# Cisco IQ Link Operations Guide v1.2.0

## Introduzione

Cisco IQTM offre miglioramenti e funzionalità progettati per migliorare la visibilità degli asset, offrire informazioni più dettagliate negli ambienti e semplificare la gestione dei casi. Inoltre, le funzioni di AI, come l'Assistente AI, ottimizzano i risultati operativi e l'esperienza utente di Cisco IQ fornendo una comprensione contestuale che consente 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 account devono utilizzare le credenziali seguenti:

- 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
- Contesto account predefinito: Default-Cliente

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

### Impostazione della protezione dell'amministratore locale

È possibile modificare la password e impostare le domande di sicurezza tramite il menu Profilo utente nella home page.

Impostazioni blocco

Durante la distribuzione è possibile configurare le impostazioni di blocco dell'account seguenti:

- Stato blocco: abilita o disabilita la funzione di blocco dell'account.
- Numero massimo tentativi di accesso: imposta il numero massimo di tentativi consecutivi non riusciti consentiti prima del blocco di un account (impostazione predefinita: 3; Intervallo: 0–10).
- Finestra temporale ricorrente: definisce il periodo di tempo per la registrazione dei tentativi non riusciti (impostazione predefinita: 15 minuti; Intervallo: 0-60 minuti).
- Durata: consente di impostare la durata per la quale un account rimane bloccato una volta raggiunto il numero massimo di tentativi (impostazione predefinita: 30 minuti Intervallo: 0-60 minuti).

---

Nota: Si hanno a disposizione tre (3) tentativi per immettere la password corretta entro un periodo di 15 minuti. Se tutti e tre (3) i tentativi hanno esito negativo, l'account viene temporaneamente bloccato per 30 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 30 minuti. A questo punto è possibile tentare di accedere o reimpostare la password.

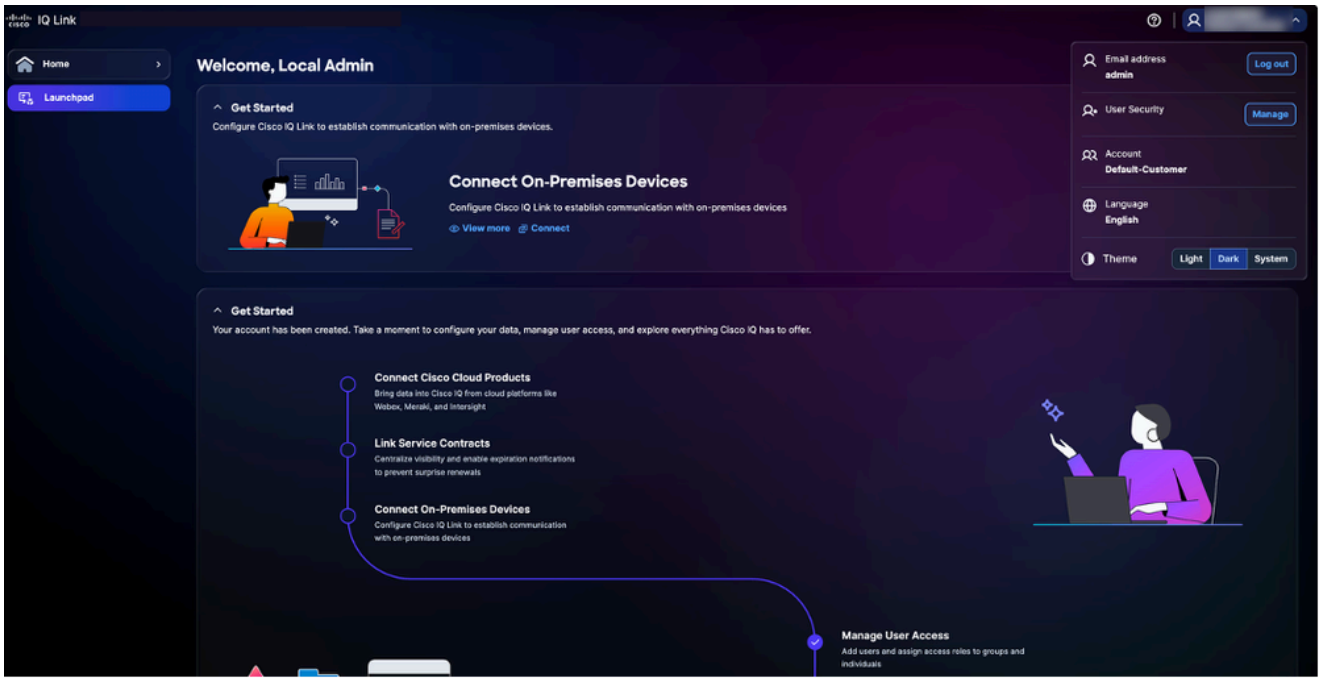
---

Impostazione di domande e risposte di sicurezza

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

Per impostare le domande di sicurezza:

1. Dalla home page, fare clic sull'icona Profilo utente. Viene visualizzato il menu a discesa.

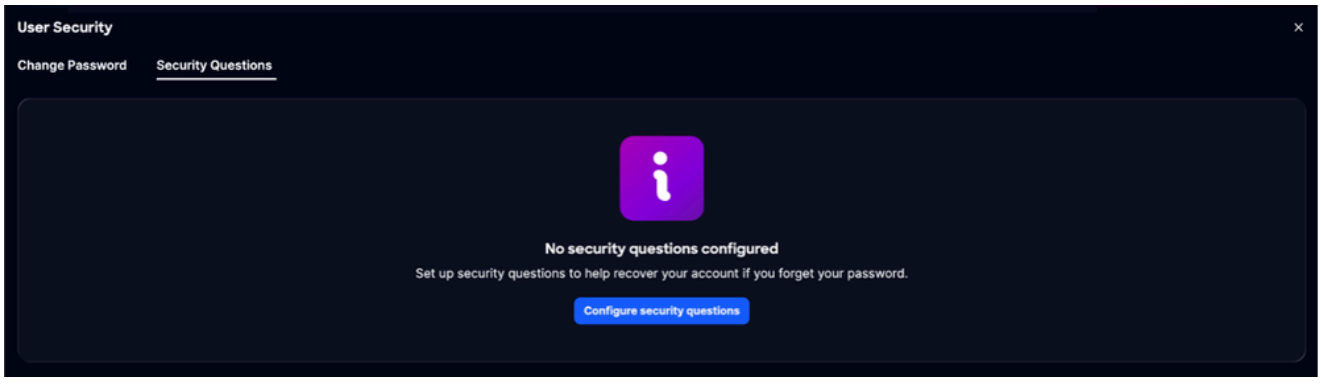



Menu Profilo utente

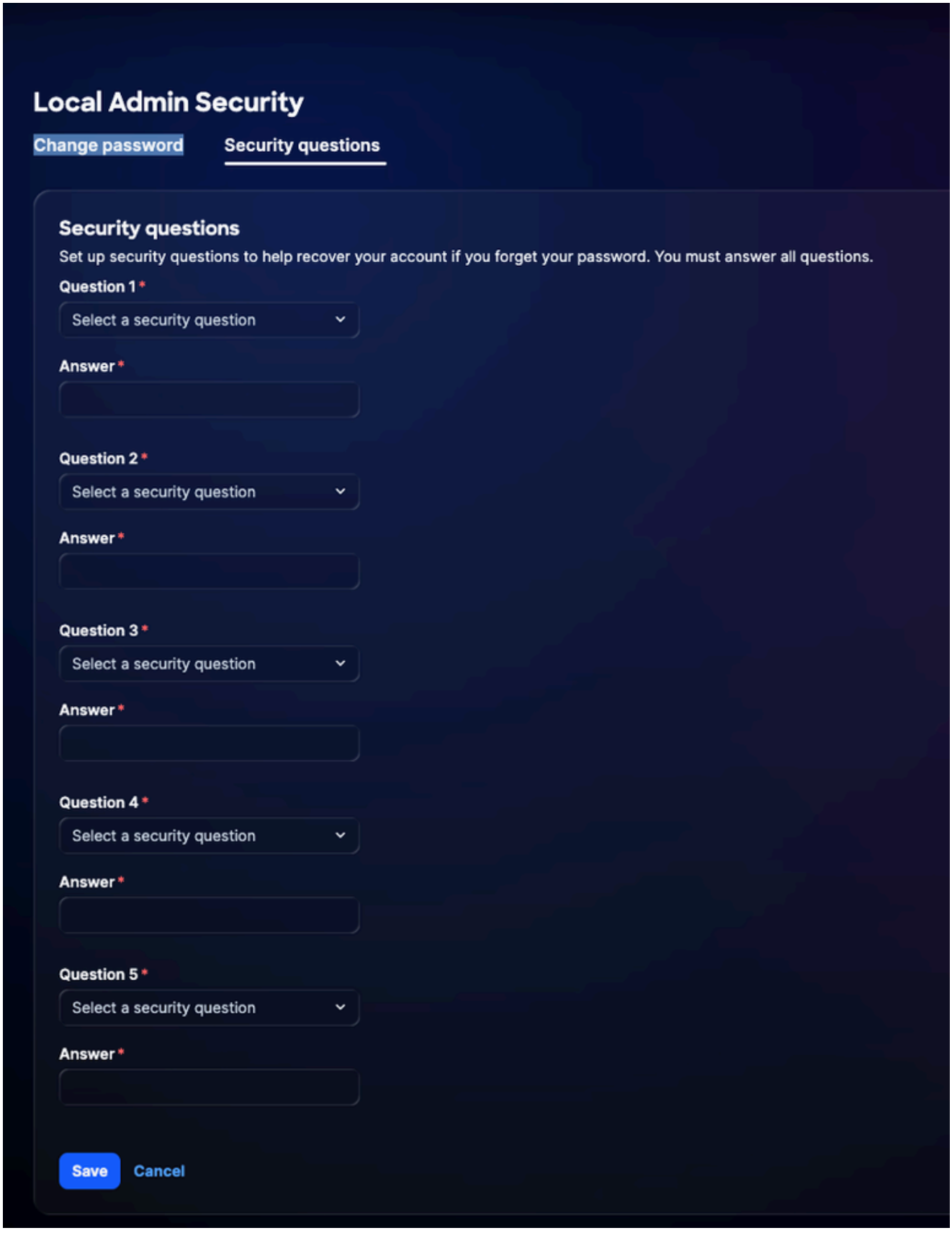
2. Fare clic su Gestisci in Protezione utente. Verrà visualizzata la pagina Sicurezza utente.


Cambia password

3. Fare clic su Domande di sicurezza per aprire la scheda.



4. Fare clic su Configura domande di sicurezza.



5. Scegliere cinque (5) domande di sicurezza dagli elenchi a discesa.
6. Inserisci la tua risposta per ogni domanda.
7. Fare clic su Save (Salva).

---

Nota: Le risposte non distinguono tra maiuscole e minuscole, ad esempio "SMITH" e "smith" sono considerati uguali.
Gli spazi aggiuntivi vengono ignorati, ad esempio " Smith" e "smith" vengono considerati uguali.

---

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

Gli amministratori di account e gli utenti locali possono gestire le password per Cisco IQ.

Per garantire la sicurezza dell'account, vengono applicati i seguenti criteri per le password:

- Restrizione al riutilizzo: la nuova password non può corrispondere a nessuna delle cinque (5) password precedenti. Questo criterio si applica ai flussi di registrazione, password dimenticata e modifica password.
- Variazione caratteri: quando si modifica la password durante l'autenticazione, almeno otto (8) caratteri della password corrente devono essere diversi nella nuova password.
- Intervallo minimo di modifica: per impostazione predefinita, è necessario attendere 24 ore prima di modificare di nuovo la password. Se è stato configurato un intervallo diverso, non sarà possibile aggiornare la password fino a quando non sarà trascorso tale intervallo.
- Scadenza password: Le password scadono ogni 60 giorni. Al primo accesso successivo alla data di scadenza, verrà richiesto di impostare una nuova password prima di poter accedere al sistema. Se è configurato su 0, la scadenza della password è disabilitata.

Prerequisiti

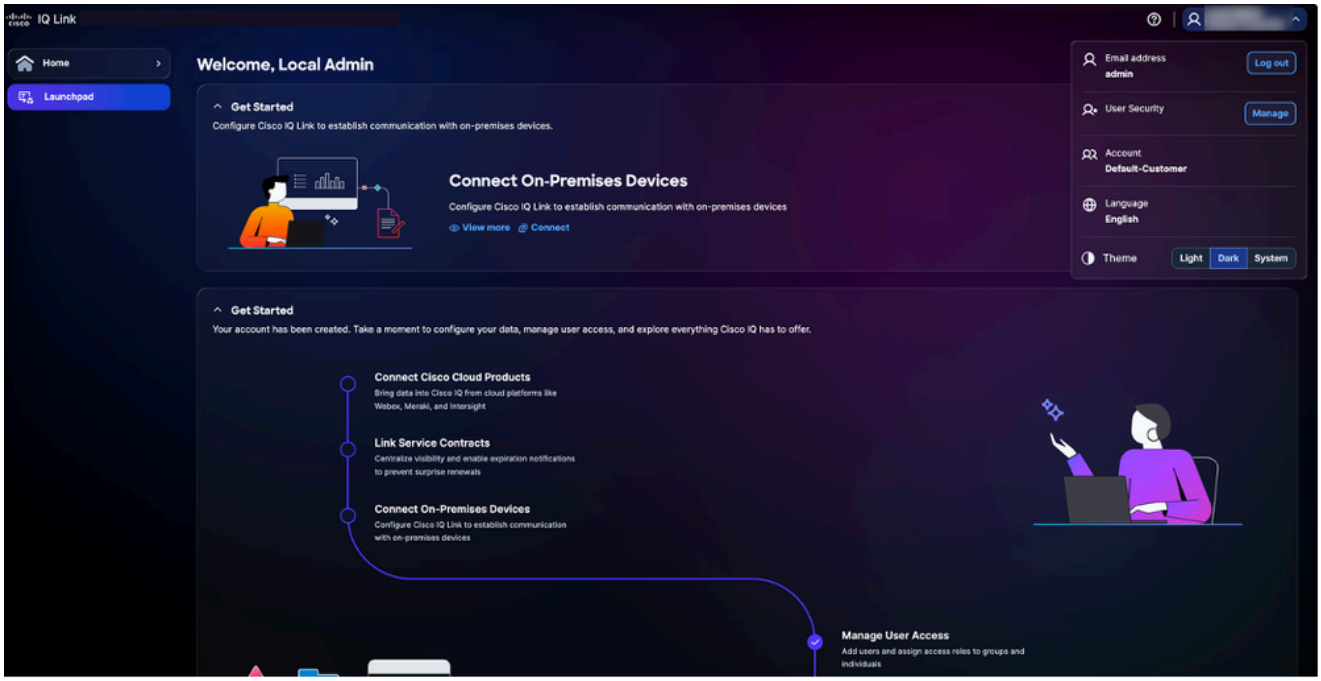
Per gestire le password, è necessario che siano soddisfatte le seguenti condizioni:

- L'utente corrente è un amministratore o un utente dell'account locale
- Si sta utilizzando un account locale (non Single Sign-On (SSO) o autenticazione esterna)
- È stato eseguito l'accesso a Cisco IQ Link
- Si conosce la password corrente

Modifica delle password

Per modificare una password:

1. Dalla home page, fare clic sull'icona Profilo utente. Viene visualizzato il menu a discesa.




Menu Profilo utente

2. Fare clic su Gestisci in Protezione utente. Verrà visualizzata la pagina Sicurezza utente.


Cambia password

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

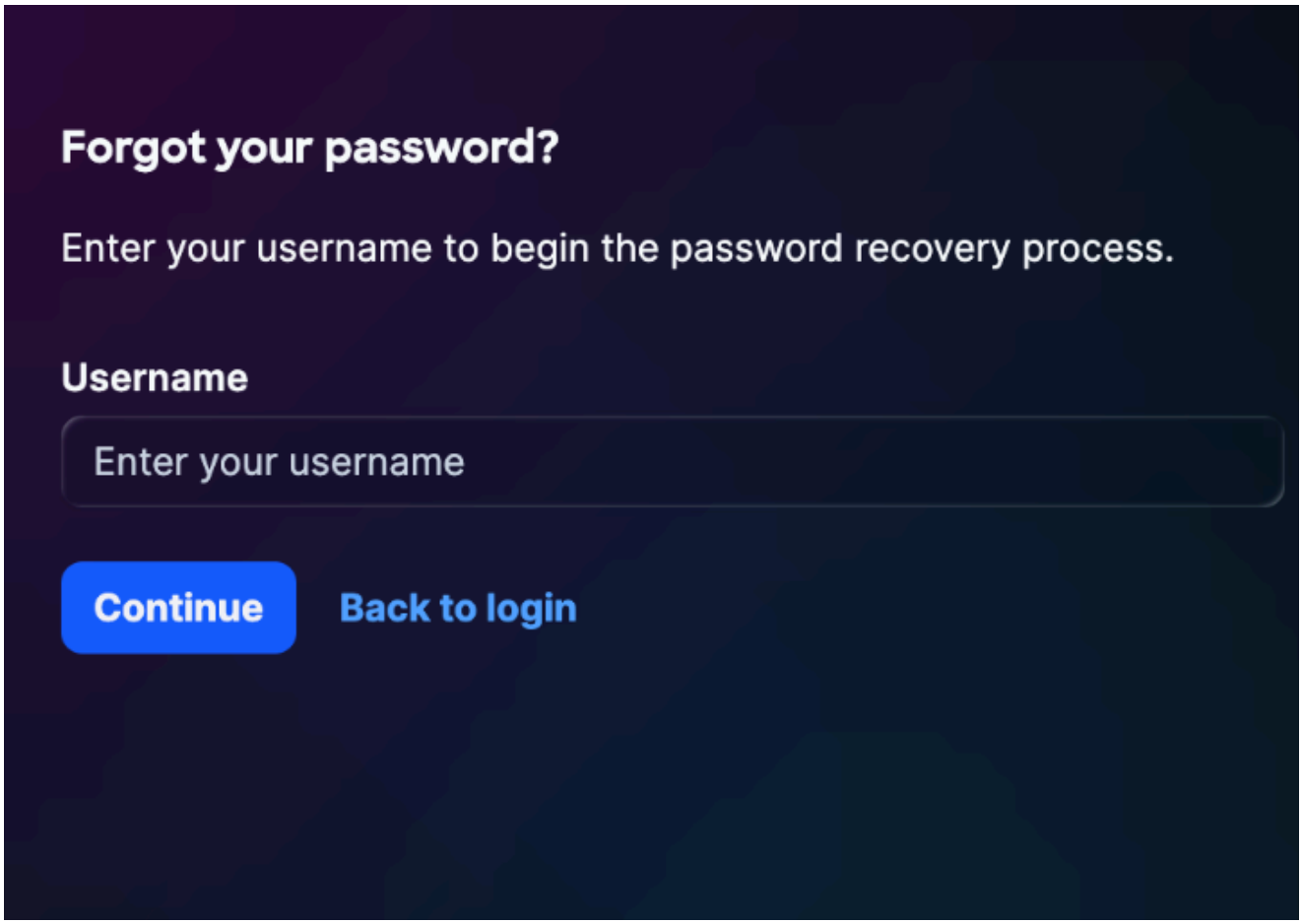
La password viene aggiornata nel sistema Cisco IQ, inclusa la macchina virtuale Cisco IQ (VM).

### 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.

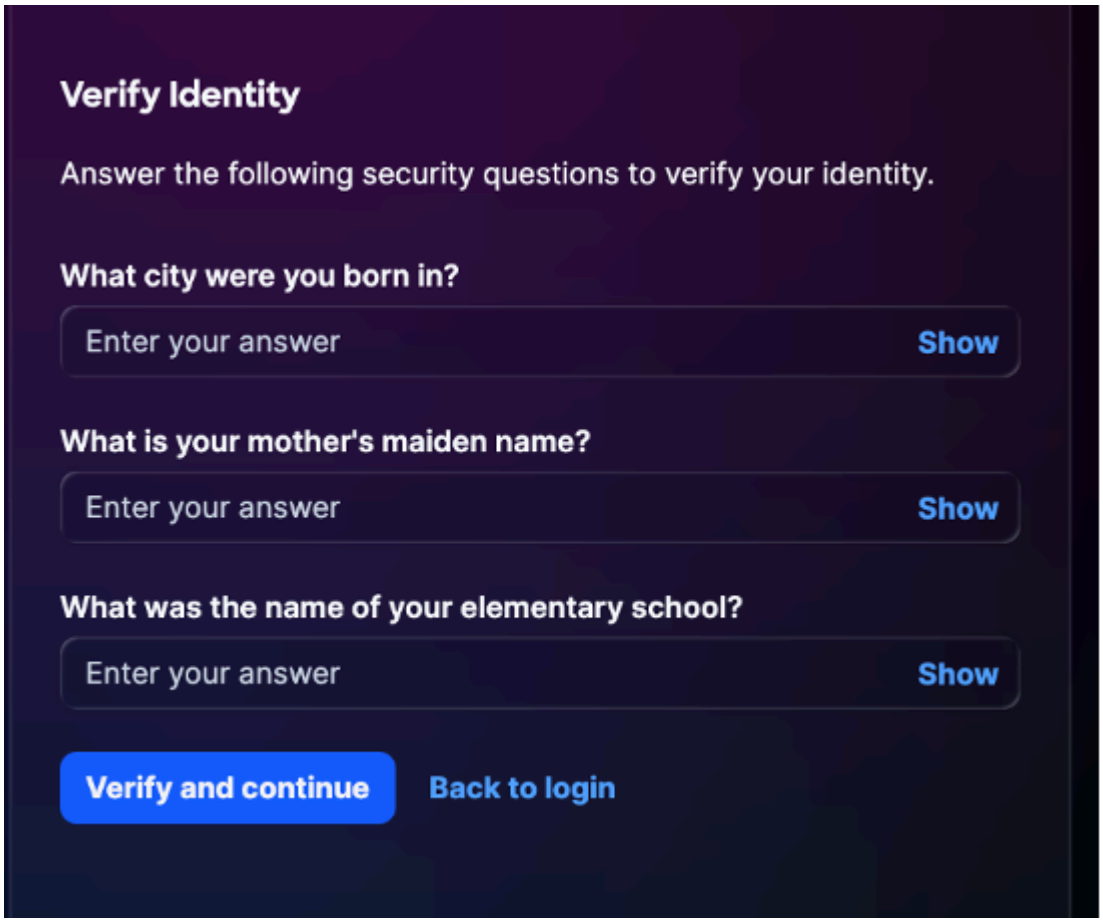
Per reimpostare una password dimenticata:

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

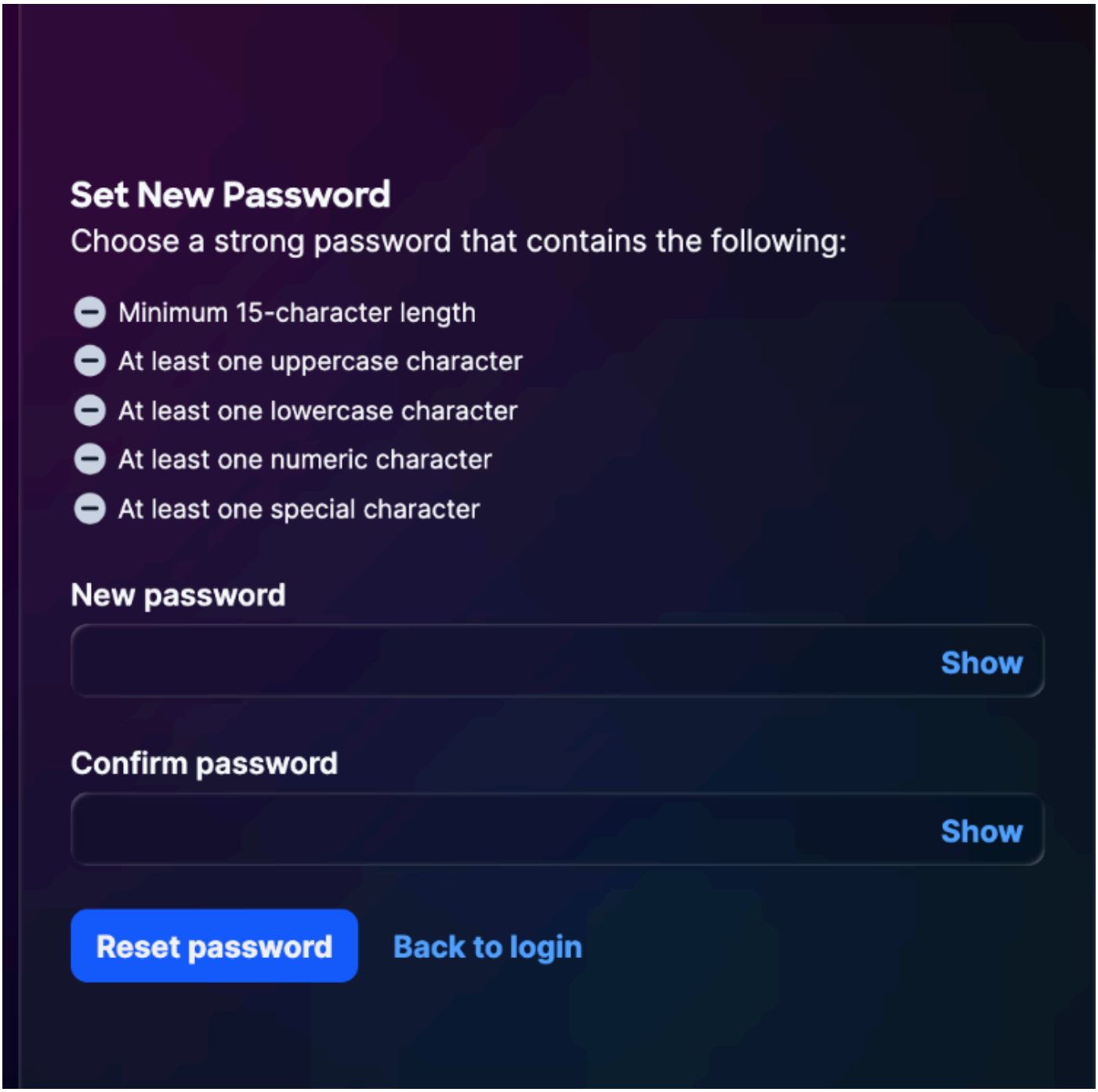
---

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

Hai a disposizione tre (3) tentativi per rispondere correttamente alle domande di sicurezza entro un periodo di 15 minuti. Se tutti e tre (3) i tentativi hanno esito negativo, l'account viene temporaneamente bloccato per 30 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 30 minuti. A questo punto è possibile tentare di accedere o reimpostare la password.

7. Inserire la nuova password.

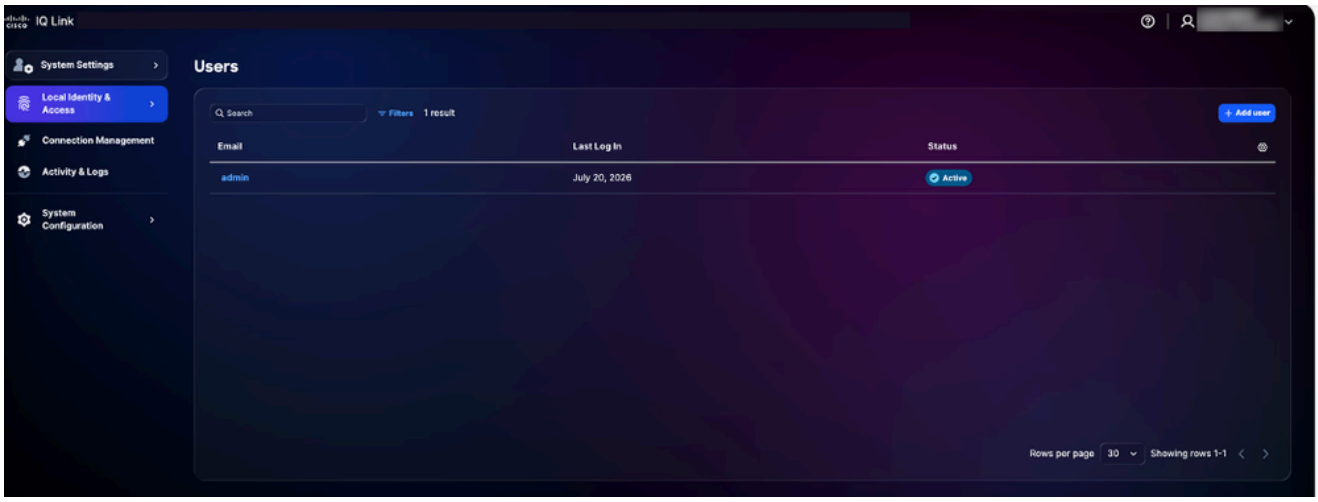
8. Inserire nuovamente la password per confermarla.

