

Guida al funzionamento di Cisco IQ Virtual Appliance 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 funzionalità di AI, come Cisco IQ AI Assistant, ottimizzano i risultati operativi e l'esperienza utente di Cisco IQ fornendo una comprensione contestuale che consente di prendere decisioni proattive e informate e di semplificare i processi per il coinvolgimento e il successo del cliente.

Cisco IQ On-Prem Air-Gapped è una delle modalità di implementazione di Cisco IQ, progettata per i clienti in settori altamente regolamentati con rigorosi requisiti di conformità, sovranità sui dati e sicurezza. In questa modalità, Cisco IQ viene fornito come macchina virtuale (VM) indipendente, nota come Cisco IQ Virtual Appliance (VA). Il VA è interamente gestito presso la sede del cliente ed è completamente isolato dalle reti esterne. Per mantenere questo isolamento, gli aggiornamenti software e i pacchetti di manutenzione vengono ottenuti da Cisco IQ SaaS e trasferiti all'appliance VA tramite un processo manuale approvato.

Cisco IQ On-Prem Air-Gapped estende le funzionalità chiave di Cisco IQ SaaS agli ambienti con air-gapped, consentendo ai team mission-critical di operare con velocità e intelligenza diagnostica paragonabili a quelle delle aziende connesse al cloud.

Per accedere a Cisco IQ VA, aprire un browser supportato e selezionare <https://<fqdn-of-the-appliance>>. Effettuare l'accesso utilizzando il nome utente e la password di amministratore impostati durante il processo di installazione.

 Nota: Cisco IQ VA è attualmente limitato ai clienti iscritti al programma Controlled Availability. L'accesso per il download del software di sistema VA e di pacchetti operativi aggiuntivi (moduli, regole e autorizzazioni) dal portale Cisco IQ è disponibile esclusivamente per determinati clienti. Per ulteriori informazioni, contattare il rappresentante commerciale.

Gestione connessione (raccolta dati)

Cisco IQ VA è una soluzione on-premises per la raccolta dei dati di rete che offre una visibilità completa sull'infrastruttura. Raccoglie i dati tramite Catalyst Center e Direct Connection. Semplifica la gestione dell'autenticazione di rete e dell'individuazione dei dispositivi. La

configurazione della raccolta dati è costituita da:

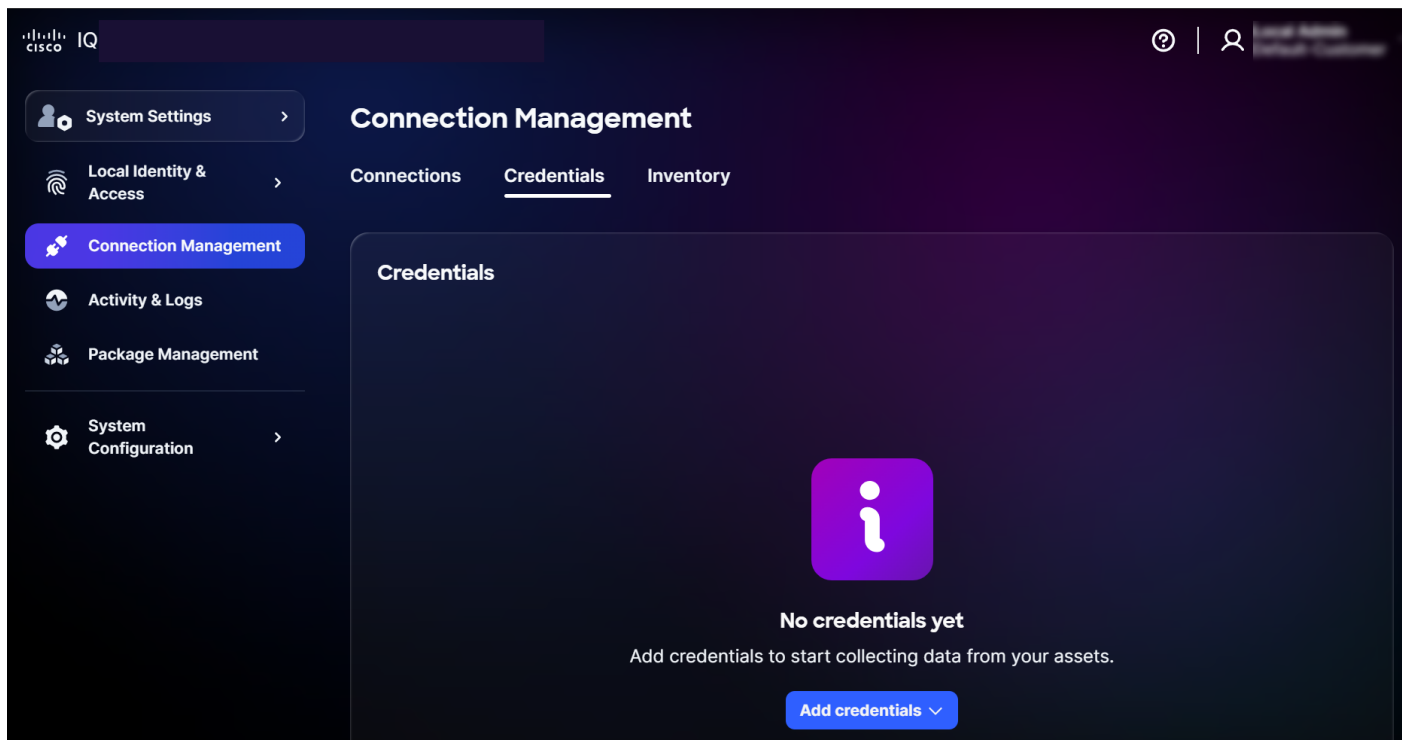
- Creazione di set di credenziali: Stabilire i protocolli di autenticazione (ad esempio, SNMP (Simple Network Management Protocol) v1/v2c/v3) per comunicare con i dispositivi di rete. La centralizzazione delle credenziali in base all'area di protezione o alla posizione (ad esempio, "SanJose-SNMPv3") 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

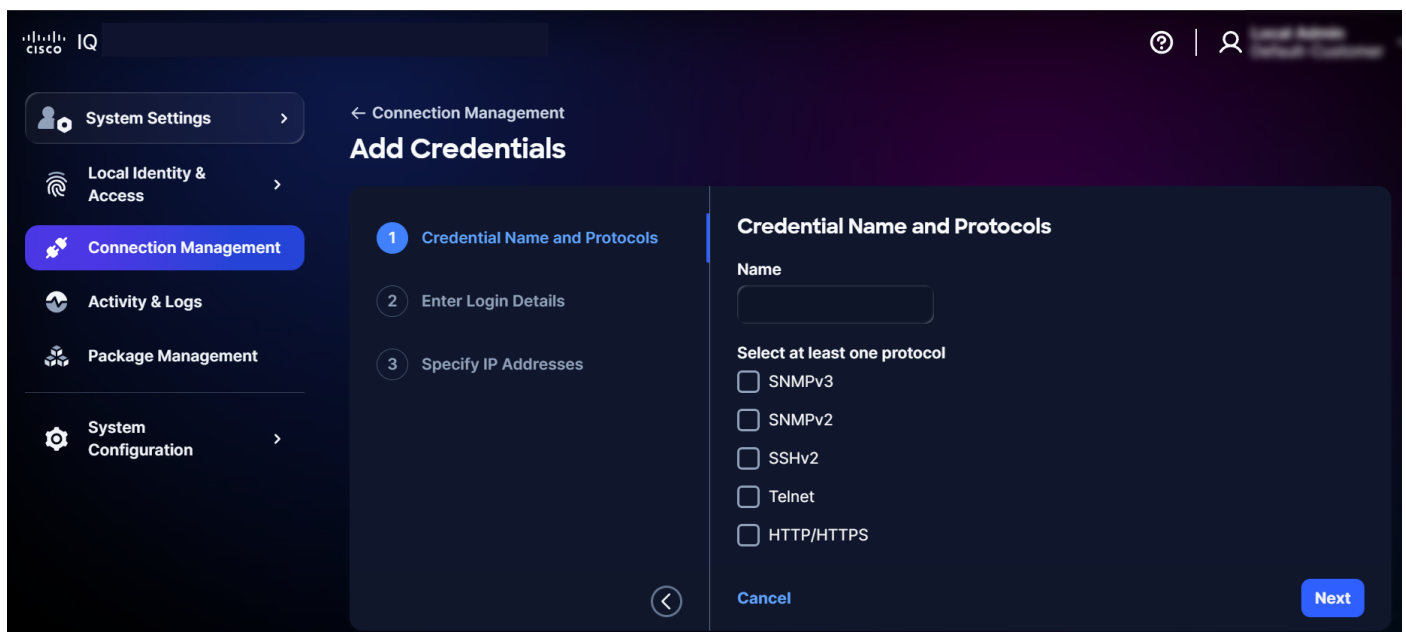
Per eseguire la raccolta dei dati, è innanzitutto necessario aggiungere le credenziali. Per aggiungere le credenziali:

1. Da Impostazioni di sistema, scegliere Gestione connessione. Viene visualizzata la pagina Gestione connessione.
2. Fare clic sulla scheda Credenziali.



Scheda Credeniali

3. Fare clic su Aggiungi credenziali.



Aggiungi credenziali

4. Immettere un nome.

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

6. Fare clic su Next (Avanti).

The screenshot shows the 'Add Credentials' window in the Cisco IQ Link interface. The left sidebar contains navigation options: System Settings, Local Identity & Access, Connection Management (highlighted), Activity & Logs, Package Management, and System Configuration. The main panel has three steps: 1. Credential Name and Protocols, 2. Enter Login Details, and 3. Specify IP Addresses. Step 2 is active. The 'Enter Login Details' section is for the 'SNMPv3' protocol and includes fields for Username, Engine ID (optional), Authorization algorithm, Authorization password (with a 'Show' button), Privacy algorithm (optional), and Privacy password (with a 'Show' button). At the bottom, there are 'Back' and 'Next' buttons.

Aggiungi dettagli credenziali

 Nota: Nell'immagine precedente è illustrata la visualizzazione quando sono selezionati tutti i protocolli nel passaggio precedente. L'interfaccia visualizza solo i protocolli selezionati.

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

8. Fare clic su Next (Avanti).

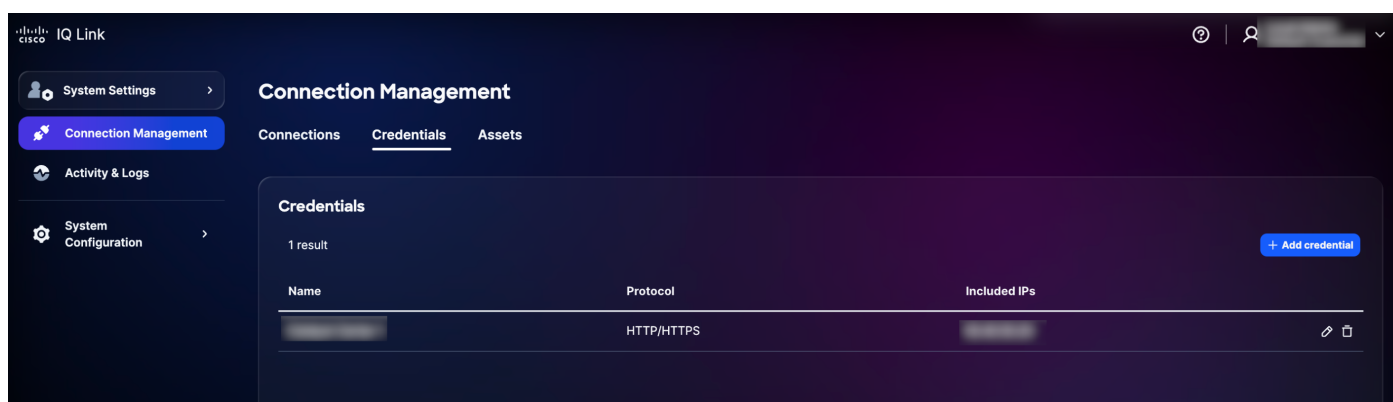
The screenshot shows the 'Add Credentials' window in the Cisco IQ Link interface, specifically the 'Specify IP Addresses' step. The left sidebar is the same as in the previous screenshot. The main panel shows three steps: 1. Credential Name and Protocols, 2. Enter Login Details, and 3. Specify IP Addresses. Step 3 is active. The 'Specify IP Addresses' section has a text area for 'Included IPs' with a placeholder example: 'e.g. *-*-*, 192.168.1.0/24, 172.16.*.*'. At the bottom, there are 'Back', 'Save and add another credential', and 'Save' buttons.

Specifica indirizzi IP

9. Immettere gli IP inclusi.

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

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



Credenziali aggiunte

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

Selezione credenziali e logica di corrispondenza

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

- **Livello di priorità:** Quando a un dispositivo vengono applicati più set di credenziali, Cisco IQ li valuta in base alla corrispondenza specifica con il dispositivo; il sistema applica la seguente priorità, con le corrispondenze più specifiche che hanno la precedenza:
 - **Corrispondenza esatta IP:** Priorità massima
 - **Match con caratteri jolly:** la priorità dipende dal numero di stelle finali; meno stelle indicano una corrispondenza più specifica e quindi una priorità più alta

- Regole di formattazione con caratteri jolly: I caratteri jolly (*) sono supportati solo come caratteri finali negli indirizzi IP. devono essere applicati da destra a sinistra.
 - Formati supportati:
 - 1.2.3.* (priorità massima)
 - 1.2.*
 - 1.*.*
 - *.*.* (priorità più bassa)
 - 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 1: 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)

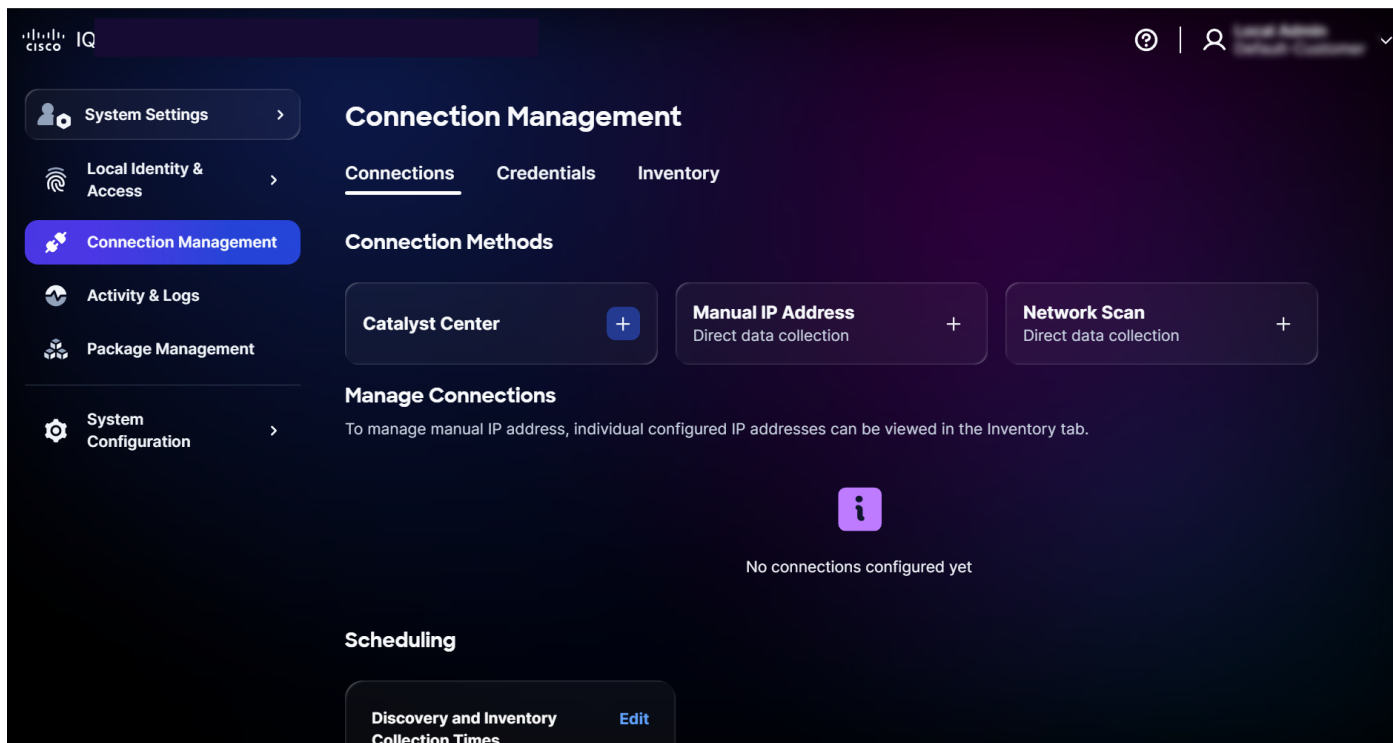
 Nota: Se un dispositivo rientra in più categorie sovrapposte, il sistema seleziona sempre il set di credenziali con la più alta specificità (in altre parole, il minor numero di caratteri jolly finali).

Raccolta dei dati tramite Catalyst Center

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

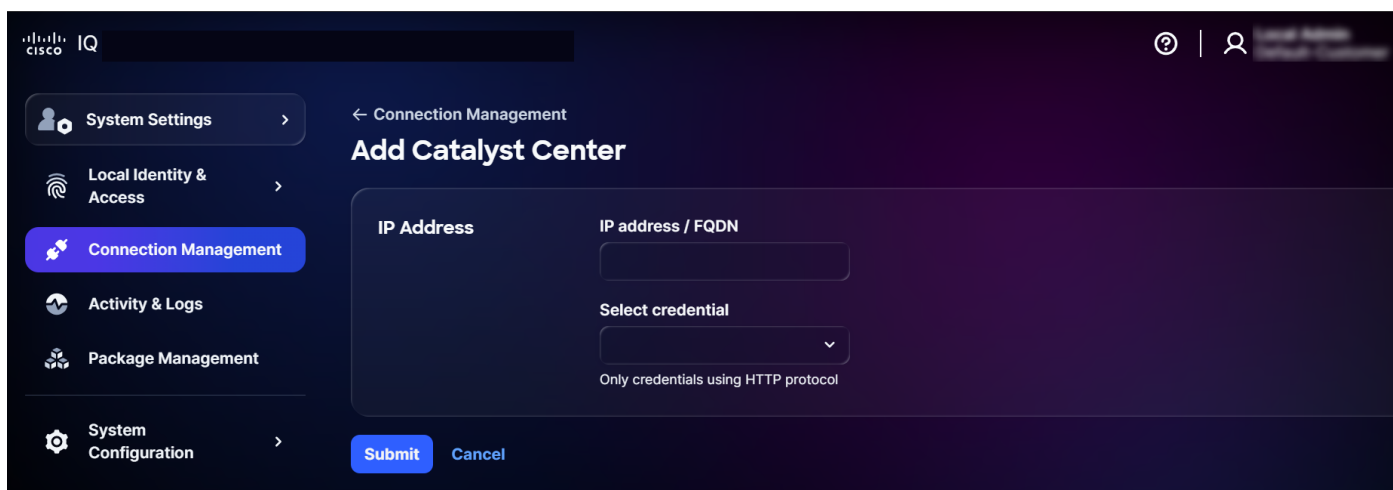
Per la raccolta dei dati con Catalyst Center:

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

configurate.

