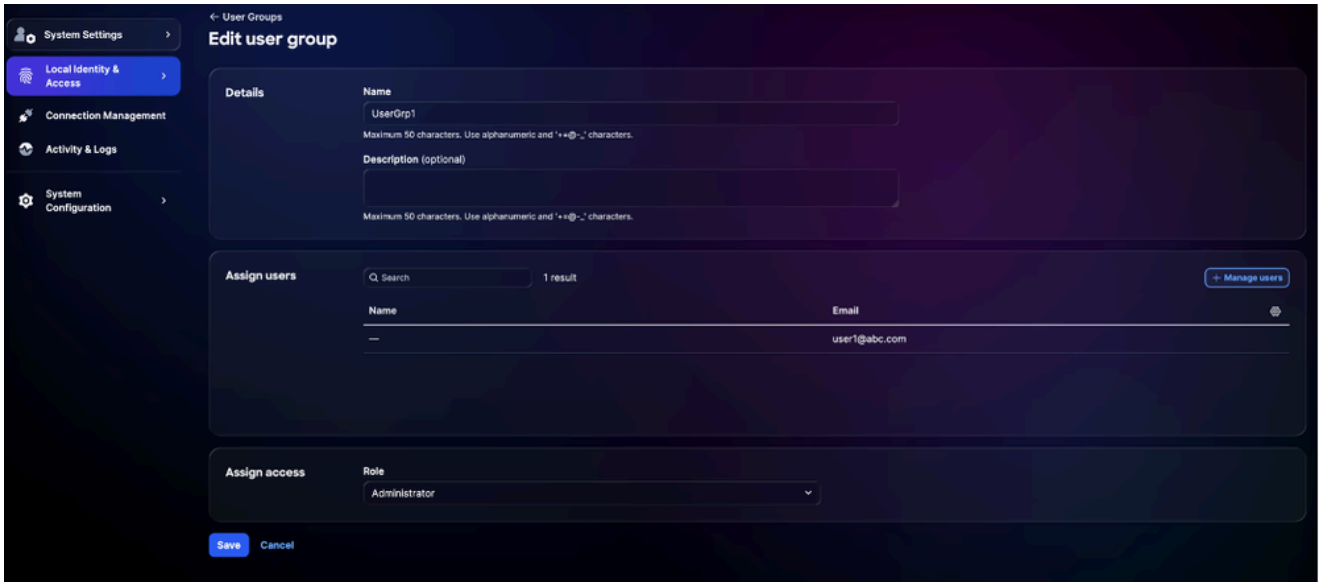
Le nouveau groupe d'utilisateurs s'affiche dans la liste Groupes d'utilisateurs avec le rôle qui lui a

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 More en regard du groupe et choisissez Edit. La page Modifier un groupe d'utilisateurs s'affiche.



Modifier le groupe d'utilisateurs

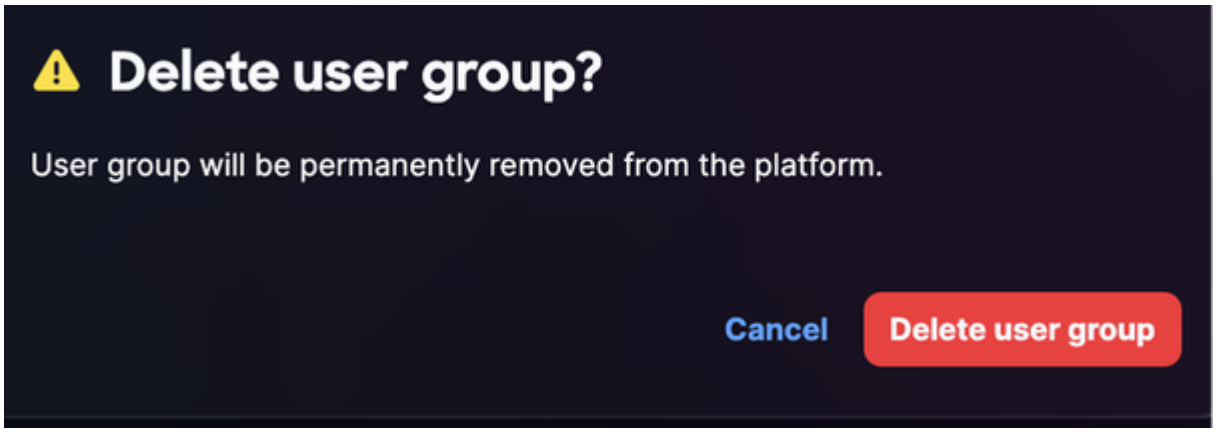
3. Effectuez les modifications souhaitées.
4. Cliquez sur Save.

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 Cisco IQ Link, les administrateurs de compte peuvent configurer différents paramètres. Les administrateurs de compte peuvent se connecter à Cisco IQ Link en utilisant l'administration locale ou la configuration du fournisseur d'identité (IDP).

Configuration SAML d'Okta IDP pour SSO

Conditions requises pour configurer IDP SAML

- Accès administrateur de compte local à Cisco IQ Link
- 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.

2. Définissez les attributs suivants pour l'instance Cisco IQ Link.
Tableau 1 : Attributs de liaison Cisco IQ

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

Tableau 2 : 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 Consumer Service (ACS)	https://mymanagementhost.mydomain.com/saml/acs
Format ID nom	Adresse électronique	S. O.
Nom d'utilisateur	Nom d'utilisateur	S. O.

3. Configurez les instructions d'attribut obligatoires suivantes.

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: .*

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

Tableau 3 : 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 SP sont requises pour ADFS IDP 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

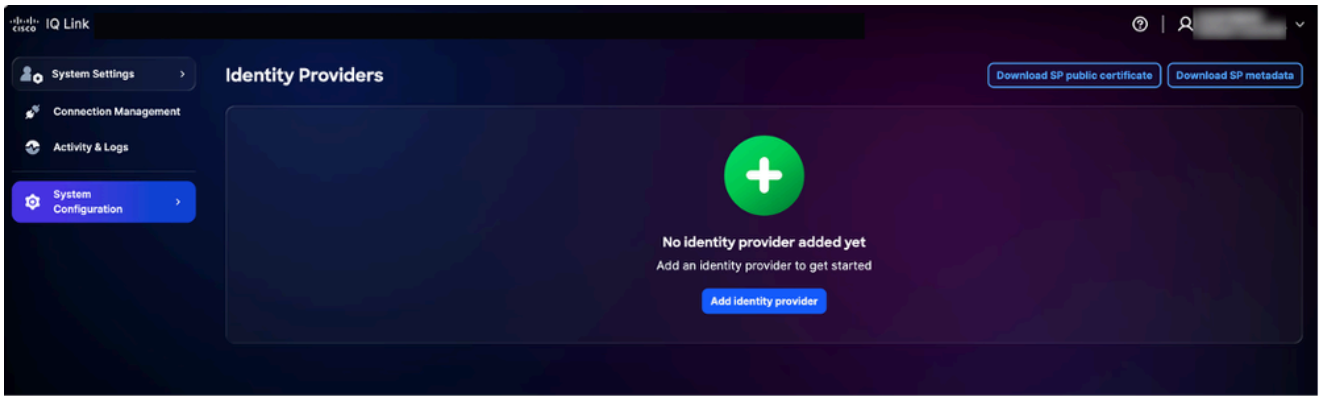
5. Cliquez sur l'icône Download pour télécharger le fichier « SP Metadata ».

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

Ajout du PDI Okta

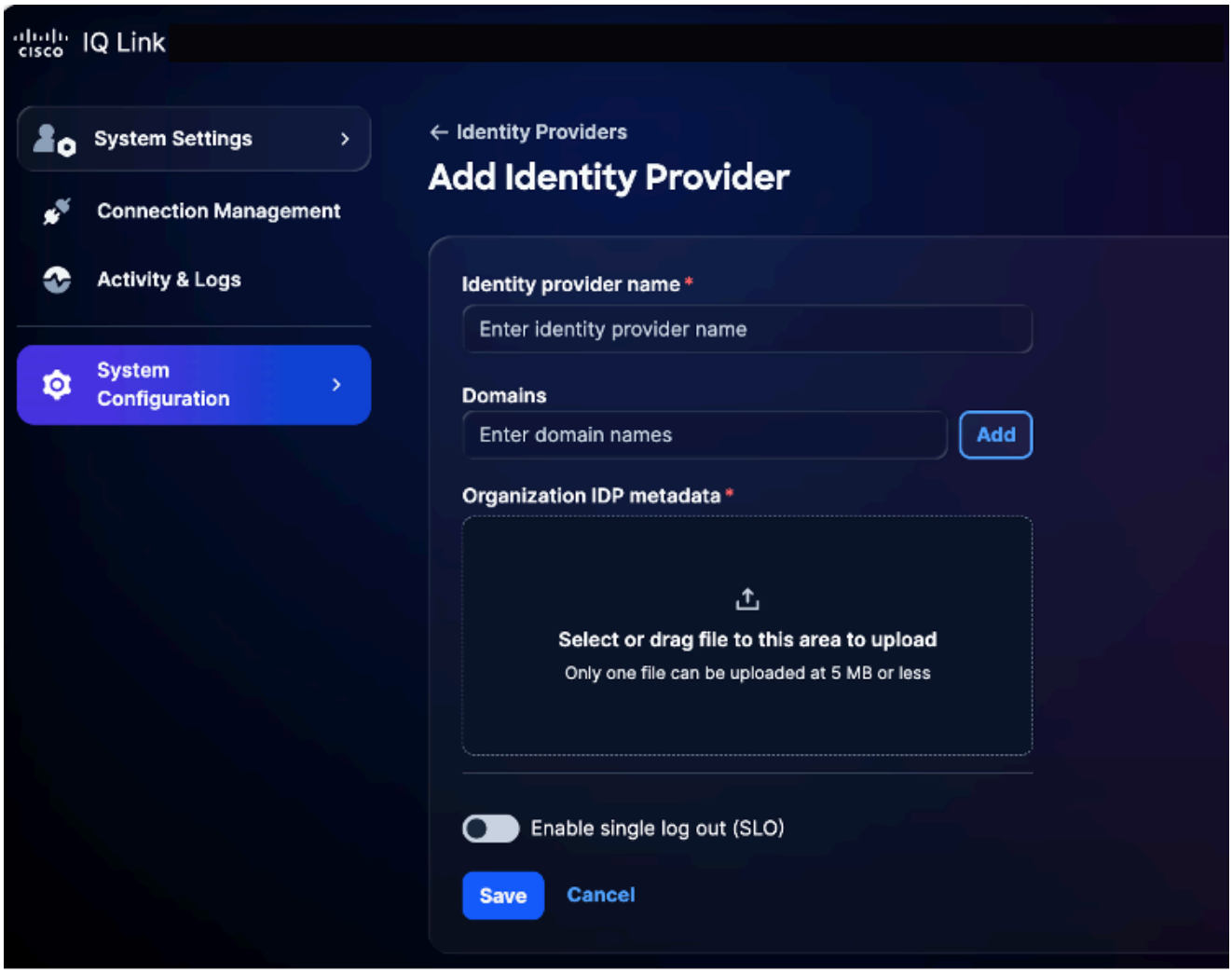
Pour ajouter un IDP dans Cisco IQ Link :

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



Page d'accueil IDP

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



Ajouter un fournisseur d'identité

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

3. Entrez le nom du fournisseur d'identité.

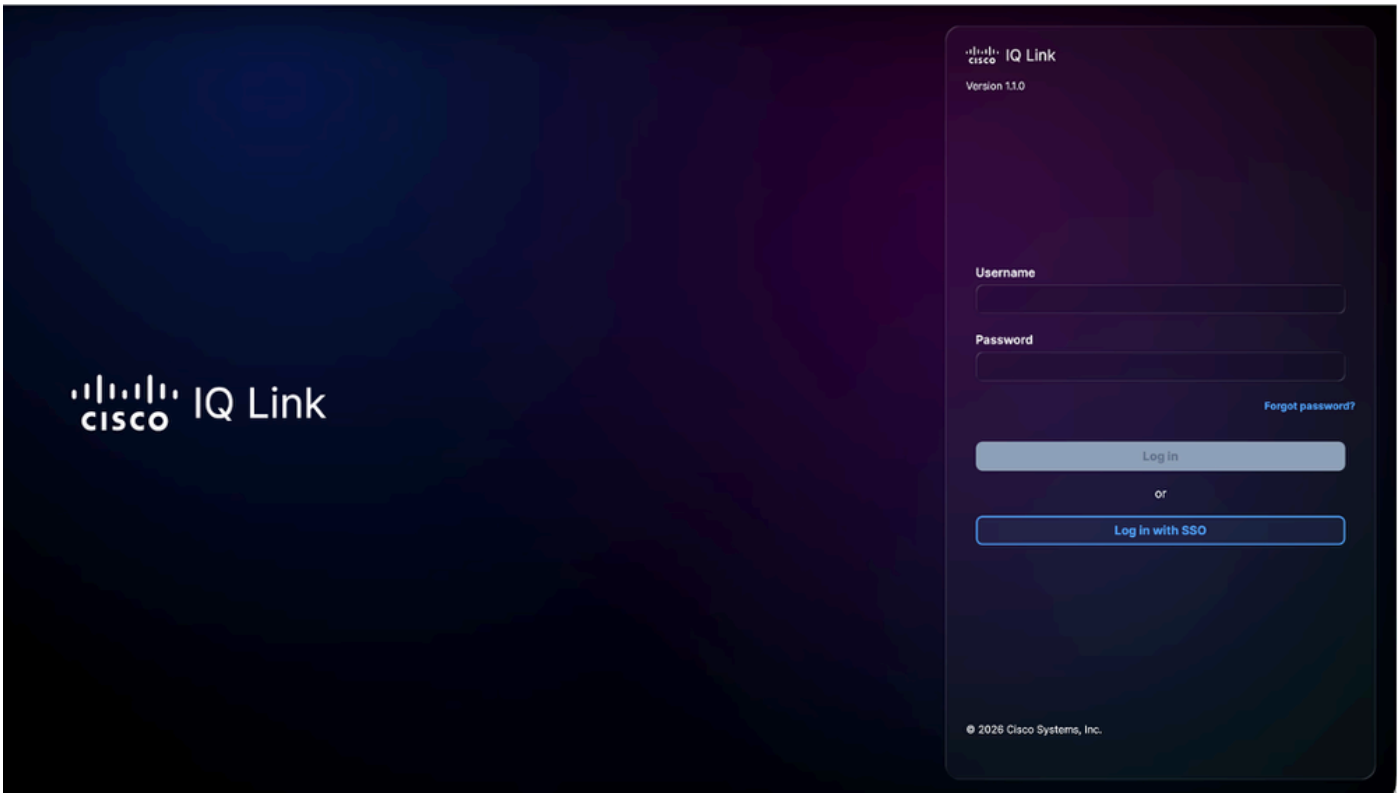
4. Cliquez sur Add pour ajouter un nom de domaine configuré Cisco IQ Link au champ Domains.

5. Faites glisser 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 les détails de l'entité du fournisseur de services (SP).

6. (Facultatif) Activez le bouton bascule Enable single logout. Vous pouvez également activer le SLO ultérieurement.

7. Cliquez sur Enregistrer.

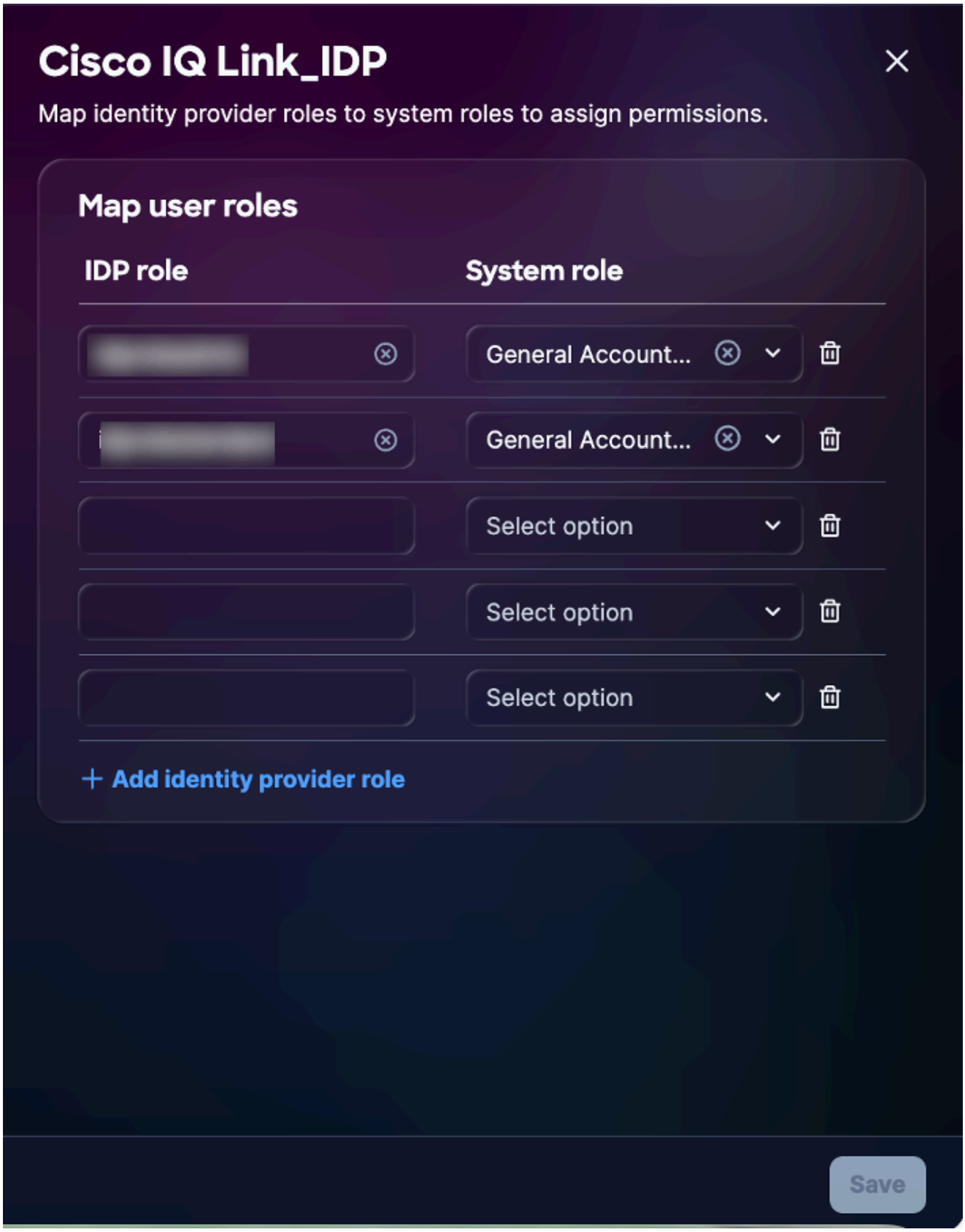
Une fois configurée, la page de connexion affiche une option permettant de se connecter avec SSO (via IDP).



