Cisco IQ Link Operations Guide v1.1.0

Introduzione

Cisco IQ™ offre ai clienti miglioramenti e funzionalità progettate per migliorare la visibilità degli asset, offrire informazioni più dettagliate sui propri ambienti e semplificare la gestione dei casi. Inoltre, le funzionalità di AI, come Cisco IQ AI Assistant, ottimizzano i risultati operativi e l'esperienza utente di Cisco IQ fornendo una comprensione contestuale che consente agli utenti di prendere decisioni proattive e informate e di semplificare i processi per il coinvolgimento e il successo del cliente.

Cisco IQ Link raccoglie e trasmette in modo sicuro la telemetria degli asset dalla rete locale a Cisco IQ, abilitando analisi predittive basate sull'IA che consentono di migliorare la visibilità della rete, anticipare i problemi e aumentare l'efficienza operativa.

Autenticazione locale

Per accedere a Cisco IQ Link, gli amministratori devono utilizzare le seguenti credenziali:

- Nome utente predefinito: admin
- Password predefinita: password impostata durante il processo di installazione di Cisco IQ Link; per ulteriori informazioni, vedere la Cisco IQ Link Getting Started Guide

Dopo l'accesso, nella home page vengono visualizzati l'utente predefinito "admin" e il nome dell'account "Default-Customer".

Impostazione della protezione dell'amministratore locale

È possibile modificare la password e impostare le domande di sicurezza tramite il menu Local Admin Security in System Configuration.

Si hanno a disposizione tre (3) tentativi per immettere la password corretta entro un periodo di dieci (10) minuti. Se tutti e tre (3) i tentativi hanno esito negativo, l'account viene temporaneamente bloccato per 60 minuti per proteggere la protezione.

Non è possibile tentare l'accesso durante il periodo di blocco. Viene visualizzato il messaggio:

"Account bloccato a causa di troppi tentativi non riusciti. Riprova più tardi.", inclusa l'ora di scadenza del blocco.

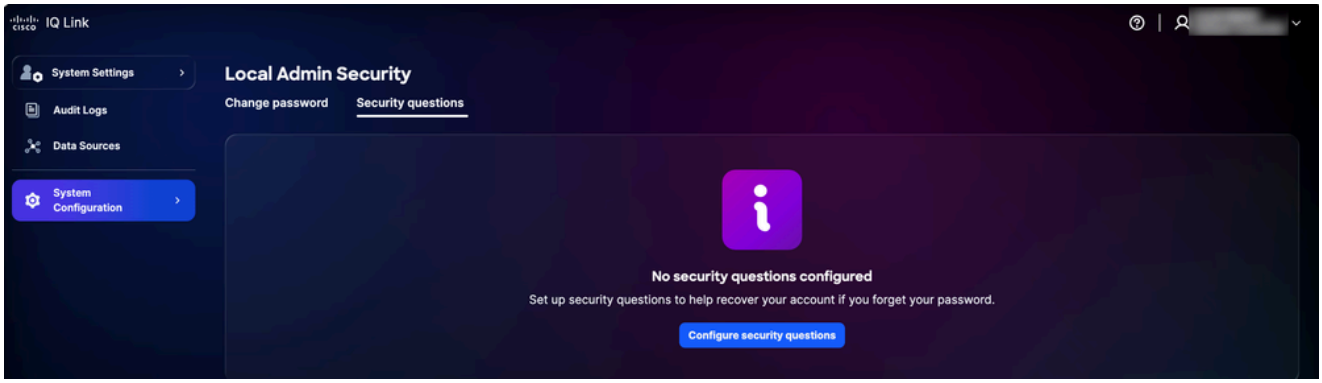
L'account si sblocca automaticamente dopo 60 minuti. A questo punto è possibile tentare di accedere o reimpostare la password.

Impostazione di domande e risposte di sicurezza

Le domande di sicurezza aiutano a verificare la tua identità se dimentichi la password. Per abilitare la funzionalità di reimpostazione della password, gli amministratori devono impostare le risposte a cinque (5) domande di sicurezza. Si tratta di un'installazione unica.

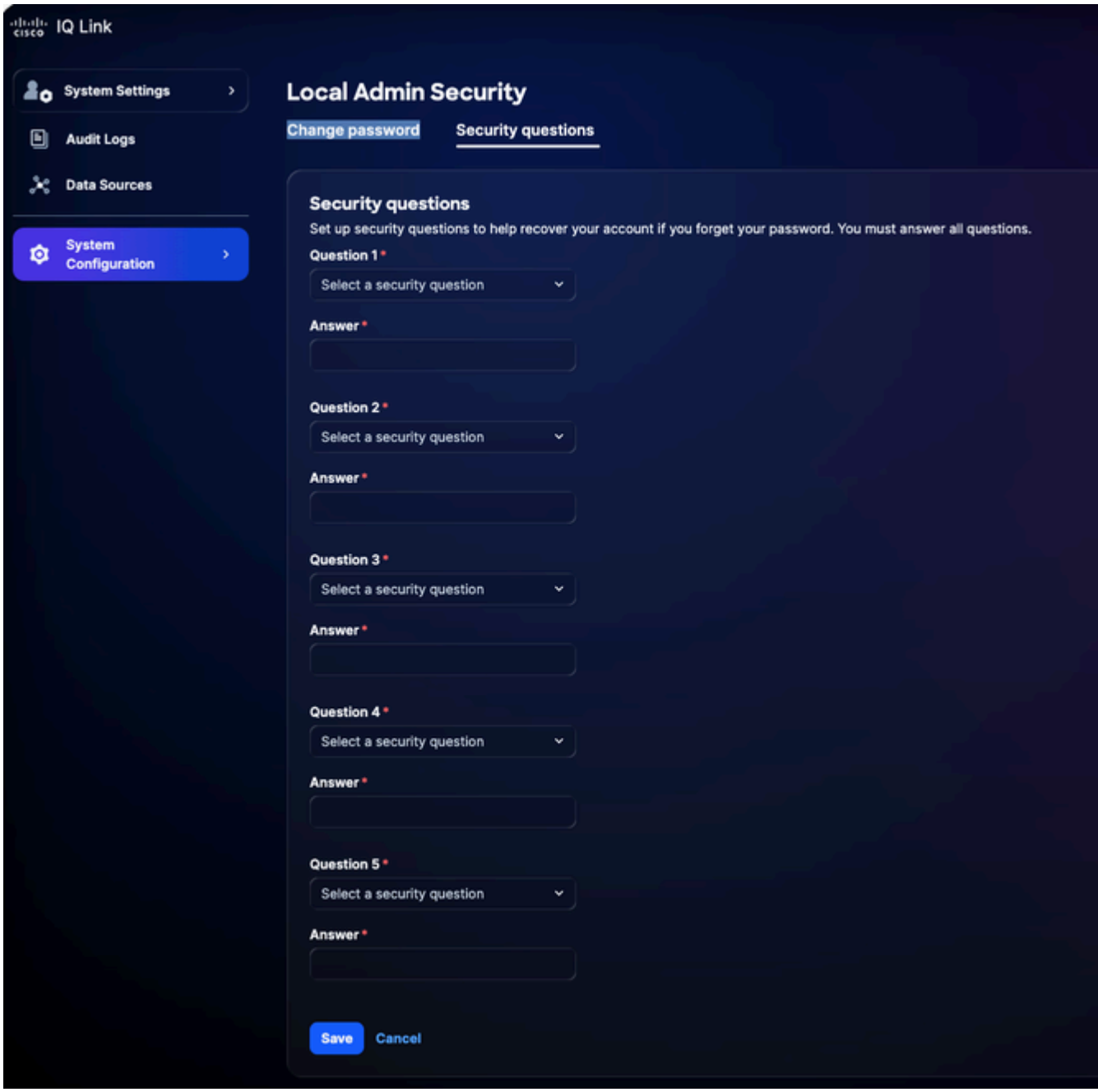
Per impostare le domande di sicurezza:

1. Da Impostazioni di sistema, scegliere Configurazione di sistema > Protezione amministratore locale > Domande di sicurezza.



Domande di sicurezza

2. Fare clic su Configura domande di sicurezza.



Domande di sicurezza

3. Scegliere cinque (5) domande di sicurezza dagli elenchi a discesa.

4. Inserisci la tua risposta per ogni domanda.

5. Fare clic su Save (Salva).

Note:
· Le risposte non distinguono tra maiuscole e minuscole; ad esempio, "SMITH" e "smith" sono considerati uguali
· Gli spazi in eccesso vengono ignorati, il che significa che "Smith" e "Smith" vengono trattati allo stesso modo

---

Nota: Se necessario, è possibile aggiornare le risposte in un secondo momento. Quando si aggiornano le risposte, tutte le risposte precedenti vengono sostituite, pertanto è necessario fornire di nuovo le risposte a tutte e cinque le domande (5) e non solo a quelle che si desidera modificare.

Gestione delle password

La password di Cisco IQ può essere gestita solo dagli amministratori locali.

Prerequisiti

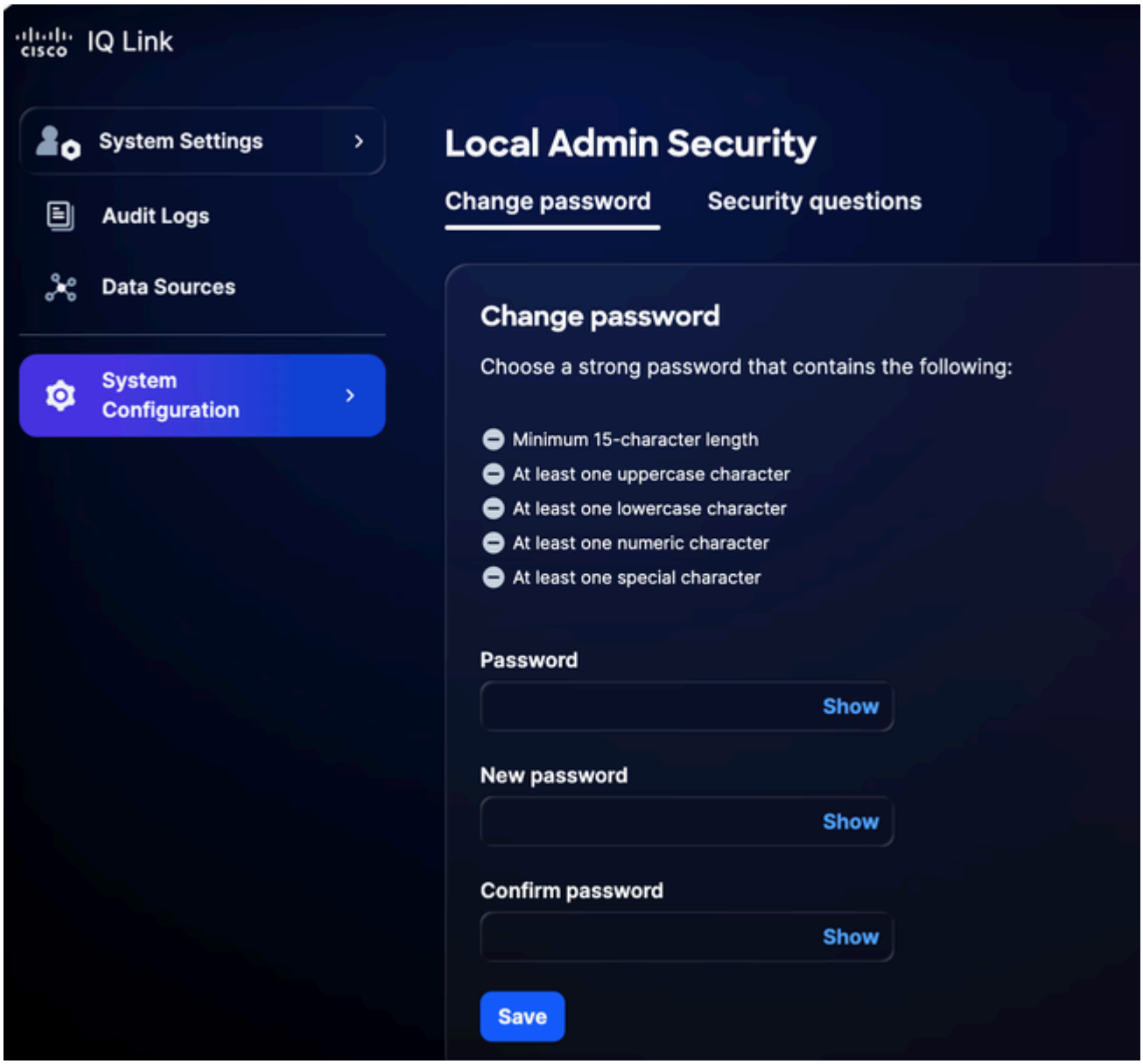
Per gestire le password, è necessario che siano soddisfatte le seguenti condizioni:

- L'utente corrente è un amministratore locale
- Si sta utilizzando un account Administrator locale (non Single Sign-On (SSO) o autenticazione esterna)
- Sei connesso a Cisco IQ
- Si conosce la password corrente

Modifica delle password

Per modificare la password:

1. Da System Settings (Impostazioni di sistema), selezionare System Configuration (Configurazione di sistema) > Local Admin Security (Protezione amministratore locale) > Change Password (Modifica password).



Cambia password

2. Immettere la password corrente.
3. Immettere la nuova password.
4. Immettere nuovamente la nuova password per confermarla.
5. Fare clic su Save (Salva).

La password viene aggiornata nel sistema Cisco IQ, inclusa la macchina virtuale Cisco IQ (VM).

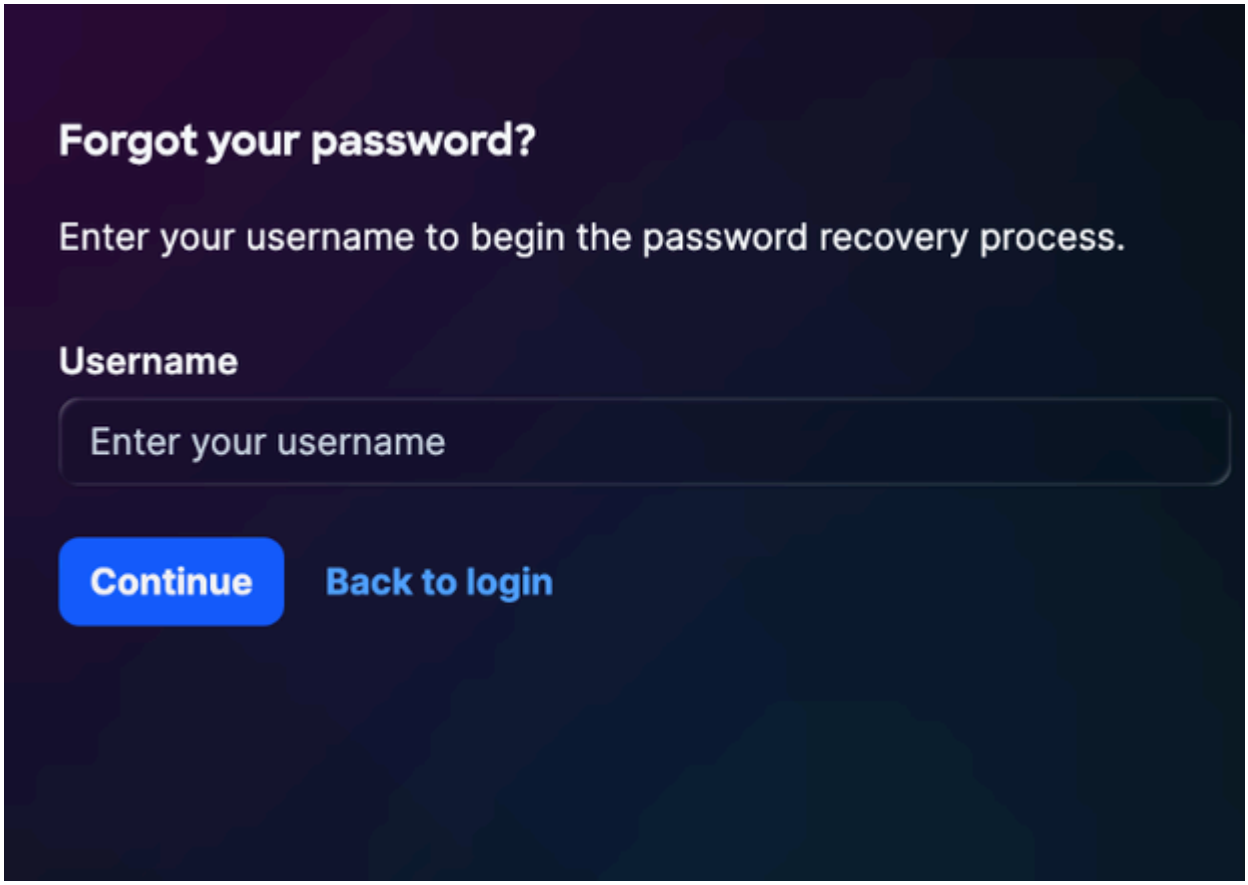
Reimpostazione di una password dimenticata

Se le domande di sicurezza sono state impostate in precedenza, è possibile reimpostare una password dimenticata utilizzando il processo di verifica delle domande di sicurezza. Per ulteriori

informazioni, vedere Impostazione di domande e risposte di protezione.