9. Fare clic su Sottometti.

## Aggiunta di utenti locali

Gli amministratori account possono aggiungere utenti all'account Cisco IQ. Per aggiungere un nuovo utente:

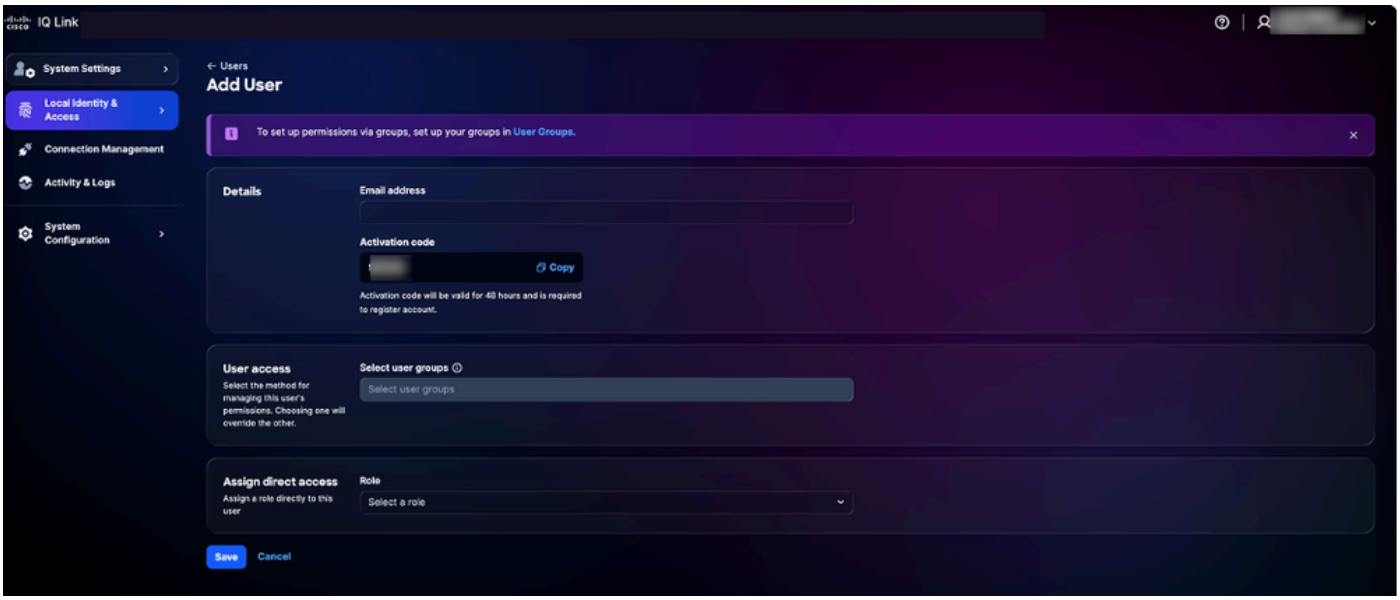
1. Passare a Impostazioni di sistema > Identità locale e accesso > Utenti. Verrà visualizzata la pagina Utenti. Vengono elencati tutti gli utenti locali esistenti con il relativo stato.




Pagina Utenti

Nota: L'icona Altre opzioni non viene visualizzata per gli amministratori account (come mostrato nell'immagine precedente).

2. Fare clic su Aggiungi utenti. Verrà visualizzata la pagina Aggiungi utente.




Aggiungi utente

3. Inserire l'indirizzo e-mail.

4. Inserire il codice di attivazione.

---

Nota: Il codice di attivazione viene visualizzato per impostazione predefinita. Condividerlo con l'utente, poiché è necessario per completare la registrazione.

---

5. Nell'elenco a discesa Accesso utente, scegliere il gruppo di utenti dall'elenco a discesa Seleziona gruppi di utenti.

---

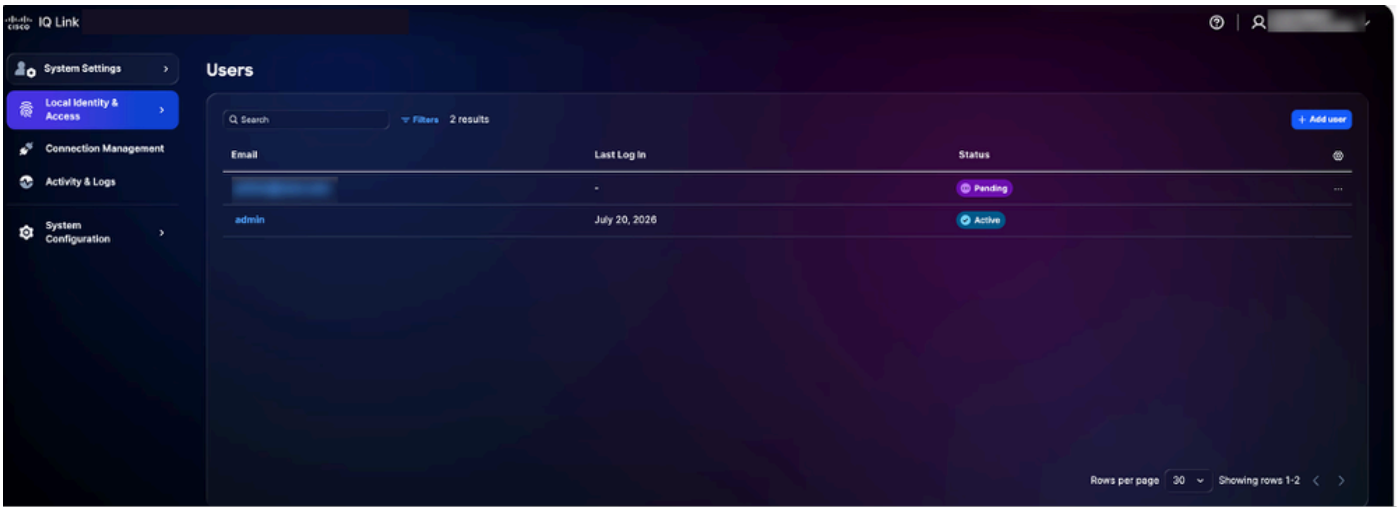
Nota: Gli utenti ereditano l'accesso dal gruppo selezionato.

---

6. In Assegna accesso diretto, scegliere il ruolo dall'elenco a discesa Ruolo. Sono disponibili due (2) ruoli:

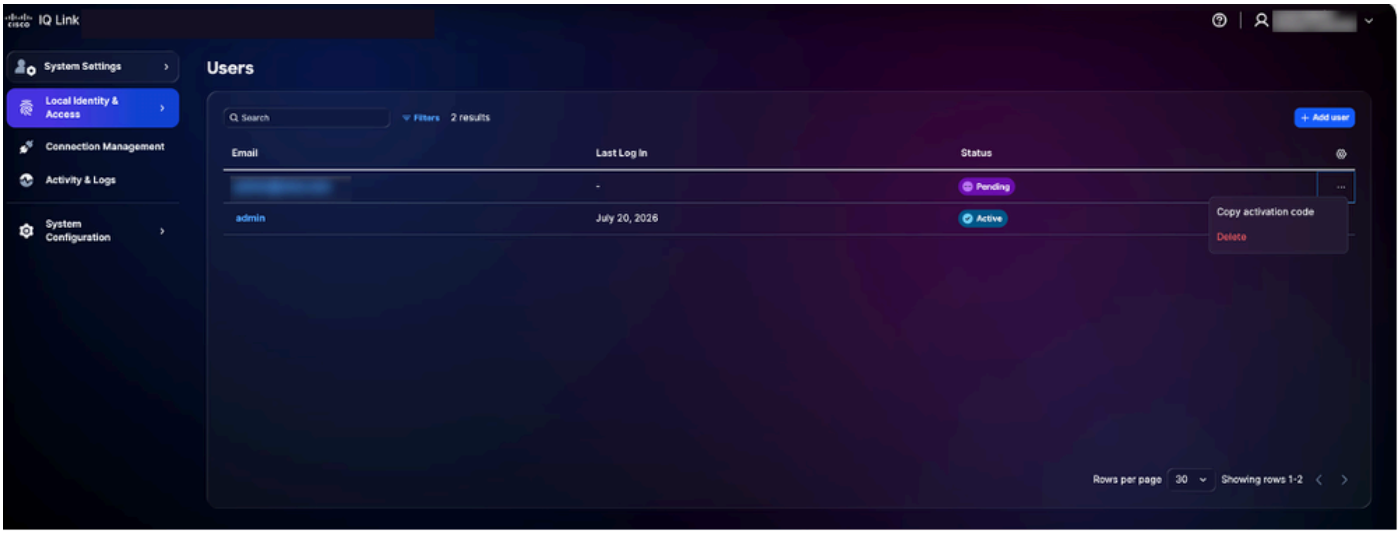
- Visualizzatore: Visualizza e accedi alle applicazioni
- Amministratore: Accesso alle applicazioni e gestione delle impostazioni di sistema, ad eccezione di Gestione sistema e IDP

7. Fare clic su Salva. Il nuovo utente viene creato e visualizzato nell'elenco degli utenti con lo stato In sospeso. In sospeso indica che l'utente non ha ancora completato l'attivazione automatica.




Nuovo utente aggiunto

8. Individuare nell'elenco l'utente appena creato e verificare che nella colonna Stato sia visualizzato In sospeso.




Copia codice di attivazione

9. Fare clic sull'icona Altre opzioni > Copia codice di attivazione accanto all'utente appena creato. Il codice di attivazione viene copiato negli Appunti.

10. Condividere questo codice con l'utente in modo sicuro, ad esempio tramite un canale interno protetto. Il codice di attivazione deve essere utilizzato una sola volta ed è necessario per completare la registrazione.

---

Nota: Non condividere il codice di attivazione su canali non protetti. Se il codice viene perso o compromesso, utilizzare l'icona Menu per rigenerare un nuovo codice di attivazione che invalida quello precedente

---

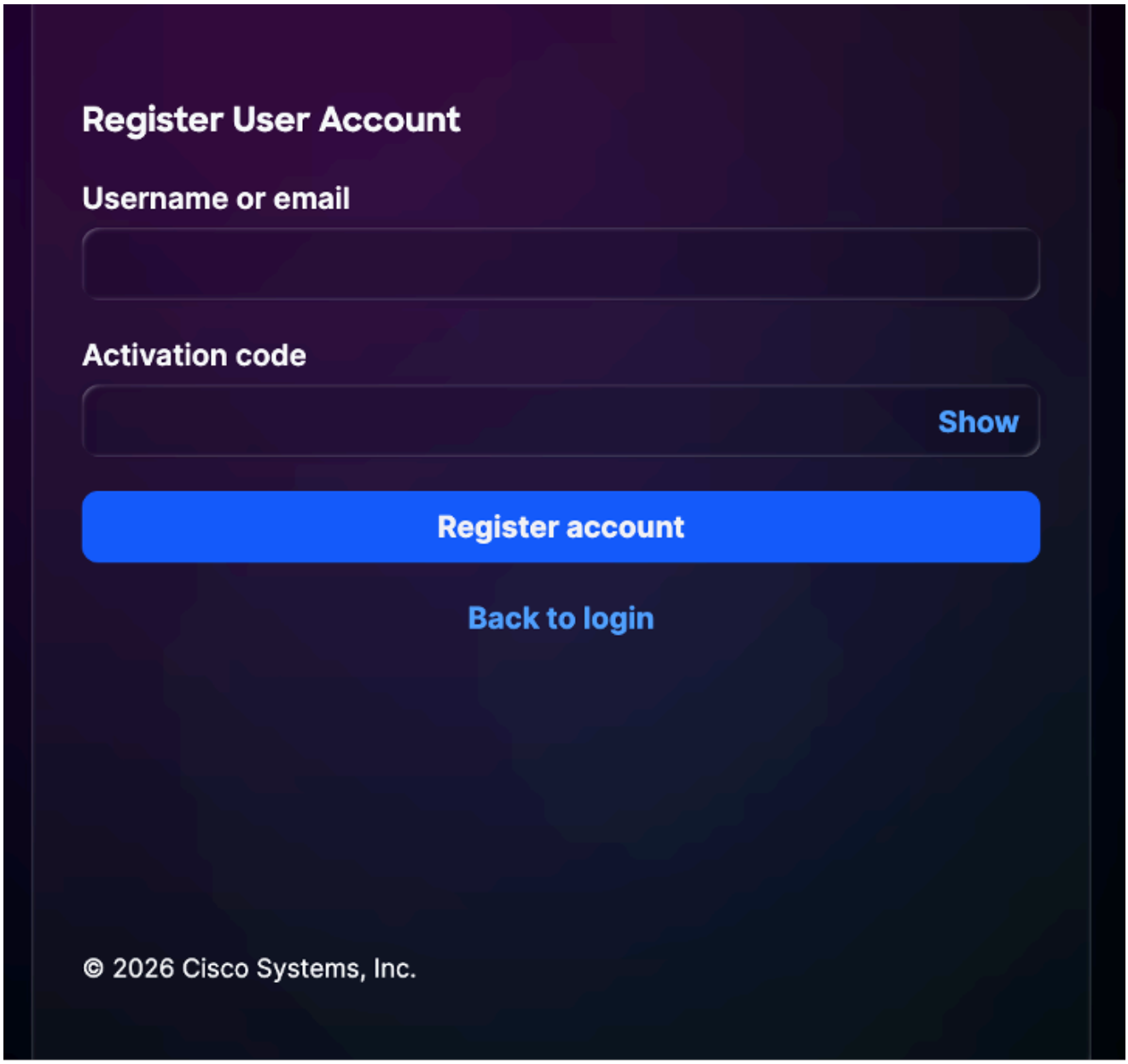
Nota: i codici di attivazione sono validi per 48 ore. Se il codice scade, contattare l'amministratore dell'account per richiederne uno nuovo.

11. Per disconnettersi, fare clic sull'icona Utente nell'angolo superiore destro e selezionare Disconnetti. Viene visualizzata di nuovo la pagina di accesso di Cisco IQ.

Registrazione nuovo account utente

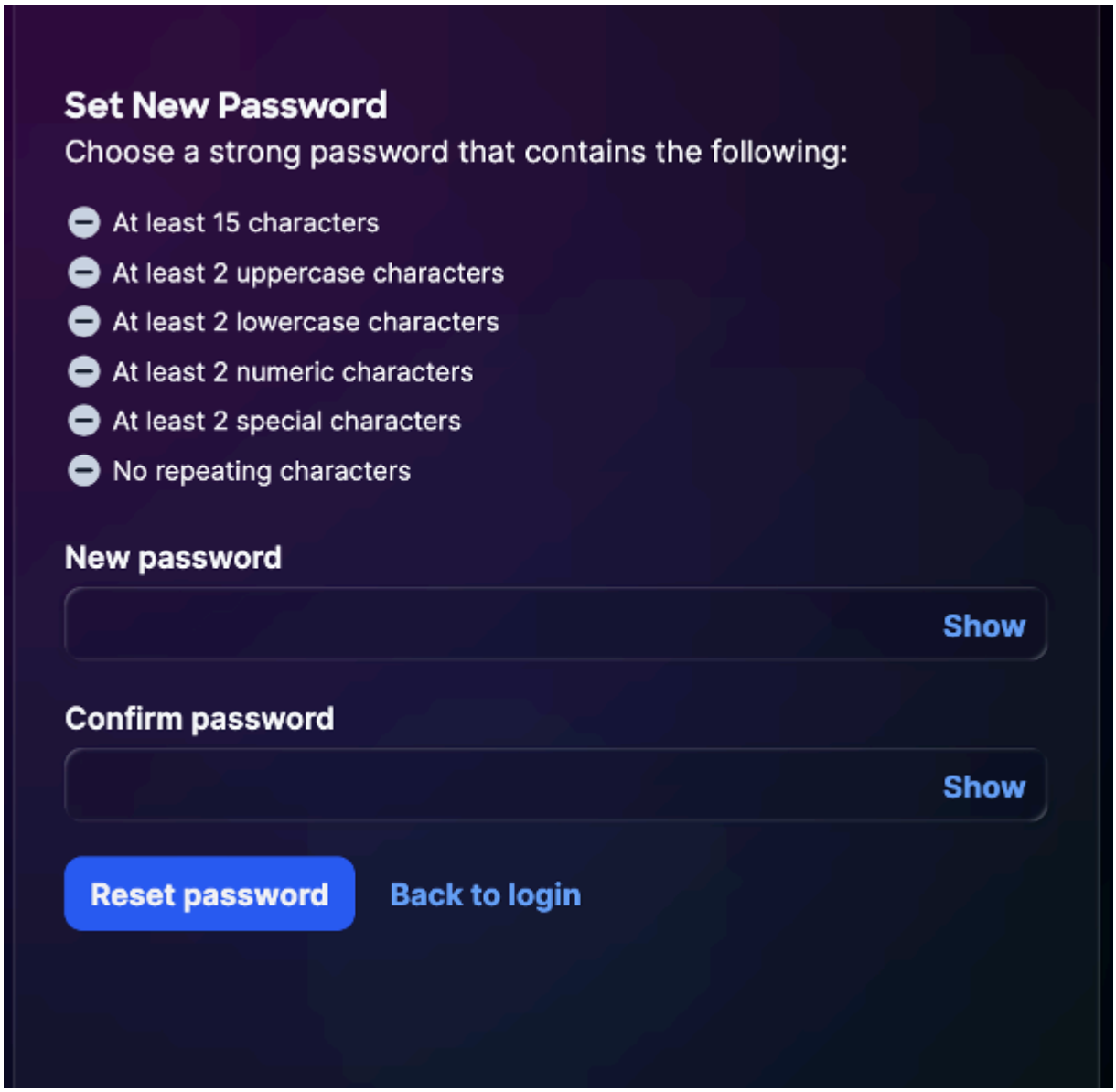
Per registrare il nuovo account utente:

1. Nella pagina di accesso, fare clic sul collegamento Registra un nuovo account utente.




Nuovo account utente

2. Immettere il nome utente o l'indirizzo di posta elettronica utilizzato al momento della creazione dell'utente (ad esempio, user1@abc.com).
3. Immettere il codice di attivazione condiviso dall'amministratore account.
4. Fare clic su Registra account. Viene visualizzata la finestra Imposta nuova password.




Password nuovo account utente

5. Immettere una nuova password.
6. Immettere nuovamente la password in Conferma password.
7. Al primo accesso riuscito, all'utente viene richiesto di configurare cinque (5) domande di sicurezza (per ulteriori informazioni, vedere Impostazione di domande e risposte di sicurezza).

## Gestione dei gruppi di utenti locali

I gruppi di utenti consentono agli amministratori degli account di gestire insieme i ruoli per più utenti locali. Anziché assegnare un ruolo a ogni utente singolarmente, un amministratore degli account può creare un gruppo, associarvi un ruolo e un set di utenti e aggiornare il ruolo o l'appartenenza in un'unica posizione. La gestione di tutti i gruppi di utenti viene eseguita dalla pagina Identità locale e accesso.

---

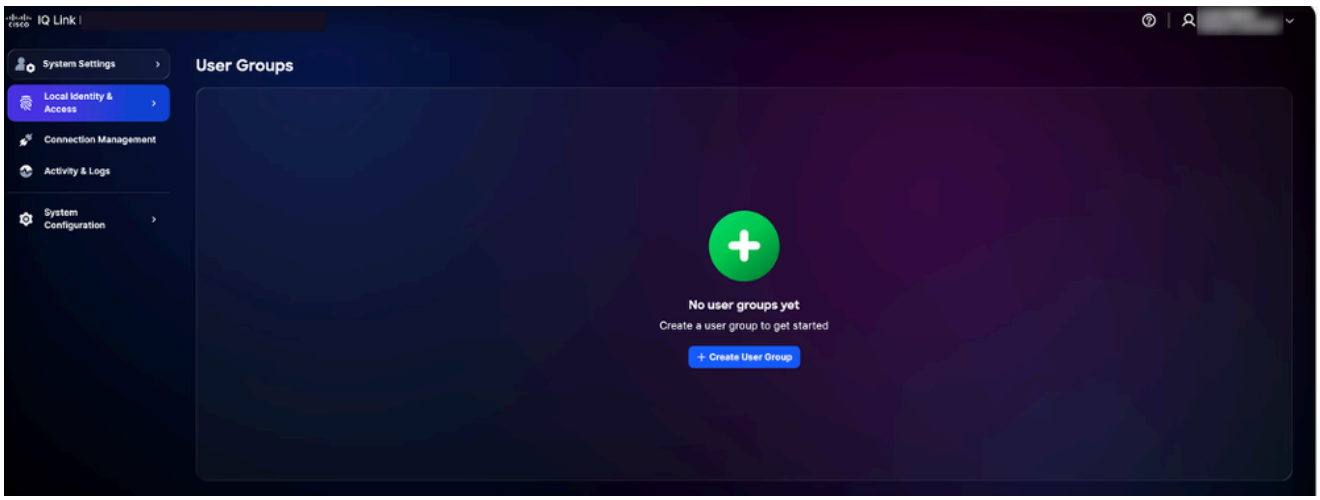
Nota: Solo un amministratore di account può creare, modificare o eliminare i gruppi di utenti. I gruppi sono composti da utenti locali esistenti; prima di poter aggiungere gli utenti a un gruppo, è necessario crearli.

---

Creazione di un gruppo di utenti

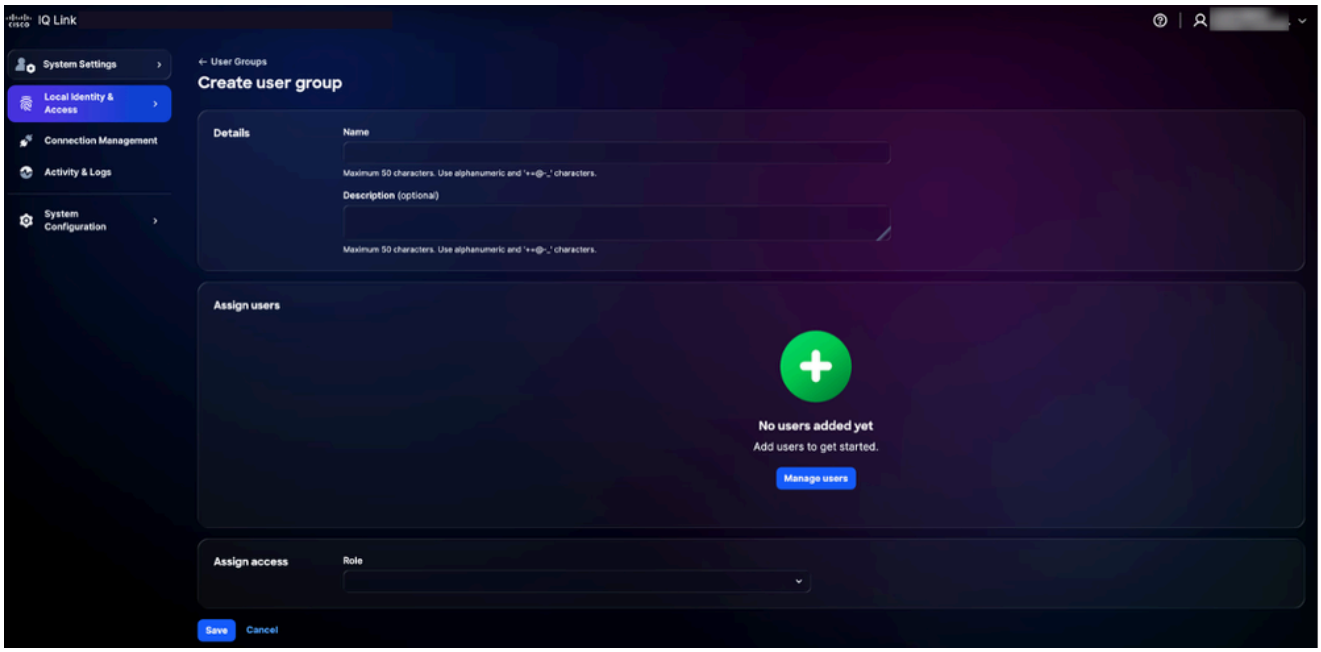
Per creare un gruppo di utenti:

1. Da Impostazioni di sistema, scegliere Identità locale e accesso > Gruppi di utenti. Viene visualizzata la pagina Gruppi di utenti.




Gruppi di utenti

2. Fare clic su Crea gruppo utenti. Viene visualizzata la pagina Crea gruppo utenti.




Crea gruppo utenti

3. Completare le sezioni seguenti:

- Dettagli
  - Nome: Immettere un nome univoco per il gruppo, ad esempio Operatori di sola lettura
  - Descrizione (facoltativa): Breve descrizione del gruppo (massimo 50 caratteri; caratteri alfanumerici e + = @ - _ consentiti)

- Assegna utenti

  Cercare e selezionare uno o più utenti locali esistenti da aggiungere al gruppo.

  Nota: Per aggiungere utenti non ancora elencati, fare clic su Gestisci utenti.

- Assegna accesso

  - Ruolo: Selezionare il ruolo di sistema da assegnare a tutti i membri del gruppo. Sono disponibili i seguenti ruoli:

    - Visualizzatore: Visualizza e accedi alle applicazioni (sola lettura)
    - Amministratore: Accedere alle applicazioni e gestire le impostazioni di sistema

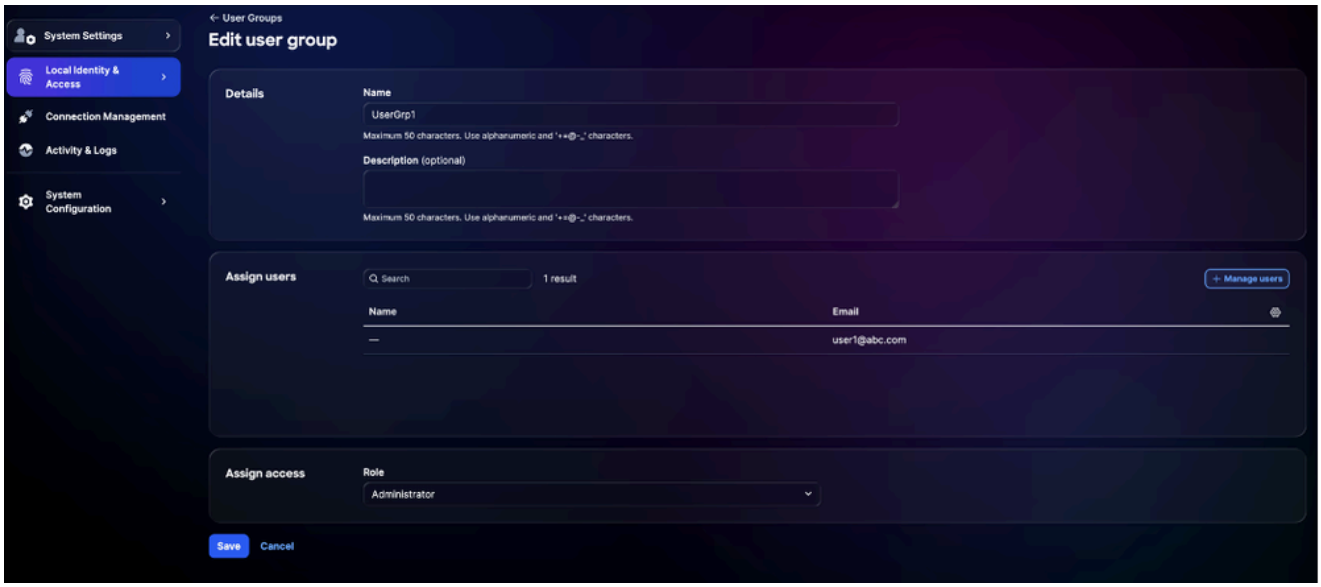
4. Fare clic su Salva.

Il nuovo gruppo di utenti viene visualizzato nell'elenco Gruppi di utenti insieme al ruolo assegnato e al numero di membri.

Modifica di un gruppo di utenti

Per modificare un gruppo di utenti:

1. Dalla lista Gruppi di utenti, individuare il gruppo che si desidera modificare.
2. Fare clic sull'icona Altro accanto al gruppo e scegliere Modifica. Viene visualizzata la pagina Modifica gruppo di utenti.




Modifica gruppo di utenti

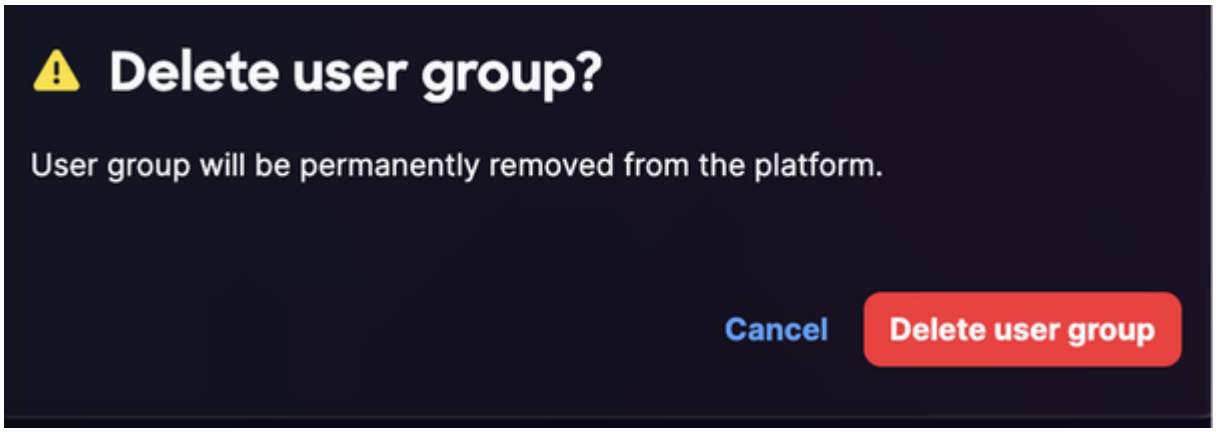
3. Apportare le modifiche desiderate.
4. Fare clic su Save (Salva).

Il gruppo aggiornato viene visualizzato nell'elenco Gruppi utenti. Il nuovo ruolo diventa effettivo per tutti i membri del gruppo.