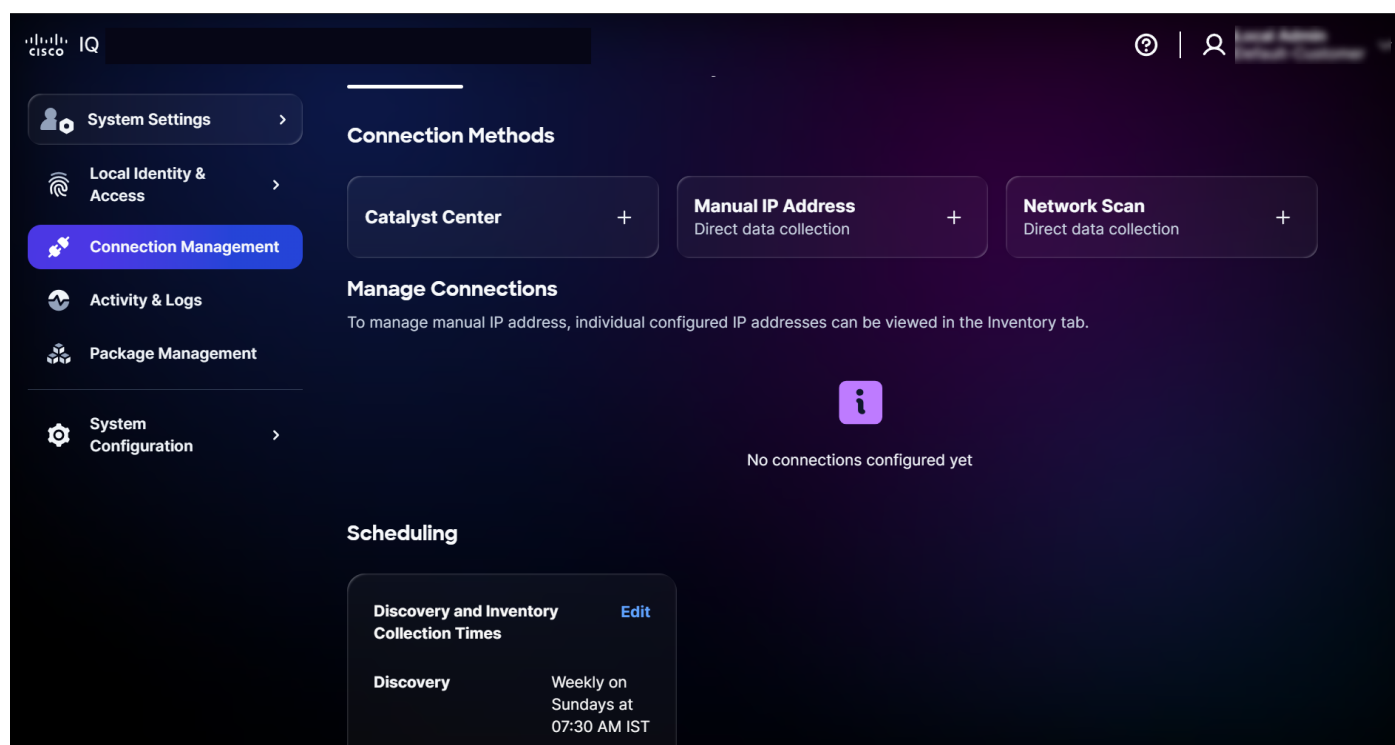
6. Pianificare una raccolta. Per ulteriori informazioni, vedere [Pianificazione](#).

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

Raccolta manuale dei dati

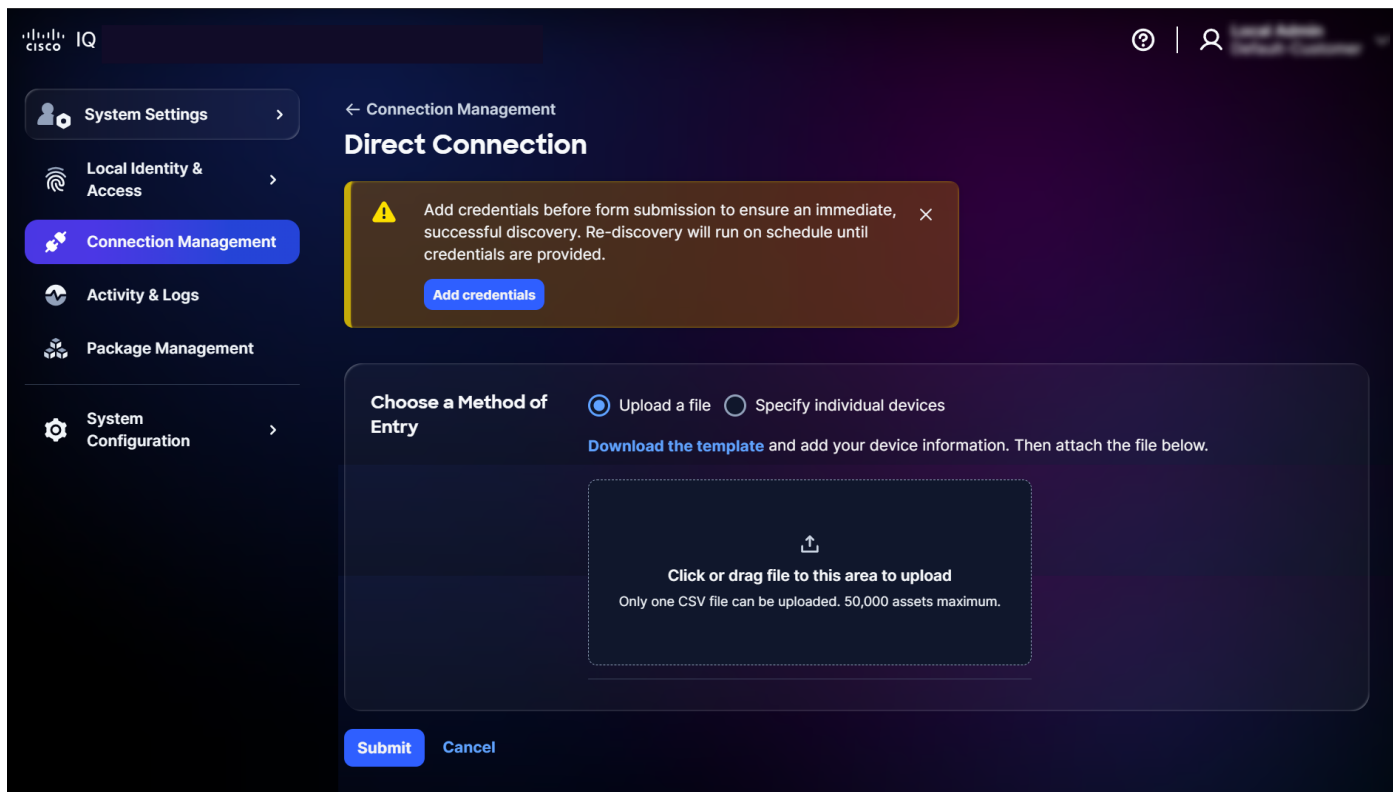
Per aggiungere dispositivi per la connessione dati diretta:

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



Gestione connessione

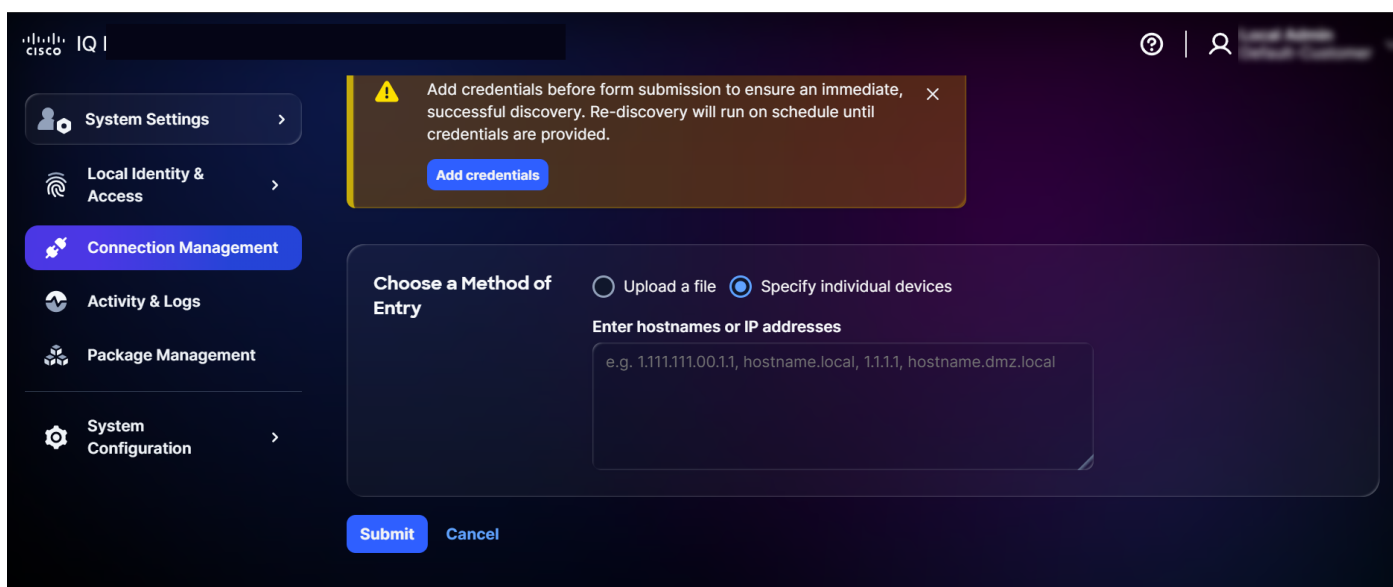
2. Fare clic su Manual IP Address (Indirizzo IP manuale). Viene visualizzata la pagina Connessione diretta con due (2) opzioni per la raccolta dei dati.



Carica file

3. Fare clic sull'opzione preferita da Choose a Method of Entry (Scegli metodo di immissione) e fornire le informazioni sul dispositivo utilizzando uno dei metodi seguenti:

- Carica file: Fare clic o trascinare il file



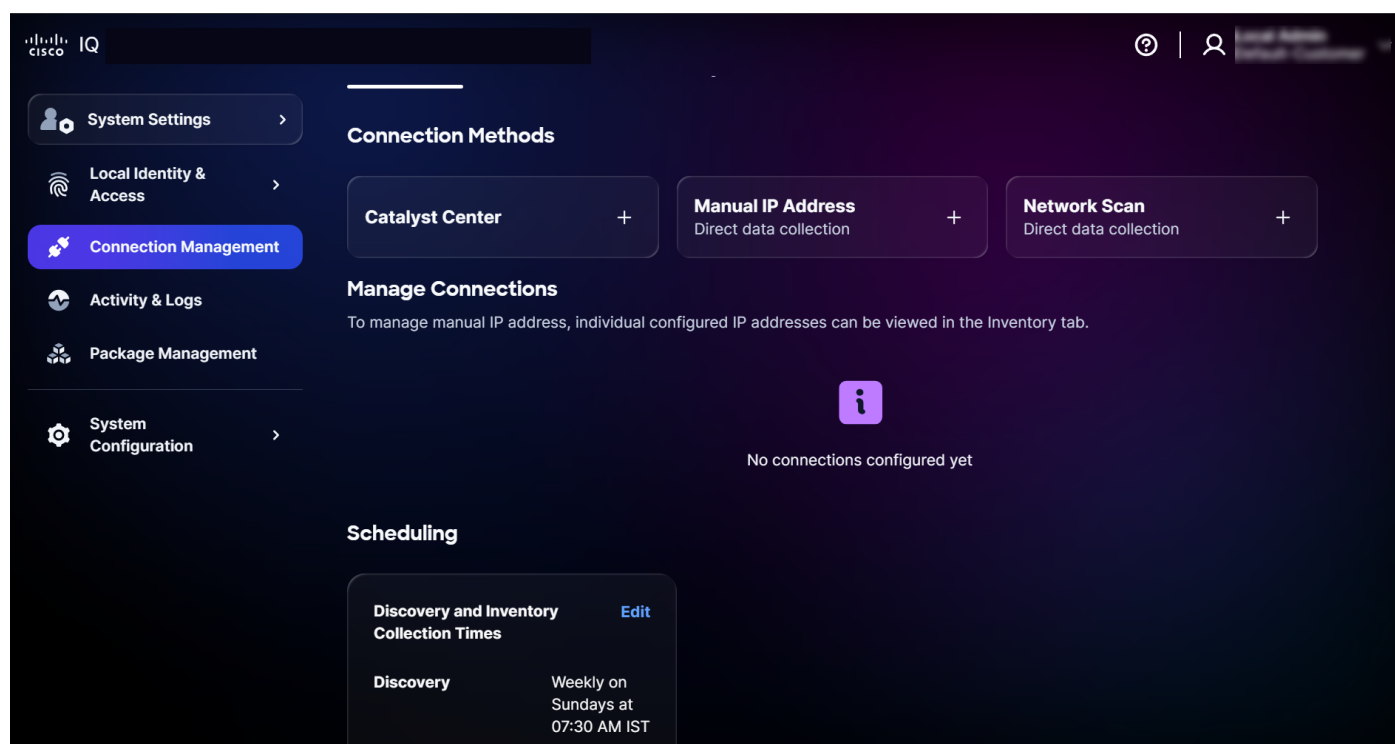
Specificare i singoli dispositivi

- Specificare i singoli dispositivi: Immettere un nome host, un indirizzo IP o un elenco delimitato da virgole di nomi host e/o indirizzi IP
4. Fare clic su Invia. Dopo l'invio, l'utente viene reindirizzato alla scheda Asset.
 5. Pianificare una raccolta. Per ulteriori informazioni, vedere [Pianificazione](#).

 Nota: Cisco IQ VA 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.

Scansione della rete

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



Scansione della rete

2. Fare clic su Scansione rete. Viene visualizzata la pagina Connetti risorse per scansione di rete con tre (3) opzioni.

System Settings >

Local Identity & Access >

Connection Management

Activity & Logs

Package Management

System Configuration >

← Connection Management

Connect Assets by Network Scan

Scan Method

☒ Specify IP Range ☐ Specify Discovery Protocol (CDP/LLDP) ☐ File Upload

Name

IP Start **IP End**

Schedule Scan

Frequency **Time**

Connect assets **Cancel**

- Specifica intervallo IP: Definire un intervallo di indirizzi IP per i dispositivi di destinazione compresi nell'intervallo per l'individuazione della rete o le attività di gestione
- Specificare il protocollo Discovery Protocol (CDP/LLDP): Scegliere il protocollo di individuazione della rete da utilizzare
- Caricamento file: Caricare un file, ad esempio file di configurazione o dati

3. Immettere il nome.

4. Immettere IP Start e IP End.

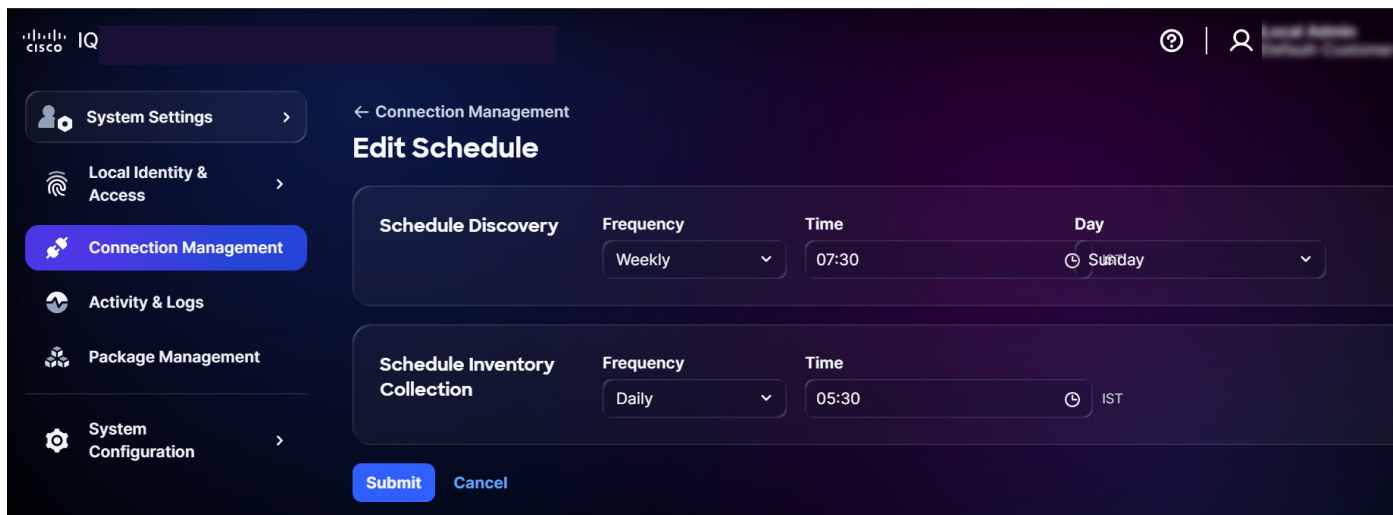
5. In Pianifica scansione, scegliere Frequenza e ora.

6. Fare clic su Connetti risorse.

Programmazione

La programmazione consente di definire quando Cisco IQ VA 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 Virtual Appliance le modifiche apportate alle pianificazioni di individuazione e raccolta.

Installazione di pacchetti (moduli, regole e autorizzazioni)

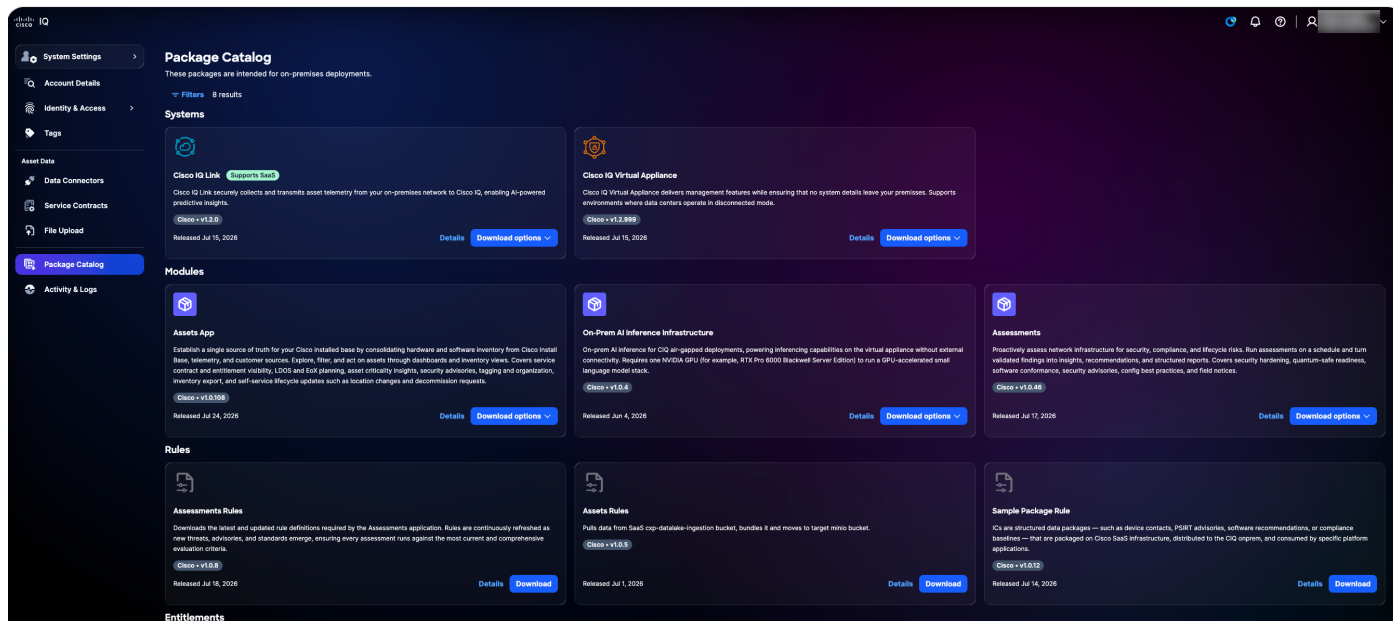
È possibile gestire il ciclo di vita del software (ovvero l'installazione e la configurazione) di moduli operativi, regole, diritti e funzionalità specializzate basate su IA all'interno di VA. È possibile installarle scaricando le versioni più recenti da Cisco IQ (SaaS) e passando al catalogo pacchetti. Nel Catalogo pacchetti vengono visualizzate le istanze software disponibili. Consente di monitorare e gestire gli aggiornamenti senza problemi, garantendo un monitoraggio e una gestione efficienti delle istanze del sistema.

Aggiunta di moduli

Un modulo è un pacchetto software standalone che fornisce funzionalità di base all'interno del VA. Si tratta di un servizio indipendente con un proprio ciclo di vita, che consente l'installazione, la manutenzione e il ridimensionamento. L'utilizzo delle risorse, inclusi CPU, GPU (Graphics Processing Unit) e RAM, viene assegnato dinamicamente in base alle dimensioni di distribuzione

(Piccola, Media o Grande) selezionate durante l'installazione iniziale.

1. Accedere a [Cisco IQ](#).
2. Passare a Impostazioni di sistema > Catalogo package.

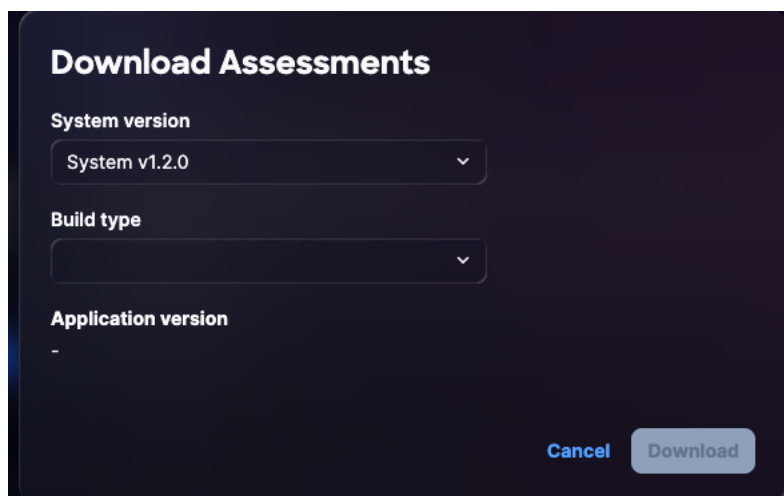


Catalogo pacchetto

3. Dalla scheda del modulo desiderata, fare clic su Download options > Installation packages (Opzioni di download > Pacchetti di installazione). Viene visualizzata la finestra Download.