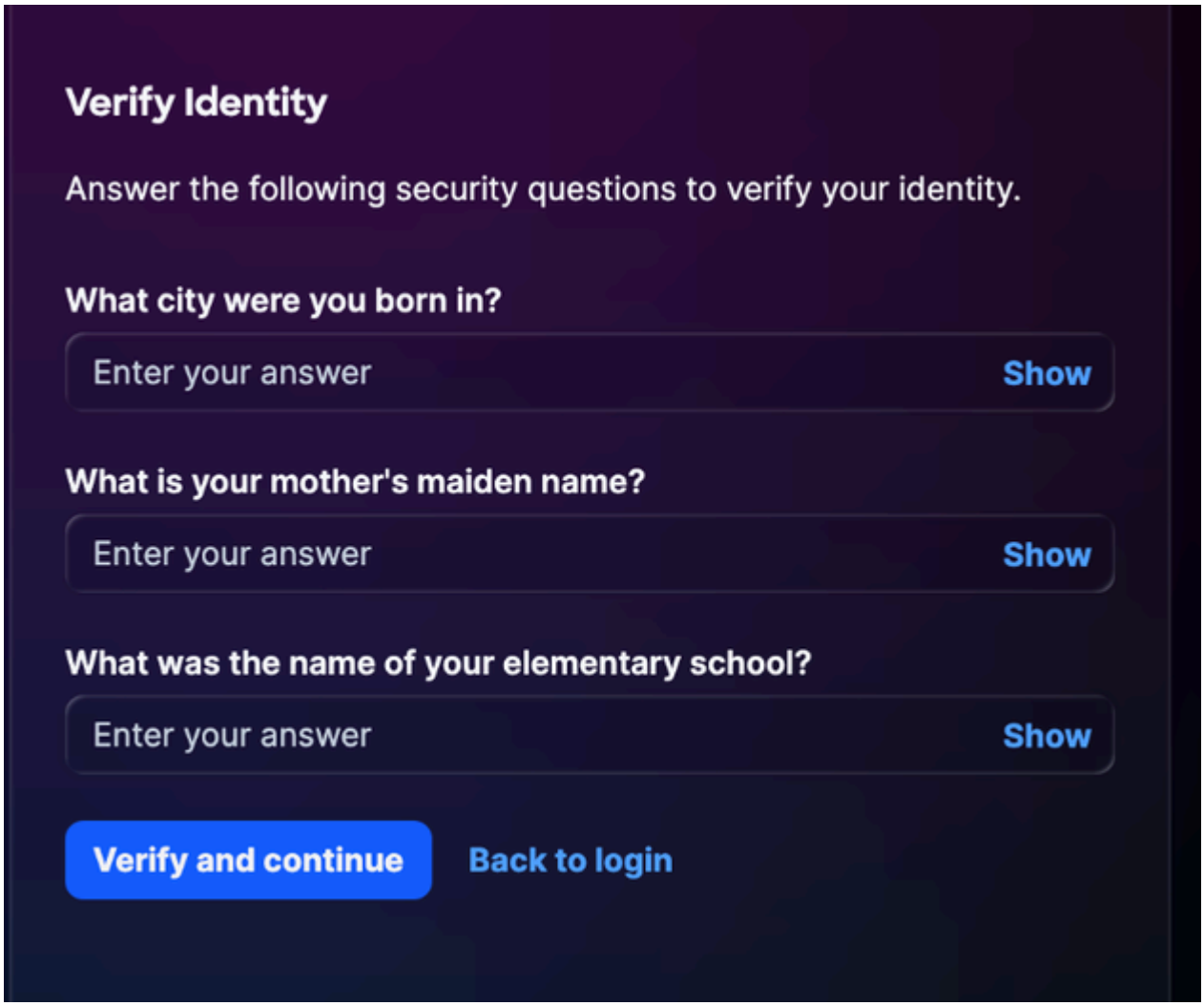
Per reimpostare una password dimenticata:

1. Passare alla pagina di accesso di Cisco IQ Link.
2. Fare clic su Password dimenticata.



Password dimenticata

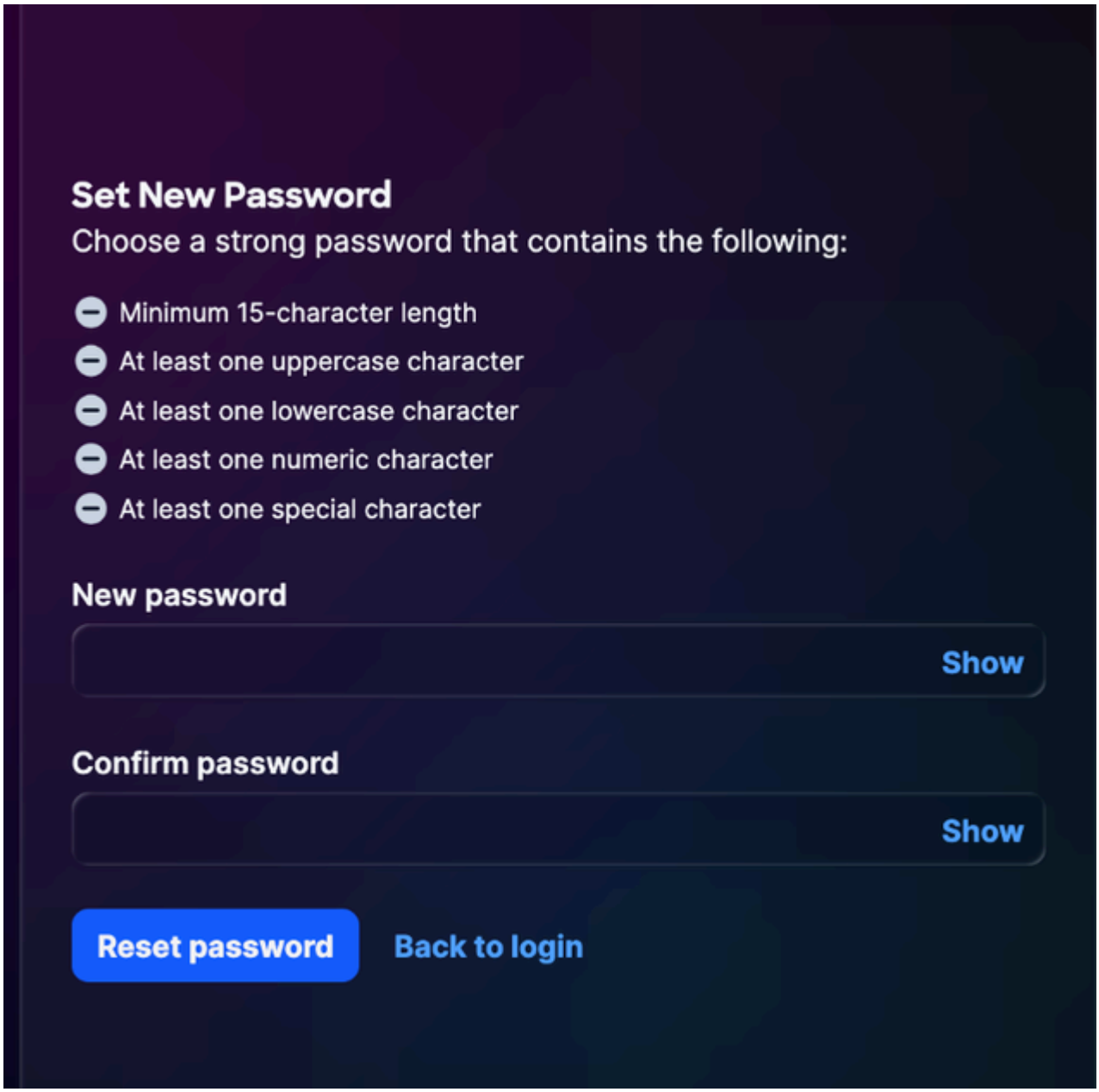
3. Immettere il nome utente.
4. Fare clic su Continue (Continua). La pagina Verifica identità visualizza tre (3) domande di sicurezza casuali sulle cinque (5) domande configurate in precedenza.



Verifica identità

Nota: Le domande di sicurezza sopra riportate sono specifiche per ogni utente e variano di conseguenza.

5. Inserire le risposte per tutte e tre (3) le domande visualizzate.
6. Fare clic su Verifica e continuare. Se la risposta inviata corrisponde alle risposte salvate in precedenza, verrà richiesto di immettere una nuova password.



Reimposta password

Nota: Hai a disposizione tre (3) tentativi per rispondere correttamente alle domande di sicurezza entro un periodo di dieci (10) minuti. Se tutti e tre (3) i tentativi hanno esito negativo, l'account viene temporaneamente bloccato per 60 minuti per proteggere la protezione.

Non è possibile reimpostare la password durante il periodo di blocco. Viene visualizzato il messaggio: "Account bloccato a causa di troppi tentativi di verifica non riusciti. Riprova più tardi.", inclusa l'ora di scadenza del blocco.

L'account si sblocca automaticamente dopo 60 minuti. A questo punto è possibile tentare di accedere o reimpostare la password.

---

7. Immettere la nuova password.

8. Immettere nuovamente la password per confermarla.

9. Fare clic su Invia.

Configurazione del provider di identità

Dopo aver eseguito l'accesso a Cisco IQ Link, gli amministratori possono configurare varie impostazioni. Gli amministratori possono accedere a Cisco IQ Link utilizzando l'amministrazione locale o la configurazione del provider di identità (IDP).

Configurazione SAML IDP Okta per SSO

Prerequisiti per la configurazione di SAML IDP

- Accesso come amministratore locale al collegamento Cisco IQ
- Accesso al portale IDP

Configurazione SAML IDP per SSO

Per configurare IDP Security Assertion Markup Language (SAML) per SSO:

1. Passare al portale IDP.
2. Impostare gli attributi seguenti per l'istanza di Cisco IQ Link.

Attributi collegamento Cisco IQ

Campo	Valore
Nome applicazione	<Nome applicazione>
Ambiente	Applicazione aziendale ESP
Gruppi di proprietari applicazione	Proprietario delle impostazioni IDP
Mailer team	Mailer per il team

Campo	Valore
Destinatari	Non forza lavoro
Categoria caricamento	Selezionare "New Onboarding" (Nuovo caricamento)

Parametri di configurazione SAML

Parametro	Configurazione	Esempio
Destinatari (ID entità)	Nome FQDN	mymanagementhost.mydomain.com
URL Single Sign-On	Endpoint ACS SAML	https://mymanagementhost.mydomain.com/saml/acs
Formato ID nome	Indirizzo email	N/D
Nome utente applicazione	Username	N/D

3. Configurare le seguenti istruzioni di attributo obbligatorie.

Nota: Le modifiche agli attributi IDP dipendono dal provider e dalla configurazione specifici. Di seguito vengono illustrati l'IDP Cisco e i relativi attributi.

- Prima voce
    - Nome: Username
    - Valore: user.login
- Seconda voce
    - Nome: Posta elettronica primaria
    - Valore: user.email
- Istruzioni di attributi di gruppo
    - Nome: gruppi

- Filtro: REGEX
- Valore: .*

4. Configurare le impostazioni SLO (Single Logout) nell'applicazione.

Impostazioni di configurazione SLO

Campo	Valore
Certificato di firma	Per Okta, questo certificato è necessario solo se si sceglie di abilitare SLO. Scaricare il certificato di firma utilizzando il download del certificato SP nei provider di identità. Salvare il file come sp-public-key.crt. Per ulteriori informazioni, vedere Configurazione della disconnessione singola.
Metadati SP	I metadati SP sono necessari solo per l'IDP ADFS (e non per Okta).
Abilitare la disconnessione singola?	Sì o No
URL di disconnessione singolo	https://mymanagementhost.mydomain.com/saml/logout
Autorità emittente SP (ID gruppo di destinatari/entità o URL ACS)	https://mymanagementhost.mydomain.com

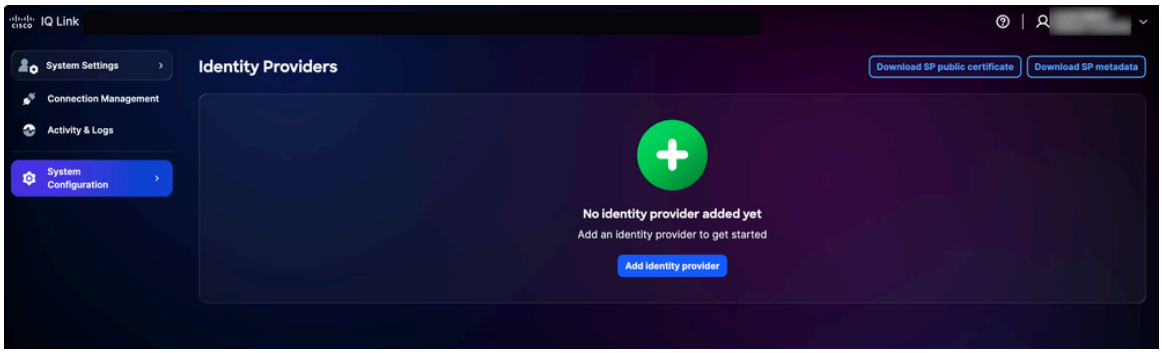
5. Fare clic sull'icona Download per scaricare il file "SP Metadata".

6. Eseguire il provisioning o creare l'applicazione come richiesto dal provider.

Aggiunta di IDP

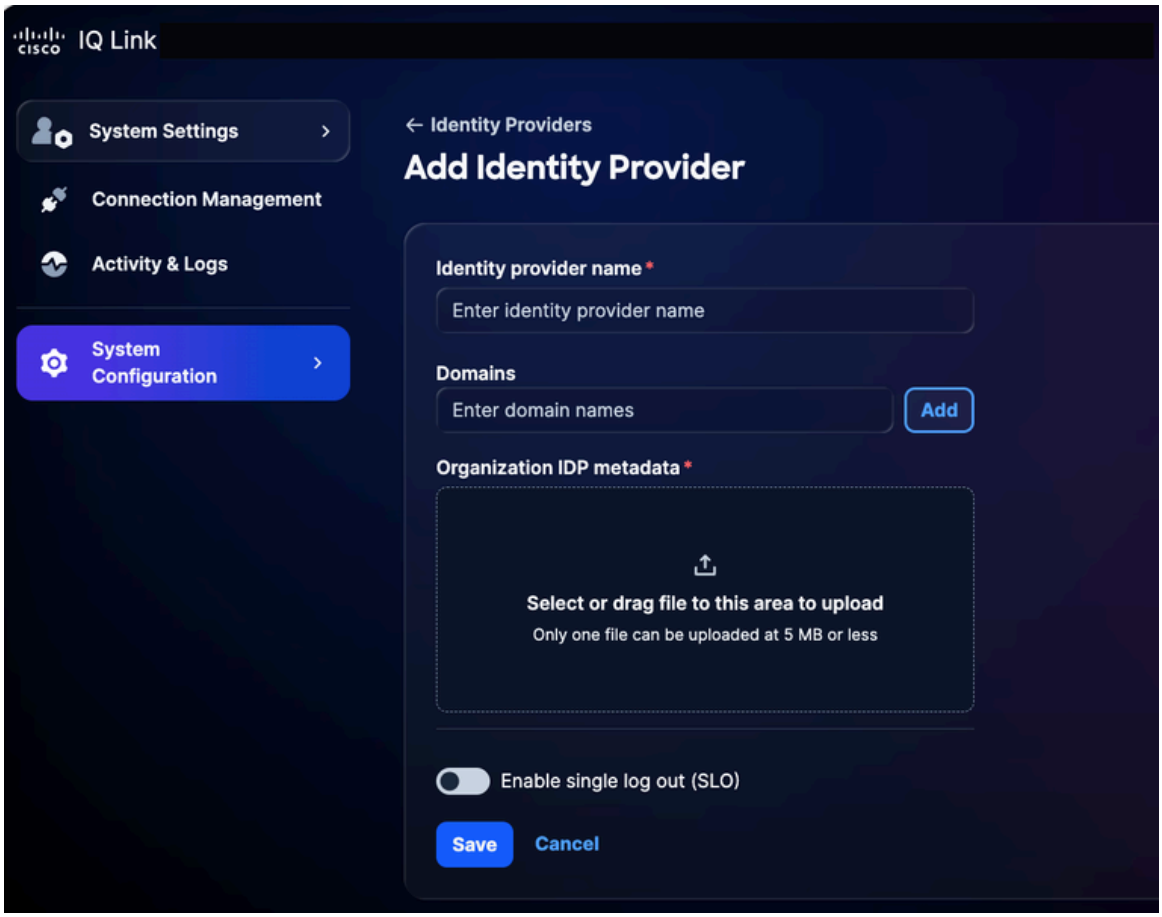
Per aggiungere un IDP in Cisco IQ Link:

1. Da Impostazioni di sistema, scegliere Configurazione di sistema > Provider di identità. Viene visualizzata la pagina Provider di identità.



Home page di IDP

2. Fare clic su Aggiungi provider di identità. Viene visualizzata la pagina Aggiungi provider di identità.



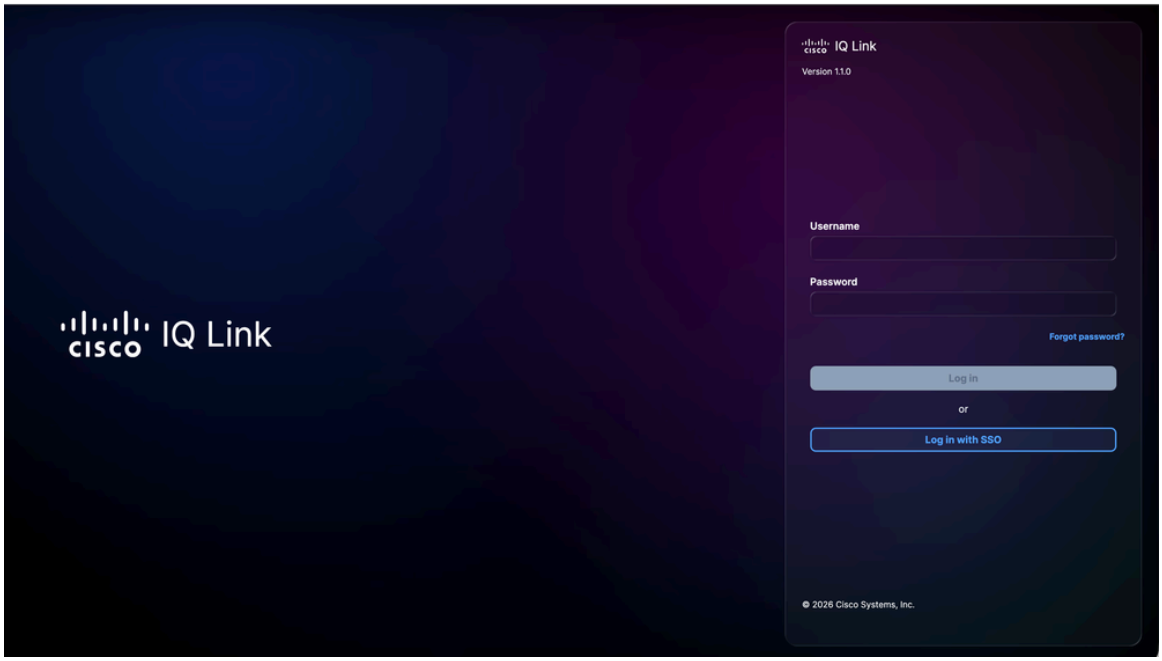
Aggiungi provider di identità

Nota: È possibile aggiungere un solo (1) IDP alla volta.

3. Immettere il nome del provider di identità.

4. Fare clic su Add (Aggiungi) per aggiungere un nome di dominio configurato dal collegamento Cisco IQ al campo Domini.

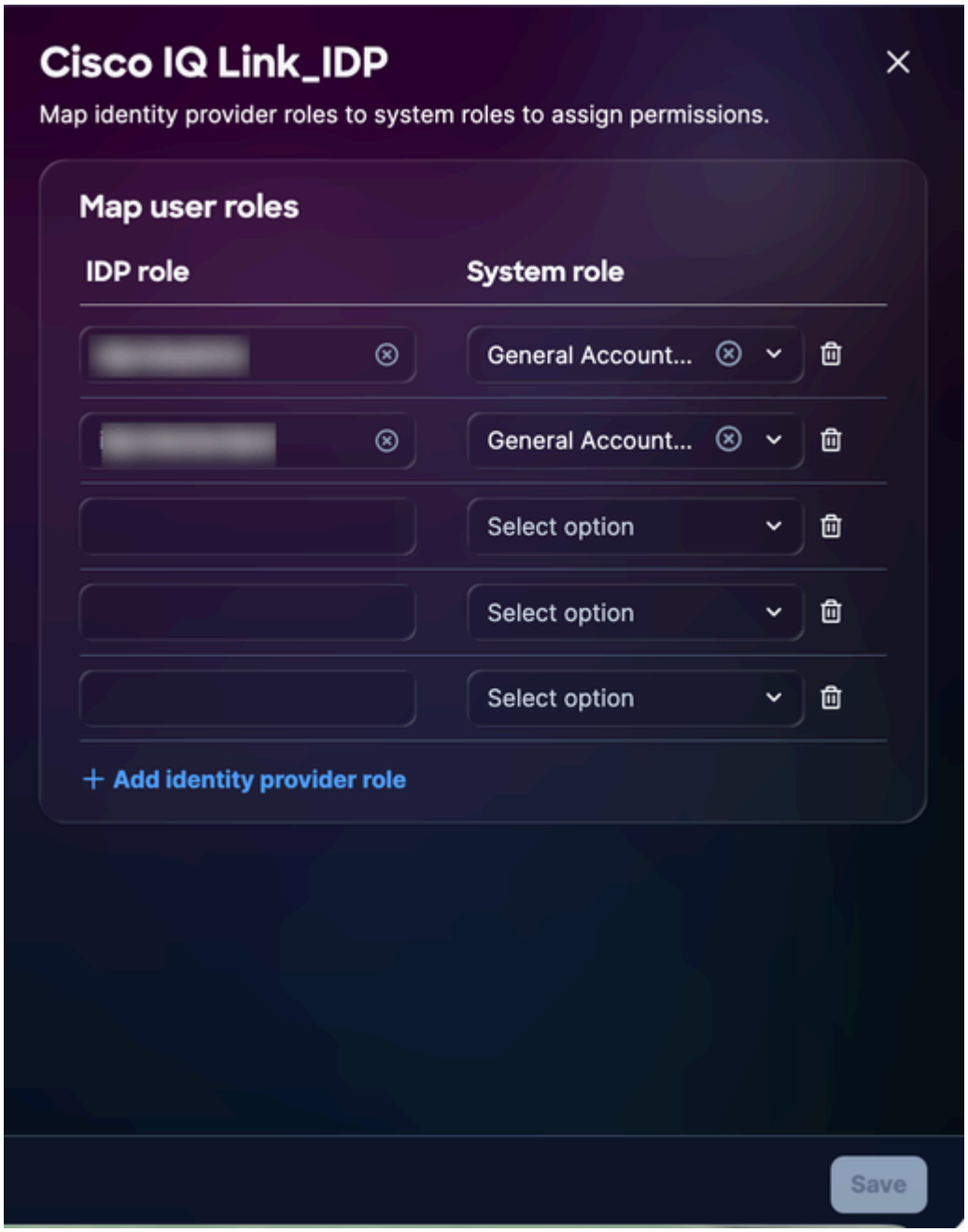
5. Trascinare o caricare il file di metadati SAML ottenuto dall'applicazione IDP nel campo metadati IDP organizzazione. Questo file contiene i dettagli del certificato e i dettagli dell'entità del provider di servizi (SP).
6. (Facoltativo) Attivare il pulsante Abilita disconnessione singola. È possibile attivare lo SLO anche in un secondo momento.
7. Fare clic su Save (Salva).
8. Una volta configurata, la pagina di login visualizza un'opzione per eseguire il login con SSO (tramite IDP).