## Eliminazione di un gruppo di utenti

Per eliminare un gruppo di utenti:

1. Dalla lista Gruppi di utenti, individuare il gruppo che si desidera eliminare.
2. Fare clic sull'icona Altre opzioni accanto al gruppo e selezionare Elimina.




Elimina gruppo di utenti

3. Confermare l'eliminazione quando richiesto.

Il gruppo viene rimosso dall'elenco Gruppi utenti.

Nota: L'eliminazione di un gruppo di utenti comporta la rimozione dell'assegnazione di ruolo basata su gruppo da tutti i membri. I singoli account utente non vengono eliminati.

## Configurazione del provider di identità

Dopo aver eseguito l'accesso a Cisco IQ Link, l'amministratore account può configurare diverse impostazioni. Gli amministratori degli account possono accedere a Cisco IQ Link usando l'amministrazione locale o la configurazione di Identity Provider (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.
Tabella 1: 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 |
| Destinatari | Non forza lavoro |
| Categoria caricamento | Selezionare "New Onboarding" (Nuovo caricamento) |

Tabella 2: Parametri di configurazione SAML

| Parametro | Configurazione | Esempio |
|---|---|---|
| Destinatari (ID entità) | Nome dominio completo (FQDN) | mymanagementhost.mydomain.com |
| URL Single Sign-On | Endpoint SAML Assertion Consumer Service (ACS) | 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.

Tabella 3. 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 |

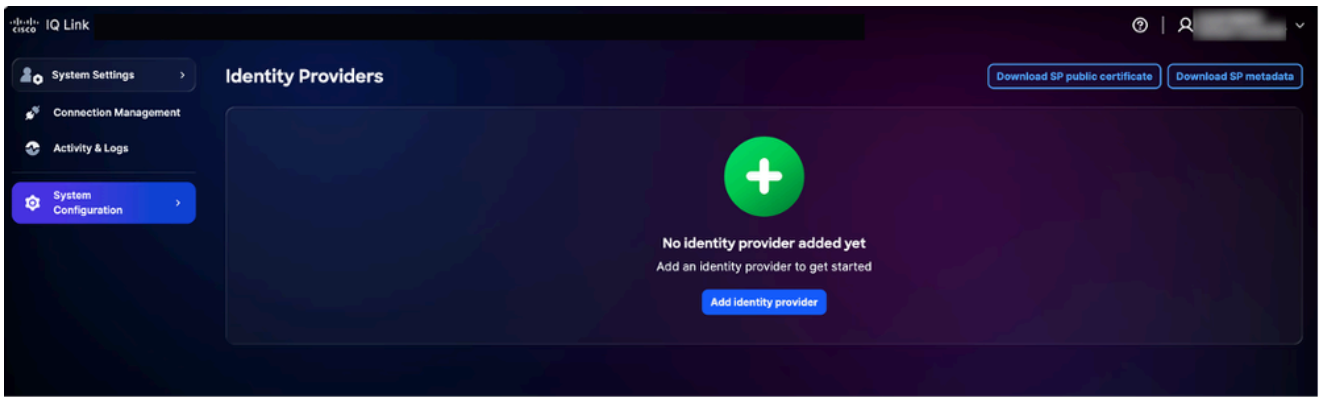
5. Fare clic sull'icona Download per scaricare il file "SP Metadata".

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

Aggiunta di IDP Okta

Per aggiungere un IDP in Cisco IQ Link:

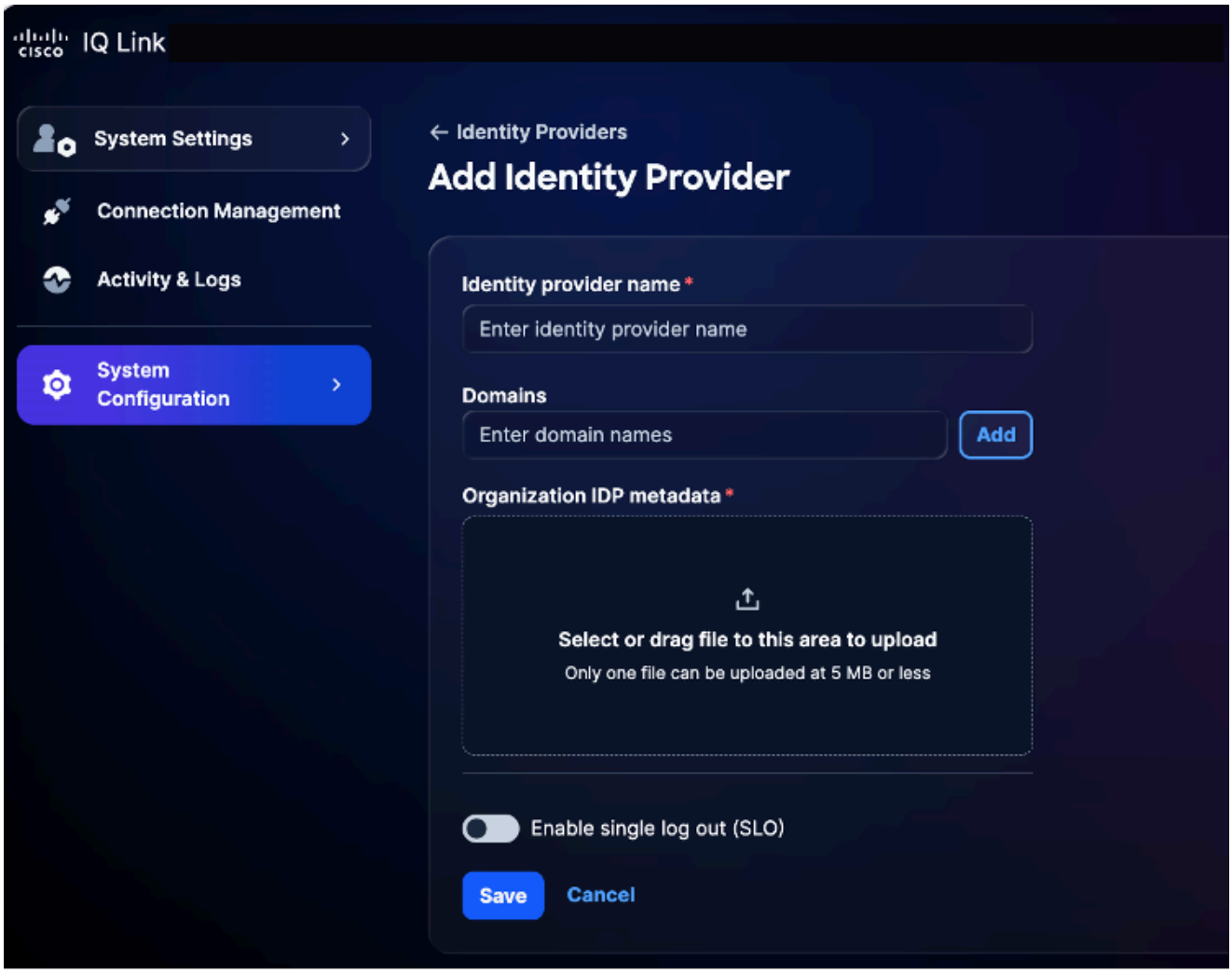
1. Da Impostazioni di sistema, scegliere Configurazione di sistema > Provider di identità. Viene visualizzata la pagina Provider di identità.




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. Inserire il nome del provider di identità.

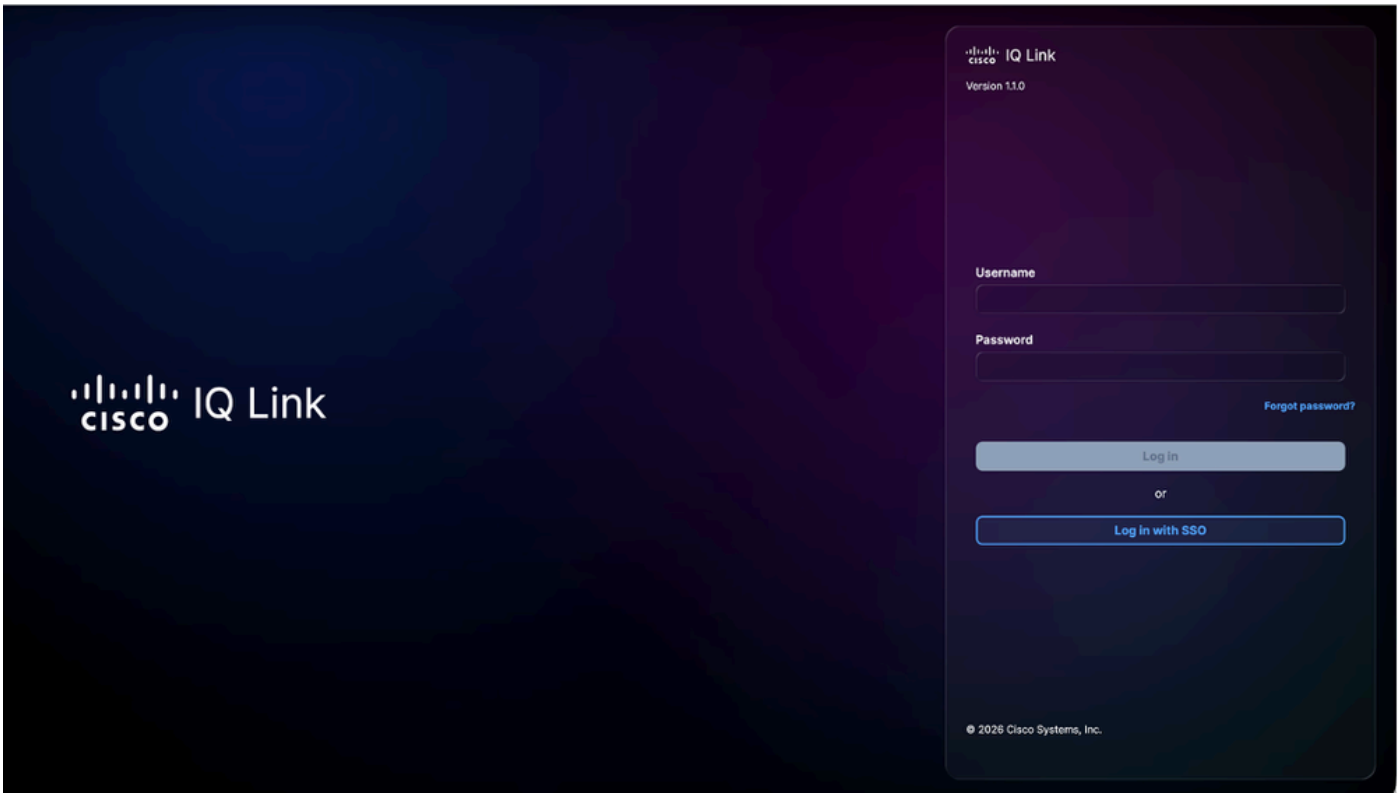
4. Fare clic su Add per aggiungere un nome di dominio configurato dal collegamento Cisco IQ al campo Domini.

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 Salva.

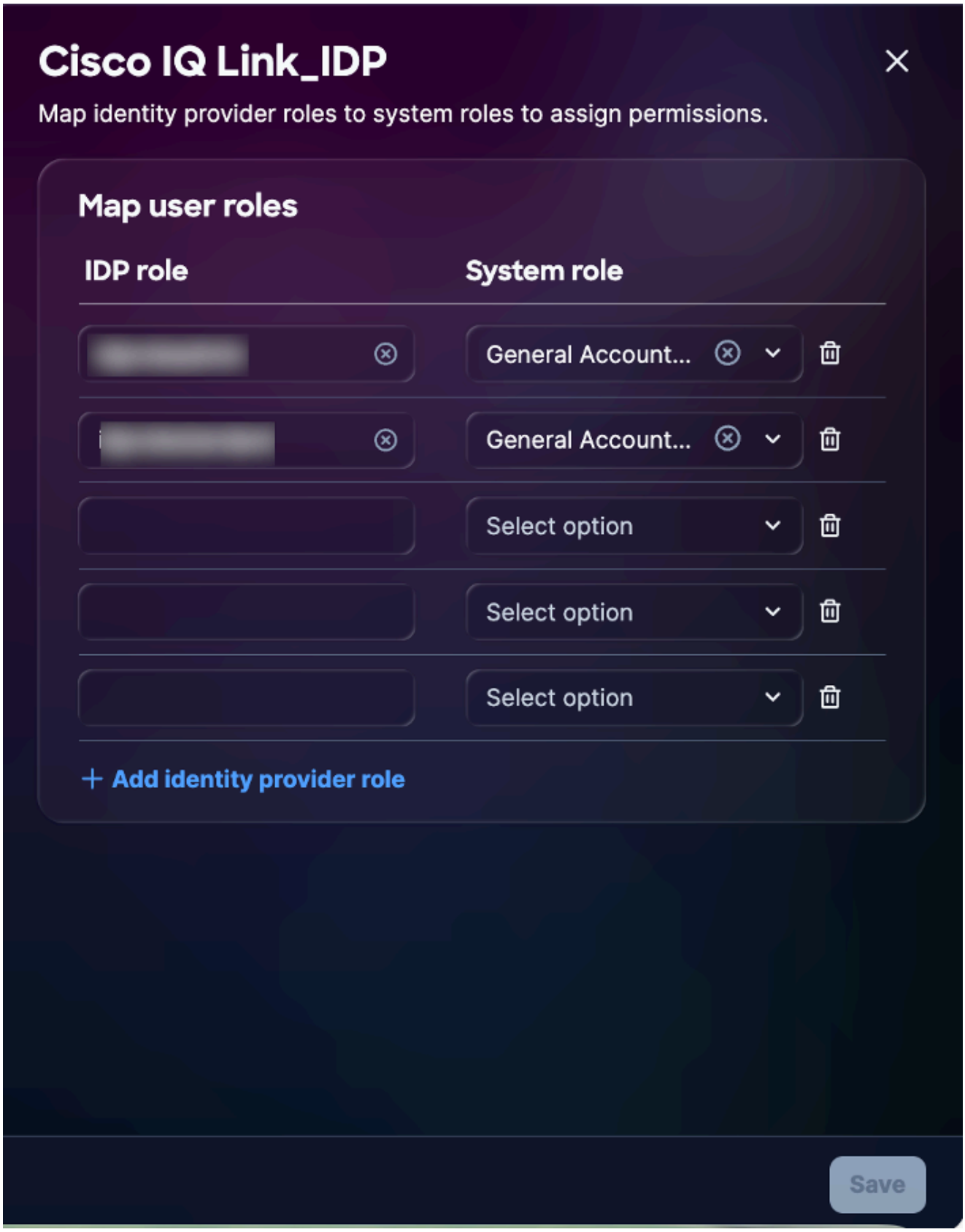
Una volta configurata, la pagina di login visualizza un'opzione per eseguire il login con SSO (tramite IDP).




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

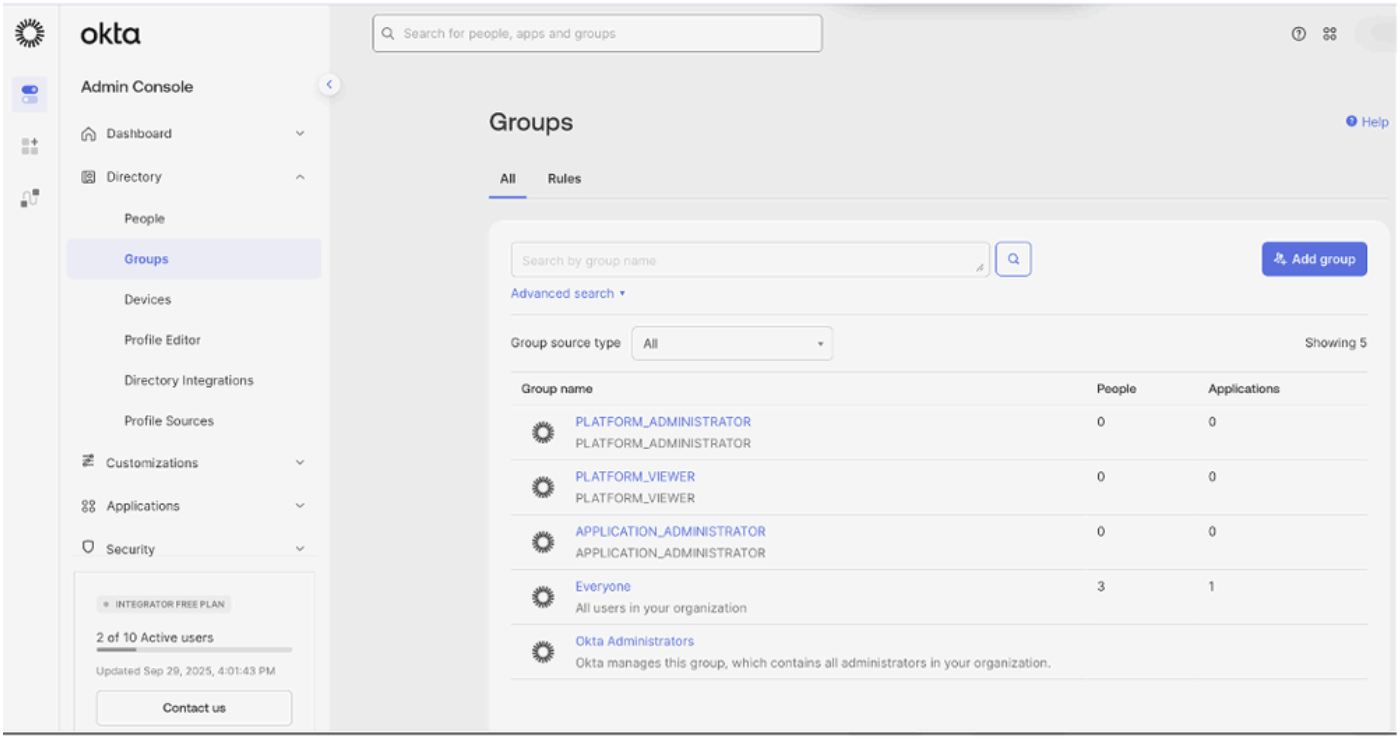
autorizzazioni complete per eseguire tutte le azioni nel prodotto

- Visualizzatore account generale: Il Visualizzatore 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 come richiesto facendo clic su Aggiungi ruolo provider di identità.

4. Fare clic su Salva.

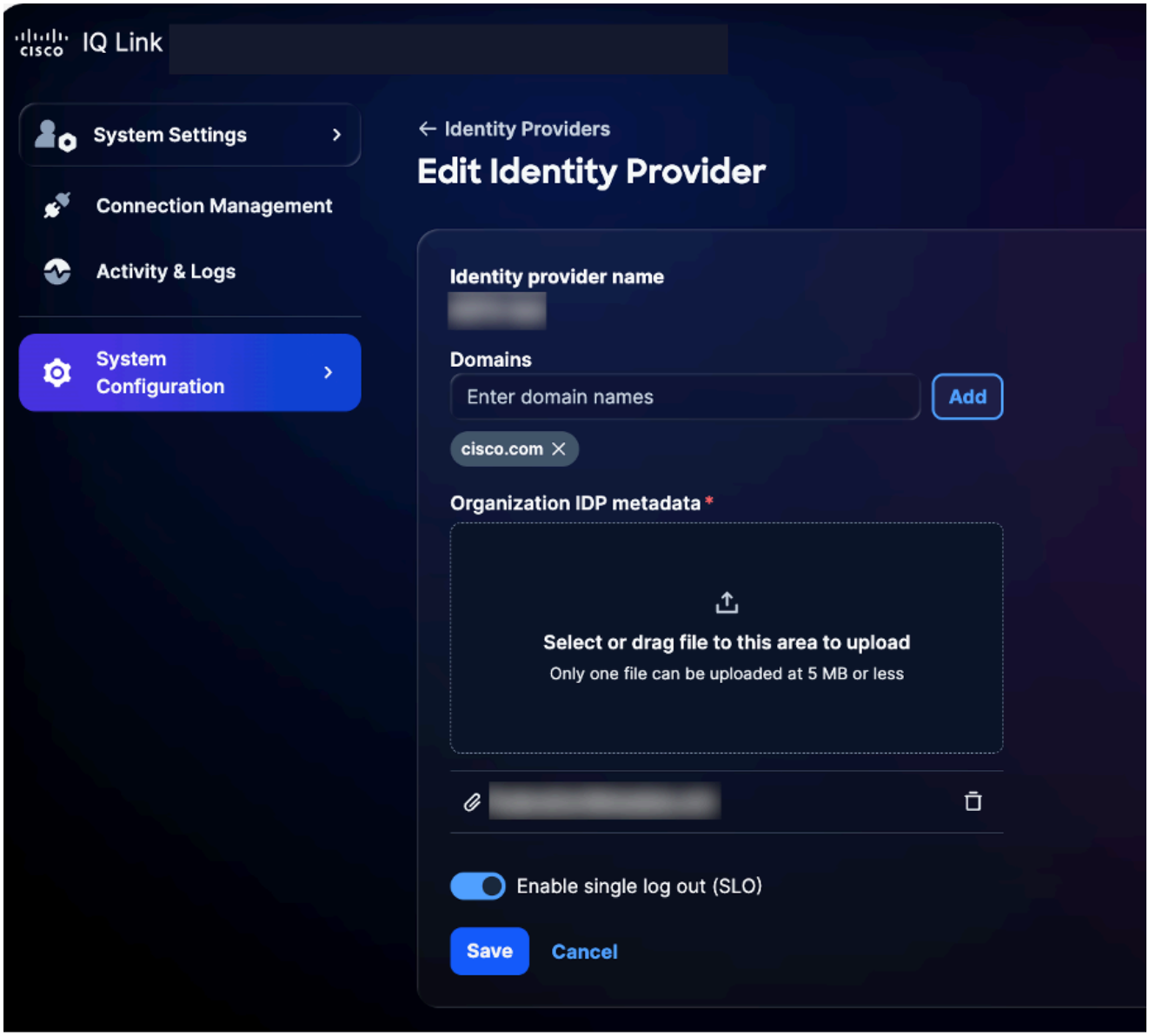
Configurazione disconnessione singola

Se si sceglie di abilitare la configurazione SLO (Single Logout Configuration), 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 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.



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 dell'account 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:

Tabella 4. 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 (AD) 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 AD configurata
- Certificati SSL/TLS (Transport Layer Security) su ADFS
- Accesso come amministratore di account 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)

Tabella 5. 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 AD | 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 per ottenere i dettagli dal file salvato come parte del passaggio 3.
10. Fare clic su Sfoglia per selezionare il file di metadati SP 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.

---

Nota: Non selezionare "Autorizza tutti con MFA" a meno che nel server ADFS non sia stata configurata una scheda Multi-Factor Authentication (MFA) registrata, ad esempio Azure MFA o *Time-Based One-Time Password (TOTP).
Se questo criterio è abilitato senza un provider MFA configurato, ADFS autentica l'utente ma alla fine nega la richiesta con lo stato urn:oasis:names:tc:SAML:2.0:status:RequestDenied. Poiché la risposta SAML non contiene alcuna asserzione, il plug-in ha esito negativo e

---

segnala un errore di tipo "indirizzo di posta elettronica mancante".

Problema: Viene selezionata l'opzione "Permit Everyone with MFA".

Soluzione temporanea: In PowerShell, controllare il criterio corrente eseguendo il comando seguente.

```
Get-AdfsRelyingPartyTrust -Name “

     ”).AccessControlPolicyName
```

Per impostare "Permit Everyone" (nessun requisito MFA), eseguire il comando seguente:

```
Set-AdfsRelyingPartyTrust -TargetName “

     ” -AccessControlPolicyName “Permit everyone”
```

È inoltre possibile creare l'attendibilità del componente tramite PowerShell:

```
Add-AdfsRelyingPartyTrust `
    -Name “

     ” `
    -Identifier “

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

        ”) `
    -AccessControlPolicyName “Permit everyone” `
    -IssuanceAuthorizationRules ’=> issue(Type = “http://schemas.microsoft.com/authorization/claims/per
```

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.

Tabella 6. Richieste di rimborso necessarie

| Richiesta di rimborso | Scopo | Origine |
|---|---|---|
| Email | Identificatore utente | Posta elettronica |
| Nome visualizzato | Nome completo dell'utente | Nome visualizzato AD |
| UPN | Infrastruttura a chiave pubblica (PKI)/autenticazione certificato | ADFS mappa il certificato client a un utente AD tramite il nome dell'entità utente (UPN) |
| 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.Iss

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

3. Applicare le regole attestazione eseguendo il seguente comando:

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

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

---

Avviso: Per ogni account utente di Active Directory è necessario che l'attributo mail sia compilato. Se questo attributo è mancante, l'asserzione SAML non contiene un'attestazione basata su posta elettronica, con conseguente rifiuto dell'autenticazione.

---

Per aggiornare l'indirizzo di posta elettronica di un utente, eseguire il comando di PowerShell seguente:

```
Set-ADUser -Identity “

     ” -EmailAddress “

      ”
```

Verifica dei gruppi di utenti

1. Impostare il nome utente per controllare l'appartenenza al gruppo dell'utente.

```
$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
```

Configurazione di 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 seguenti opzioni:

---

Nota: Il certificato SP è rilasciato da un'autorità di certificazione (CA) 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

- Se il certificato SP è rilasciato da una CA (non autofirmato), importare il certificato CA emittente nell'archivio certificati radice:

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

3. Applicare le modifiche riavviando il servizio ADFS.

```
Restart-Service adfssrv
```

## Impostazione dell'autenticazione PKI/certificato

In questa sezione viene descritto come aggiungere l'autenticazione basata su certificato, ovvero un certificato di smart card o software, insieme alle password. Questa sezione può essere ignorata se è sufficiente l'autenticazione basata solo su password.

### Installazione del ruolo CA di Servizi certificati Active Directory

Per installare il ruolo CA Servizi certificati Active Directory:

1. Verificare se nel dominio esiste già una CA dell'organizzazione (Enterprise) eseguendo il comando seguente:

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

Se il comando restituisce una risposta valida, è possibile ignorare la parte restante di questa sezione. L'ambiente è già configurato. Se il comando indica che non è stata trovata alcuna CA, andare al passaggio 2.

2. Installare il ruolo CA eseguendo il comando seguente:

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

3. Configurare il ruolo CA eseguendo il comando seguente:

```
Install-AdcsCertificationAuthority `
    -CAType EnterpriseRootCA `
    -CACommonName “


     ” `
    -KeyLength 2048 `
    -HashAlgorithmName SHA256 `
    -CryptoProviderName “RSA#Microsoft Software Key Storage Provider” `
    -ValidityPeriod Years `
    -ValidityPeriodUnits 10 `
    -Force
```

4. Installazione mediante il seguente comando:

```
certutil -ca
```

5. Verificare che il servizio sia attivo e raggiungibile eseguendo il comando seguente:

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

Configurazione di un modello di certificato

Per configurare un modello di certificato con l'utilizzo chiavi avanzato per l'autenticazione client:

1. Aprire certsrv.msc ed espandere il nodo CA.
2. Fare clic con il pulsante destro del mouse su Modelli di certificato > Gestisci.
3. Duplicare il modello User.

Nota: Il modello predefinito Utente funziona o è valido solo se il certificato emesso da include l'utilizzo chiavi avanzato per l'autenticazione client.

4. Configurare le impostazioni nelle schede seguenti:

- Informazioni generali: Immettere "CIQ Autenticazione utente" nel campo Nome con un periodo di validità di un (1) anno
- Gestione richieste: Selezionare Firma e crittografia dall'elenco a discesa Scopo e selezionare la casella di controllo Consenti esportazione chiave privata
- Nome soggetto: Selezionare Genera da informazioni di Active Directory e includere un messaggio di posta elettronica nei campi Oggetto e SAN

Avviso: I campi Subject e SAN devono contenere un UPN dell'utente o un messaggio di posta elettronica corrispondente a un account AD. ADFS mappa il certificato a un utente AD utilizzando questi campi.

- Interni: Verificare che i criteri dell'applicazione includano "Autenticazione client (1.3.6.1.5.5.7.3.2)"
- Security: Aggiungere utenti di dominio e concedere loro autorizzazioni di lettura e registrazione

5. Pubblicare il modello utilizzando il seguente comando:

```
Add-CATemplate -Name “CIQUserAuthentication” -Force
```

Registrazione di un certificato utente

1. Eseguire il login come utente di destinazione.
2. Registrare il certificato eseguendo il comando seguente:

```
certreq -enroll -user “CIQUserAuthentication”
```

3. Verificare l'installazione del certificato eseguendo il seguente comando:

```
Get-ChildItem Cert:| Where-Object {
    $_.EnhancedKeyUsageList.ObjectId -contains “1.3.6.1.5.5.7.3.2”
} | Format-Table Subject, Thumbprint, NotAfter -AutoSize
```

Esportazione di un certificato utente da Windows e installazione sul client (Mac)

Per esportare un certificato utente da Windows a Mac:

1. Esportare il certificato da Windows come file PFX eseguendo i comandi seguenti:

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

     *” }

$password = ConvertTo-SecureString -String “

      ” -Force -AsPlainText

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

2. Trasferire il file user-cert.pfx sul dispositivo Mac.

3. Importare il certificato nel portachiavi Mac eseguendo il seguente comando:

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

     ”
```

Nota: Dopo aver importato il certificato, è necessario chiudere e riaprire il browser per poterlo riconoscere.

4. Affidarsi alla CA su Mac eseguendo:

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

Abilitazione degli endpoint di autenticazione dei certificati ADFS

Per abilitare gli endpoint di autenticazione dei certificati ADFS:

1. Abilitare gli endpoint del certificato ADFS richiesti eseguendo i comandi seguenti:

```
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificate

Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificatetransport

Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificate

Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificatetransport
```

2. Verificare che tutti gli endpoint siano abilitati eseguendo il comando seguente:

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

Format-Table AddressPath, Enabled, Proxy -AutoSize
```

Abilitazione dell'autenticazione del certificato come principale

Per abilitare l'autenticazione certificato come principale:

1. Configurare i provider di autenticazione primari per l'accesso alla rete Intranet ed Extranet utilizzando il comando seguente:

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

2. Verificare che entrambi gli elenchi includano CertificateAuthentication e FormsAuthentication utilizzando i seguenti comandi:

```
(Get-AdfsGlobalAuthenticationPolicy).PrimaryIntranetAuthenticationProvider

(Get-AdfsGlobalAuthenticationPolicy).PrimaryExtranetAuthenticationProvider
```

3. Controllare la configurazione corrente della porta del client TLS utilizzando il seguente comando:

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

4. Se TlsClientPort non è 49443, aggiornare la porta e riavviare il servizio ADFS utilizzando i comandi seguenti:

```
Set-AdfsProperties -TlsClientPort 49443

Restart-Service adfssrv
```

Correzioni SChannel/TLS (CRITICHE per PKI)

La procedura descritta nelle sezioni seguenti consente di risolvere gli errori CERT_E_UNTRUSTEDROOT (0x800B0109) che impediscono il funzionamento dell'autenticazione dei certificati.