Nota: Per le immagini di esempio viene utilizzato il modulo Assessment.



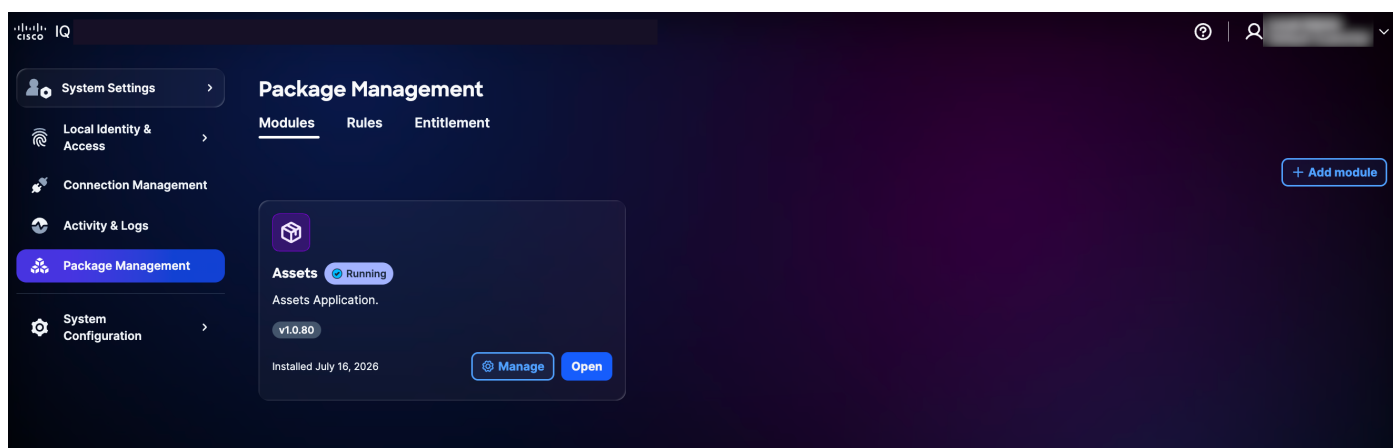
Scarica

4. Selezionare una Versione sistema dall'elenco a discesa.
5. Selezionare un tipo di generazione dall'elenco a discesa.
6. Fare clic su Download per salvare il file localmente.



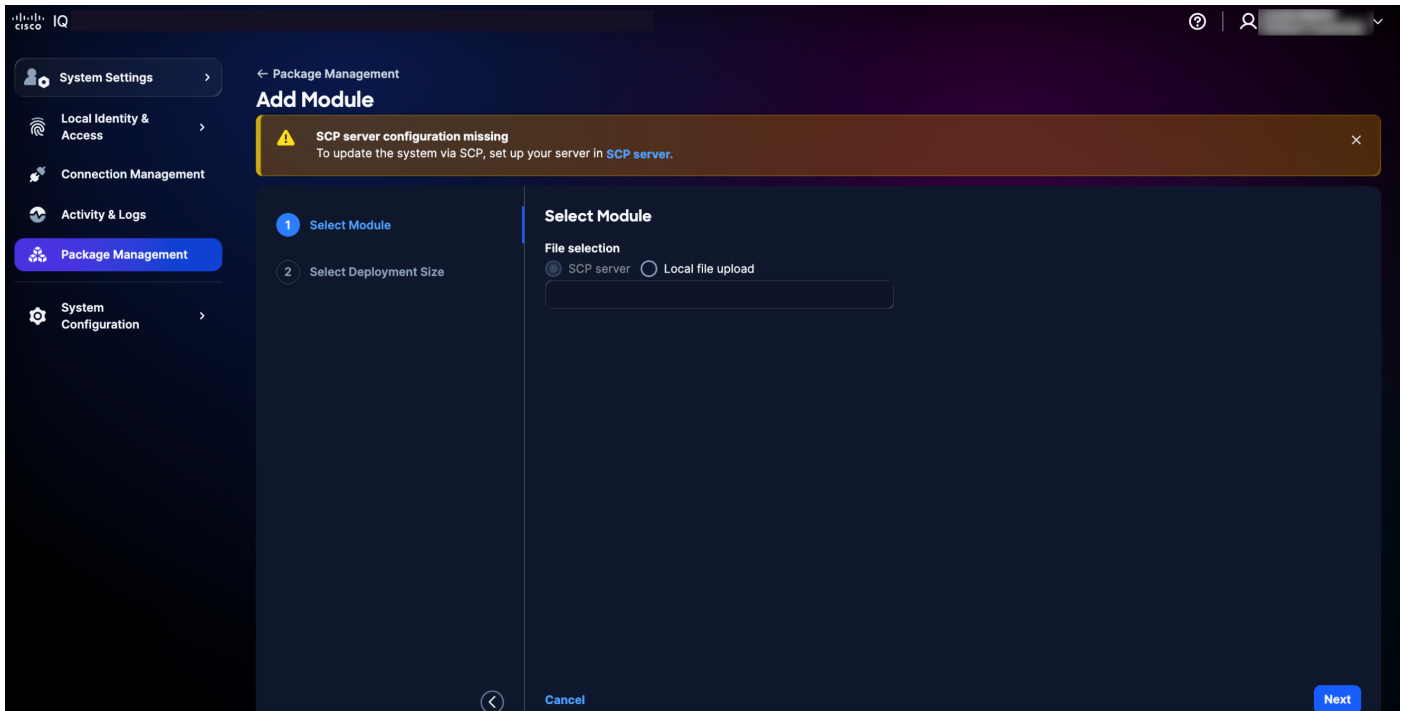
Nota: I file di installazione sono di grandi dimensioni (10-25 GB); assicurarsi di disporre di spazio su disco sufficiente prima di eseguire il download.

7. Passare a VA.
8. Passare a Home > Impostazioni di sistema > Gestione pacchetti. Viene visualizzata la pagina Gestione package con le schede riportate di seguito.
 - Moduli
 - Regole
 - Diritti



Moduli

9. Fare clic su Aggiungi modulo.

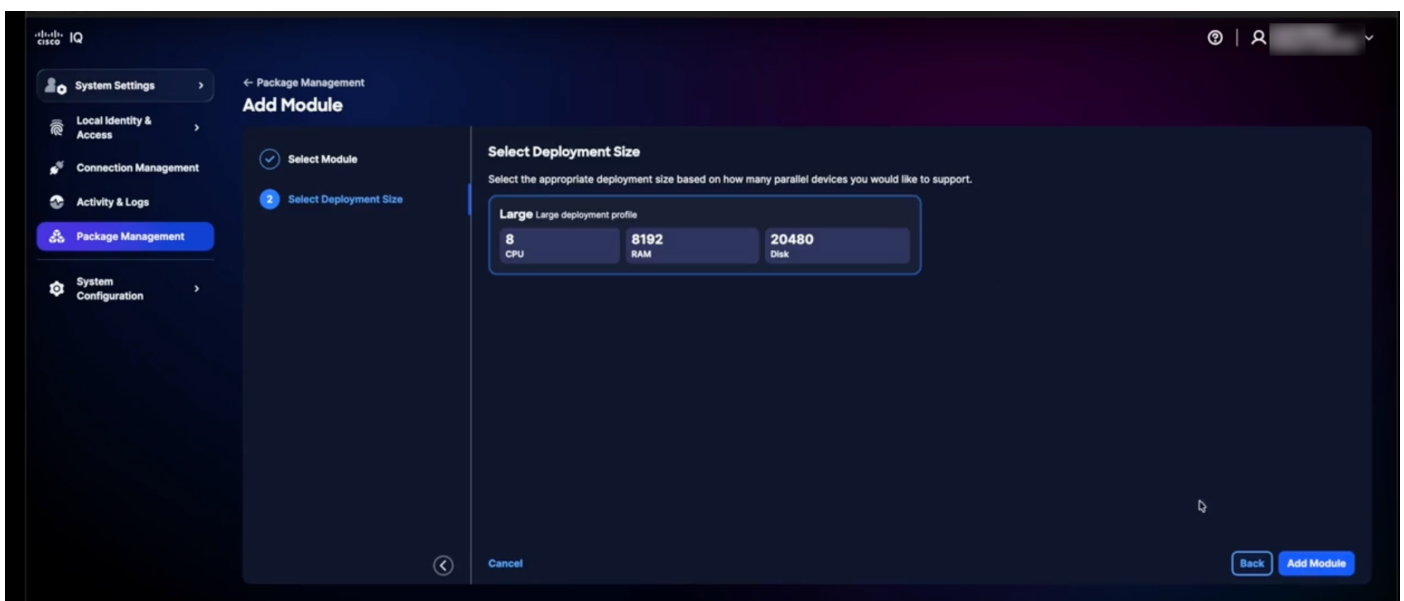


Aggiungi modulo

10. Scegliere l'opzione di selezione dei file desiderata:

- Server SCP: Immettere il nome esatto del pacchetto di installazione (consigliato per i file di grandi dimensioni)
- Caricamento file locale: Trascina il file di installazione scaricato (non consigliato per file di 30 GB o superiori a causa del tempo di caricamento)

11. Fare clic su Next (Avanti).

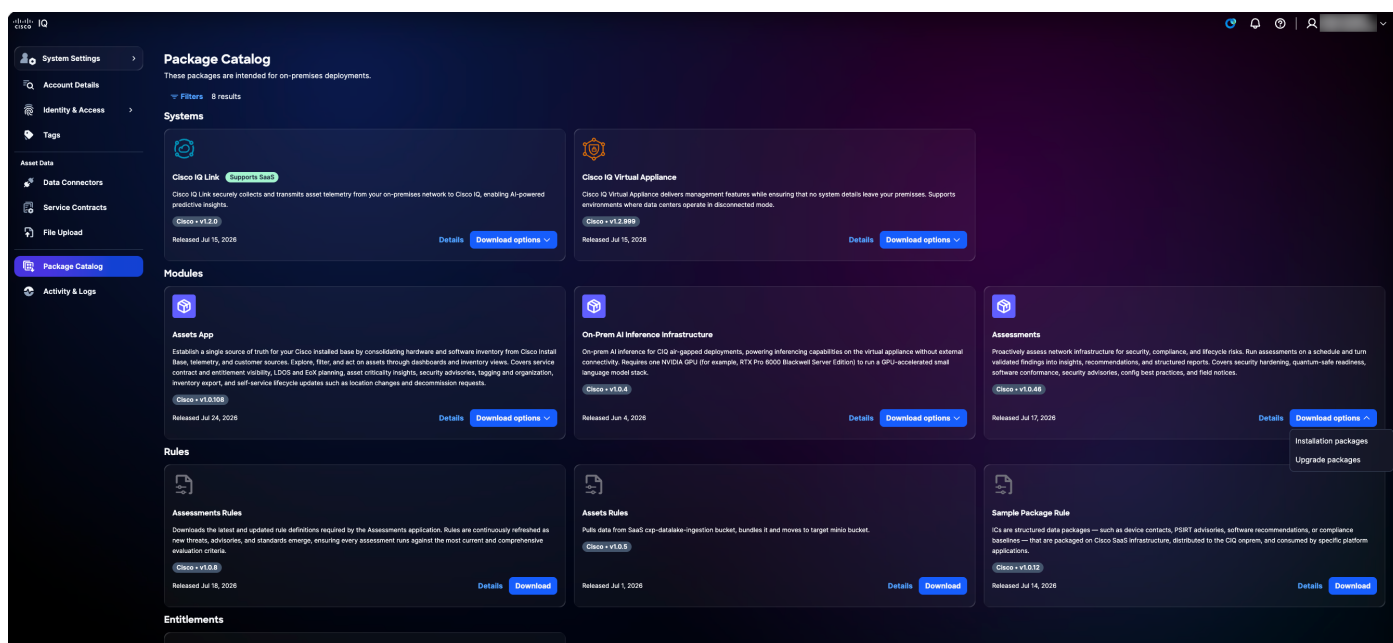


Dimensioni distribuzione

- Scegliere le dimensioni della distribuzione, ad esempio Piccola, Media o Grande. Queste dimensioni sono predefinite e determinano i requisiti delle risorse.
- Fare clic su Add Module. Il modulo appena installato viene visualizzato nella scheda Moduli in Gestione pacchetti. Una volta completato, lo stato del modulo cambia in "In esecuzione" e diventa disponibile il pulsante Apri.

Aggiornamento di un modulo

I moduli più recenti vengono continuamente aggiornati nel catalogo pacchetti (in Cisco IQ). Per eseguire l'aggiornamento alla versione più recente:



Connetti risorse tramite analisi della rete

- Dalla scheda del modulo desiderata, fare clic su Download options (Opzioni di download) > Upgrade packages (Pacchetti di aggiornamento). Viene visualizzata la finestra Download.



Nota: Il modulo Assessment viene utilizzato come esempio per le immagini.

Upgrade Assessments

System version

System v1.2.0



Current app version



Build type



Application version

-

Cancel

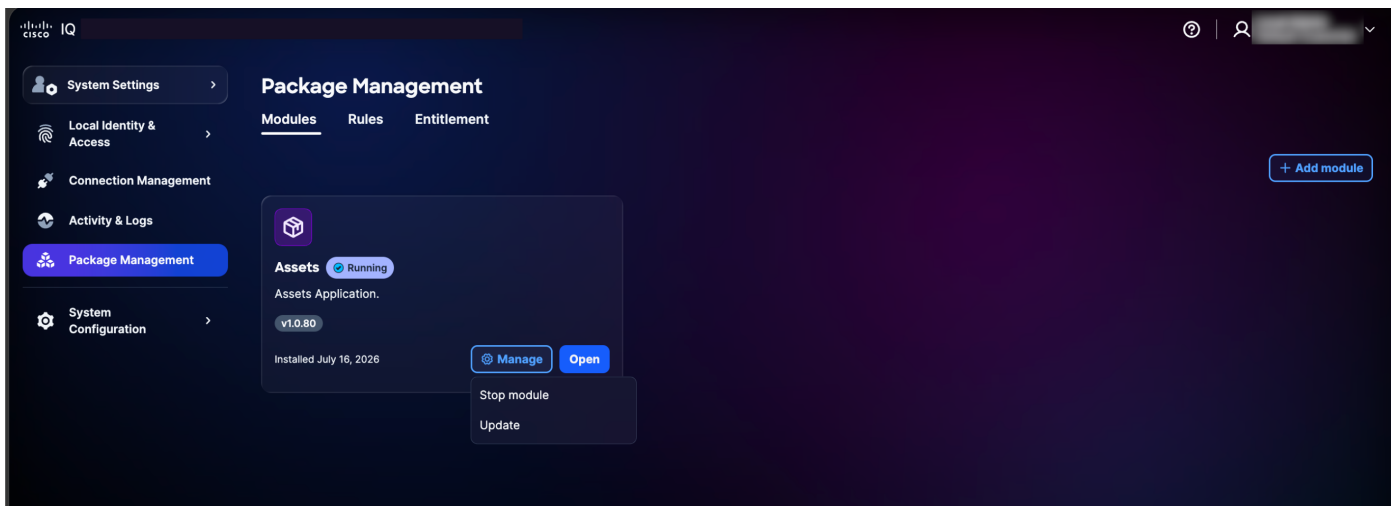
Download

Scarica

2. Selezionare una versione di sistema dall'elenco a discesa.
3. Scegliere una versione corrente dell'app dall'elenco a discesa.
4. Selezionare un tipo di generazione dall'elenco a discesa.
5. Fare clic su Download per salvare il file localmente.
6. Passare a VA e completare l'installazione del file scaricato.

Gestione dei moduli

Dopo aver aggiunto un modulo, è possibile modificarlo dalla pagina Gestione package facendo clic su Gestisci. Le opzioni di modifica disponibili includono il ridimensionamento e l'aggiornamento a una versione superiore. Per gestire un modulo:



Tipo di aggiornamento

1. Dalla pagina Gestione package, fare clic su Gestisci > Aggiorna per il modulo desiderato.
2. Scegliere il tipo di aggiornamento:
 - Modifica solo le dimensioni della distribuzione
 - Aggiorna versione
3. Se è selezionata l'opzione Cambia dimensioni distribuzione, fare clic su Avanti e scegliere le nuove dimensioni di distribuzione nella pagina seguente.

O

Se si seleziona Aggiorna versione, viene visualizzata l'opzione Selezione file. Scegliere SCP Server e immettere il nome esatto del pacchetto di installazione oppure scegliere Caricamento file locale e trascinare il file di installazione scaricato.

4. Fare clic su Next (Avanti). Viene visualizzata la pagina Seleziona pianificazione aggiornamento.
5. Per aggiornare la programmazione, scegliere una delle seguenti opzioni del pulsante di opzione:
 - Aggiorna
 - Aggiorna in seguito



Nota: Alcuni moduli supportano gli aggiornamenti senza downtime. Se è necessario interrompere l'attività, i dettagli verranno visualizzati in un banner.

6. Se si seleziona Aggiorna in seguito, immettere la data e l'ora.

7. Fare clic su Next (Avanti). Viene visualizzato il Riepilogo aggiornamento.

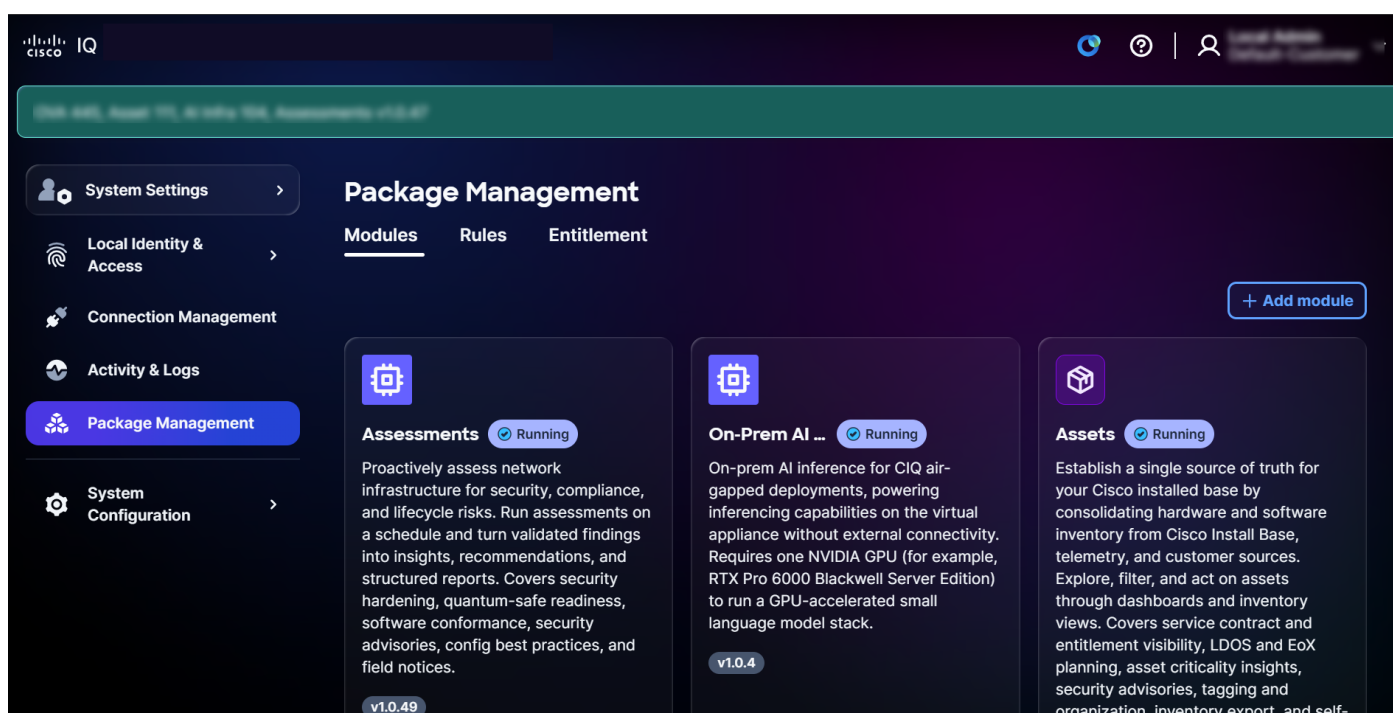


Nota: È possibile accedere alle note sulla versione dal Riepilogo aggiornamenti.

8. Fare clic su Aggiorna modulo e passare alla scheda Modulo. Nel modulo viene visualizzato lo stato "aggiornamento pianificato".

