Guide d'exploitation de la liaison Cisco IQ version 1.1.0

Introduction

Cisco IQ™ offre aux clients des améliorations et des fonctionnalités conçues pour améliorer la visibilité sur les ressources, fournir des informations plus intelligentes sur l'ensemble de leurs environnements et rationaliser la gestion des dossiers. En outre, des fonctionnalités d'IA telles que Cisco IQ AI Assistant optimisent les résultats opérationnels et l'expérience utilisateur Cisco IQ en fournissant une compréhension contextuelle qui permet aux utilisateurs 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 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.

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

Configuration de la sécurité administrateur local

Vous pouvez modifier votre mot de passe et configurer des questions de sécurité via le menu Local Admin Security dans System Configuration.

Vous avez trois (3) tentatives de saisie du mot de passe correct dans un délai de dix (10) minutes.

Si les trois (3) tentatives échouent, votre compte se verrouille temporairement pendant 60 minutes pour protéger votre sécurité.

Vous ne pouvez pas tenter de vous connecter pendant la période de verrouillage. Le système affiche le message suivant : «Compte verrouillé en raison d'un trop grand nombre de tentatives ayant échoué. Veuillez réessayer ultérieurement. », y compris la date d'expiration du verrouillage.

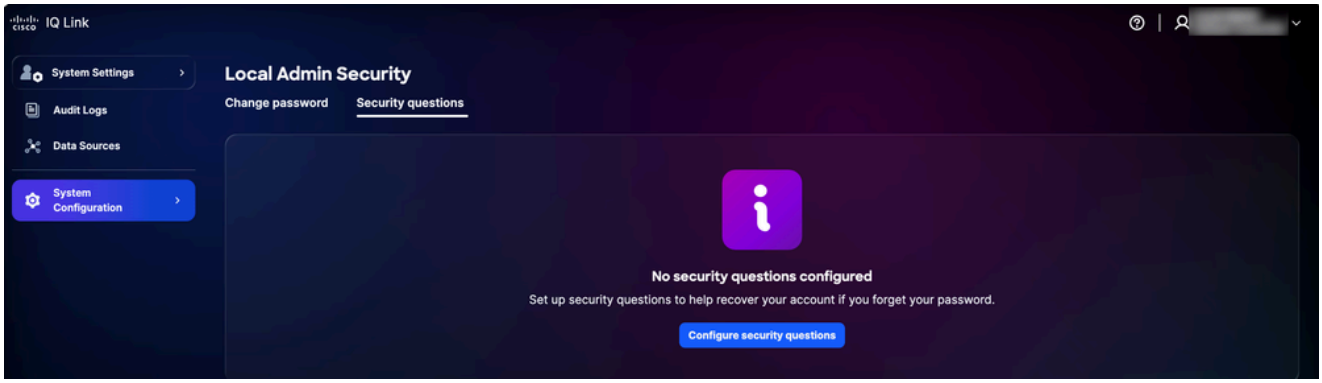
Votre compte se déverrouille automatiquement au bout de 60 minutes. Vous pouvez alors tenter de vous connecter ou de réinitialiser votre mot de passe.

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 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.

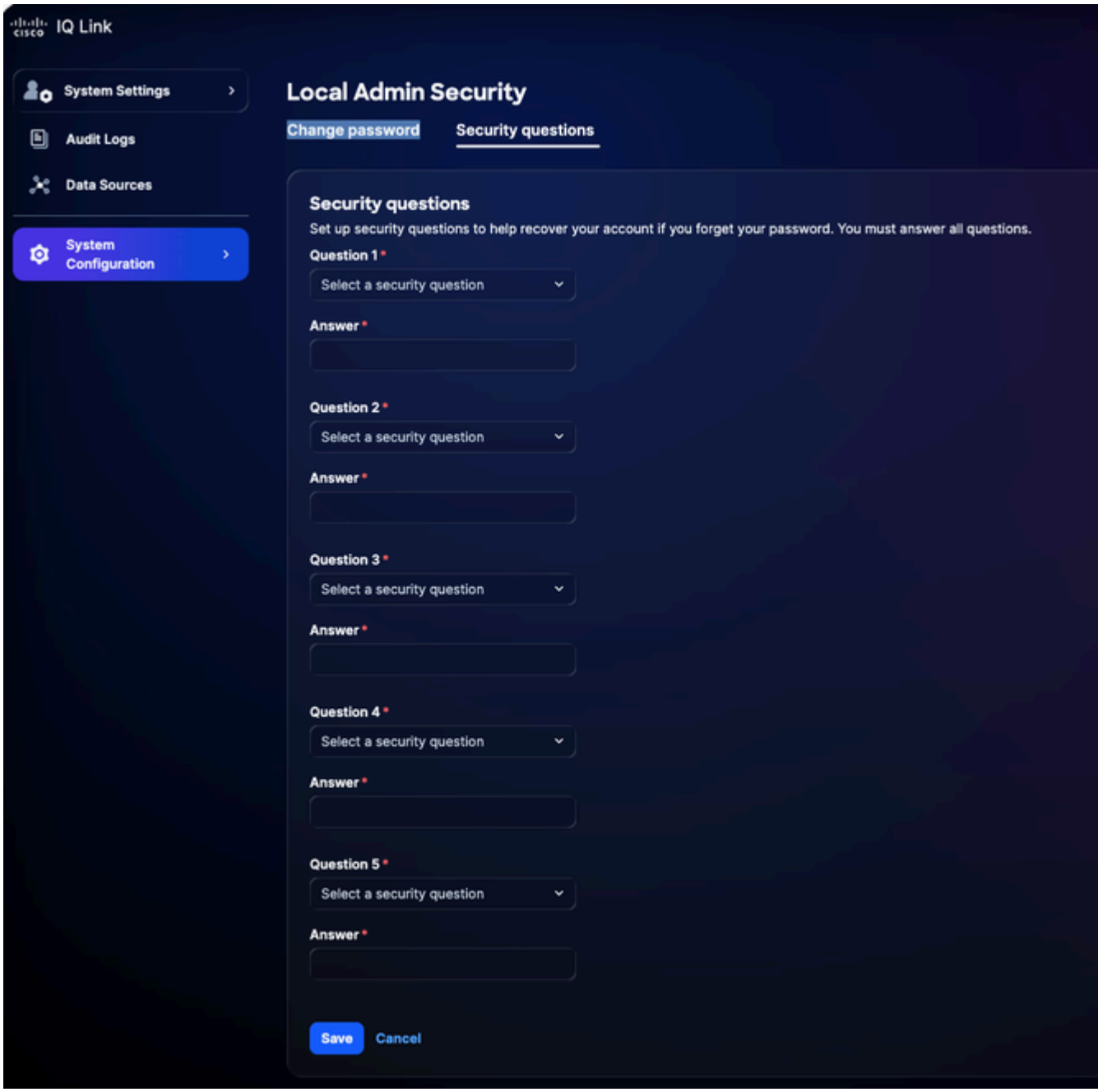
Pour configurer les questions de sécurité :

1. Dans Paramètres système, choisissez Configuration système > Sécurité de l'administrateur local > Questions de sécurité.



Questions de sécurité

2. Cliquez sur Configurer les questions de sécurité.



Questions de sécurité

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

Remarques :
· Les réponses ne sont pas sensibles à la casse ; par exemple, « SMITH » et « smith » sont considérés comme identiques
· Les espaces supplémentaires sont ignorés, ce qui signifie que « Smith » et « Smith » sont traités de la même façon

---

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

Seuls les administrateurs locaux peuvent gérer le mot de passe pour Cisco IQ.

Conditions préalables

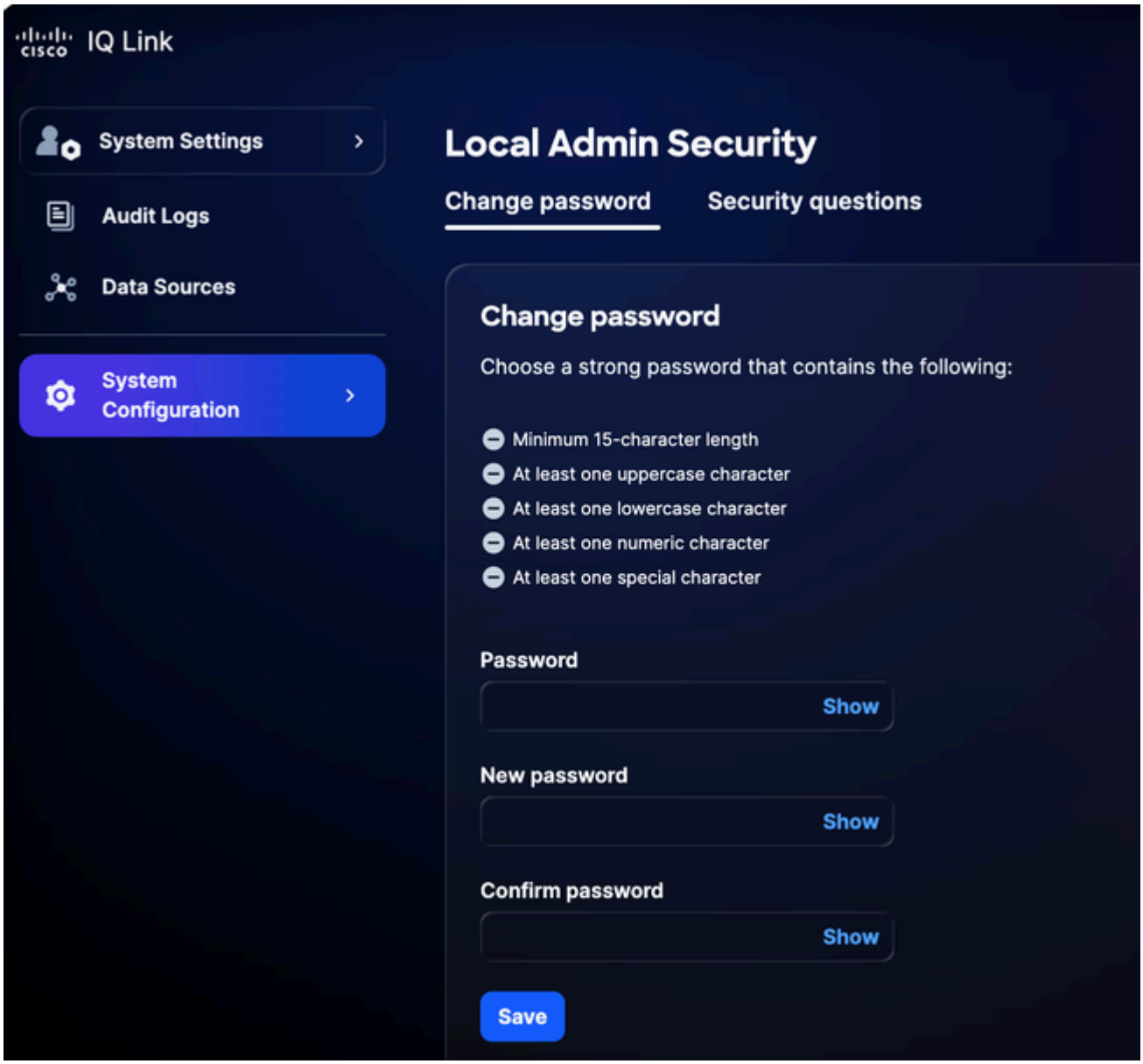
Pour gérer les mots de passe, les conditions suivantes doivent être remplies :

- Vous êtes un administrateur local
- Vous utilisez un compte Administrateur local (pas SSO (Single Sign-On) ou une authentification externe)
- Vous êtes connecté à Cisco IQ
- Vous connaissez le mot de passe actuel

Modification des mots de passe

Pour modifier le mot de passe :

1. Dans Paramètres système, accédez à Configuration système > Sécurité de l'administrateur local > Modifier le mot de passe.



Modifier le mot de passe

2. Saisissez le mot de passe actuel.
3. Saisissez le nouveau mot de passe.
4. Saisissez à nouveau le nouveau mot de passe pour le confirmer.
5. Cliquez sur Save.

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

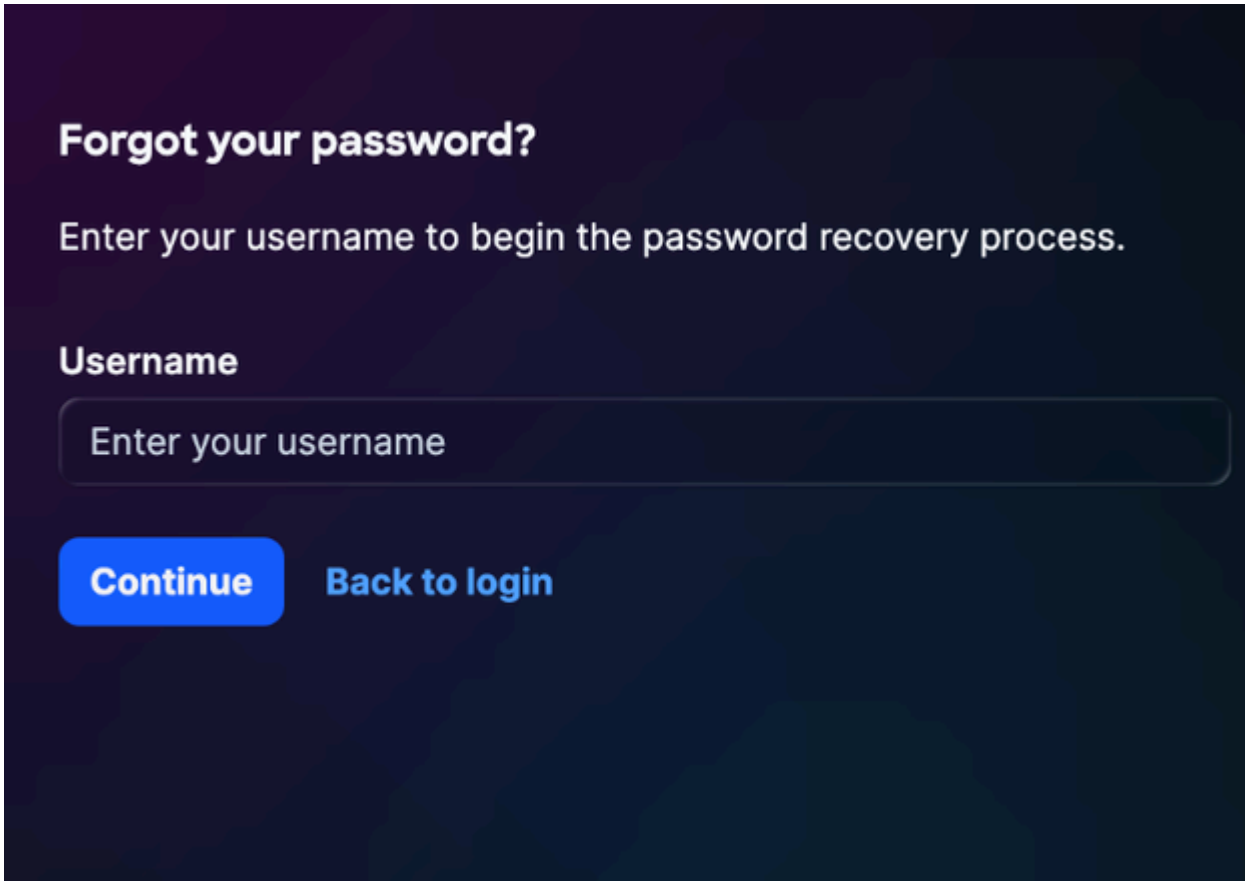
Réinitialisation d'un mot de passe oublié

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.