Binding dei certificati SSL sulla porta 49443

Per associare i certificati SSL alla porta 49443:

1. Rimuovere gli eventuali binding a certificati SSL esistenti sulla porta 49443 utilizzando il comando seguente:

```
netsh http delete sslcert hostnameport=

    :49443
```

2. Creare un nuovo binding con la negoziazione dei certificati client abilitata utilizzando il comando

seguente:

```
netsh http add sslcert hostnameport=

     :49443 `
    certhash=

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

3. Verificare che la negoziazione dei certificati client sia abilitata utilizzando il comando seguente:

```
netsh http show sslcert hostnameport=

     :49443
```

Pulizia dell'archivio certificati (CRITICAL)

Per pulire l'archivio certificati:

Avviso: Windows SChannel rifiuta tutti i certificati client se nell'archivio radice attendibile sono presenti certificati non autofirmati. Questa è la causa principale degli errori di PKI.

1. Identificare i certificati non autofirmati nell'archivio radice attendibile eseguendo il comando seguente:

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

2. Spostare questi certificati nell'archivio CA intermedio eseguendo il comando seguente:

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

3. Verificare che nell'archivio radice non rimangano certificati non autofirmati eseguendo il comando seguente:

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

Correzioni al Registro di sistema SChannel (CRITICAL)

Per configurare le impostazioni del Registro di sistema di SChannel in modo da garantire la corretta autenticazione dei certificati:

1. Definire la variabile del percorso del Registro di sistema utilizzando il comando seguente:

```
$regPath = “HKLM:”
```

2. Applicare le impostazioni del Registro di sistema definite nella tabella seguente utilizzando i comandi seguenti:

```
Set-ItemProperty -Path $regPath -Name “ClientAuthTrustMode” -Value 2 -Type DWord

Set-ItemProperty -Path $regPath -Name “SendTrustedIssuerList” -Value 0 -Type DWord
```

Tabella 7. Impostazioni del Registro di sistema di Schannel

| Impostazione | Valore | Scopo |
|---|---|---|
| ModalitàAttendibilitàAutenticazioneClient | 2 | Abilita il trust CA esclusivo per correggere il percorso di convalida predefinito. |
| InviaElencoEmittentiAttendibili | 0 | Impedisce al server di inviare l'elenco completo degli emittenti attendibili durante l'handshake TLS. |

Verifica dell'archivio certificati CA

Per verificare l'archivio certificati CA:

---

Nota: Il certificato CA che rilascia i certificati utente deve trovarsi nell'archivio SystemCertificatesstore per garantire che venga riconosciuto correttamente.

---

1. Definire l'identificazione personale del certificato CA utilizzando il comando seguente:

```
$caThumbprint = “

    ”
```

2. Verificare che il certificato CA sia già presente in LocalMachinestore utilizzando il comando seguente:

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

Se il certificato non viene trovato, importarlo in LocalMachinestore:

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

Riavvio del server ADFS (OBBLIGATORIO)

Riavviare il server ADFS utilizzando il comando seguente:

```
Restart-Computer -Force
```

---

Nota: La modifica del Registro di sistema ClientAuthTrustMode ha effetto solo dopo il riavvio del server.

---

## 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.

## Configurazione su Cisco IQ

Per configurare su Cisco IQ:

1. Trasferire adfs-metadata.xml nella workstation.
2. In Cisco IQ, selezionare System Settings > System Configuration > Identity Providers (Impostazioni di sistema > Configurazione sistema > Provider di identità).
3. Caricare il file di metadati ADFS per estrarre automaticamente il certificato IDP, l'ID entità e l'URL SSO.

4. Salvare la configurazione.

---

Nota: Se ADFS esegue il rollover automatico del certificato per la firma di token, è necessario riesportare il file di metadati e caricarlo in Cisco IQ per garantire la continuità dell'autenticazione.

---

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 Abilita 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 di poter trovare i gruppi da AD 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”] }
```

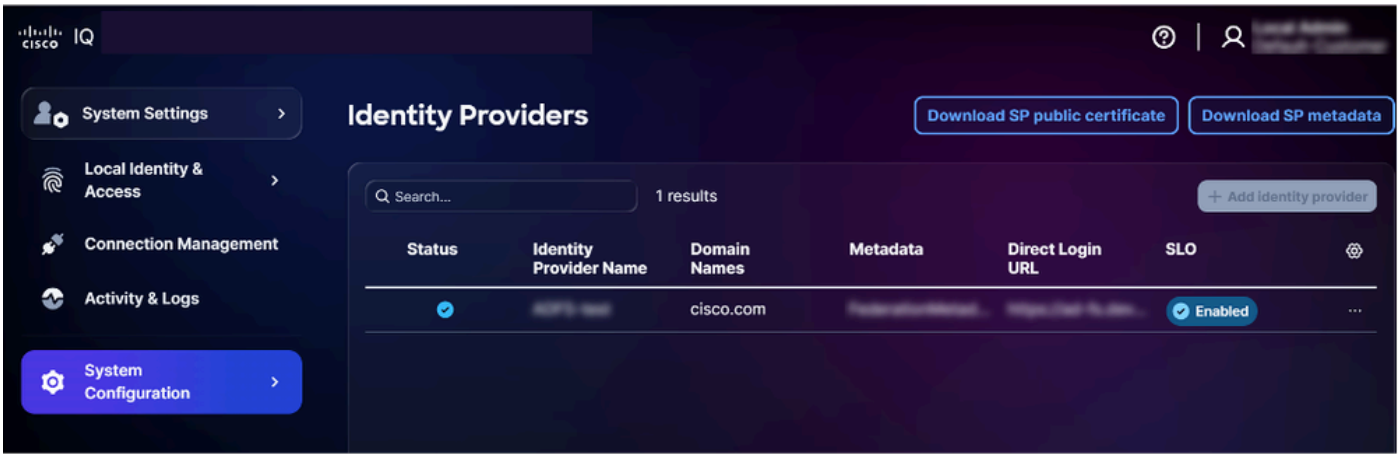
Il sistema esegue query su Active Directory direttamente tramite il protocollo LDAP (Lightweight Directory Access Protocol), senza richiedere moduli aggiuntivi. Le informazioni sul gruppo vengono restituite nel formato Nome distinto completo, ad esempio:

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

Visualizzatori CXIQ,OU=Gruppi,DC=dev,DC=esempio,DC=com

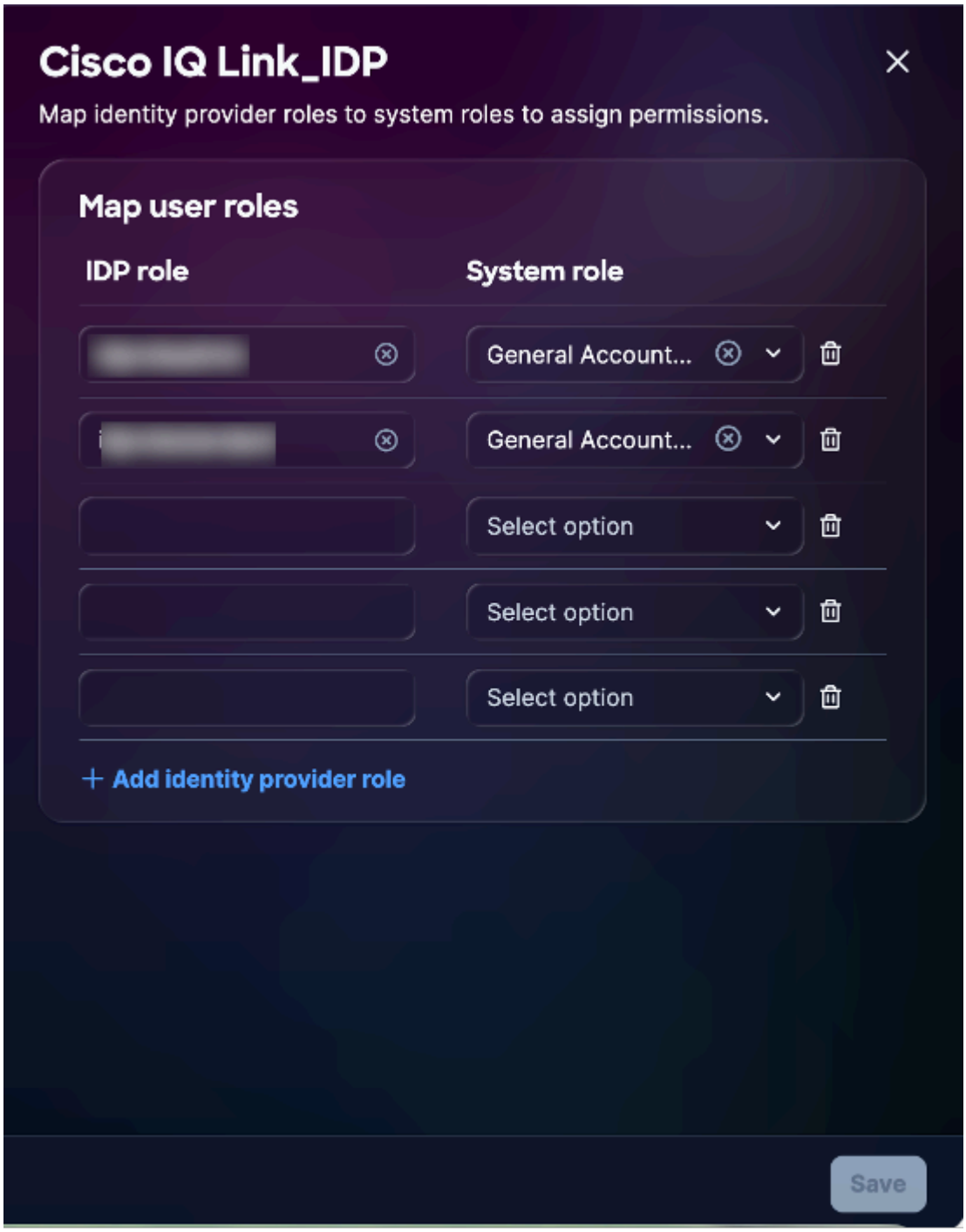
Se i gruppi richiesti non sono elencati, è necessario crearli in AD da un amministratore account prima di poter completare il mapping dei ruoli ADFS.

Per configurare il mapping dei ruoli:




Mapping 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.
- Visualizzatore account generale: Il Visualizzatore 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 Salva. Lo stato viene aggiornato a Operazione riuscita.

Test certificato client SChannel

Per verificare che SChannel sia configurato correttamente per accettare i certificati client, aprire una nuova finestra di PowerShell ed eseguire il comando seguente:

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


     :49443/adfs/ls/"
```

L'output previsto è una risposta HTTP, ad esempio un reindirizzamento o la pagina ADFS. Se si verifica un errore di handshake TLS, la connessione non è riuscita.

Test completo del browser per il flusso PKI

Prima di iniziare il test completo del browser per il flusso PKI, verificare che il certificato utente sia installato nel portachiavi macOS (per ulteriori informazioni, vedere Importazione del certificato utente sul computer client (macOS) in Configurazione dell'autenticazione basata su certificato).

Per provare:

1. Passare all'URL di accesso SAML applicazione. L'ADFS presenta le opzioni relative al certificato e alla password.
2. Scegliere Autenticazione certificato. Il browser richiede il certificato.
3. Caricare il certificato. ADFS autentica l'utente, reindirizza la richiesta con una risposta SAML e stabilisce una nuova sessione.

Test completo del browser per il flusso delle password

Prima di iniziare il test end-to-end del browser per il flusso di password:

1. Passare all'URL di accesso SAML applicazione. L'ADFS presenta le opzioni relative al certificato e alla password.
2. Selezionare Autenticazione password/moduli.
3. Immettere il nome utente.
4. Immettere la password.
5. Verificare che l'accesso sia riuscito.

---

Nota: Entrambi i flussi devono funzionare contemporaneamente.

---

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.

Tabella 8. 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<br>• Attributo gruppo errato: Deve essere http://schemas.xmlsoap.org/cla ims/Group<br>• 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<br>• Mancata corrispondenza 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
```

## Configurazione SAML di Microsoft Entra ID per SSO

In questa sezione vengono fornite indicazioni per configurare Microsoft Entra ID (Entra ID) come provider di identità SAML per Cisco IQ, in modo da supportare sia l'autenticazione basata su password che l'autenticazione basata su PKI/certificati (CBA).

Prerequisiti per configurare Entra ID SAML per SSO

- Tenant Microsoft Entra ID (ad esempio, "ciqtestdev.onmicrosoft.com")
- Accesso con ruolo Amministratore globale o Amministratore applicazioni a Cisco IQ
- Connettività tra Entra ID (cloud) e Cisco IQ
- CA aziendale installata o raggiungibile (necessaria solo per PKI)
- Punto di distribuzione CRL (Certificate Revocation List) raggiungibile da Internet (richiesto solo per PKI)

Tabella 9. Configurazione server Entra ID

| Articolo | Descrizione | Esempio |
|---|---|---|
| ID tenant | Identificatore tenant ID entrante | 37352d8f-0ebe-4762-8161-8775ffe897cb |
| FQDN Cisco IQ | Nome host distribuzione | <FQDN-CIQ-UTENTE> |
| ID entità IDP | URL autorità emittente ID entrante | https://sts.windows.net/<ID-TENANT>/ |
| URL SSO IDP | Endpoint di accesso SAML | https://login.microsoftonline.com/<ID-TENANT>/saml2 |
| Dominio società | Dominio e-mail per utenti | <DOMINIO-UTENTE> |

Configurazione dell'applicazione SAML Entra ID

Creazione di un'applicazione enterprise

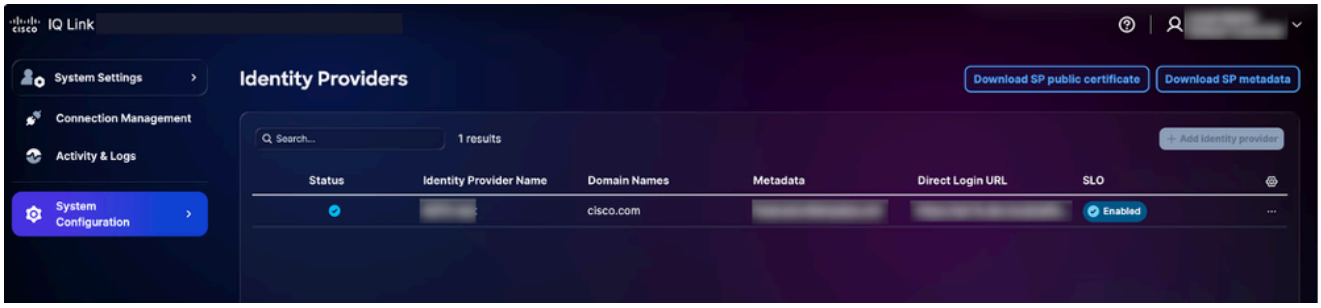
1. Accedere all'interfaccia di amministrazione di Microsoft Entra.
2. Passare a Identità > Applicazioni > Applicazioni aziendali.
3. Fare clic su Nuova applicazione > Crea applicazione personalizzata.
4. Immettere il nome, ad esempio "Cisco IQ".
5. Scegliere Integra qualsiasi altra applicazione non presente nella raccolta (Non-gallery).

6. Fare clic su Crea.

Configurazione di SAML Single Sign-On

Per configurare SAML Single Sign-On, è necessario caricare il file di metadati SP. Per ottenerlo, eseguire la procedura seguente da Virtual Appliance (VA):

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 metadati SP per scaricarli. Questo file di metadati SP scaricato viene caricato per completare la configurazione SAML Single Sign-On.
3. Fare clic sul pulsante Upload Metadata file (Carica file metadati) per caricare il file di metadati SP. Dopo il corretto caricamento, i dati del file di metadati SP verranno inseriti automaticamente nella schermata SAML-Based Single Sign-on.

È inoltre possibile scegliere di immettere manualmente questi dettagli per configurare le impostazioni del servizio Single Sign-on. Per configurare manualmente il servizio Single Sign-on SAML:

1. Nell'applicazione enterprise, passare a Single Sign-On e scegliere SAML.
2. Nella sezione Configurazione SAML di base, fare clic su Modifica e immettere quanto segue:
    a. Identificatore (ID entità): <FQDN-CIQ-UTENTE>
    b. URL risposta (URL ACS): https://<FQDN-CIQ-UTENTE>/saml/acs
    c. URL di accesso: https://<FQDN-CIQ-UTENTE>/saml/login
    d. URL di disconnessione: https://<FQDN-CIQ-UTENTE>/saml/logout
3. Fare clic su Save (Salva).

Nota: L'ID entità deve corrispondere esattamente a quello utilizzato da Cisco IQ come ID entità SP. Si tratta in genere del nome di dominio completo della distribuzione.

4. Per configurare gli attributi e le attestazioni SAML, nella sezione Attributi e attestazioni fare clic su Modifica.

5. Configurare le seguenti attestazioni:

Tabella 10. Attestazioni SAML richieste

| Richiesta di rimborso | Attributo di origine | Spazio dei nomi |
|---|---|---|
| Identificatore utente univoco (NameID) | user.nomeprincipaleutente | (predefinito) |
| indirizzo email | user.mail | http://schemas.xmlsoap.org/ws/2005/05/identity/claims |
| nomedato | user.nomedato | http://schemas.xmlsoap.org/ws/2005/05/identity/claims |
| cognome | user.cognome | http://schemas.xmlsoap.org/ws/2005/05/identity/claims |
| nome | user.nomeprincipaleutente | http://schemas.xmlsoap.org/ws/2005/05/identity/claims |
| gruppi | user.assignedroles | (VUOTO — cancella lo spazio dei nomi) |

Nota: Per l'affermazione dei gruppi:
- Utilizzare user.assignedroles come origine - non utenti.gruppi
- Il campo Namespace deve essere vuoto. In questo modo il nome dell'attributo nell'asserzione SAML è costituito semplicemente da gruppi anziché da un URI (Uniform Resource Identifier) completo
- Non aggiungere un'attestazione basata su gruppo duplicata con user.groups perché ciò causa conflitti

Configurazione dei ruoli applicazione

I ruoli dell'app sono configurati nella registrazione dell'app (non nell'applicazione enterprise); per configurare i ruoli applicazione:

1. Passare a Identità > Applicazioni > Registrazioni app.
2. Individuare e scegliere l'applicazione.
3. Vai a Ruoli app > Crea ruolo app.
4. Per ogni ruolo necessario, configurare quanto segue:

- Nome visualizzato: Ad esempio, Cisco IQ Admins

- Tipi di membro consentiti: Utenti/Gruppi
- Valore: Ad esempio, Cisco IQ Admins
- Descrizione: Ad esempio, Cisco IQ Administrators

5. Fare clic su Applica.

---

Nota: Creare ruoli corrispondenti ai requisiti di mapping dei ruoli Cisco IQ (ad esempio, CXIQ Admins, CXIQ Developers, CXIQ Viewers).

---

I ruoli applicazione vengono utilizzati al posto delle attestazioni basate su gruppo per i motivi seguenti:

- I tenant solo cloud non possono inviare nomi visualizzati di gruppi senza una licenza P1 o P2
- sAMAccountName funziona solo per i gruppi sincronizzati da Active Directory locale
- L'origine ID gruppo invia UUID (Universally Unique Identifier) difficili da mappare
- I ruoli applicazione inviano valori stringa esatti corrispondenti alle aspettative del ruolo Cisco IQ

Assegnazione di utenti ai ruoli applicazione

Per assegnare gli utenti ai ruoli applicazione:

1. Tornare a Applicazione enterprise > Utenti e gruppi.
2. Fare clic su Aggiungi utente/gruppo.
3. Scegliere gli utenti e assegnare il ruolo app appropriato.
4. Fare clic su Assegna. I valori dei ruoli vengono visualizzati come stringhe leggibili nell'attributo dei gruppi di asserzione SAML.

Download di metadati e certificati IDP

Per scaricare i metadati e il certificato IDP:

1. Dall'applicazione Enterprise, passare alla sezione Single Sign-on > Certificato di firma SAML.

2. Scarica XML metadati federazione (salva come entra-id-metadata.xml).

   O

   Scaricare il certificato (Base64) per la voce manuale del certificato.

3. Prendere nota dei seguenti valori dalla sezione Imposta:

- URL di accesso (URL SSO IDP)
- ID entità Azure AD (IDP)
- URL di disconnessione (URL SLO IDP)

---

Nota: Poiché l'ID Entra ruota periodicamente i certificati di firma, è necessario scaricare nuovamente i metadati e caricarli in VA ogni volta che il certificato attivo viene modificato per garantire un servizio SSO ininterrotto.

---

Aggiunta di IDP ID entroide

---

Nota: I percorsi APISIX per SAML vengono creati automaticamente quando si aggiunge un IDP in Cisco IQ, eliminando la necessità di configurare manualmente il percorso.

---

Per aggiungere l'IDP ID Entra:

1. Accedere a VA come amministratore dell'account.
2. Passare a Impostazioni di sistema > Configurazione di sistema > Provider di identità.
3. Fare clic su Aggiungi provider di identità.
4. Immettere il nome dell'IDP (ad esempio, "Entra ID").
5. Immettere i domini (ad esempio, "ciqtestdev.onmicrosoft.com" o il dominio della società).
6. (Facoltativo) Attivare il pulsante Abilita disconnessione singola, se necessario.
7. Trascinare o caricare il file entra-id-metadata.xml ottenuto da Entra ID nel campo Carica metadati IDP.
8. Fare clic su Save (Salva).

---

Nota: Lo stato rimane "Incompleto" fino al completamento del mapping dei ruoli. si tratta di un comportamento previsto.

---

Configurazione del mapping dei ruoli

Per configurare il mapping dei ruoli:

1. Dall'IDP aggiunto, scegliere l'icona Altre opzioni > Mappa ruoli. Viene visualizzata la pagina Mapping ruoli utente.
2. Immettere un ruolo IDP per ogni ruolo di sistema. Sono supportati i seguenti ruoli di sistema:

Tabella 11. Ruoli di sistema

| Ruolo del sistema | Ruolo IDP (valore ruolo applicazione) | Descrizione |
|---|---|---|
| Amministratore account generale | Amministratori CXIQ | Autorizzazioni complete per tutte le azioni |
| Visualizzatore account generale | Sviluppatori CXIQ | Accesso in sola lettura |
| Visualizzatore account generale | Visualizzatori CXIQ | Accesso in sola lettura |

Nota: Utilizzare le stringhe dei valori del ruolo app esattamente come configurato in Entra ID (per ulteriori informazioni, vedere Configurazione dei ruoli app in Configurazione dell'applicazione SAML Entra ID).

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

Verifica del flusso SAML (autenticazione password)

Per verificare il flusso SAML:

1. Aprire un browser in modalità Incognito o Private.
2. Accedere a https://<YOUR-CIQ-FQDN>/saml/login.
3. Verificare di essere reindirizzati alla pagina di accesso Microsoft.
4. Eseguire l'autenticazione con le credenziali (e con l'autenticazione a più fattori, se configurata).
5. Dopo l'autenticazione, verificare di essere reindirizzati a /saml/acs e che venga visualizzata l'applicazione Cisco IQ.

6. Verificare l'estrazione dei gruppi eseguendo il comando seguente:

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

Output previsto

```
SAML 2.0 compliant authentication successful for user: user@domain.com with full name: N/A and 1 groups
Extracted group: CXIQ Admins (original: CXIQ Admins)
Total groups extracted: 1
```

Configurazione dell'autenticazione basata su certificati

In questa sezione viene descritto come aggiungere CBA insieme alle password. Questa sezione può essere ignorata se è sufficiente l'autenticazione basata solo su password.