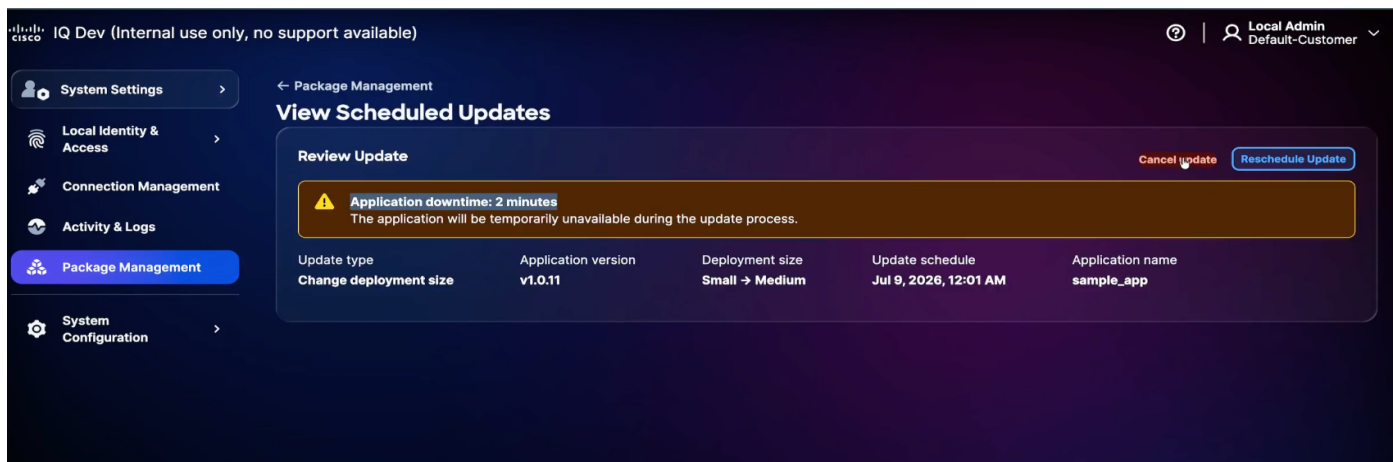
Modifica delle programmazioni

È inoltre possibile visualizzare, modificare o annullare gli aggiornamenti pianificati. Per modificare o annullare un aggiornamento pianificato:



Modifica della pianificazione

1. Dalla pagina Gestione package, fare clic su Gestisci > Visualizza aggiornamento pianificato del modulo desiderato. Viene visualizzata la finestra Visualizza aggiornamenti pianificati.



Pianifica aggiornamenti

2. Fare clic su Annulla aggiornamento o su Riprogramma aggiornamento come richiesto.
3. Seguire le istruzioni visualizzate sullo schermo per completare le operazioni.



Nota: Se un'operazione del modulo (ad esempio, l'installazione, l'aggiornamento o il ridimensionamento) ha esito negativo, scegliere una delle opzioni seguenti:

Riprova: Nell'interfaccia utente viene visualizzato il pulsante Riprova, che consente di ripetere l'operazione. Registri: Se un errore persiste, fare clic su Registri per visualizzare informazioni di diagnostica dettagliate. Questo è il metodo principale per identificare la causa degli errori di installazione o di runtime.

Installazione delle regole

Una regola è un componente specializzato o un componente aggiuntivo che estende o modifica la funzionalità di un modulo esistente. Le regole non sono concepite per funzionare come programmi autonomi; sono "collegati" a un modulo per fornire regole, logiche o funzionalità specifiche. Le regole sono legate a moduli specifici. Quando una regola viene installata, viene collegata al modulo supportato. Le regole consentono di aggiornare o personalizzare il sistema senza richiedere un aggiornamento completo del modulo principale. Se è necessario un nuovo insieme di regole o funzionalità, è sufficiente aggiungere una nuova regola al modulo esistente.

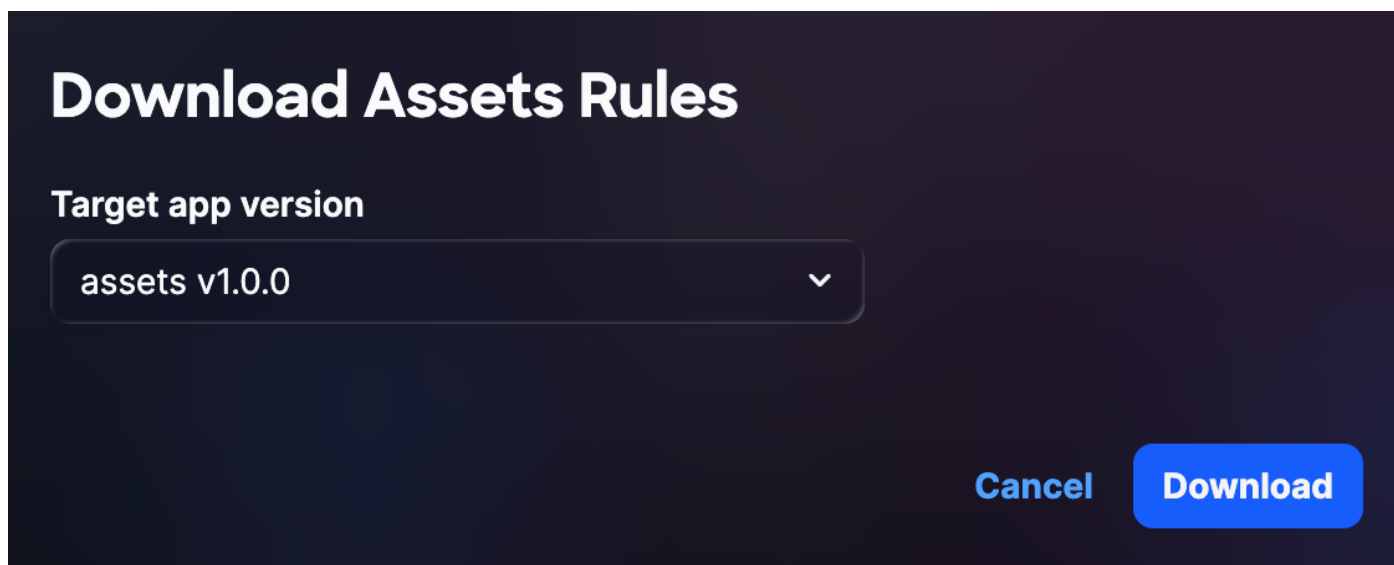
Per scaricare una regola:

1. Accedere a [Cisco IQ](#).
2. Passare a Impostazioni di sistema > Catalogo package.

3. Dalla scheda regole desiderata, fare clic su Download.



Nota: L'immagine di esempio seguente è relativa a una regola Assets.



Scarica

4. Scegliere una versione dell'app di destinazione dall'elenco a discesa.

5. Fare clic su Download per salvare il file localmente.



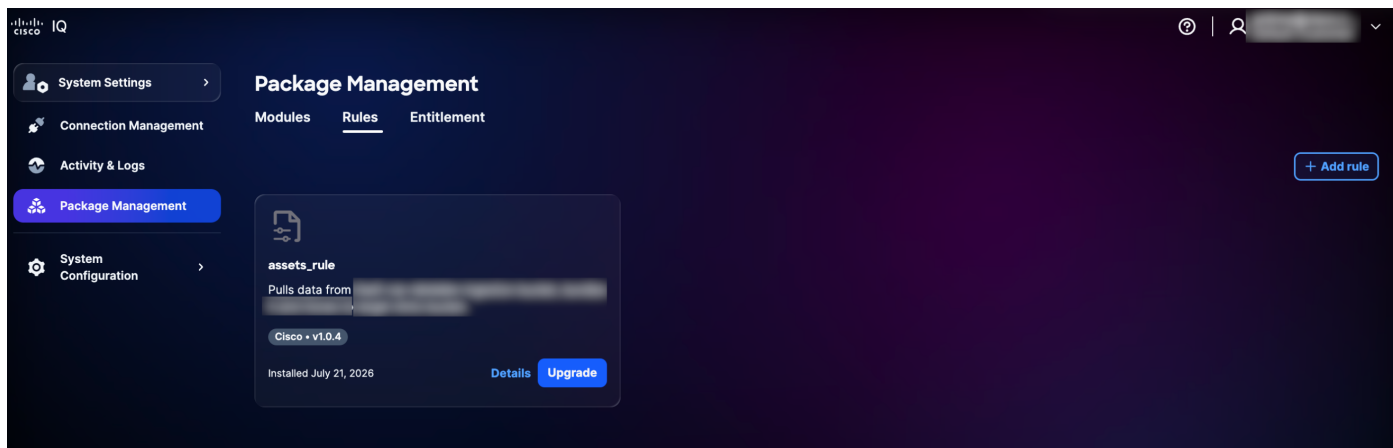
Nota: I file di installazione sono di grandi dimensioni (10-25 GB); assicurarsi di disporre di spazio su disco sufficiente prima di eseguire il download.

6. Passare a VA.

7. Passare a Home > Impostazioni di sistema > Gestione pacchetti. Viene visualizzata la pagina Gestione package con le schede riportate di seguito.

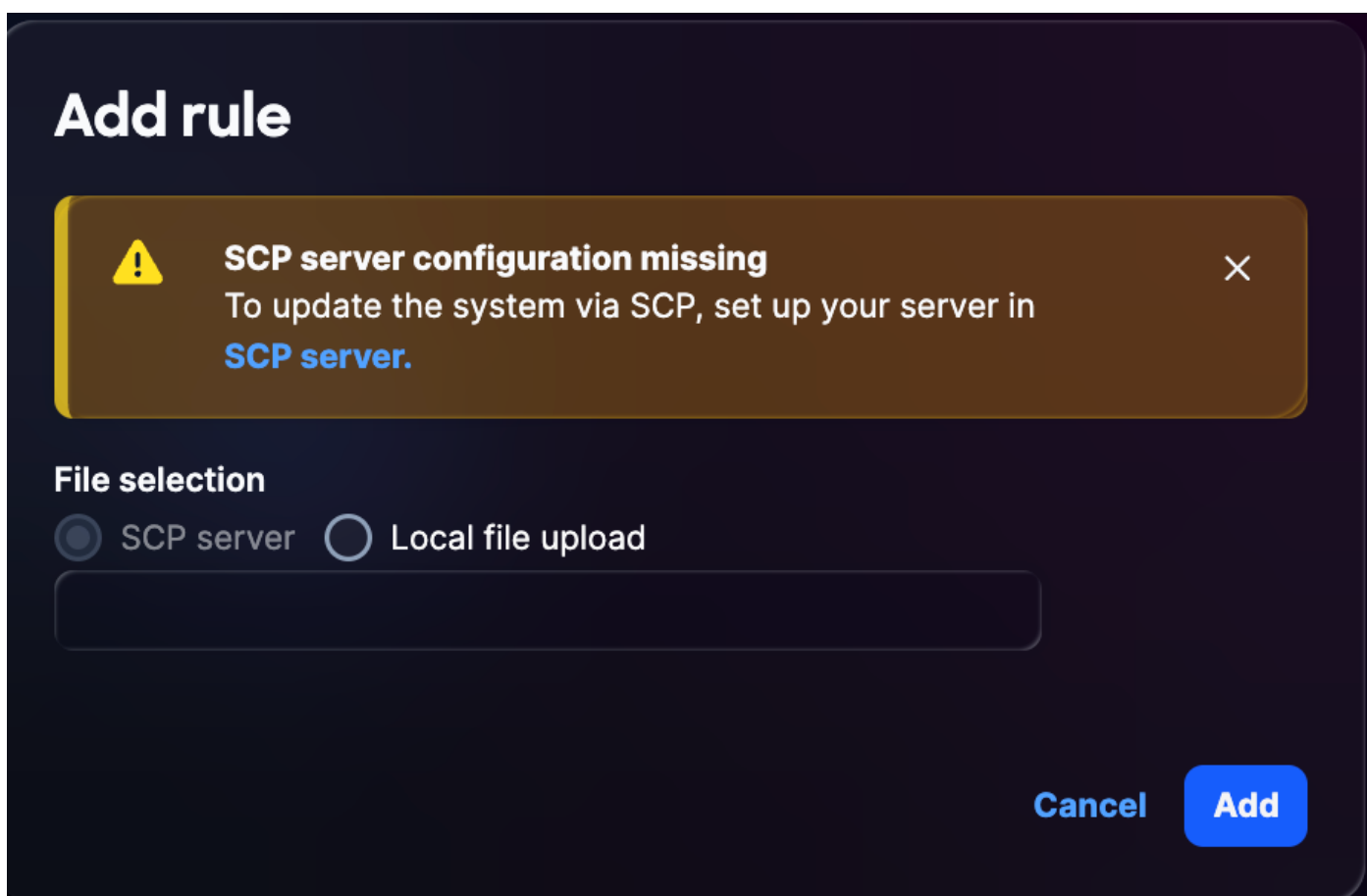
- Moduli
- Regole
- Diritti

8. Fare clic sulla scheda Regole.



Gestione pacchetti

9. Fare clic su Aggiungi regola.



Aggiungi regola

10. Scegliere l'opzione di selezione dei file desiderata:

- Server SCP (Secure Copy Protocol): Immettere il nome esatto del file del pacchetto di

installazione. Questo metodo è consigliato per i file di grandi dimensioni.

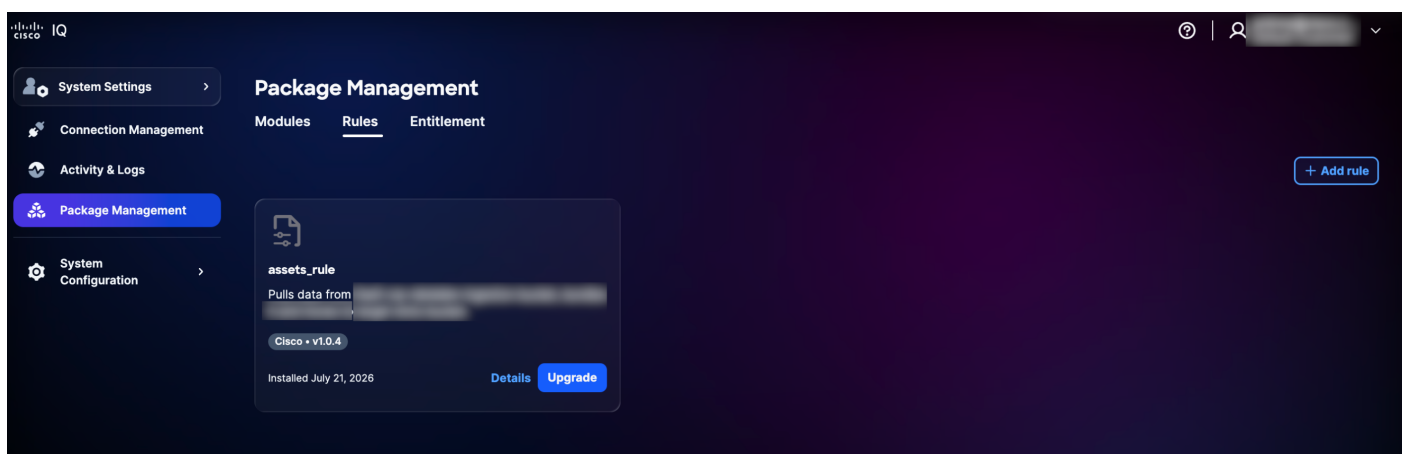
- Caricamento file locale: Trascinare il file di installazione scaricato.

11. Fare clic su Add. La regola aggiunta viene visualizzata in Gestione pacchetti.

Aggiornamento delle regole

Per aggiornare le regole:

1. Passare a Impostazioni di sistema > Gestione pacchetti in VA.



Aggiornamento

2. Dalla regola desiderata, fare clic su Aggiorna. Viene visualizzata la finestra Regola di aggiornamento.

Upgrade Rule

File selection

☒ SCP server ☐ Local file upload

Cancel

Add

Regola di aggiornamento

3. Scegliere l'opzione di selezione dei file desiderata:

- Server SCP (Secure Copy Protocol): Immettere il nome esatto del file del pacchetto di installazione. Questo metodo è consigliato per i file di grandi dimensioni.
- Caricamento file locale: Trascinare il file di installazione scaricato.

4. Fare clic su Add.

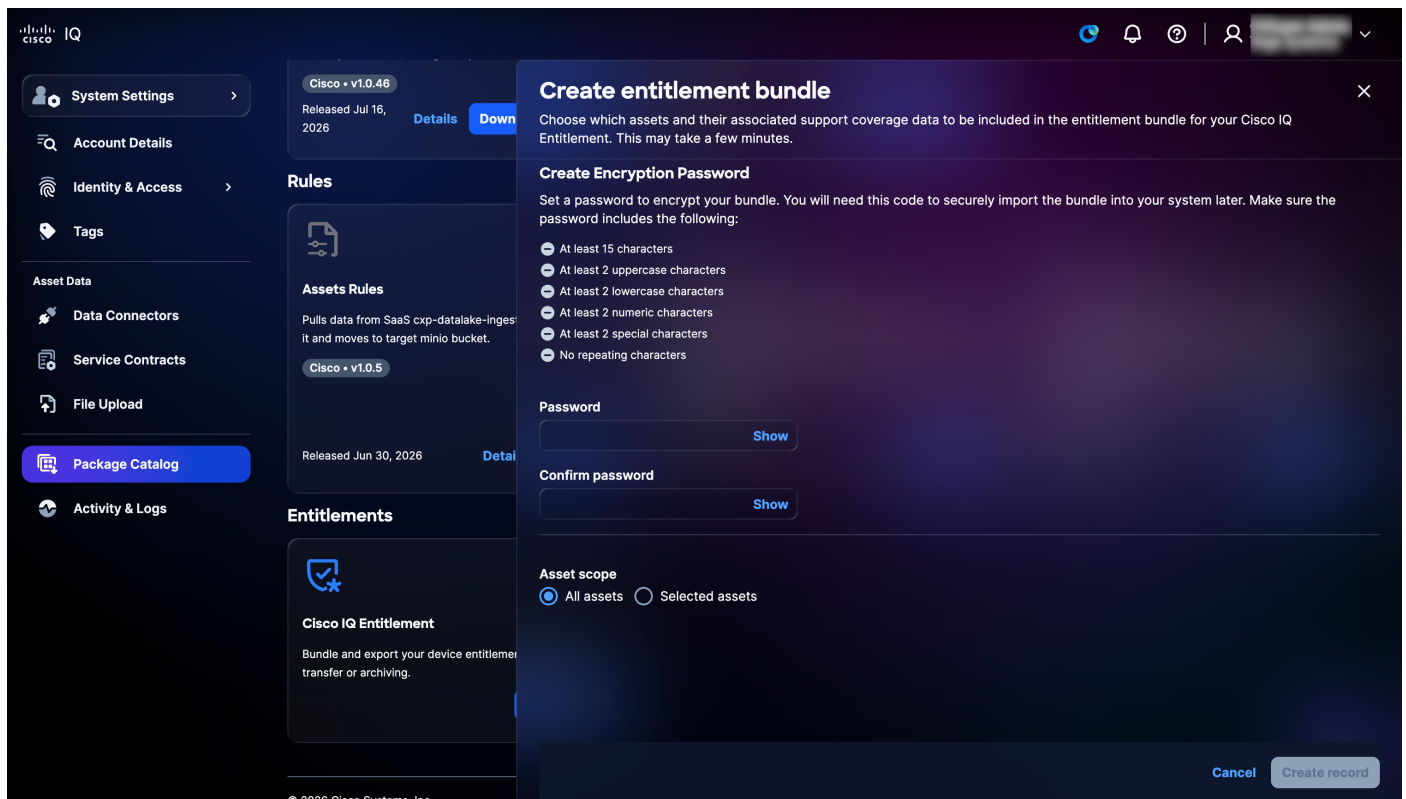


Nota: Queste regole vengono applicate alla raccolta di telemetria di dispositivi pianificati ricorrenti. Per un'applicazione immediata, è possibile avviare manualmente la raccolta di telemetria dei dispositivi.

Installazione delle autorizzazioni

La Documentazione di titolarità consente di convalidare il diritto dell'organizzazione di utilizzare funzionalità software, moduli o servizi specifici. Per installare un diritto:

1. Accedere a [Cisco IQ](#).
2. Passare a Impostazioni di sistema > Catalogo package.
3. Dalla scheda dei diritti fare clic su Crea record. Viene visualizzata la finestra Crea aggregazione diritti.



Crea pacchetto di autorizzazioni

4. Immettere una password. Fare riferimento alle regole per la creazione della password visualizzate sullo schermo.
5. Immettere nuovamente la stessa password in Conferma password.
6. Scegliere il pulsante di scelta Ambito asset preferito.
 - Tutti gli asset: Include tutti gli asset collegati all'utente
 - Risorse selezionate: Consente di scegliere dispositivi specifici allineati all'ambiente; se questa opzione è selezionata, selezionare le caselle di controllo di tutte le risorse applicabili
7. Fare clic su Crea record per salvare il file localmente.