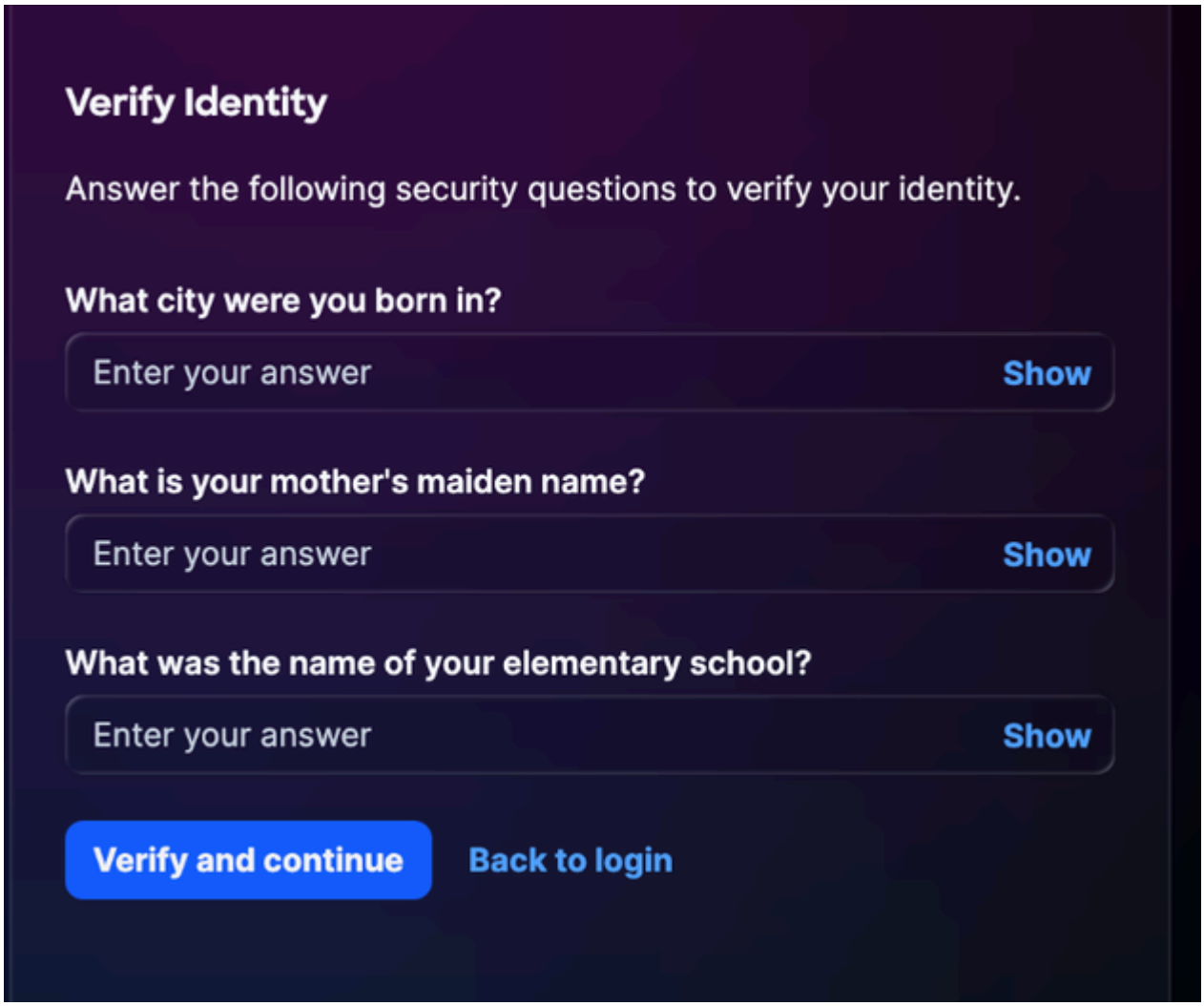
Pour réinitialiser un mot de passe oublié :

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



Mot de passe oublié

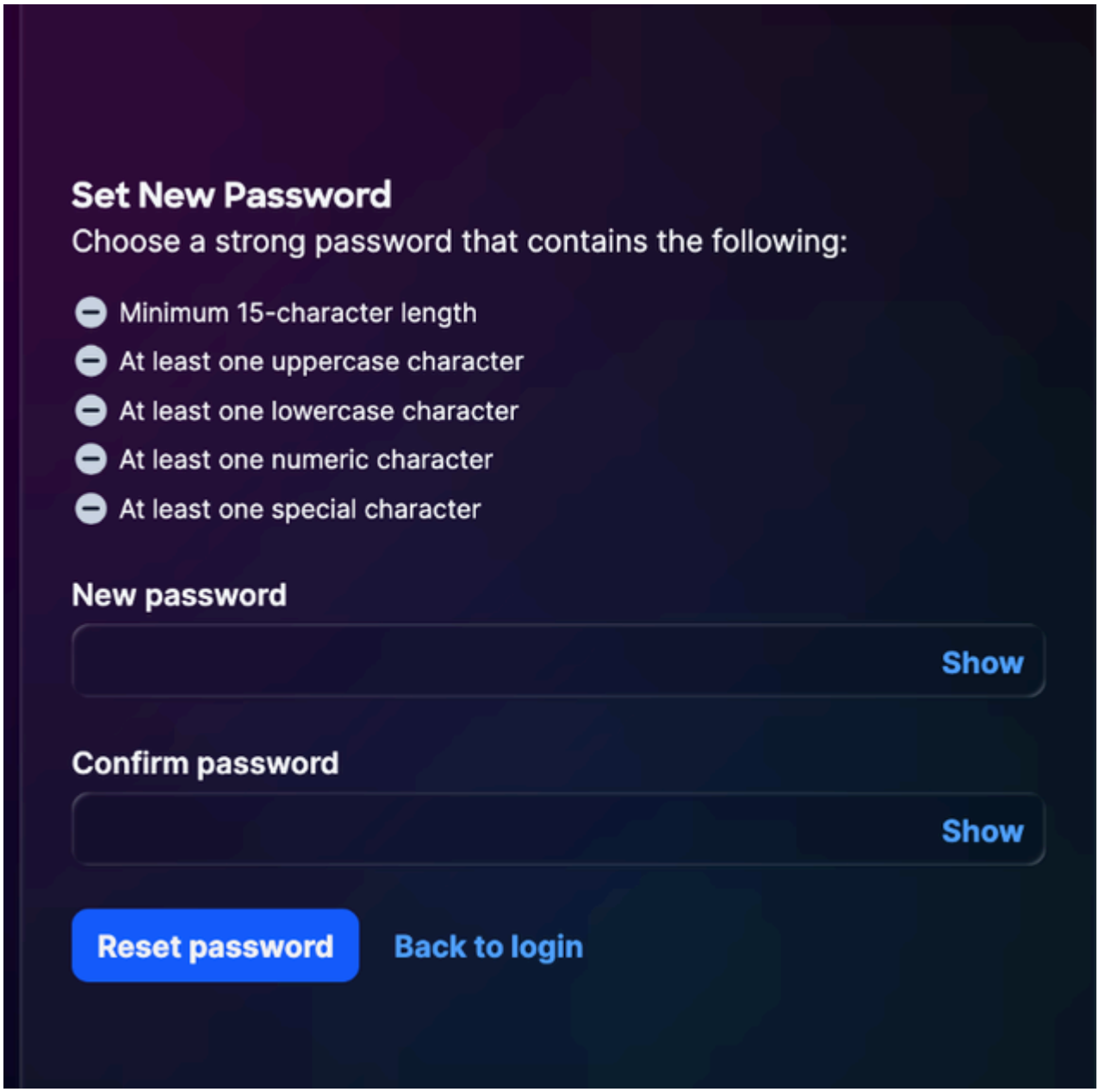
3. Saisissez le nom d'utilisateur.
4. Cliquez sur Continuer. La page Vérifier l'identité affiche trois (3) questions de sécurité aléatoires sur les cinq (5) questions précédemment configurées.



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 Verify 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

Remarque : Vous avez trois (3) tentatives pour répondre correctement aux questions de sécurité dans un délai de dix (10) minutes. Si les trois (3) tentatives échouent, votre compte se verrouille temporairement pendant 60 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 60 minutes. Vous pouvez alors tenter de vous connecter ou de réinitialiser votre mot de passe.

---

7. Saisissez le nouveau mot de passe.

8. Entrez à nouveau le mot de passe pour le confirmer.
9. Cliquez sur Submit.

Configuration du fournisseur d'identité

Une fois connectés à Cisco IQ Link, les administrateurs peuvent configurer différents paramètres. Les administrateurs 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 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.

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

Champ	Valeur
Public	Personnel Non Employé
Catégorie d'intégration	Sélectionnez « Nouvelle intégration ».

Paramètres de configuration SAML

Paramètre	Configuration	Exemple
Public (ID d'entité)	Nom FQDN	mymanagementhost.mydomain.com
URL d'authentification unique	Point de terminaison SAML 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.

Paramètres de configuration SLO

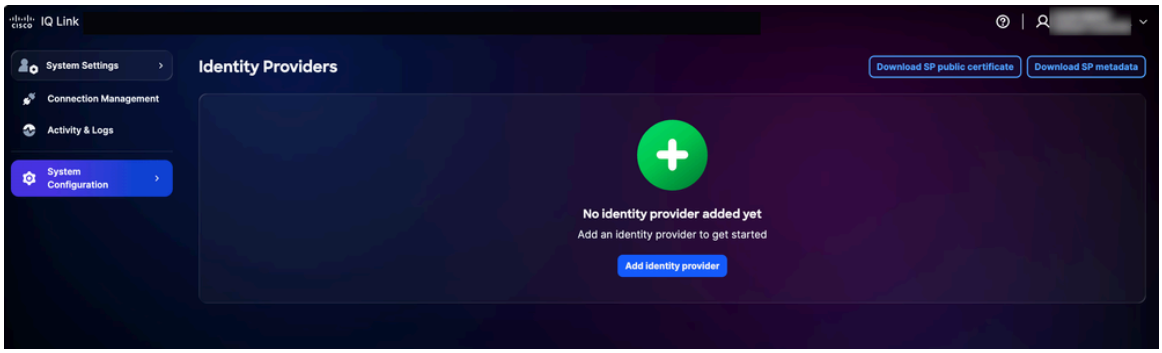
Champ	Valeur
Certificat de signature	Pour Okta, ce certificat n'est requis que si vous choisissez d'activer SLO. Téléchargez le certificat de signature à l'aide de Télécharger le certificat SP dans Fournisseurs d'identité. Enregistrez le fichier sous le nom sp-public-key.crt. Voir Configuration de déconnexion 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

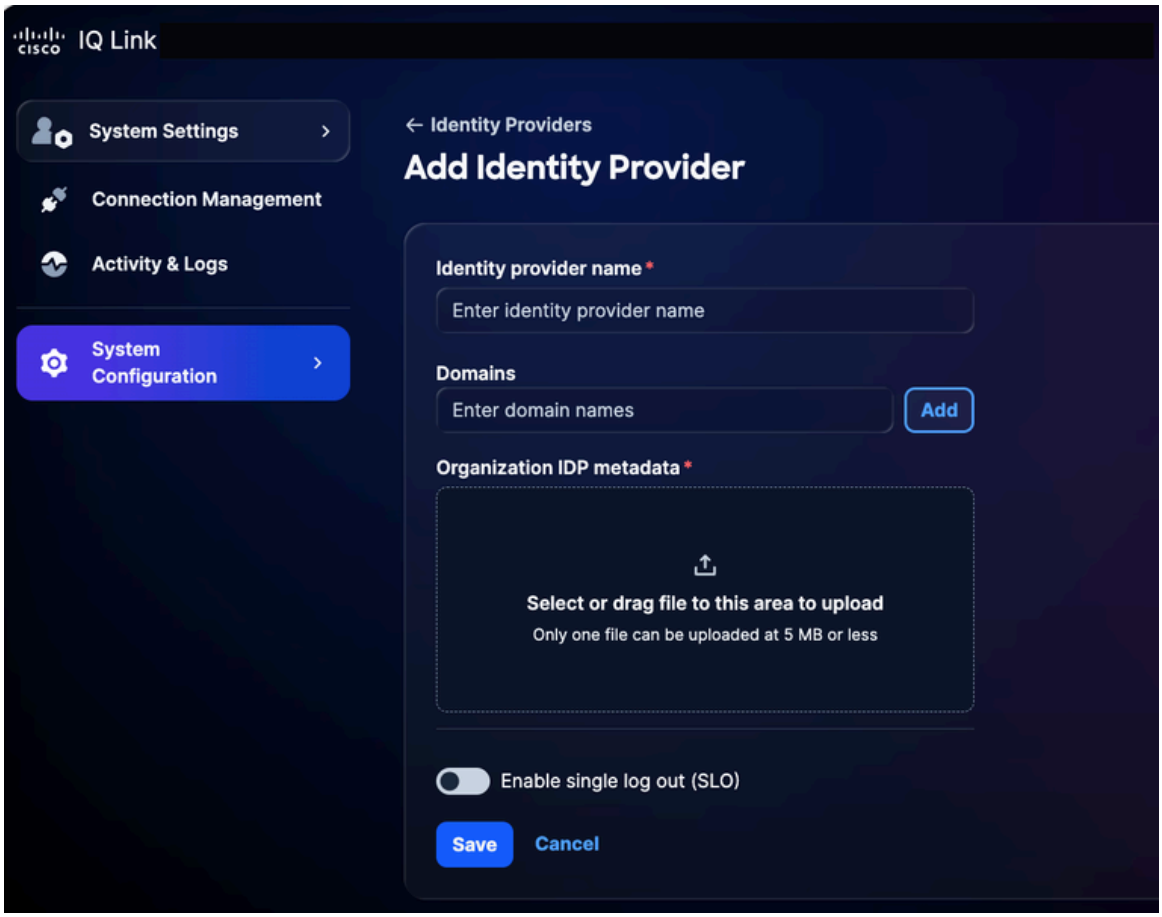
Pour ajouter un IDP dans Cisco IQ Link :

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.



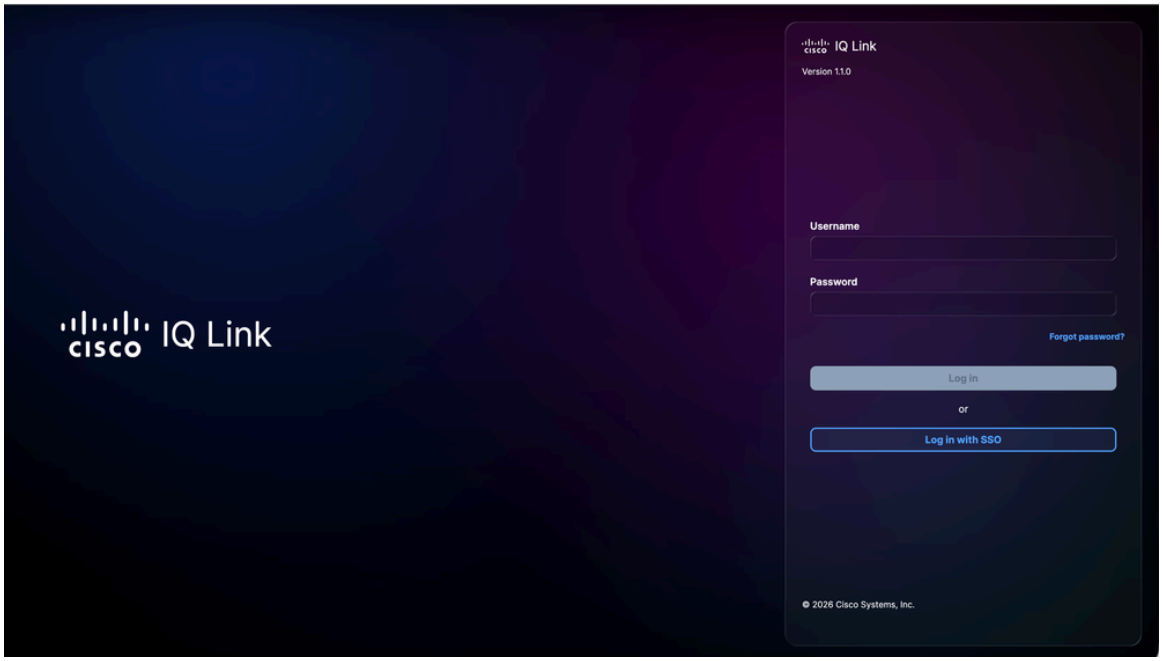
Ajouter un fournisseur d'identité

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.