Connexion à la liaison Cisco IQ

Configuration du mappage des rôles

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



Mappage des rôles utilisateur

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

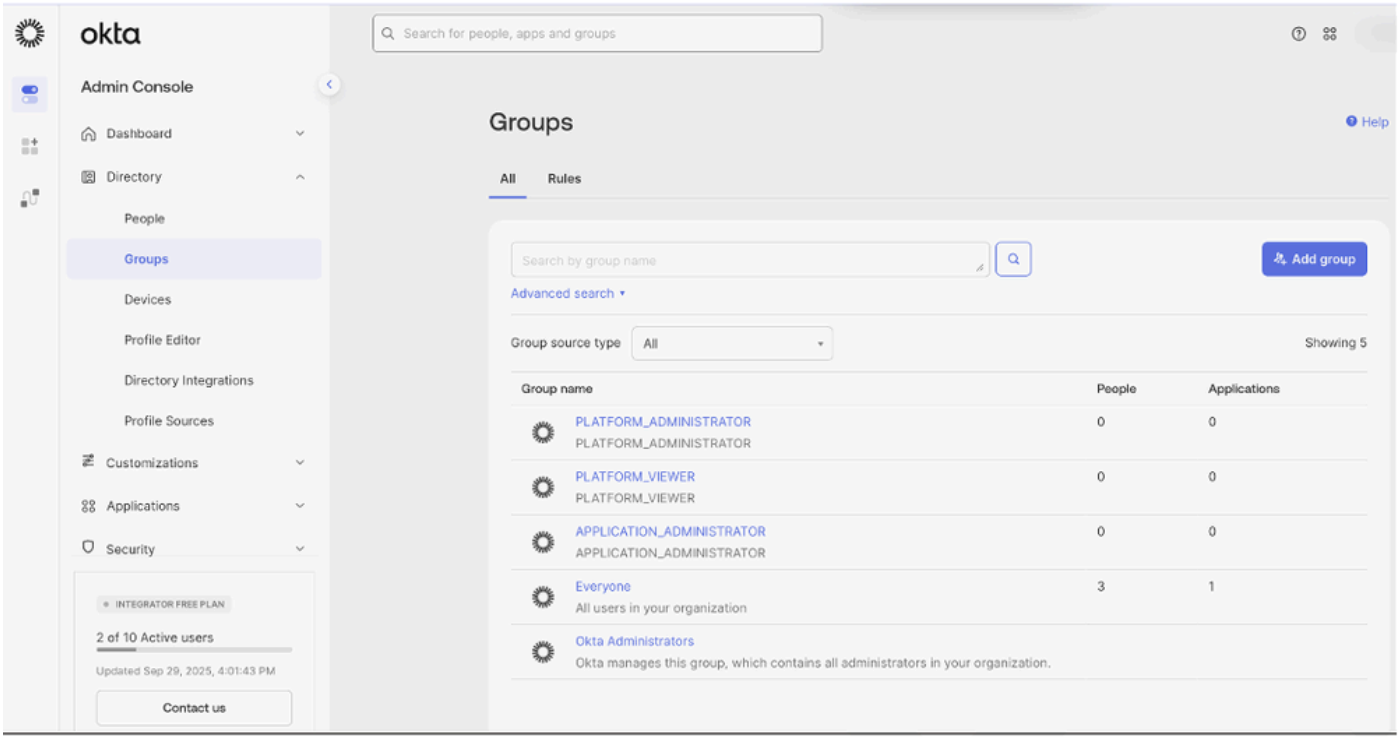
- Administrateur de compte général : L'administrateur général du compte dispose des

autorisations complètes pour effectuer toutes les actions du produit

- 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 Enregistrer.

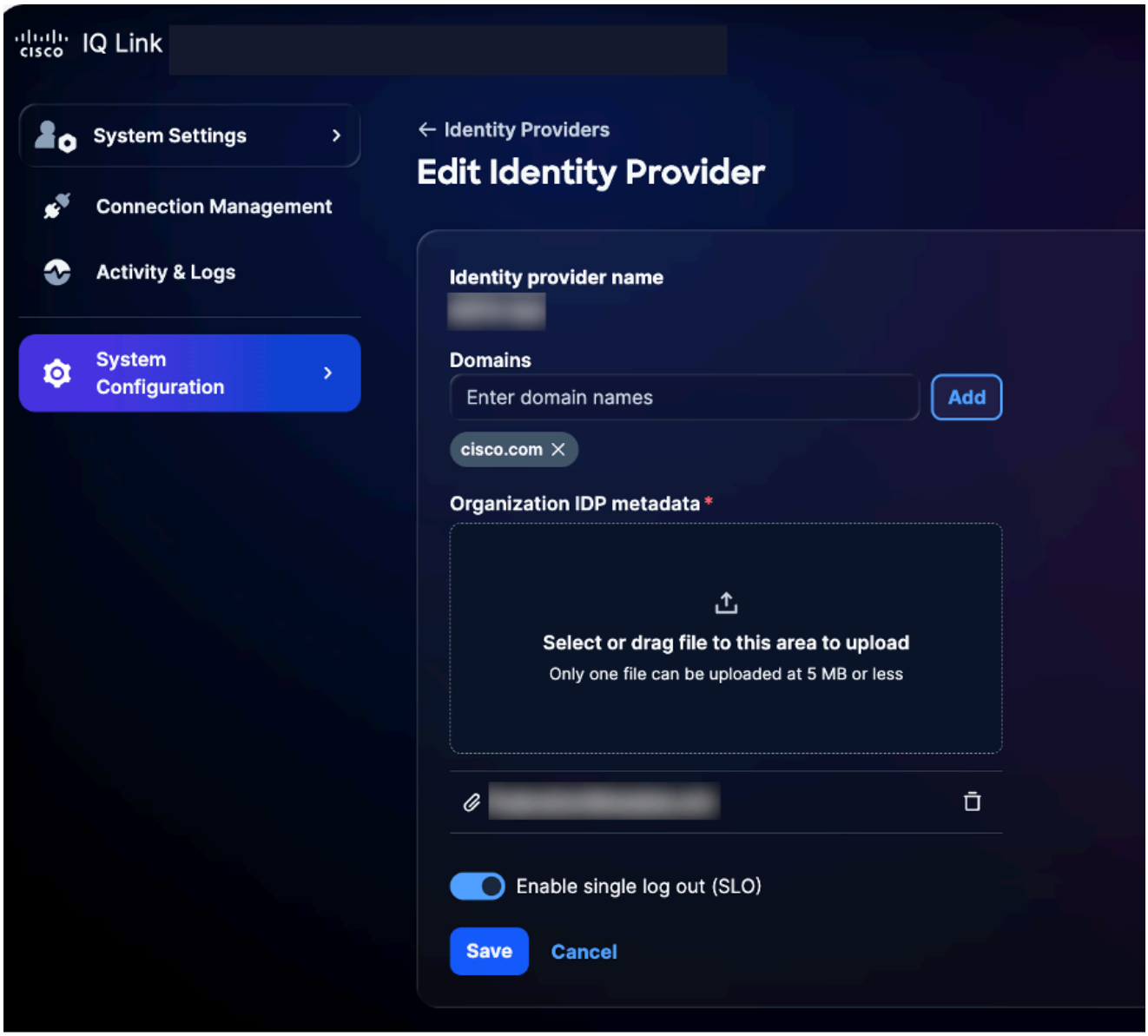
Configuration de déconnexion unique

Si vous choisissez d'activer la configuration de déconnexion unique (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 Identity Providers, cliquez sur Download SP public certificate.

Télécharger le certificat public

2. Enregistrez le fichier de téléchargement en tant que 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. Téléchargez à nouveau le fichier de métadonnées IDP.
6. Sur la page Fournisseurs d'identités, sélectionnez l'icône Autres options du IDP ajouté > Modifier.



Modifier le fournisseur d'identité

7. Activez le bouton bascule Activer la déconnexion unique (SLO).
8. Téléchargez le fichier de métadonnées nouvellement téléchargé.
9. Utilisez la liste de contrôle suivante pour vérifier la fonctionnalité SSO et SLO :

Liste de vérification :

- La connexion de l'administrateur de compte local a réussi
- Le portail IDP est configuré et provisionné
- IDP est ajouté à Cisco IQ avec le 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/SLO de bout en bout a été testé avec succès

Dépannage des problèmes IDP

La liste suivante présente 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 4 : 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 les services ADFS (Microsoft Active Directory) en tant qu'IDP SAML pour Cisco IQ.

Conditions requises pour configurer ADFS IDP SAML pour SSO

- ADFS 6.0+ est recommandé
- Windows Server 2012 R2+
- Intégration AD configurée
- Certificats SSL/TLS (Transport Layer Security) sur ADFS
- Accès administrateur de compte à Cisco IQ
- Accès administratif au serveur ADFS (Windows Server)
- Accès PowerShell sur le serveur ADFS
- Connectivité réseau entre ADFS et Cisco IQ

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

Tableau 5 : Configuration du serveur ADFS

Élément	Description	Exemple
FQDN Cisco IQ	Nom d'hôte du déploiement utilisateur	devxx-23.cx-xxx-xxx.cisco.com
URL du serveur ADFS	Adresse du serveur ADFS utilisateur	https://ad-fs.dev.local
Domaine de la société	Domaine de messagerie	company.com
Groupes AD	Nom de domaine (DN) du groupe AD	CN=Rôle - Développeurs CXIQ

Configuration des serveurs ADFS

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 Télécharger les métadonnées SP pour télécharger ces fichiers.
3. Copiez et enregistrez les fichiers service-provider-metadata.xml et service-provider-certificate.crt dans le répertoire ADFS (par exemple, C :-certificate.crt).
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 Browse pour sélectionner le fichier de métadonnées SP et terminer le téléchargement du fichier.
11. Cliquez sur Suivant.
12. Entrez un nom d'affichage (par exemple, « CIQ-Stage »), ajoutez les notes 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 « Permit Everyone with MFA » (Autoriser tout le monde avec MFA) sauf si votre serveur ADFS dispose d'un adaptateur MFA (Multi-Factor Authentication) enregistré (par exemple, Azure MFA ou *Time-Based One-Time Password (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
```

Pour définir l'option Autoriser tout le monde (pas de condition d'AMF), exécutez la commande suivante :

```
Set-AdfsRelyingPartyTrust -TargetName “

     ” -AccessControlPolicyName “Permit everyone”
```

Vous pouvez également créer l'approbation de la partie de confiance via 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/per
```

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 6 : 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 (Public Key Infrastructure)/certificat	ADFS mappe le certificat client à un utilisateur AD via le nom d'utilisateur principal (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 approbation de partie de confiance (par exemple, « Cisco IQ - Stage »).

```
$relyingPartyName = “Cisco IQ - Stage”
```

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

```
$claimRules = @’

@RuleTemplate = “LdapClaims”

@RuleName = “Send Email and Name”

c:[Type == “http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname ”, Issuer == “AD
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/ws/2005/05/identity/claims/em

@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.Iss

@RuleName = “Send Group Membership”
c:[Type == “http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname ”, Issuer == “AD
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/claims/Group”), query = “;mem
’@@
```

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

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

Write-Host “Claim rules configured successfully!” -ForegroundColor Green
```

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.

```
$username = “testuser”
```

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.

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

Exemple de rapport :

```
CN=Role - CXIQ Developers,OU=Role Groups,DC=dev,DC=local
```

Configuration d'ADFS pour approuver le certificat de signature SP

1. Sur 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
```

OU

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

```
Import-Certificate -FilePath “C:-iq-onprem-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 d'autorité de certification en exécutant la commande suivante :

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

3. Configurez le rôle d’autorité de certification 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. Installez 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 sur 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 UPN d'un utilisateur ou un e-mail correspondant 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, Thumbprint, NotAfter -AutoSize
```

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 :

```
Enable-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 AddressPath, Enabled, Proxy -AutoSize
```

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”, “WindowsAuthentication”, “FormsAu
-PrimaryExtranetAuthenticationProvider @(“CertificateAuthentication”, “FormsAuthentication”, “Microsoft
```

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 :

```
netsh 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)” -ForegroundColor Red
```

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

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

3. Vérifiez qu'aucun certificat non auto-signé ne reste dans le magasin racine 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 7 : 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 d'autorité de certification qui émet des certificats utilisateur doit être dans le 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 LocalMachinestore à l'aide de la commande suivante :

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

Si le certificat est introuvable, importez-le dans LocalMachinestore :

```
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 du registre ClientAuthTrustMode prend uniquement effet 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 Metadata”}).FullUrl

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.
2. Remplacez <your-adfs-server> par le nom d'hôte de votre serveur ADFS.
3. 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 Paramètres système > Configuration système > Fournisseurs d'identités.
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. Entrez le nom du fournisseur d'identité.
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.

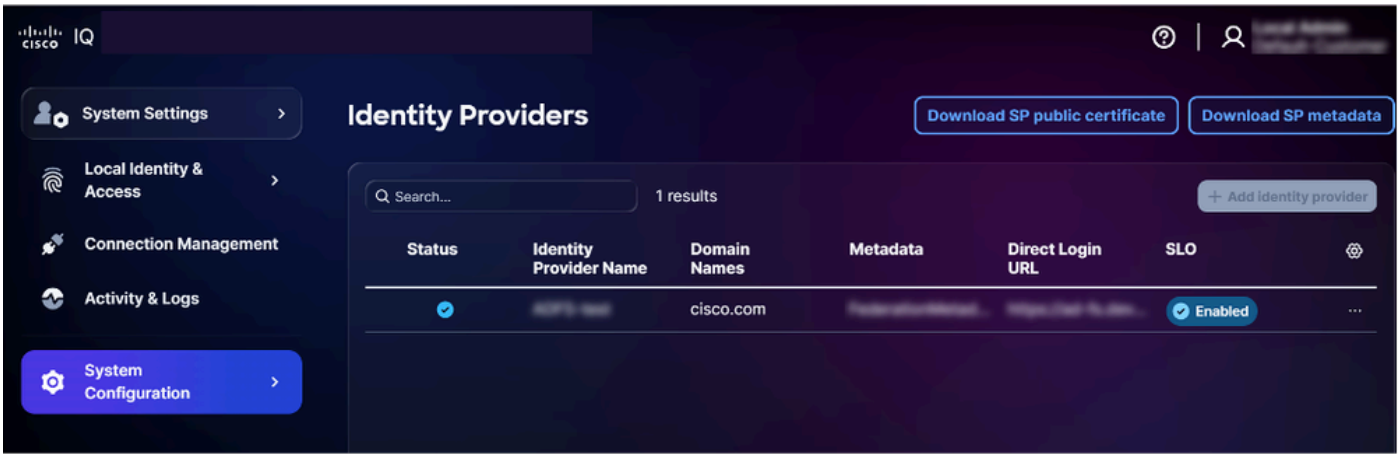
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = "(&(objectClass=group)(cn=Role - CXIQ*))"
$searcher.PropertiesToLoad.Add("distinguishedName") | Out-Null
$searcher.PropertiesToLoad.Add("cn") | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties["distinguishedname"]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

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

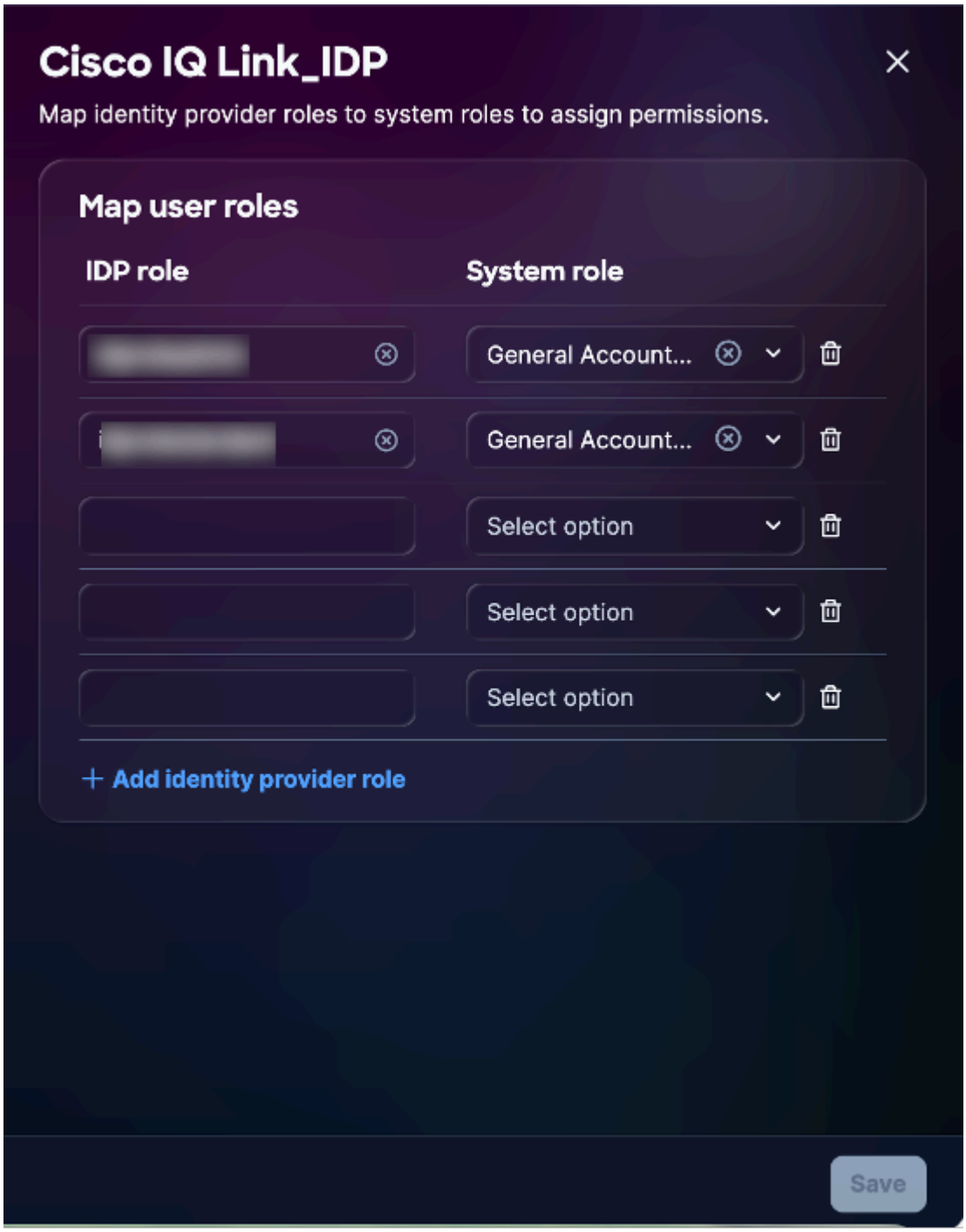
Si les groupes requis ne sont pas répertoriés, ils doivent être créés dans Active Directory par un administrateur de compte avant que vous puissiez effectuer le mappage de rôle ADFS.

Pour configurer le mappage des rôles :



Mapper les rôles

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



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, les développeurs CXIQ) et non des noms de domaine complets.

3. Cliquez sur Enregistrer. 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 la machine client (macOS) sous Configuration de l'authentification basée sur certificat pour plus d'informations).

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 Certificate Authentication. Le navigateur vous invite à saisir le 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 8 : 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 • Attribut de groupe incorrect : Doit être http://schemas.xmlsoap.org/cla ims/Group • L'utilisateur ne fait pas partie des groupes AD
Échec du décodage	« Impossible de déchiffrer l'assertion » dans les journaux	Vérifier la configuration du certificat ADFS

Problème	Symptômes / Description	Causes / Contrôles / Contournements et solutions
Boucle de connexion	Blocage dans une boucle d'authentification ou de connexion	• URL ACS non valide : Vérifiez : https://your-fqdn/saml/acs • Incompatibilité de cookies : Vérifier les cookies du navigateur pour le 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 : confirme 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'assure que le certificat de cryptage correct est associé à l'approbation de la partie de confiance Cisco IQ

```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object EncryptionCertificate | Format-List
```

- Vérifier la configuration des terminaux SAML : Vérifie 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 - Stage” | 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 l'authentification basée sur mot de passe et PKI/certificat (CBA).