 Nota: Dopo aver creato il pacchetto di autorizzazioni, non allontanatevi dalla schermata corrente. Se si passa a un'altra pagina, il bundle viene invalidato ed è necessario rigenerarlo per abilitare l'opzione di download.

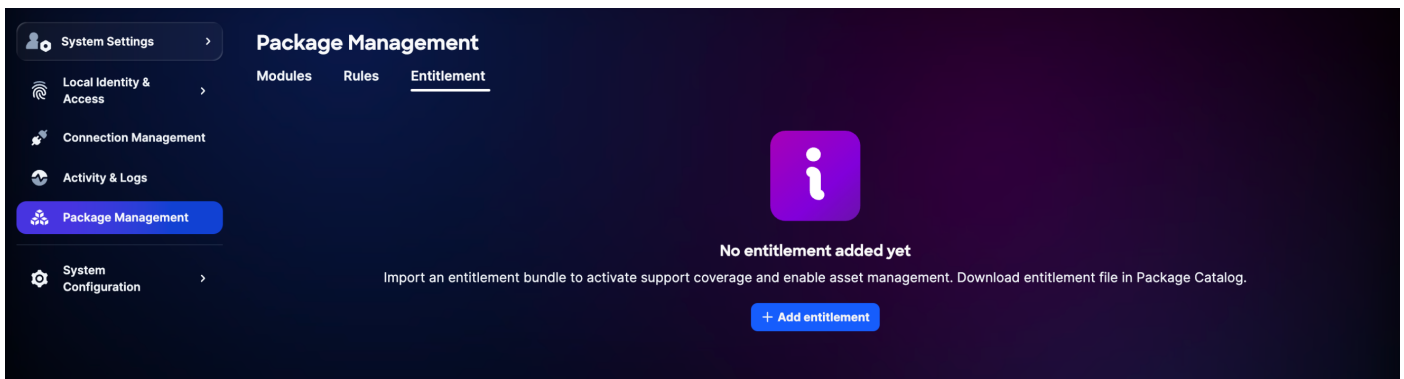
 Nota: I file di installazione sono di grandi dimensioni (10-25 GB); assicurarsi di disporre di spazio su disco sufficiente prima di eseguire il download.

8. Accedere a VA.

9. Passare a Home > Impostazioni di sistema > Gestione pacchetti. La pagina Gestione package contiene le schede riportate di seguito.

- Moduli
- Regole
- Diritti

10. Fare clic sulla scheda Diritti.



Scheda Diritto

11. Fare clic su Aggiungi diritto.

Add Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

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

Aggiungi diritto

12. Scegliere l'opzione di selezione dei file desiderata.

- Server SCP (Secure Copy Protocol): Immettere il nome esatto del file del pacchetto di installazione; questo metodo è consigliato per i file di grandi dimensioni
- Caricamento file locale: Trascinare il file di installazione scaricato

13. Immettere una password.

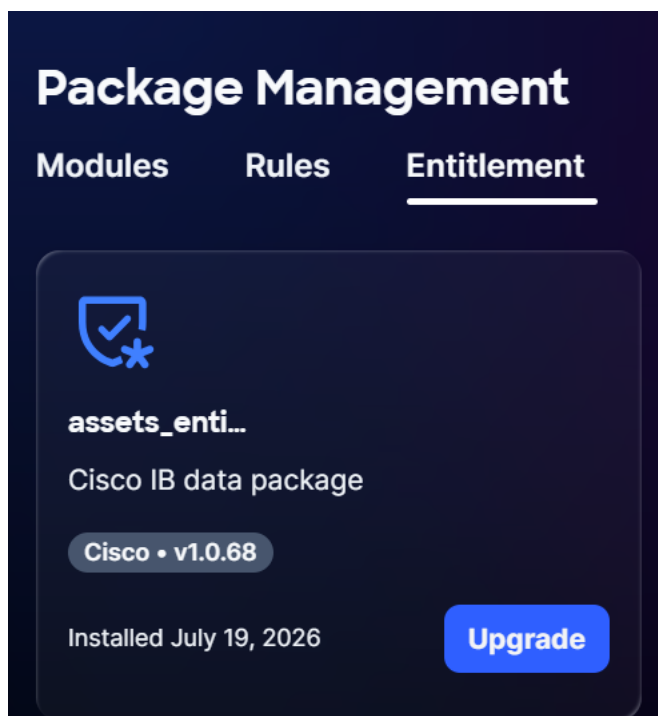
14. Fare clic su Add. Il diritto appena installato viene visualizzato nella scheda Diritto in Gestione pacchetti.

15. Per abilitare i diritti, attendere da 5 a 10 minuti dopo averli aggiunti, quindi avviare la raccolta di telemetria del dispositivo.

 Nota: L'aggiunta di un contratto di assistenza nel processo di adesione comporta l'aggiunta di tutti i dispositivi collegati a tale contratto all'inventario locale delle risorse dei dispositivi. È possibile filtrare i dispositivi in base al numero di serie, utilizzare più ID account o selezionare dispositivi specifici per gestire i diritti.

Aggiornamento dei diritti

Per aggiornare un diritto:



Aggiornamento dei diritti

1. Dal diritto desiderato, fare clic su Aggiorna.

Upgrade Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

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

Aggiorna diritto

2. Scegliere l'opzione di selezione dei file desiderata:

- Server SCP (Secure Copy Protocol): Immettere il nome esatto del file del pacchetto di installazione; questo metodo è consigliato per i file di grandi dimensioni
- Caricamento file locale: Trascinare il file di installazione scaricato

3. Immettere una password.

4. Fare clic su Add.

Caratteristiche con tecnologia AI

Il modulo di infrastruttura di inferenza dell'IA locale consente funzionalità basate sull'IA locali in VA. Esegue un modello SLM (Small Language Model) localmente, consentendo al sistema di rispondere ai prompt basati su AI. Una volta installato, è possibile interagire con esso direttamente all'interno dell'interfaccia VA.

Sono supportati i seguenti tipi di query:

- Risorse: Identificazione delle risorse a rischio a causa di stato di fine ciclo di vita, valuta o non conformità del software, vulnerabilità della sicurezza e lacune nella copertura dei contratti
- Inventario: Richiedi analisi basata su AI sugli asset presenti nel tuo inventario

Il pacchetto di installazione dell'infrastruttura di inferenza AI locale è disponibile nel catalogo dei pacchetti Cisco IQ e viene distribuito come gli altri moduli, ad esempio Assets.

 Nota: È possibile eseguire una sola (1) infrastruttura di inferenza dell'IA locale per GPU alla volta. L'installazione richiede circa 40-45 minuti. I file di installazione sono di grandi dimensioni (circa 30 GB); assicurarsi di disporre di spazio su disco sufficiente prima di eseguire il download.

Prerequisiti per l'infrastruttura di inferenza dell'IA locale

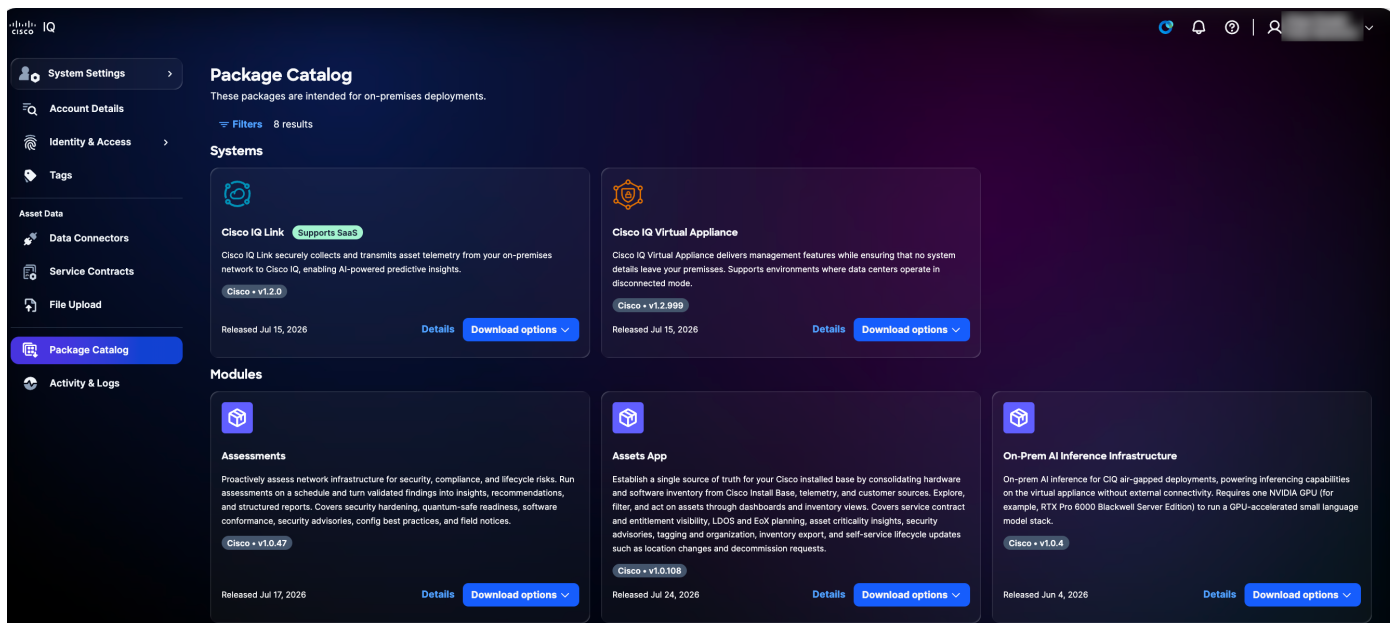
Prima di installare l'infrastruttura di inferenza dell'IA locale, è necessario che siano soddisfatte le seguenti condizioni:

- La VA deve includere una VM con accesso GPU; il modulo SLM richiede una GPU e non può essere eseguito senza
- La VM GPU deve disporre di almeno 80 GB di VRAM GPU

Installazione dell'infrastruttura di inferenza dell'IA locale

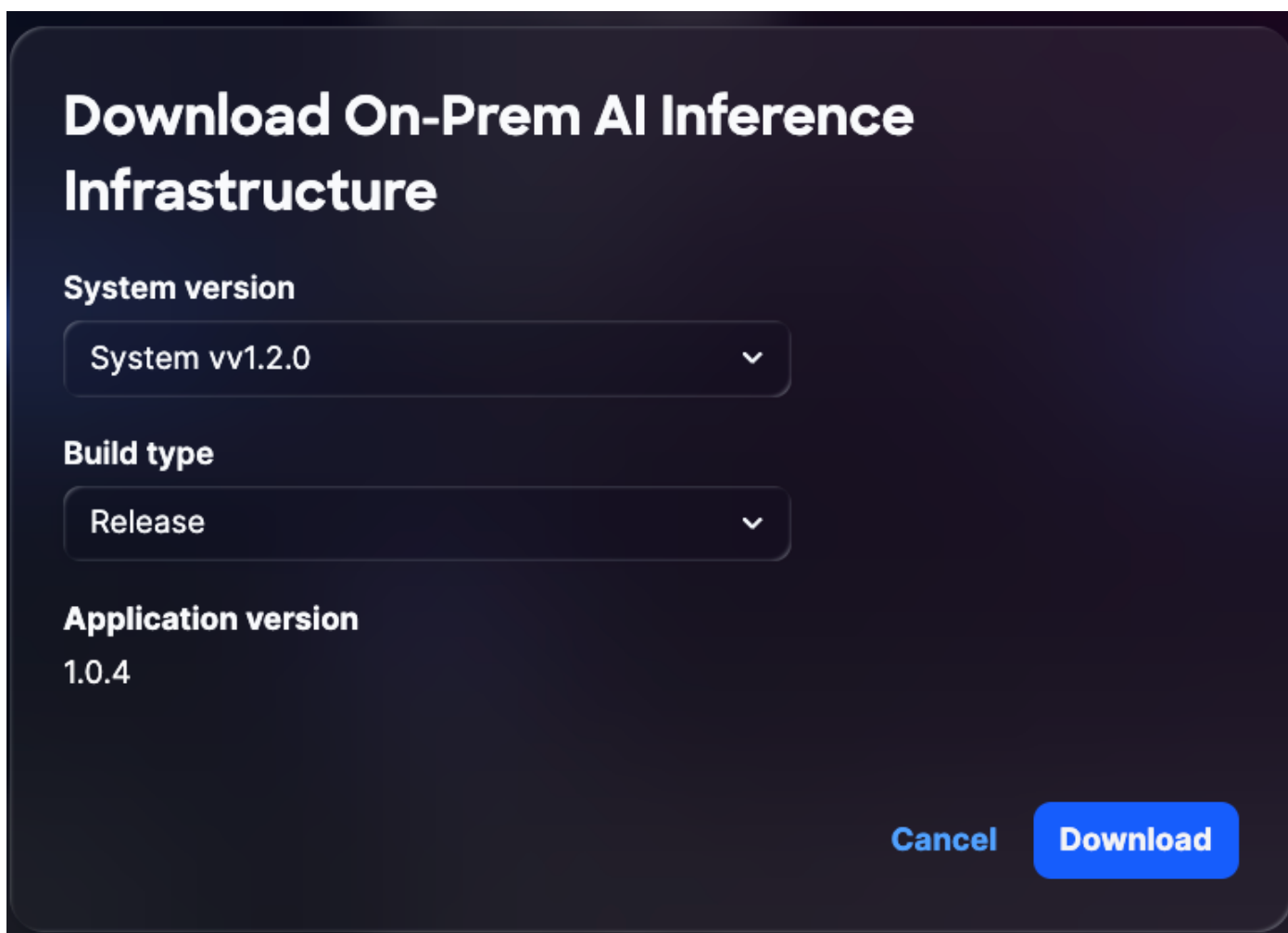
Per installare l'infrastruttura di inferenza AI locale sulla VA, scaricare il modulo dell'infrastruttura di inferenza AI locale da Cisco IQ SaaS:

1. Accedere a [Cisco IQ](#).
2. Passare a Impostazioni di sistema > Catalogo package.



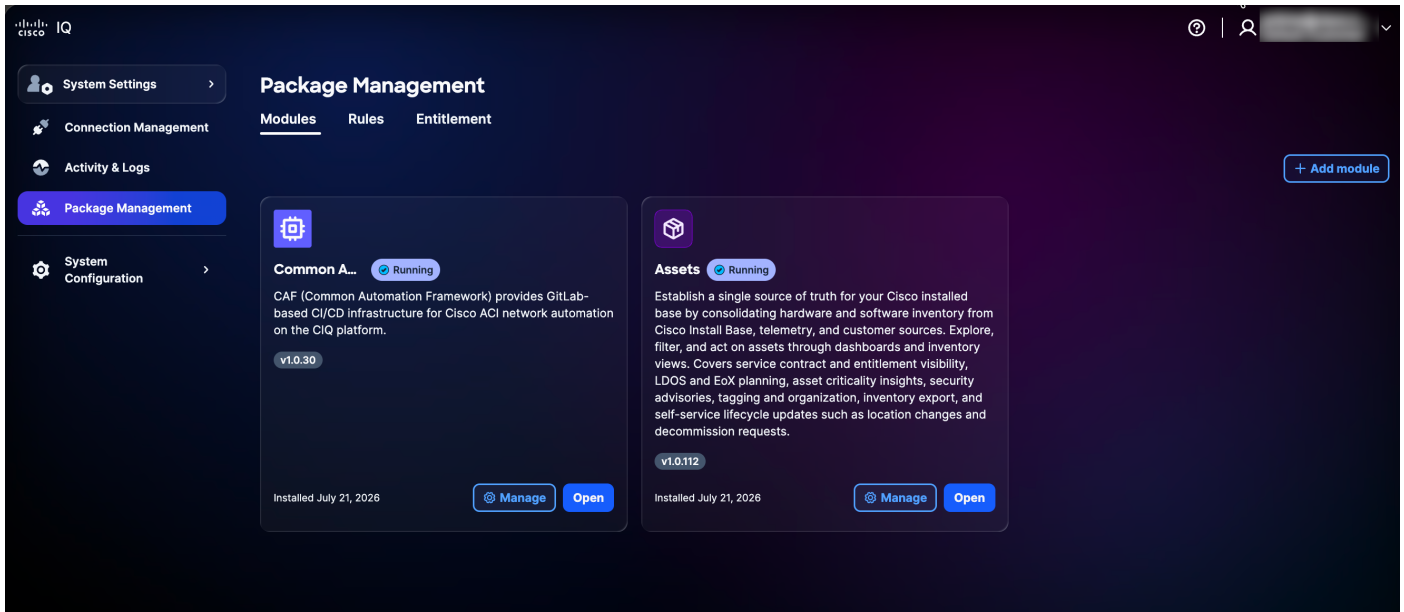
Installa pacchetto

3. Dalla scheda Infrastruttura inferenza AI locale, fare clic su Opzioni di download > Pacchetti di installazione. Viene visualizzata la finestra Scarica applicazione.



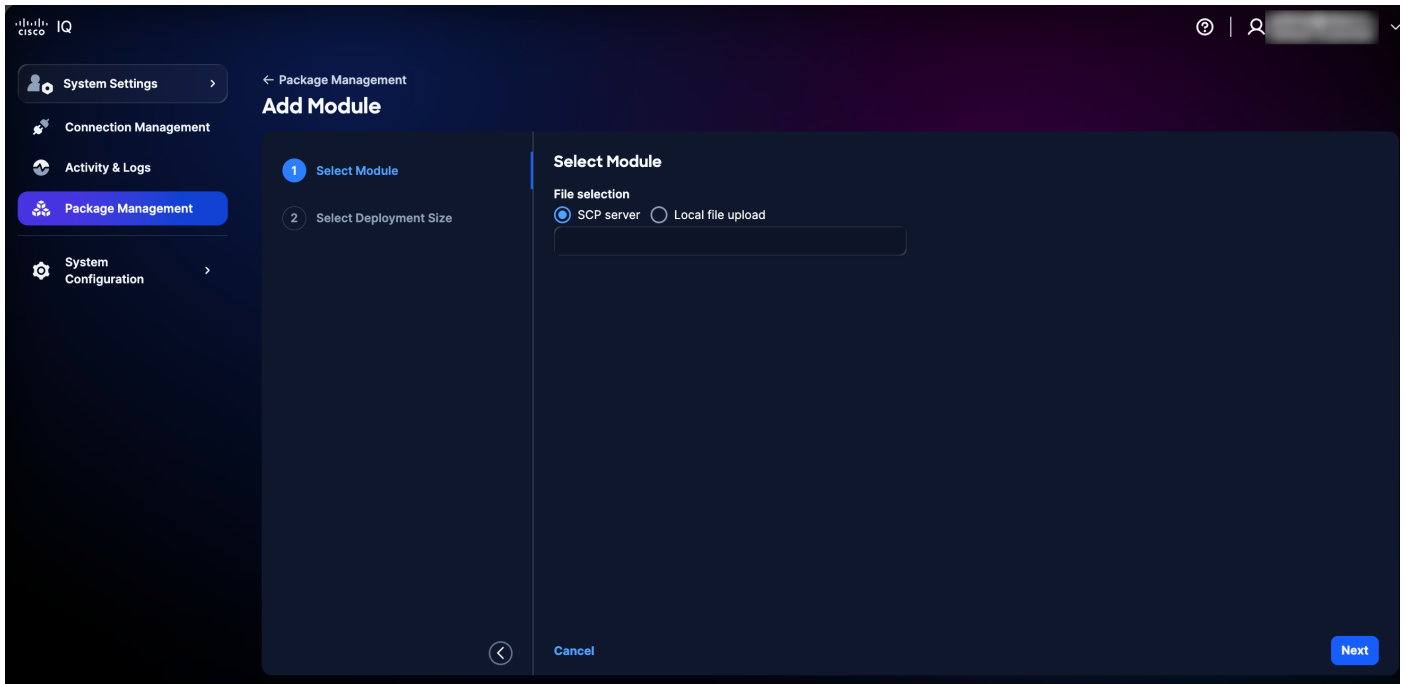
Scarica infrastruttura di inferenza AI

4. Selezionare una versione di sistema dall'elenco a discesa.
5. Selezionare un tipo di generazione dall'elenco a discesa.
6. Fare clic su Download (Scarica).
7. Passare a VA.



Gestione pacchetti

8. Passare a Home > Impostazioni di sistema > Gestione pacchetti. Viene visualizzata la pagina Gestione package con le schede riportate di seguito.
 - Moduli
 - Regole
 - Diritti
9. Dalla scheda Moduli, fare clic su Aggiungi moduli.