Login al collegamento Cisco IQ

Configurazione mapping ruoli

1. Dall'IDP aggiunto, selezionare l'icona Altre opzioni > Mappa ruoli. Viene visualizzata la pagina Mapping ruoli utente.



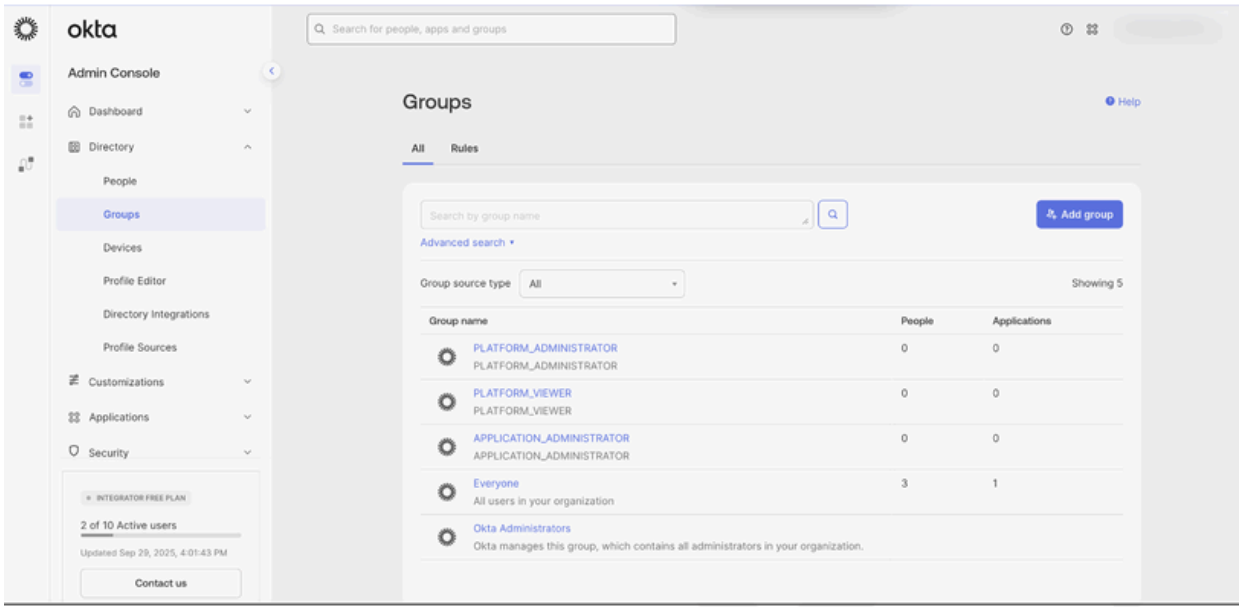
Mapping ruoli utente

2. Immettere un ruolo IDP per il ruolo di sistema selezionato. Sono supportati i seguenti ruoli di sistema:

    - _amministratore account_generale: L'amministratore dell'account generale dispone di autorizzazioni complete per eseguire tutte le azioni nel prodotto
    - _visualizzatore account_generale: Il visualizzatore di account generale dispone di accesso in sola lettura

---

Nota: Il ruolo IDP è un campo di testo aperto. Deve corrispondere esattamente al nome del gruppo o del ruolo configurato nell'IDP dell'organizzazione. Di seguito è riportato un esempio di gruppi Okta.



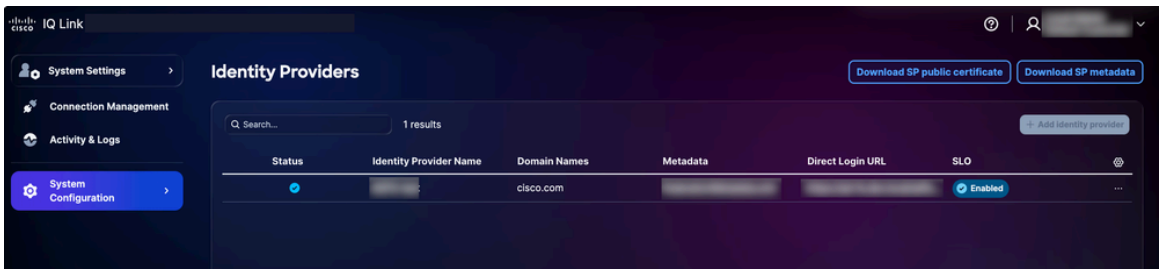
Riferimento mapping ruoli

3. Eseguire il mapping di ruoli aggiuntivi in base alle esigenze facendo clic su Aggiungi ruolo provider di identità.
4. Fare clic su Save (Salva).

Configurazione disconnessione singola

Se si sceglie di abilitare SLO, è necessario caricare i metadati che includono l'URL SLO. È possibile configurare questa impostazione modificando le impostazioni del provider di identità e attivando l'opzione Abilita disconnessione singola. Per completare la configurazione dello SLO:

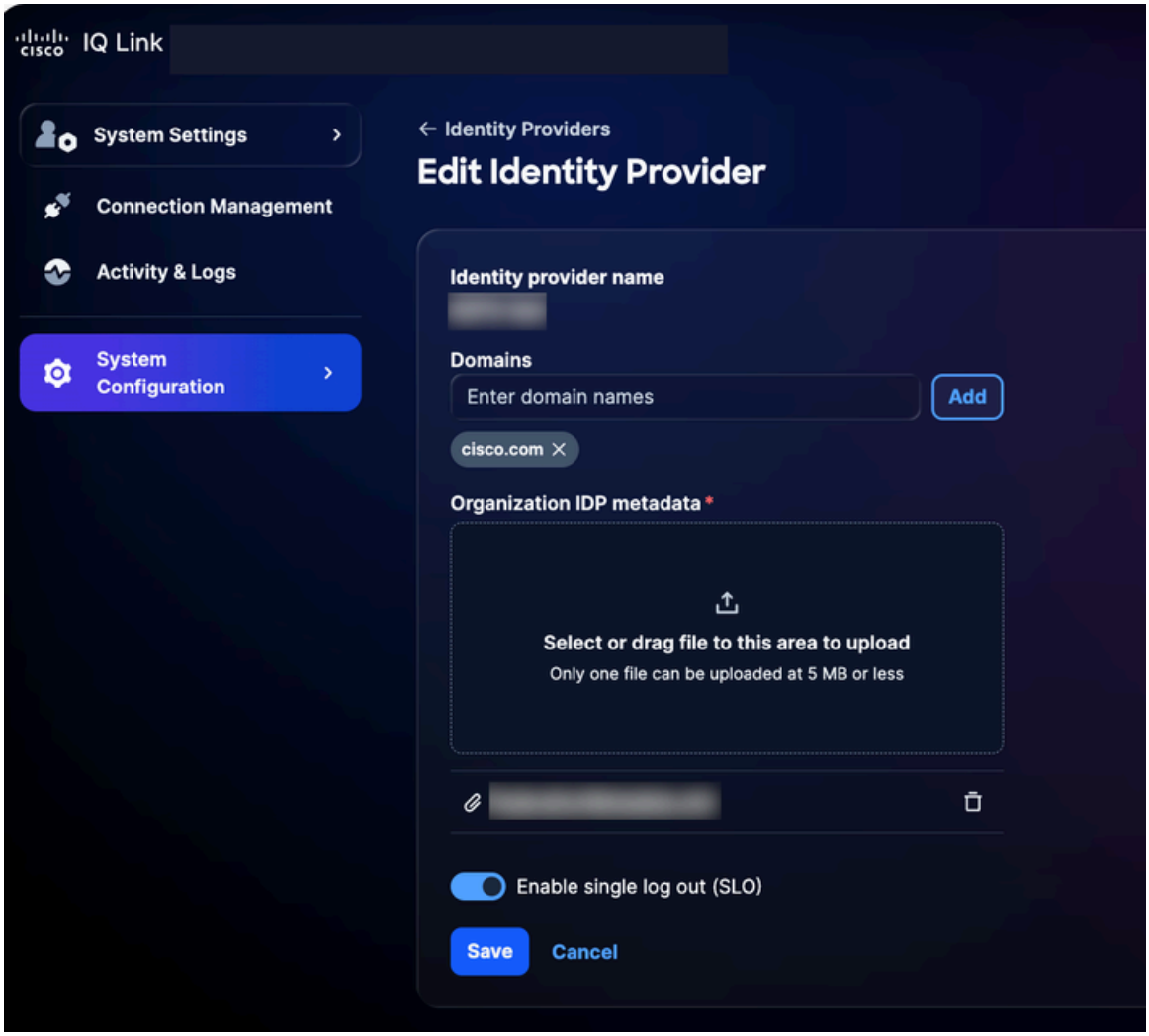
1. Dalla pagina Provider di identità, fare clic su Scarica certificato pubblico SP.



Scarica certificato pubblico

2. Salvare il file scaricato come sp-public-key.crt.
3. Passare al portale IDP.
4. Caricare il file del certificato di firma generato nella sezione Configurazione SAML IDP per SSO.

5. Scaricate nuovamente il file di metadati IDP.
6. Nella pagina Provider di identità, scegliere l'icona Altre opzioni dell'IDP aggiunto > Modifica.



Modifica provider di identità

7. Attivare il pulsante Attiva disconnessione singola (SLO).
8. Caricare il file di metadati appena scaricato.
9. Utilizzare l'elenco di controllo seguente per verificare la funzionalità SSO e SLO:

Elenco di controllo per la verifica:

- Accesso dell'amministratore locale riuscito
- Il portale IDP è configurato e sottoposto a provisioning
- L'IDP viene aggiunto a Cisco IQ con lo stato "Operazione riuscita"
- I mapping dei ruoli vengono configurati e testati

- I metadati SP vengono scaricati ed estratti
- Se SLO è abilitato, la configurazione SLO è completata con il certificato di firma reale
- Il flusso SSO/SLO end-to-end è stato testato

Risoluzione dei problemi relativi a IDP

L'elenco seguente descrive i problemi comuni e le possibili soluzioni per identificare e risolvere rapidamente i problemi relativi allo stato IDP, agli errori dei certificati, agli errori di accesso SSO e alla configurazione degli SLO:

Risoluzione dei problemi

Problema	Soluzione
Lo stato dell'IDP è "Incompleto"	Verificare le configurazioni di mapping dei ruoli
Errori certificato	Verifica del formato e della validità del certificato
Errori di accesso SSO	Convalida mapping di attributi e assegnazioni di gruppi
SLO non funzionante come previsto	Verificare che il certificato sia caricato correttamente e che gli URL SLO siano configurati

Configurazione SAML IDP ADFS per SSO

In questa sezione vengono fornite indicazioni per configurare Microsoft Active Directory Federation Services (ADFS) come provider di identità SAML per Cisco IQ.

Prerequisiti per configurare SAML IDP ADFS per SSO

- Si consiglia ADFS 6.0+
- Windows Server 2012 R2+
- Integrazione con Active Directory configurata
- Certificati SSL/TLS su ADFS
- Accesso come amministratore a Cisco IQ
- Accesso amministrativo al server ADFS (Windows Server)
- Accesso PowerShell al server ADFS
- Connettività di rete tra ADFS e Cisco IQ
- Dettagli di configurazione del server ADFS (come indicato nella tabella seguente)

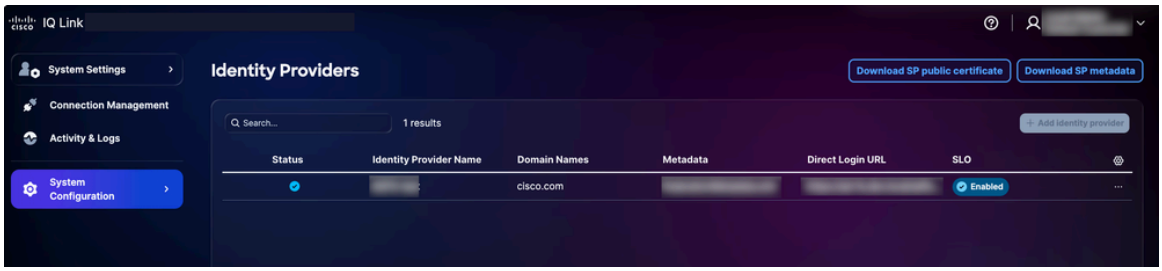
Configurazione server ADFS

Articolo	Descrizione	Esempio
FQDN Cisco IQ	Nome host distribuzione utente	devxx-23.cx-xxx-xxx.cisco.com
URL server ADFS	Indirizzo server ADFS utente	https://ad-fs.dev.local
Dominio società	Dominio e-mail	company.com
Gruppi AD	Nomi di dominio (DN) del gruppo Active Directory	CN=Ruolo - Sviluppatori CXIQ

Configurazione dei server ADFS

Per configurare ADFS:

1. Da Impostazioni di sistema, scegliere Configurazione di sistema > Provider di identità. Viene visualizzata la pagina Provider di identità.



Opzioni per il download

2. Fare clic su Scarica certificato pubblico SP e Scarica metadati SP per scaricare questi file.
3. Copiare e salvare i file service-provider-metadata.xml e service-provider-certificate.crt nella directory ADFS (ad esempio, C:-certificate.crt).
4. Accedere al server ADFS.
5. Dal menu Gestione ADFS, fare clic su Attendibilità componente.
6. Dal menu Trust relying party, fare clic su Aggiungi trust relying party. Verrà aperta la nuova procedura guidata.
7. Fare clic sul pulsante di opzione Claims Aware.
8. Fare clic su Start per procedere con la configurazione.
9. Fare clic su Importa dati sul componente da un file.
10. Fare clic su Sfoglia per selezionare il file dei metadati del provider di servizi e completare il caricamento del file.
11. Fare clic su Next (Avanti).
12. Immettere un nome visualizzato (ad esempio, "CIQ-Stage"), aggiungere eventuali note pertinenti e fare clic su Avanti.
13. Nella pagina Scegli criterio di controllo di accesso fare clic su Autorizza tutti o sul criterio richiesto dalla configurazione di protezione dell'organizzazione.
14. Fare clic su Next (Avanti) nelle altre schermate.
15. Fare clic su Chiudi per completare la configurazione dell'attendibilità del componente.

Configurazione delle regole attestazione ADFS

Per configurare le regole di attestazione ADFS, eseguire i passaggi elencati nelle sezioni seguenti.

Richieste di rimborso necessarie

Fare riferimento alla tabella seguente per le attestazioni obbligatorie.

Richieste di rimborso necessarie

Richiesta di rimborso	Scopo	Origine
Email	Identificatore utente	Posta elettronica
Nome visualizzato	Nome completo dell'utente	Nome visualizzato AD
IDNome	Oggetto SAML	Trasformato da posta elettronica
Gruppi	Accesso basato sui ruoli	Appartenenza al gruppo AD (memberOf)

Applicazione delle regole attestazione

1. Definire il nome dell'attendibilità componente (ad esempio, "Cisco IQ - Fase").

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

2. Definire le regole attestazione per inviare le informazioni sugli utenti e l'appartenenza ai gruppi a 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.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. Applicare le regole attestazione eseguendo il comando seguente:

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

Verifica dei gruppi di utenti

1. Impostare il nome utente per verificare l'appartenenza dell'utente ai gruppi.

```
$username = “testuser”
```

2. Per individuare l'account dell'utente, eseguire i comandi seguenti:

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

$user = $searcher.FindOne()
```

3. Visualizzare i gruppi a cui appartiene l'utente.

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

Output di esempio:

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

Configurare ADFS per considerare attendibile il certificato di firma SP

1. Nel server ADFS, importare il certificato SP nell'archivio Persone attendibili.

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

2. Scegliere una delle opzioni seguenti:

Nota: Il certificato SP è rilasciato da un'autorità di certificazione interna che ADFS non è in grado di convalidare tramite la catena di attendibilità standard.

- Disabilita convalida catena a livello globale per il componente

```
Set-AdfsRelyingPartyTrust `
    -TargetIdentifier “


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

O

- Importa il certificato CA emittente nell'archivio Autorità di certificazione radice attendibili

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

3. Applicare le modifiche riavviando il servizio ADFS.

```
Restart-Service adfssrv
```

Esportazione dei metadati ADFS

È possibile scaricare i metadati ADFS utilizzando PowerShell o il browser Web.

PowerShell

Per esportare i metadati ADFS utilizzando PowerShell:

1. Aprire PowerShell nel server ADFS.
2. Eseguire i comandi seguenti per scaricare il file di metadati.

```
$metadataUrl = (Get-AdfsEndpoint | Where-Object {$_.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
```

Dopo l'esecuzione dei comandi, il file di metadati viene salvato in C:-metadata.xml.

Browser Web

Per esportare i metadati ADFS utilizzando un browser Web:

1. Passare a https://<your-adfs-server>/FederationMetadata/2007-06/FederationMetadata.xml.
2. Sostituire <your-adfs-server> con il nome host del server ADFS.
3. Quando richiesto, salvare il file XML dei metadati nel computer.

Aggiunta di IDP ADFS

1. Nella pagina Provider di identità fare clic su Aggiungi provider di identità.
2. Immettere il nome del provider di identità.
3. Immettere i domini (ad esempio, company.com).
4. (Facoltativo) Attivare il pulsante Attiva interruttore di disconnessione singola, se necessario.
5. Trascinare o caricare il file di metadati SAML ottenuto dall'applicazione IDP nel campo Carica metadati IDP.
6. Fare clic su Save (Salva).

Nota: Lo stato viene visualizzato come "Incompleto" fino al completamento del mapping dei ruoli. si tratta di un comportamento normale.