Prerequisiti per l'analisi costi/benefici

- Windows Server con Servizi certificati Active Directory con CA Enterprise configurata (ad esempio, "DEV-ADCS-CA")
- Accesso come amministratore di PowerShell sul server CA
- L'UPN del certificato deve corrispondere all'ID Entra userPrincipalName
- Il punto di distribuzione CRL deve essere accessibile da Internet

Creazione di un modello di certificato in Servizi certificati Active Directory

1. Aprire certtmpl.msc sul server CA.
2. Duplicare il modello User e denominarlo "EntraUserCert".
3. Configurare il modello:

- Informazioni generali: Nome visualizzato EntraUserCert, validità 1-2 anni
- Gestione richieste: Scopo = Firma e crittografia
- Nome soggetto: Selezionare Fornitura nella richiesta

- Interni: I criteri dell'applicazione devono includere l'autenticazione client (1.3.6.1.5.5.7.3.2)
- Security: Concedi autorizzazioni di lettura e registrazione a utenti autenticati

4. Pubblicare il modello utilizzando il comando seguente:

```
Add-CATemplate -Name “EntraUserCert” -Force
```

Richiesta e rilascio di un certificato utente

1. Creare un file di configurazione del certificato (INF), ad esempio C:-cert.inf, utilizzando lo script di PowerShell seguente:

```
@”
[Version]
Signature = “`$Windows NT`$”

[NewRequest]
Subject = “CN=



     ”
KeyLength = 2048
KeySpec = 1
KeyUsage = 0xa0
MachineKeySet = FALSE
ProviderName = “Microsoft RSA SChannel Cryptographic Provider”
RequestType = PKCS10

[RequestAttributes]
CertificateTemplate = EntraUserCert

[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.2
OID = 1.3.6.1.4.1.311.20.2.2

[Extensions]
2.5.29.17 = “{text}”
_continue_ = “upn=



      &”
_continue_ = “email=



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

2. Sostituire <USER-UPN> con l'UPN Entra ID, ad esempio user@ciqtestdev.onmicrosoft.com.

3. Per generare il certificato, eseguire il seguente comando:

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

4. Per inviare la richiesta alla CA, eseguire il comando seguente:

```
certreq -submit -config “

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

5. Per installare il certificato nella CA, eseguire il comando seguente:

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

Esportazione dei certificati

- Per esportare il certificato utente come file PFX (per client), eseguire lo script seguente:

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

     *” }
$password = ConvertTo-SecureString -String “

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

- Per esportare il certificato radice CA (per Entra ID), eseguire lo script seguente:

```
Get-ChildItem Cert:| Where-Object { $_.Subject -like “*

     *” } |
Select-Object -First 1 | Export-Certificate -FilePath C:-root.cer -Type CERT
```

Importazione del certificato utente sul computer client (macOS)

- Per importare il certificato utente (PFX), eseguire il comando seguente:

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

     ”
```

- Per importare il certificato radice CA, eseguire il comando seguente:

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

- Per impostare il certificato CA su Considera sempre attendibile l'accesso al portachiavi:
    1. Aprire Keychain Access.
    2. Individuare il certificato CA e fare clic su Get Info (Ottieni informazioni).
    3. In Trust (Attendibilità), impostare su "Always Trust" (Sempre attendibile).

---

Nota: Dopo l'importazione, uscire e riaprire il browser per il riconoscimento del certificato.

---

### Caricamento del certificato radice CA nell'ID Entra

1. Accedere all'interfaccia di amministrazione di Microsoft Entra.
2. Passare a Protezione > Protezione > Autorità di certificazione.
3. Fare clic su Upload e selezionare il file ca-root.cer.
4. Contrassegnarlo come certificato CA radice.
5. Immettere l'URL del punto di distribuzione CRL (deve essere raggiungibile pubblicamente).

### Abilitazione di CBA nei metodi di autenticazione Entra ID

1. Passare a Protezione > Metodi di autenticazione > Criteri.
2. Fare clic su Autenticazione basata su certificati per configurare.
3. Abilitare l'analisi costi/benefici e aggiungere gli utenti o i gruppi target.
4. In Configura impostare il livello di protezione su Autenticazione a fattore singolo.

### Configurazione dell'associazione del nome utente

Nella configurazione CBA, andare alla scheda Binding nome utente e impostare il binding seguente:

- Campo certificato: NomePrincipale
- Attributo utente: NomePrincipaleUtente

In questo modo l'UPN nel nome alternativo soggetto del certificato viene mappato all'utente Entra ID.

### Verifica del flusso CBA

1. Aprire un browser in modalità Incognito o Private.
2. Accedere a https://<YOUR-CIQ-FQDN>/saml/login.
3. Nella pagina di accesso a Microsoft, immettere l'e-mail dell'utente e fare clic su Avanti.
4. Scegliere Usa un certificato o una smart card (o potrebbe essere richiesta

automaticamente).

5. Scegliere il certificato utente applicabile quando il browser richiede la selezione del certificato.
6. Verificare che Entra ID convalidi il certificato, reindirizzi con una risposta SAML e crei una sessione.

---

Nota: Verificare di aver selezionato il certificato client corretto. Se si seleziona un certificato errato, ad esempio un certificato di un altro utente o un certificato scaduto, si verifica un errore di autenticazione.

---

Risoluzione dei problemi relativi agli ID interni

L'elenco seguente descrive i problemi comuni e le possibili soluzioni per identificare e risolvere rapidamente i problemi relativi alla configurazione SAML Entra ID.

Tabella 12. Risoluzione dei problemi

| Problema | Causa | Fix |
|---|---|---|
| Risposta SAML non valida - indirizzo di posta elettronica mancante | Asserzione SAML senza attributo NameID o email | Verificare la configurazione delle attestazioni Entra ID (per ulteriori informazioni, vedere Configurazione di SAML Single Sign-On in Configurazione dell'applicazione SAML Entra ID). Verificare che l'attributo di posta dell'utente sia compilato. |
| Totale gruppi estratti: 0 | Attestazioni basate su gruppo non configurate o origine errata | Utilizzate user.assignedroles come origine. Assicurarsi che l'utente sia assegnato a un ruolo applicazione (per ulteriori informazioni, vedere Assegnazione di utenti ai ruoli applicazione in Configurazione dell'applicazione SAML Entra ID). |
| Attestazioni di gruppo duplicate | Sia user.groups che user.assignedroles attivi | Rimuovere l'attestazione user.groups. Mantieni solo user.assignedroles. |
| Gruppi visualizzati come UUID | L'attributo di origine è "ID gruppo" | Utilizzare l'approccio Ruoli applicazione (per ulteriori informazioni, vedere Configurazione dei ruoli applicazione in Configurazione dell'applicazione SAML Entra ID). |
| Il nome dell'attributo mostra l'URI lungo | Il campo dello spazio dei nomi non è vuoto | Cancellare il campo Spazio dei nomi nelle impostazioni delle attestazioni basate su gruppi. |
| Firma SAML non valida | Certificato IdP ruotato o non corrispondente | Scaricare nuovamente i metadati da Entra ID e caricarli nuovamente in Cisco IQ. |

| Problema | Causa | Fix |
|---|---|---|
| ADSTS500191 | CRL non raggiungibile da Internet | Pubblicare il CRL su un URL accessibile pubblicamente o utilizzare un approccio CA autofirmato (per ulteriori informazioni, vedere Soluzione CRL per ambienti lab). |
| Certificato non richiesto | Certificato non incluso in portachiavi, CA non attendibile nel client o CBA non abilitato | Verificare che il certificato utente sia stato importato in macOS Keychain Access (vedere Importazione del certificato utente sul computer client (macOS) in Configurazione dell'autenticazione basata su certificato per ulteriori dettagli), CBA è abilitato in Entra ID con le impostazioni richieste (vedere Abilitazione di CBA in Metodi di autenticazione Entra ID in Configurazione dell'autenticazione basata su certificato per ulteriori dettagli) e Chrome è stato riavviato per applicare le modifiche. |
| Asserzione SAML scaduta | Distanza di clock tra i sistemi | Aumentare clock_skew_seconds nella configurazione del plug-in (il valore predefinito è 300, utilizzare 30000 per lab). |
| Stato "Incompleto" in VA | Mapping ruoli non ancora configurato | Completare il mapping dei ruoli (per ulteriori informazioni, vedere Configurazione del mapping dei ruoli). |

Soluzione CRL per i problemi di raggiungibilità

Se il punto di distribuzione CRL della CA non è raggiungibile da Internet (comune nelle impostazioni di laboratorio), utilizzare una CA autofirmata senza requisiti CRL:

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

# Create user cert signed by the CA
$userCert = New-SelfSignedCertificate `
    -Subject “CN=



     ” `
    -CertStoreLocation “Cert:” `
    -Signer $rootCA `
    -KeyUsage DigitalSignature `
    -KeyLength 2048 `
```

```
    -NotAfter (Get-Date).AddYears(2) `
    -TextExtension @(
        “2.5.29.37={text}1.3.6.1.5.5.7.3.2”,
        “2.5.29.17={text}upn=



      &email=



       ”
)
```

Caricare solo il certificato CA radice in Entra ID. Poiché è autofirmato senza CDP, Entra ID non tenta la convalida CRL.

Elenco di controllo per il completamento dell'installazione

In questa sezione viene descritto un elenco di controllo completo per la configurazione di VA con Microsoft Entra ID SAML Application e CBA opzionale.

Impostazione applicazione SAML ID voce

- Crea applicazione enterprise (non raccolta) in Entra ID
- Configurare la configurazione SAML di base immettendo manualmente i metadati SP
- Configurazione di attributi e attestazioni (inclusi e-mail, nome e gruppi con user.assignedroles)
- Crea ruoli app nella registrazione app
- Assegna utenti a ruoli applicazione
- Scarica XML metadati federazione

Configurazione Cisco IQ

- Aggiunta di un provider di identità in Cisco IQ tramite il caricamento di metadati Entra ID

- Configura mapping ruoli per mappare i valori del ruolo applicazione ai ruoli di sistema Cisco IQ
- Verifica completa del funzionamento dell'accesso basato su password
- Verificare che i gruppi siano estratti correttamente nei registri

Autenticazione basata su certificati (facoltativa)

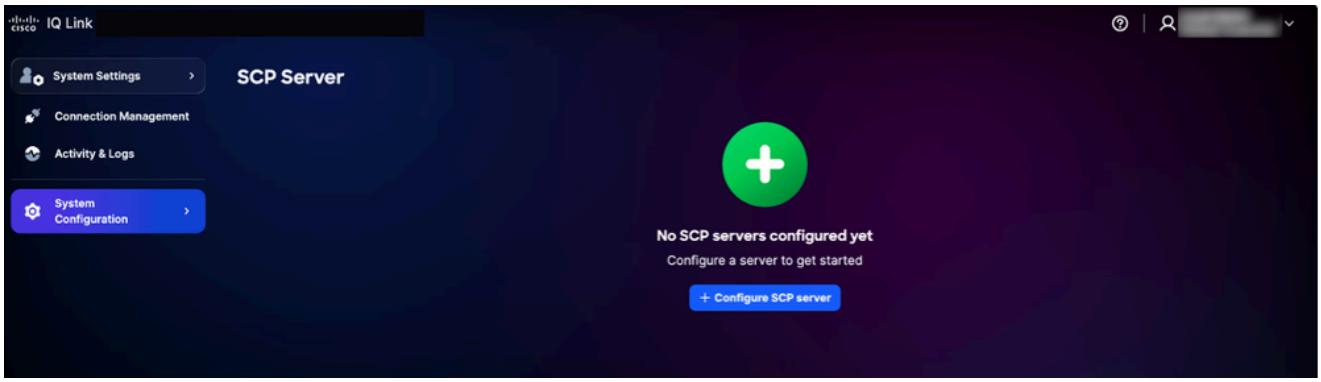
- Crea modello di certificato in Servizi certificati Active Directory con utilizzo chiavi avanzato di autenticazione client
- Rilascia certificato utente con UPN corrispondente all'utente Entra ID
- Esporta certificato utente come PFX e installa nel computer client
- Considera attendibile il certificato CA nel computer client
- Carica il certificato radice CA nell'ID Entra in Protezione > Autorità di certificazione
- Abilita CBA nei metodi di autenticazione
- Configura associazione nome utente (PrincipalName e userPrincipalName)
- Verifica completa del funzionamento dell'accesso CBA

# 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 l'applicazione di patch nell'installazione di Cisco IQ.

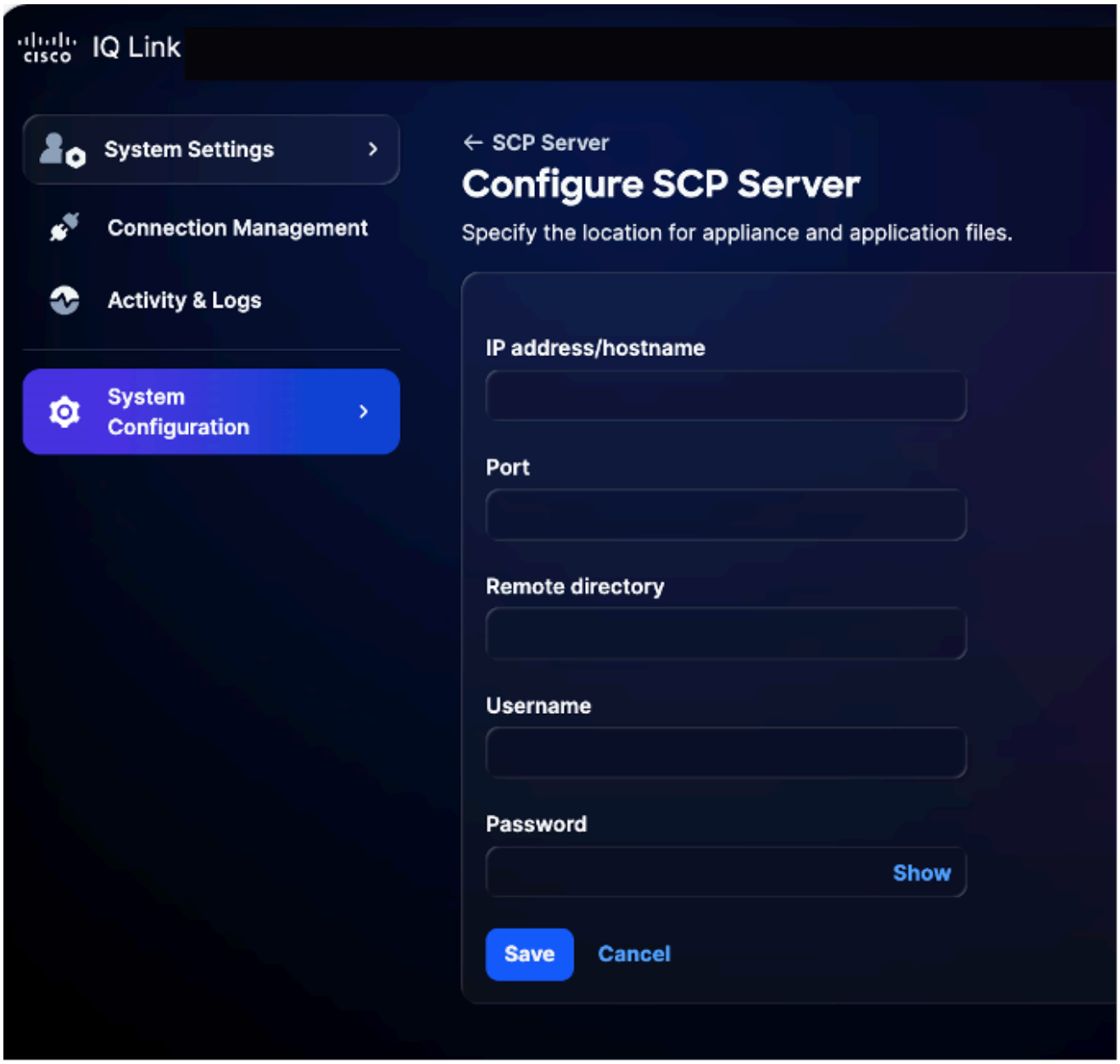
Per aggiungere un server SCP:

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.

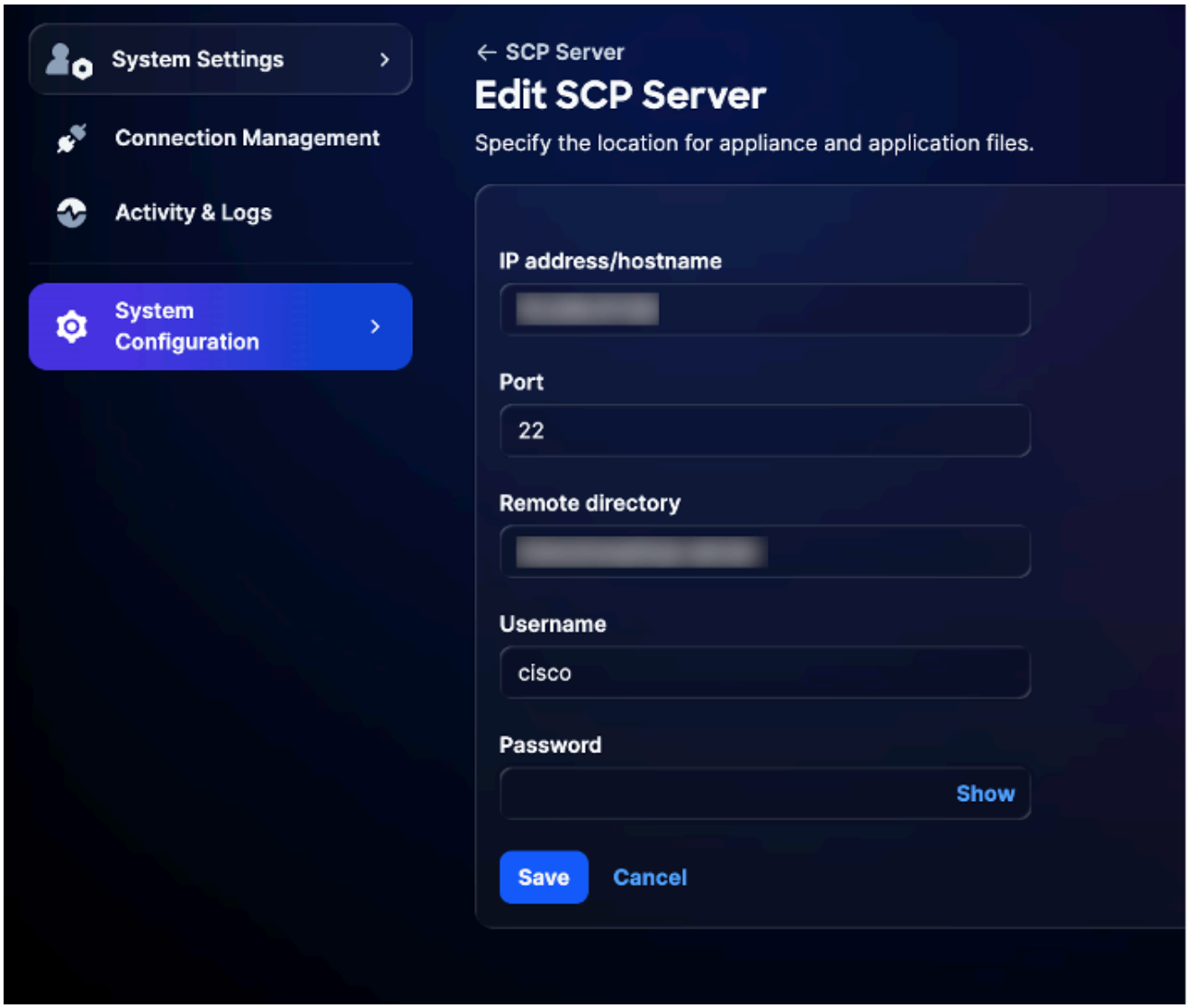
## Modifica di server SCP esistenti

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

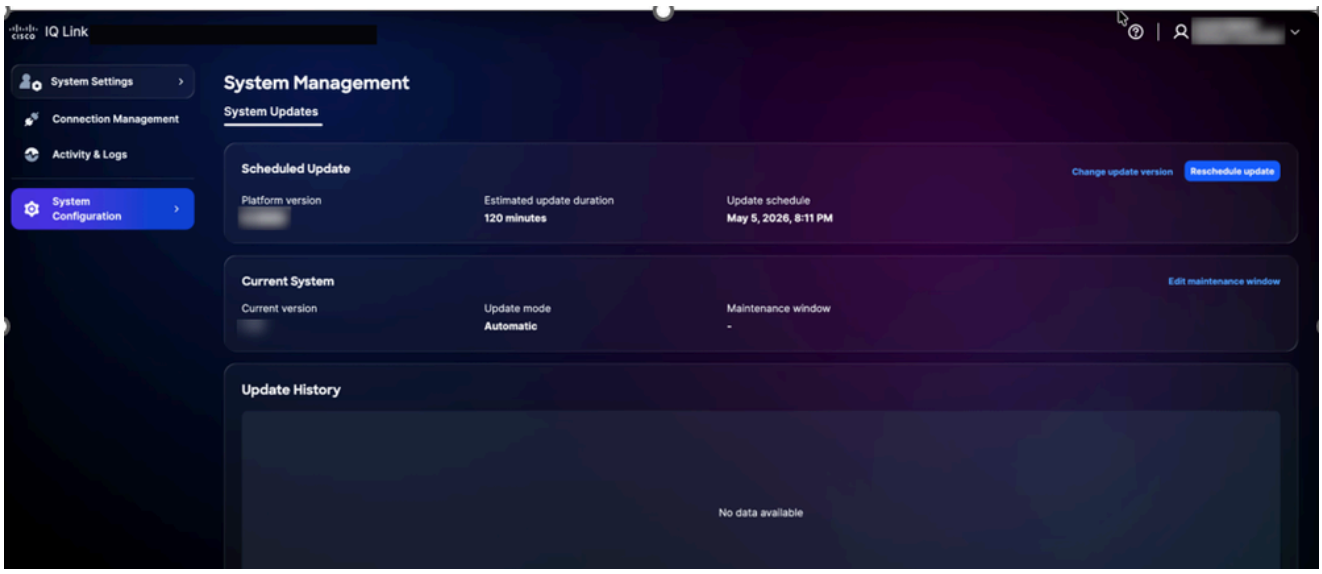
È possibile eseguire l'aggiornamento all'ultima versione di Cisco IQ Link tramite l'interfaccia utente. La verifica può essere effettuata anche dalla pagina Cisco IQ Data Connectors.

## Riprogrammazione dell'aggiornamento del sistema

Per riprogrammare l'aggiornamento del sistema:

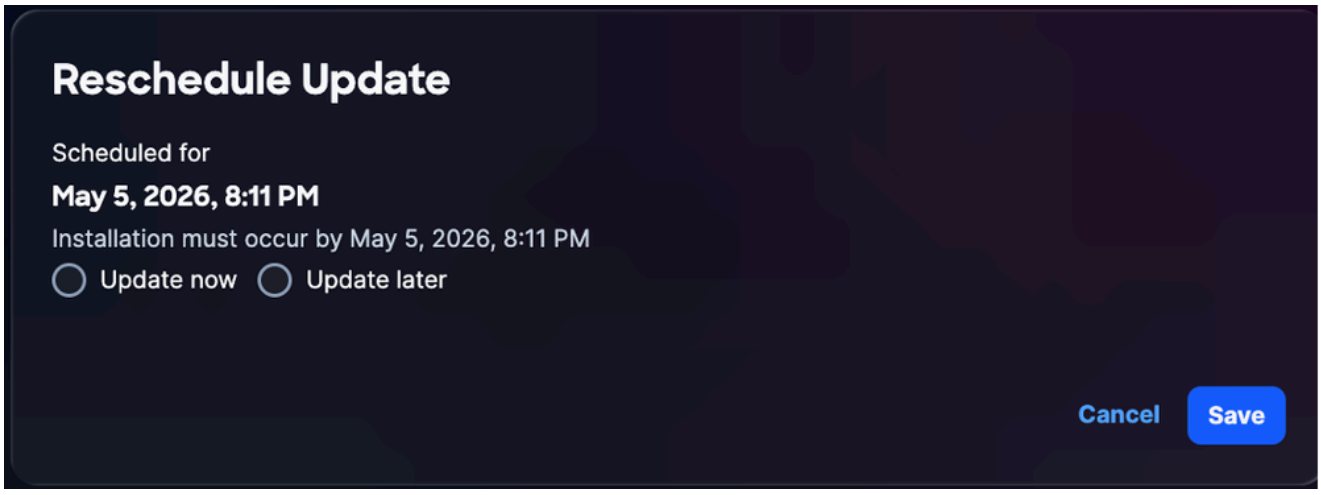
1. Da Amministrazione, scegliere Configurazione sistema > Gestione sistema. Viene

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

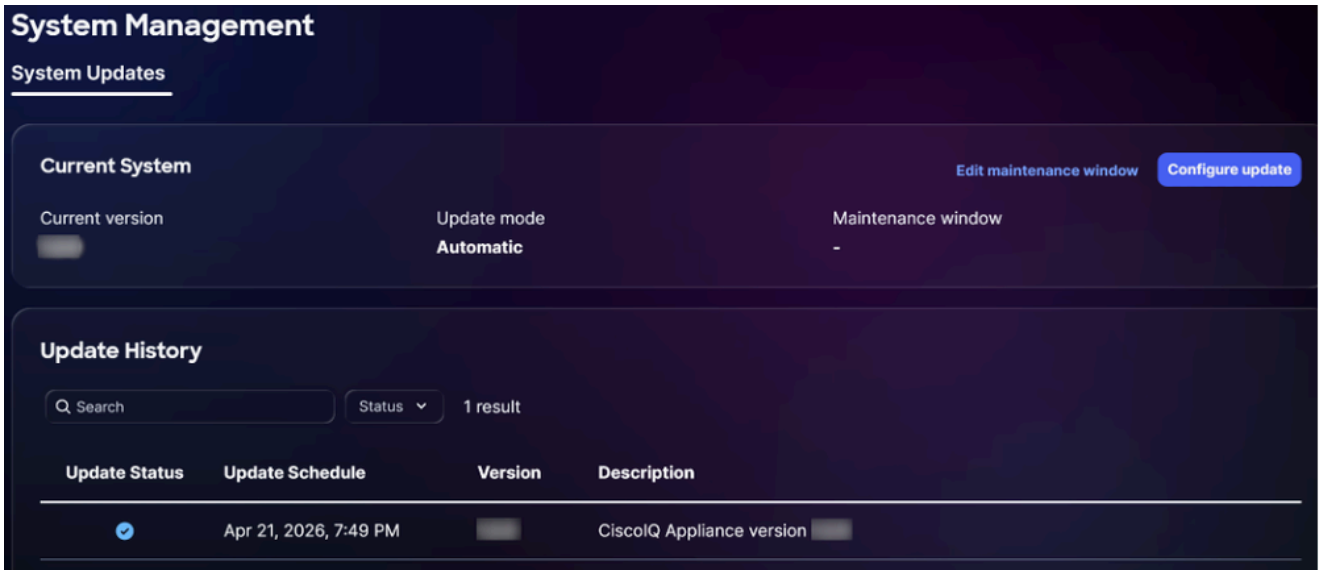
2. Fare clic su Riprogramma aggiornamento.




Ripianifica aggiornamento

3. Scegliere il pulsante di scelta Aggiorna ora per la riprogrammazione immediata o il pulsante di scelta 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.

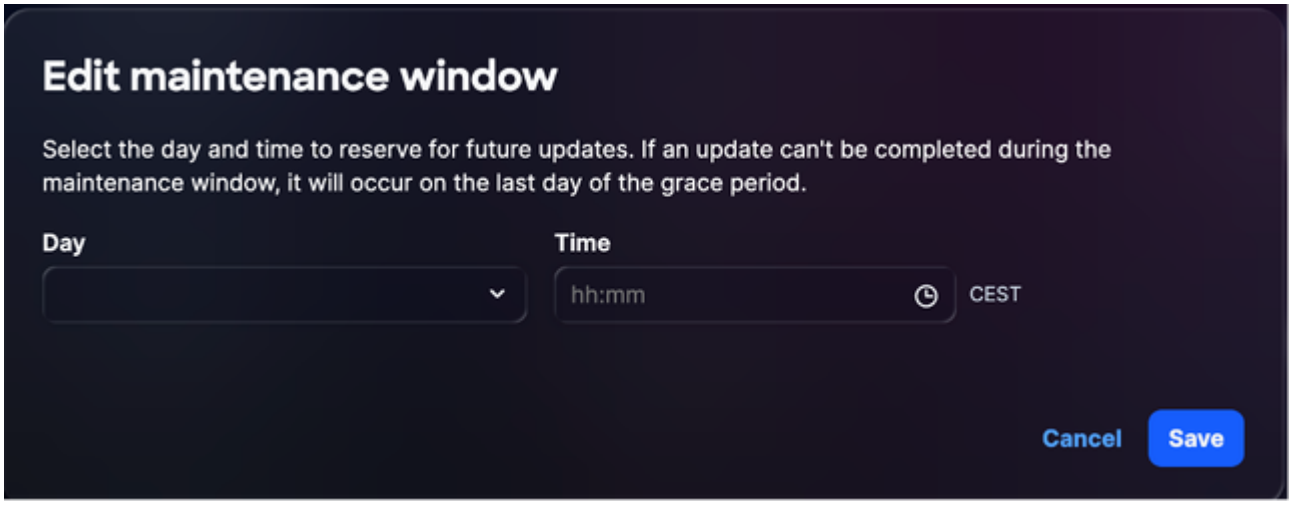



Aggiornamento completato

Modifica delle pianificazioni di aggiornamento del sistema

È possibile creare una pianificazione personalizzata per gli aggiornamenti del sistema. Se è stata configurata una pianificazione personalizzata, gli aggiornamenti vengono eseguiti in date definite dall'utente, a condizione che rientrino nel periodo di tolleranza massimo. Per creare una pianificazione di aggiornamento del sistema:

1. Dalla sezione Sistema corrente della pagina Gestione sistema, fare clic su Modifica finestra manutenzione.




Modifica finestra di manutenzione

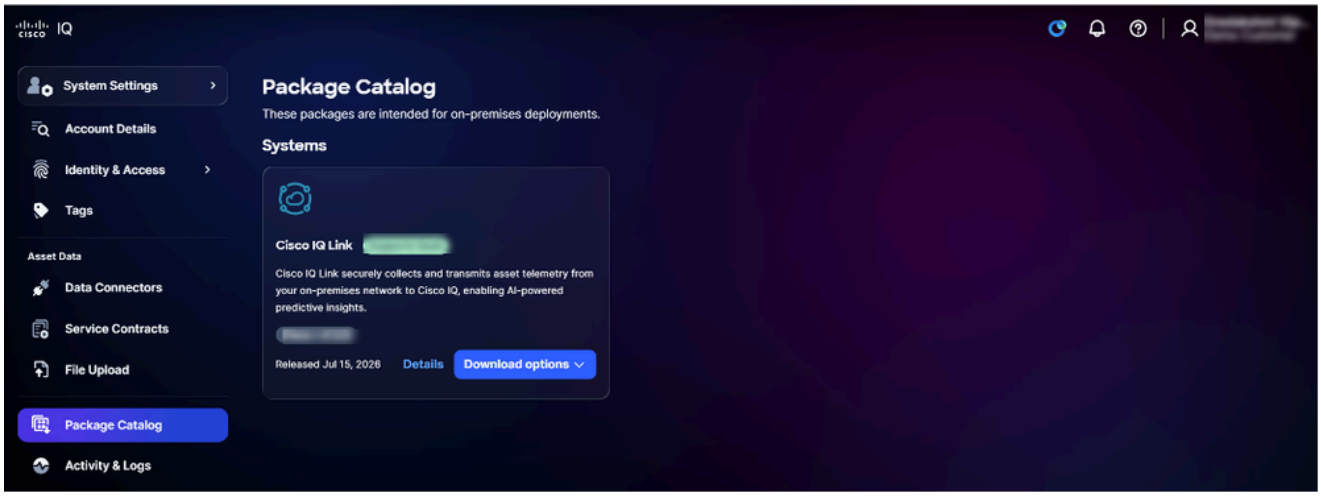
2. Selezionare un'opzione dagli elenchi a discesa Giorno e Ora.
3. Fare clic su Salva. La finestra di manutenzione è stata pianificata correttamente. L'aggiornamento viene attivato in base alla pianificazione visualizzata.

Nota:
- Se non è stata configurata alcuna pianificazione di aggiornamento, il sistema imposta automaticamente un periodo di tolleranza di due (2) settimane per gli aggiornamenti senza riavvio e di quattro (4) settimane per gli aggiornamenti che richiedono un riavvio. Dopo questi periodi di prova, gli aggiornamenti devono essere eseguiti manualmente.
- In caso di errore durante l'aggiornamento, il sistema esegue fino a due (2) tentativi automatici. Un terzo tentativo è pianificato ma richiede l'avvio manuale.