Seleziona modulo

10. Scegliere l'opzione di selezione dei file desiderata:

- Server SCP: Immettere il nome esatto del pacchetto di installazione (consigliato per i file di grandi dimensioni).
- Caricamento file locale: Trascinare il file di installazione scaricato (non consigliato per file di 30 GB o superiori a causa del tempo di caricamento). Nota: Il metodo di caricamento dei file locali ha una soglia di 20 minuti. Se il processo di caricamento supera questa durata, l'installazione non riesce. L'utilizzo di un server SCP è il metodo preferito per garantire un'installazione corretta e stabile.

11. Fare clic su Next (Avanti). Il sistema inizia a caricare il file.

12. Scegliere una Dimensione distribuzione (ad esempio, Piccola, Media o Grande).

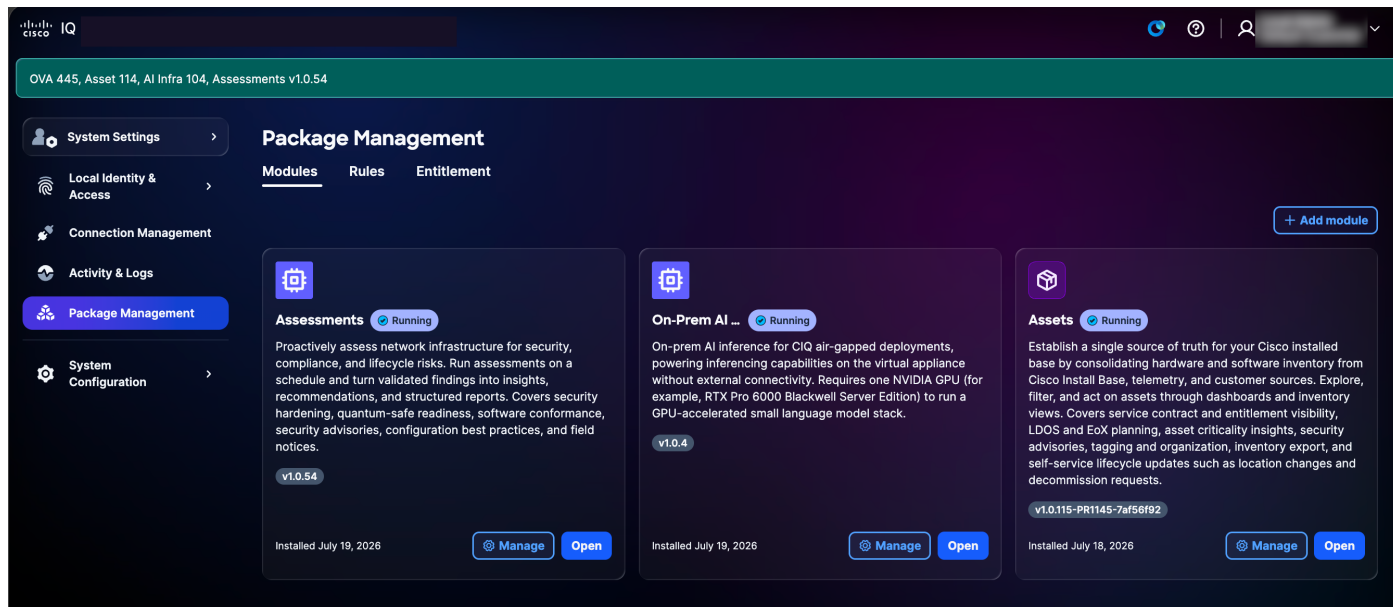
13. Fare clic su Add Module. L'installazione ha inizio e richiede circa 40-45 minuti.

Una volta completata l'installazione, nella scheda Modulo di Gestione pacchetti viene visualizzato Infrastruttura inferenza IA locale.

 Nota: È possibile eseguire un solo modulo di infrastruttura di inferenza IA locale per GPU. Il modulo utilizza circa il 90% della VRAM della GPU. Il tentativo di installare un'istanza aggiuntiva nella stessa GPU non è supportato.

Gestione del modulo sull'infrastruttura di inferenza dell'IA locale

Una volta installato, il modulo dell'infrastruttura di inferenza AI locale può essere gestito dalla scheda Applicazioni in Gestione pacchetti.



Modifica dell'infrastruttura di inferenza AI

Per gestire il modulo, fare clic su Gestisci accanto al modulo Infrastruttura inferenza IA locale. Per ulteriori informazioni, vedere [Gestione dei moduli](#).

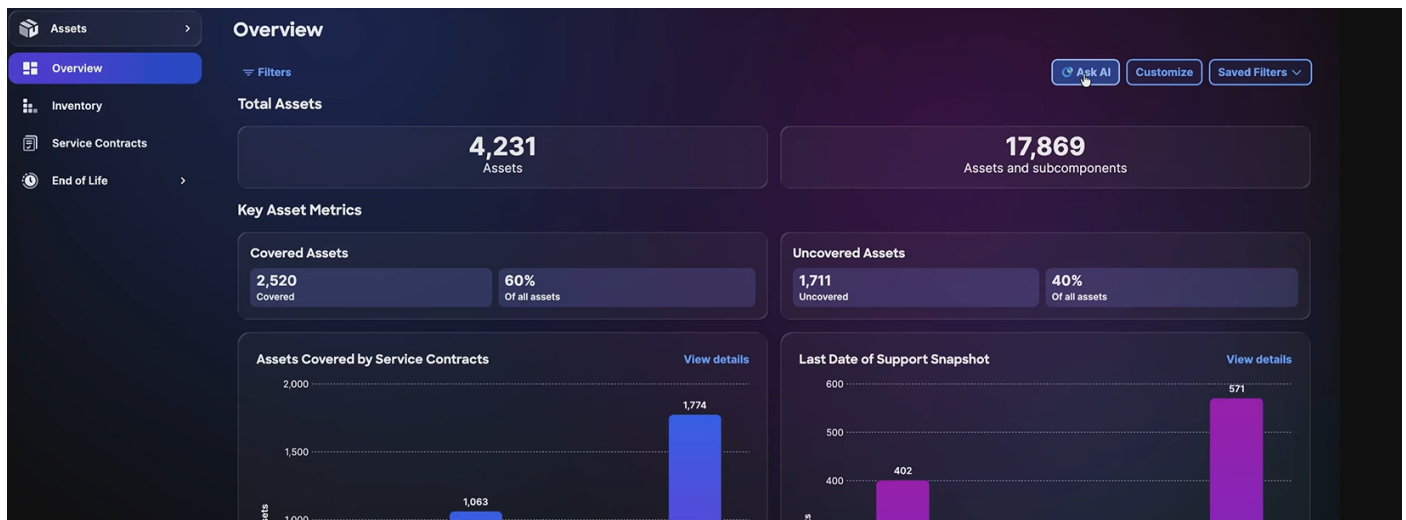
Utilizzo di funzioni basate su AI

Una volta installato correttamente il modulo Infrastruttura di inferenza AI locale, il pulsante Chiedi AI diventa disponibile nell'interfaccia VA.

Chiedi AI in Assets

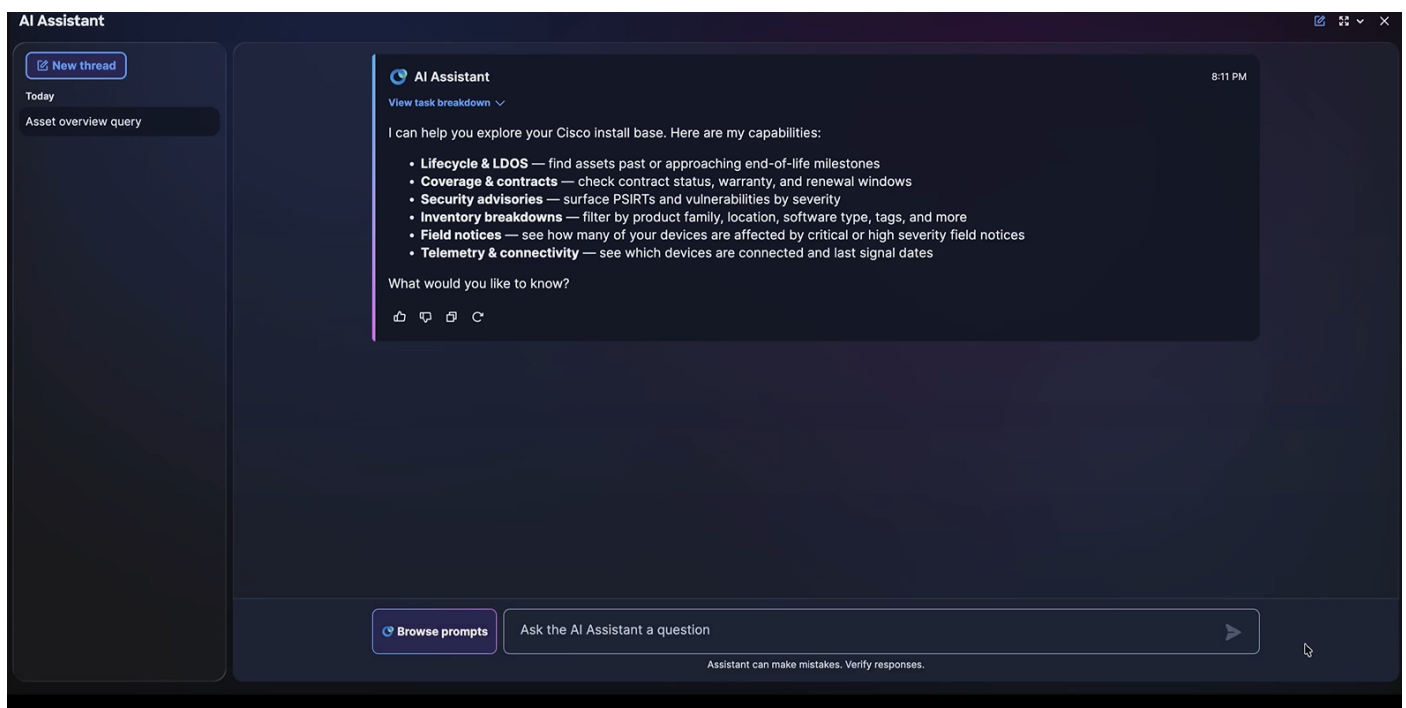
Per utilizzare l'API Ask in Asset:

1. Scegliere il menu Home > Asset. Viene visualizzata la pagina Asset.



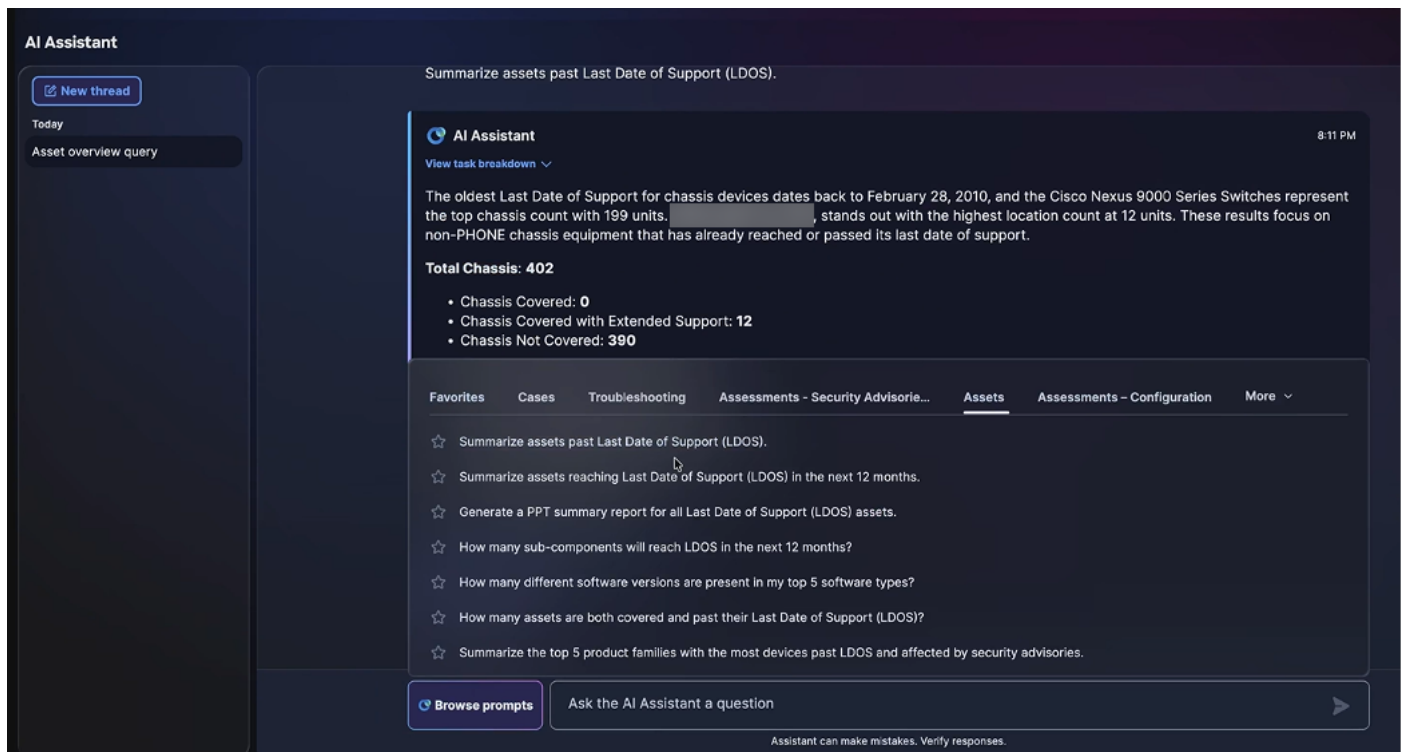
Pagina Asset

2. Fare clic su Chiedi AI. Viene avviata l'infrastruttura di inferenza dell'IA locale.



Prompt di ricerca

3. Fare clic su Sfoglia prompt per visualizzare i prompt disponibili oppure immettere una domanda personalizzata nel campo Fai una domanda all'Assistente AI.



Serie di richieste

4. Fare clic sul prompt desiderato o premere Invio. SLM locale genera una risposta.

Analisi IA in Inventory

Il modulo Infrastruttura di inferenza IA locale fornisce l'analisi automatizzata basata sull'IA nella sezione Inventario. I risultati dell'analisi vengono visualizzati automaticamente dopo il popolamento dei dati di inventario.

Per visualizzare l'analisi AI in Inventory:

1. Selezionare il menu Home > Magazzino. Viene visualizzata la pagina Magazzino.

Assets

Overview

Inventory

Service Contracts

End of Life

Assets

Q Search

1 Equipment type

Filters (1)

4231 results

Reset filters

Export

Saved Filters

Insights

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

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

Full Analysis

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

Inventario

- Visualizzate l'analisi generata dall'IA. I risultati vengono visualizzati nella vista inventario quando i dati sono disponibili.

 Nota: Fare clic su Analisi completa per visualizzare visualizzazioni quali grafici, dashboard e grafici che forniscono ulteriori informazioni.

Caratteristiche comuni dei moduli

In questa sezione vengono descritte in dettaglio le funzionalità di base condivise tra tutti i moduli. Queste funzionalità offrono un'esperienza utente coerente, ottimizzano le prestazioni del sistema e semplificano i workflow amministrativi

Analisi dei dati

Il pannello Insights fornisce un'analisi basata su AI dei dati presenti in quella pagina, fornendo informazioni pratiche per migliorare la sicurezza e lo stato dell'ambiente di rete.

 Nota: La feature di analisi è disponibile solo nelle pagine selezionate.

Assets

Q Search Product family Product ID Location Tags Filters (1) 1716 results Reset filters Export

Insights

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

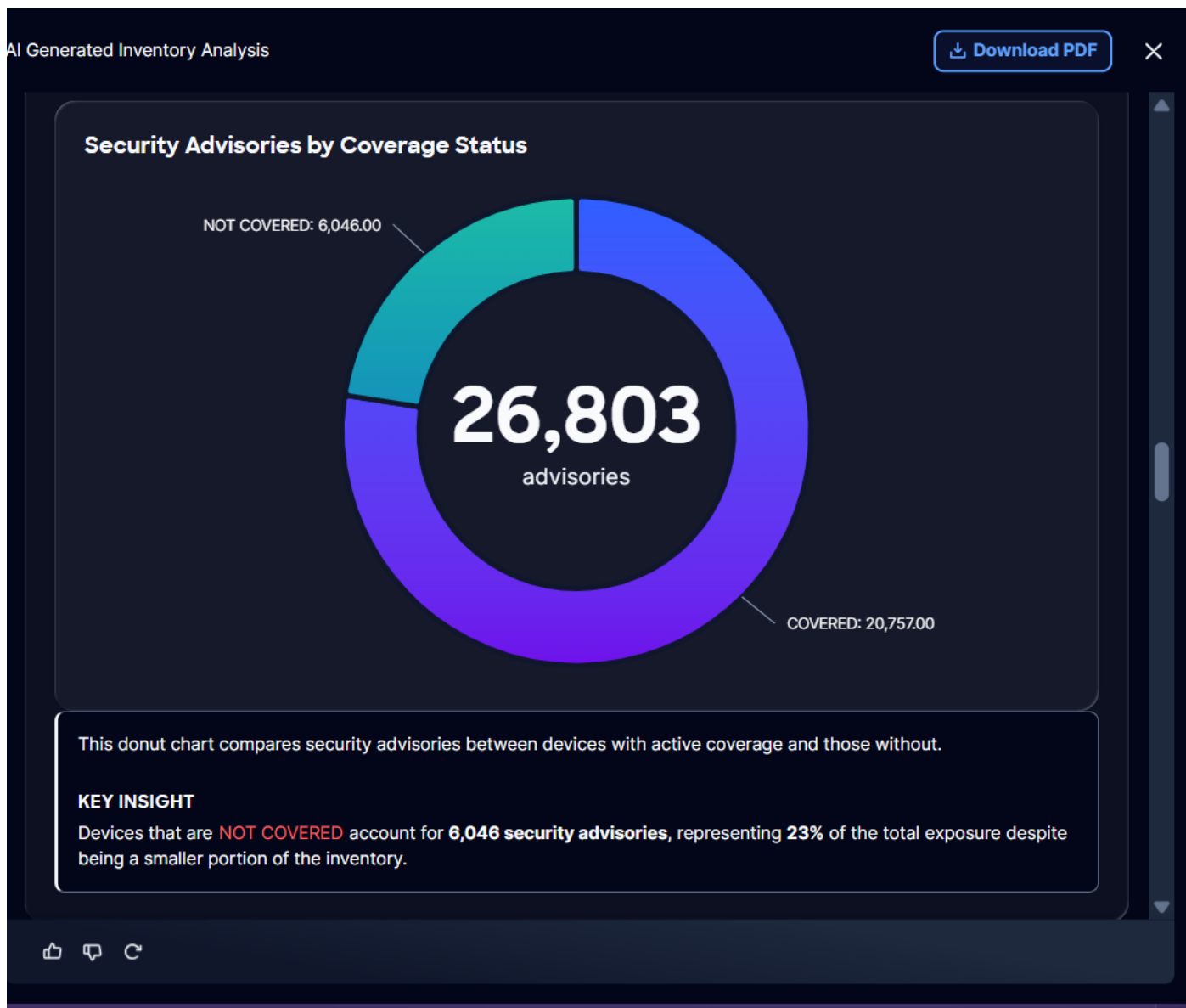
Full Analysis

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

Pannello informazioni approfondite

Nel pannello Informazioni approfondite sono disponibili le seguenti opzioni:

- Fare clic sull'icona Espandi per espandere il pannello e visualizzare ulteriori informazioni
- Fare clic sull'icona Thumbs Up o Thumbs Down per fornire un feedback sulle informazioni generate dall'AI
- Fare clic su Analisi completa per visualizzare informazioni aggiuntive, analisi più approfondite e visualizzazioni quali grafici, dashboard e grafici



Analisi completa

In un'analisi completa sono disponibili le seguenti opzioni:

- Fare clic su Scarica PDF per salvare una copia offline dell'analisi per i record o per la collaborazione

Esportazione delle informazioni

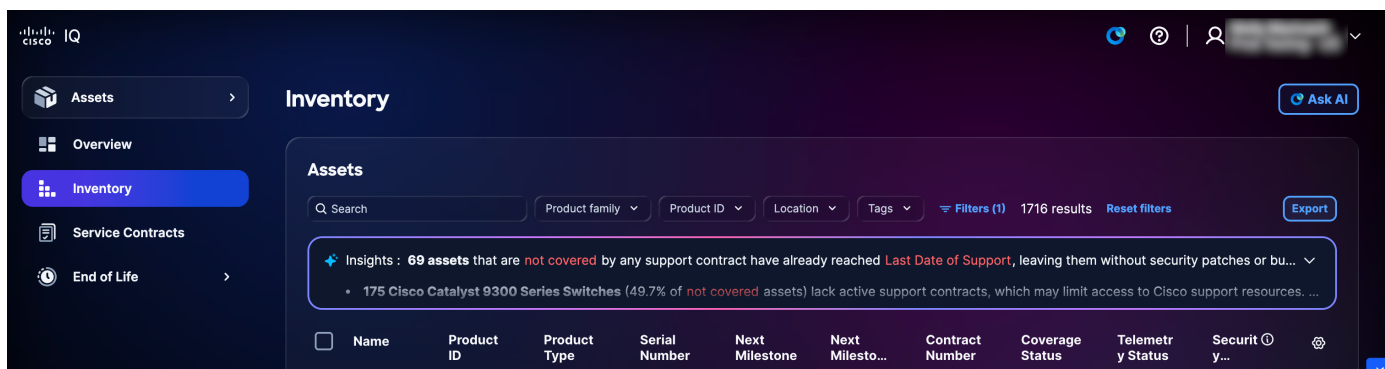
La funzionalità di esportazione consente di esportare visualizzazioni personalizzate per le informazioni relative a risorse e protezione in formato xls o csv.