Conditions requises pour configurer l'ID supplémentaire SAML pour SSO

- Client Microsoft Entra ID (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 (requise pour PKI uniquement)
- Point de distribution de la liste de révocation de certificats (CRL) accessible depuis Internet (requis pour PKI uniquement)

Tableau 9 : 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-DOMAINE>

Configuration de l'application SAML ID entrée

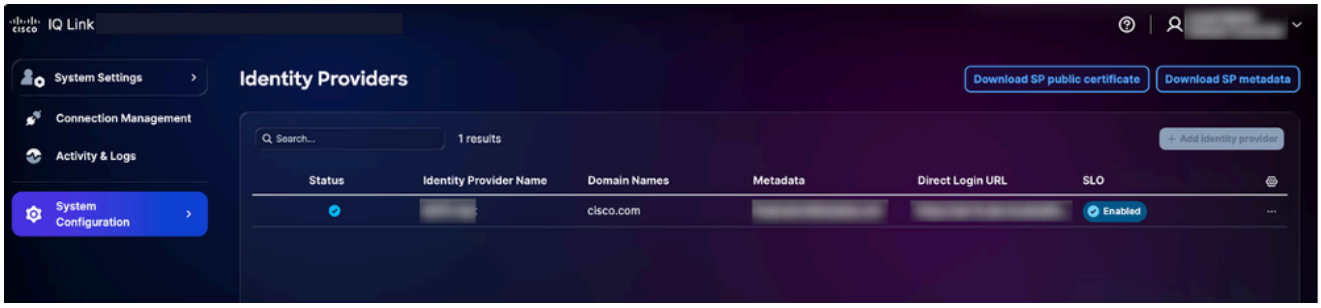
Création d'une application d'entreprise

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. Saisissez 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. Pour l'obtenir, procédez comme suit à partir de l'appliance virtuelle (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 Single Sign-on basé sur SAML après un 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 :

1. Dans l'application d'entreprise, accédez à Authentification unique et sélectionnez SAML.

2. Dans la section Configuration SAML de base, cliquez sur Modifier et entrez les éléments suivants :

   a. Identificateur (ID d'entité) : <YOUR-CIQ-FQDN>

   b. URL de réponse (URL ACS) : https://<YOUR-CIQ-FQDN>/saml/acs

   c. URL de connexion : https://<YOUR-CIQ-FQDN>/saml/login

   d. URL de déconnexion : https://<YOUR-CIQ-FQDN>/saml/logout

3. 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.

---

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

5. Configurez les revendications suivantes :

Tableau 10 : 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/claims
prénom	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
nom de famille	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
nom	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
groupes	utilisateur.assignerdroles	(VIDE — effacer l'espace de noms)

Remarque : Pour les groupes revendiquent :
- Utilisez user.assignedroles comme source — pas utilisateur.groupes
- 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 provoque 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, visualiseurs 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 identificateurs 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, accédez à la section Authentification unique > Certificat de signature SAML.
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. Saisissez un rôle IDP pour chaque rôle système. Les rôles système suivants sont pris en charge :

Tableau 11 : Rôles système

Rôle système	Rôle IDP (Valeur du rôle d'application)	Description
Administrateur général de compte	Administrateurs CXIQ	Autorisations complètes pour toutes les actions
Visualiseur de compte général	Développeurs CXIQ	Accès en lecture seule
Visualiseur de 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 sous Configuration de l'application SAML ID supplémentaire pour plus de détails).

---

3. Cliquez sur Enregistrer. 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 est affichée.
6. Vérifiez l'extraction du groupe en exécutant la commande suivante :

```
kubectl -ncxue logs deployment/apisix –since=5m | grep -E “authentication successful|Extracted group|To
```

Résultats attendus

```
SAML 2.0 compliant authentication successful for user: user@domain.com with full name: N/A and 1 groups
Extracted group: CXIQ Admins (original: CXIQ Admins)
Total groups extracted: 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 services de certificats Active Directory (CS) avec CA d'entreprise configurée (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 UPN d'ID supplémentaire (par exemple, user@ciqtestdev.onmicrosoft.com).

3. Pour générer le certificat, exécutez la commande suivante :

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

4. Pour soumettre 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 -P “

     ”
```

- 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

Cette opération fait correspondre l'UPN du nom alternatif de l'objet 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. Sur la page de connexion de Microsoft, saisissez l'adresse e-mail de l'utilisateur et cliquez sur Next.
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 12 : 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 Entra ID (voir Configuration de l'authentification unique SAML sous Configuration de l'application SAML Entra ID pour plus de détails). Vérifiez que l'attribut de messagerie de l'utilisateur est renseigné.

Problème	Motif	Régler
Nombre total de groupes extraits : 0	Revendications de groupe non configurées 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 sous Configuration de l'application SAML avec ID supplémentaire pour plus de détails).
Revendications de groupe en double	user.groups et user.assignedroles actifs	Supprimez la revendication user.groups. Ne conserver que les utilisateurs.assignés.
Groupes affichés comme UUID	L'attribut source est « ID de groupe »	Utilisez l'approche Rôles d'application (voir Configuration des rôles d'application sous Configuration de l'application SAML avec ID supplémentaire pour plus de détails).
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 d'Entra ID et téléchargez à nouveau vers Cisco IQ.
AADSTS500191	CRL inaccessible depuis Internet	Publiez la liste de révocation de certificats sur une URL accessible au public ou utilisez une approche d'autorité de certification auto-signée (voir Solution de contournement des listes de révocation de certificats pour les environnements de laboratoire pour plus de détails).
Certificat non demandé	Certificat non inclus dans la chaîne de clés, CA non approuvé sur le client ou CBA non activé	Vérifiez que le certificat utilisateur est importé dans macOS Keychain Access (voir Importation du certificat utilisateur sur l'ordinateur client (macOS) sousConfiguration de l'authentification basée sur certificat pour plus de détails), CBA est activé dans Entra ID avec les paramètres requis (voir Activation de CBA dans Entra ID Authentication Methods sous Configuration de l'authentification basée sur certificat pour plus de détails) et Chrome est redémarré pour appliquer les modifications.
Assertion SAML expirée	Inversion d'horloge entre les systèmes	Augmentez clock_skew_seconds dans la configuration du plug-in (par défaut, 300, utilisez 30000 pour les travaux pratiques).
État « Incomplet » dans VA	Mappage des rôles non encore configuré	Mappage complet des rôles (voir Configuration du mappage des rôles pour plus de détails).

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. Comme il est auto-signé sans CDP, Entra ID ne tente pas la validation CRL.

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 la configuration SAML de base en saisissant 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 XML des métadonnées de fédération

Configuration de Cisco IQ

- Ajoutez un fournisseur d'identité dans Cisco IQ en téléchargeant les métadonnées Entra ID
- Configurer le mappage des rôles pour mapper les valeurs des rôles 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
- Émettre un certificat utilisateur avec un UPN correspondant à l'utilisateur Entra ID
- Exporter le certificat utilisateur en tant que 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 CBA dans les méthodes d'authentification
- Configurer la liaison de nom d'utilisateur (PrincipalName et userPrincipalName)

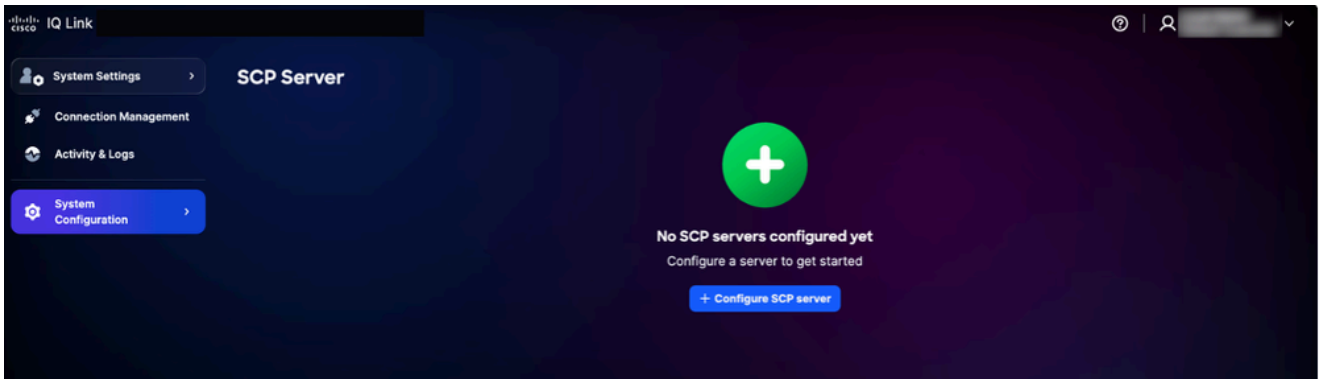
- Vérifier que la connexion CBA fonctionne de bout en bout

Ajout de serveurs SCP

Ce serveur SCP (Secure Copy Protocol) est un prérequis pour l'importation de fichiers de mise à niveau essentiels pour l'ajout, la mise à niveau ou l'application de correctifs à l'installation de Cisco IQ.

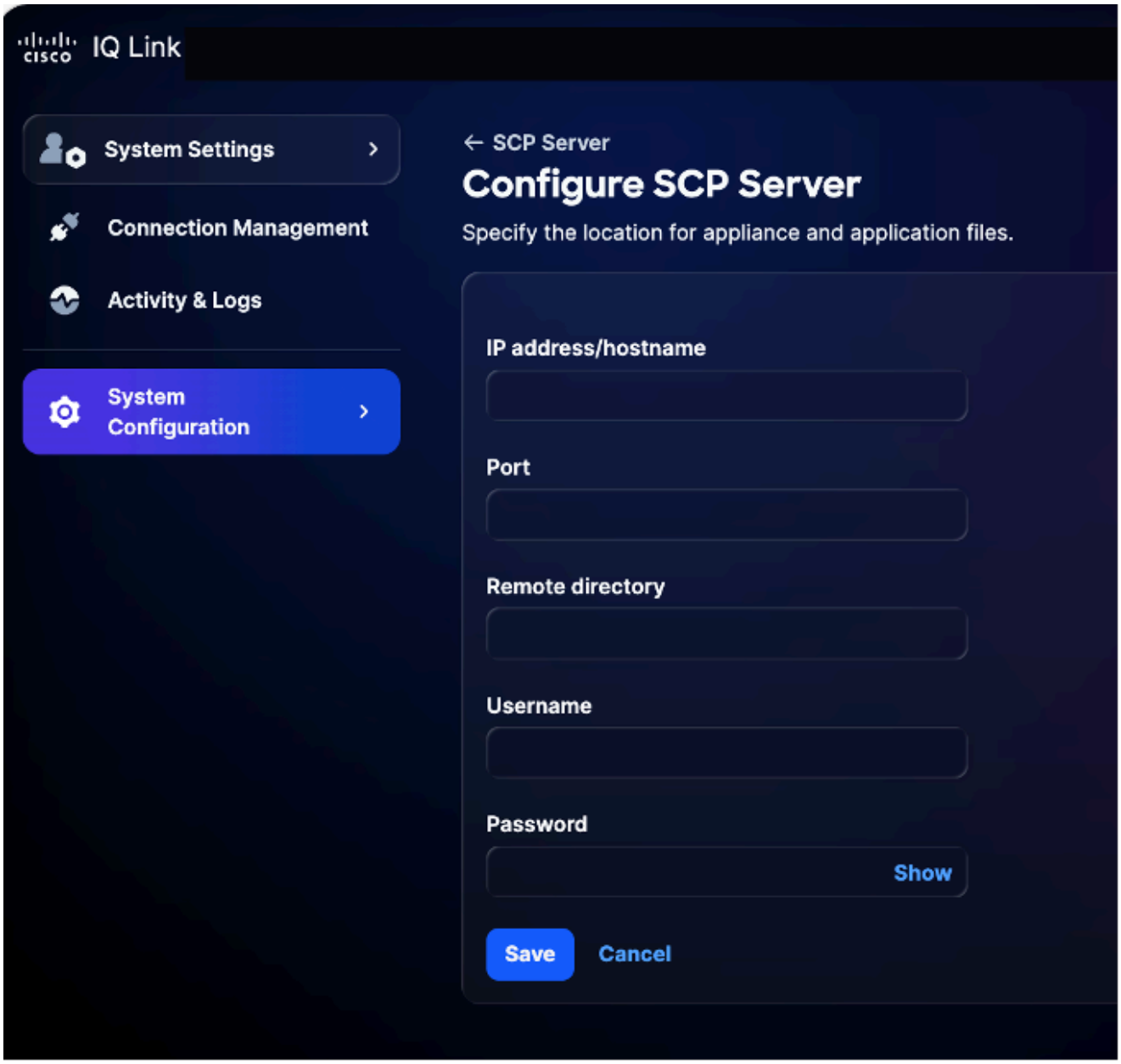
Pour ajouter un serveur SCP :

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



Page d'accueil du serveur SCP

2. Cliquez sur Configure SCP Server.



Configurer le serveur SCP

3. Saisissez l'adresse IP/le nom d'hôte.
4. Saisissez un numéro de port.
5. Entrez le répertoire distant.
6. Saisissez un nom d'utilisateur.
7. Saisissez un mot de passe.
8. Cliquez sur Save. Une confirmation s'affiche.

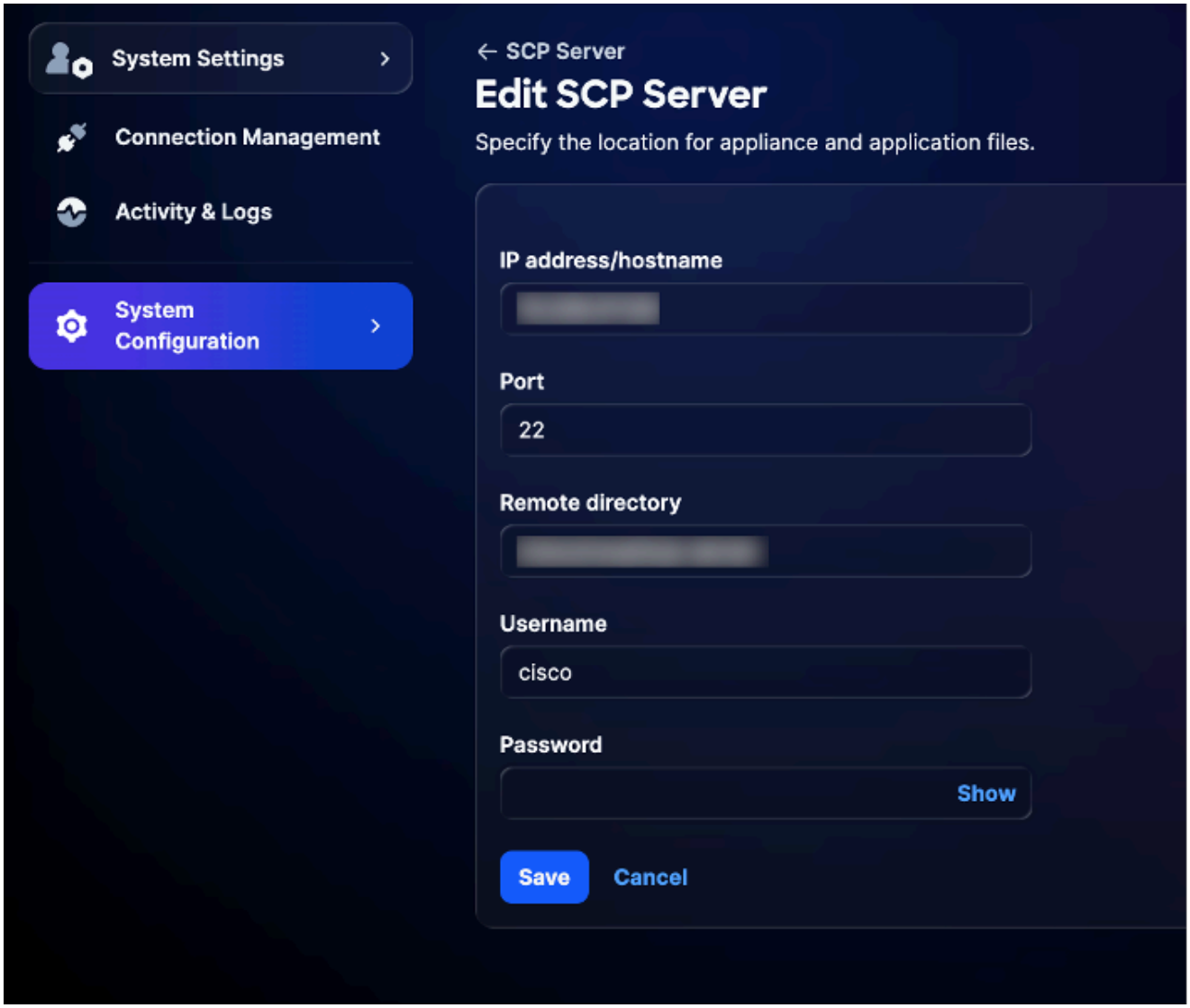
Modification des serveurs SCP existants

Pour modifier un serveur SCP existant :

1. Accédez à la page SCP Server.

Serveur SCP

2. Cliquez sur Edit pour le serveur SCP existant souhaité.



Modification du serveur SCP

3. Modifiez les détails selon vos besoins.

4. Cliquez sur Save.

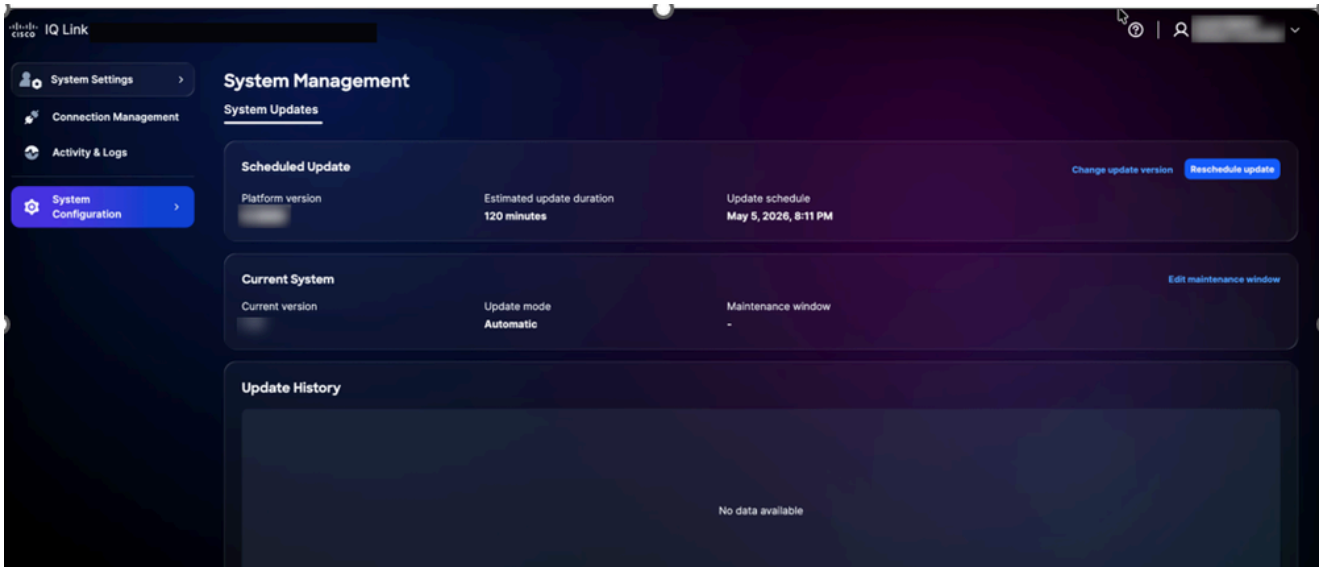
Gestion du système

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

Replanifier la mise à jour système

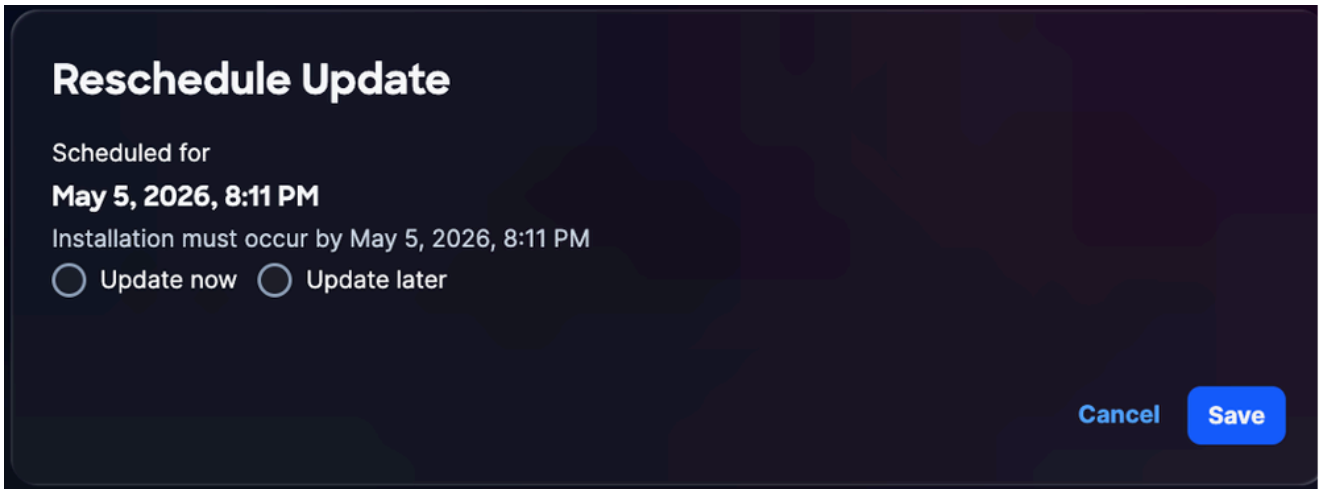
Pour replanifier la mise à jour du système :

1. Dans Administration, choisissez System Configuration > System Management. 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.