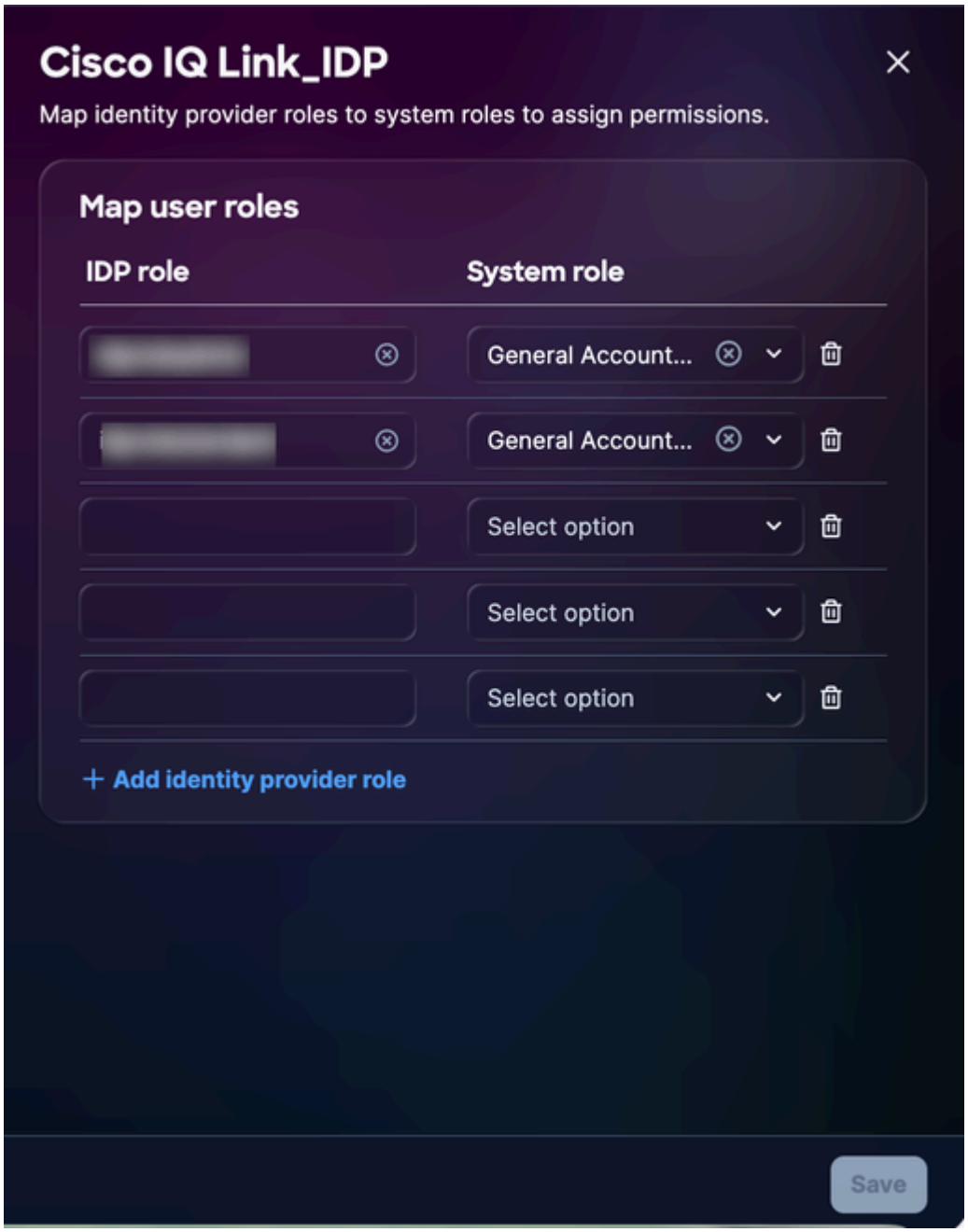
5. Faites glisser et déposez ou téléchargez le fichier de métadonnées SAML obtenu à partir de l'application IDP dans le champ de métadonnées IDP de l'organisation. Ce fichier contient les détails du certificat et les détails de l'entité du fournisseur de services (SP).
6. (Facultatif) Activez le bouton bascule Activer la déconnexion unique. Vous pouvez également activer le SLO ultérieurement.
7. Cliquez sur Save.
8. 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.



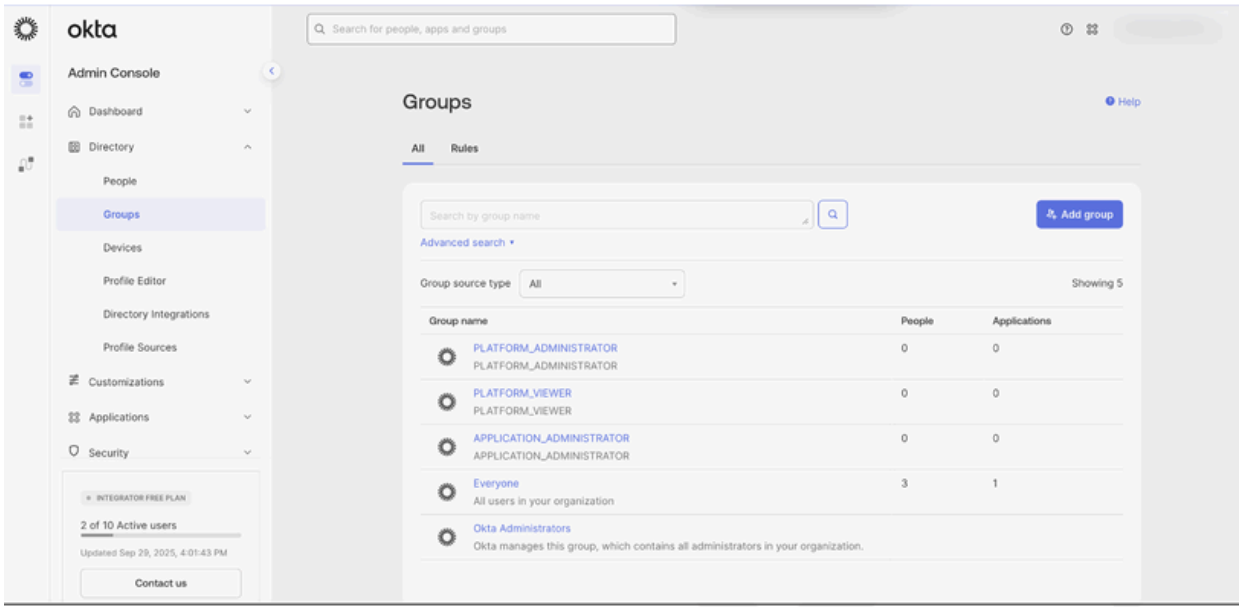
Mappage des rôles utilisateur

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

    - _administrateur_compte_général : L'administrateur général du compte dispose des autorisations complètes pour effectuer toutes les actions du produit
    - _visionneuse_compte_général : L'afficheur de compte général a un accès en lecture seule

---

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



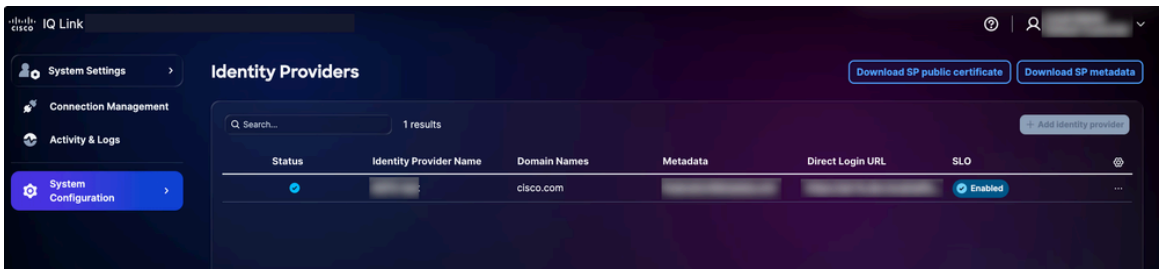
Référence de mappage de rôle

3. Mappez des rôles supplémentaires si nécessaire en cliquant sur Ajouter un rôle de fournisseur d'identité.
4. Cliquez sur Save.

Configuration de déconnexion unique

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

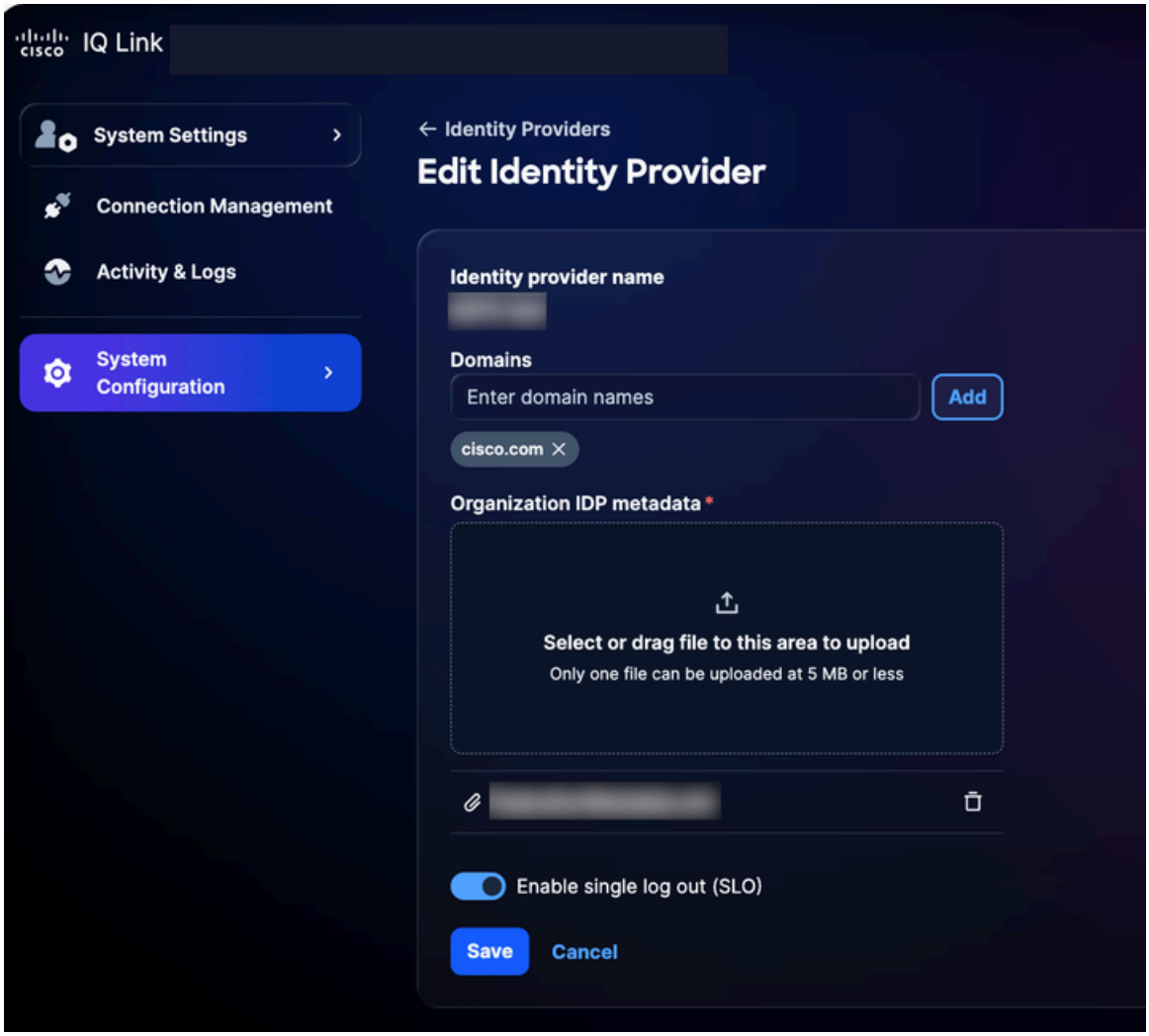
1. Sur la page Identity Providers, cliquez sur Download SP public certificate.



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 la section 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 nouveau fichier de métadonnées téléchargé.
9. Utilisez la liste de contrôle suivante pour vérifier la fonctionnalité SSO et SLO :

Liste de vérification :

- La connexion de l'administrateur local a réussi
- Le portail IDP est configuré et provisionné
- IDP est ajouté à Cisco IQ avec 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 :

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 (Active Directory Federation Services) de Microsoft 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 Active Directory configurée
- Certificats SSL/TLS sur ADFS
- Accès administrateur à Cisco IQ
- Accès administratif au serveur ADFS (Windows Server)
- Accès PowerShell sur le serveur ADFS
- Connectivité réseau entre ADFS et Cisco IQ
- Détails de la configuration du serveur ADFS (comme indiqué dans le tableau ci-dessous)

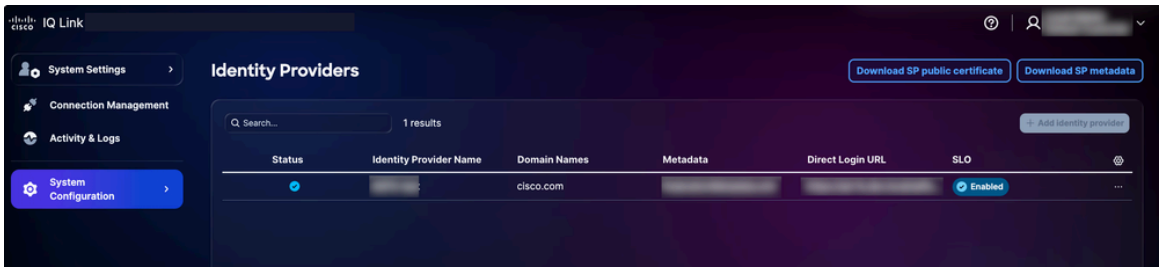
Configuration du serveur ADFS

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 Active Directory	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.
10. Cliquez sur Browse pour sélectionner le fichier de métadonnées du fournisseur de services 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.

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.

Demandes requises

Demande	Objectif	Source
Courriel	Identifiant utilisateur	Courrier AD
Nom d’affichage	Nom complet de l'utilisateur	Nom d'affichage AD
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 utilisateur et l'appartenance à un groupe à Cisco IQ.

```
$claimRules = @’

@RuleTemplate = “LdapClaims”

@RuleName = “Send Email and Name”

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

@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.Issu
```

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

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

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

Vérification des groupes d'utilisateurs

1. Définissez le nom d'utilisateur pour vérifier l'appartenance des utilisateurs 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
```

Configurer ADFS pour faire confiance au 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

- Importer le certificat de l'autorité de certification émettrice dans le magasin Autorités de certification racine de confiance

```
Import-Certificate -FilePath “C:-iq-onprem-ca.cer” -CertStoreLocation “Cert:”
```

3. Appliquez les modifications en redémarrant le service ADFS.

```
Restart-Service adfssrv
```

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.

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. Saisissez 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 à utiliser dans Active Directory 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”] }
```

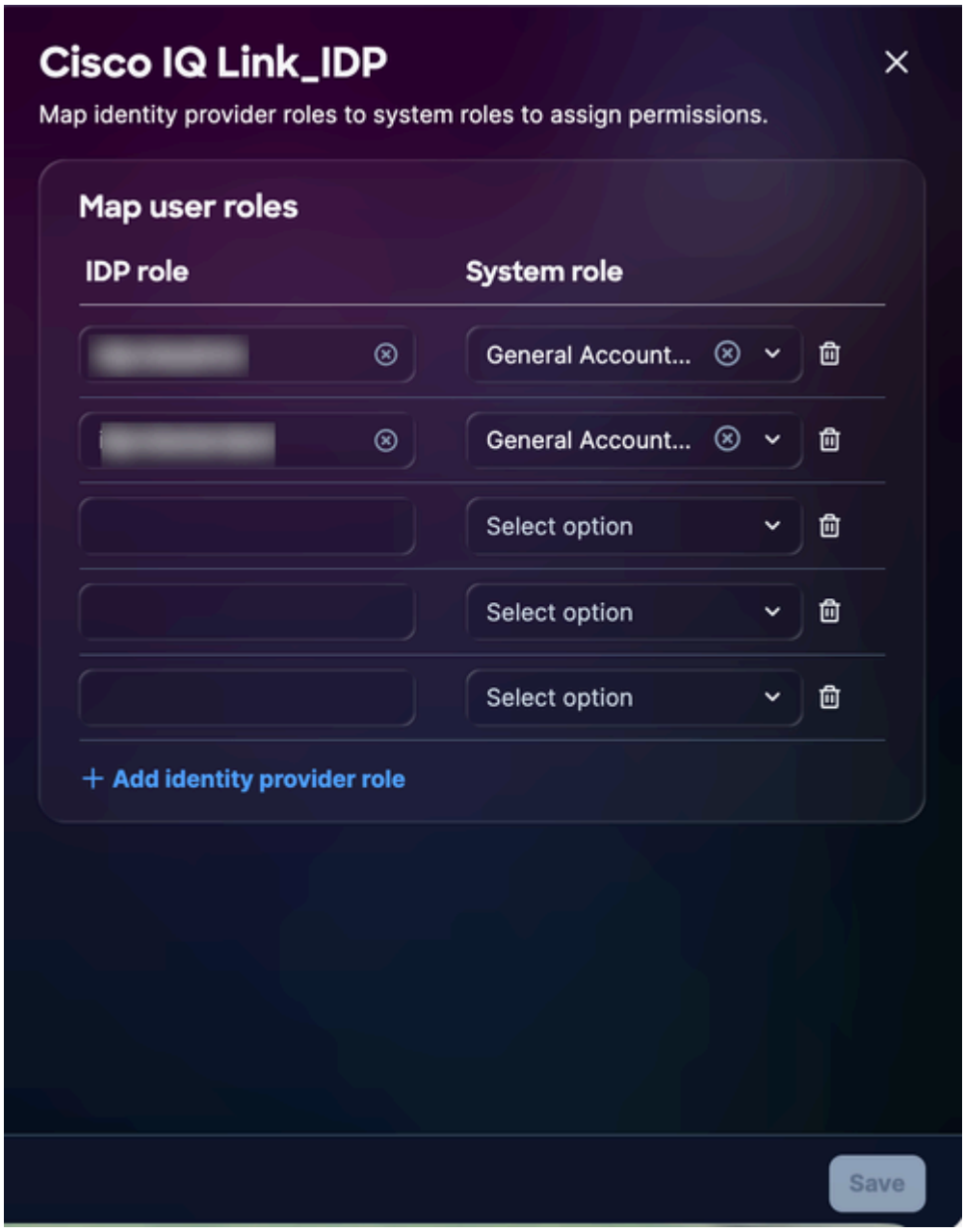
Le système interroge Active Directory directement via LDAP, sans nécessiter de modules supplémentaires. Les informations de groupe sont renvoyées au format complet du nom distinctif (DN), par exemple :

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 pour que vous puissiez effectuer le mappage de rôles ADFS.