## Aggiornamento manuale del sistema

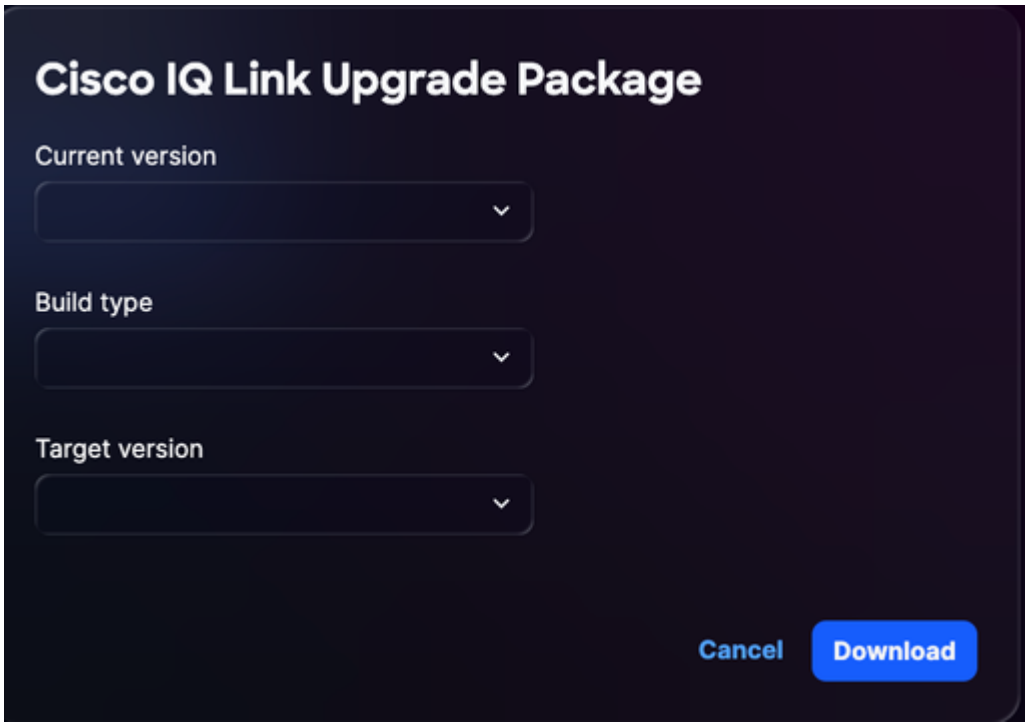
Negli scenari in cui la distribuzione automatica da Cisco IQ SaaS non è disponibile o è ritardata, è possibile eseguire manualmente un aggiornamento del sistema scaricando il bundle di aggiornamento direttamente da Cisco IQ SaaS. Per aggiornare manualmente il sistema:

1. Accedere a Cisco IQ SaaS e selezionare Home > Impostazioni di sistema > Catalogo pacchetti.



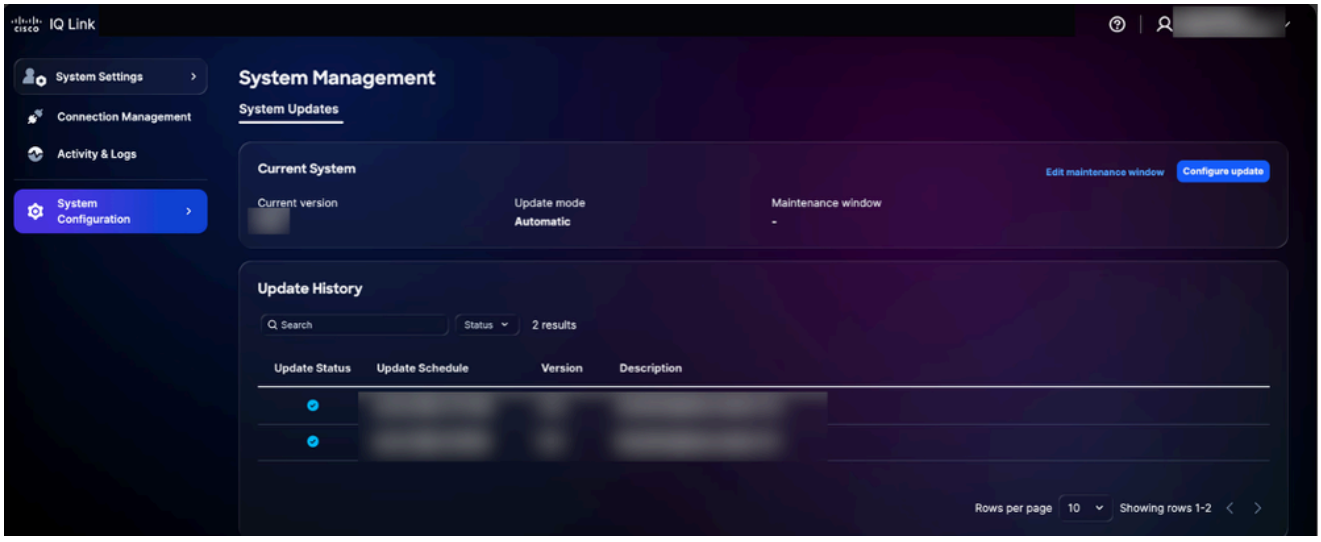

Catalogo pacchetto

2. Nella sezione Cisco IQ Link, fare clic su Download options (Opzioni di download) > Upgrade packages (Pacchetti di aggiornamento).



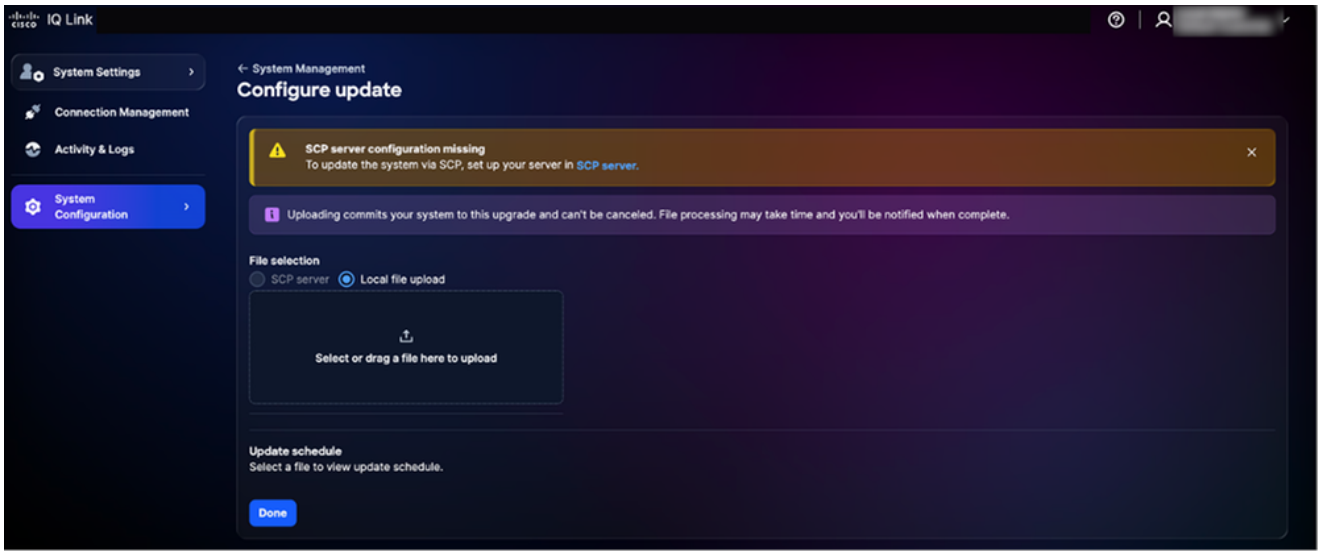

Pacchetto di aggiornamento

3. Selezionare la versione corrente dall'elenco a discesa.
4. Selezionare il tipo di generazione dall'elenco a discesa.
5. Selezionare la versione di destinazione dall'elenco a discesa.
6. Fare clic su Download (Scarica). Il bundle di aggiornamento viene scaricato.
7. Passare al collegamento Cisco IQ.
8. Da Impostazioni di sistema, scegliere Configurazione di sistema > Gestione sistema.




Configura aggiornamento

9. Fare clic su Configura aggiornamento.




Caricamento file locale

10. Fare clic sul pulsante di opzione Caricamento file locale.
11. Selezionare o trascinare il file del bundle di aggiornamento scaricato nel campo di caricamento.
12. Selezionate Fatto (Done). Dopo il corretto aggiornamento del sistema viene visualizzato un messaggio di conferma.

## Configurazione certificati SSL

In Cisco IQ è preinstallato e abilitato un certificato autofirmato predefinito, ma è possibile 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.

Impossibile modificare o eliminare il certificato SSL 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.

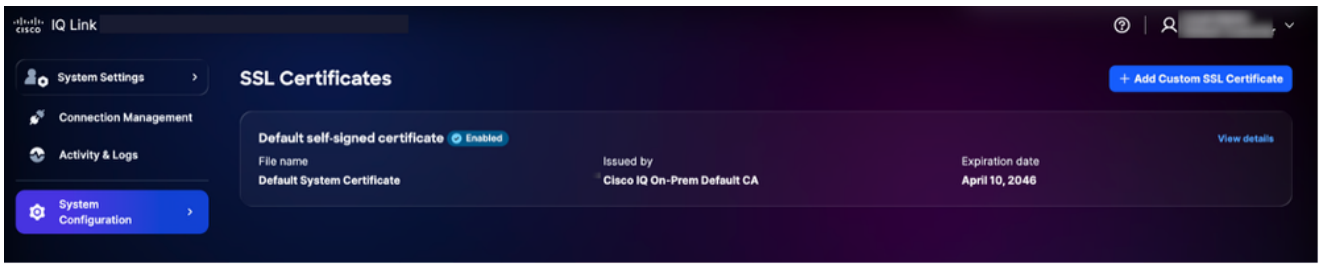
---

Dopo aver aggiunto, modificato o eliminato un certificato SSL, è necessario caricare il nuovo certificato SSL come descritto in Configurazione disconnessione singola 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.



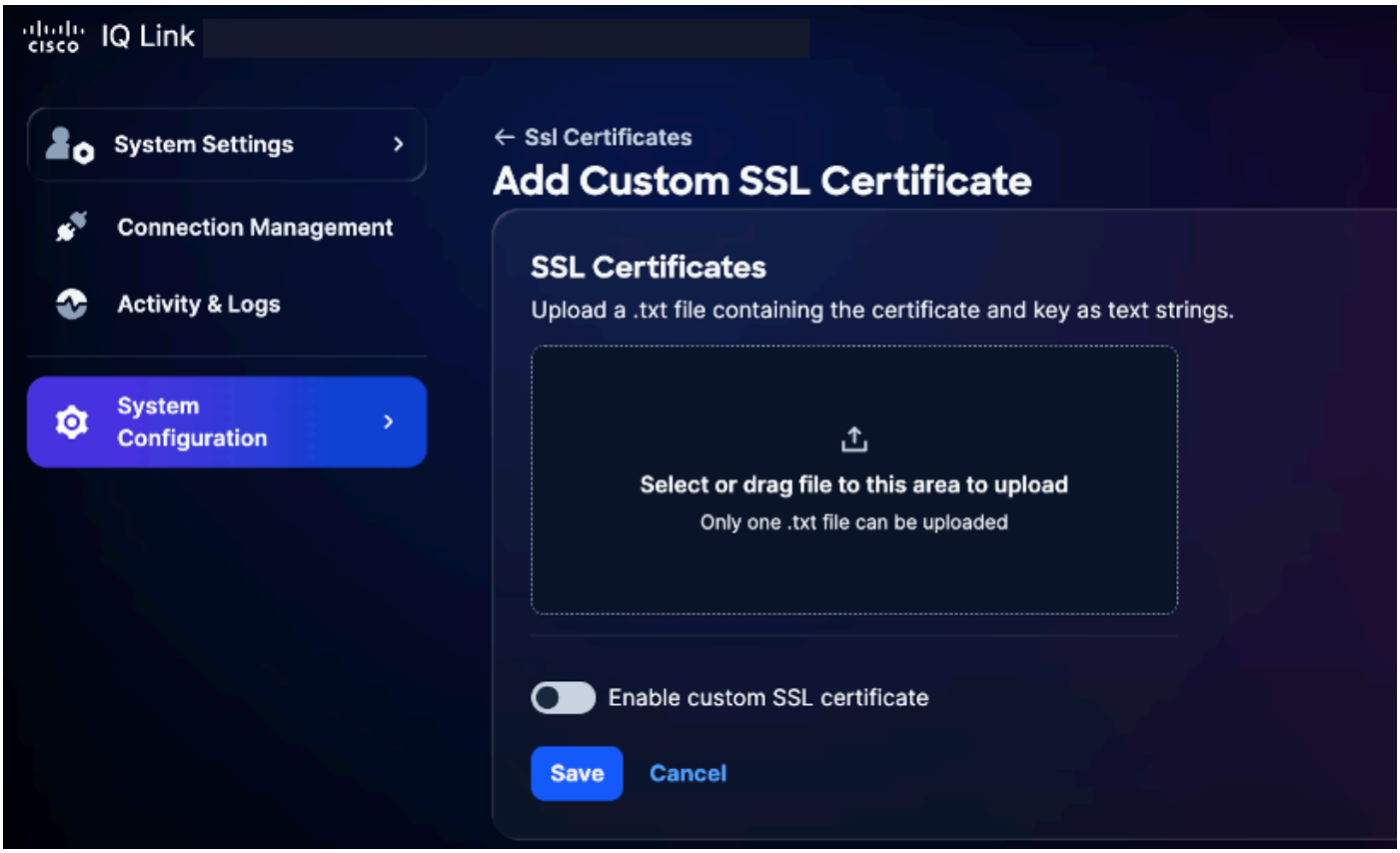

Aggiunta del certificato SSL

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 Mail come stringhe di testo
- È possibile caricare un solo file .txt alla volta
- Il file deve contenere sia il certificato che la chiave privata

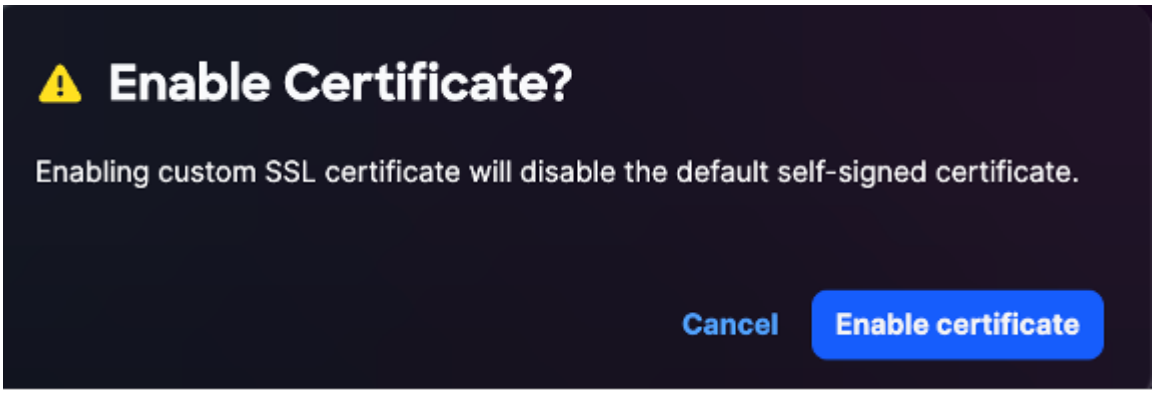
---




Carica certificato SSL

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

4. Attivare il pulsante Abilita certificato SSL personalizzato.




Modifica certificato SSL

---

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

---

5. Fare clic su Abilita certificato.

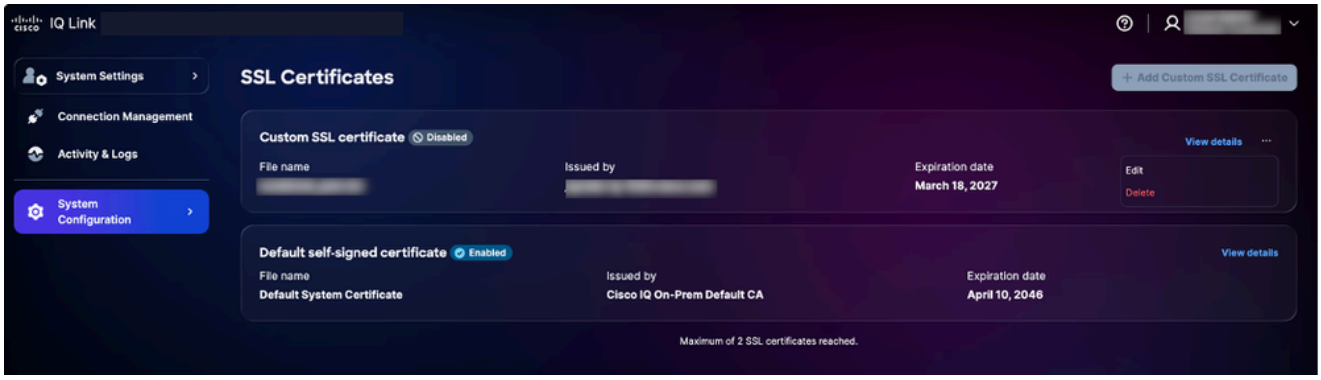
6. Fare clic su Salva.

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

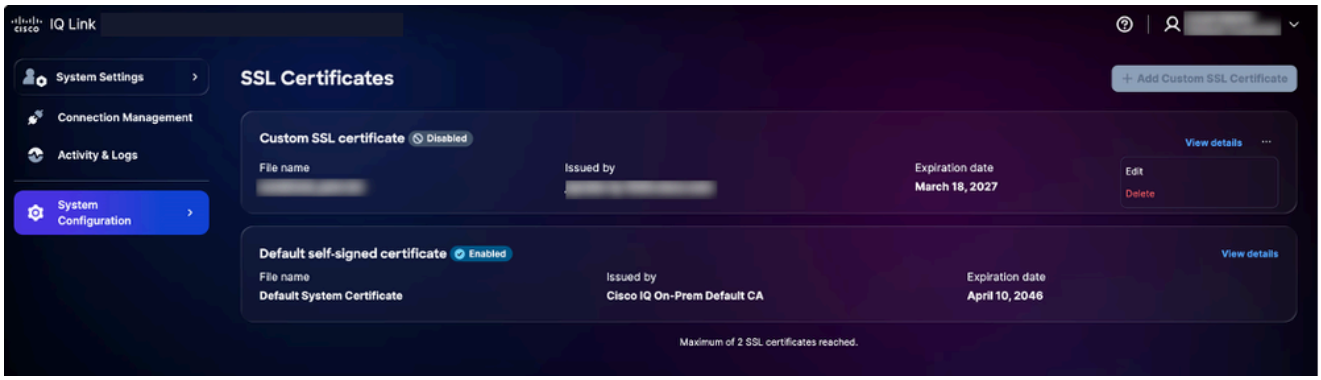
---

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 personalizzato 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 account possono configurare i server syslog esterni per esportare i registri di sistema. È possibile configurare fino a due (2) server syslog.

---

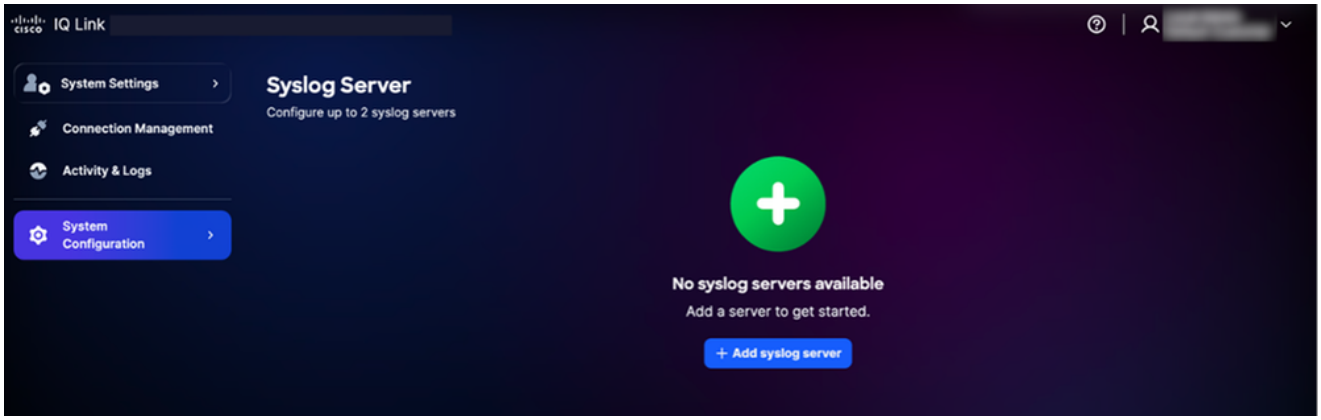
Nota: È necessario specificare il server Syslog come indirizzo IP e non come FQDN.

---

## Aggiunta di server syslog

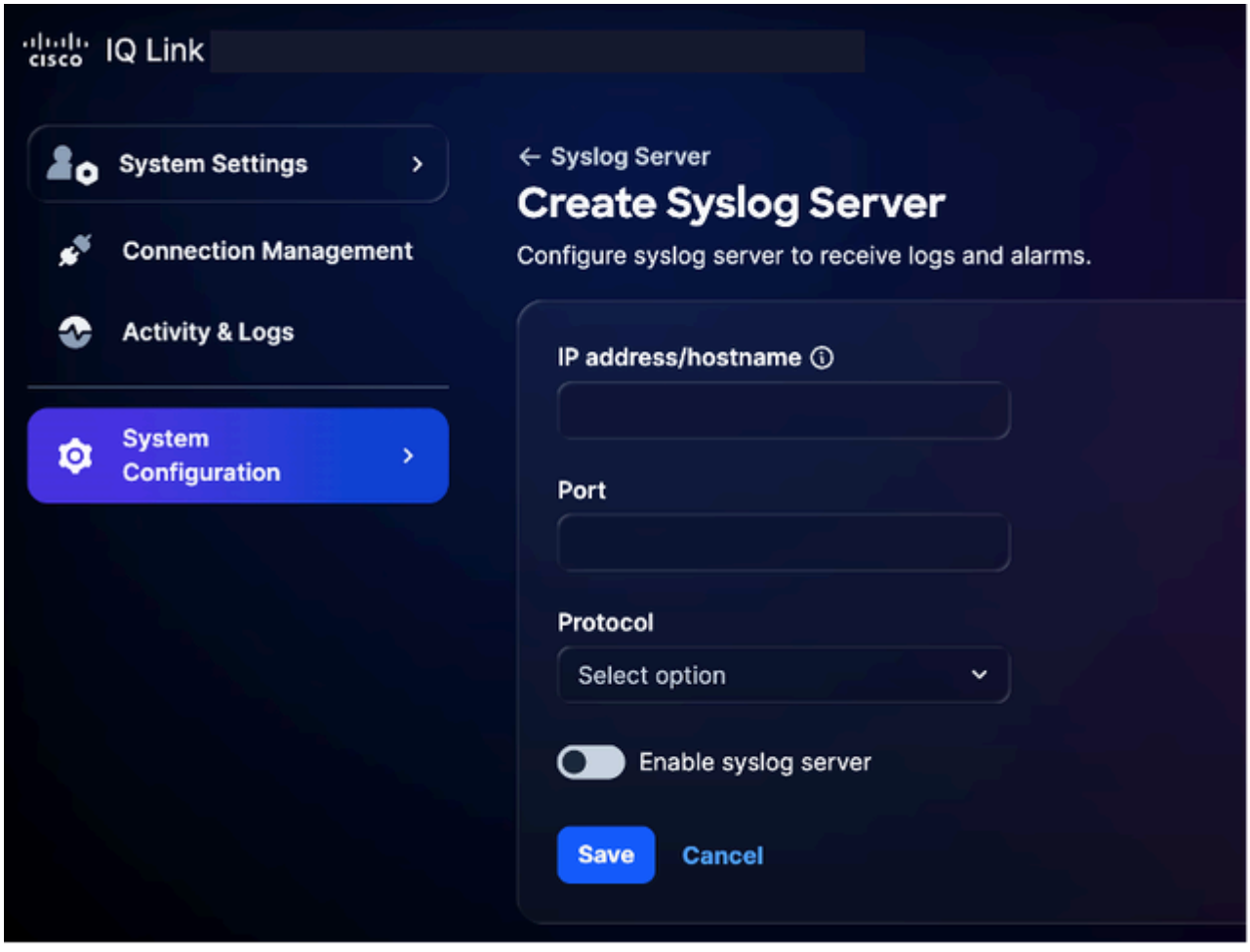
Per aggiungere un server syslog:

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.



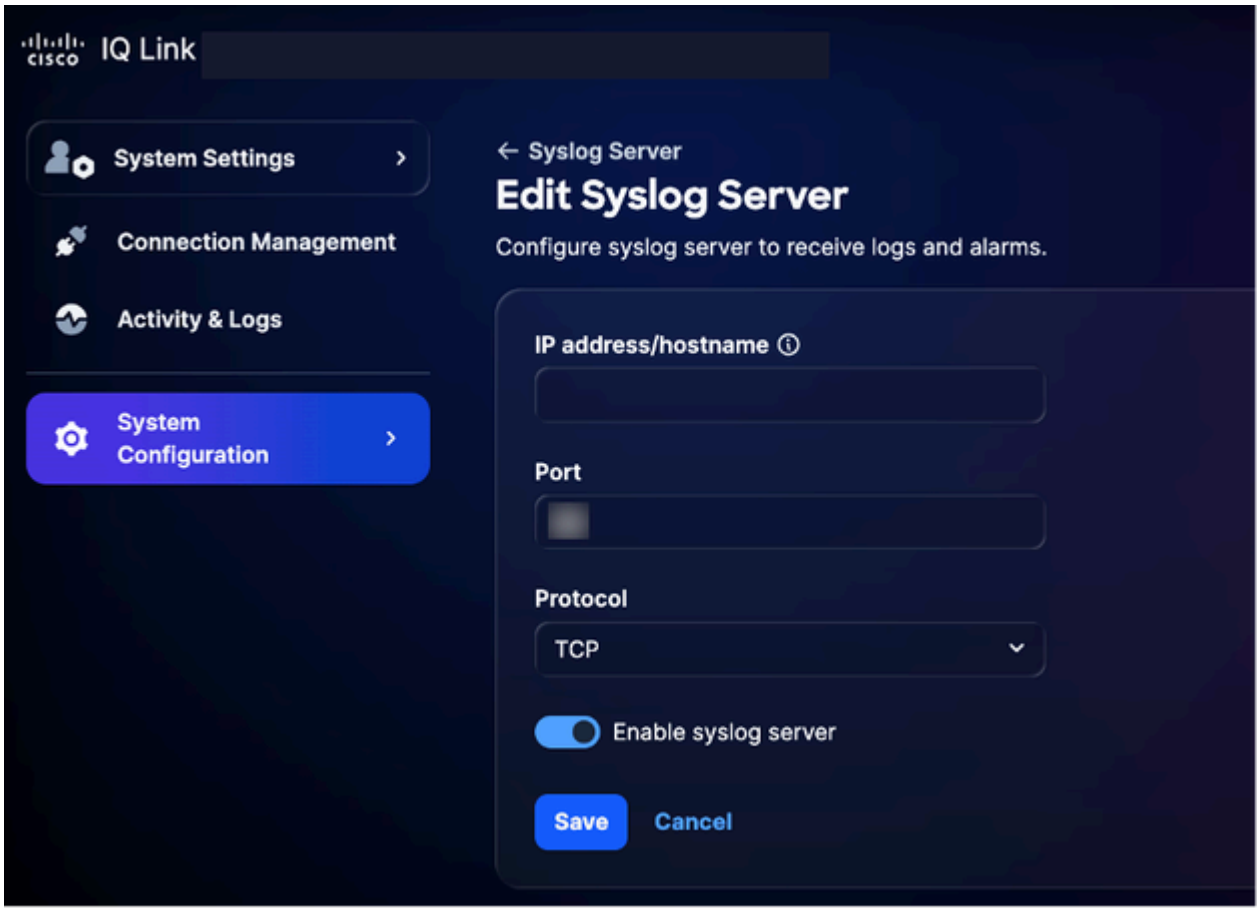
Crea server syslog

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

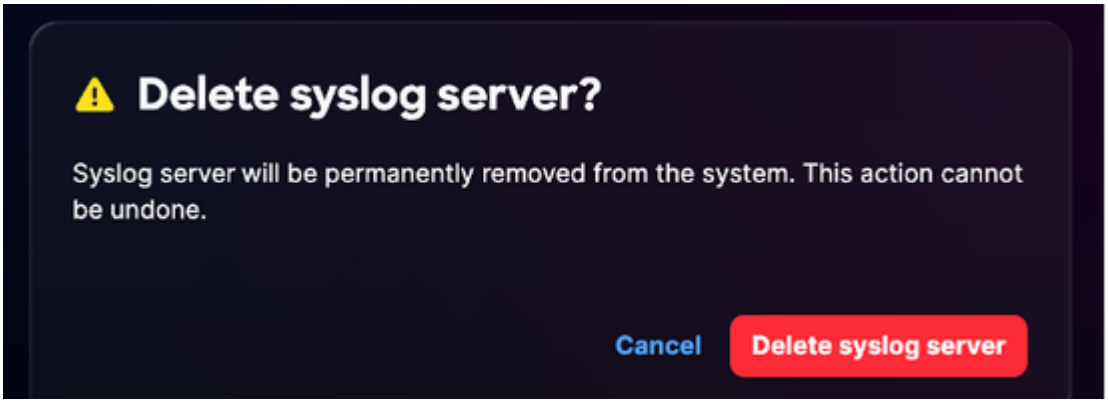
3. Modificare i dettagli o disattivare l'opzione Abilita server syslog, come richiesto.

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.