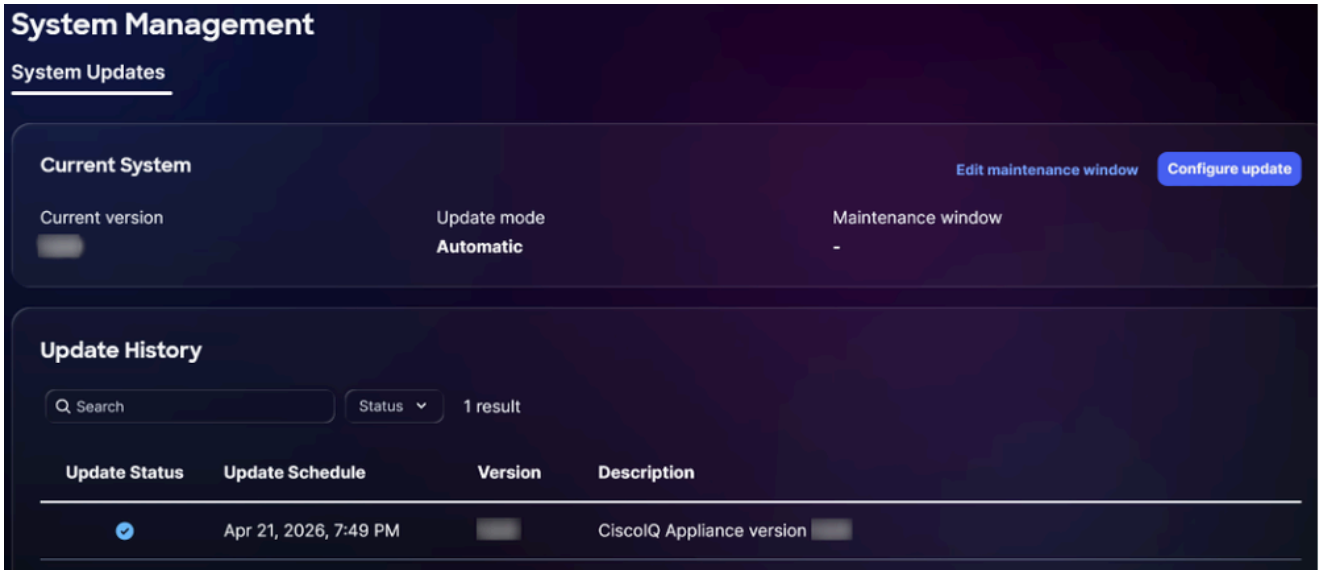
Mise à niveau du système

2. Cliquez sur Replanifier la mise à jour.



Reprogrammer la mise à niveau

3. Sélectionnez la case d'option Mettre à jour maintenant pour une replanification immédiate ou la case d'option Mettre à jour plus tard pour programmer une autre heure.
4. Cliquez sur Save. Une confirmation s'affiche et vous êtes redirigé vers la page d'accueil Mise à jour du système.

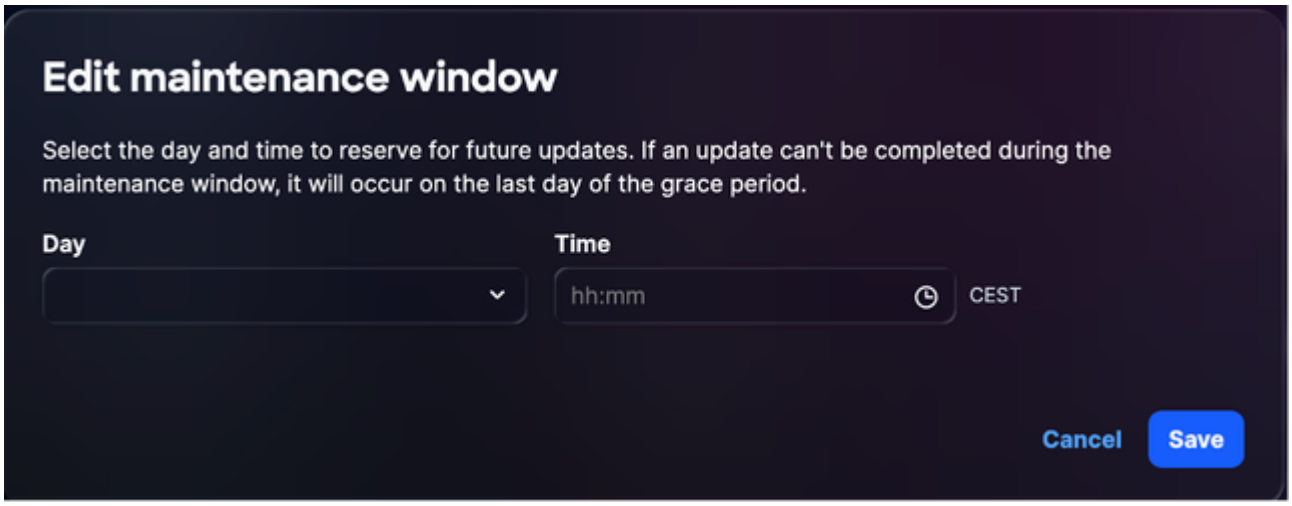


Mise à niveau réussie

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 :

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



Modifier la fenêtre de maintenance

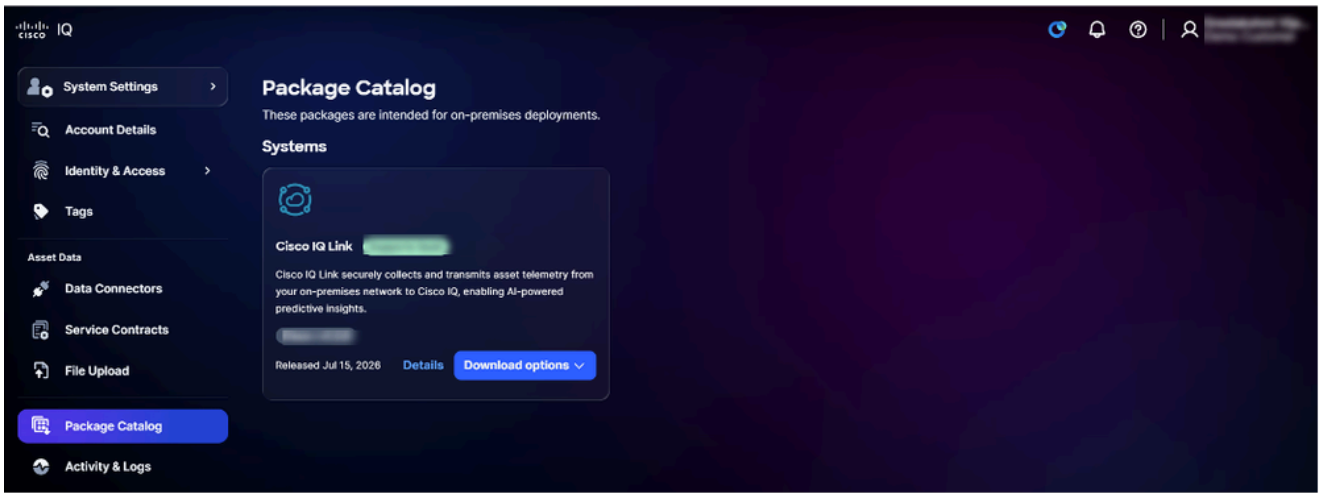
2. Choisissez une option dans les listes déroulantes Jour et Heure.
3. Cliquez sur Enregistrer. La fenêtre de maintenance a été planifiée avec succès. La mise à jour est déclenchée en fonction du calendrier affiché.

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.

Mise à niveau manuelle du système

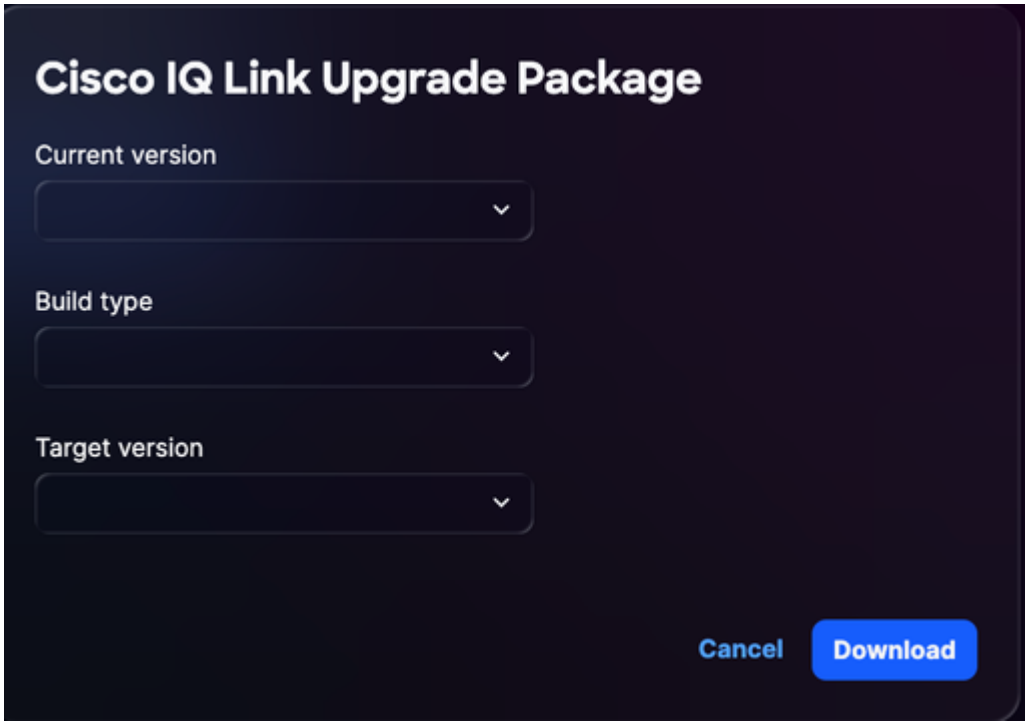
Dans les cas où la distribution automatique à partir de Cisco IQ SaaS n'est pas disponible ou est retardée, vous pouvez effectuer manuellement une mise à niveau du système en téléchargeant le bundle de mise à niveau directement à partir de Cisco IQ SaaS. Pour mettre à niveau manuellement le système :

1. Connectez-vous à Cisco IQ SaaS et choisissez Home > System Settings > Package Catalog.



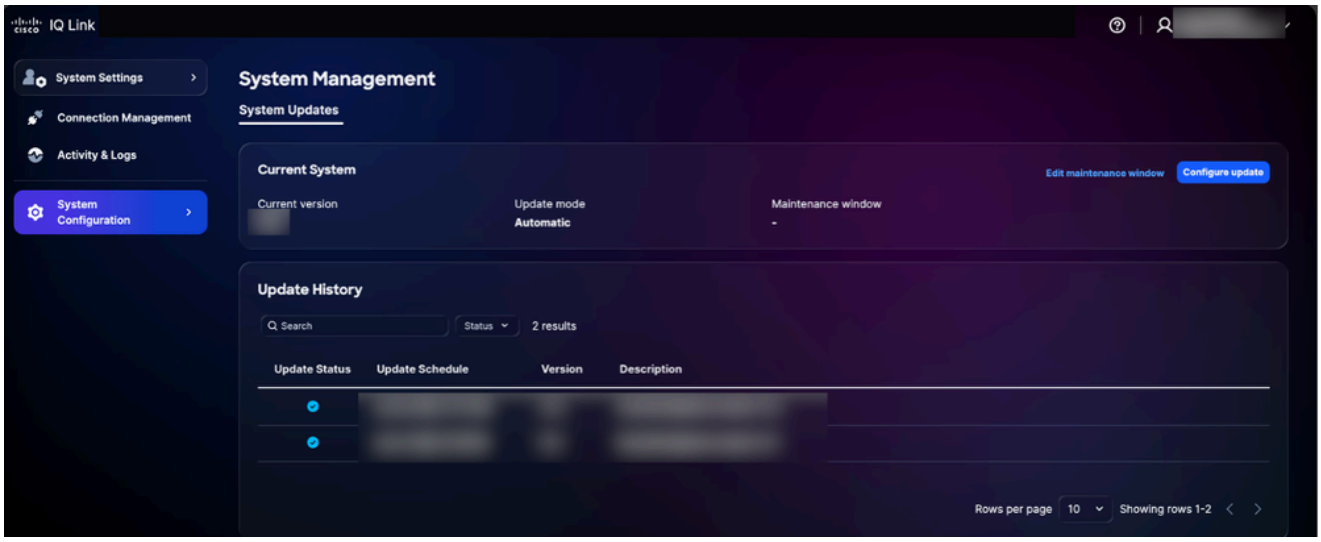
Catalogue de packages

2. Dans la section Cisco IQ Link, cliquez sur Download options > Upgrade packages.



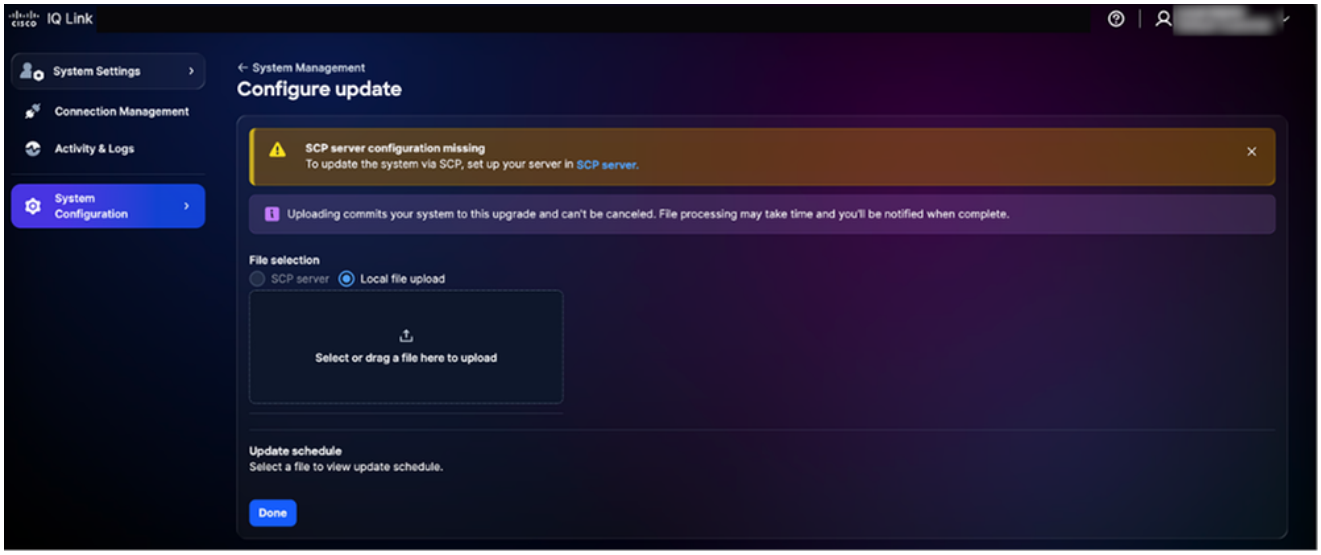
Package de mise à niveau

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



Configurer la mise à jour

9. Cliquez sur Configurer la mise à jour.



Téléchargement de fichier local

10. Activez la case d'option Téléchargement de fichier local.
11. Sélectionnez ou faites glisser le fichier de bundle de mise à niveau téléchargé dans le champ de téléchargement.
12. Cliquez sur Terminé. Un message de confirmation s'affiche une fois que le système a été mis à jour.

Configuration des certificats SSL

Un certificat auto-signé par défaut est préinstallé et activé dans Cisco IQ, mais vous pouvez 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.

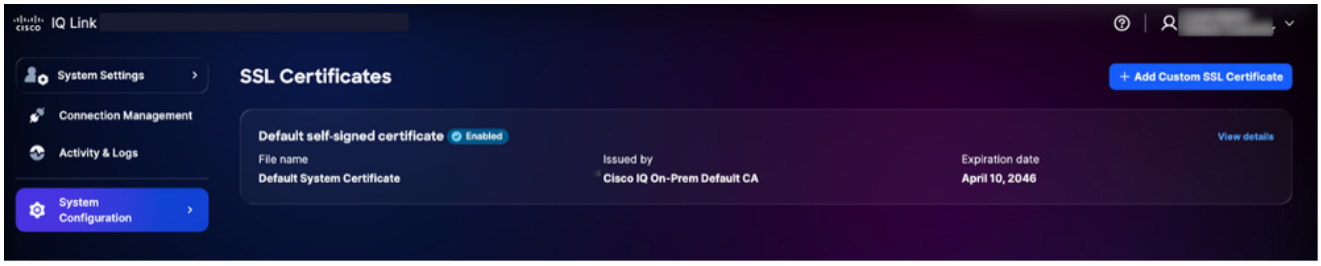
Remarque : Le certificat doit avoir au moins 90 jours de validité restants. Un certificat est considéré comme « proche de l'expiration » lorsqu'il lui reste moins de 90 jours avant son expiration.

Après avoir ajouté, modifié ou supprimé un certificat SSL, vous devez télécharger le nouveau certificat SSL comme indiqué dans la Configuration de déconnexion unique pour l'IDP Okta ou l'IDP ADFS.