Pour configurer le mappage des rôles :

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



Mappage des rôles

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

    - _administrateur_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.
    - general_account__viewer : L'afficheur de compte général 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 Save. L'état est mis à jour en Réussite.

Vérification et test

Test de l'authentification

1. Dans un navigateur en mode Incognito ou Privé, accédez à https://your-cisco-iq-domain.com/login.
2. Connectez-vous à l'aide de vos informations d'identification Active Directory au format domaine\nom d'utilisateur ou user@domain.local.
3. Vérifiez que vous êtes redirigé vers la page d'accueil de Cisco IQ (après l'authentification réussie).
4. Vérifiez que les rôles affectés affichent les noms de groupe analysés corrects (par exemple, Développeurs CXIQ) dans votre profil utilisateur.

Test de déconnexion

Pour tester la déconnexion, cliquez sur Déconnexion de Cisco IQ. Le message « Déconnexion, veuillez patienter... » s'affiche et vous êtes redirigé vers la page Connexion Cisco IQ. Le système ferme également la session ADFS. Si vous tentez d'accéder directement à ADFS, vous êtes invité à vous reconnecter.

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.

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

Problème	Symptômes / Description	Causes / Contrôles / Contournements et solutions
		• Attribut de groupe incorrect : Doit être http://schemas.xmlsoap.org/claims/Group • L'utilisateur ne fait pas partie des groupes AD
Échec du décodage	Échec du déchiffrement de l'assertion dans les journaux	Vérifier la configuration du certificat ADFS
Boucle de connexion	Blocage dans une boucle d'authentification ou de connexion	• URL ACS non valide : 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

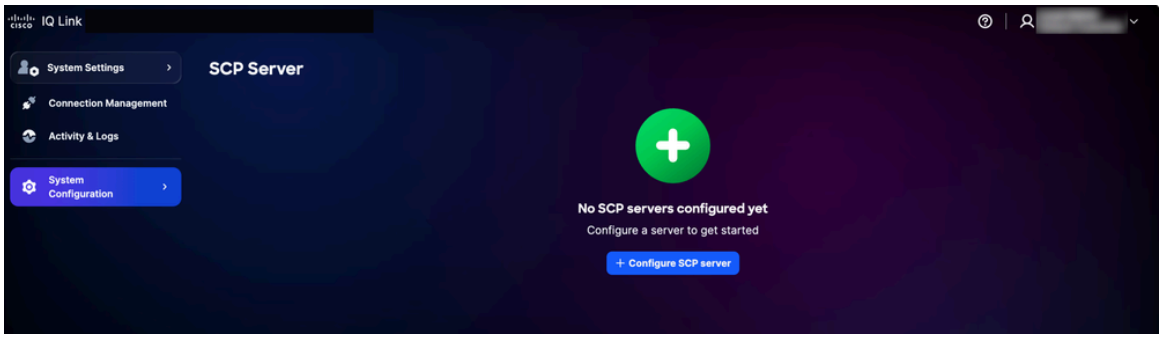
```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object SamlEndpoints
```

Ajout de serveurs SCP

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

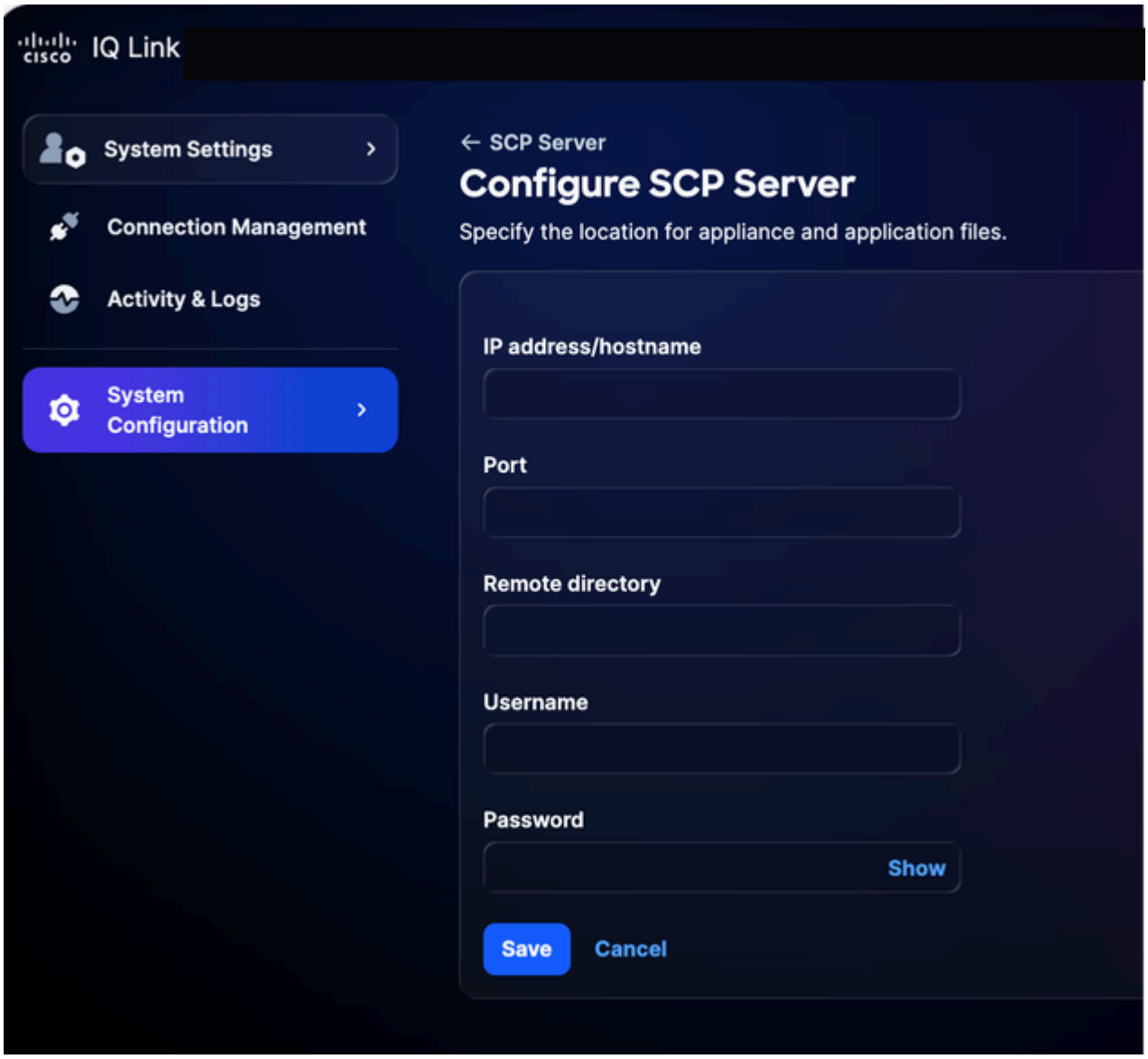
Pour ajouter un serveur SCP :

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.



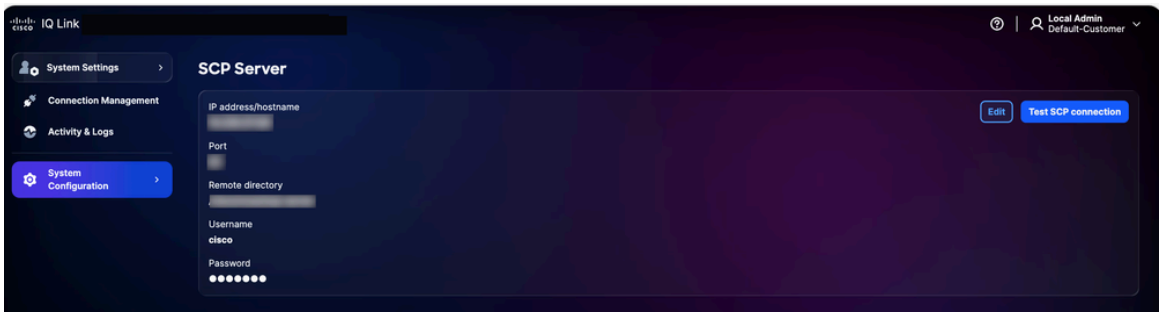
Configurer le serveur SCP

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

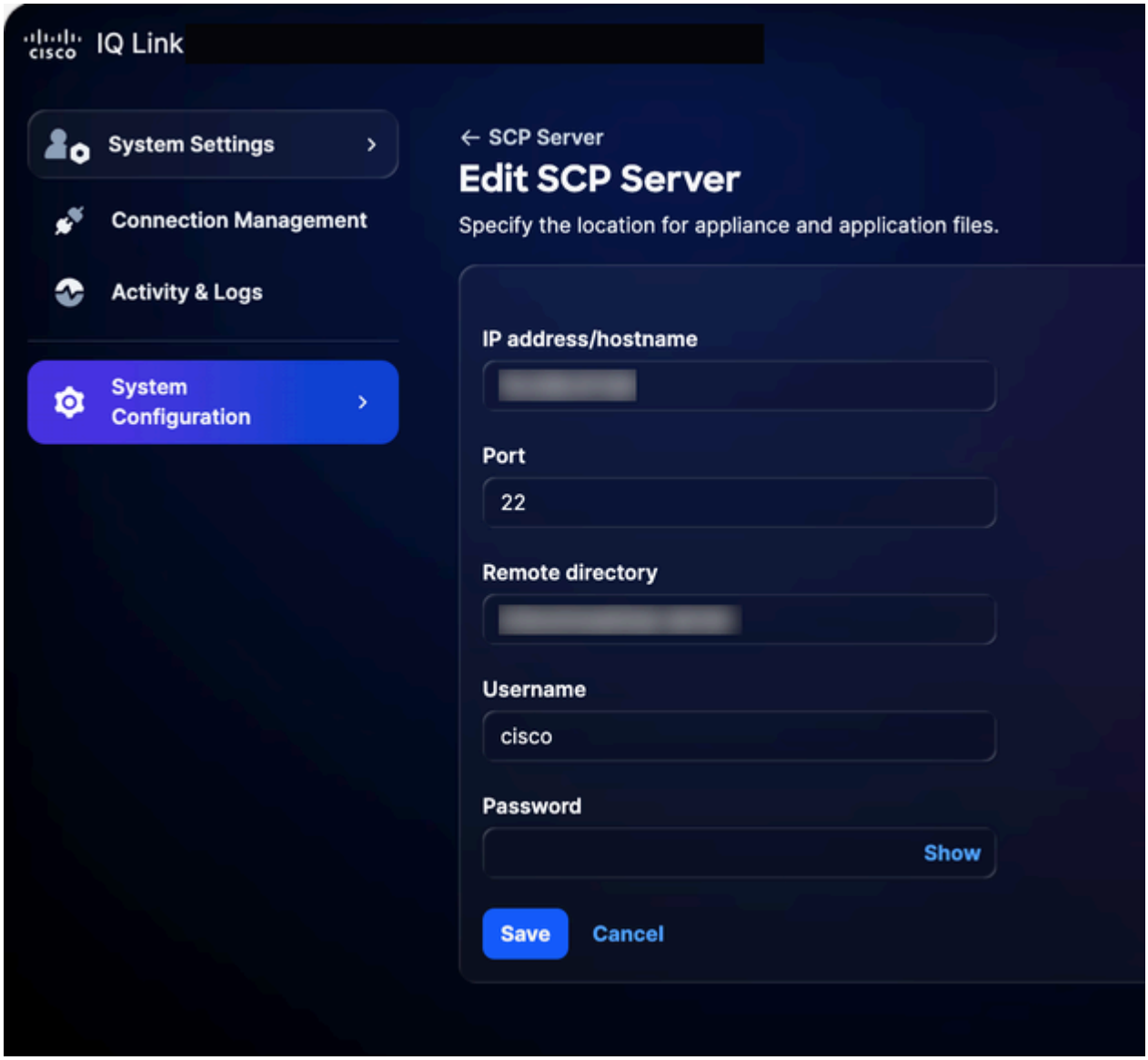
Pour modifier un serveur SCP existant :

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.

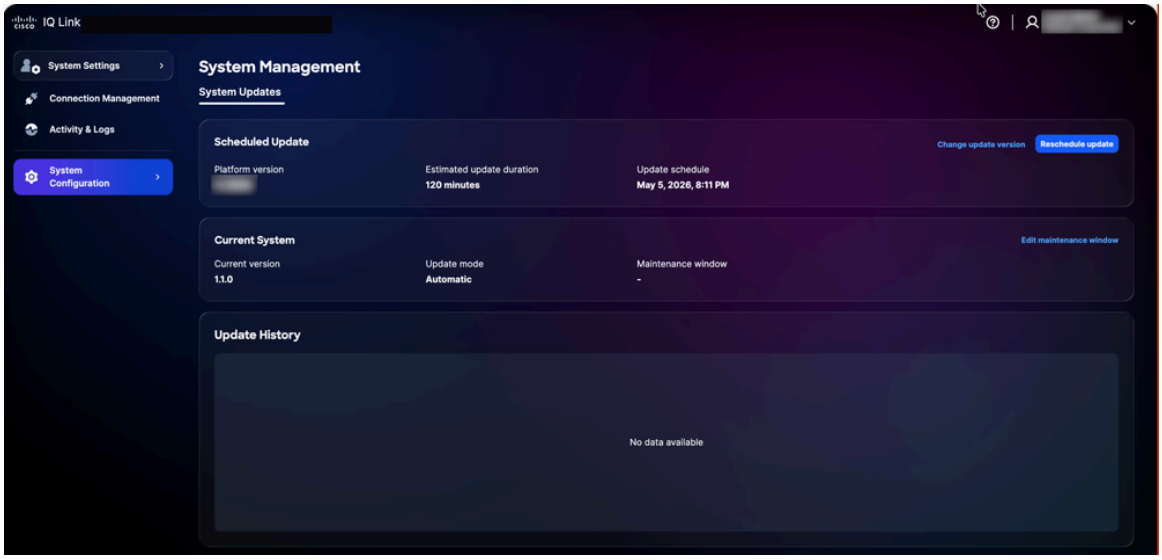
4. Cliquez sur Save.

Gestion du système

Les clients peuvent 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 Cisco IQ Data Connectors.

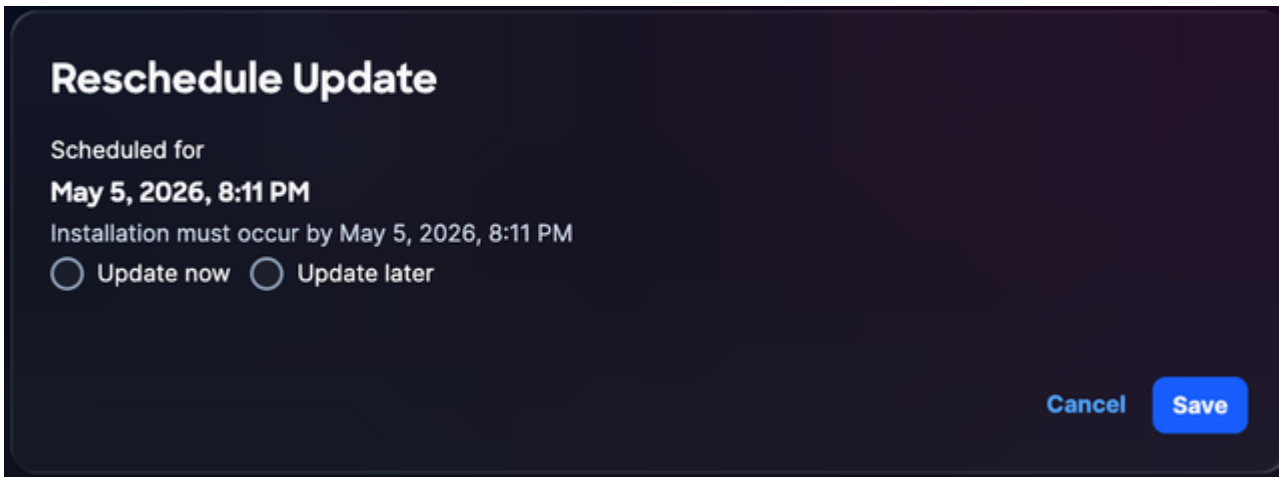
Pour replanifier la mise à jour du système :

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

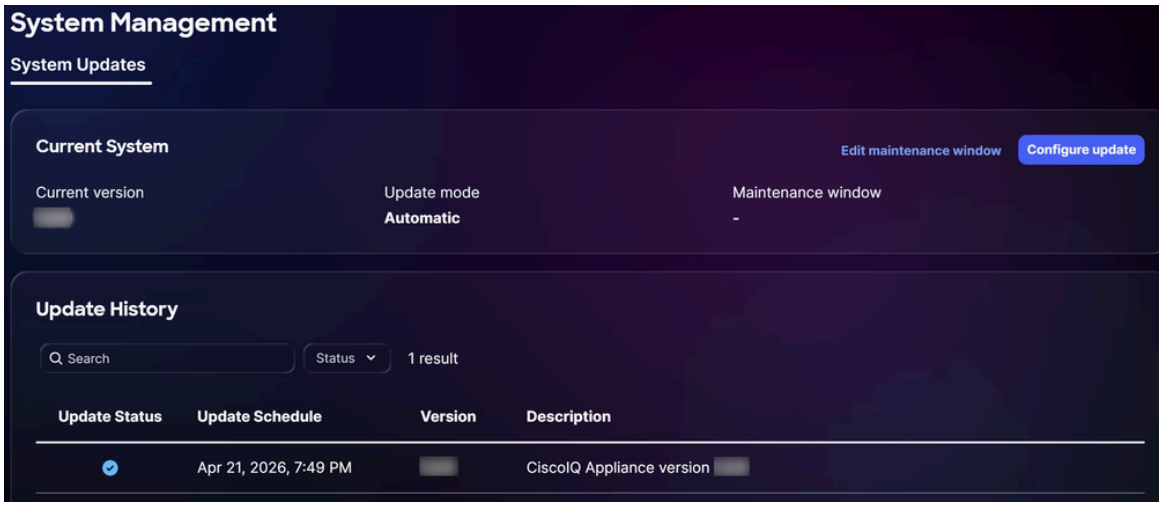
2. Cliquez sur Replanifier la mise à jour.