Configurazione del mapping dei ruoli

Prima di procedere alla configurazione del mapping dei ruoli, verificare che sia possibile trovare i gruppi di Active Directory da utilizzare per il mapping. Per trovare i gruppi da Active Directory, eseguire il comando di PowerShell seguente.

```
$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”] }
```

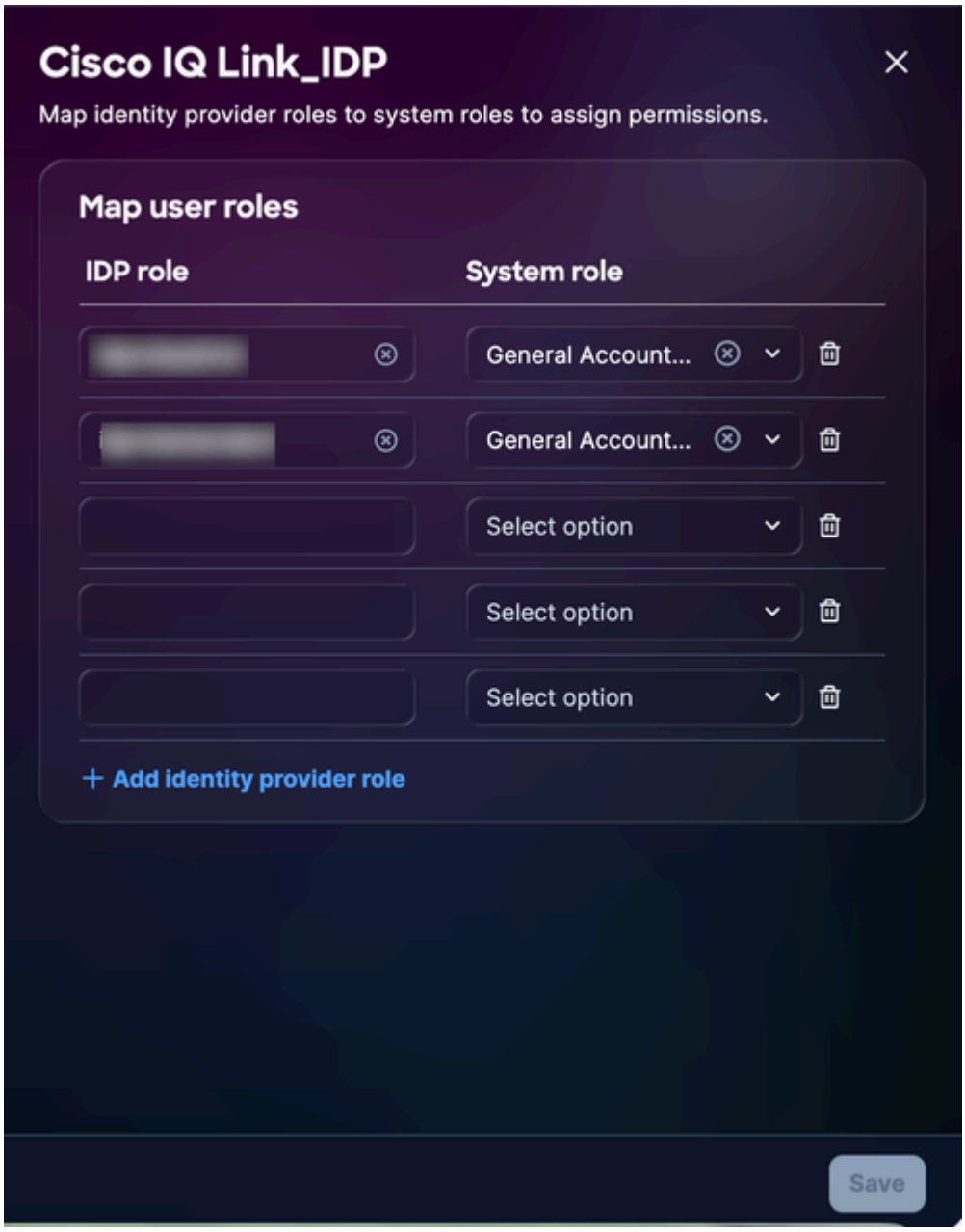
Il sistema esegue una query su Active Directory direttamente tramite LDAP, senza richiedere moduli aggiuntivi. Le informazioni sul gruppo vengono restituite in formato DN (Distinguished Name) completo, ad esempio:

CN=Ruolo - Sviluppatori CXIQ,OU=Gruppi,DC=dev,DC=esempio,DC=com CN=Ruolo - Visualizzatori CXIQ,OU=Gruppi,DC=dev,DC=esempio,DC=com

Se i gruppi richiesti non sono elencati, è necessario crearli in Active Directory da un amministratore prima di poter completare il mapping dei ruoli ADFS.

Per configurare il mapping dei ruoli:

1. Dall'IDP aggiunto, scegliere l'icona Altre opzioni > Mappa ruoli. Viene visualizzata la pagina Mapping ruoli utente.



Mapping ruoli

2. Immettere un ruolo IDP per il ruolo di sistema selezionato. Sono supportati i seguenti ruoli di sistema:

   - _amministratore account_generale: L'amministratore dell'account generale dispone di autorizzazioni complete per eseguire tutte le azioni nel prodotto. Il ruolo IDP (nome analizzato) è CXIQ Admins.
   - general_account_viewer: Il visualizzatore di account generale dispone di accesso in sola lettura. Il ruolo IDP (nome analizzato) è Sviluppatori CXIQ e Visualizzatori CXIQ.

   > Nota: Utilizzare nomi analizzati (ad esempio, sviluppatori CXIQ) e non nomi di dominio completi.

3. Fare clic su Save (Salva). Lo stato viene aggiornato a Operazione riuscita.

Verifica e collaudo

Test di autenticazione

1. In un browser in modalità Incognito o Private, passare a https://your-cisco-iq-domain.com/login.
2. Eseguire l'accesso utilizzando le credenziali di Active Directory nel formato dominio omeutente o user@domain.local.
3. Verificare di essere reindirizzati alla home page di Cisco IQ (dopo l'autenticazione).
4. Confermare che i ruoli assegnati visualizzino i nomi dei gruppi analizzati corretti (ad esempio, CXIQ Developers) nel proprio profilo utente.

Test della disconnessione

Per verificare la disconnessione, fare clic su Disconnetti da Cisco IQ. Viene visualizzato il messaggio "Logging out, please wait..." (Disconnessione in corso, attendere...) e l'utente viene reindirizzato alla pagina di accesso a Cisco IQ. Il sistema termina anche la sessione ADFS. Se si tenta di accedere direttamente ad ADFS, verrà richiesto di eseguire nuovamente l'accesso.

Risoluzione dei problemi relativi ad ADFS

L'elenco seguente descrive i problemi comuni e le possibili soluzioni per identificare e risolvere rapidamente i problemi relativi allo stato di ADFS, agli errori dei certificati, agli errori di accesso SSO e alla configurazione degli SLO.

Problemi ADFS

Problema	Sintomi / Descrizione	Cause / Controlli / Soluzioni alternative e correzioni
Gruppi non estratti	Nessun ruolo dopo l'accesso	• Regola attestazione mancante: Eseguire nuovamente le istruzioni in Configurazione delle regole attestazione ADFS

Problema	Sintomi / Descrizione	Cause / Controlli / Soluzioni alternative e correzioni
		• Attributo gruppo errato: Deve essere http://schemas.xmlsoap.org/claims/Group • L'utente non è incluso nei gruppi AD
Decrittografia non riuscita	"Impossibile decrittografare l'asserzione" nei log	Controllare la configurazione del certificato ADFS
Loop di accesso	Bloccato nell'autenticazione o nel loop di accesso	• URL ACS non valido: Verifica: https://your-fqdn/saml/acs • Mancata corrispondenza del cookie: Verificare i cookie del browser per il dominio corretto

Comandi di diagnostica per la risoluzione dei problemi

Per garantire una corretta integrazione tra l'ambiente ADFS e Cisco IQ, utilizzare i seguenti comandi diagnostici. Questi comandi consentono di verificare l'accessibilità dei metadati, le configurazioni dei certificati e le impostazioni degli endpoint.