Ajout d'un certificat SSL personnalisé

Pour ajouter un certificat SSL personnalisé :

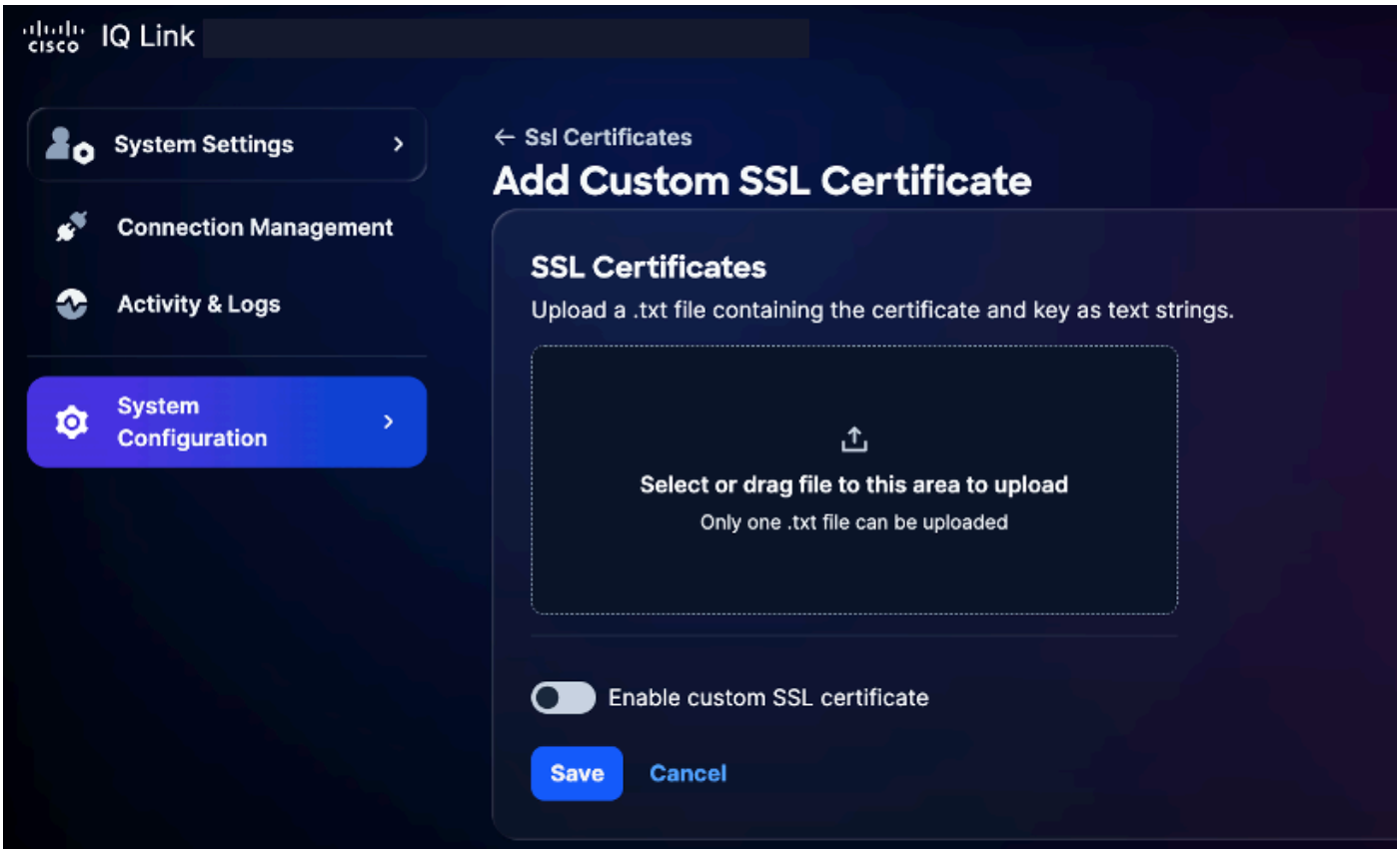
1. Dans Paramètres système, choisissez Configuration système > Certificats SSL. La page SSL Certificates s'affiche et répertorie tous les certificats SSL de votre système.



Ajout du certificat SSL

2. Cliquez sur Ajouter un certificat SSL personnalisé.

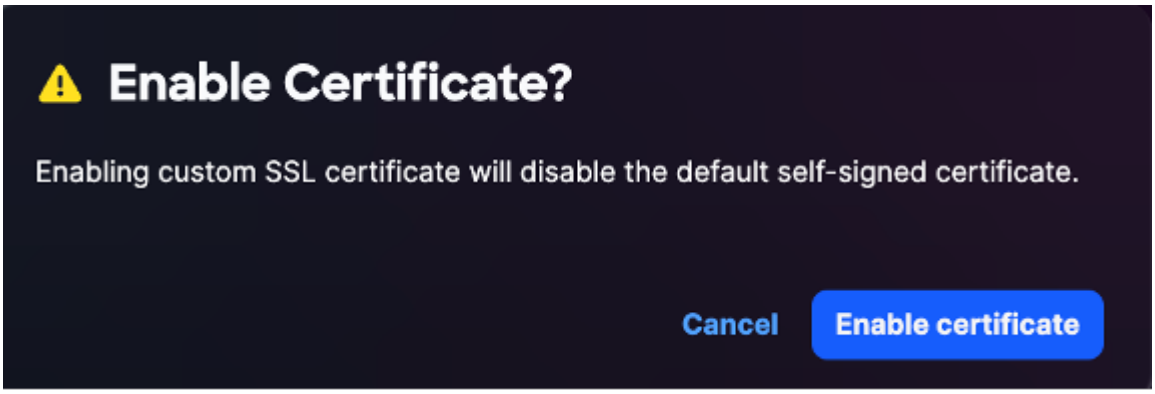
Remarques :
- Télécharger un fichier .txt qui inclut le certificat et la clé codés par messagerie Privacy-Enhanced sous forme de chaînes de texte
- Un seul fichier .txt peut être téléchargé à la fois
- Le fichier doit contenir le certificat et la clé privée



Télécharger le certificat SSL

3. Faites glisser et déposez ou téléchargez le certificat SSL personnalisé dans le champ Certificat SSL.

4. Activez le bouton bascule Activer le certificat SSL personnalisé.



Modifier le certificat SSL

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

5. Cliquez sur Enable certificate.

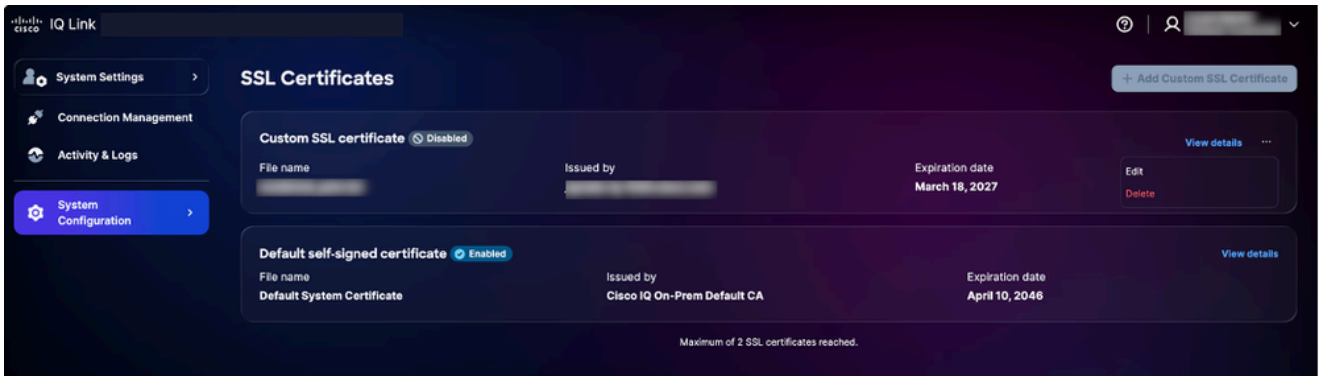
6. Cliquez sur Enregistrer.

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

Modification des certificats SSL personnalisés

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.



Modifier le certificat SSL

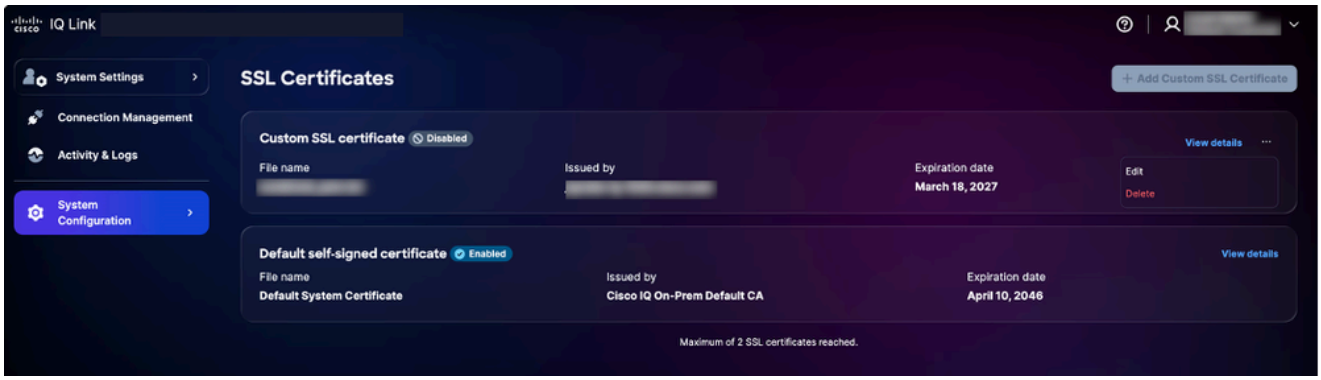
2. Cliquez sur l'icône Autres options > Modifier. La page Edit SSL Certificate s'affiche.
3. Modifiez les détails du certificat selon les besoins.
4. Cliquez sur Save.

Suppression de certificats SSL personnalisés

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 personnalisé souhaité.



Supprimer le certificat SSL

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

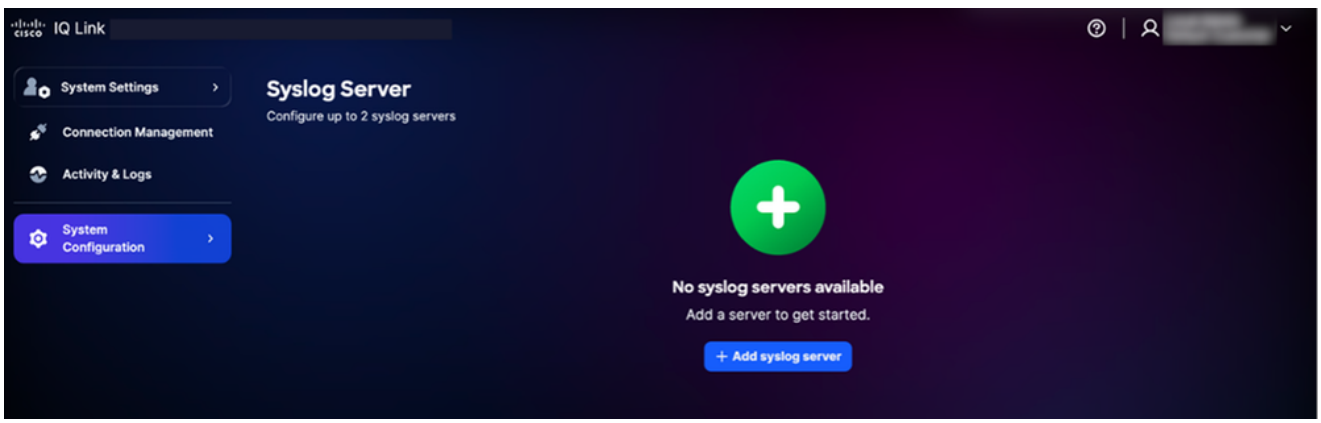
Les utilisateurs dotés du rôle Administrateur de compte peuvent configurer des serveurs syslog externes pour exporter les journaux système. Vous pouvez configurer jusqu'à deux (2) serveurs syslog.

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

Ajout de serveurs Syslog

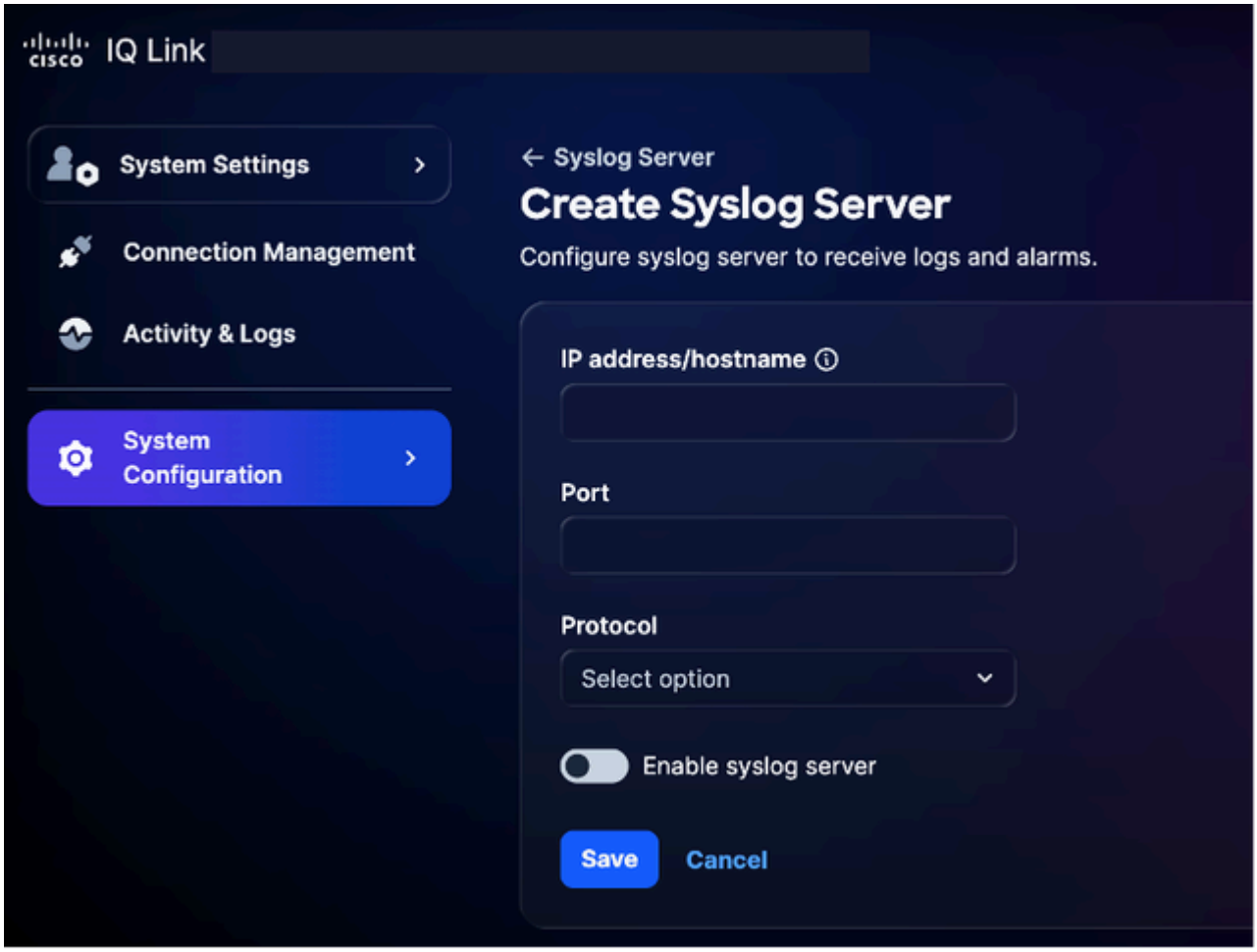
Pour ajouter un serveur Syslog :

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

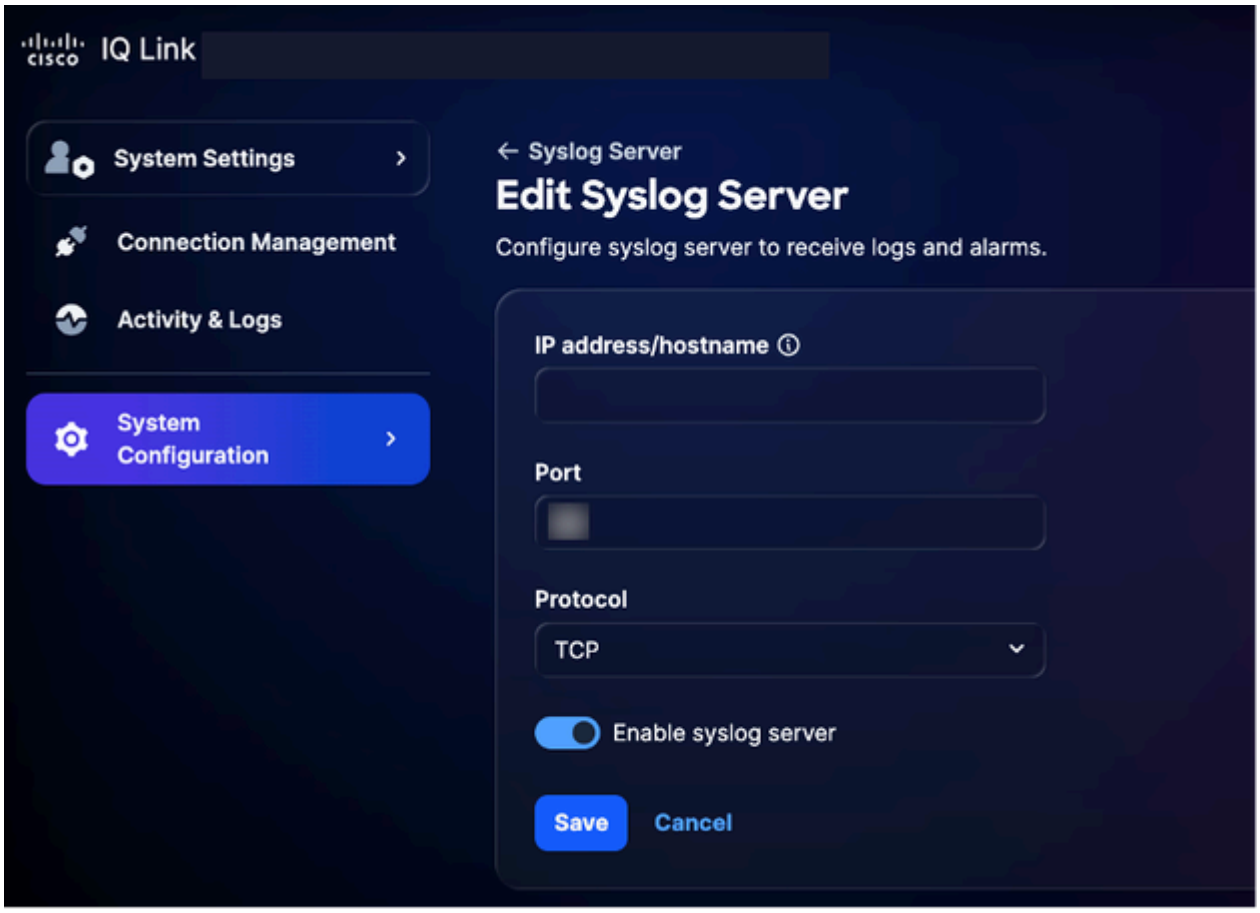
3. Saisissez l'adresse IP/le nom d'hôte.
4. Saisissez un numéro de port.
5. Sélectionnez le protocole applicable dans la liste déroulante Protocol (par exemple, UDP ou TCP).
6. Activez le bouton bascule Activer le serveur Syslog.
7. Cliquez sur Save. Une confirmation s'affiche et le nouveau serveur Syslog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

Modification des serveurs Syslog configurés

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.