Reprogrammer la mise à niveau

3. Cliquez sur Mettre à jour maintenant pour une replanification immédiate ou sur 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

Configuration des certificats SSL

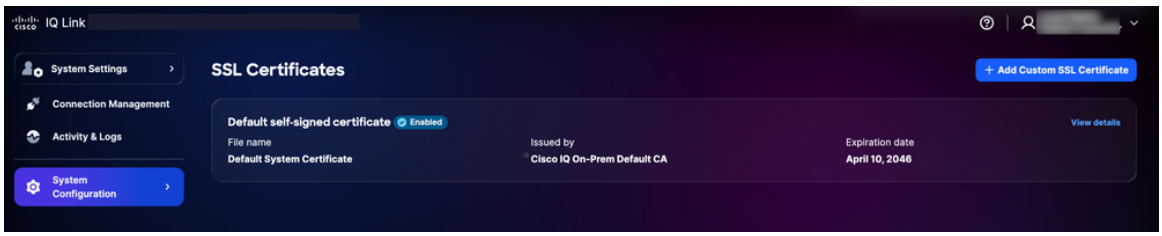
Un certificat auto-signé par défaut est préinstallé et activé dans Cisco IQ, mais les utilisateurs peuvent télécharger des certificats SSL personnalisés. Lorsqu'un certificat SSL personnalisé est activé, il est utilisé pour les connexions HTTPS ; si le certificat est désactivé ou supprimé, le système revient automatiquement au certificat par défaut.

Remarque : Le certificat doit avoir au moins 90 jours de validité restants. Un certificat est considéré comme « presque arrivé à expiration » lorsqu'il lui reste moins de 90 jours avant son expiration. Après l'ajout, la modification ou la suppression d'un certificat SSL, le client doit télécharger le nouveau SSL comme indiqué dans la section Finalisation de la configuration de SLO pour l'IDP Okta ou l'IDP ADFS.

Ajout d'un certificat SSL personnalisé

Pour ajouter un certificat SSL personnalisé :

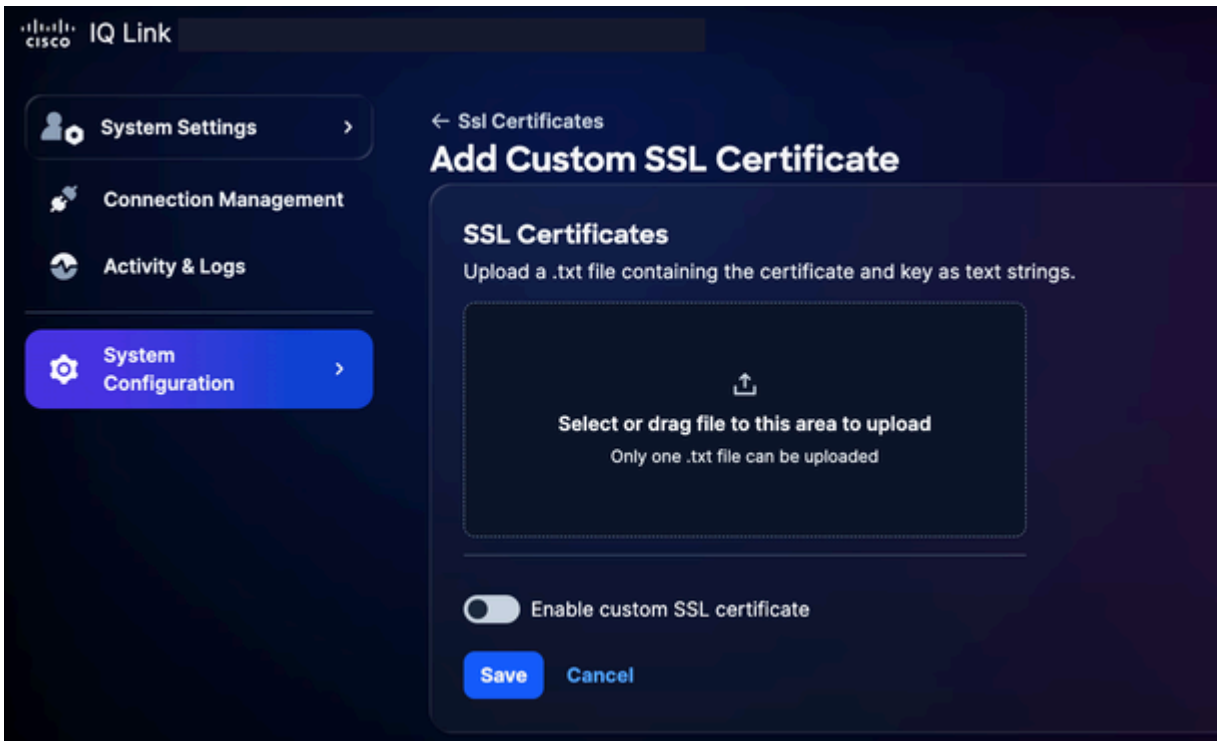
1. Dans Paramètres système, choisissez Configuration système > Certificats SSL. La page SSL Certificates s'affiche et répertorie tous les certificats SSL de votre système.



Ajout du certificat SSL

2. Cliquez sur Ajouter un certificat SSL personnalisé.

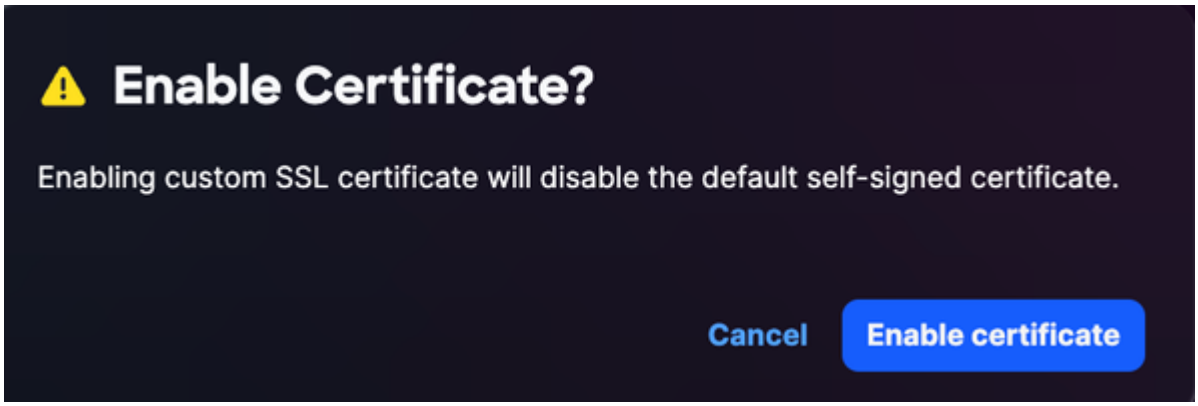
Remarques :
· Téléchargez un fichier .txt qui inclut à la fois le certificat et la clé codés par courrier Privacy-Enhanced comme chaînes de texte
· Un seul fichier .txt peut être téléchargé à la fois
· Le fichier doit contenir le certificat et la clé privée



Télécharger des certificats 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.



Activer le certificat

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

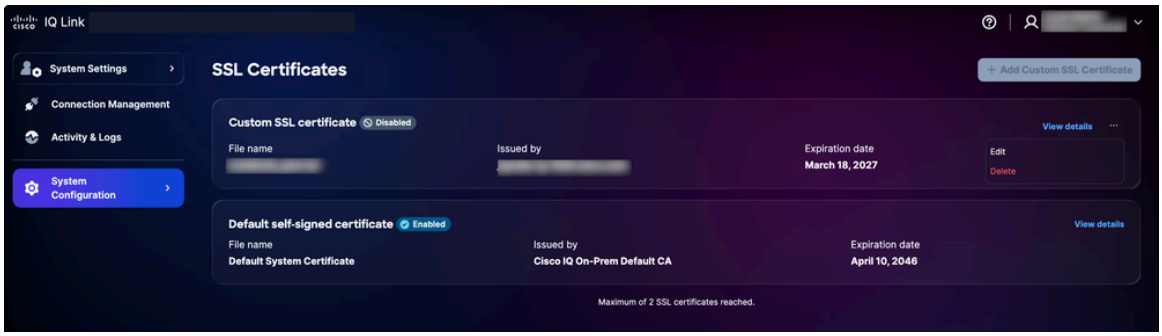
5. Cliquez sur Activer le certificat.
6. Cliquez sur Save.

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

Modification 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

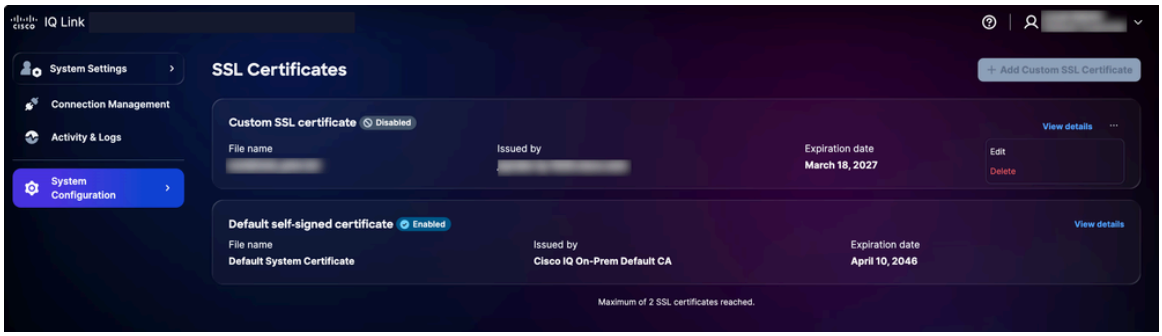
2. Cliquez sur l'icône Autres options > Modifier. La page Edit SSL Certificate s'affiche.
3. Modifiez les détails du certificat selon les besoins.
4. Cliquez sur Save.

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 personnel 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

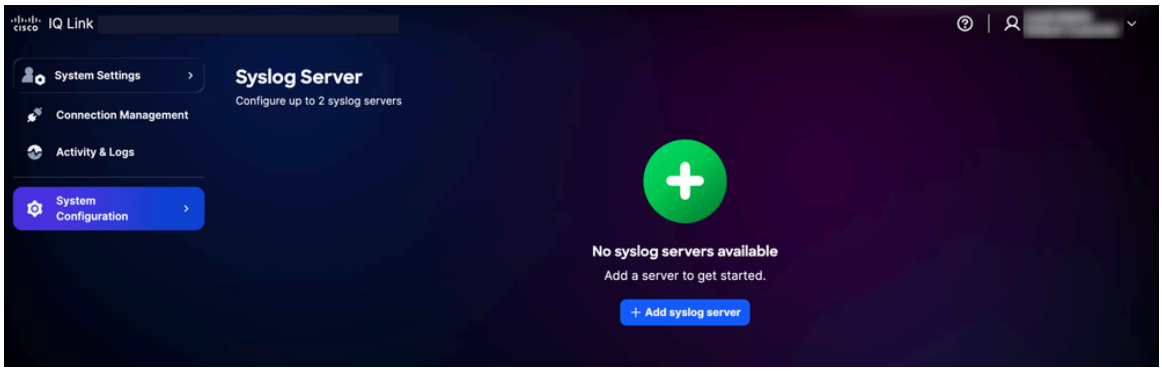
Les utilisateurs dotés du rôle Administrateur peuvent configurer des serveurs Syslog externes pour exporter les journaux système. Vous pouvez configurer jusqu'à deux (2) serveurs syslog.

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

Ajout de serveurs Syslog

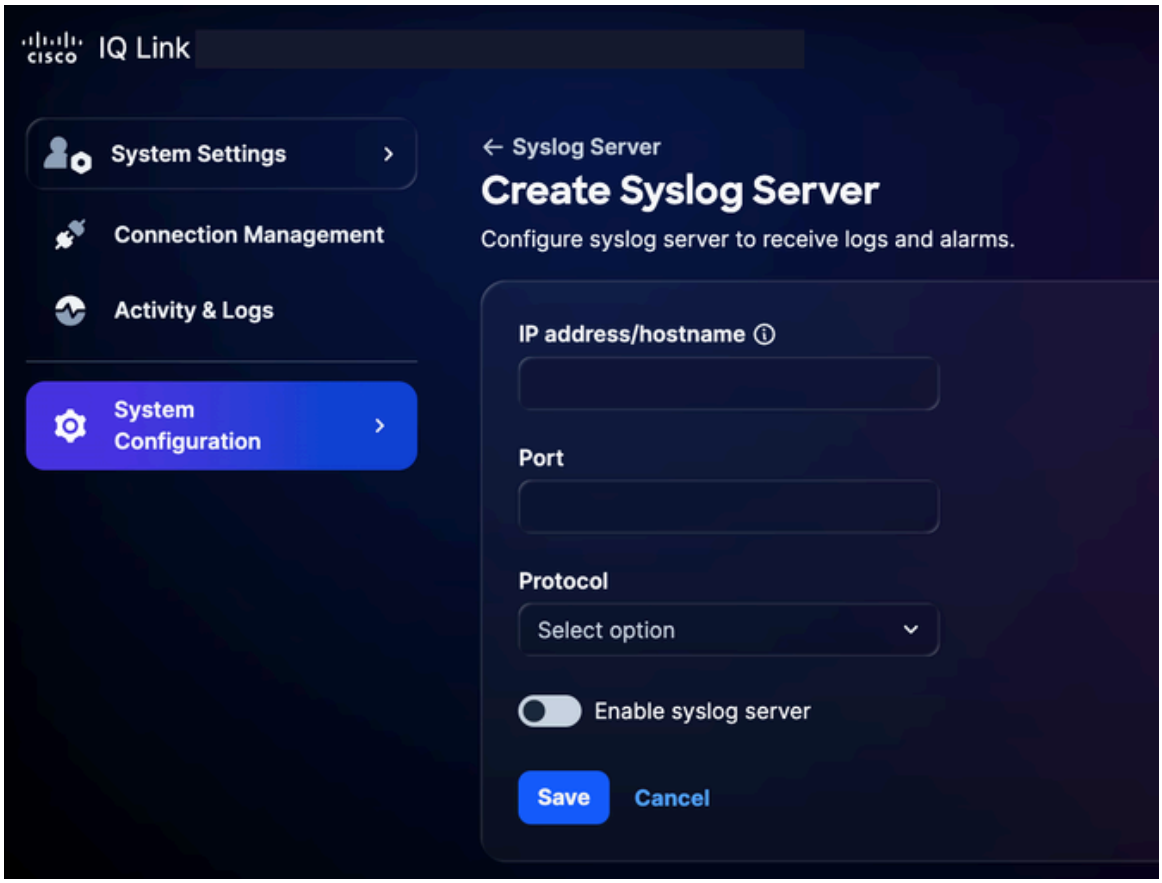
Pour ajouter un serveur Syslog :

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.