- Verificare l'accessibilità dei metadati ADFS: conferma che i metadati federativi ADFS sono raggiungibili e accessibili al pubblico; si tratta di un passo fondamentale per stabilire la fiducia iniziale

```
curl -k https://

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

- Convalida il certificato di crittografia: Assicura che il certificato di crittografia corretto sia associato all'attendibilità del componente Cisco IQ

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

- Verifica configurazione endpoint SAML: Verifica che gli endpoint SAML per il trust Cisco IQ siano configurati correttamente e che le richieste e le asserzioni di autenticazione vengano instradate agli URL previsti

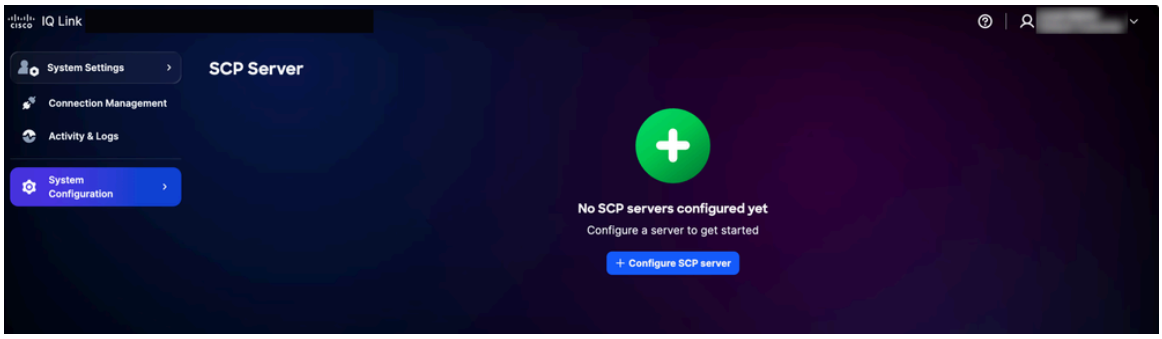
```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object SamlEndpoints
```

Aggiunta di server SCP

Questo server SCP (Secure Copy Protocol) è un prerequisito per l'importazione dei file di aggiornamento essenziali per l'aggiunta, l'aggiornamento o la correzione dell'installazione di Cisco IQ.

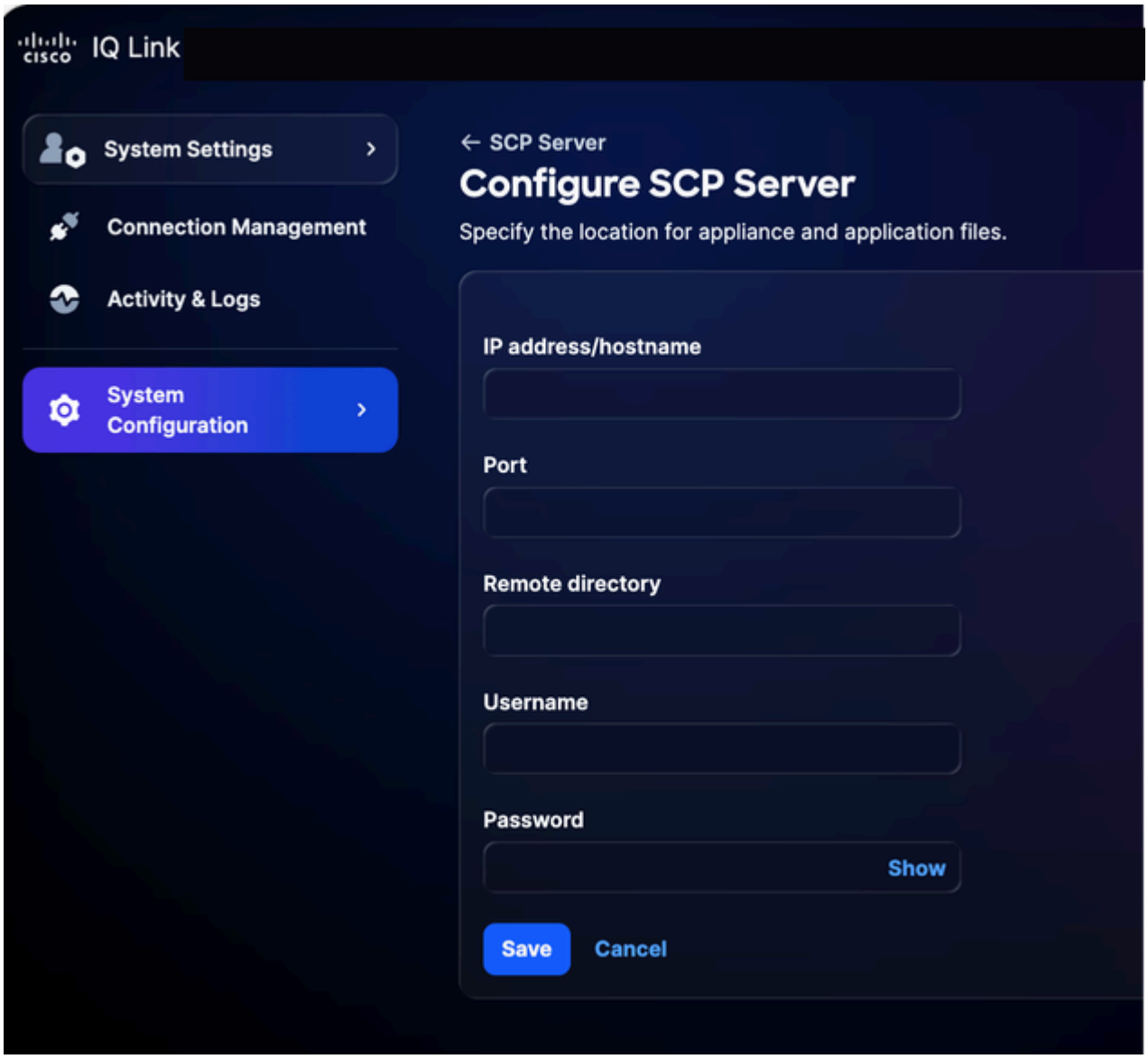
Per aggiungere un server SCP:

1. Da Impostazioni di sistema, scegliere Configurazione di sistema > Server SCP. Viene visualizzata la pagina SCP Server.



Home page del server SCP

2. Fare clic su Configure SCP Server (Configura server SCP).



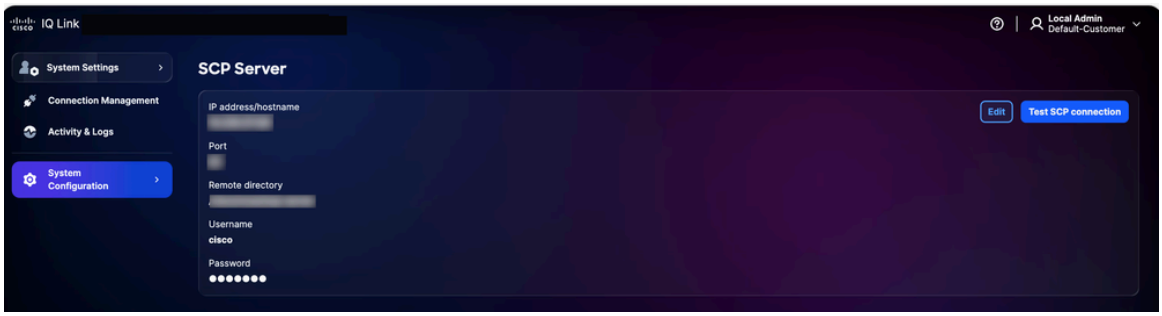
Configura server SCP

3. Immettere l'indirizzo IP o il nome host.
4. Immettere un numero di porta.
5. Immettere la directory remota.
6. Immettere un nome utente.
7. Immettere una password.
8. Fare clic su Save (Salva). Viene visualizzata una conferma.

Modifica di server SCP esistenti

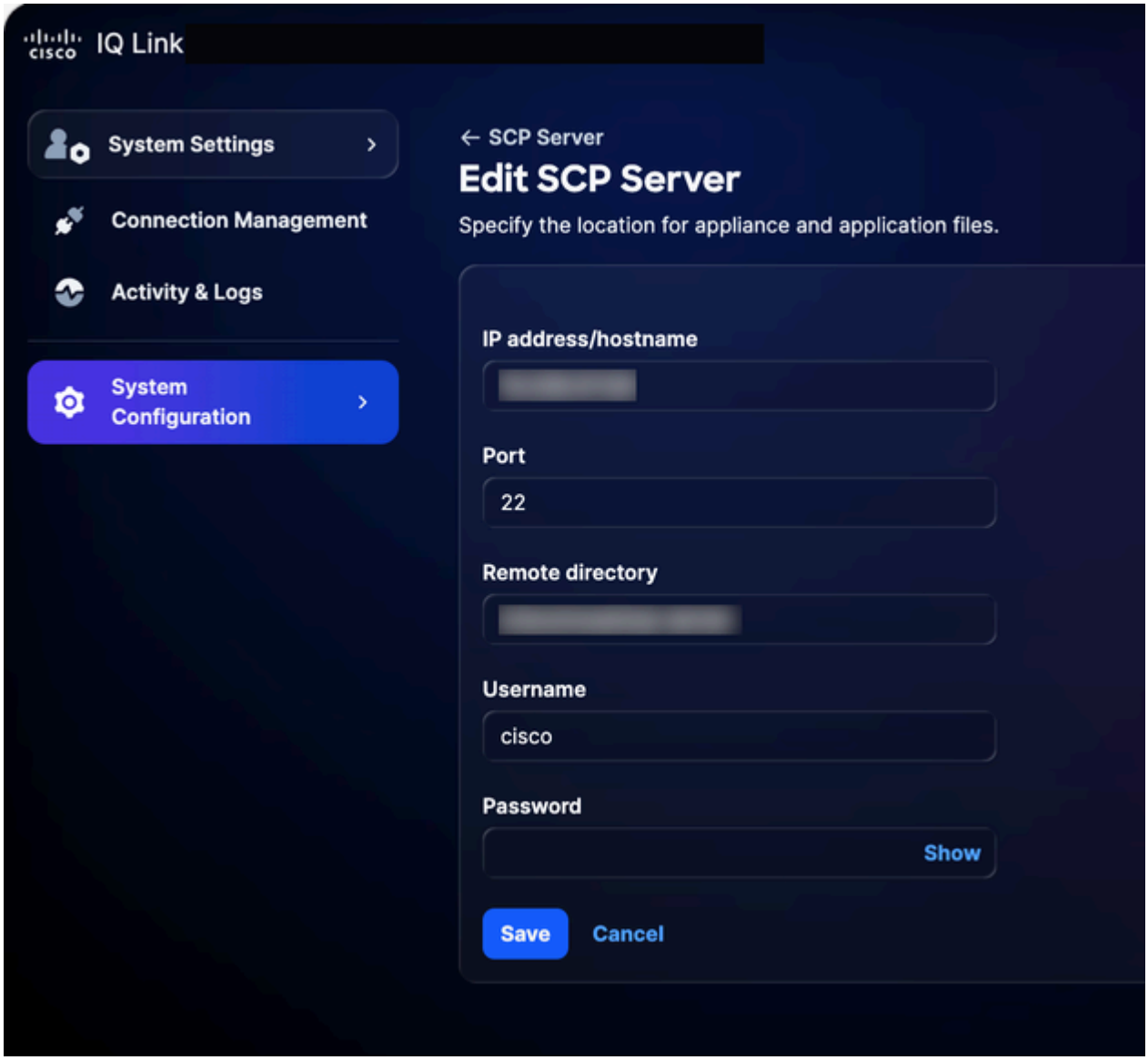
Per modificare un server SCP esistente:

1. Passare alla pagina SCP Server.



Server SCP

2. Fare clic su Edit (Modifica) per specificare il server SCP desiderato esistente.



Modifica del server SCP

3. Modificare i dettagli in base alle esigenze.

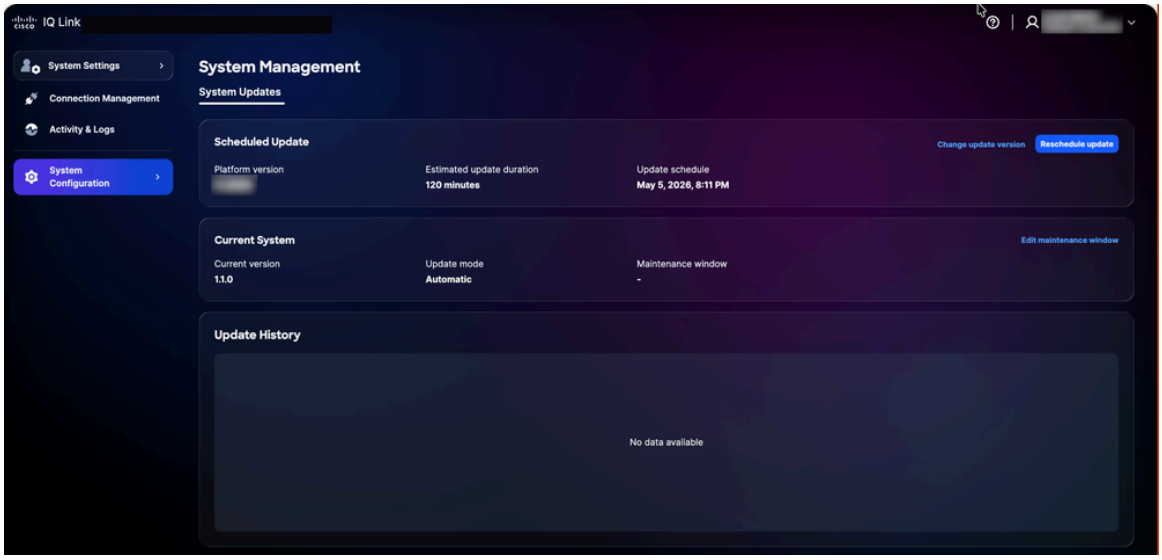
4. Fare clic su Save (Salva).

Gestione del sistema

I clienti possono eseguire l'aggiornamento all'ultima versione di Cisco IQ Link tramite l'interfaccia utente. È possibile effettuare la verifica anche dalla pagina Cisco IQ Data Connector.

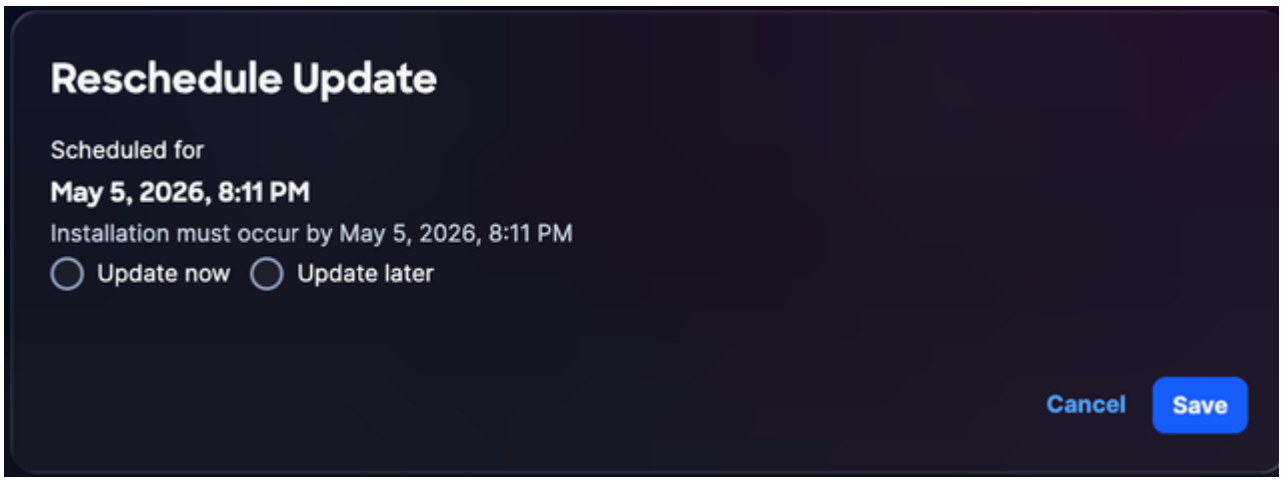
Per riprogrammare l'aggiornamento del sistema:

1. Da Amministrazione, scegliere Configurazione sistema > Gestione sistema. Viene visualizzata la pagina Gestione sistema. In questa pagina viene visualizzata la versione del sistema attualmente in esecuzione; se non sono stati configurati aggiornamenti, la sezione Cronologia aggiornamenti è vuota.



Aggiornamento del sistema

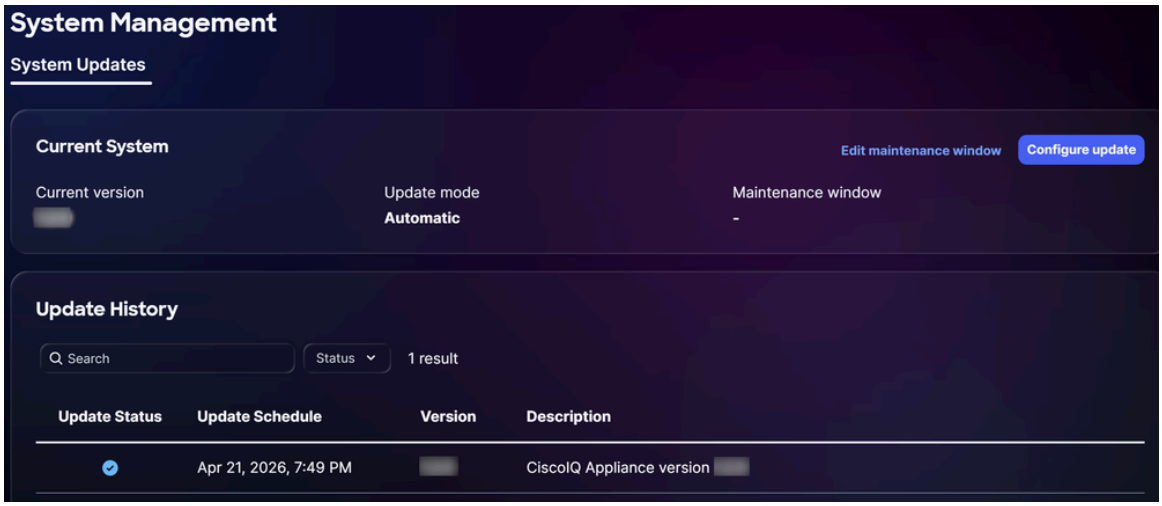
2. Fare clic su Riprogramma aggiornamento.



Ripianifica aggiornamento

3. Fare clic su Aggiorna ora per eseguire immediatamente la riprogrammazione oppure su Aggiorna in seguito per programmare un'altra operazione.

4. Fare clic su Save (Salva). Viene visualizzata una conferma e l'utente viene reindirizzato alla home page di System Update.



Aggiornamento completato

Configurazione certificati SSL

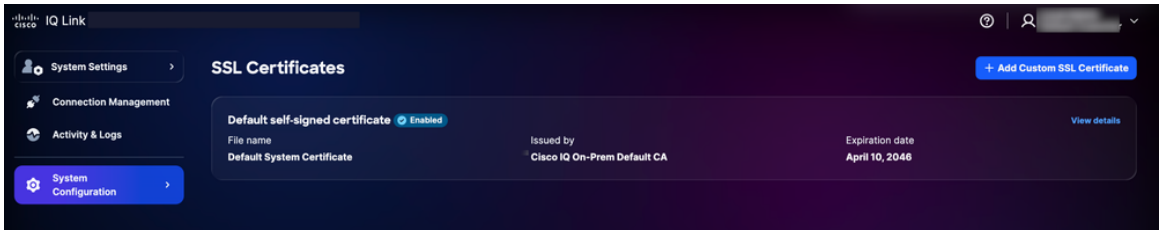
In Cisco IQ è preinstallato e abilitato un certificato autofirmato predefinito, ma gli utenti possono caricare certificati SSL personalizzati. Quando un certificato SSL personalizzato è abilitato, viene utilizzato per le connessioni HTTPS; se il certificato viene disabilitato o eliminato, il sistema ripristina automaticamente il certificato predefinito.

Nota: Il certificato deve avere almeno 90 giorni di validità rimanenti. Un certificato è considerato "prossimo alla scadenza" quando mancano meno di 90 giorni alla scadenza. Dopo aver aggiunto, modificato o eliminato un certificato SSL, il cliente deve caricare il nuovo SSL come indicato nella sezione Completamento della configurazione SLO per l'IDP Okta o l'IDP ADFS.

Aggiunta del certificato SSL personalizzato

Per aggiungere un certificato SSL personalizzato:

1. Da Impostazioni di sistema, scegliere Configurazione di sistema > Certificati SSL. Viene visualizzata la pagina Certificati SSL, in cui sono elencati tutti i certificati SSL per il sistema in uso.

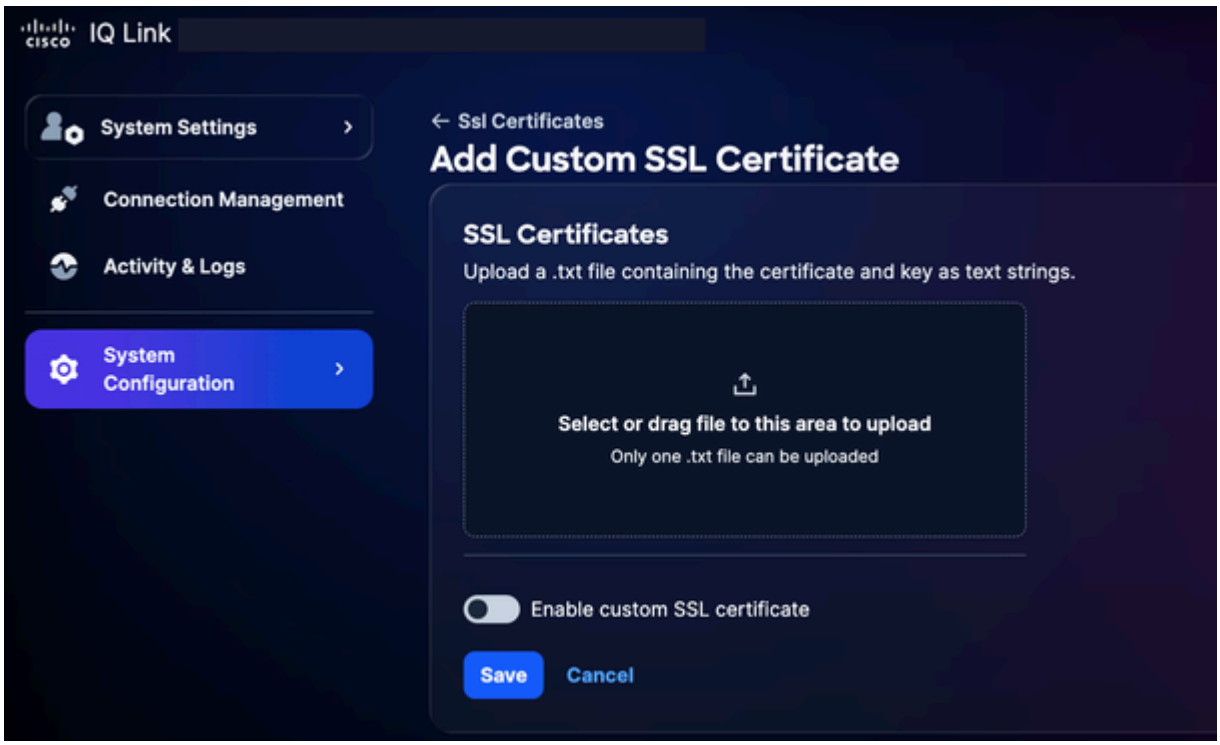


Aggiunta del certificato SSL

2. Fare clic su Aggiungi certificato SSL personalizzato.

Note:
· Caricare un file .txt che includa sia il certificato e la chiave codificati tramite posta con Privacy Enhanced come stringhe di testo
· È possibile caricare un solo file .txt alla volta
· Il file deve contenere sia il certificato che la chiave privata

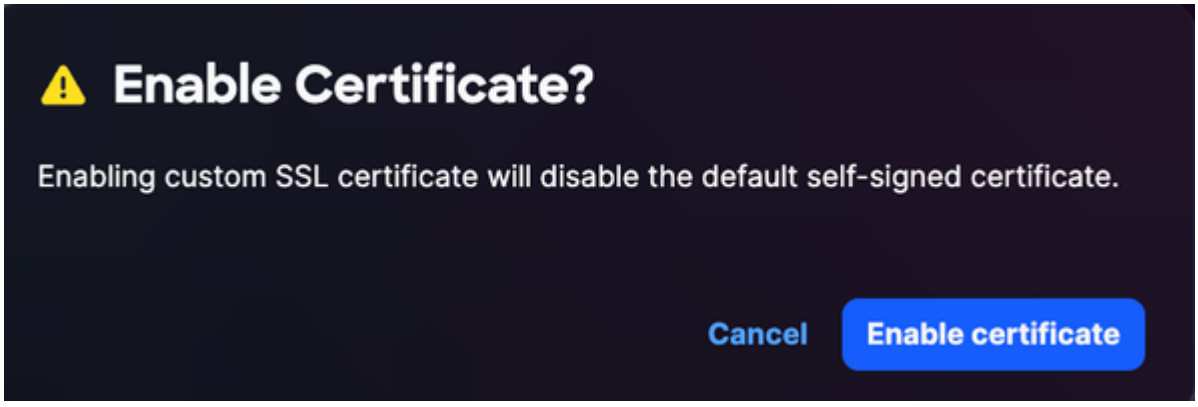
---



Carica certificati SSL

3. Trascinare o caricare il certificato SSL personalizzato nel campo Certificato SSL.

4. Attivare il pulsante Abilita certificato SSL personalizzato.



Abilita certificato

Nota: Tenere l'interruttore OFF se si desidera caricare il certificato senza attivarlo immediatamente.

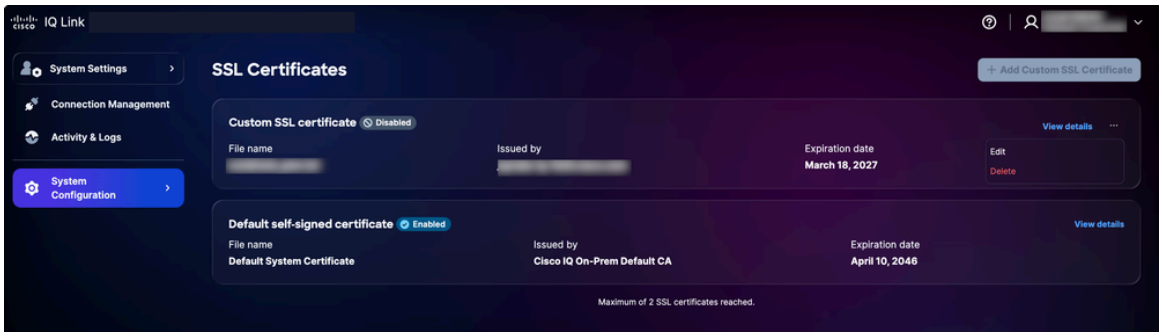
5. Fare clic su Abilita certificato.
6. Fare clic su Save (Salva).

Il certificato SSL personalizzato è abilitato e attivo. Il certificato di sistema predefinito viene disattivato automaticamente.

Modifica di certificati SSL personalizzati