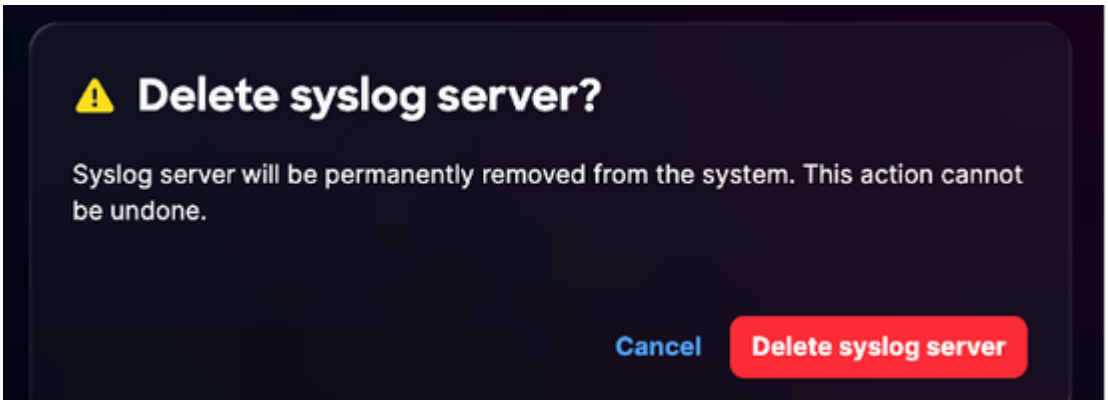
Modifier le serveur Syslog

3. Modifiez les détails ou désactivez le bouton Enable syslog server, selon les besoins.
4. Cliquez sur Save.

Suppression des serveurs Syslog configurés

Pour supprimer un serveur syslog configuré :

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

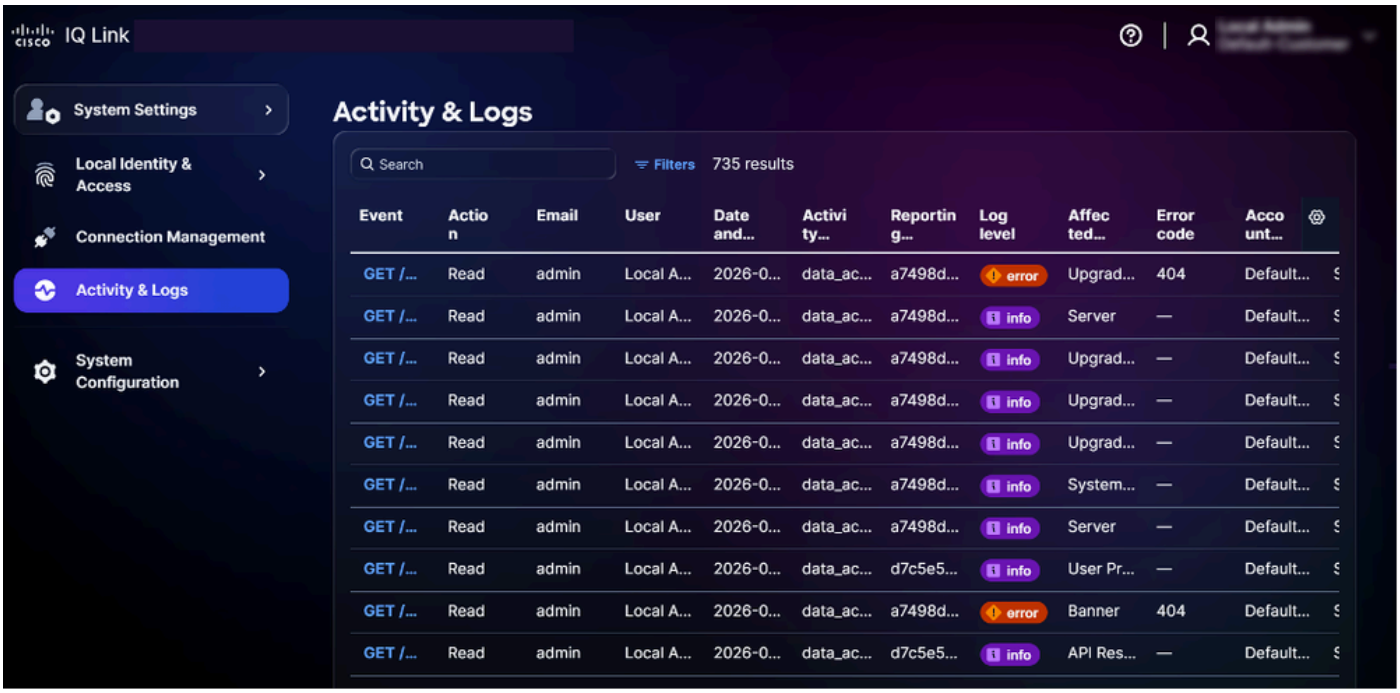


Confirmation

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.



Activité et journaux

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

Exercice et journaux :

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

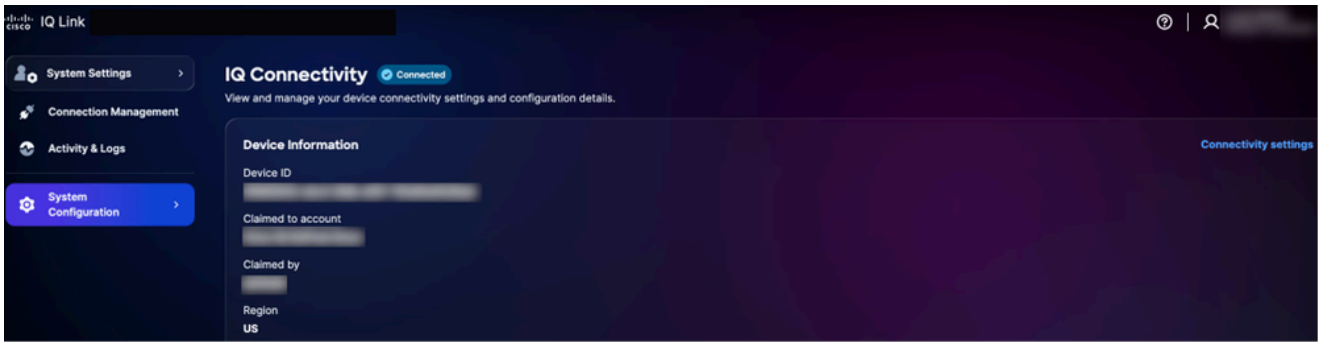
Les options de filtre suivantes sont disponibles :

- Date : Filtre les journaux dans une plage de temps spécifique
- Niveau du journal : 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 : Filtre les journaux pour un code d'erreur spécifique

Connectivité IQ

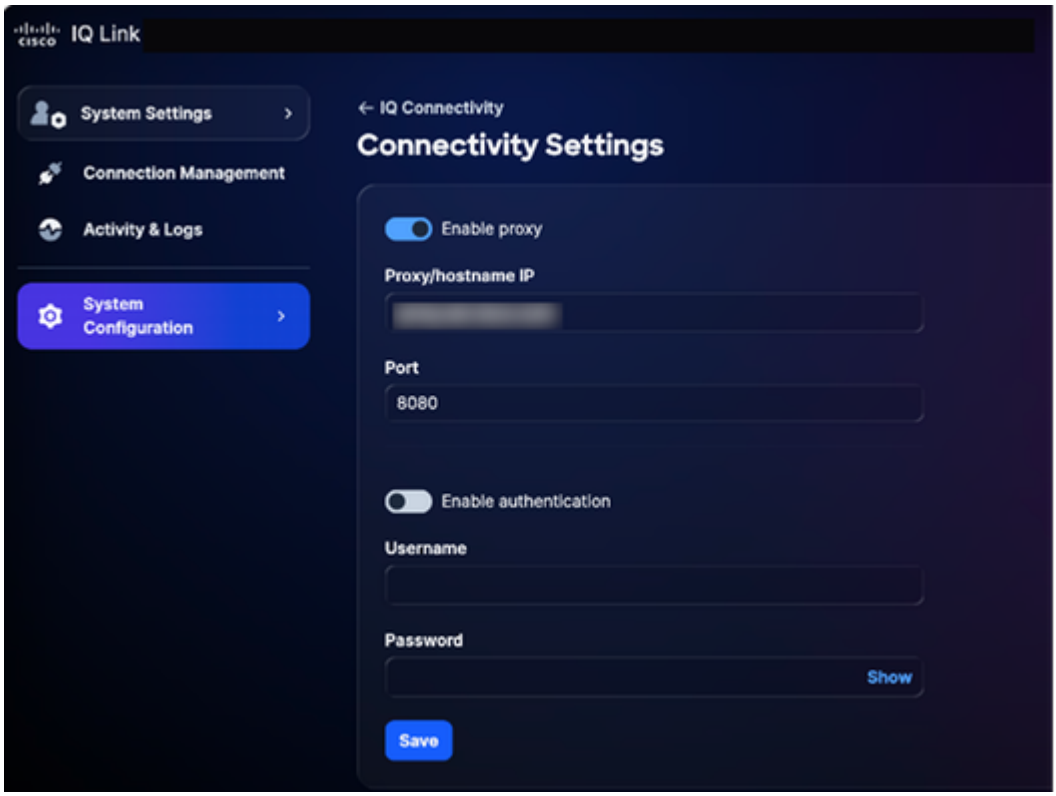
Pour afficher et gérer les paramètres de connectivité et les détails de configuration de votre périphérique :

1. Dans Paramètres système, choisissez Configuration système > Connectivité IQ. La page IQ Connectivity s'affiche.



Connectivité IQ

2. Cliquez sur Connectivity settings.



Paramètres de connectivité

3. Mettez à jour les détails si nécessaire.
4. Cliquez sur Save.

Gestion des connexions (collecte de données)

Cisco IQ Link est une solution sur site de collecte de données réseau, conçue pour offrir 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 est résumée ci-dessous :

- 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

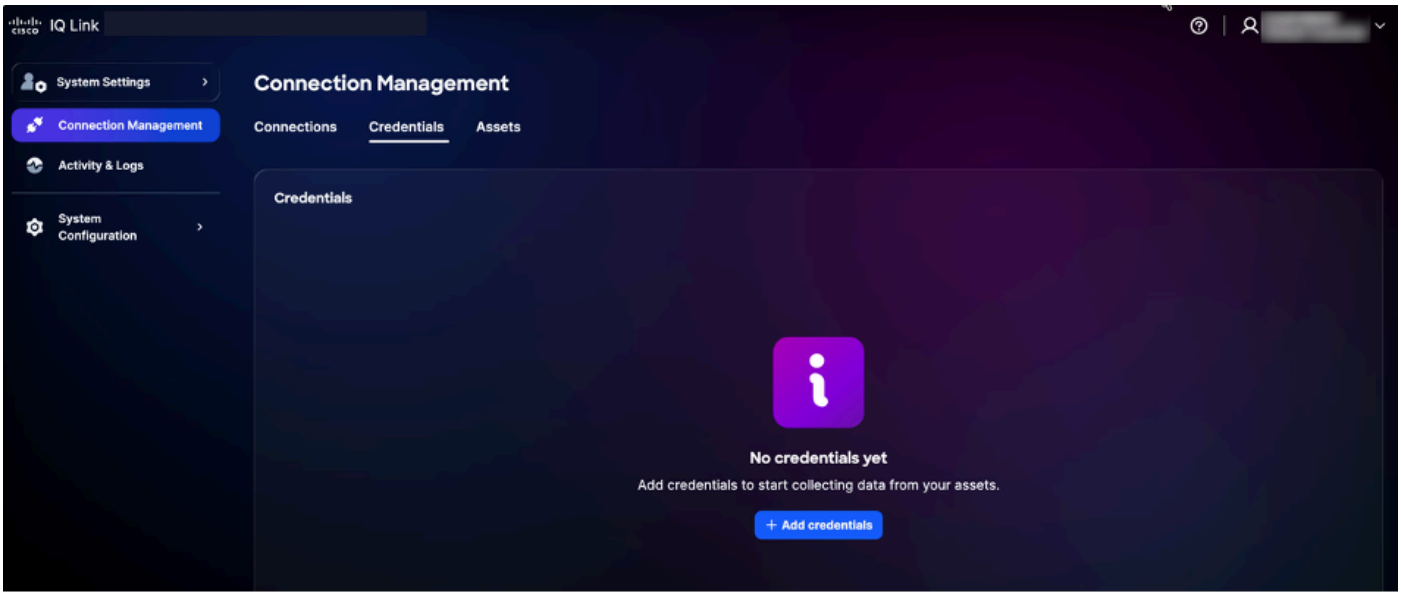
garantit que votre configuration reste précise au fur et à mesure que votre réseau se développe.

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

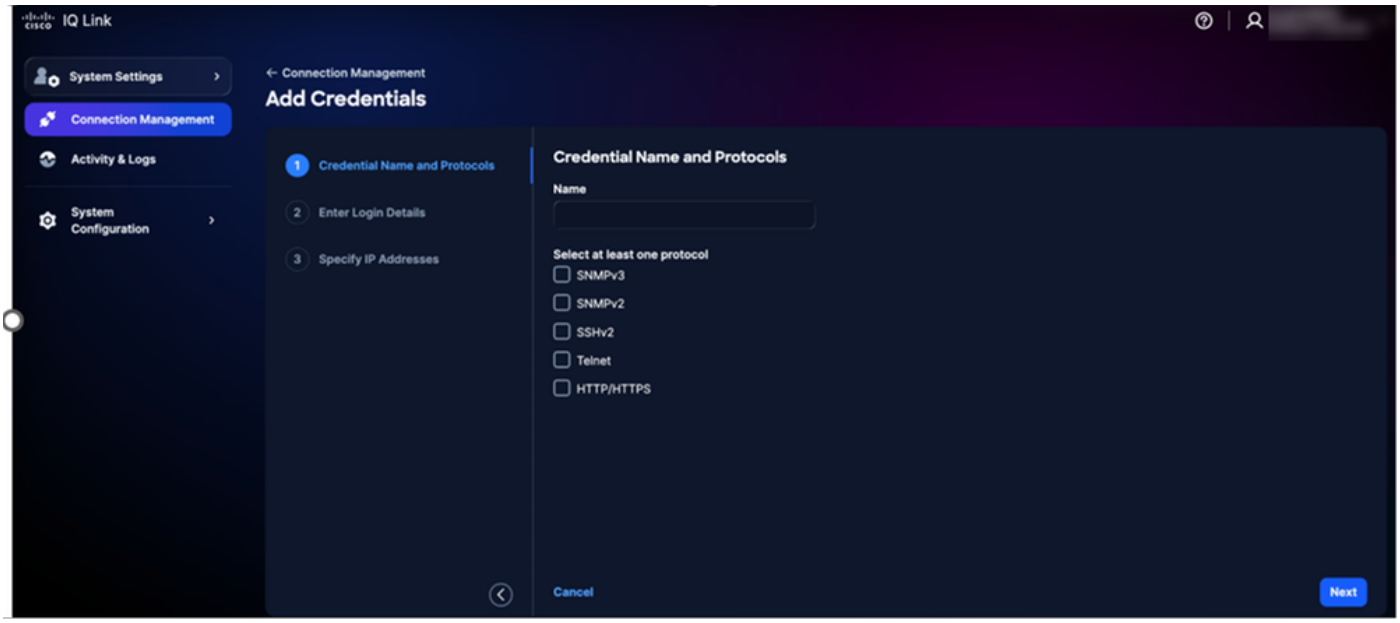
Vous devez d'abord ajouter des informations d'identification pour collecter des données. Pour ajouter des informations d'identification :

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.

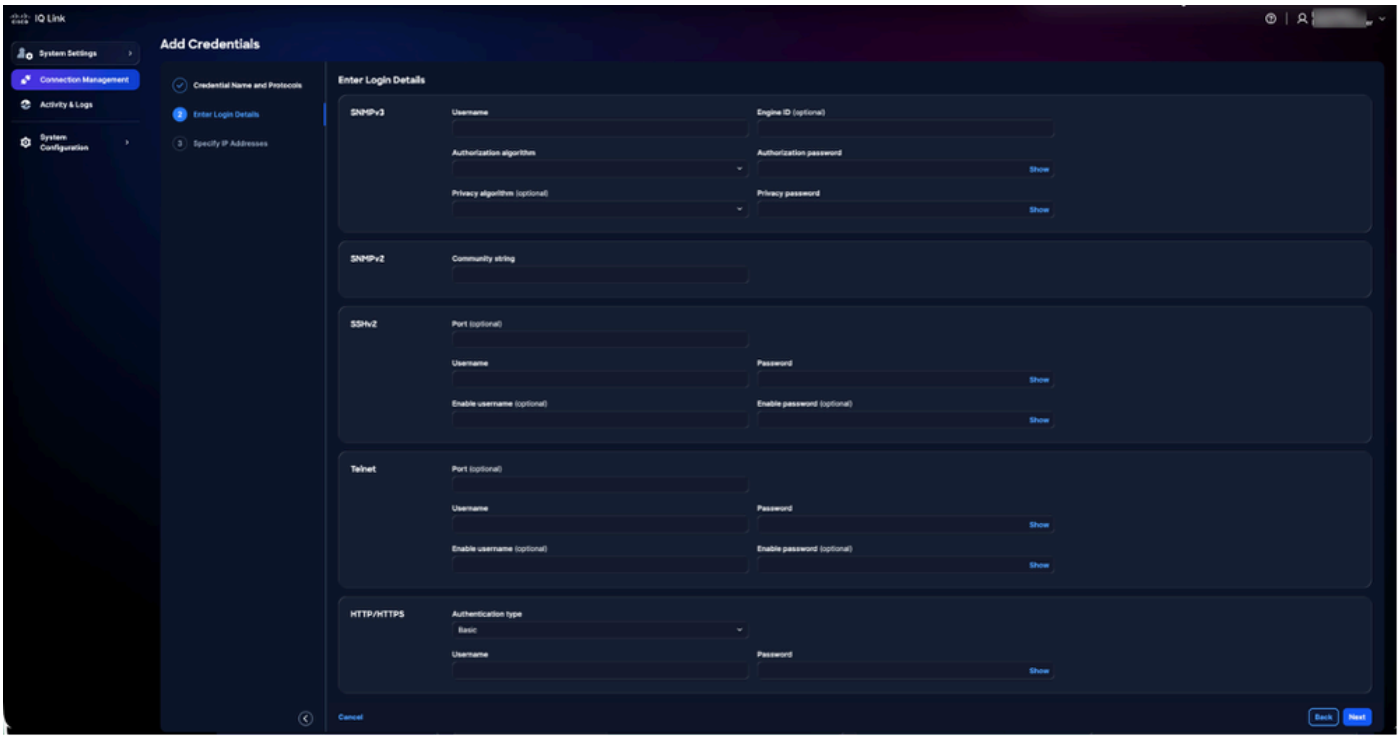


Ajouter des identifiants

4. Saisissez un nom.

5. Cochez toutes les cases du protocole applicable.

6. Cliquez sur Suivant.

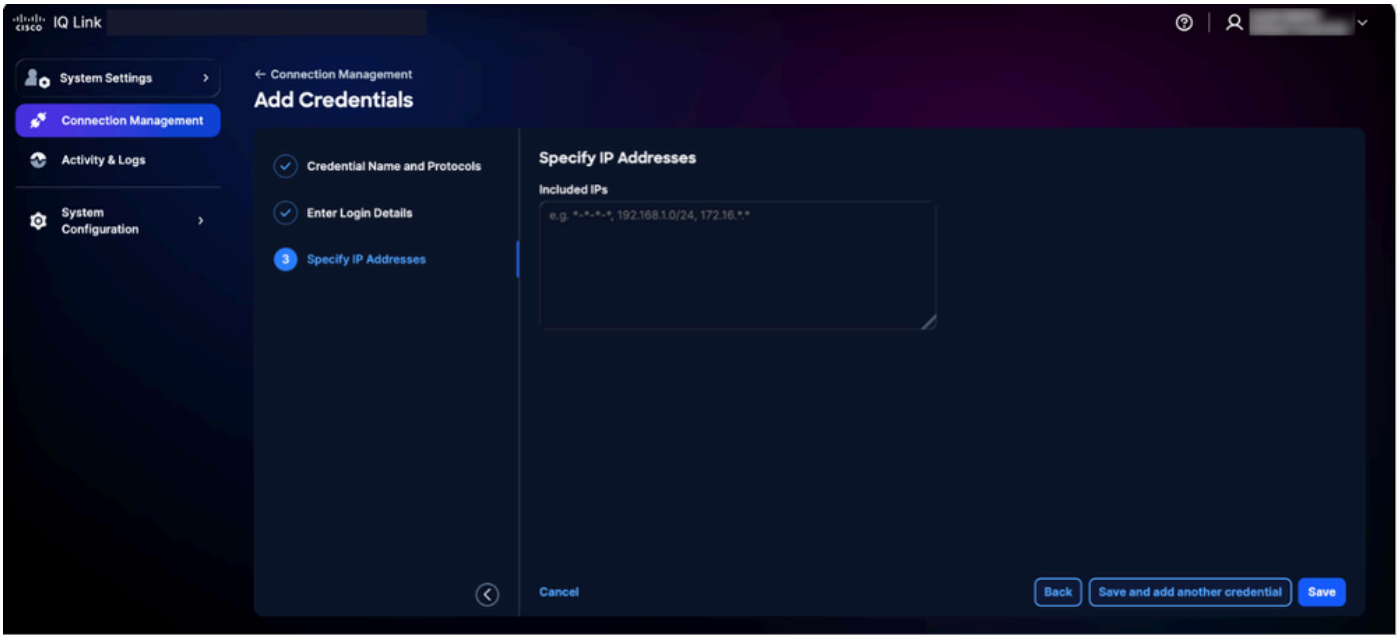


Ajouter des informations d'identification

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 spécifiques que vous avez choisis.