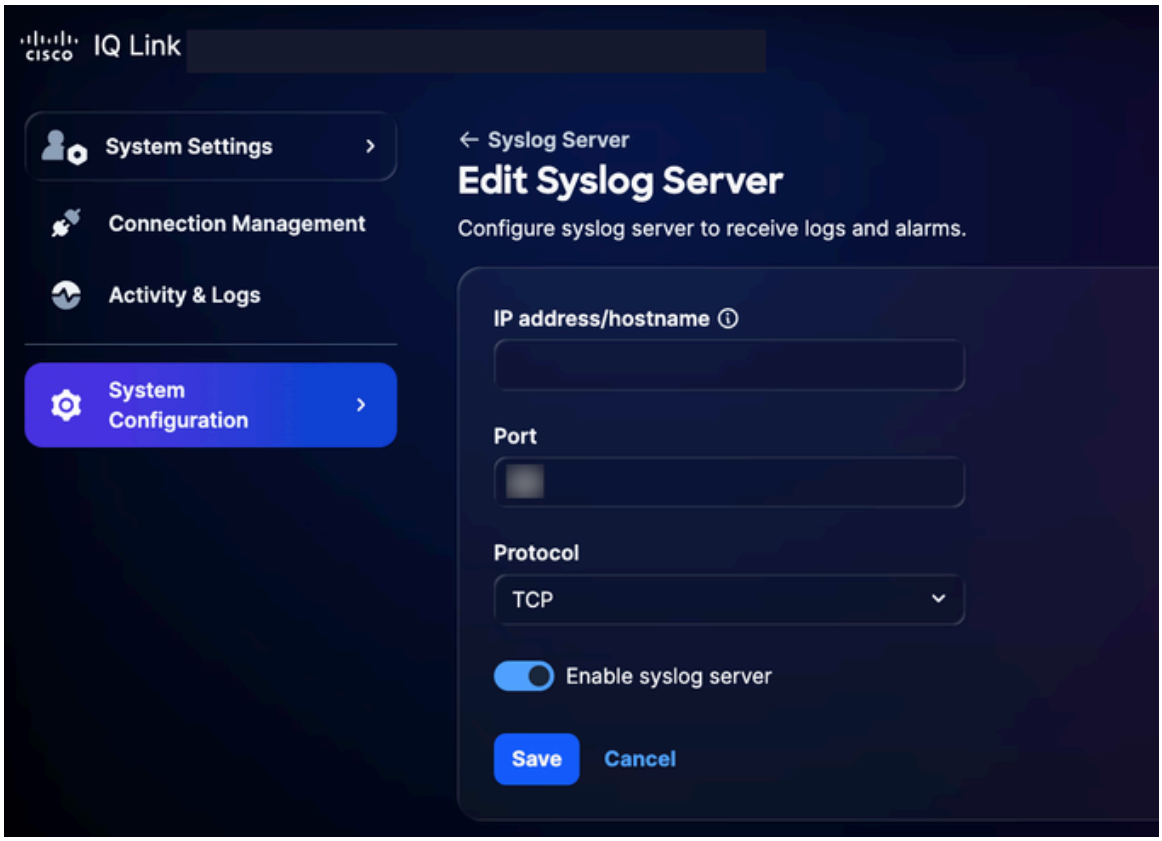
Créer un serveur Syslog

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.



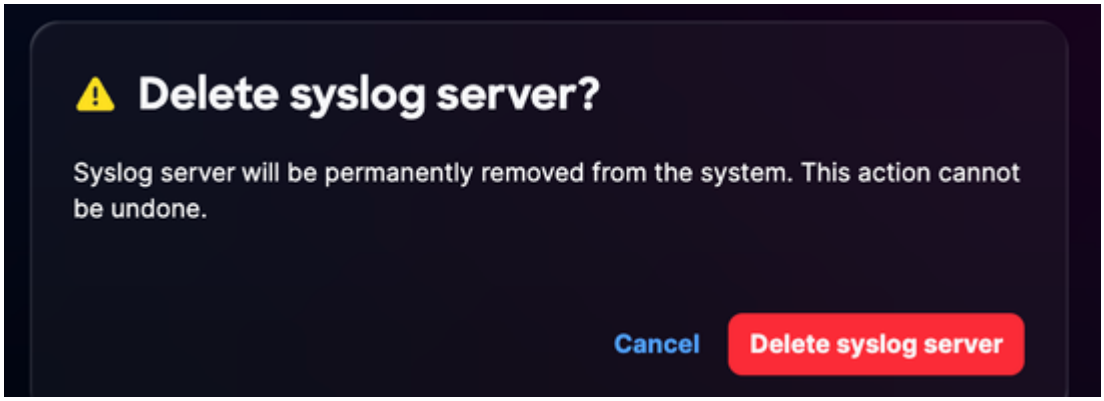
Modifier le serveur Syslog

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.

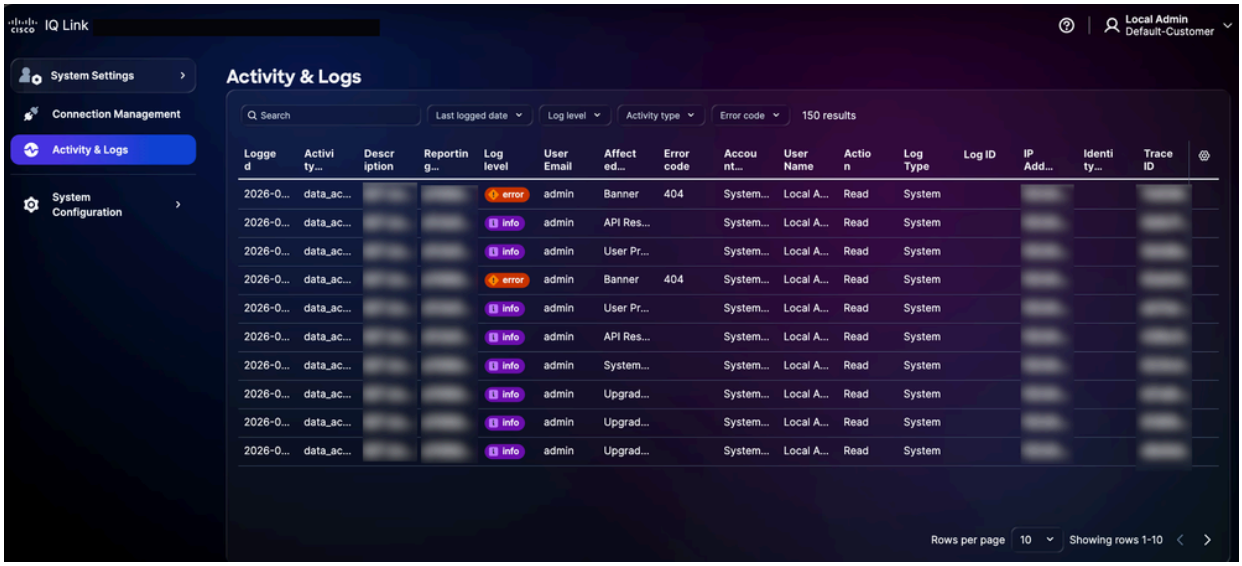


Confirmation

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, ce qui permet aux administrateurs 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
- Enregistrer toutes les opérations d'API au niveau de la passerelle

Les options de filtre suivantes sont disponibles :

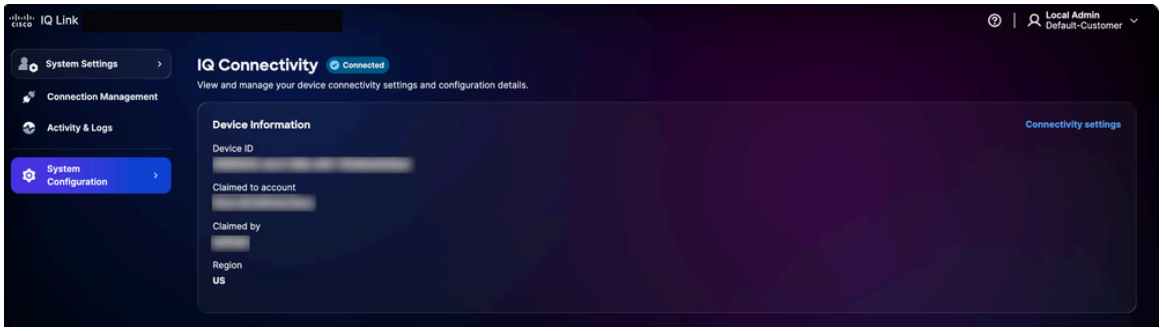
- Date : Filtre les journaux dans une plage de temps spécifique
- Niveau du journal : Filtre les journaux par gravité (par exemple, erreur, avertissement et informations)
- Type d'activité : Filtre les journaux par type d'activité du système

- Code d'erreur : Filtre les journaux pour un code d'erreur spécifique

Connectivité IQ

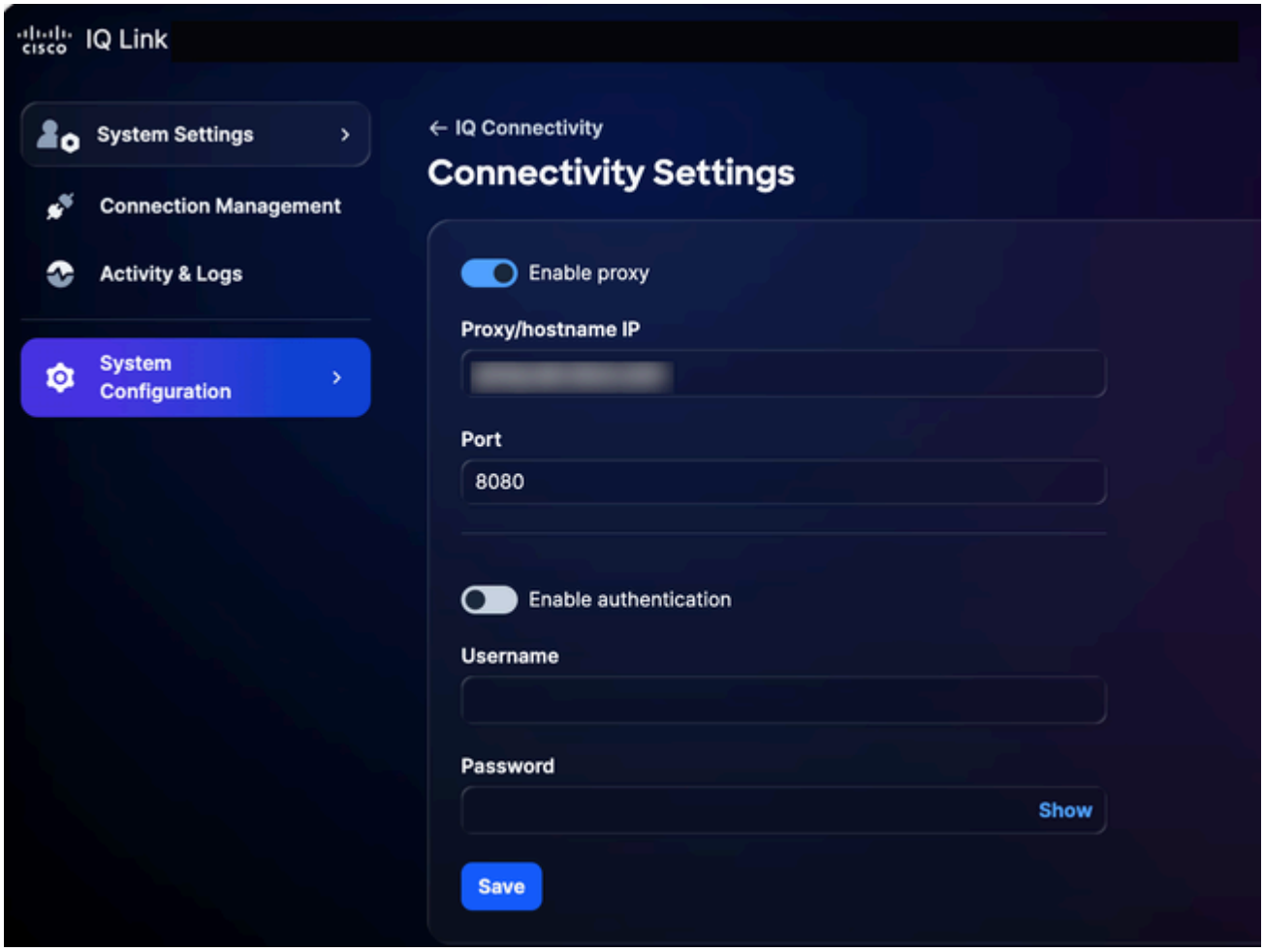
Pour afficher et gérer les paramètres de connectivité et les détails de configuration de votre périphérique :

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



Connectivité IQ

2. Cliquez sur Connectivity settings.



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

Gestion des connexions (collecte de données)

Cisco IQ Link est une solution déployée sur site pour la collecte de données réseau, conçue pour fournir 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 peut être résumée comme suit :

- Création de jeux d'informations d'identification : Établissez les protocoles d'authentification (par exemple, SNMP 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.

Remarque : Cisco IQ Link nécessite un compte d'utilisateur configuré avec le niveau de privilège 15 sur le périphérique pour authentifier les ressources directement connectées.

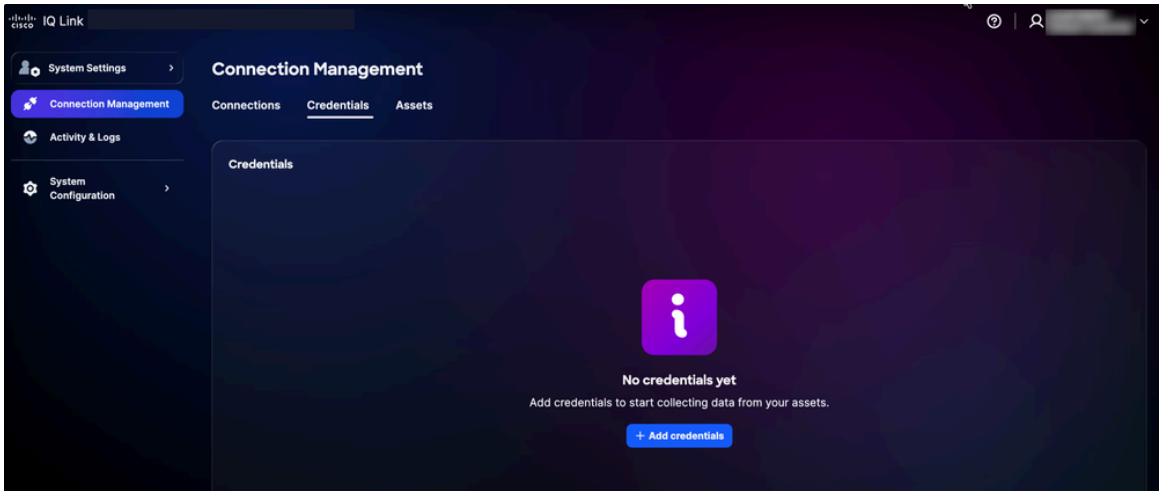
- Mappage des informations d'identification à Inventory : Associez vos jeux d'informations d'identification à vos ressources d'inventaire pour automatiser le processus d'authentification. En créant des règles qui lient des plages IP spécifiques à des jeux d'informations d'identification définis, le système 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

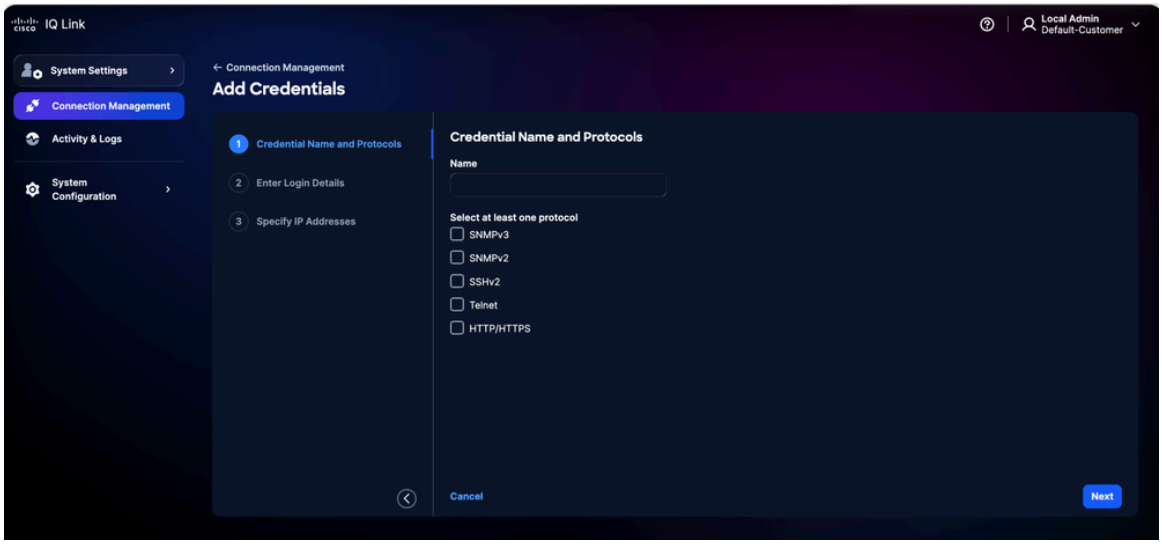
Vous devez d'abord ajouter des informations d'identification pour collecter des données. Pour ajouter des informations d'identification :