È possibile modificare il certificato SSL personalizzato per caricare un nuovo certificato o per disabilitare il certificato attualmente abilitato. Per modificare:

1. Passare al certificato SSL personalizzato desiderato.



Modifica certificato SSL

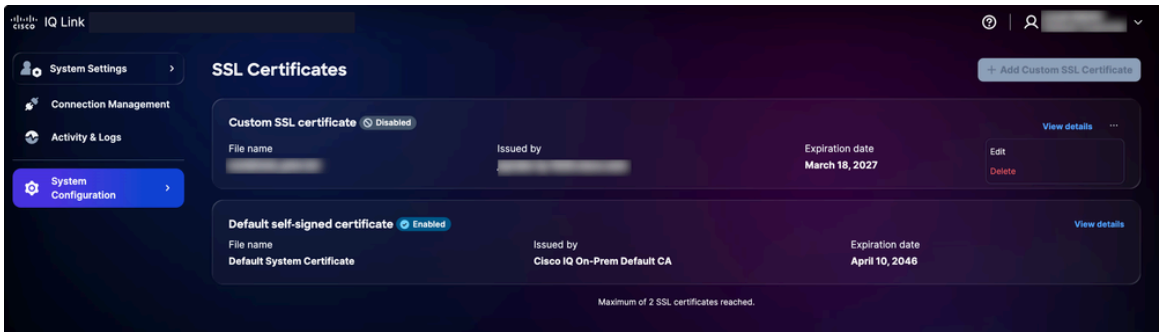
2. Scegliere l'icona Altre opzioni > Modifica. Verrà visualizzata la pagina Modifica certificato SSL.
3. Modificare i dettagli del certificato come richiesto.
4. Fare clic su Save (Salva).

Eliminazione dei certificati SSL personalizzati

Avviso: Un certificato SSL personalizzato può essere eliminato in qualsiasi momento, ma si tratta di un'azione irreversibile. è possibile caricare un nuovo certificato personalizzato in qualsiasi momento dopo l'eliminazione.

Per eliminare:

1. Passare al certificato SSL personale desiderato.



Elimina certificato SSL

2. Scegliere l'icona Altre opzioni > Elimina.
3. Fare clic su Elimina certificato. Il certificato personalizzato viene eliminato e il certificato predefinito viene riattivato automaticamente.

Configurazione server Syslog

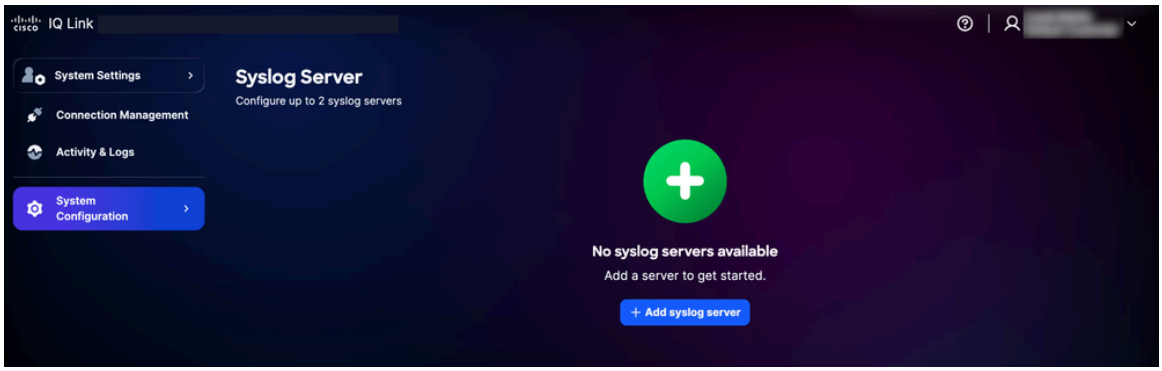
Gli utenti con il ruolo Amministratore possono configurare i server syslog esterni per l'esportazione dei registri di sistema. È possibile configurare fino a due (2) server syslog.

Nota: È necessario specificare il server Syslog come indirizzo IP e non come nome di dominio completo (FQDN).

Aggiunta di server syslog

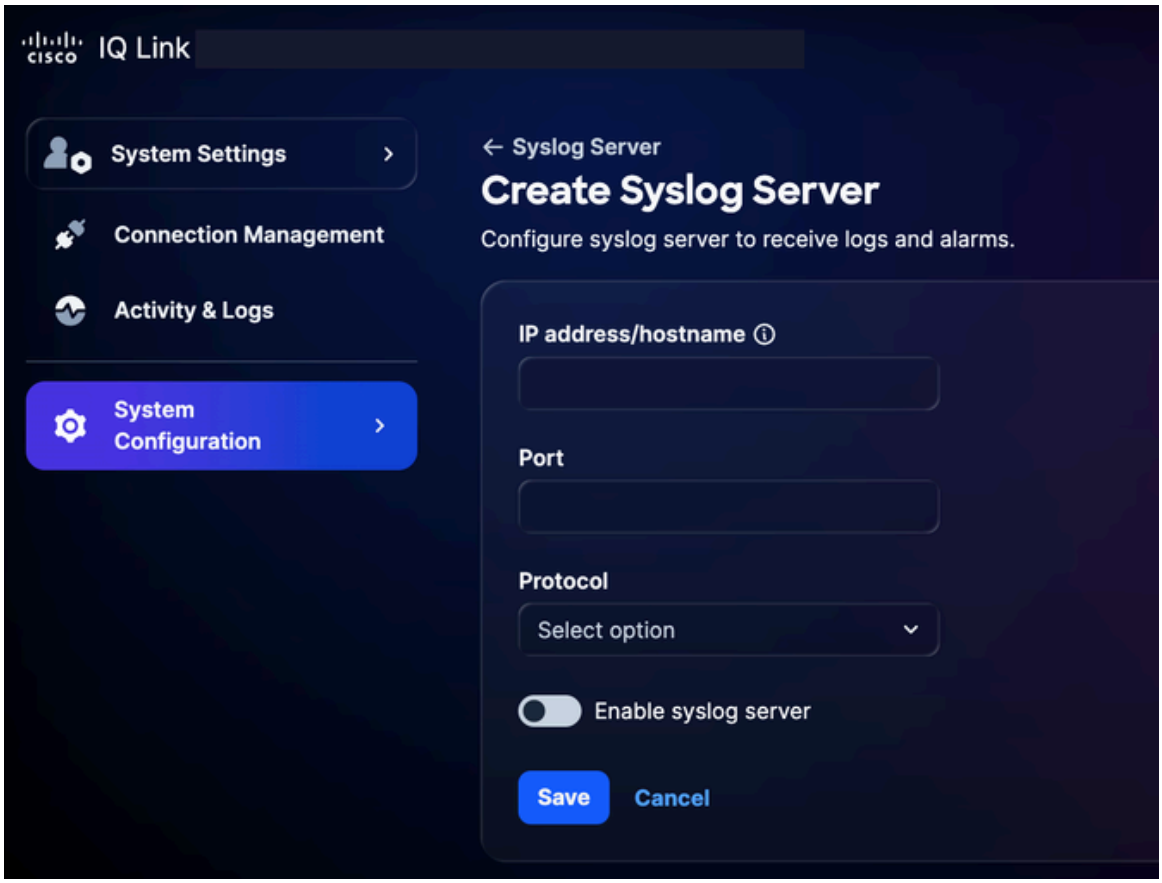
Per aggiungere un server syslog:

1. Da Impostazioni di sistema, scegliere Configurazione di sistema > Syslog Server. Viene visualizzata la pagina Syslog Server.



Aggiungi server syslog

2. Fare clic su Add syslog server (Aggiungi server syslog). Viene visualizzata la pagina Crea Syslog Server.



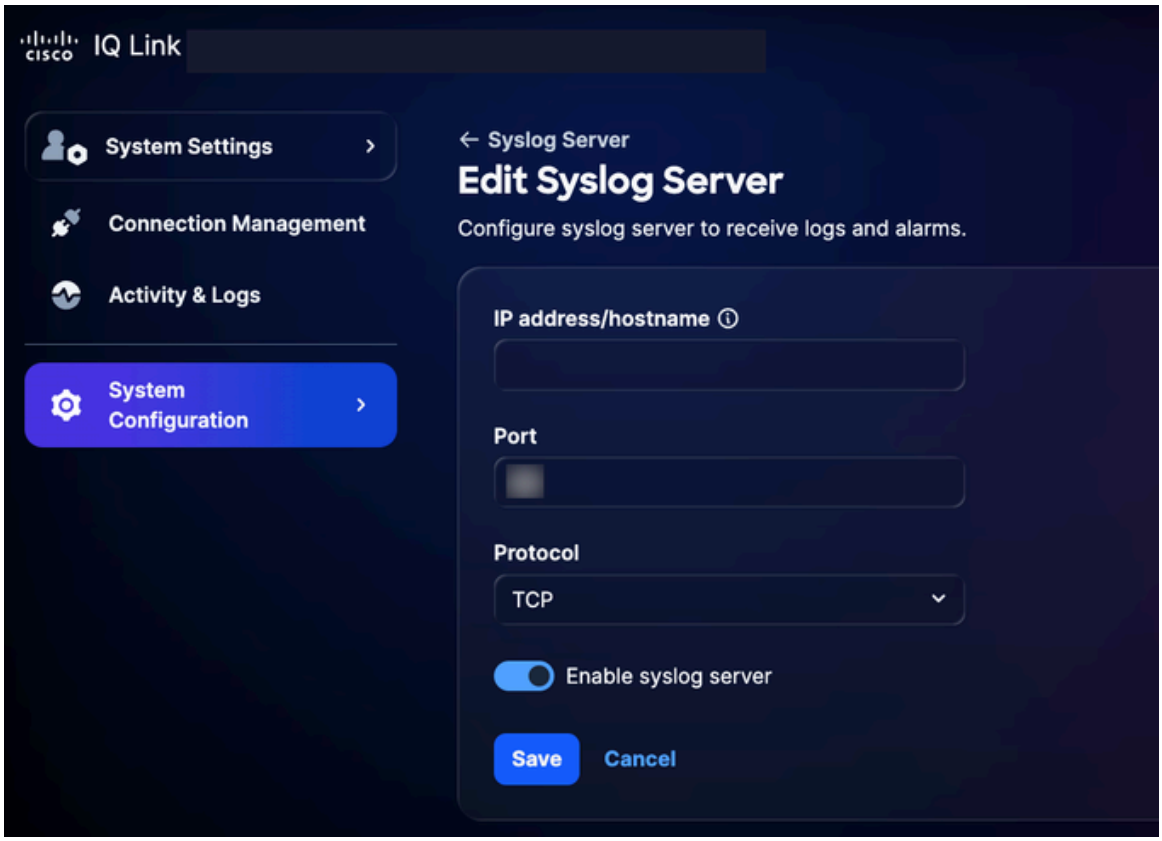
Crea server syslog

3. Immettere l'indirizzo IP o il nome host.
4. Immettere un numero di porta.
5. Selezionare il protocollo desiderato dall'elenco a discesa Protocollo (ad esempio, UDP o TCP).
6. Attivare il pulsante Abilita server syslog.
7. Fare clic su Save (Salva). Viene visualizzata una conferma e il server syslog appena aggiunto viene visualizzato nella home page del server syslog.

Modifica dei server syslog configurati

Per modificare un server syslog configurato:

1. Passare al server syslog desiderato.
2. Scegliere l'icona Altre opzioni > Modifica. Viene visualizzata la pagina Modifica Syslog Server.



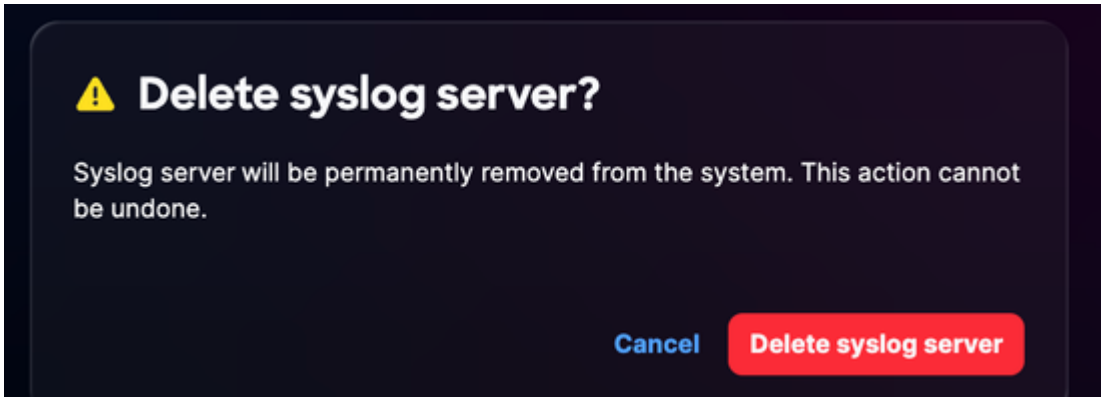
Modifica server syslog

3. Modificare i dettagli o disattivare l'opzione Abilita server syslog, come richiesto.
4. Fare clic su Save (Salva).

Eliminazione dei server syslog configurati

Per eliminare un server syslog configurato:

1. Passare al server syslog desiderato.
2. Scegliere l'icona Altre opzioni > Elimina. Viene visualizzata una conferma.

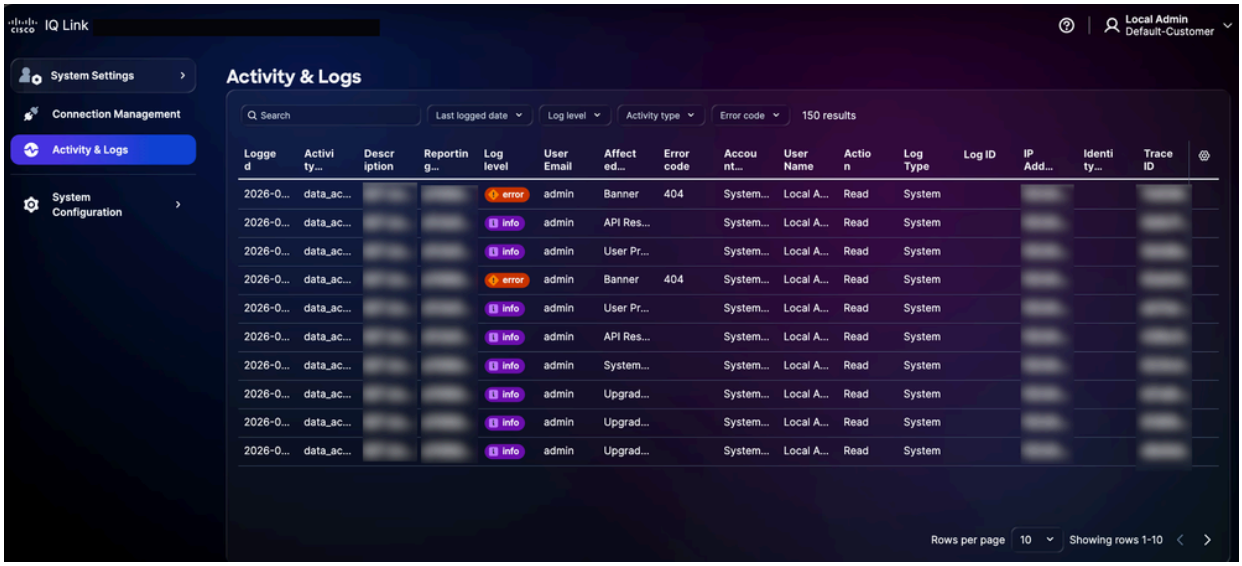


Conferma

3. Fare clic su Delete syslog server (Elimina server syslog).

Registri attività

I registri attività forniscono una registrazione dettagliata delle azioni e delle modifiche degli utenti in Cisco IQ, consentendo agli amministratori di tenere traccia delle attività degli utenti e mantenere la trasparenza.



Registri attività

Per visualizzare attività e registri, selezionare Attività e registri dal menu Impostazioni di sistema.

Log attività:

- Supportare filtri, impaginazione e funzionalità di ricerca per trovare e gestire facilmente le informazioni
- Registra tutte le operazioni API a livello di gateway

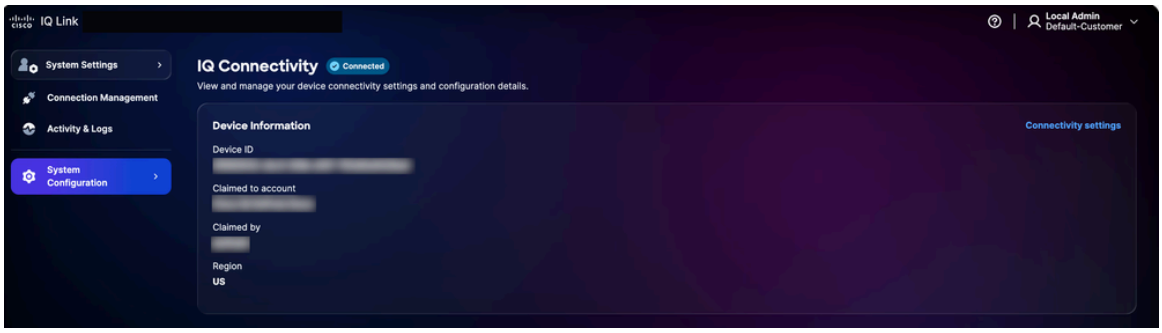
Sono disponibili le seguenti opzioni di filtro:

- Data: Filtra i registri in base a un intervallo di tempo specifico
- Livello log: Filtra i registri in base alla gravità (ad esempio, errore, avviso e informazioni)
- Tipo di attività: Filtra i registri in base al tipo di attività del sistema
- Codice errore: Filtra i registri per un codice di errore specifico

Connettività IQ

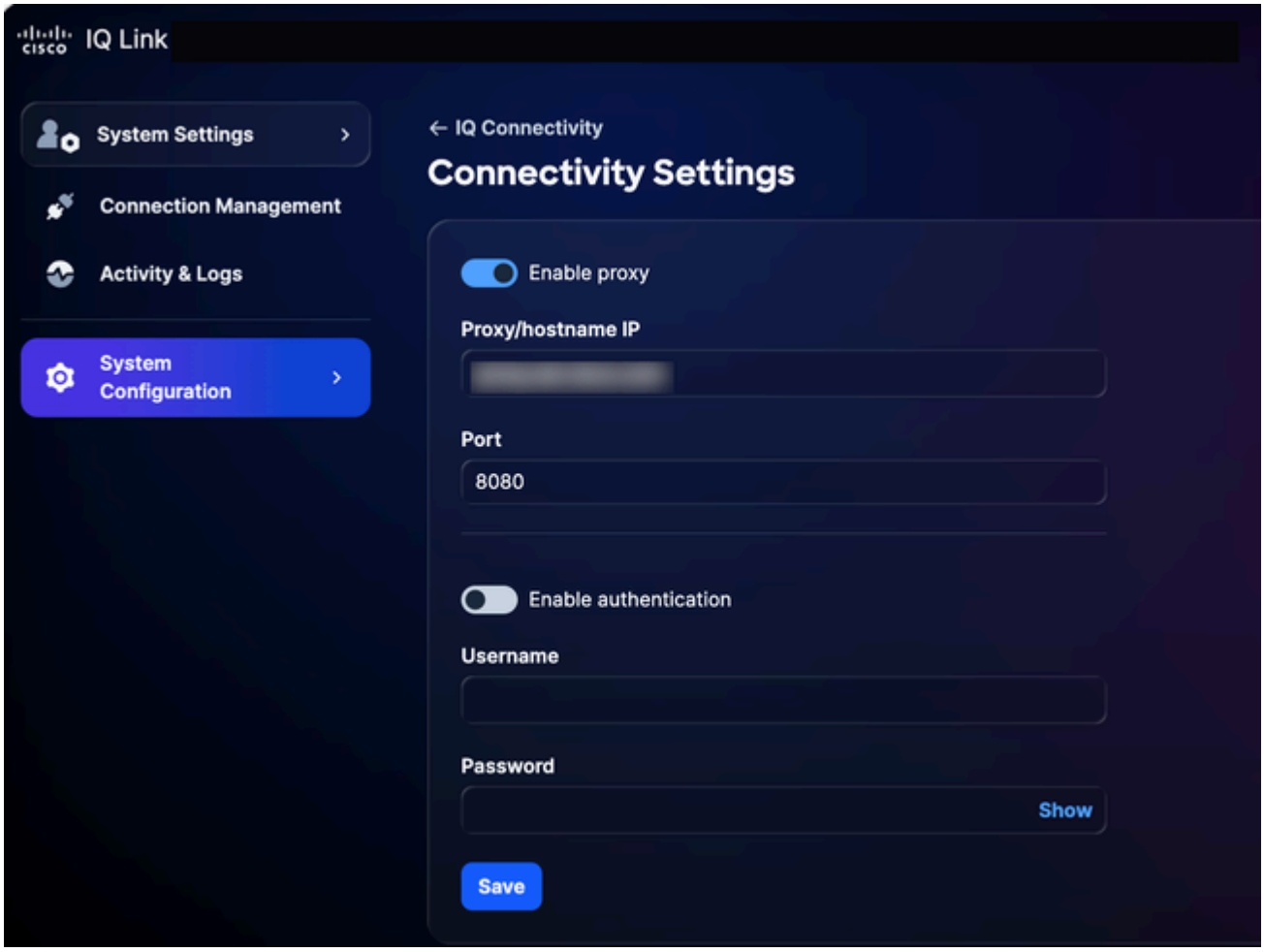
Per visualizzare e gestire le impostazioni di connettività del dispositivo e i dettagli di configurazione:

1. Da Impostazioni di sistema, scegliere Configurazione di sistema > Connettività IQ. Viene visualizzata la pagina Connettività IQ.



Connettività IQ

2. Fare clic su Impostazioni connettività.



Impostazioni connettività

3. Aggiornare i dettagli in base alle esigenze.

4. Fare clic su Save (Salva).

Gestione connessione (raccolta dati)

Cisco IQ Link è una soluzione implementata in loco per la raccolta dei dati di rete, progettata per fornire una visibilità completa dell'infrastruttura. Raccoglie i dati tramite Catalyst Center e Direct Connection. Semplifica la gestione dell'autenticazione di rete e dell'individuazione dei dispositivi. La configurazione della raccolta dati può essere riepilogata come segue:

- Creazione di set di credenziali: Stabilire i protocolli di autenticazione (ad esempio, SNMP v1/v2c/v3) per comunicare con i dispositivi di rete. La centralizzazione delle credenziali in base all'area di protezione o alla posizione (ad esempio, "SanJose-SNMPv3") consente di aggiornare le password in un'unica posizione, con la propagazione automatica delle modifiche a tutti i dispositivi associati.

Nota: Per autenticare gli asset connessi direttamente, Cisco IQ Link richiede un account utente configurato con il livello di privilegio 15 sul dispositivo.