7. Entrez les détails de connexion pour chaque protocole sélectionné.

8. Cliquez sur Suivant.

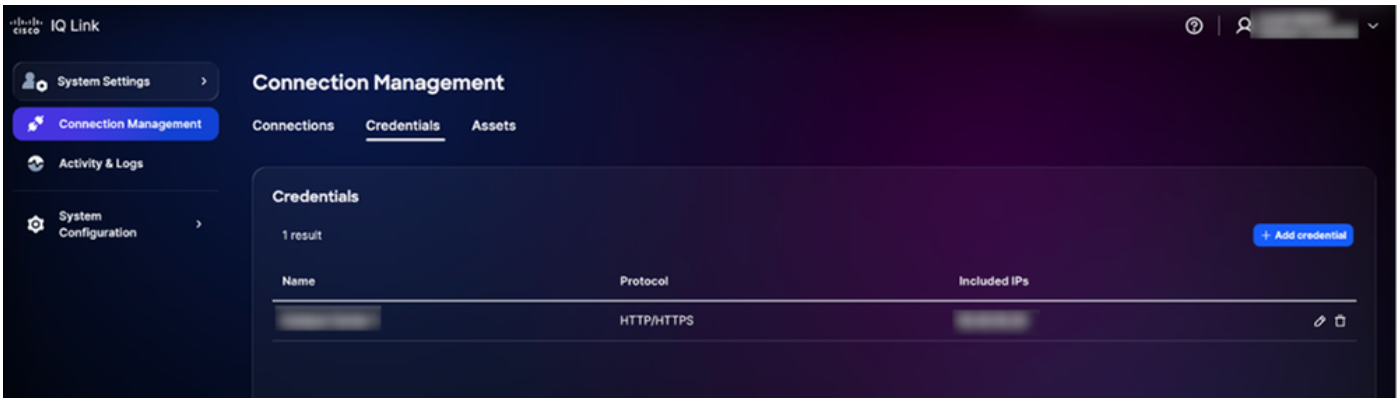


Spécifier les adresses IP

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 Enregistrer. 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 parmi les caractères génériques)

    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 13 : 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)

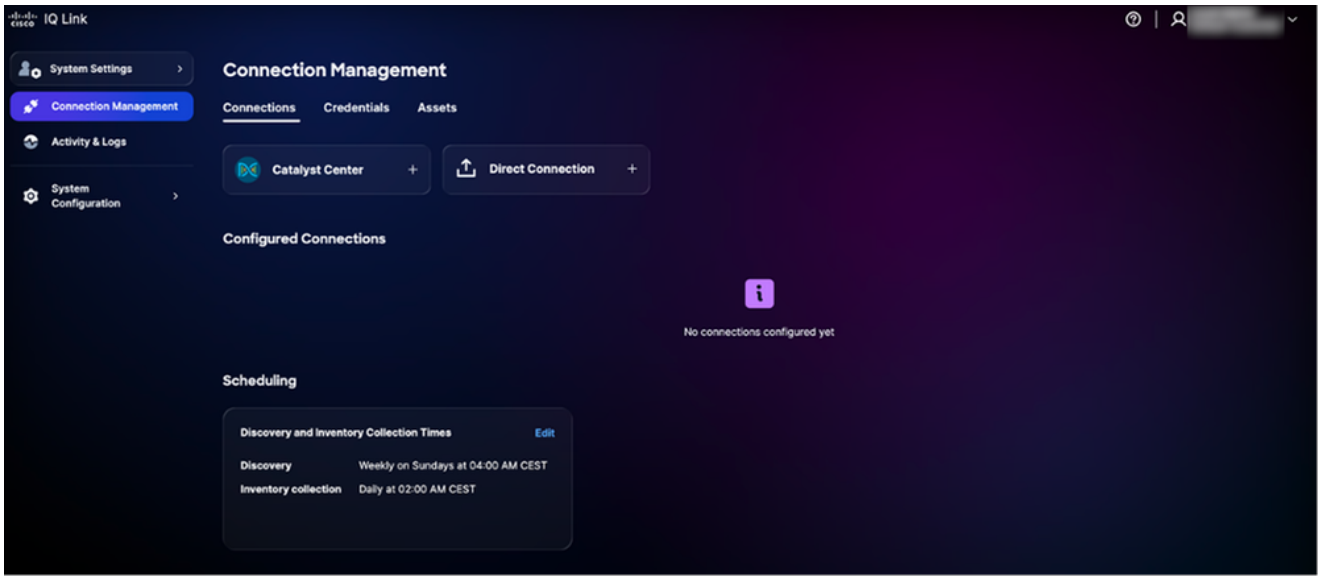
Remarque : Si un périphérique appartient à plusieurs catégories qui se chevauchent, le système sélectionne toujours l'ensemble d'informations d'identification ayant la plus grande spécificité (en d'autres termes, le moins de caractères génériques de fin).

Collecte de données avec Catalyst Center

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

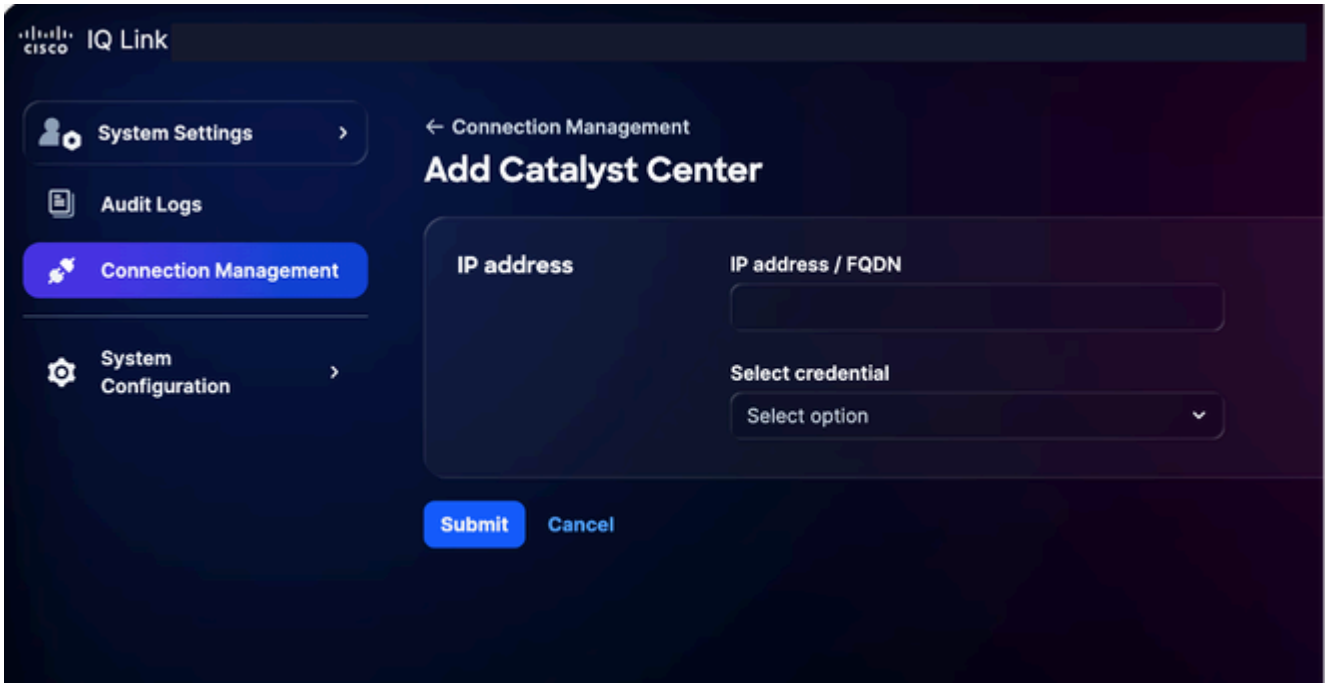
Pour la collecte de données avec Catalyst Center :

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



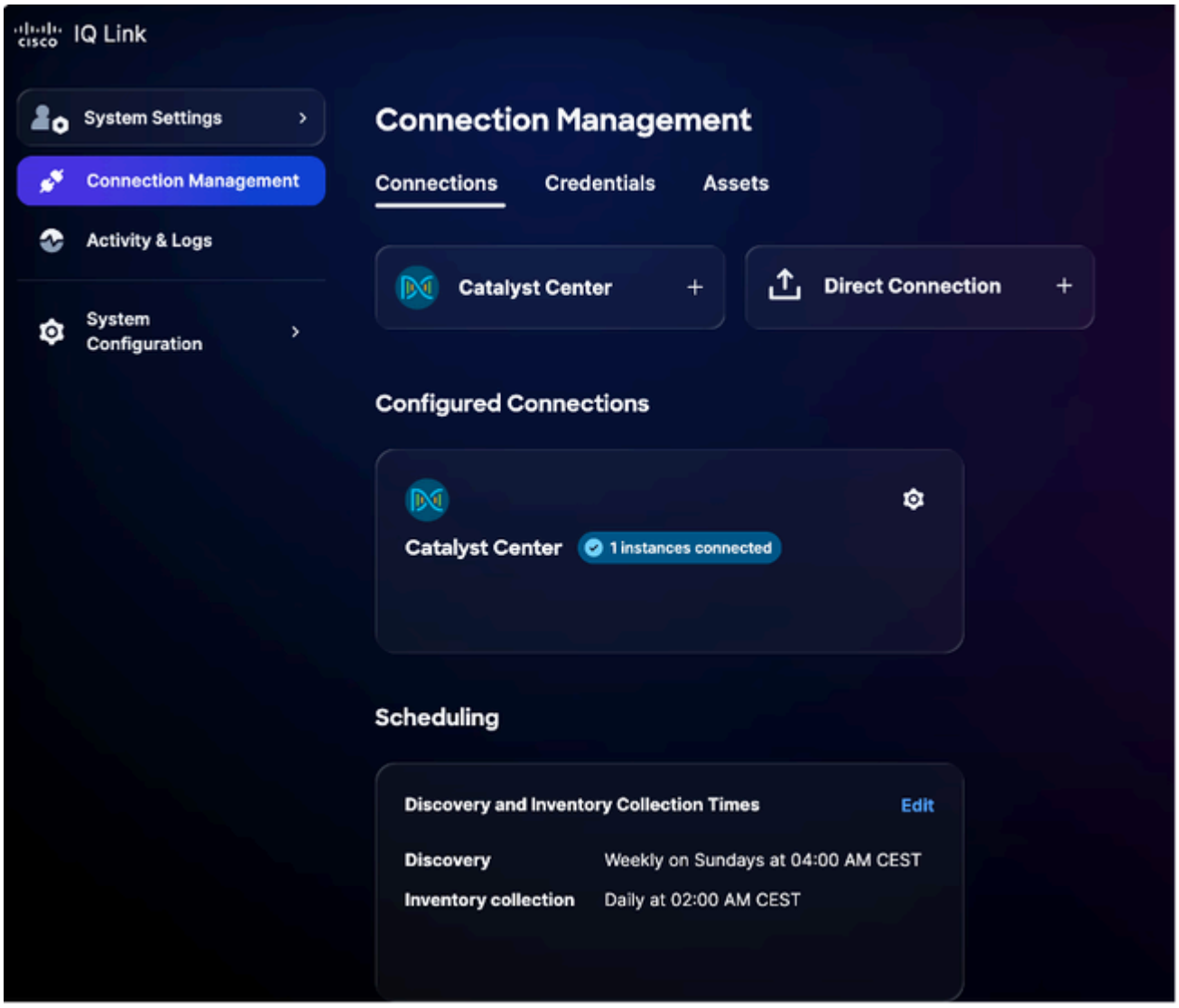
Gestion des connexions

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.
5. Cliquez sur Submit. Une confirmation s'affiche (cela peut prendre jusqu'à 75 minutes). Vous pouvez afficher le Catalyst Center nouvellement ajouté sous Connexions configurées.



Ajout réussi de Catalyst Center

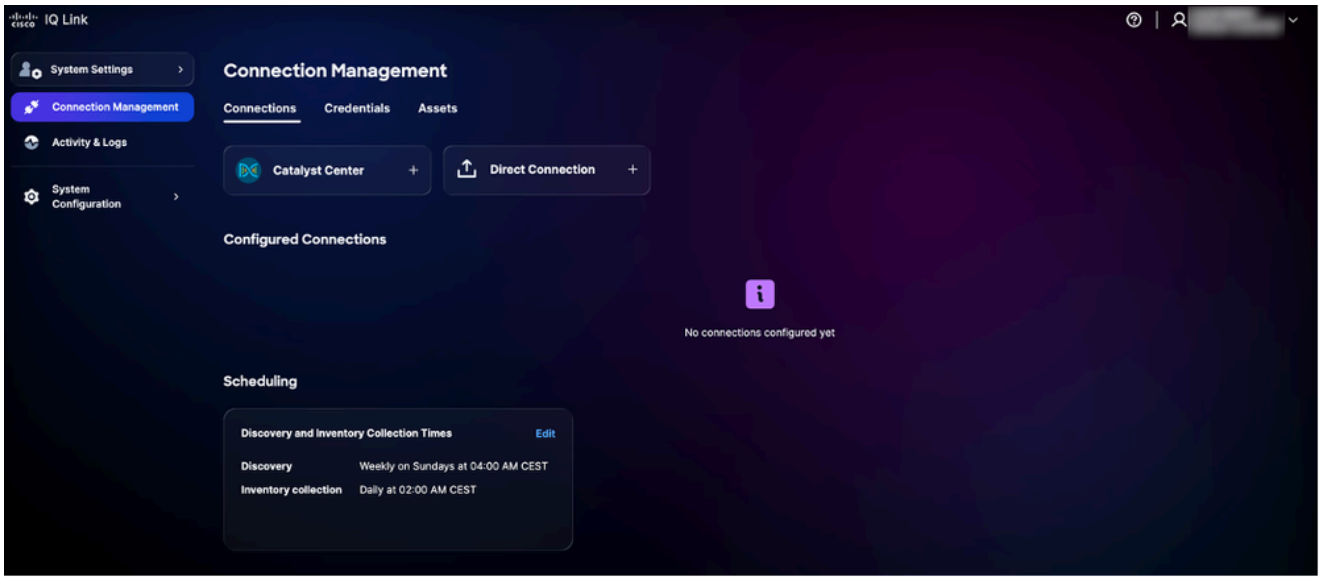
6. Planifier une collecte. Voir Planification pour plus de détails.

Remarque : Cisco IQ Link 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.

Connexion directe

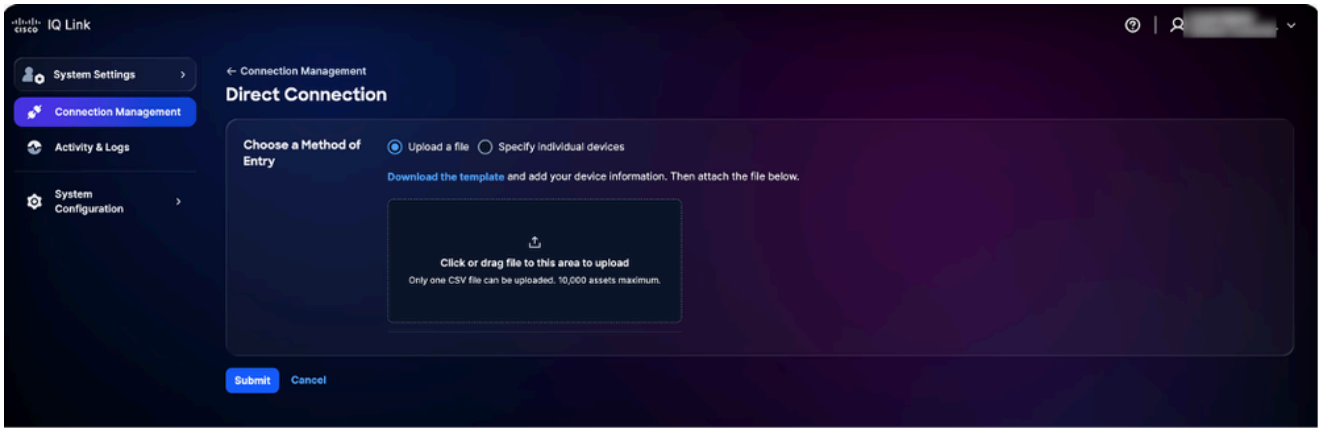
Pour ajouter des périphériques pour une connexion directe :

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



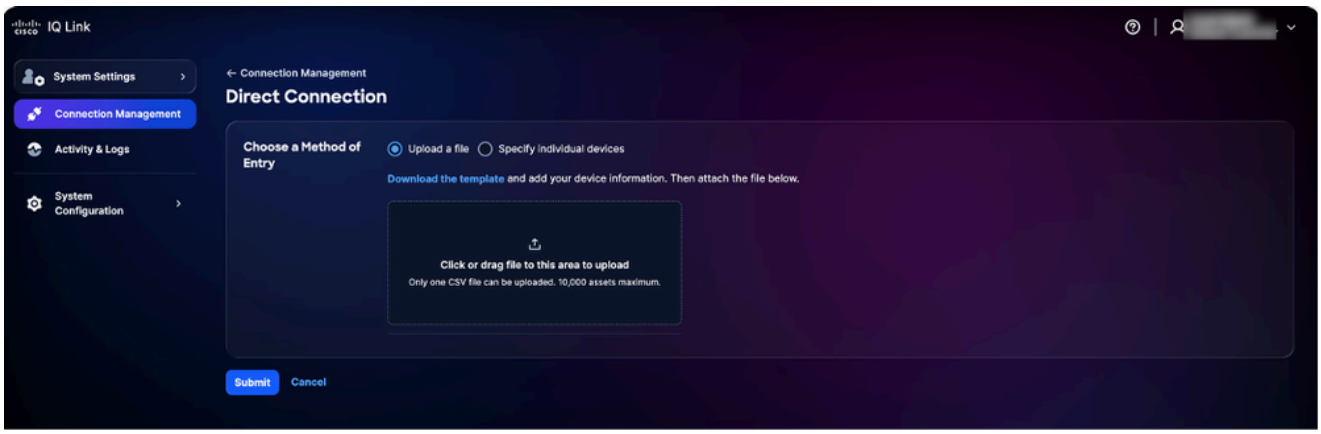
Gestion des connexions

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



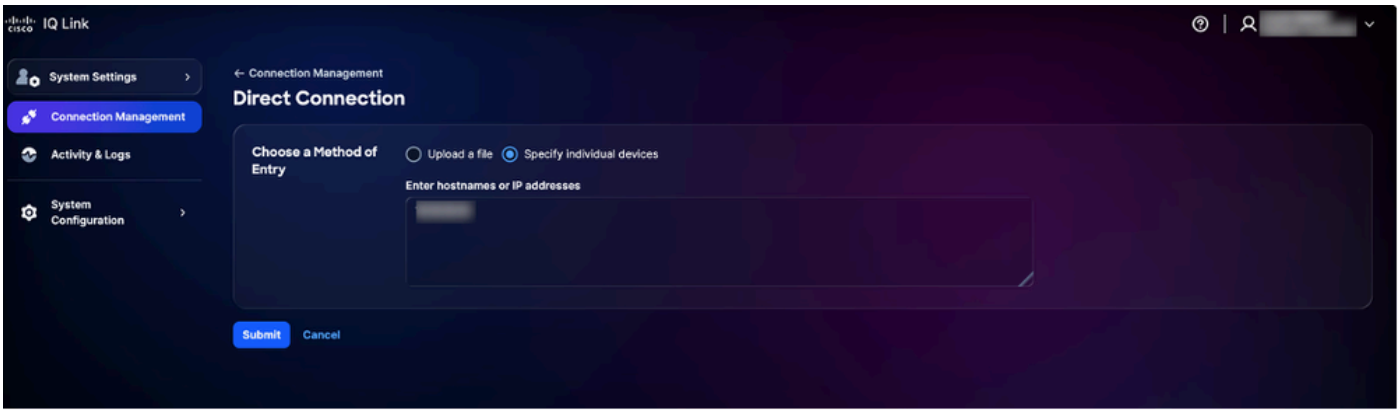
Télécharger le fichier

3. Cliquez sur l'option préférée pour Choisir une méthode d'entrée et envoyez vos périphériques en utilisant l'une des méthodes suivantes :



Télécharger un fichier

- Télécharger un fichier : Cliquez ou faites glisser le fichier et cliquez sur Envoyer



Spécifier des périphériques individuels

- Spécifier les périphériques individuels : Entrez un nom d'hôte unique, des adresses IP ou une liste de noms d'hôtes et/ou d'adresses IP séparés par des virgules, puis cliquez sur Submit

Vous êtes redirigé vers l'onglet Actifs après l'envoi réussi.