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



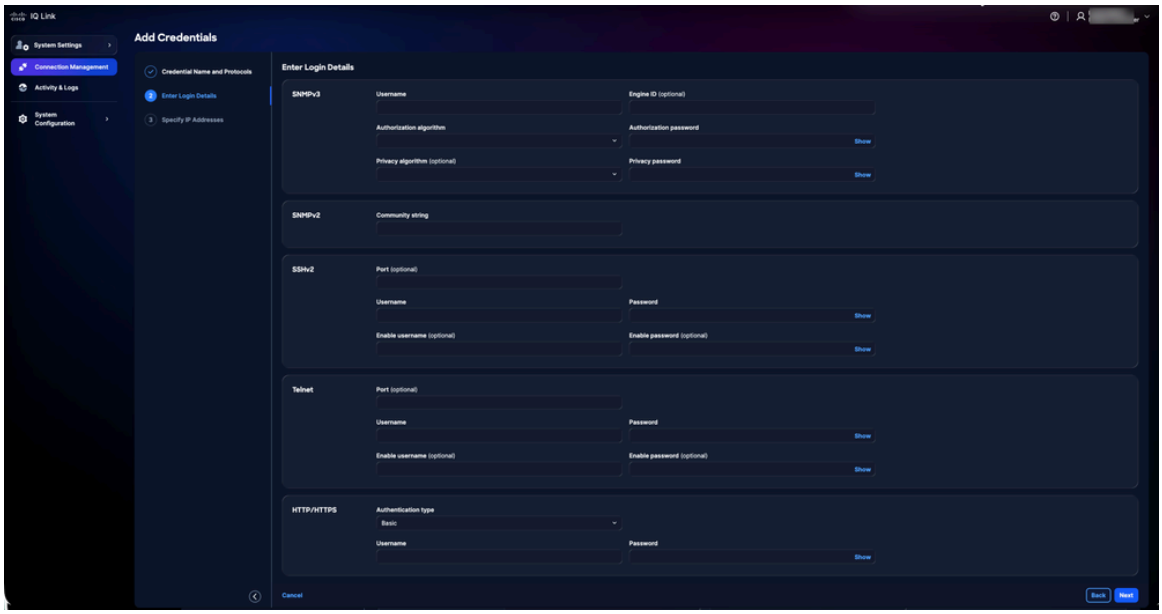
Onglet Informations d'identification

3. Cliquez sur Ajouter des informations d'identification.



Ajouter des identifiants

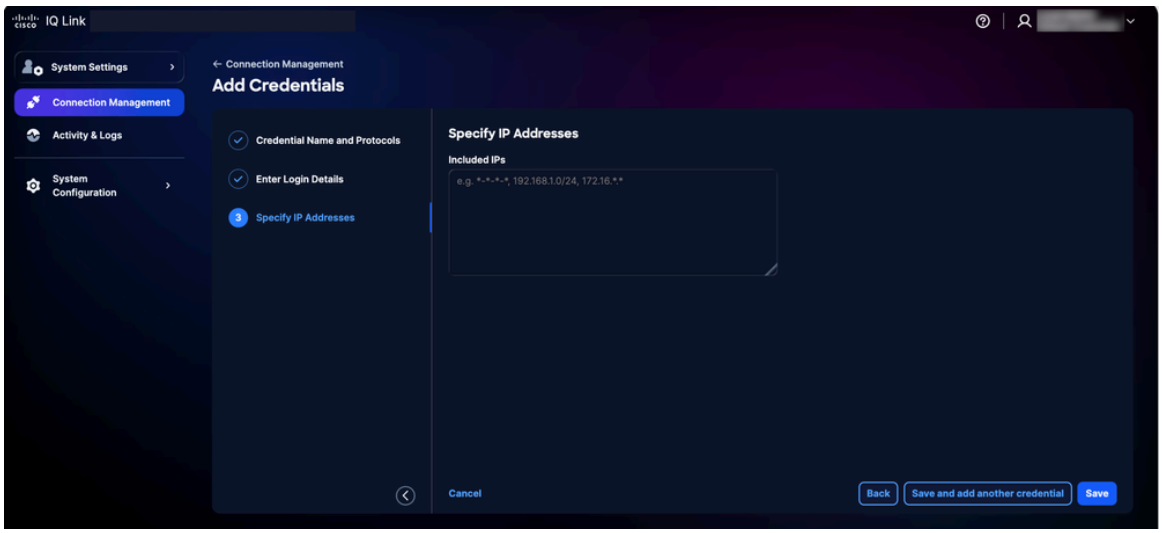
4. Saisissez Name.
5. Cochez toutes les cases du protocole applicable.
6. Cliquez sur Suivant.



Ajouter des informations d'identification

Remarque : Pour l'image ci-dessus, nous illustrons la vue lorsque tous les protocoles sont sélectionnés à l'étape précédente. Votre interface affiche uniquement les protocoles spécifiques que vous avez choisis.

7. Saisissez les informations de connexion pour chaque protocole sélectionné.
8. Cliquez sur Suivant.



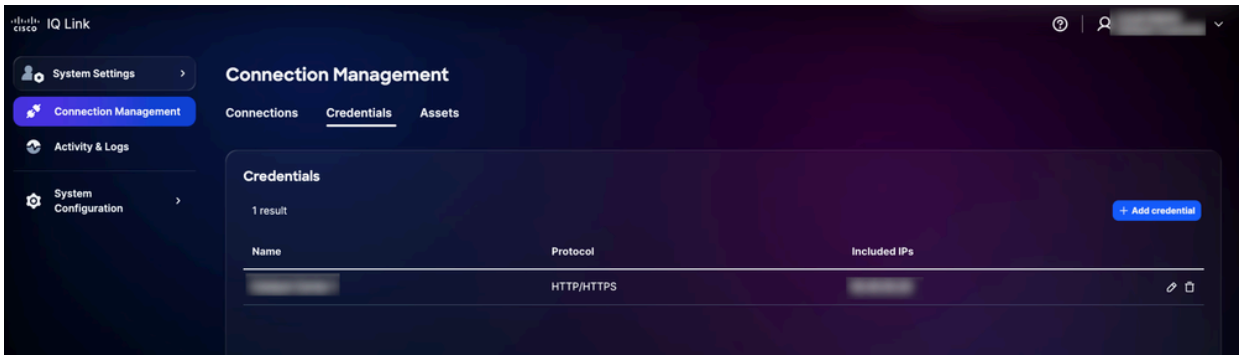
Spécifier les adresses IP

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



Informations d'identification ajoutées

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

Sélection des informations d'identification et logique correspondante

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

- Classement des priorités : Lorsque plusieurs jeux d'informations d'identification s'appliquent à un périphérique, Cisco IQ les évalue en fonction de leur correspondance spécifique avec le périphérique ; le système applique la priorité suivante, avec des correspondances plus spécifiques prioritaires :
    - Correspondance IP exacte : Priorité la plus élevée
    - Correspondance générique de fin :** **La priorité dépend du nombre d'étoiles de fin ; moins d'étoiles indiquent une correspondance plus spécifique et donc une priorité plus élevée
- Règles de mise en forme générique : Les caractères génériques (*) ne sont pris en charge que comme caractères de fin dans une adresse IP ; ils doivent être appliqués de droite à gauche.
    - Formats pris en charge :

      1.2.3.* (Priorité la plus élevée 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.

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)

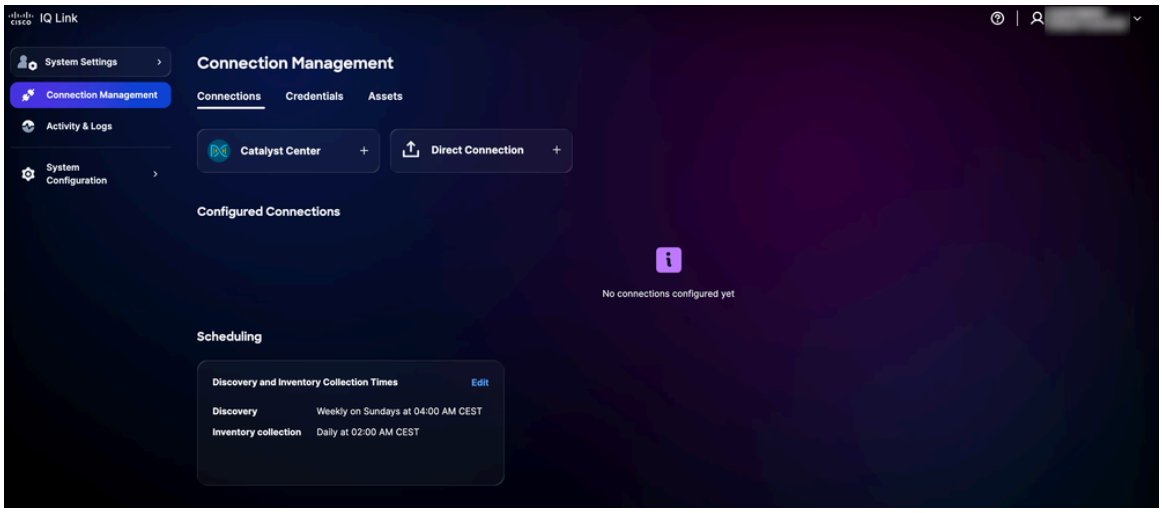
Remarque : Si un périphérique appartient à plusieurs catégories qui se chevauchent, le système sélectionne toujours l'ensemble d'informations d'identification ayant la plus grande spécificité (en d'autres termes, le moins de caractères génériques de fin).

Collecte de données avec Catalyst Center

Pour la collecte de données avec Catalyst Center :

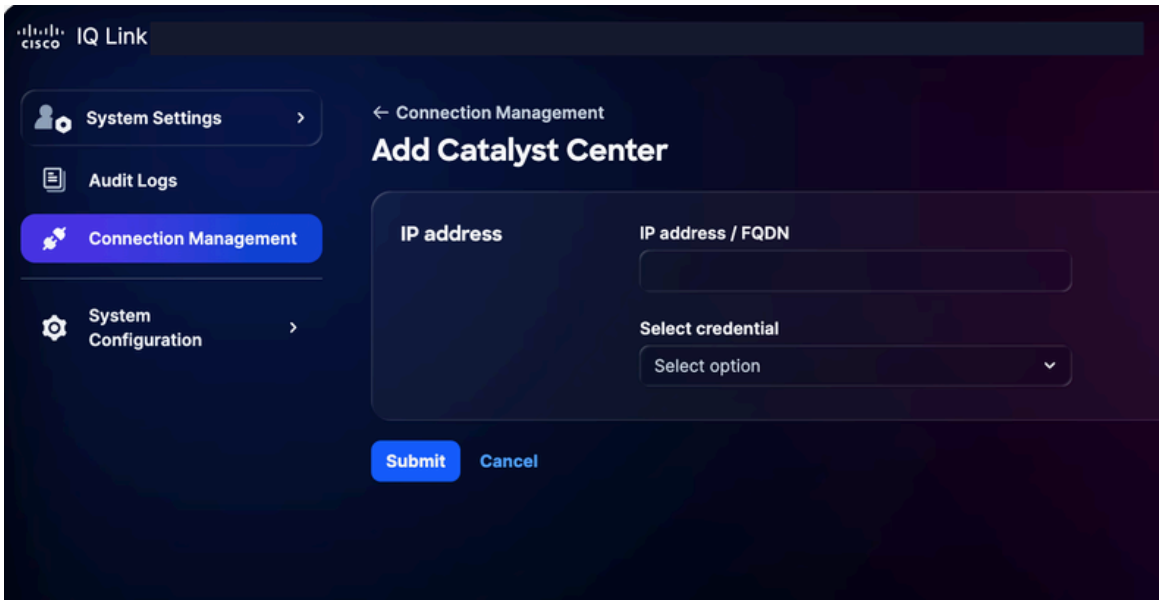
1. Dans Paramètres système, sélectionnez Gestion des connexions. La page Gestion des

connexions s'affiche.



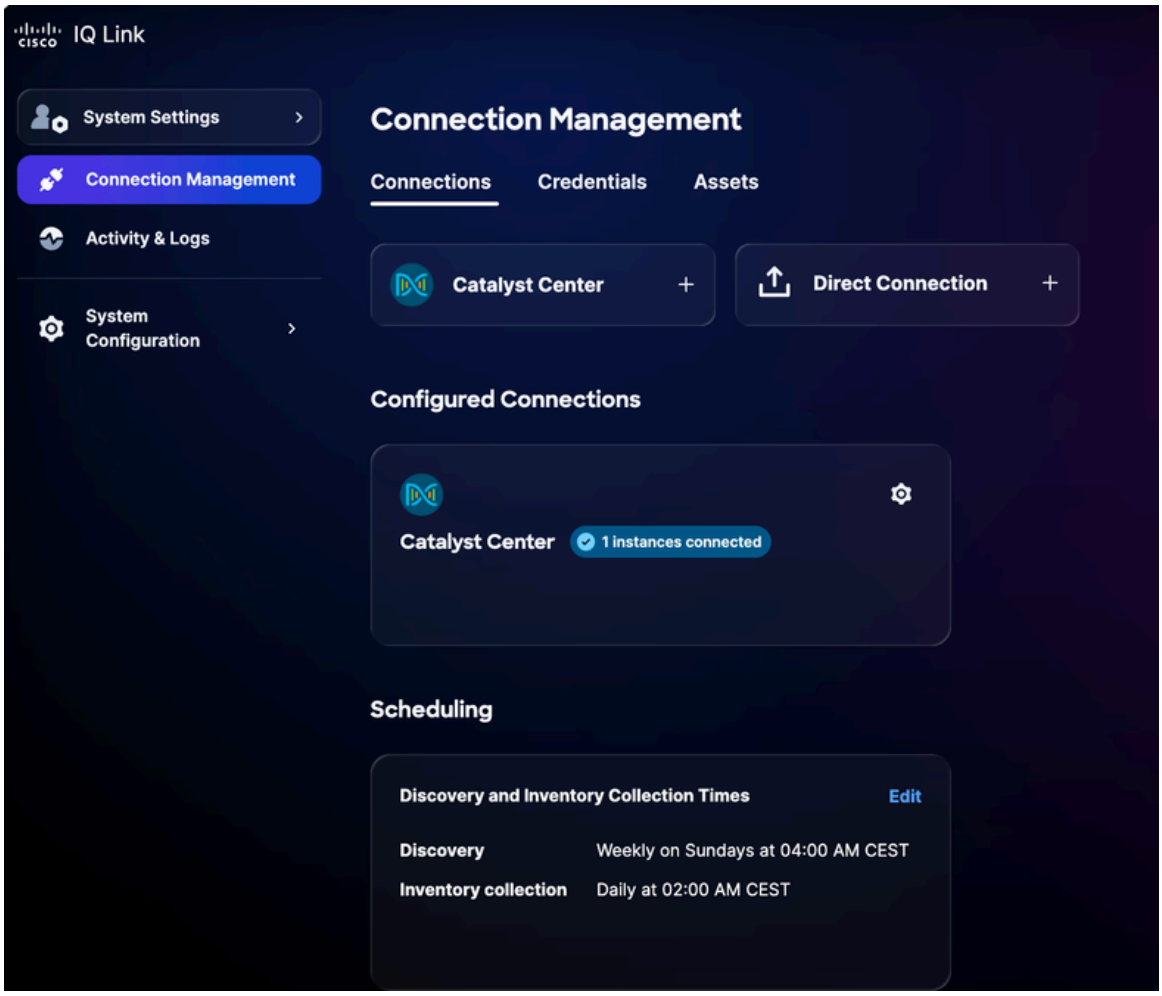
Gestion des connexions

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

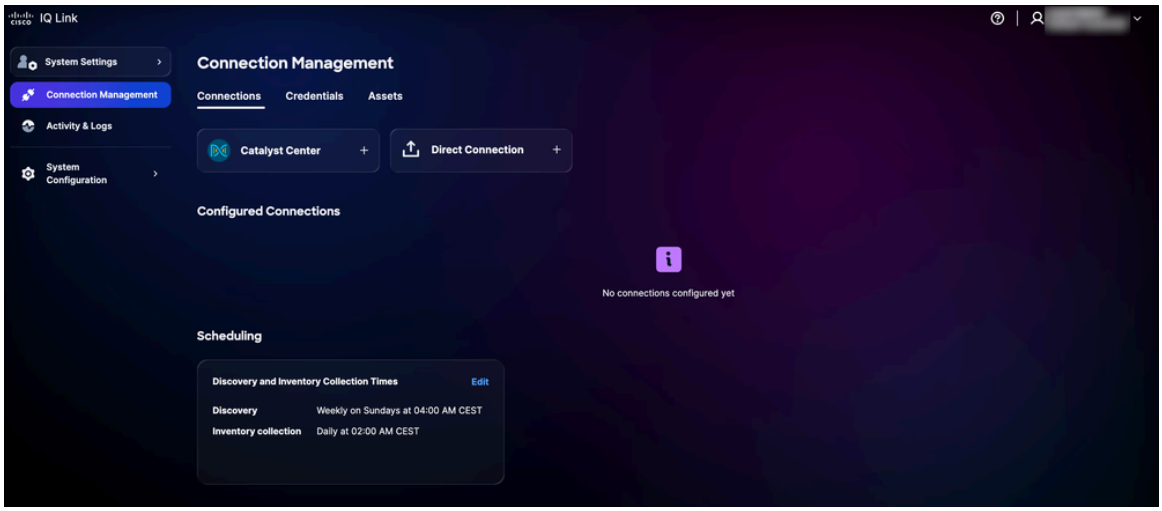
6. Planifier une collecte. Voir Planification pour plus de détails.