- Mapping delle credenziali sul magazzino: Mappare le serie di credenziali con le risorse di inventario per automatizzare il processo di autenticazione. Creando regole che collegano intervalli IP specifici a set di credenziali definiti, il sistema applica automaticamente l'autenticazione corretta durante la raccolta dei dati. In questo modo si eliminano gli errori di immissione manuali e si garantisce la precisione della configurazione in base alla crescita della rete.

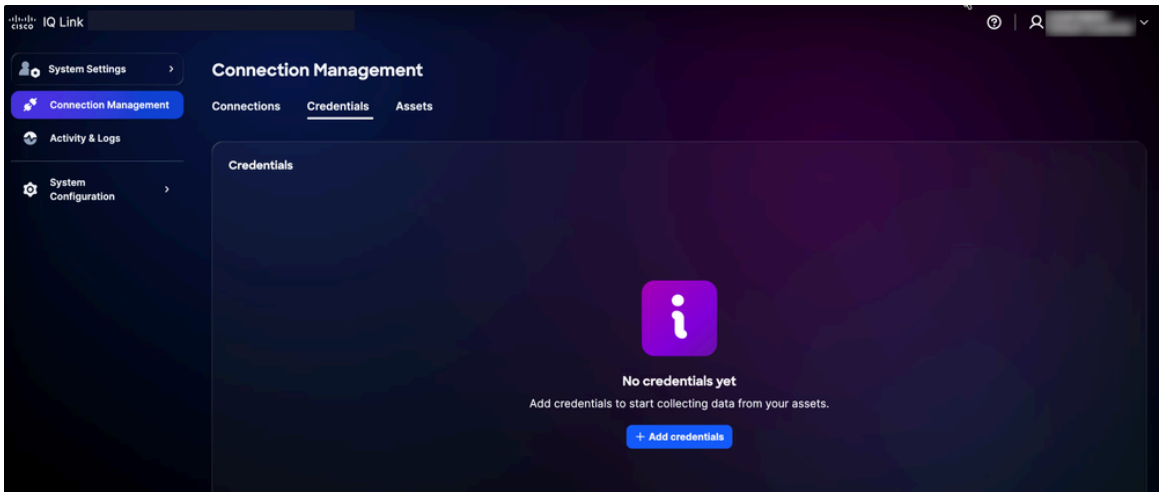
Nota: Per l'individuazione dei dispositivi sono richiesti SNMPv2c/SNMPv3 e SSH e prima di configurare Catalyst Center è necessario fornire le credenziali HTTP/HTTPS.

Aggiunta di credenziali

Per eseguire la raccolta dei dati, è innanzitutto necessario aggiungere le credenziali. Per aggiungere le credenziali:

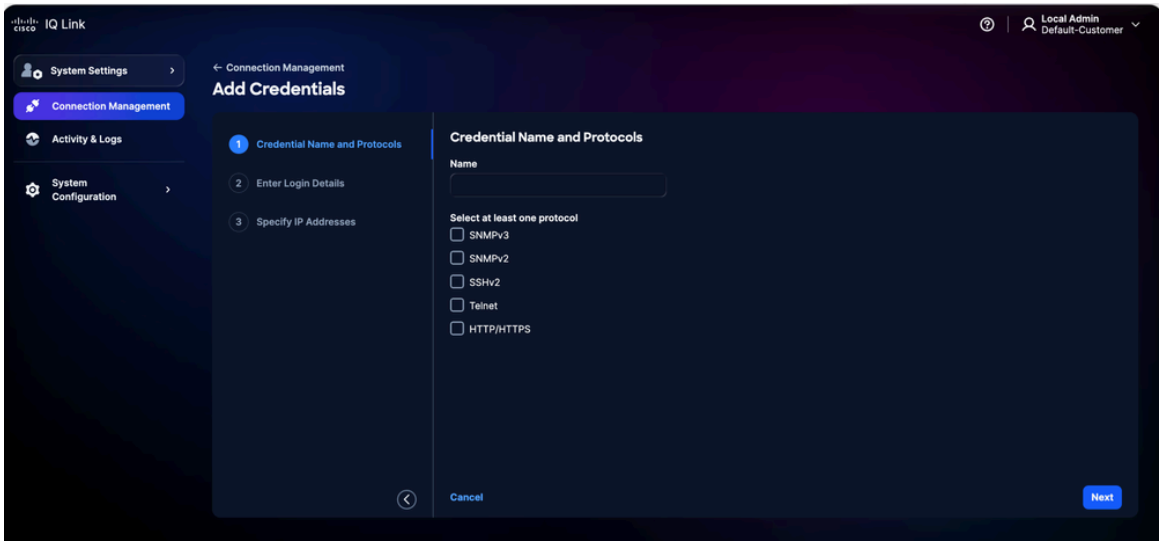
1. Da Impostazioni di sistema, scegliere Gestione connessione. Viene visualizzata la pagina Gestione connessione.

2. Fare clic sulla scheda Credenziali.



Scheda Credenziali

3. Fare clic su Aggiungi credenziali.

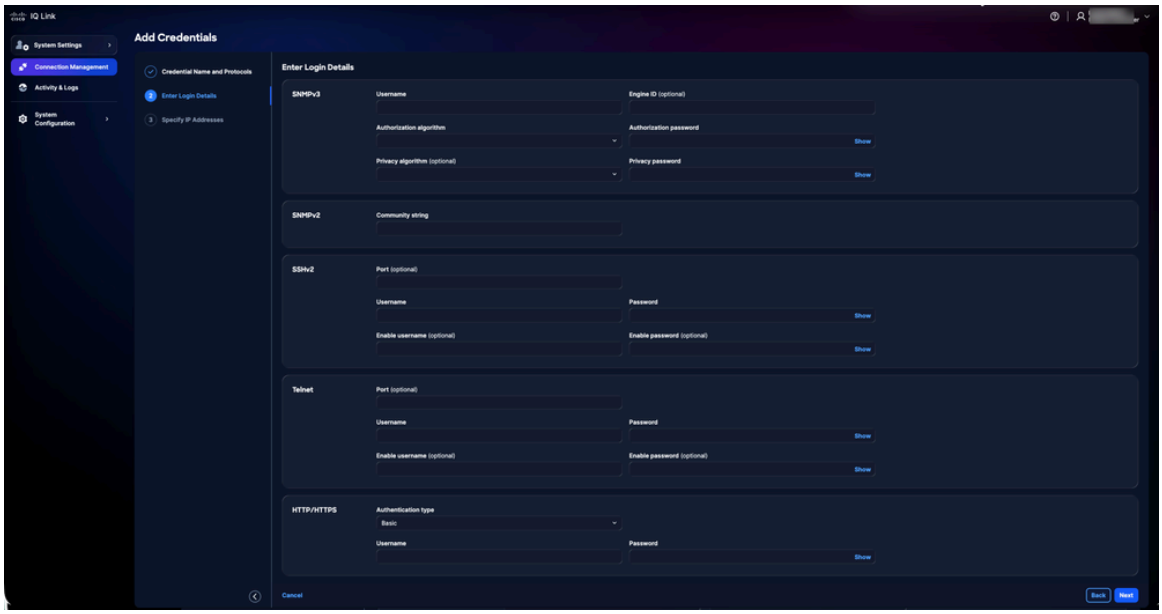


Aggiungi credenziali

4. Immettere il nome.

5. Selezionare tutte le caselle di controllo dei protocolli applicabili.

6. Fare clic su Next (Avanti).

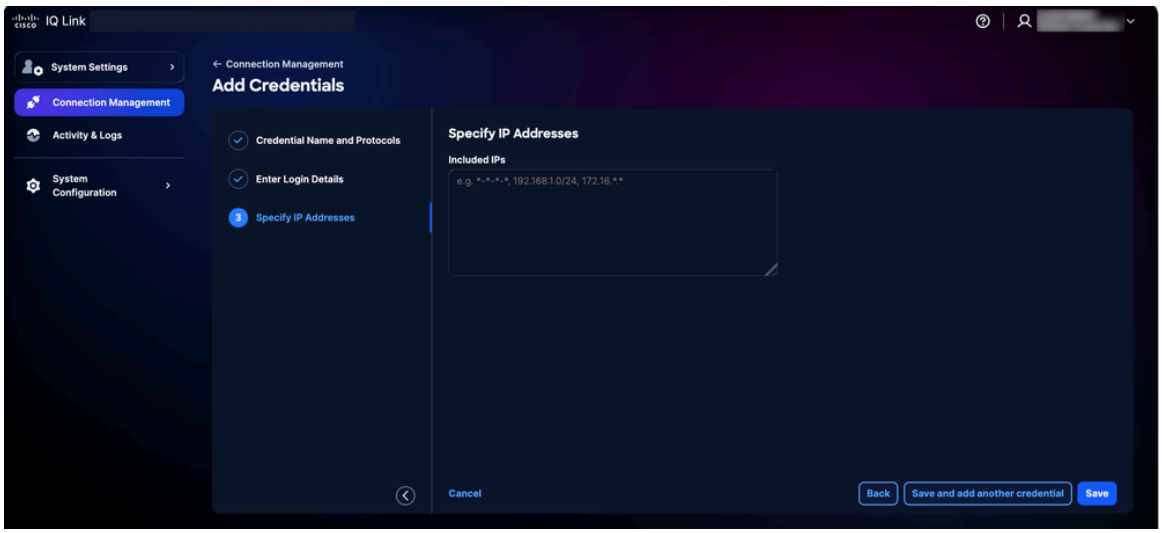


Aggiungi dettagli credenziali

Nota: Nell'immagine precedente è illustrata la visualizzazione quando nel passaggio precedente sono stati selezionati tutti i protocolli. Sull'interfaccia verranno visualizzati solo i protocolli specifici scelti.

7. Immettere i dettagli di accesso per ogni protocollo selezionato.

8. Fare clic su Next (Avanti).

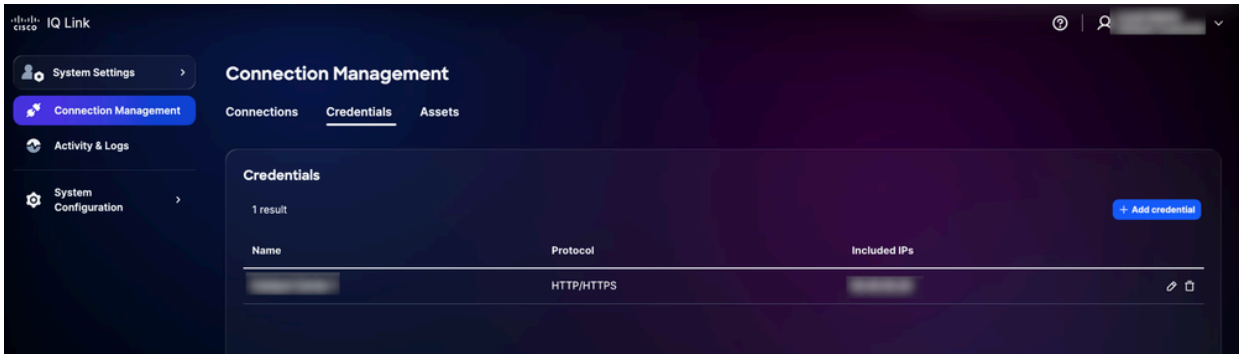


Specifica indirizzi IP

9. Immettere gli IP inclusi.

Nota: Questo campo definisce gli indirizzi IP o gli intervalli IP in cui è possibile utilizzare le credenziali per stabilire una connessione. Supporta una combinazione di IP e maschere IP (utilizzando la notazione con caratteri jolly). Per informazioni dettagliate sui formati supportati, vedere Selezione delle credenziali e logica di corrispondenza.

10. Fare clic su Save (Salva). Viene visualizzata una conferma e l'utente viene reindirizzato alla scheda Credenziali.



Credenziali aggiunte

È possibile modificare le credenziali facendo clic sull'icona Modifica ed eliminarle facendo clic sull'icona Elimina.

Selezione credenziali e logica di corrispondenza

Il motore di telemetria utilizza una logica di corrispondenza basata sulla priorità per determinare le credenziali da applicare durante l'individuazione e la raccolta. La comprensione di questa gerarchia garantisce l'utilizzo delle credenziali corrette per i dispositivi desiderati.

- Livello di priorità: Quando a un dispositivo vengono applicati più set di credenziali, Cisco IQ li valuta in base alla corrispondenza specifica con il dispositivo; il sistema applica la seguente priorità, con le corrispondenze più specifiche che hanno la precedenza:
    - Corrispondenza esatta IP: Priorità massima
    - Corrispondenza con caratteri jolly:** **La priorità dipende dal numero di stelle finali; meno stelle indicano una corrispondenza più specifica e quindi una priorità più alta
- Regole di formattazione con caratteri jolly: I caratteri jolly (*) sono supportati solo come caratteri finali negli indirizzi IP. devono essere applicati da destra a sinistra.
    - Formati supportati:

      1.2.3.* (Priorità massima tra i caratteri jolly)

      1.2.*

      1.*.*.*

      ..*.* (Priorità minima)
    - Formati non supportati:

Caratteri jolly iniziali (ad esempio, *.1.2.3)

Caratteri jolly tra ottetti (ad esempio, 10.10.*.20)

Utilizzo di trattini o altri delimitatori non standard

Esempio di selezione delle credenziali:

Nella tabella seguente viene illustrato come il motore di telemetria seleziona il set di credenziali più appropriato quando un dispositivo corrisponde a più modelli definiti.

Esempio di selezione delle credenziali

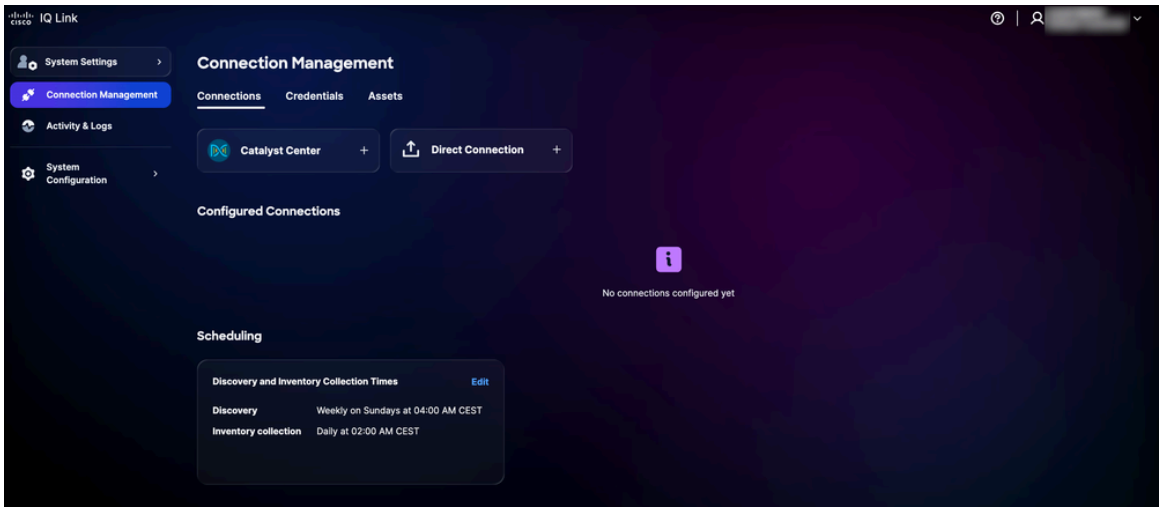
IP dispositivo	Set di credenziali disponibili	Set di credenziali selezionato
10.10.1.5	10.10.1.5, 10.10.1., 10.10.*	10.10.1.5 (Corrispondenza Esatta)
10.10.2.15	10.10.2, 10.10.*	10.10.2.* (Più specifico)
10.10.5.50	10.10...	10.10. (Più specifico)

Nota: Se un dispositivo rientra in più categorie sovrapposte, il sistema seleziona sempre il set di credenziali con la più alta specificità (in altre parole, il minor numero di caratteri jolly finali).

Raccolta dei dati tramite Catalyst Center

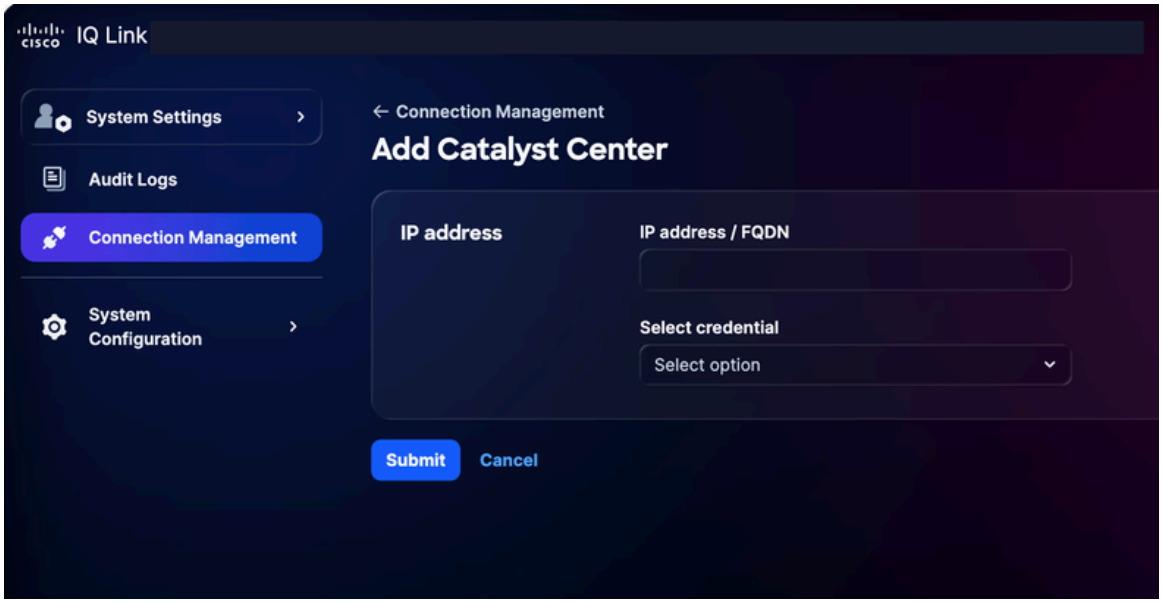
Per la raccolta dei dati con Catalyst Center:

1. Da Impostazioni di sistema, scegliere Gestione connessione. Viene visualizzata la pagina Gestione connessione.



Gestione connessione

2. Fare clic sull'opzione Catalyst Center.

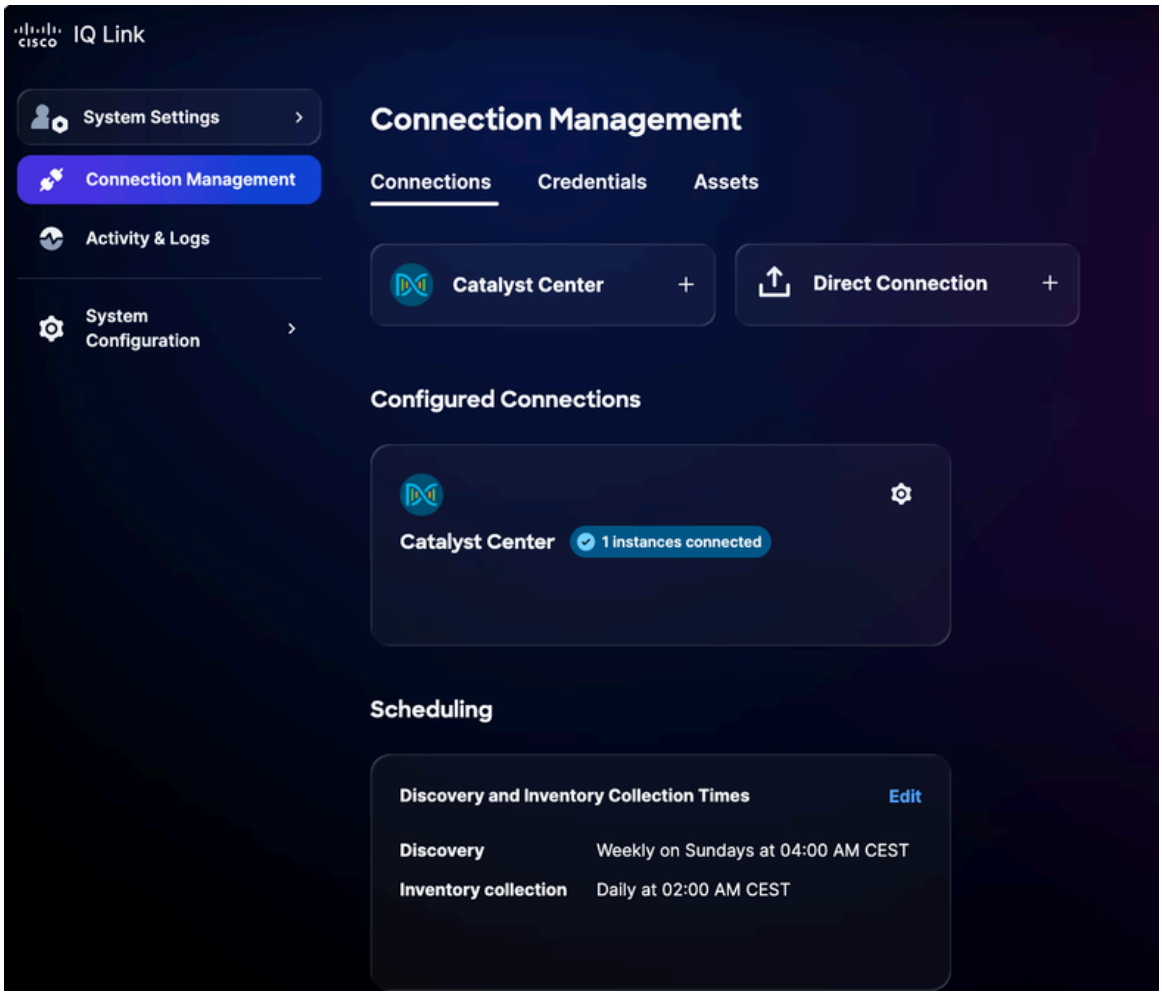


Aggiungi Catalyst Center

3. Immettere l'indirizzo IP o il FQDN.

4. Scegliere una credenziale HTTP/HTTPS configurata dall'elenco a discesa.

5. Fare clic su Invia. Viene visualizzata una schermata di conferma (l'operazione può richiedere fino a 75 minuti). È possibile visualizzare il Catalyst Center appena aggiunto in Connessioni configurate.



Aggiunta di Catalyst Center completata

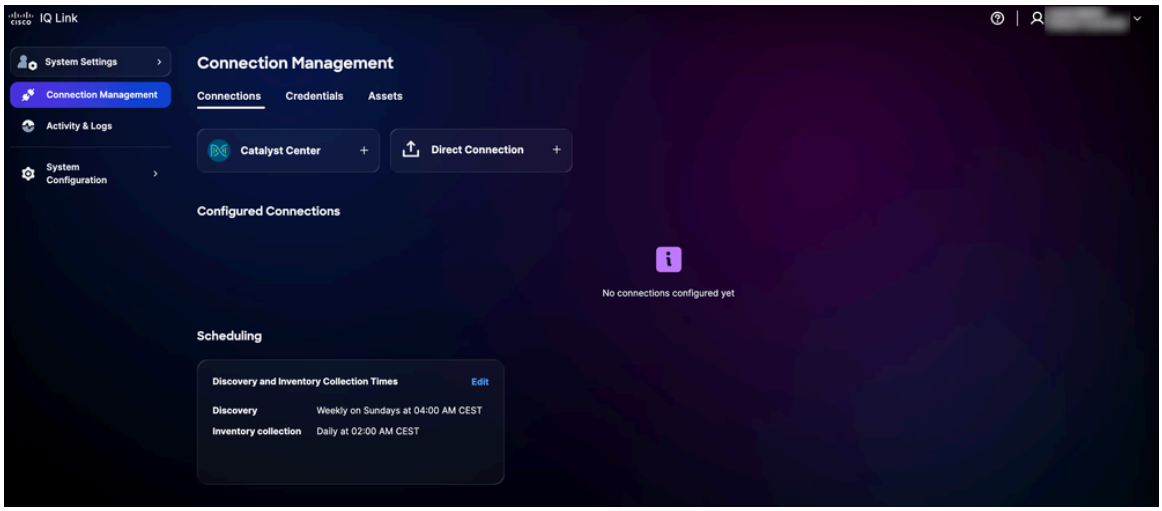