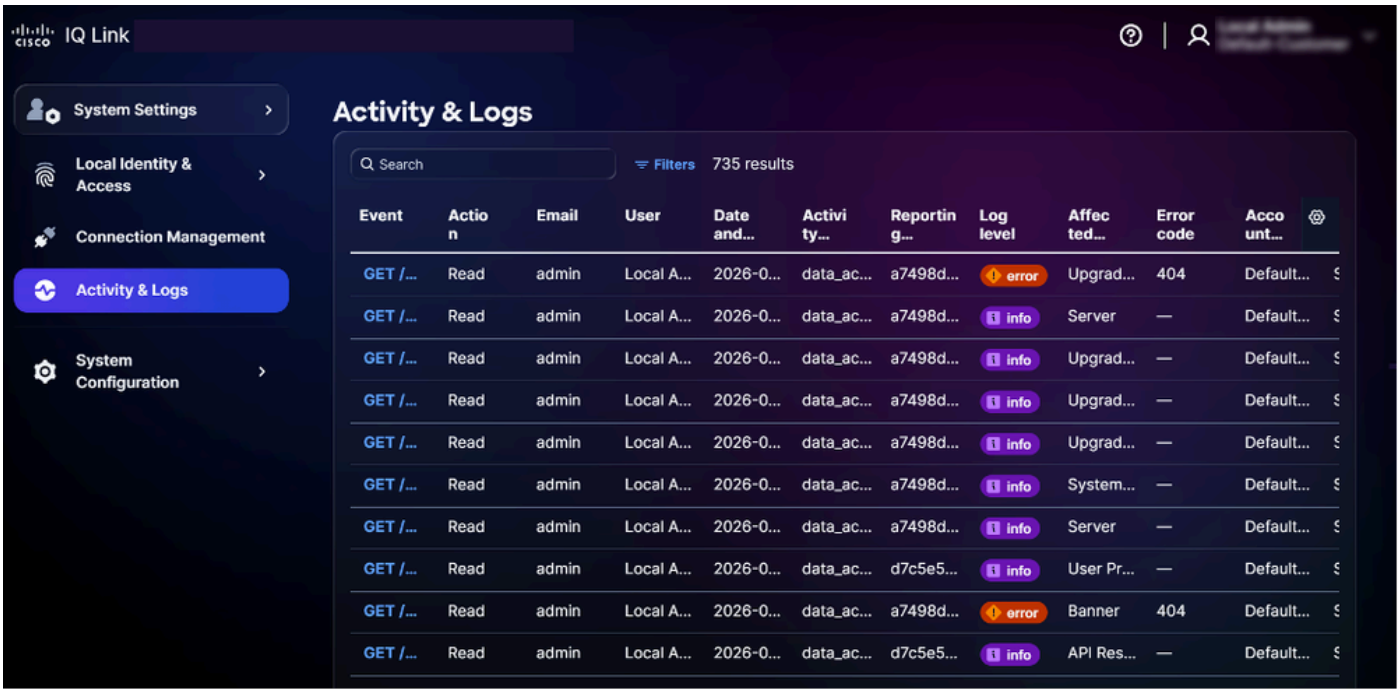



Conferma

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

## Registri attività

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




Registri attività

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

Log attività:

- Supporta filtri, impaginazione e funzionalità di ricerca per facilitare l'individuazione e la gestione delle informazioni
- Registra tutte le operazioni API a livello di gateway

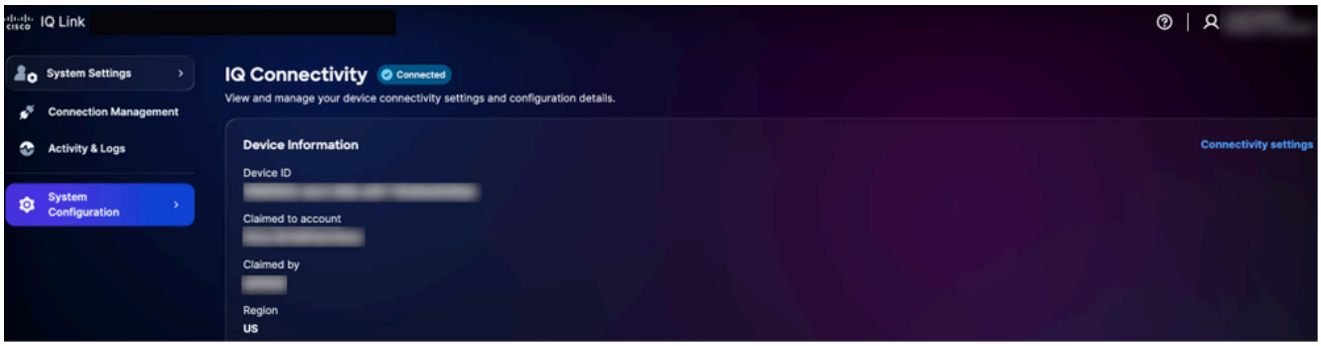
Sono disponibili le seguenti opzioni di filtro:

- 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

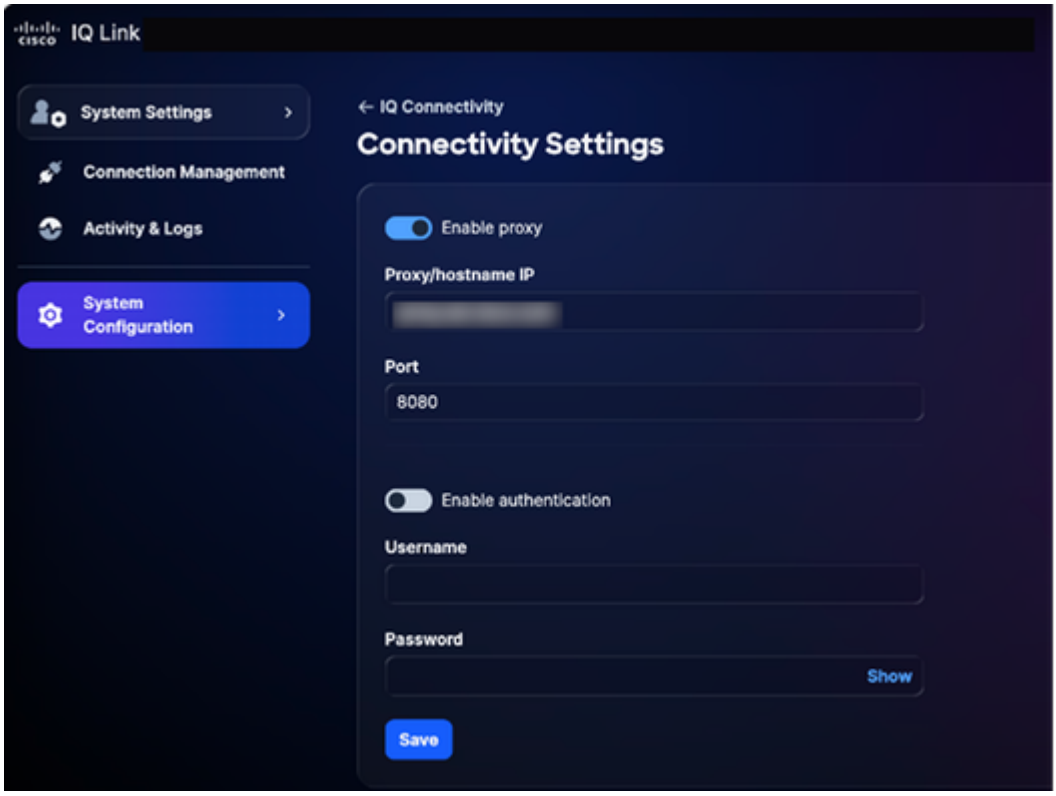
Per visualizzare e gestire le impostazioni di connettività del dispositivo e i dettagli di configurazione:

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 on-premises per la raccolta dei dati di rete, progettata per fornire una visibilità completa nell'infrastruttura. Raccoglie i dati tramite Catalyst Center e Direct Connection. Semplifica la gestione dell'autenticazione di rete e dell'individuazione dei dispositivi.

Di seguito è riportato un riepilogo della configurazione della raccolta dati:

- Creazione di set di credenziali: Stabilire i protocolli di autenticazione (ad esempio, SNMP (Simple Network Management Protocol) 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.
- 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.

---

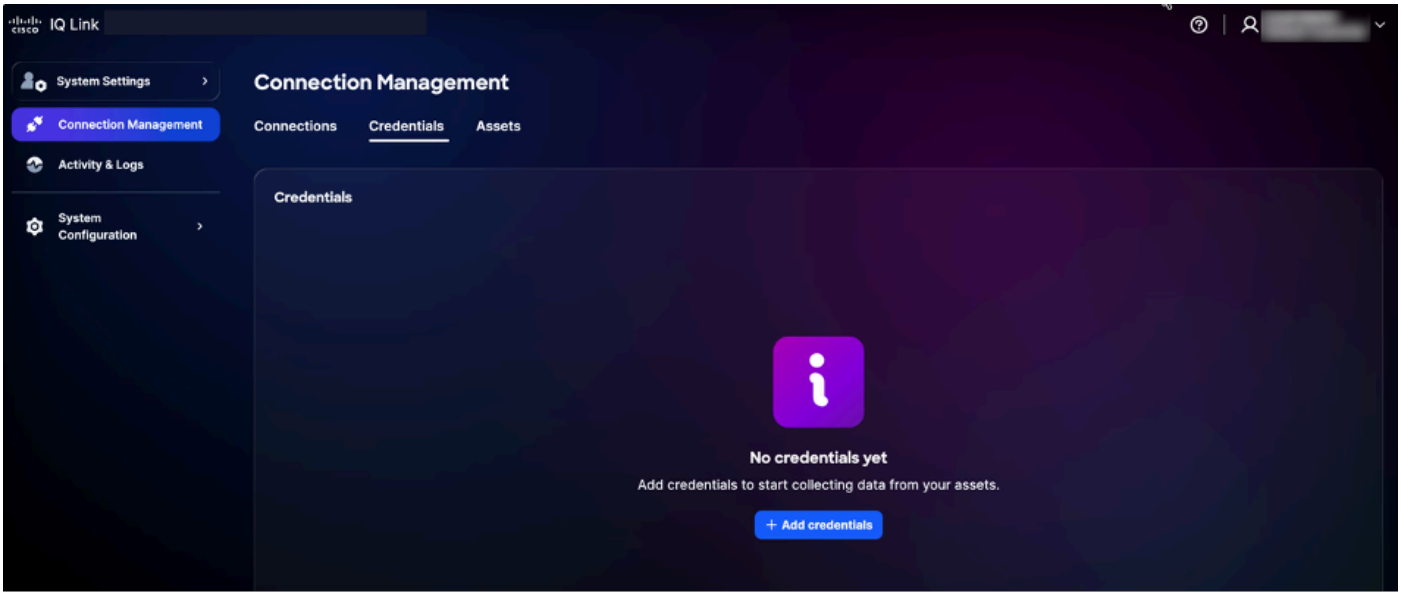
Nota: Per l'individuazione dei dispositivi sono richiesti SNMPv2c/SNMPv3 e SSH. Prima di configurare Catalyst Center, è necessario fornire le credenziali HTTP/HTTPS.

---

## Aggiunta di credenziali

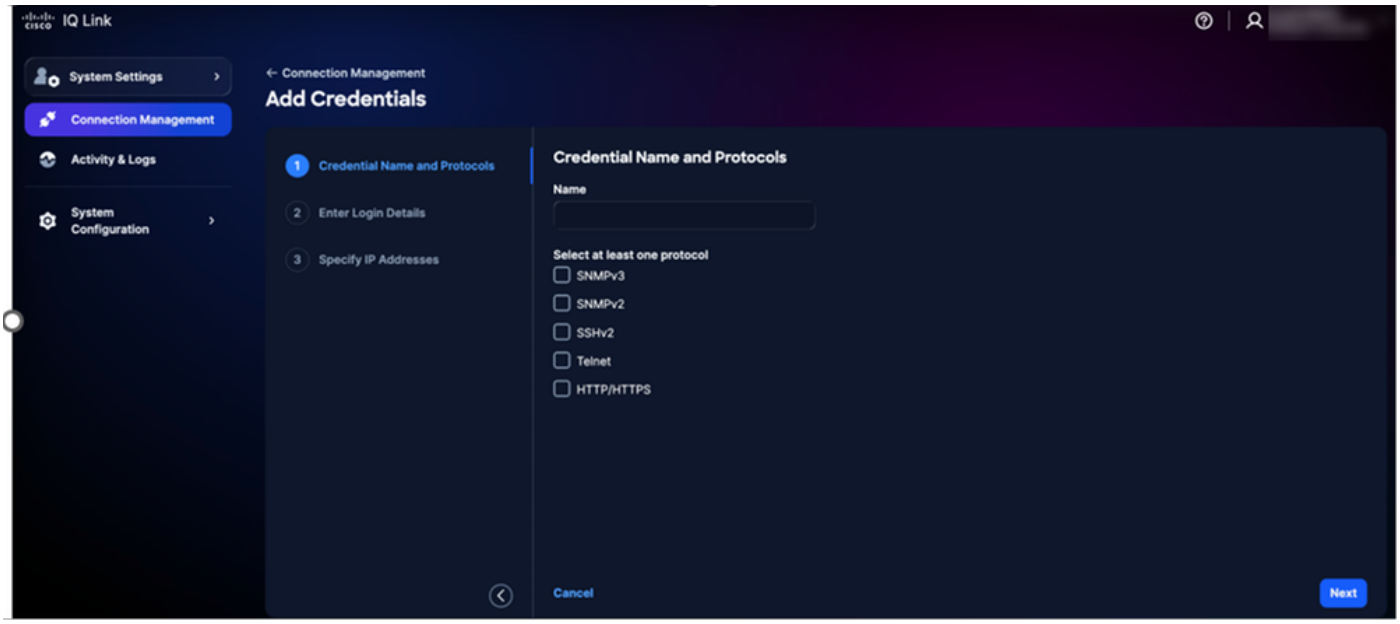
Per eseguire la raccolta dei dati, è innanzitutto necessario aggiungere le credenziali. Per aggiungere le credenziali:

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.

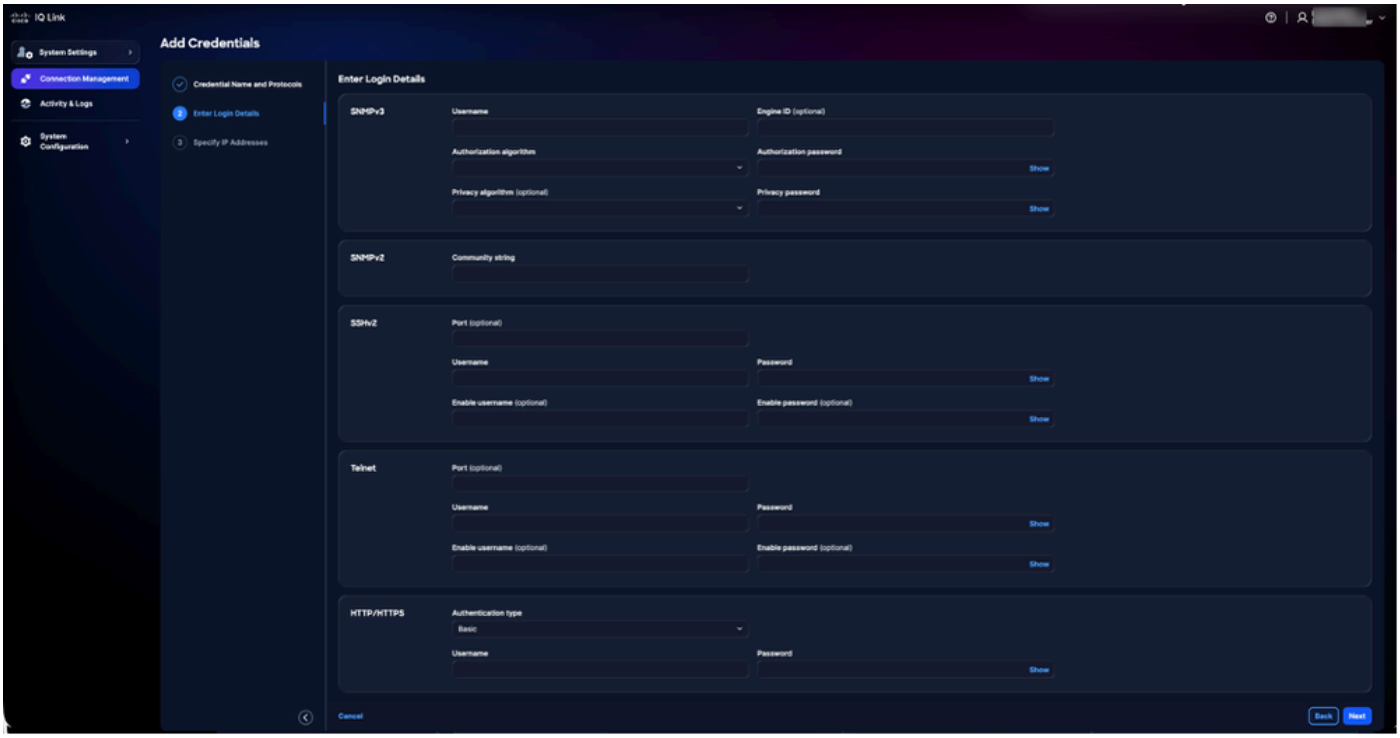



Aggiungi credenziali

4. Inserire il nome.

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

6. Fare clic su Avanti.

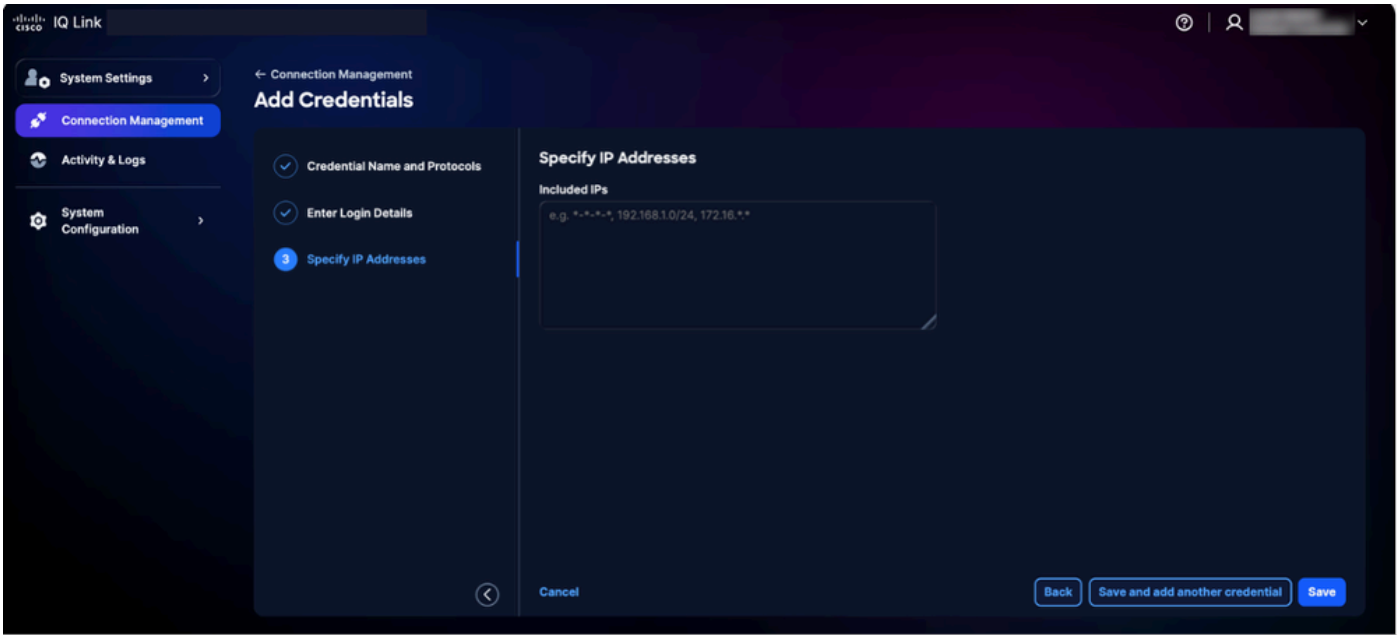



Aggiungi dettagli credenziali

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

7. Inserire i dettagli di login per ciascun protocollo selezionato.

8. Fare clic su Avanti.

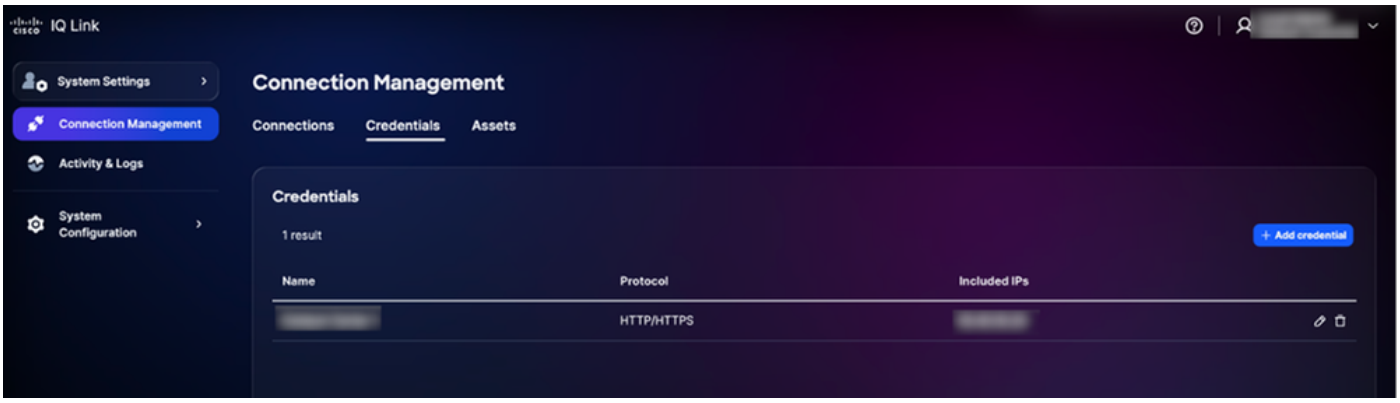



Specifica indirizzi IP

9. Inserire gli indirizzi 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 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
  - Match con caratteri jolly finali: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.

Tabella 13. 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) |

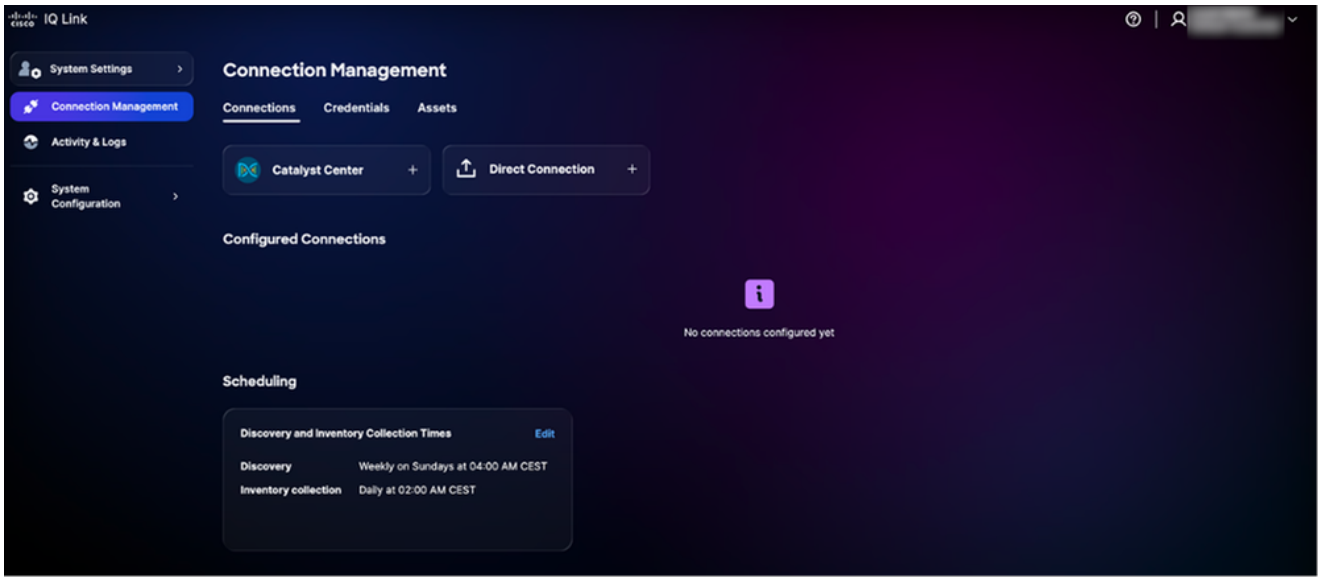
Nota: Se un dispositivo rientra in più categorie sovrapposte, il sistema seleziona sempre il set di credenziali con la più alta specificità (in altre parole, il minor numero di caratteri jolly finali).

## Raccolta dei dati tramite Catalyst Center

È possibile connettere fino a 20 Catalyst Center (non cluster) per ciascuna istanza di Cisco IQ Link.

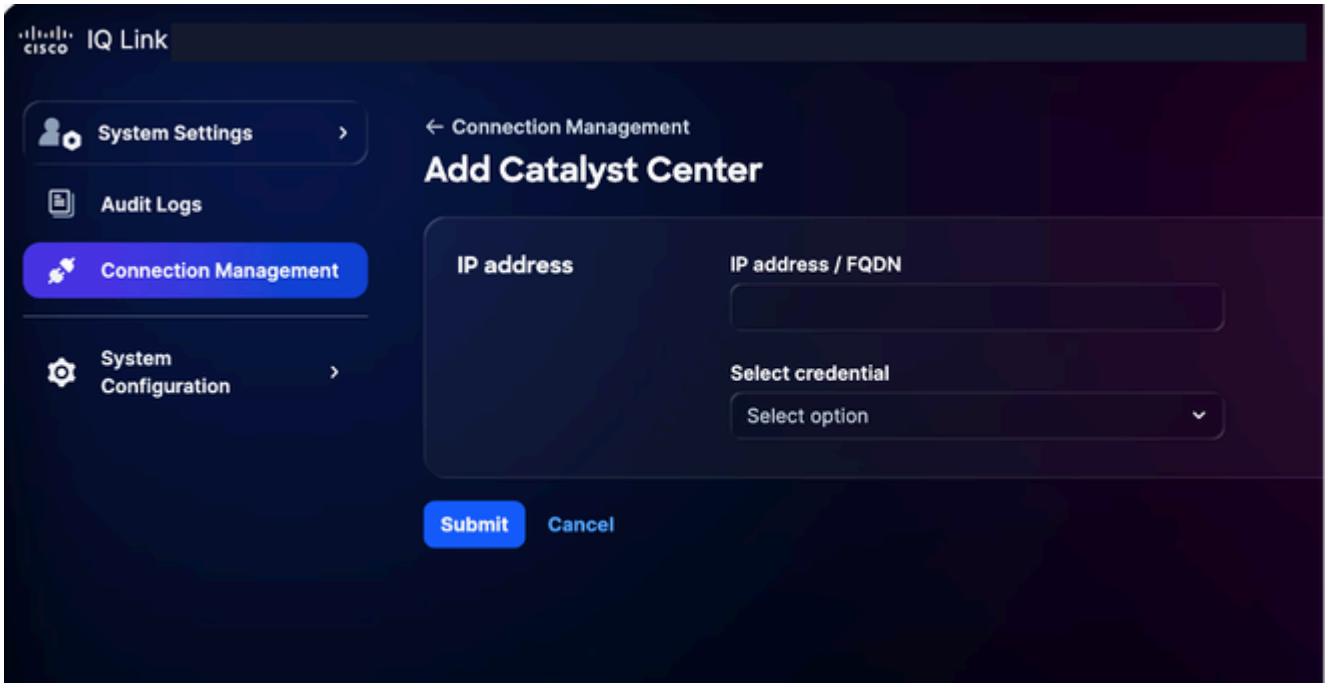
Per la raccolta dei dati con Catalyst Center:

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



Gestione connessione

2. Fare clic sull'opzione Catalyst Center.

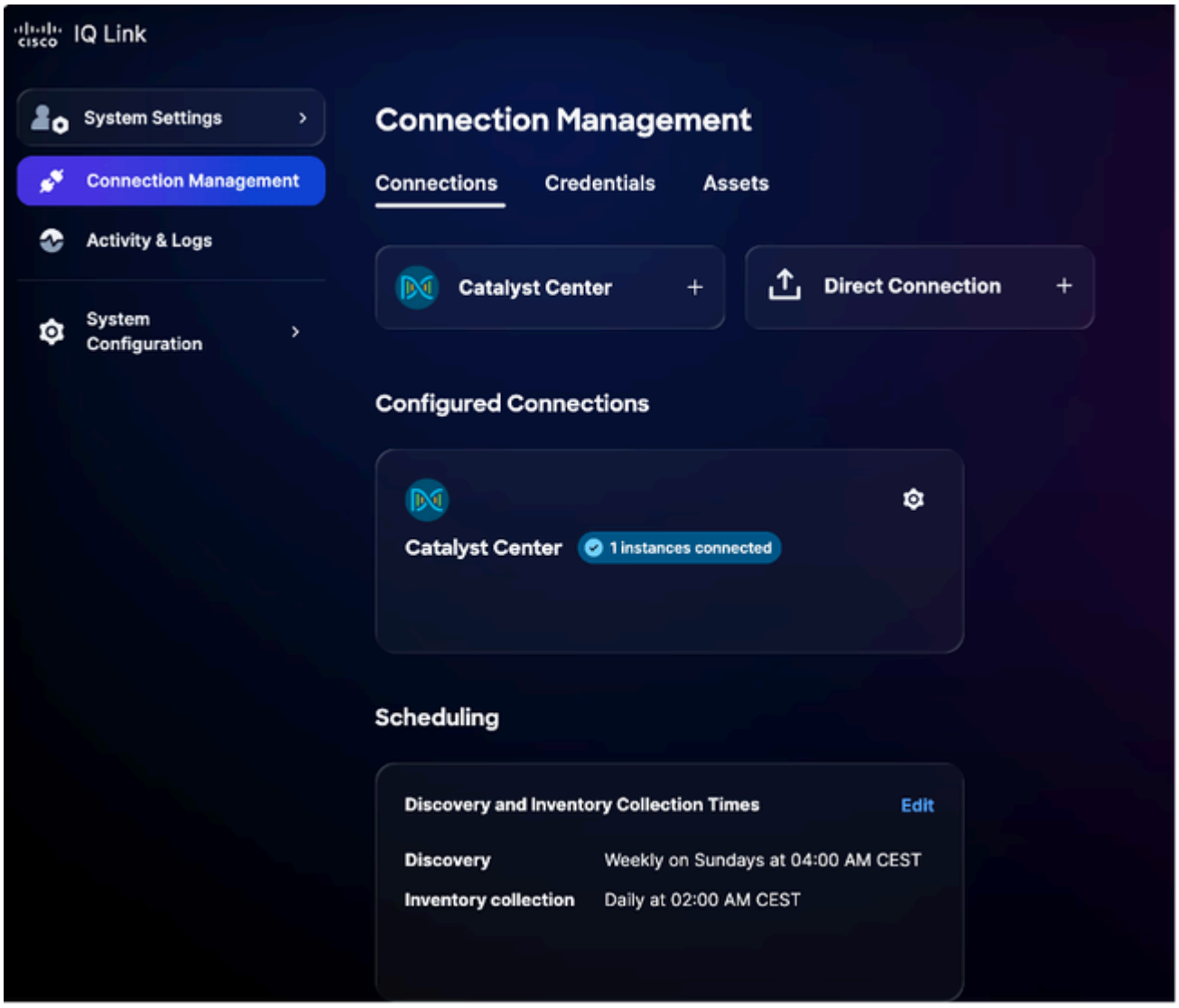



Aggiungi Catalyst Center

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

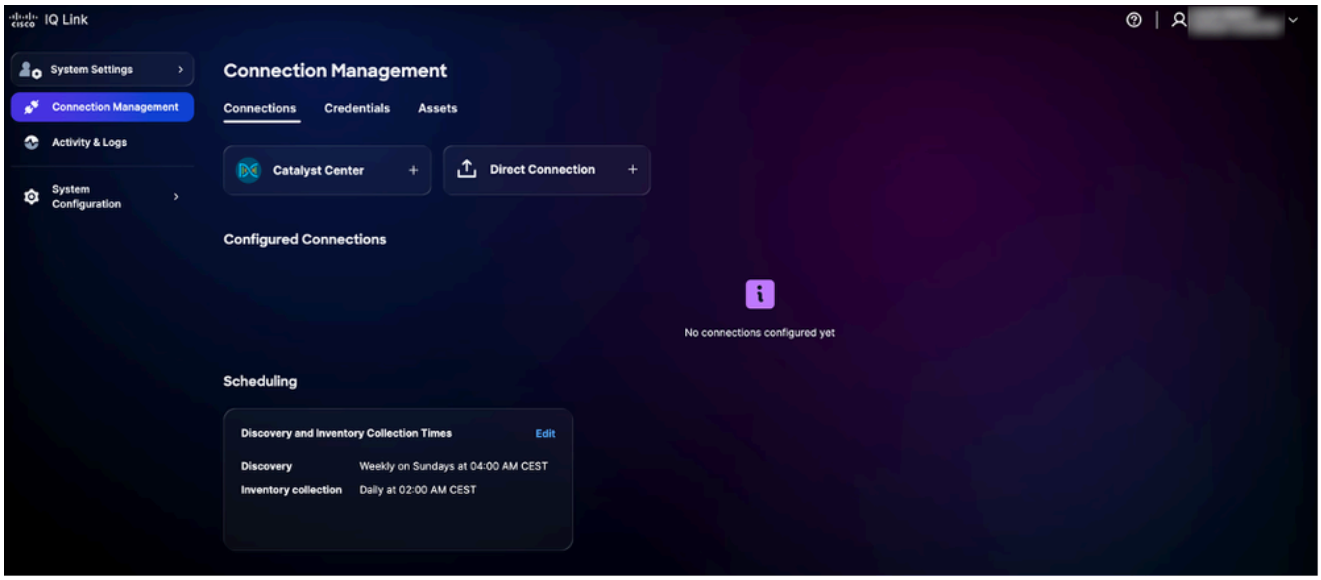
6. Pianificare una raccolta. Per ulteriori informazioni, vedere Pianificazione.

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

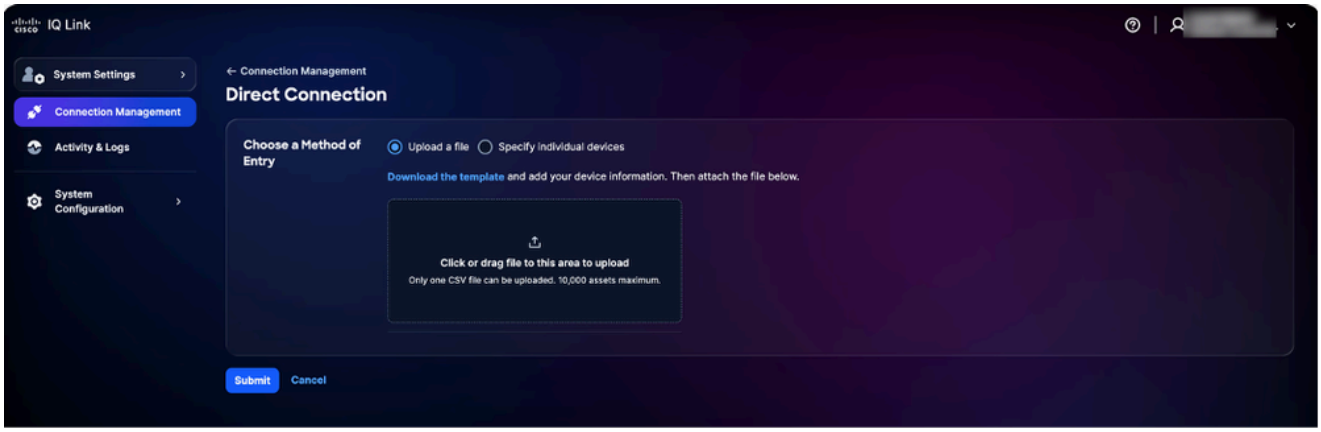
Per aggiungere dispositivi per la connessione diretta:

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



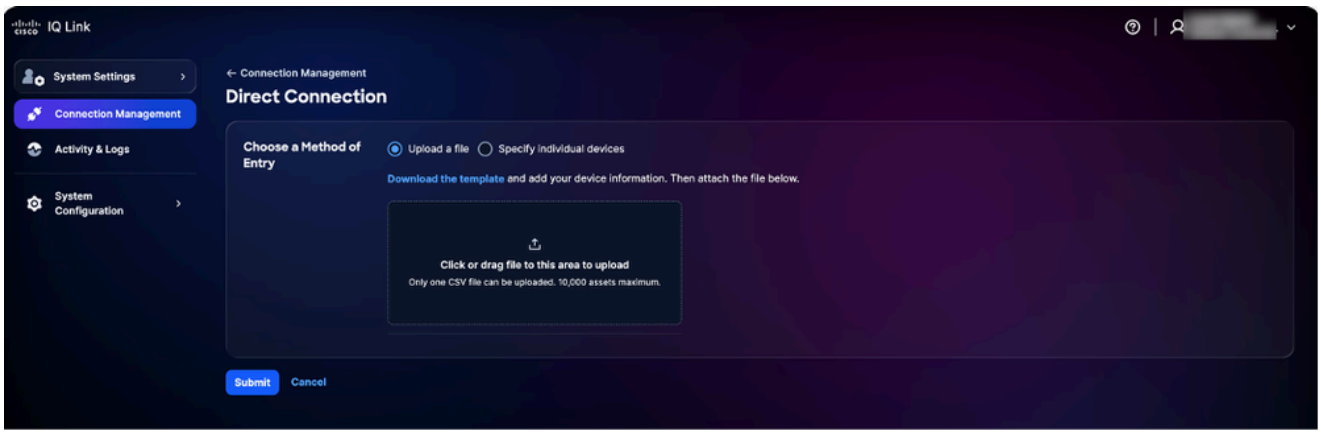

Gestione connessione

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



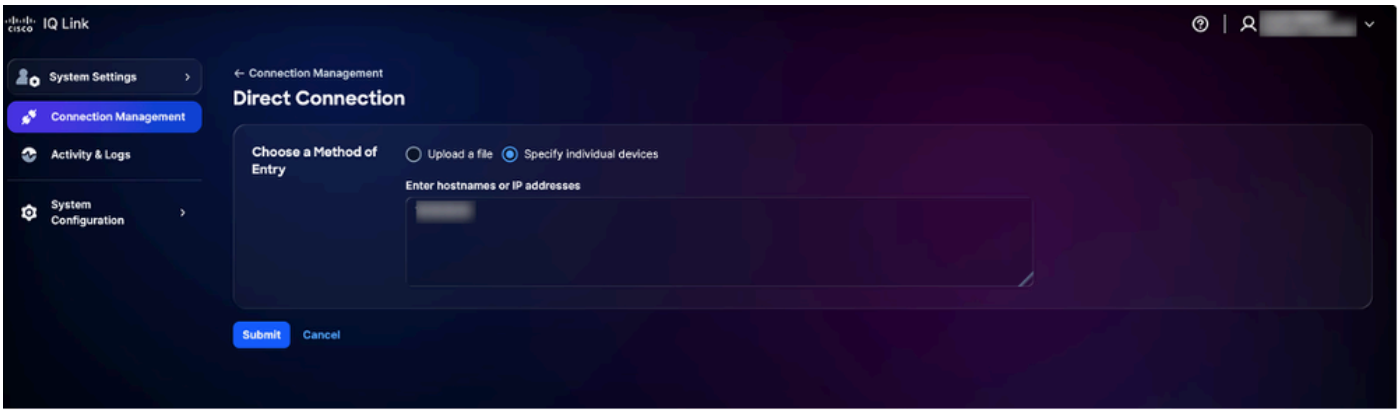

Carica file

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.

---

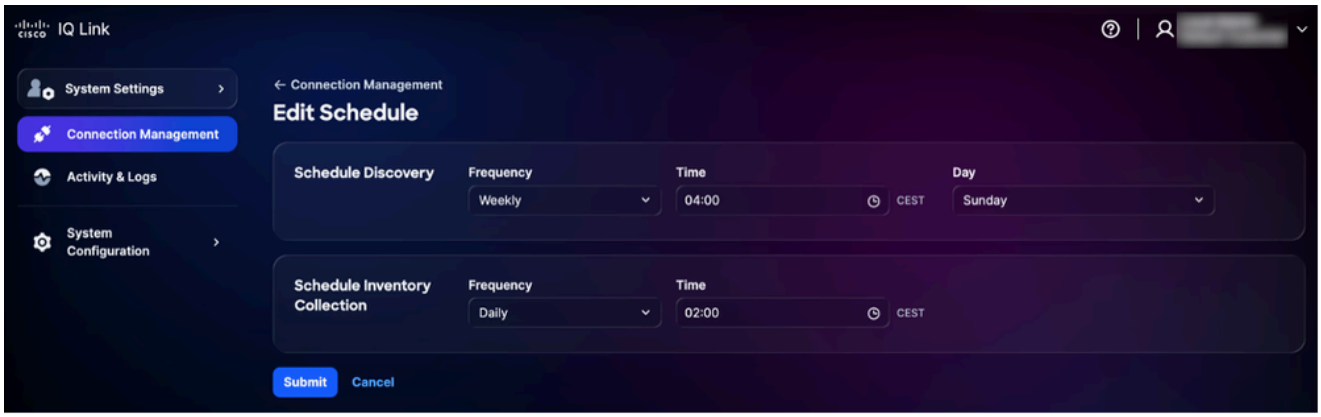
Nota: Cisco IQ Link è preconfigurato con una pianificazione automatica e il sistema avvia una pianificazione predefinita per la raccolta automatica. Si consiglia di modificare la programmazione per allinearla ai requisiti e alle finestre di manutenzione dell'organizzazione.

---

## 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

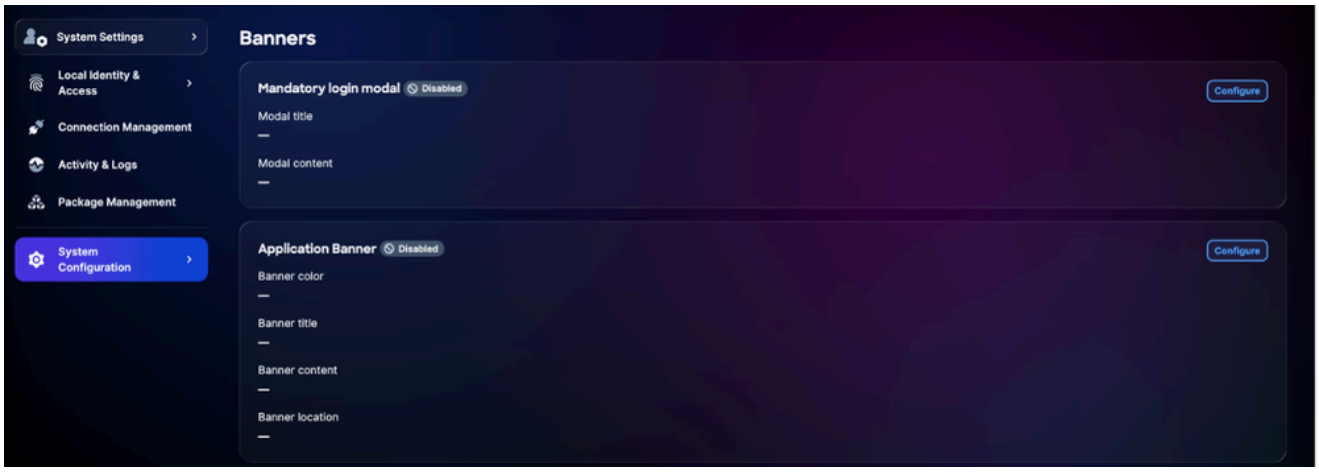
Gli amministratori degli account possono configurare banner a livello di sistema per soddisfare gli standard di sicurezza e conformità.

- Modalità di accesso obbligatoria: Prima di passare alla schermata di accesso, è necessario confermare la visualizzazione del banner obbligatorio.
- Banner applicazione: Si tratta di banner personalizzati che vengono visualizzati nell'applicazione dopo la corretta autenticazione.

## Configurazione dei banner modali di login obbligatori

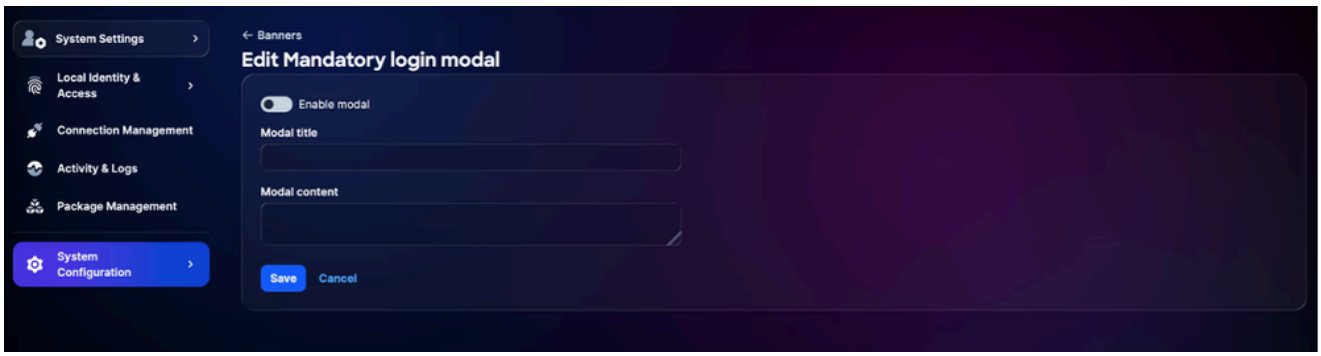
Per configurare un banner obbligatorio:

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




Configura banner obbligatorio

2. Fare clic su Configure (Configura) in Mandatory login modal (Modalità di accesso obbligatoria). Viene visualizzata la pagina modale Modifica accesso obbligatorio.



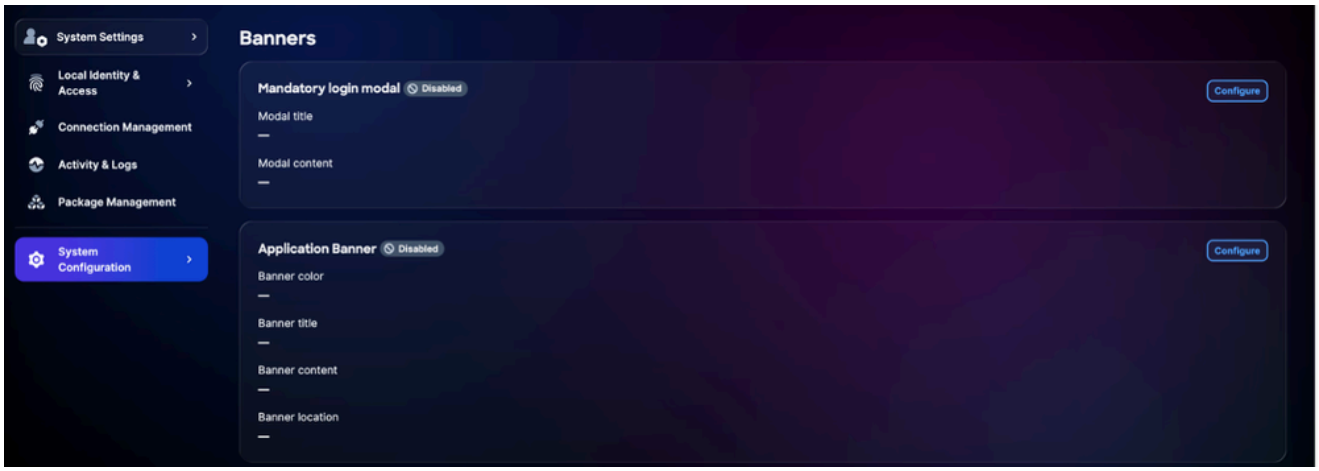

Modifica banner modale di accesso obbligatorio

3. Fare clic sull'interruttore per abilitare o disabilitare il banner.
4. Immettere il titolo modale.
5. Immettere il contenuto modale.
6. Fare clic su Save (Salva). La modalità di accesso obbligatoria è stata salvata.

## Configurazione dei banner applicazione

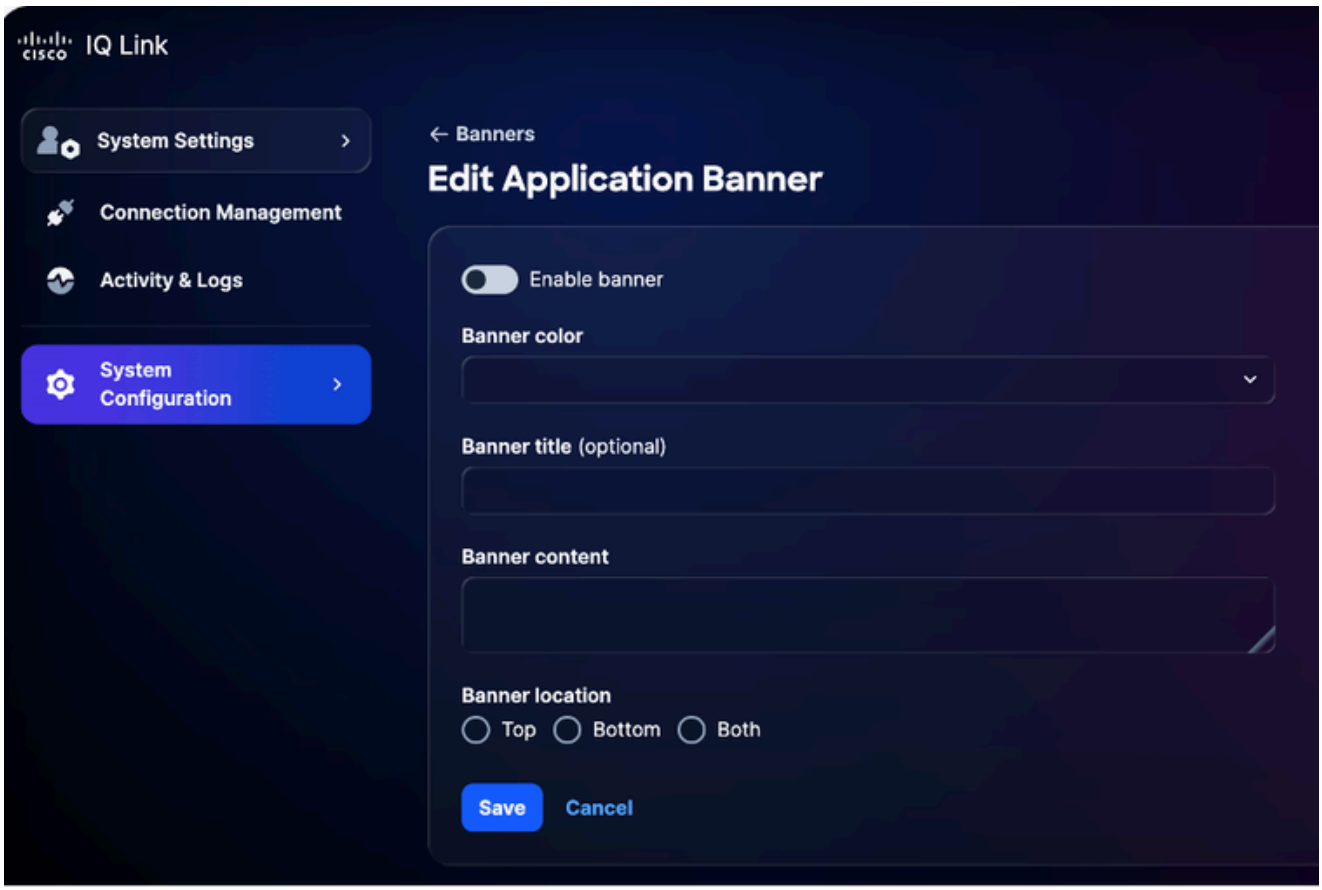
Per configurare un banner applicazione:

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




Configura intestazione

2. Fare clic su Configure (Configura) nell'intestazione dell'applicazione. 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.

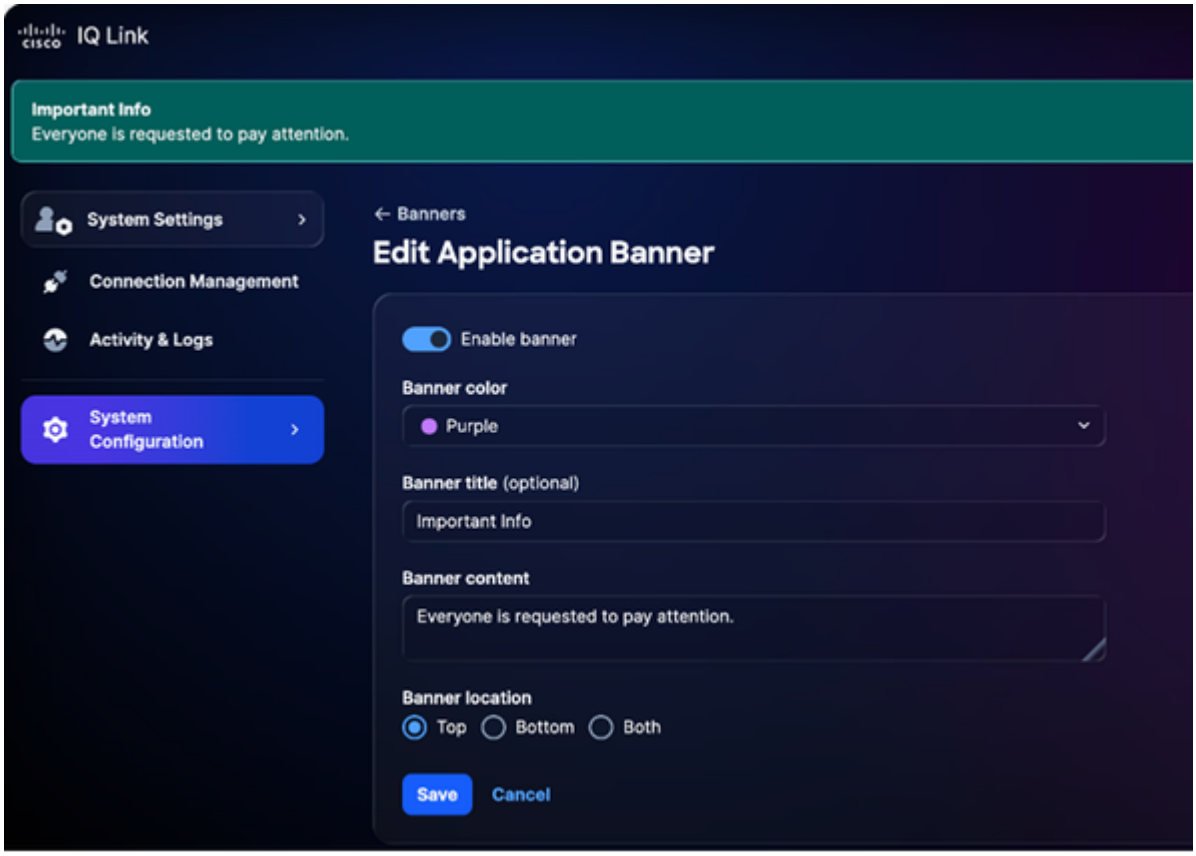
7. Selezionare una posizione per lo striscione.
8. Fare clic su Save (Salva). Il banner viene visualizzato in tutta l'applicazione.

## Modifica dei banner

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


Modifica banner applicazione

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

È possibile raccogliere i file di diagnostica 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:

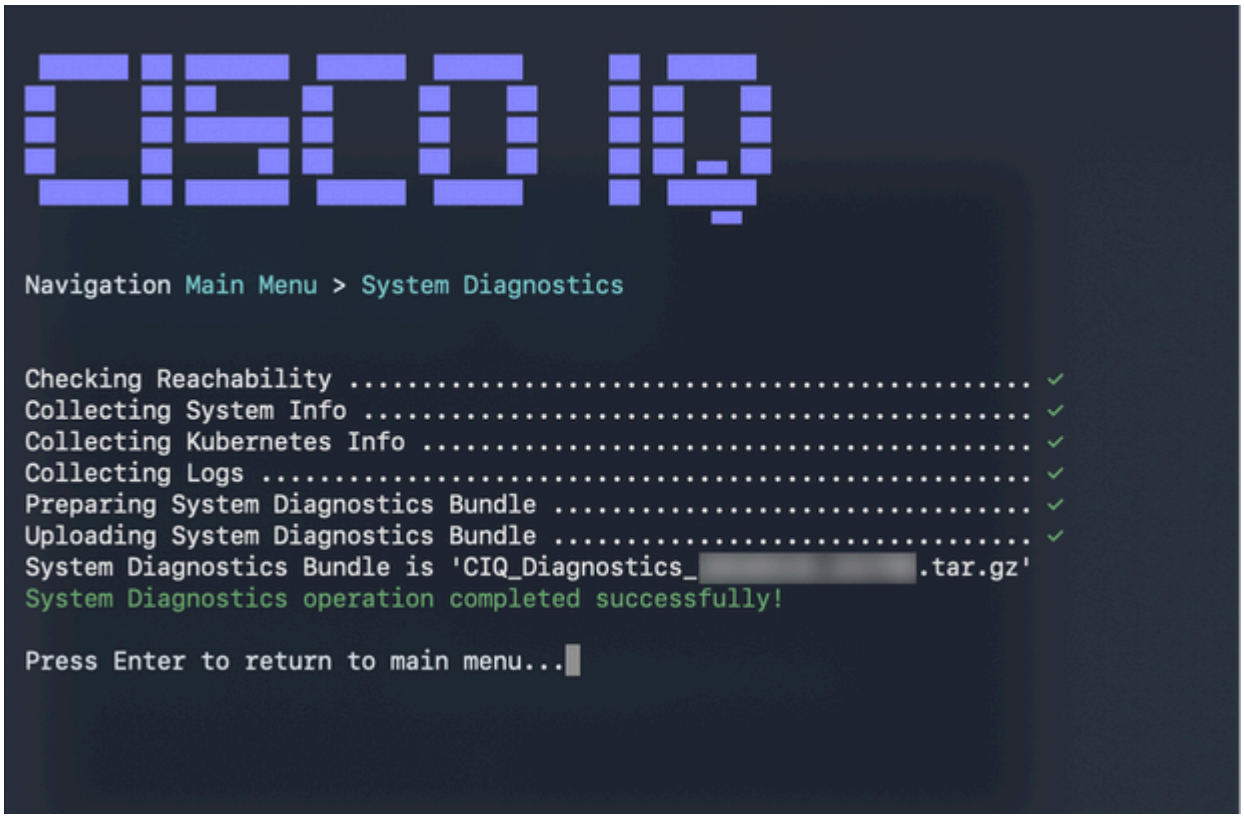
1. Accedere a Cisco IQ.


Menu principale

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


Diagnostica di sistema

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.




Operazione diagnostica di sistema completata

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).