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

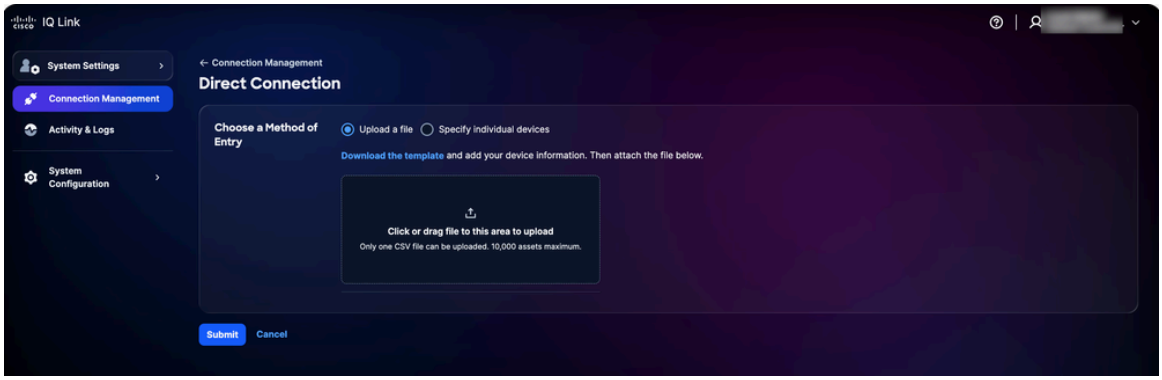
Pour ajouter des périphériques pour une connexion directe :

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



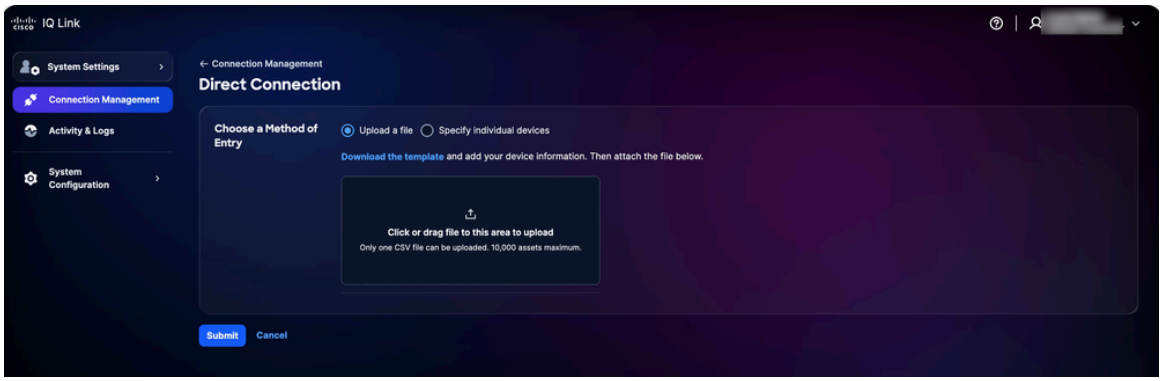
Gestion des connexions

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



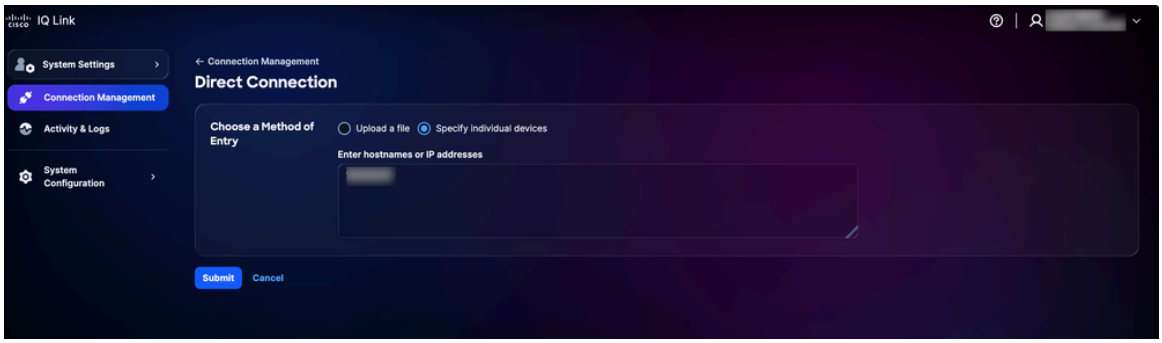
Télécharger le fichier

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.

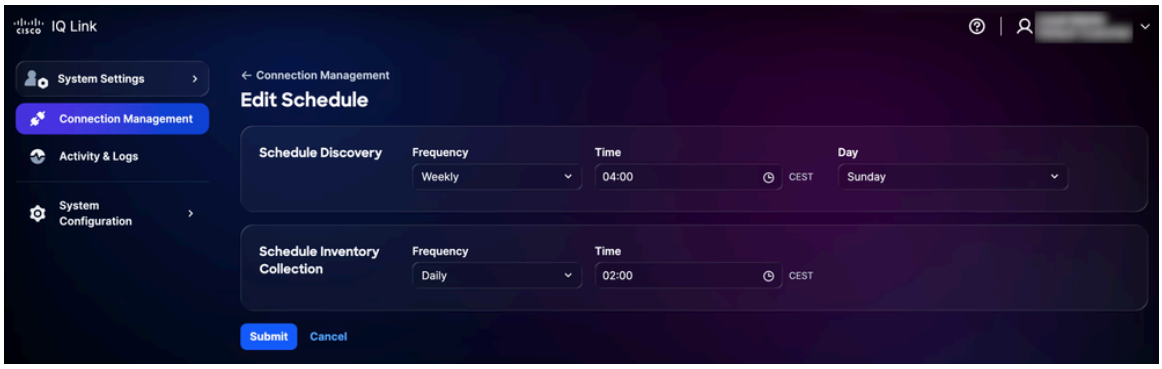
4. Planifier une collecte. Voir Planification pour plus de détails.

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.

Planification

La planification vous permet de définir quand Cisco IQ Link effectue la collecte de données automatisée. 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 peuvent configurer des bannières personnalisées qui s'affichent dans l'application.

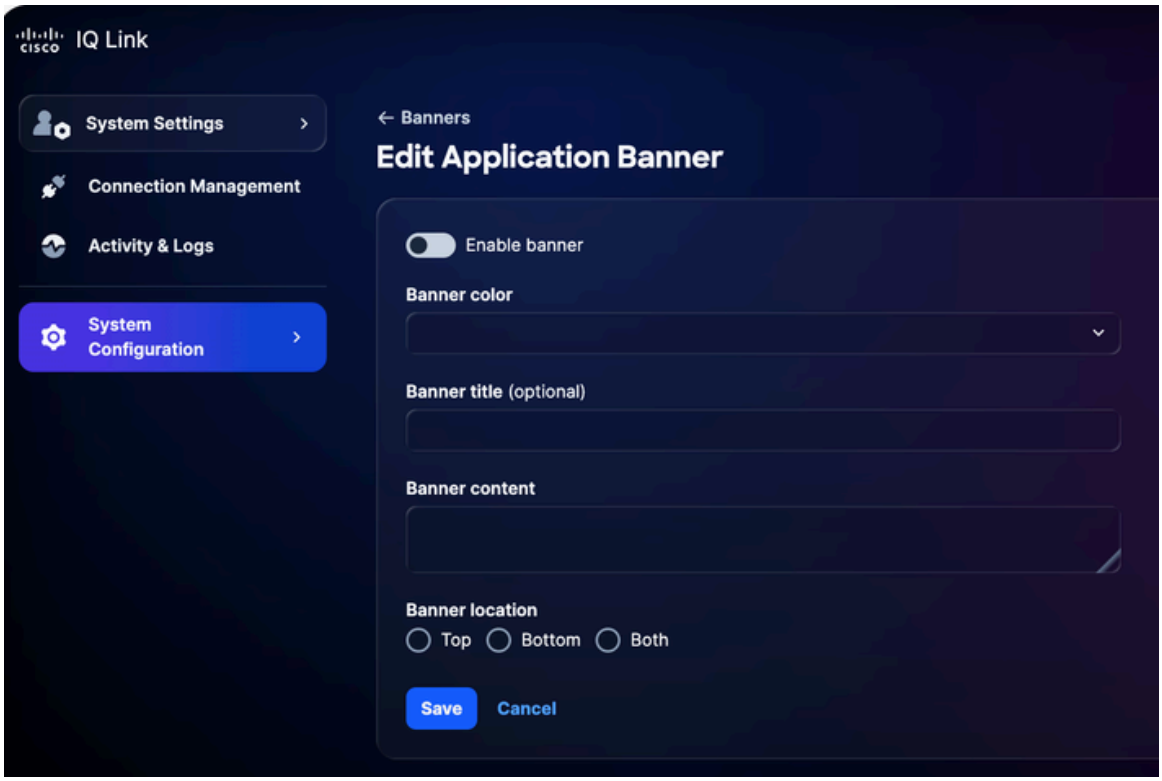
Configuration des bannières

Pour configurer une bannière :

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

Configurer la bannière

2. Cliquez sur Configurer. 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.

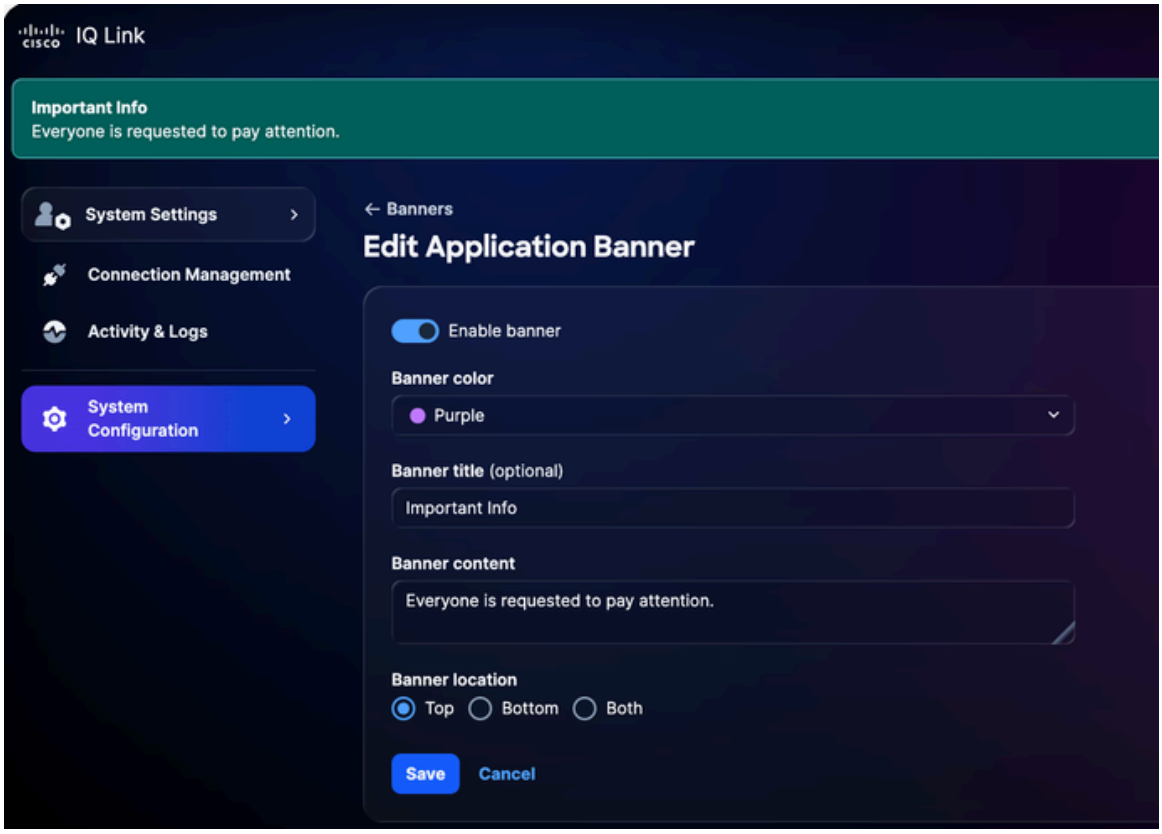
Modification des bannières

Pour modifier une bannière :

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

Modifier les bannières

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



Modifier la bannière d'application

3. Modifiez les détails souhaités.
4. Cliquez sur le bouton bascule pour activer ou désactiver la bannière.
5. Cliquez sur Save.

Dépannage

Les clients peuvent 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 :

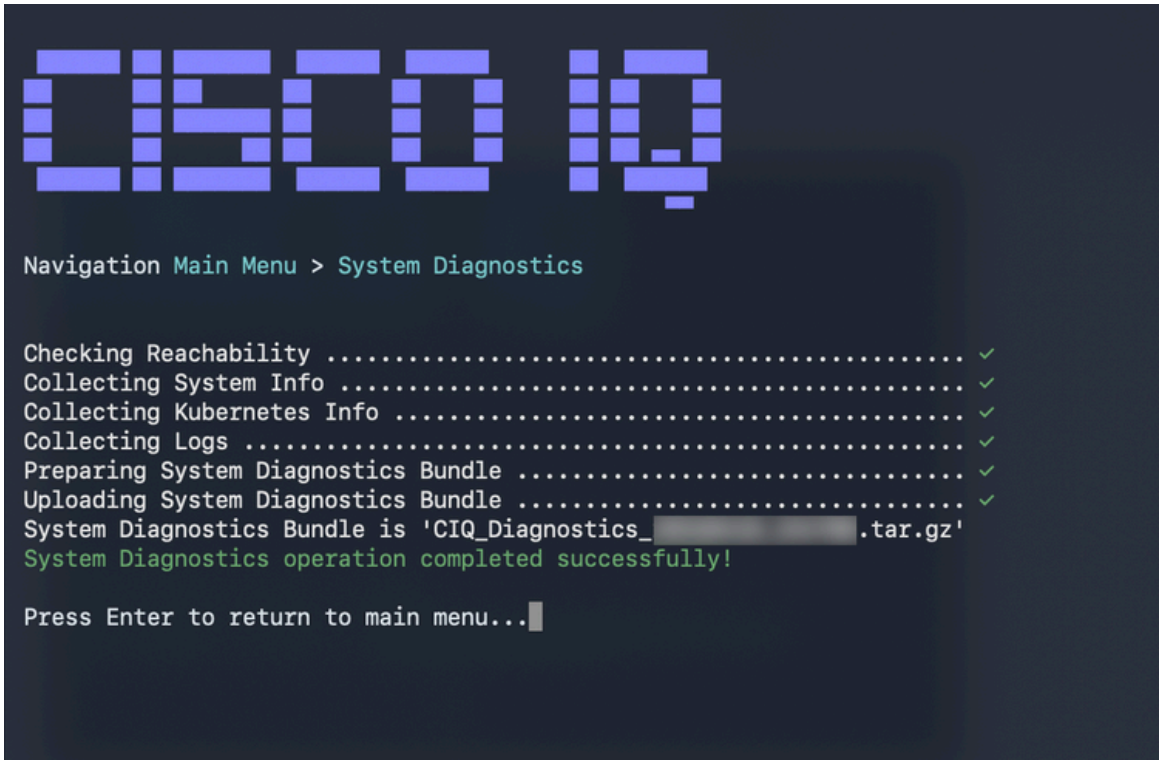
1. Connectez-vous à Cisco IQ.

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 du système Opération de diagnostic du CoSystème 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.