6. Pianificare una raccolta. Per ulteriori informazioni, vedere Pianificazione.

Nota: Cisco IQ Link è preconfigurato con una pianificazione automatica e il sistema avvia una pianificazione predefinita per la raccolta automatica. Si consiglia di modificare la programmazione per allinearla ai requisiti e alle finestre di manutenzione dell'organizzazione.

Connessione diretta

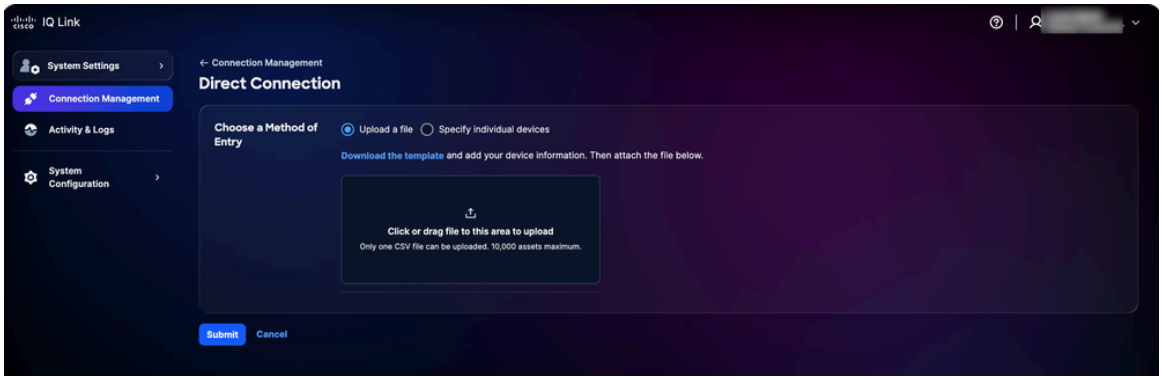
Per aggiungere dispositivi per la connessione diretta:

1. Da Impostazioni di sistema, scegliere Gestione connessione. Viene visualizzata la pagina Gestione connessione.



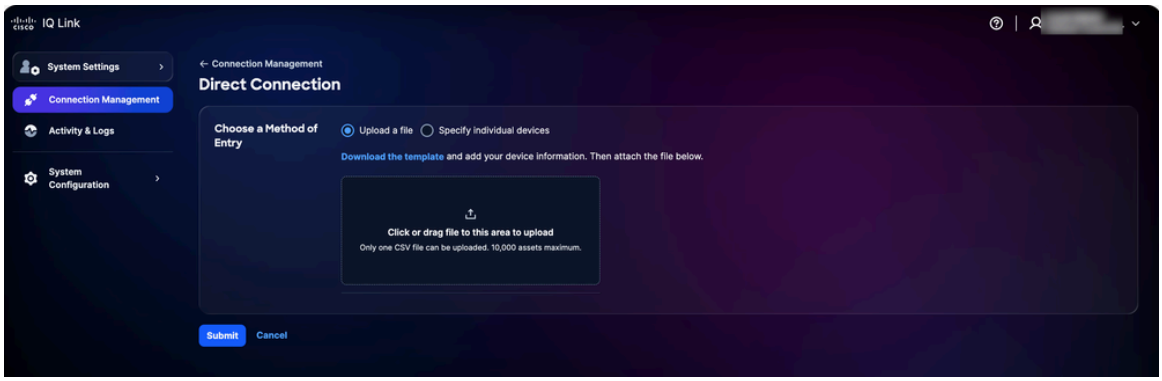
Gestione connessione

2. Fare clic su Connessione diretta. Viene visualizzata la pagina Connessione diretta con due (2) opzioni per la raccolta dei dati.



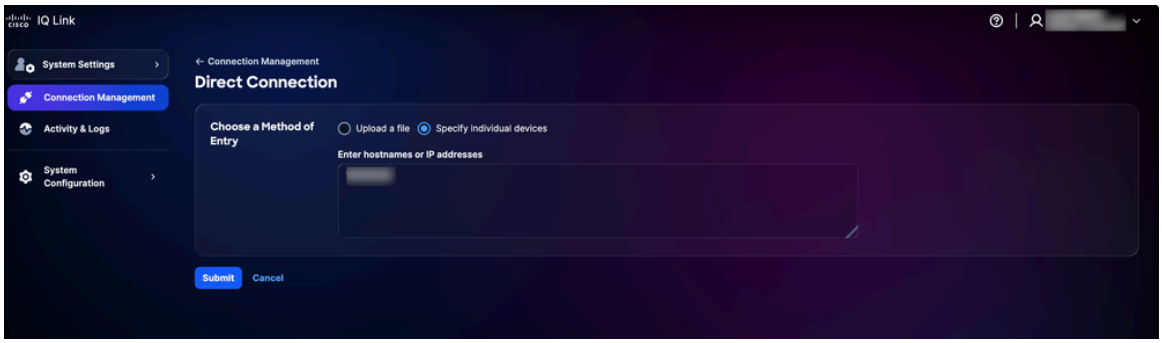
Carica file

3. Fare clic sull'opzione preferita per Scegliere un metodo di immissione e inviare i dispositivi utilizzando uno dei metodi seguenti:



Carica file

- Carica file: Fare clic sul file o trascinarlo e fare clic su Invia



Specificare i singoli dispositivi

- Specificare i singoli dispositivi: Immettere un nome host, un indirizzo IP o un elenco delimitato da virgole di nomi host e/o indirizzi IP, quindi fare clic su Invia

Dopo l'invio, l'utente viene reindirizzato alla scheda Asset.

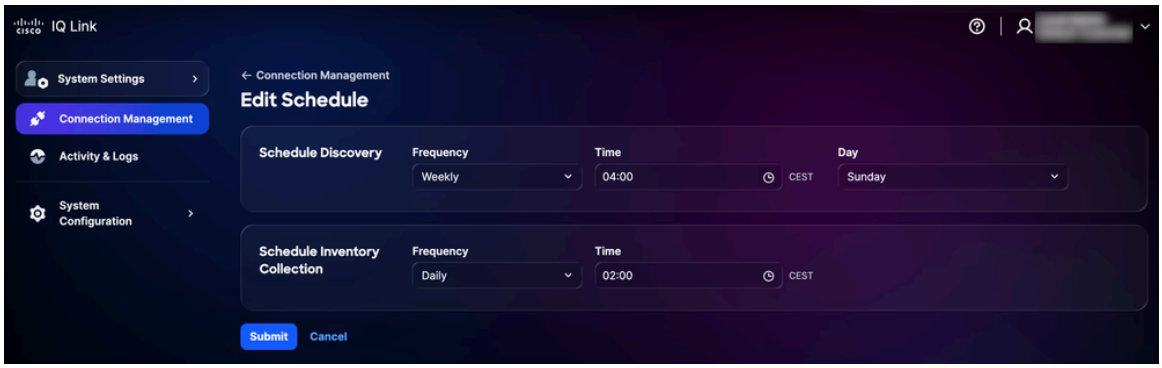
4. Pianificare una raccolta. Per ulteriori informazioni, vedere Pianificazione.

Nota: Cisco IQ Link è preconfigurato con una pianificazione automatica e il sistema avvia una pianificazione predefinita per la raccolta automatica. Si consiglia di modificare la programmazione per allinearla ai requisiti e alle finestre di manutenzione dell'organizzazione.

Programmazione

La pianificazione consente di definire quando Cisco IQ Link esegue la raccolta automatizzata dei dati. Per pianificare la raccolta:

1. Nella sezione Pianificazione della pagina Gestione connessione fare clic su Modifica per la pianificazione che si desidera modificare. Viene visualizzata la pagina Modifica pianificazione.



Modifica pianificazione

2. Nella sezione Pianificazione rilevamento, scegliere la frequenza e il giorno desiderati dagli

elenchi a discesa e immettere l'ora di inizio desiderata.

3. Nella sezione Pianifica raccolta scorte, scegliere la frequenza preferita dagli elenchi a discesa e immettere l'ora di inizio desiderata.

4. Fare clic su Invia.

Nota: Consentire 5-10 minuti per sincronizzare e riflettere accuratamente in Cisco IQ Link le modifiche apportate alle pianificazioni di individuazione e raccolta.

Banner

Gli amministratori possono configurare banner personalizzati da visualizzare in tutta l'applicazione.

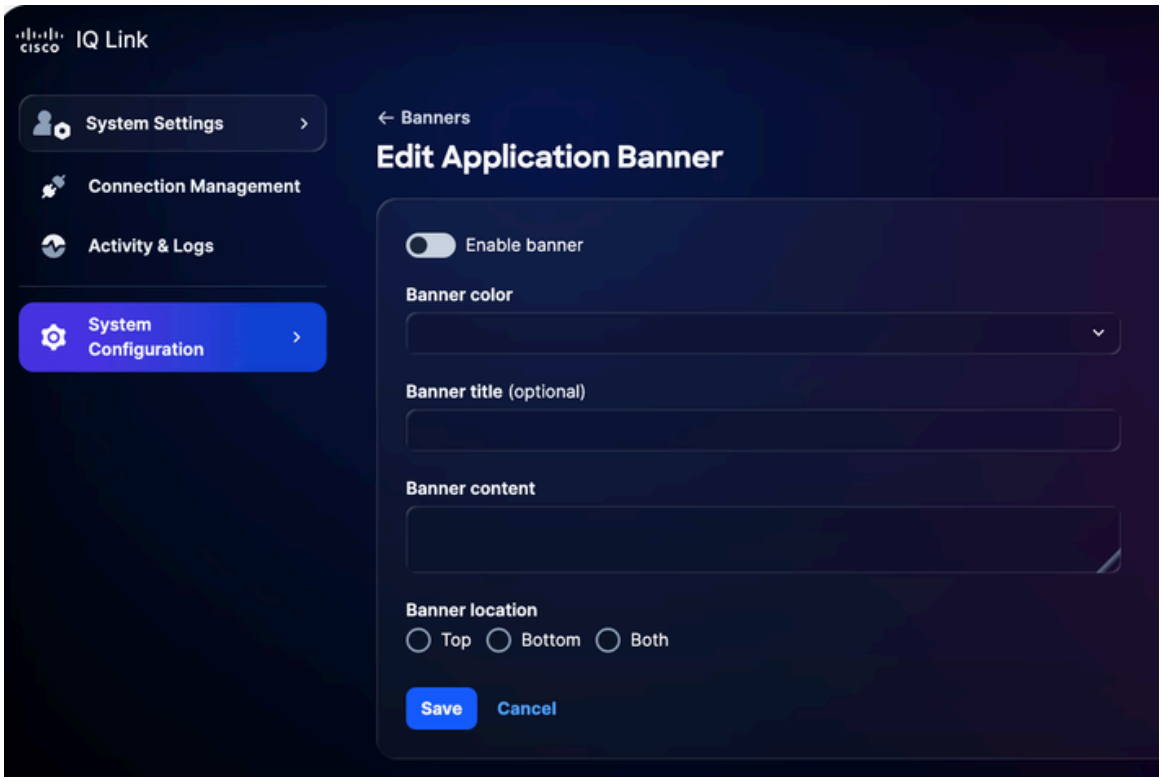
Configurazione dei banner

Per configurare un banner:

1. Da Impostazioni di sistema, scegliere Configurazione di sistema > Banner. Verrà visualizzata la pagina Banner.

Configura intestazione

2. Fare clic su Configure (Configura). Viene visualizzata la pagina Modifica banner applicazione.



Modifica banner applicazione

3. Fare clic sull'interruttore per abilitare o disabilitare il banner.
4. Selezionare un colore per l'intestazione.
5. Immettere il titolo del banner.
6. Immettere il contenuto del banner.
7. Selezionare una posizione per lo striscione.
8. Fare clic su Save (Salva). Il banner viene visualizzato in tutta l'applicazione.

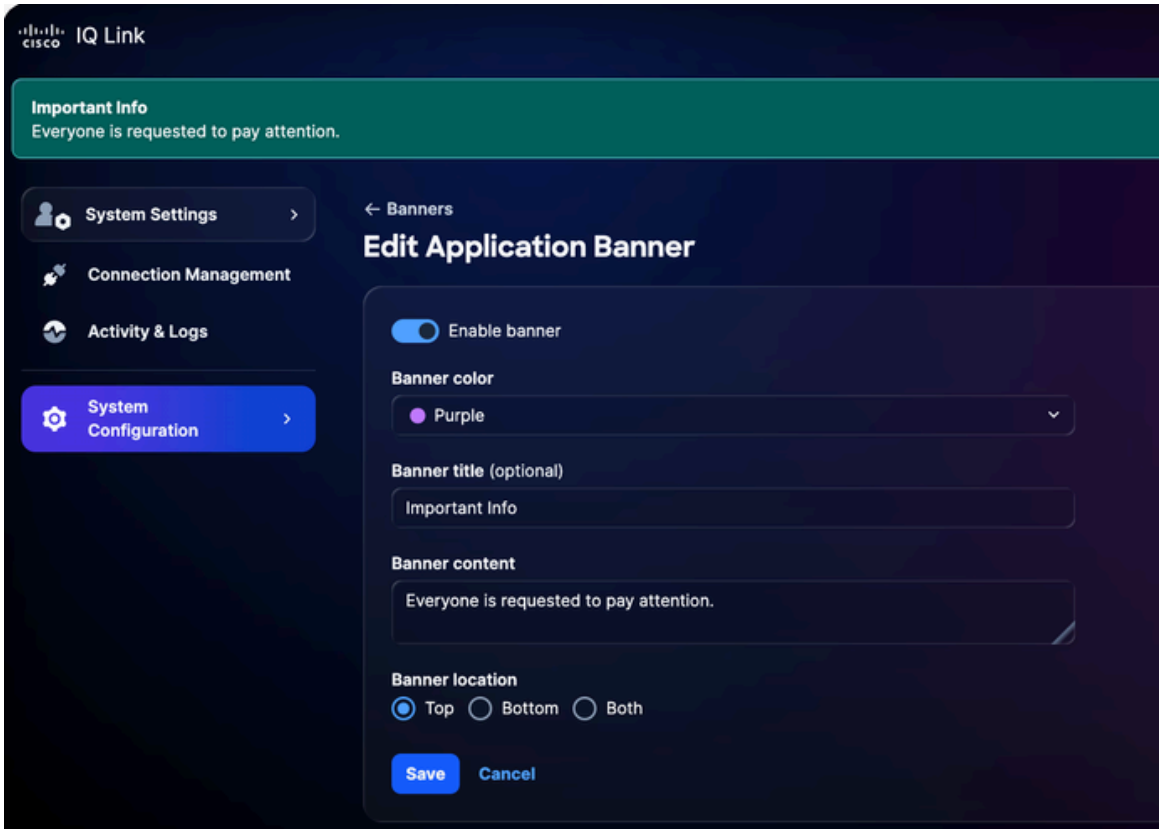
Modifica dei banner

Per modificare uno striscione:

1. Da Impostazioni di sistema, scegliere Configurazione di sistema > Banner. Verrà visualizzata la pagina Banner.

Modifica banner

2. Fare clic su Edit (Modifica). Viene visualizzata la pagina Modifica banner applicazione.



Modifica banner applicazione

3. Modificare i dettagli desiderati.
4. Fare clic sull'interruttore per abilitare o disabilitare il banner.
5. Fare clic su Save (Salva).

Risoluzione dei problemi

I clienti possono raccogliere i file diagnostici e di registro dal sistema Cisco IQ e trasferirli in modo sicuro su un server SCP. Questi file possono essere condivisi con il team di supporto durante la segnalazione di problemi per fornire un contesto utile e fornire assistenza nella risoluzione dei

problemi.

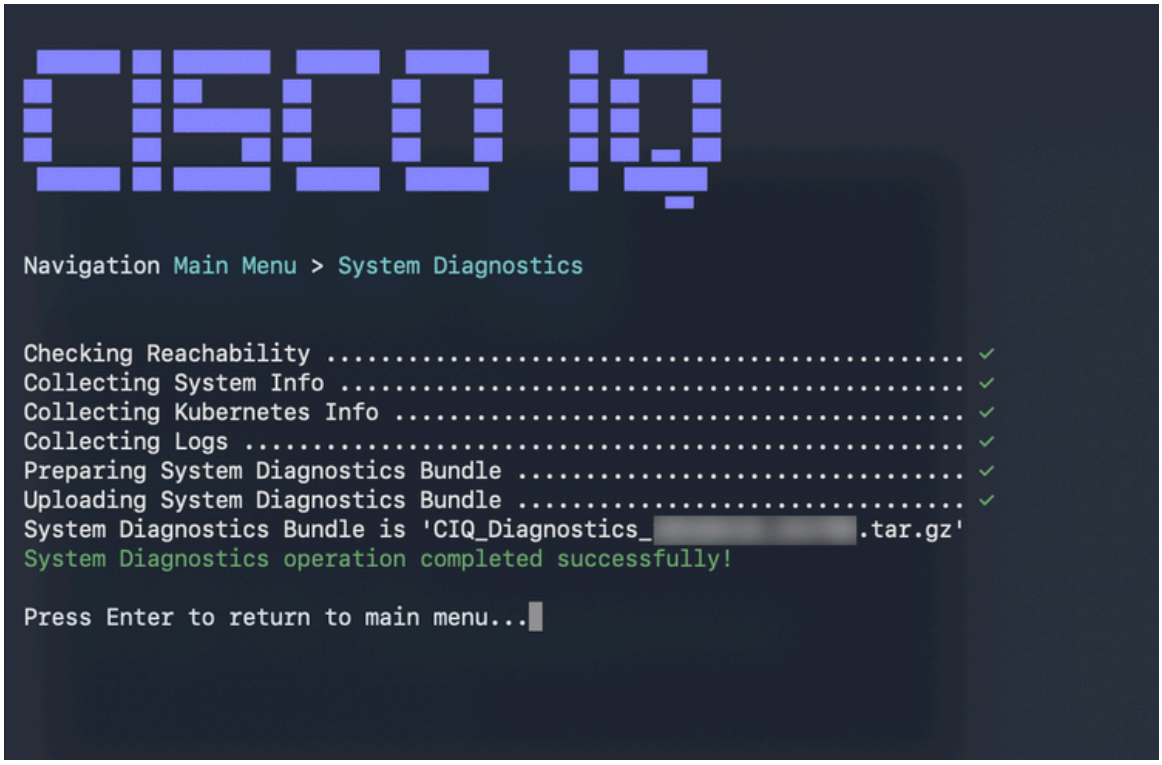
Per raccogliere i file di log e di diagnostica:

1. Accedere a Cisco IQ.

Menu principale

2. Dal menu principale di Cisco IQ, immettere "3" e premere Invio per selezionare System Diagnostics.

3. Immettere l'indirizzo del server SCP/SFTP.
4. Immettere la porta del server SCP/SFTP.
5. Immettere il percorso del server SCP/SFTP.
6. Selezionare un protocollo.
7. Immettere il nome utente.
8. Immettere la password.
9. Immettere "C" e premere Invio per continuare con la diagnostica di sistema.



Modello di completamento operazione di diagnostica CoSystem

Il sistema avvia il processo diagnostico ed esegue le seguenti azioni:

- Verifica della raggiungibilità
- Raccolta di informazioni sul sistema
- Raccolta delle informazioni Kubernetes
- Raccolta dei log
- Preparazione del pacchetto di diagnostica di sistema

- Caricamento del pacchetto di diagnostica del sistema

Una volta completato, viene visualizzato un messaggio di conferma che indica il nome del bundle generato.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).