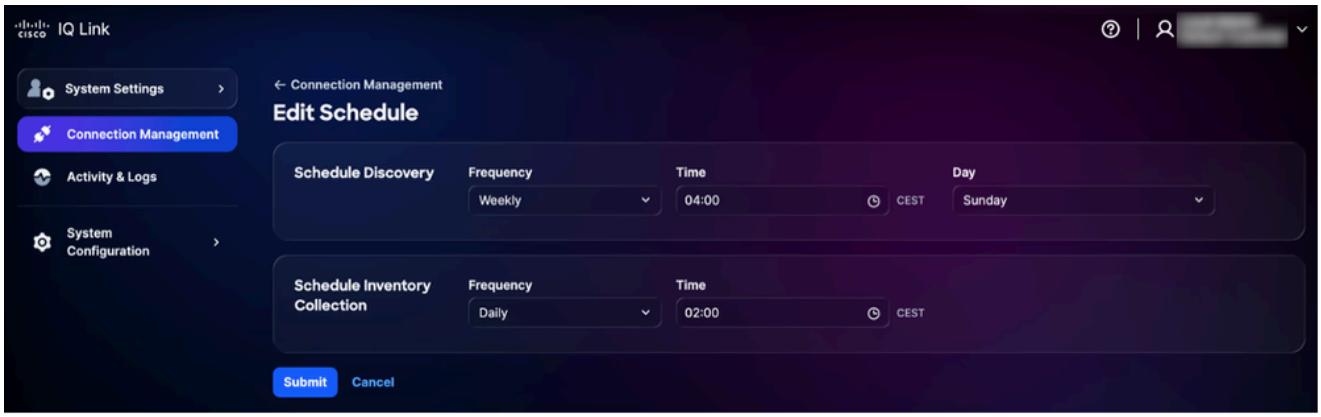
4. Programmez une collecte. Voir Planification pour plus de détails.

Remarque : Cisco IQ Link 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.

Planification

La planification vous permet de définir quand Cisco IQ Link effectue la collecte automatique 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.



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 : Attendez 5 à 10 minutes que les modifications apportées aux calendriers de détection ou de collecte soient synchronisées et reflétées avec précision dans Cisco IQ Link.

Bannières

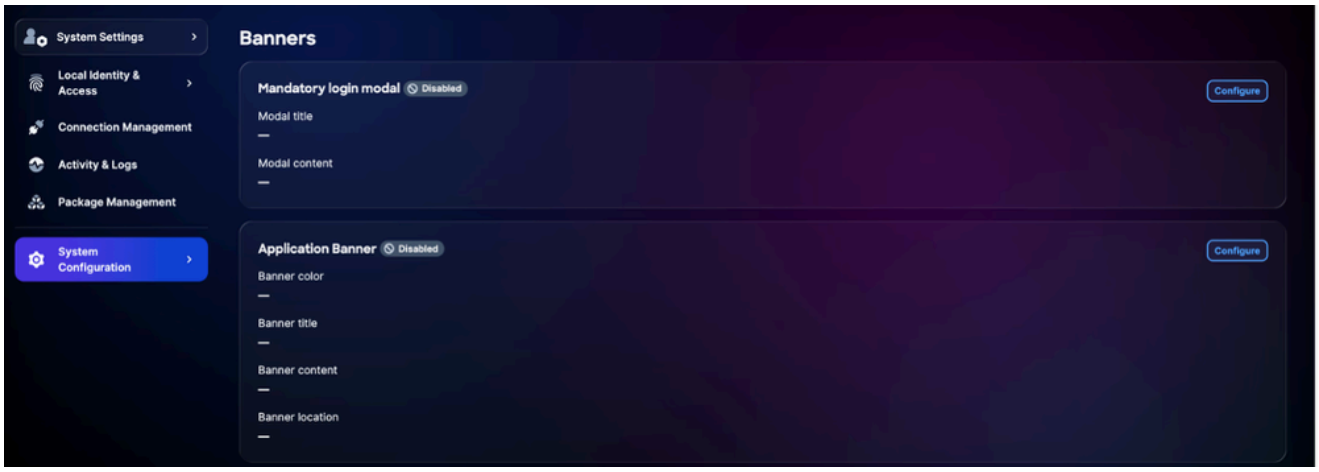
Les administrateurs de comptes peuvent configurer des bannières à l'échelle du système pour répondre aux normes de sécurité et de conformité.

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

Configuration des bannières modales de connexion obligatoire

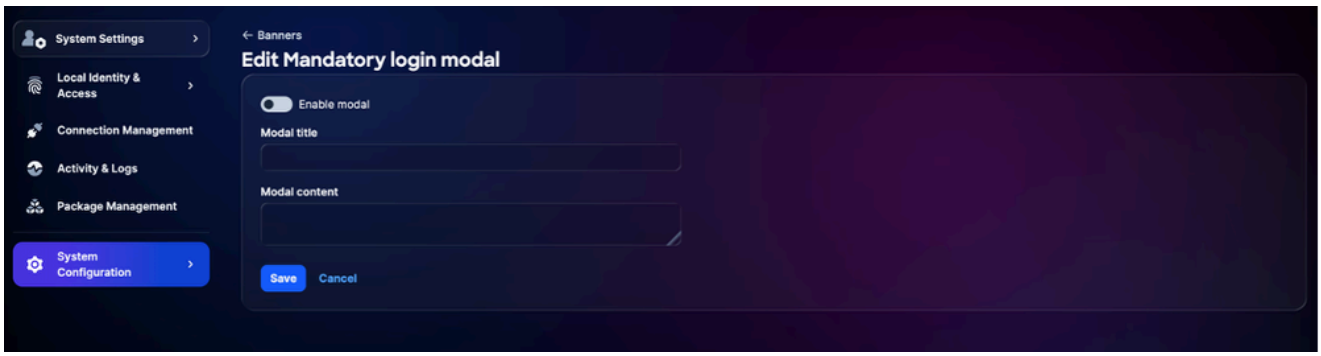
Pour configurer une bannière obligatoire :

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.



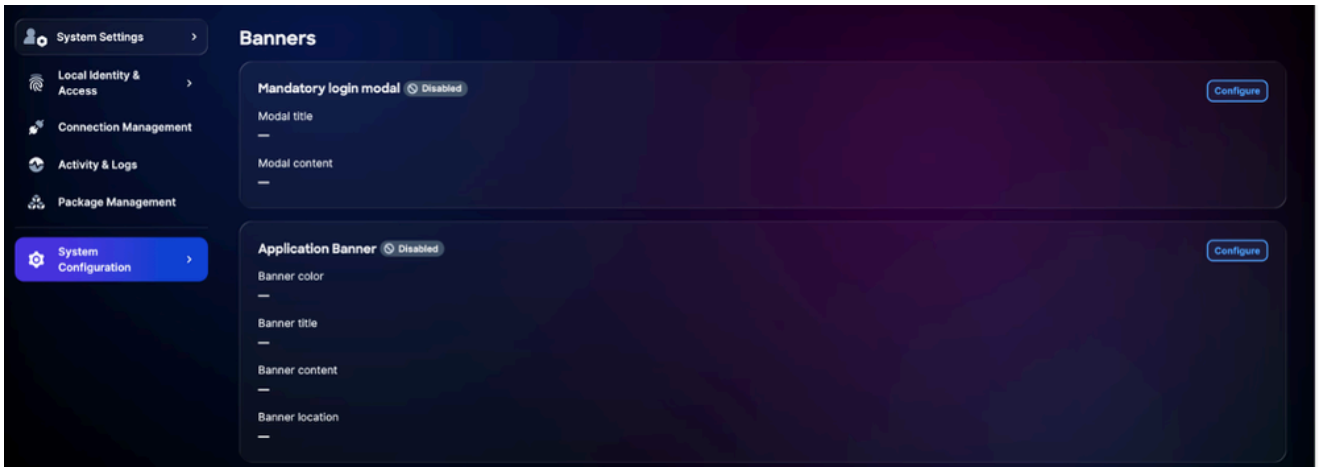
Modifier la bannière modale de connexion obligatoire

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

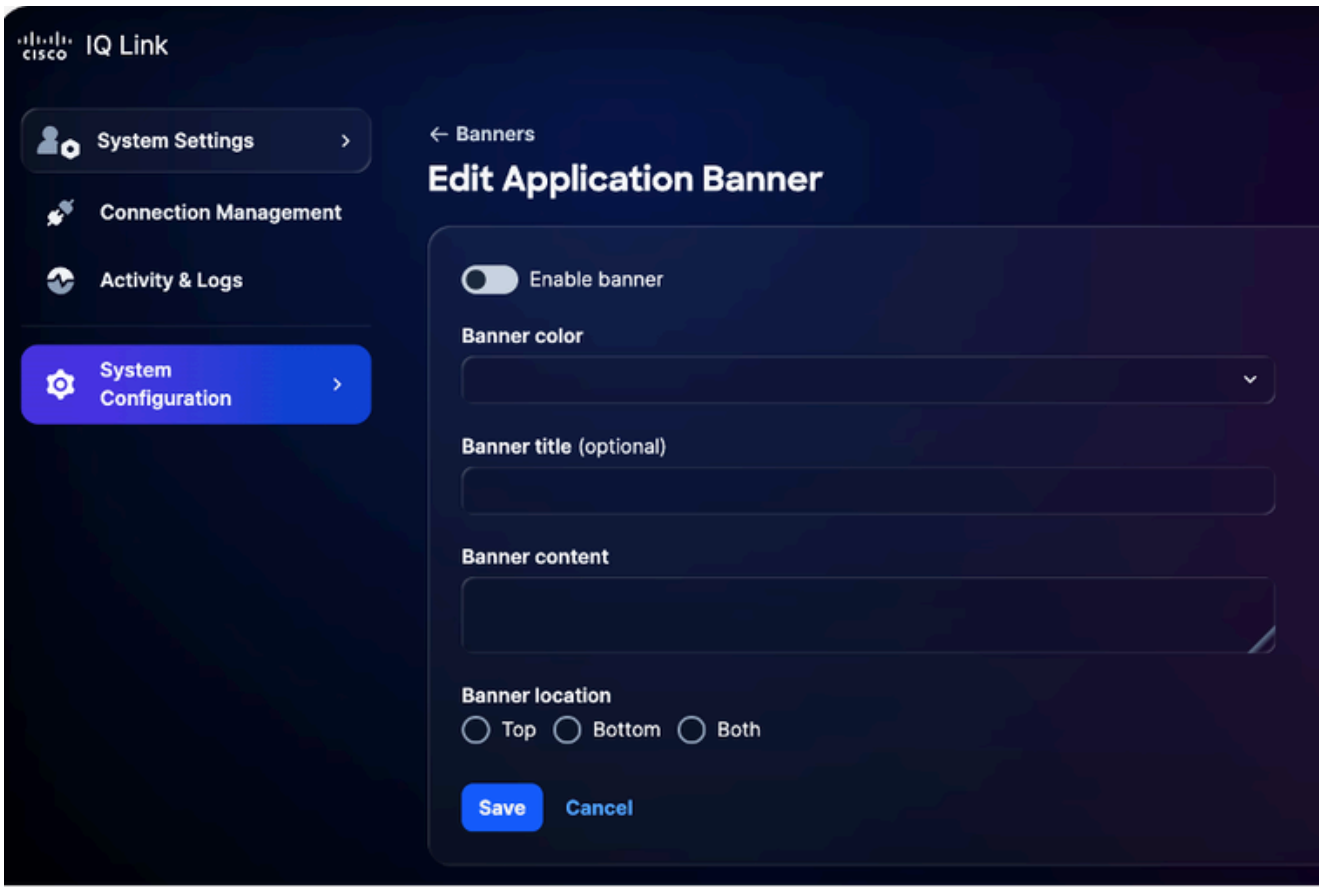
Pour configurer une bannière d'application :

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. Sélectionnez une couleur de bannière.
5. Saisissez le titre de la bannière.
6. Saisissez le contenu de la bannière.

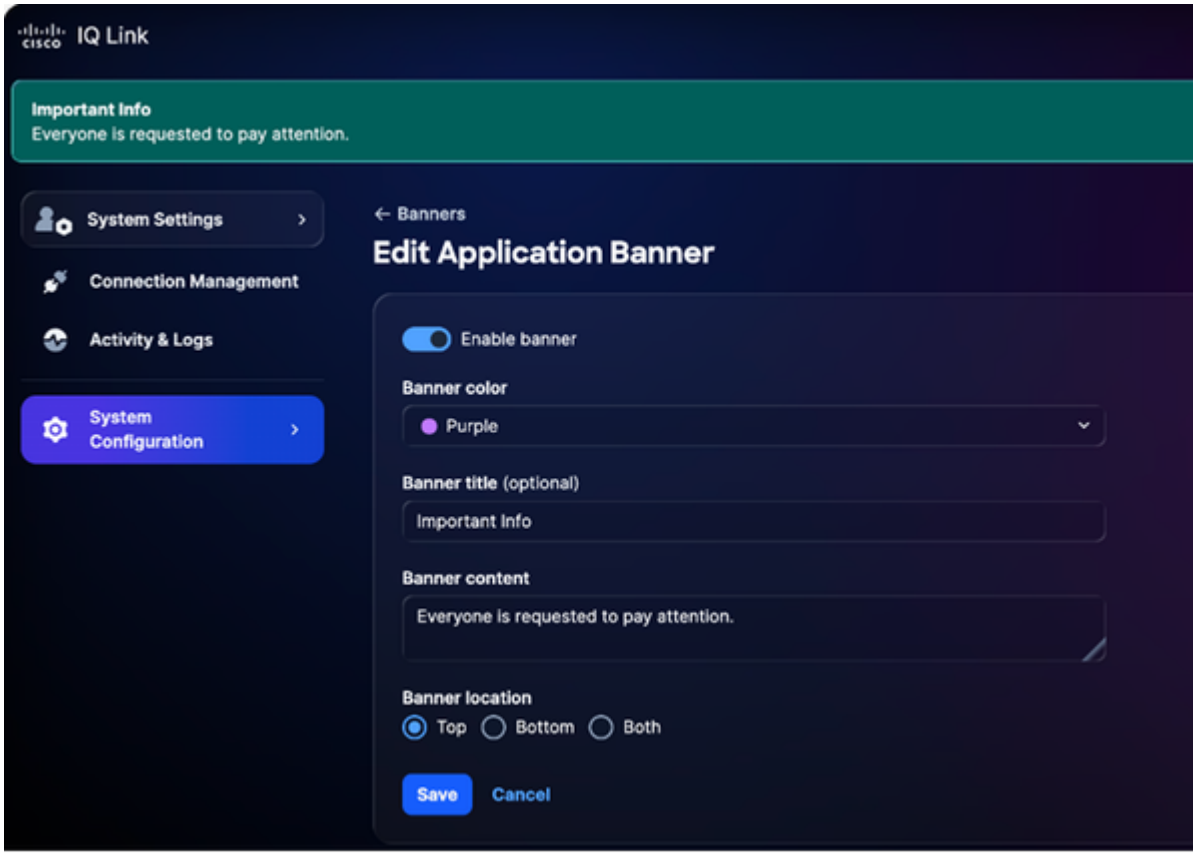
7. Sélectionnez un emplacement de bannière.
8. Cliquez sur Save. La bannière s'affiche dans l'application.

Modification des bannières

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

Modifier la bannière d'application

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 :

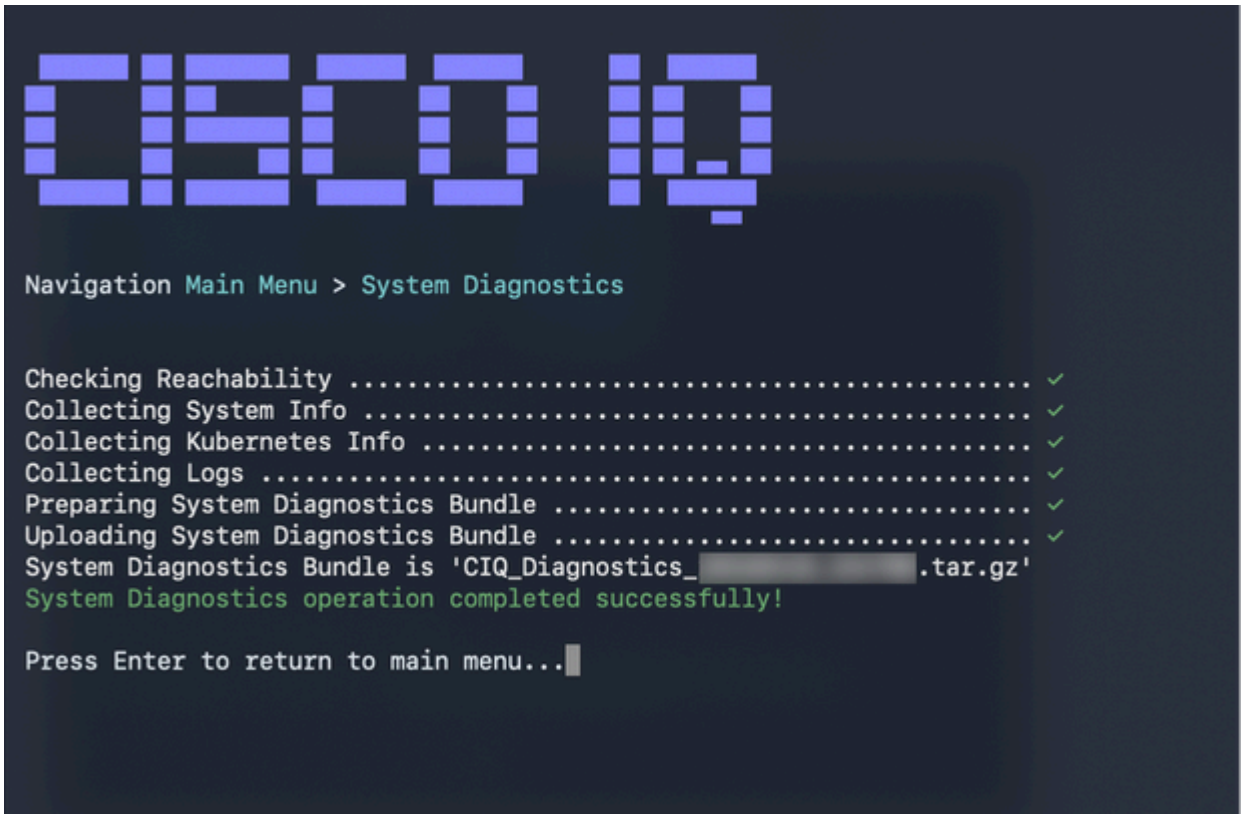
1. Connectez-vous à Cisco IQ.

Menu principal

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

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.



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.

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.