Nota: La funzione di esportazione è disponibile solo per le pagine selezionate.

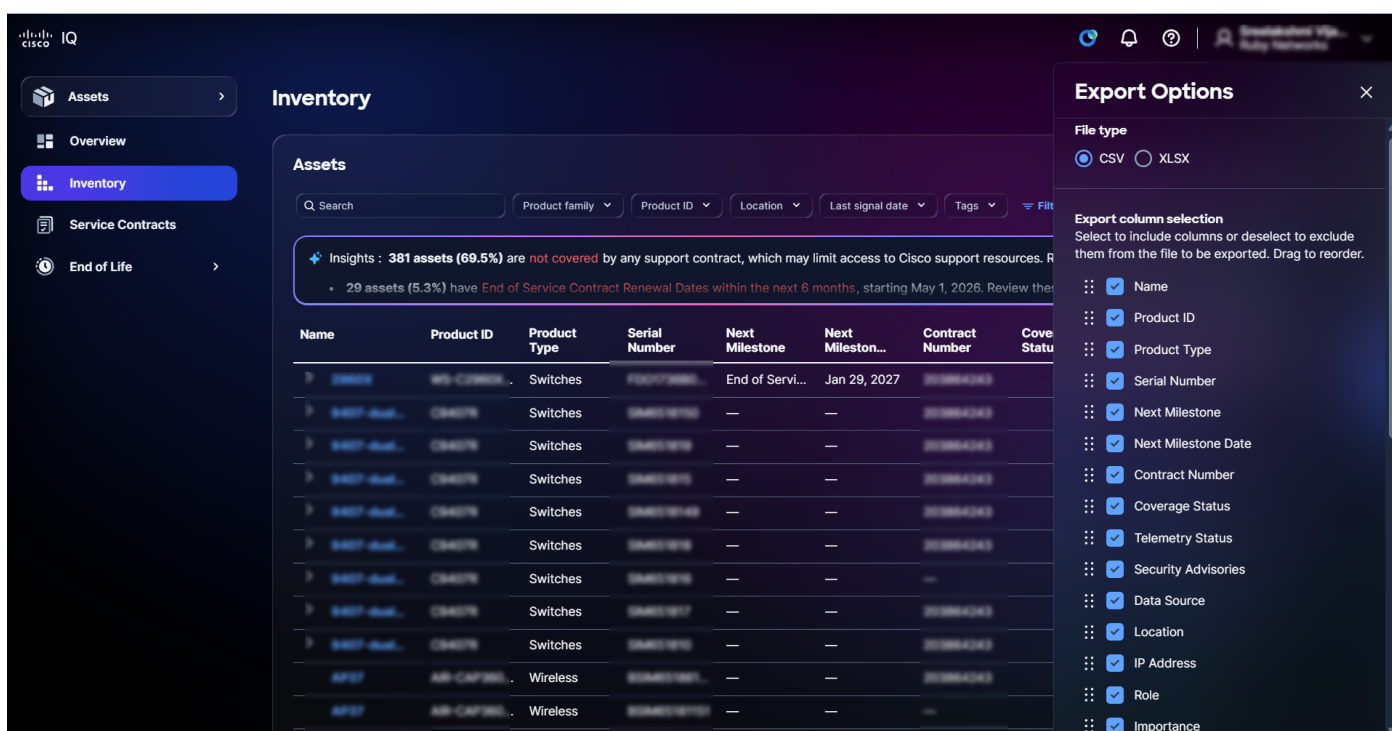
Per esportare le informazioni da una pagina:

1. Passare alla pagina.



Esportazione delle scorte nel modulo Assets

2. Fare clic su Esporta. Viene visualizzata la finestra Opzioni di esportazione.



Opzioni di esportazione

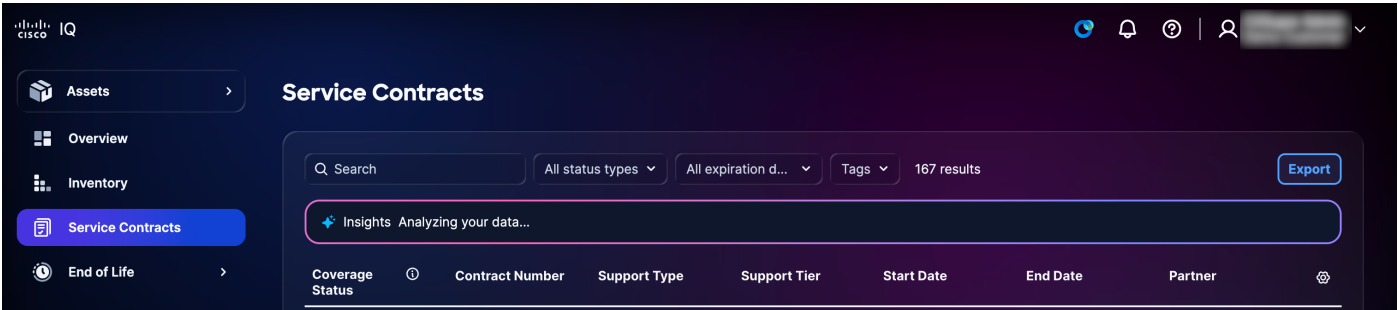
3. Selezionare un tipo di file.

4. Selezionare le caselle di controllo nelle colonne desiderate.

5. Fare clic su Esporta. Il file viene scaricato nella cartella di download locale del browser.

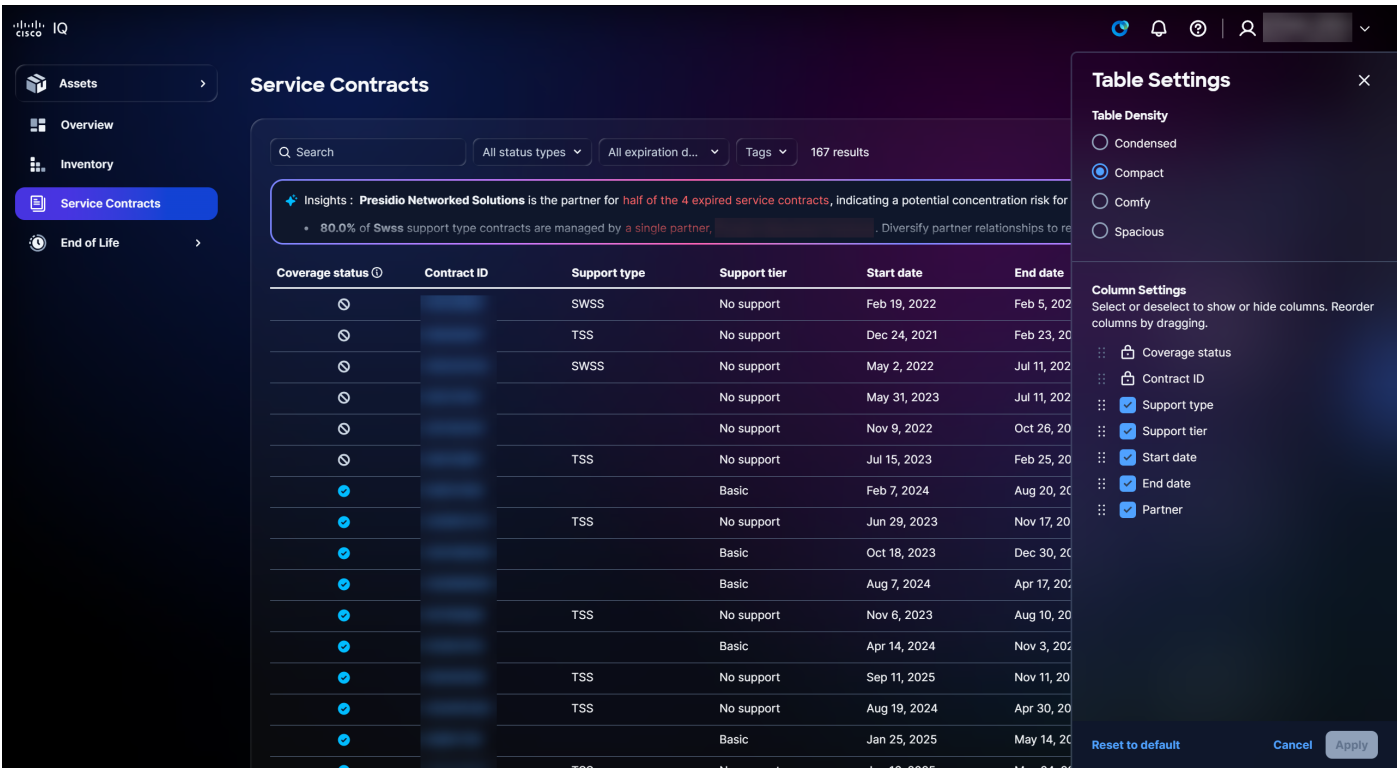
Impostazioni tabella

È possibile configurare le impostazioni della tabella per creare visualizzazioni personalizzate e ottimizzate per le diverse funzionalità del modulo.



Impostazioni tabella

Per modificare le colonne visualizzate nelle pagine selezionate, fare clic sull'icona Impostazioni tabella. Vengono visualizzate le impostazioni della tabella.



Opzioni di impostazione della tabella

Modifica della vista tabella

Per modificare la vista tabella:

1. Selezionate una delle seguenti opzioni Densità tabella (Table Density):

- Ridotta: Riduce al minimo gli elementi visivi e la spaziatura per visualizzare più informazioni
- Compatto: Riduce lo spazio vuoto e riduce la spaziatura tra gli elementi dell'interfaccia utente
- Comfort: Utilizzo di più spazi e di una maggiore spaziatura tra gli elementi
- Spazioso: Enfatisza gli spazi vuoti e gli elementi di interfaccia più grandi

2. Fare clic su Apply (Applica).

Aggiunta e rimozione di colonne

Per aggiungere o rimuovere colonne:

1. Selezionare o deselezionare le caselle di controllo Impostazioni colonna.

2. Fare clic su Apply (Applica).



Nota: Impossibile rimuovere la colonna Name dalla visualizzazione per tabella.

Modifica dell'ordine delle colonne

Per modificare l'ordine delle colonne:

1. Trascinare il nome della colonna per disporre gli elementi nell'ordine desiderato.

2. Fare clic su Apply (Applica).

Personalizzazione dei dashboard

La funzionalità Dashboard personalizzato consente di personalizzare i dashboard standard tramite una vasta gamma di opzioni di personalizzazione intuitive:

- Ridisporre i widget o i pannelli del quadro comandi mediante la funzionalità di trascinamento

della selezione

- Rimuovere i componenti non rilevanti per il flusso di lavoro
- Il layout del dashboard personalizzato viene archiviato in modo sicuro nel profilo utente e applicato automaticamente a tutte le sessioni e i dispositivi
- Ripristinare il layout originale del dashboard con una semplice opzione di ripristino

Per personalizzare un dashboard:

1. Passare al dashboard.



Personalizza

2. Fare clic su Personalizza.



Modifica dashboard

3. Modificate il quadro comandi in base alle esigenze:

- Riorganizza: Trascinare i widget nel layout desiderato
- Rimuovi: Fare clic sull'icona Elimina per rimuovere un widget
- Reset: Fare clic su Ripristina valori predefiniti per ripristinare il layout originale del dashboard

4. Fare clic su Save (Salva). Viene visualizzato un messaggio Dashboard salvato.

Il layout del dashboard viene applicato automaticamente a tutte le sessioni e i dispositivi.

Personalizzazione dei filtri

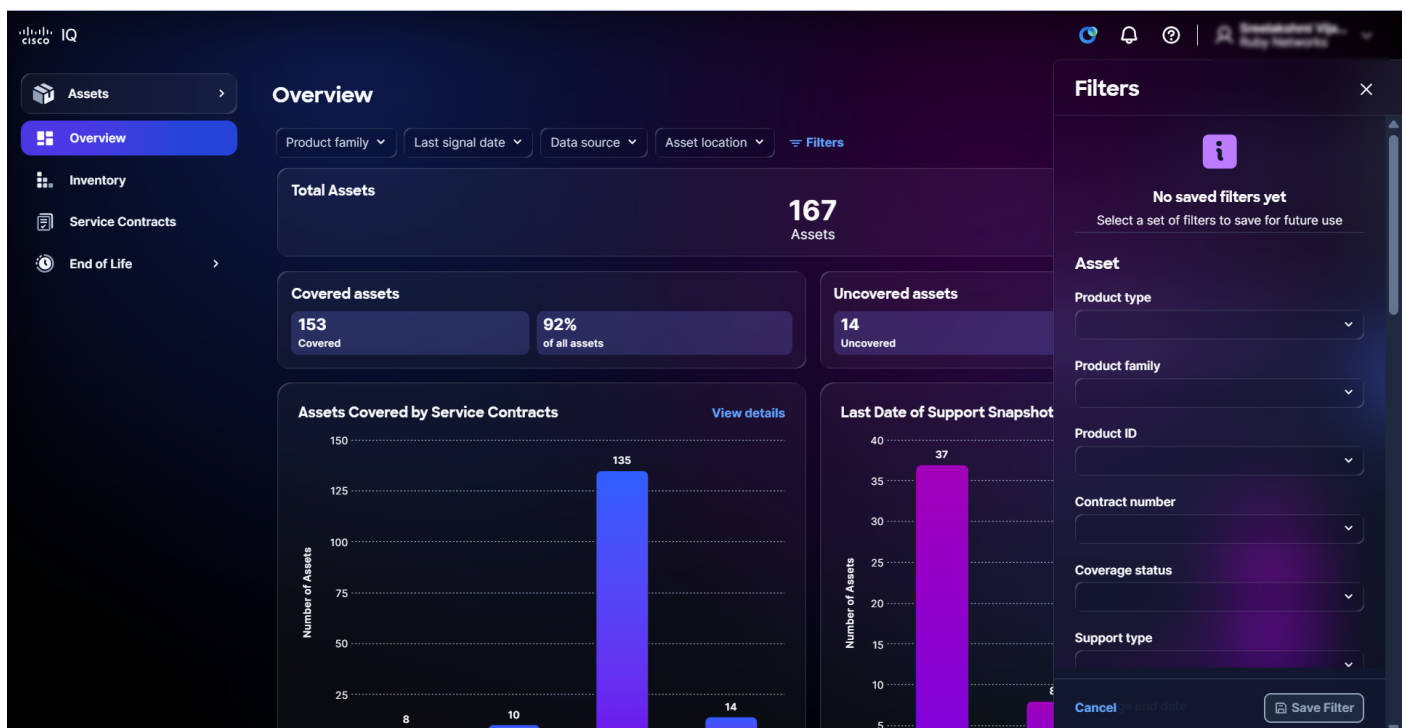
È possibile salvare le configurazioni di filtro personalizzate per qualsiasi visualizzazione del dashboard, consentendo di ripristinare facilmente le impostazioni preferite in base alle esigenze.

Tutte le preferenze dei filtri vengono archiviate in modo sicuro per singolo utente e account, garantendo un'esperienza personalizzata e coerente ogni volta che si accede a Cisco IQ.

Creazione di un filtro

Per creare un filtro personalizzato:

1. Passare al dashboard.
2. Fare clic su Filtri.



Filtri

3. Selezionare i filtri desiderati dagli elenchi a discesa.
4. Fare clic su Salva filtro. Viene visualizzata la finestra Filtro salvato con nome.

Name saved Filter

Filter name *

Custom Filter |

Cancel

Save Filter

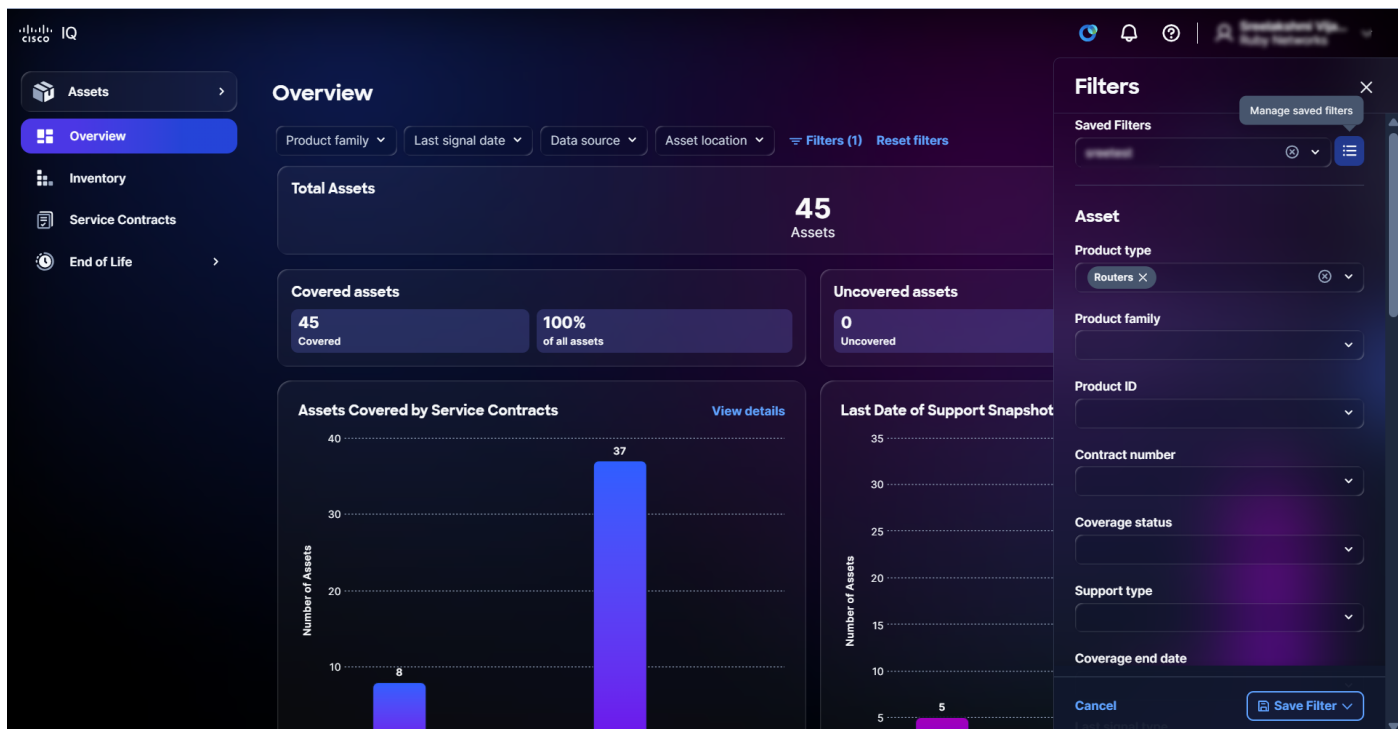
Nome filtro

5. Immettere il nome di un filtro.
6. Fare clic su Salva filtro per confermare.

Modifica del nome di un filtro

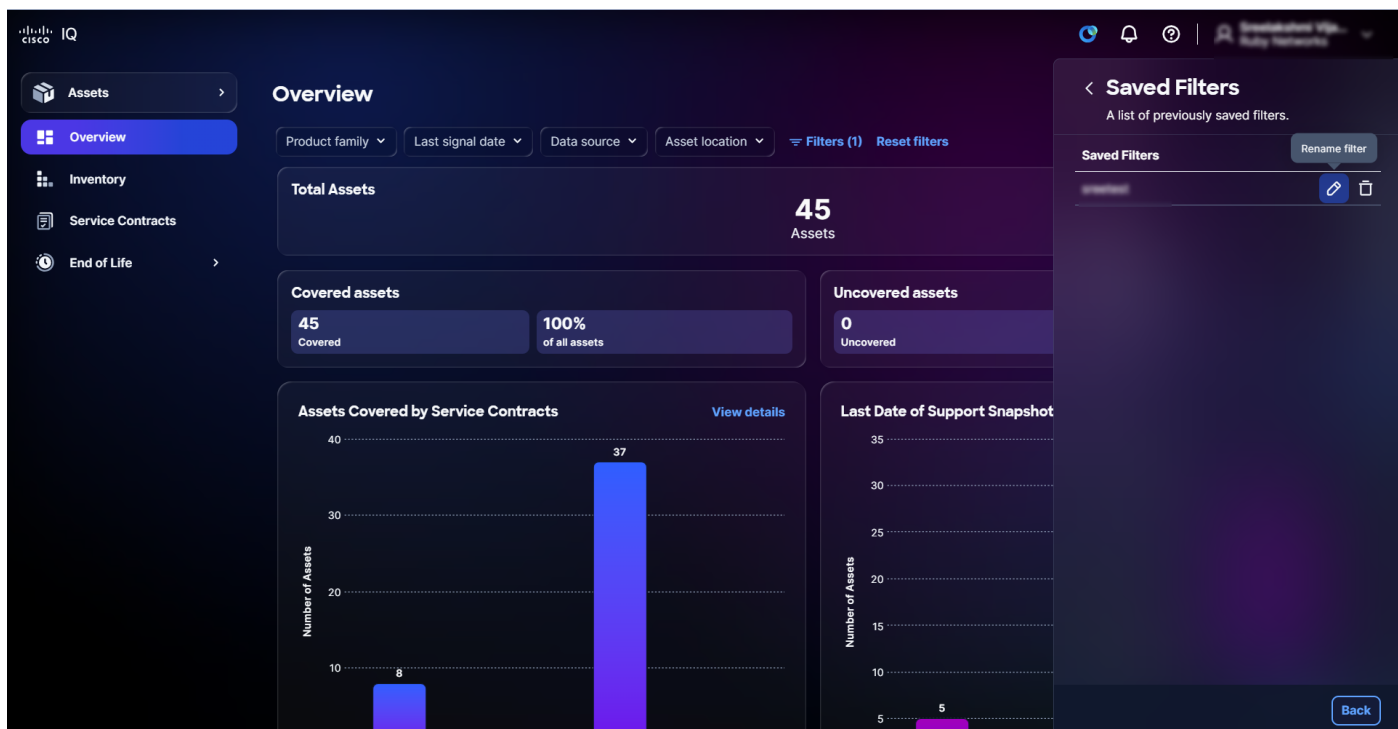
Per modificare un filtro personalizzato:

1. Fare clic su Filtri.



Gestisci filtri salvati

2. Fare clic sull'icona Gestisci filtri salvati.
3. Passare al filtro.



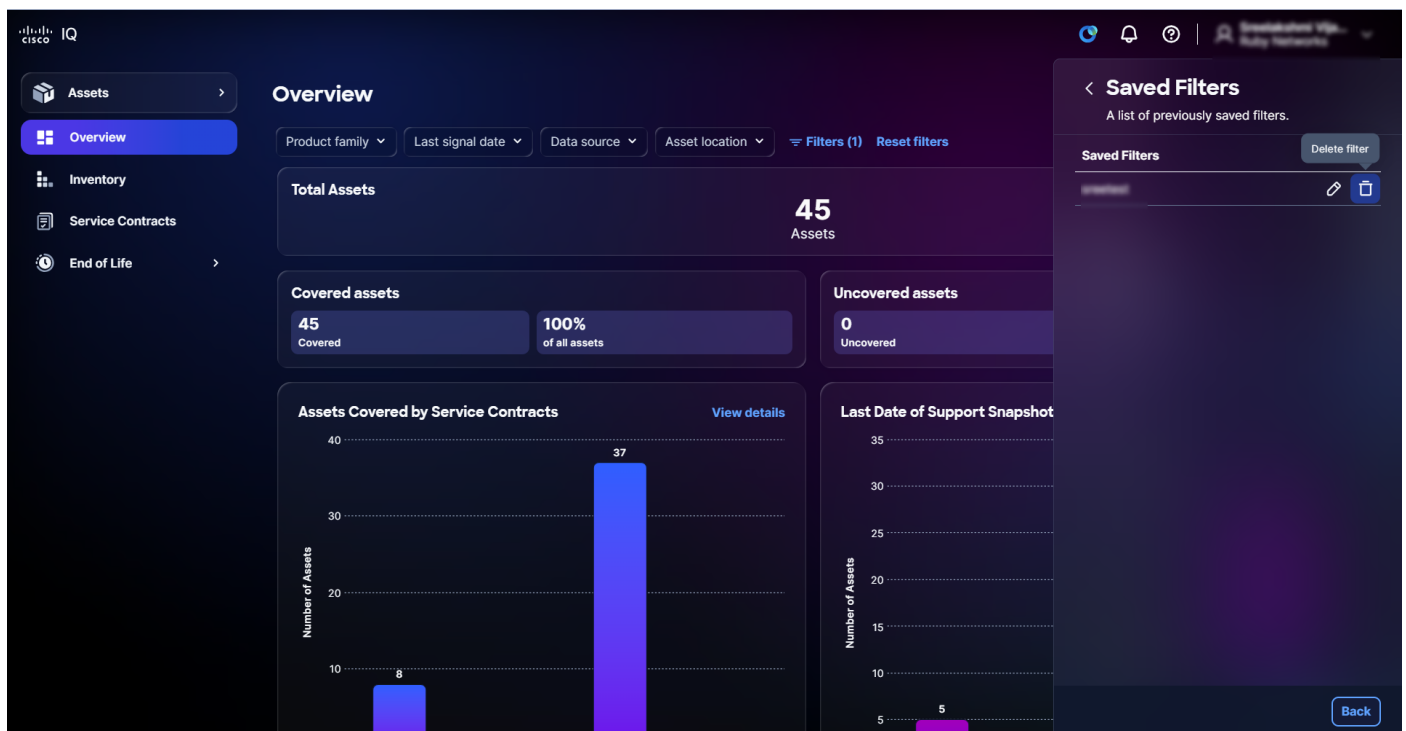
Modifica filtro

4. Fare clic sull'icona Modifica. Verrà visualizzata la finestra Filtro salvato nome.
5. Modificare il nome del filtro.
6. Fare clic su Salva filtro per confermare.

Eliminazione di un filtro

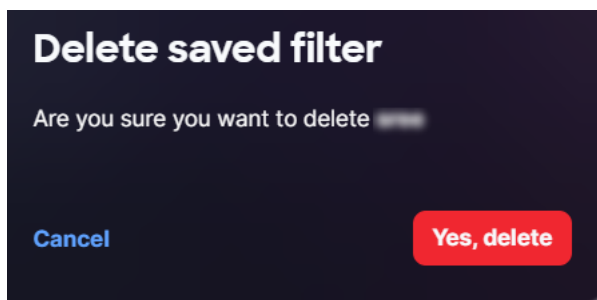
Per eliminare un filtro personalizzato:

1. Fare clic su Filtri.
2. Fare clic sull'icona Filtri salvati gestiti
3. Passare al filtro.



Elimina filtro salvato

4. Fare clic sull'icona Elimina. Viene visualizzata la finestra Elimina filtro salvato.



Conferma eliminazione filtro salvato

5. Fare clic su Sì, elimina per confermare.

Modulo Assets

Il modulo Assets offre visibilità e funzionalità di gestione complete per gli asset Cisco e costituisce la base di Cisco IQ, fornendo un elenco centralizzato di tutti i dispositivi all'interno di un'organizzazione. Raccogliendo informazioni da più fonti, funge da fonte unica di informazioni per l'inventario dei dispositivi. La gestione di un elenco di risorse completo e accurato è essenziale, in quanto altri moduli di Cisco IQ, ad esempio il modulo Valutazioni, si basano su questi dati per valutare lo stato e la sicurezza dei dispositivi.

Concetti fondamentali

Il modulo Assets si basa sui seguenti concetti fondamentali:

- **Bene:** Qualsiasi dispositivo fisico, hardware o software inventariato e gestito come parte della fornitura di servizi Cisco, con registrazione dettagliata di identità, funzione, copertura dei servizi e ciclo di vita
- **Cespiti basati su contratto:** Asset acquisiti in magazzino direttamente dai dati dei contratti di assistenza collegati, anziché tramite telemetria. Cisco IQ acquisisce i seguenti tipi di apparecchiature dai dati del contratto: Chassis, moduli, alimentatori e ventole. Queste risorse sono visibili nell'inventario anche se non è presente alcuna connessione telemetrica
- **Ultima data di supporto (LDOS):** Tracciamento di fine ciclo di vita e di fine supporto per i prodotti Cisco
- **Copertura del servizio:** Contratti di supporto attivi, garanzie e livelli di diritto associati a un componente hardware o software specifico
- **Codice asset:** Etichetta definita dall'utente assegnata a un cespite per l'organizzazione, i filtri e i flussi di lavoro operativi

- Segnale dispositivo: si riferisce a quando Cisco ha osservato per l'ultima volta un dispositivo (tramite il suo numero di serie) in base alla telemetria del dispositivo, ai casi di supporto e ai rinnovi del contratto; I dati di telemetria degli asset vengono acquisiti e arricchiti attraverso una pipeline di dati multilivello

Modulo di accesso agli asset

Per accedere alle funzioni di gestione degli asset in Cisco IQ, scegliere il menu Home > Asset o fare clic su Asset dalla sezione Applicazione della scheda Home page > Launchpad. Verrà visualizzata la pagina Panoramica.

Panoramica sui cespiti

La pagina Panoramica visualizza un dashboard che consente di valutare rapidamente lo stato e lo stato dei dispositivi.

100% Assets, Asset ID, At-risk Assets, Assets with Critical or High Security Advisories



Assets



Overview



Inventory



Service Contracts



End of Life



Overview

Filters

Ask AI

Customize

Saved Filters

Total Assets

199

Assets

928

Assets and subcomponents

Key Asset Metrics

Covered Assets

186

Covered

93%

Of all assets

Uncovered Assets

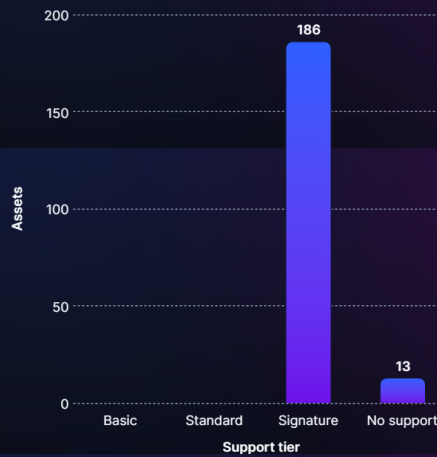
13

Uncovered

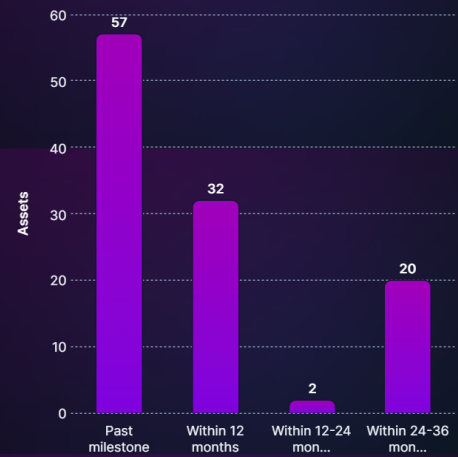
7%

Of all assets

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



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



Assets With Telemetry Enabled

186

With telemetry

93%

Of all assets

Assets Without Telemetry Enabled

13

Without telemetry

7%

Of all assets

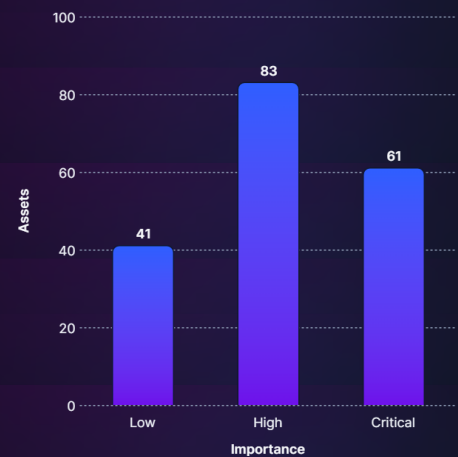
Assets With Critical or High Security Advisories [View details](#)



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

Assets by Importance [View details](#)

Importance can be evaluated for 185 assets.

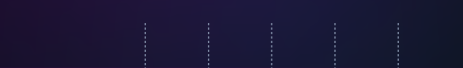


Asset Breakdown

Top 5 Product Families [View details](#)



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



Panoramica sui cespiti

Nel quadro comandi vengono visualizzate le informazioni riportate di seguito.

- Totale asset: Numero totale di asset nell'account Cisco IQ
- Metriche principali degli asset: Metriche chiave aggiuntive, ad esempio lo stato della telemetria, gli advisory della sicurezza critici e le informazioni LDOS
- Cespiti coperti: Il numero totale e la percentuale di attività coperte da contratti di assistenza
- Attività non coperte: Il numero totale e la percentuale dei cespiti non coperti da contratti di assistenza
- Cespiti coperti da contratti di assistenza: Un'analisi del numero di risorse (hardware o software) coperte dai contratti di assistenza, suddivise per livello di diritto
- Data ultima istantanea di supporto: Ripartizione del numero di attività oltre le LDOS o che raggiungono le LDOS
- Asset con telemetria abilitata: Numero totale e percentuale di asset con telemetria abilitata
- Asset senza telemetria abilitata: Numero totale e percentuale di cespiti senza telemetria abilitata
- Asset con consulenze critiche o ad alta sicurezza: Percentuale degli asset totali con la telemetria abilitata e che dispongono di avvisi critici o di protezione elevata
- Asset per importanza: Priorità assegnata a un dispositivo in relazione agli altri dispositivi della rete.
- Analisi stratificata degli asset: Visualizzazione dettagliata delle informazioni sugli asset, ad esempio famiglie di prodotti, ubicazioni di installazione, versioni software e ruoli degli asset

Filtraggio delle viste per i cespiti

È possibile filtrare la visualizzazione del dashboard scegliendo un filtro dagli elenchi a discesa oppure facendo clic su Filtri e scegliendo un'opzione dall'elenco dei filtri disponibili.



Nota: Alcuni filtri possono essere nascosti a seconda delle impostazioni di zoom. Sono disponibili diversi filtri a seconda dei ruoli e delle autorizzazioni.

Visualizzazione dei dettagli per i cespiti

Quando si fa clic su Visualizza dettagli, la pagina viene reindirizzata alla pagina Magazzino. Per ulteriori informazioni, vedere [Inventario](#).

Asset Criticality Insights

Cisco IQ include Asset Criticality Insights, una nuova funzionalità del modulo Assets che prevede il ruolo funzionale e l'importanza aziendale dei dispositivi di rete. Analizzando le configurazioni dei dispositivi e le funzionalità abilitate, Asset Criticality Insights consente di identificare gli asset che hanno il maggiore impatto sulla rete, in modo da assegnare loro le priorità per il monitoraggio e l'aggiornamento del software, la pianificazione di fine ciclo di vita e le decisioni di copertura.

 Nota: Asset Criticality Insights è disponibile esclusivamente per gli asset con livelli Standard o Signature che dispongono di connessioni telemetriche attive. Verificare che gli asset soddisfino i requisiti di configurazione per inserire informazioni dettagliate nel dashboard.

Asset Criticality Insights è disponibile nell'app Assets nelle seguenti aree:

- Panoramica sui cespiti: Filtra e visualizza le scomposizioni di riepilogo per attributi di Asset Criticality Insights
- Inventario delle risorse: Visualizzazione, ricerca, filtro e ordinamento dei dispositivi per ruolo e priorità
- Dettagli asset: Visualizzare il ruolo e l'importanza per i singoli dispositivi, con descrizioni comandi informative per ciascun valore

Sostituzione delle classificazioni di ruoli e priorità

Cisco IQ prevede automaticamente il ruolo e l'importanza di ciascuna risorsa in base ai dati di telemetria. Gli amministratori degli account possono correggere manualmente queste classificazioni quando la previsione automatica non riflette in modo accurato la funzione o la criticità dell'asset nella rete.

 Nota: I controlli di sostituzione sono disponibili solo per gli amministratori account. I valori di Ruolo e Importanza sono di sola lettura per tutti gli altri ruoli utente.

Sostituzione delle classificazioni dalla tabella Inventory

Per sostituire il ruolo o l'importanza per uno o più asset:

1. Passare a Cespiti > Magazzino.
2. Fare clic sulla casella di controllo della riga di risorsa desiderata. Per aggiornare più asset contemporaneamente, selezionare più caselle di controllo.

Assets

Overview

Inventory

Service Contracts

End of Life

Inventory

Ask AI

Assets

Search

Filters (2) 20 results Reset filters

Export Saved Filters

Insights: Of the 1 assets where Coverage Status is not covered, 1 (100.0%) have Product Description NCS 560 Route...

For 1 assets with Support Tier No Support, Product Family NCS 500 Modules leads at 1 instances (100.0%). Assets la...

4 items selected

Cancel Manage Tags

	Name	Produ ct ID	Produ ct...	Equip men...	Serial Nu...	Next Mile...	Next Mile...	Contr act...	Cover age...	Telem etry...	
☐			Modules	Module		—	—		✓	✓	0
☐			Modules	Module		—	—		⊘	✓	0
☒			Unified ...	Chassis		—	—		✓	✓	1
☐			Storage...	Chassis		—	—		✓	✓	0

Ruolo e priorità

3. Nella colonna Ruolo o Importanza, scegliere il valore corretto dall'elenco a discesa della riga del bene.
4. Fare clic su Applica per confermare la sostituzione.

Le risorse con valori sostituiti manualmente visualizzano un indicatore visivo nella colonna Ruolo o Importanza.

Nota: Per rimuovere una sostituzione configurata in precedenza e tornare alla previsione automatica, selezionare l'opzione trattino (—) dall'elenco a discesa Ruolo o Importanza.

Sostituzione delle classificazioni dai dettagli dei cespiti

Per sostituire Ruolo o Importanza dalla vista dei dettagli dei cespiti:

1. Passare a Cespiti > Magazzino e fare clic su un cespite.
2. Nel pannello dei dettagli della risorsa, individuare i campi Ruolo e Importanza.
3. Fare clic sull'elenco a discesa del campo che si desidera aggiornare e selezionare il valore corretto.
4. Fare clic su Apply (Applica) per confermare.

La vista dettagliata di un bene mostra anche una spiegazione degli attributi di telemetria che hanno informato la previsione automatica originale, per aiutare a determinare se una sostituzione è appropriata.

Visualizzazione dell'audit trail di sostituzione

Tutte le sostituzioni di ruoli e priorità vengono registrate in un audit trail a livello di account. Per accedere all'audit trail:

1. Scegliete Home > Impostazioni di sistema > Attività e registri.
2. Scegliere Filtri > Tipo di azione > Sostituisci per visualizzare solo gli eventi di sostituzione.

L'audit trail visualizza il nome dell'asset, i valori precedenti e nuovi, l'utente che ha apportato la modifica e la data e l'ora della modifica. L'audit trail può essere esportato utilizzando l'opzione Esporta.



Nota: L'audit trail può essere filtrato in base all'intervallo di date, all'utente e al nome dell'asset.

Inventario

La pagina Inventario fornisce un elenco di tutte le risorse Cisco nell'account Cisco IQ.

Inventario

Ricerca e filtraggio delle viste per inventario cespiti

È possibile filtrare la visualizzazione elenco scegliendo un filtro dagli elenchi a discesa oppure facendo clic su Filtri e scegliendo un'opzione dall'elenco dei filtri disponibili. È inoltre possibile cercare le risorse immettendo il nome della risorsa nel campo Cerca.

 Nota:

- Alcuni filtri possono essere nascosti a seconda delle impostazioni di zoom.
- Sono disponibili diversi filtri a seconda dei ruoli e delle autorizzazioni.

Analisi magazzino

Il pannello Informazioni approfondite nella pagina Inventario visualizza un'analisi basata sull'IA che fornisce un riepilogo delle risorse con particolare attenzione alla copertura del supporto, alla connettività e alle fasi cardine. Fare clic su Analisi completa per visualizzare visualizzazioni quali grafici, dashboard e grafici che forniscono ulteriori informazioni. Per ulteriori informazioni, vedere [Analisi dei dati](#) nelle funzionalità comuni dei moduli.

Esportazione del magazzino

Fare clic su Esporta per salvare un elenco di inventario filtrato in formato xls o csv. Per ulteriori informazioni, vedere [Esportazione delle informazioni](#) nelle funzionalità comuni dei moduli.

Visualizzazione dei dettagli dei cespiti

Fare clic su una risorsa per visualizzarne i dettagli. Viene visualizzata la vista dettagliata di un cespite con le seguenti schede:

- **Dettagli:** Visualizza i dettagli degli asset, ad esempio il prodotto, i dati dei segnali, l'identità, l'ubicazione, la garanzia e le informazioni sulla copertura

Cisco Catalyst Center Appliance (Gen 2) - 44 Core

Assets

Overview

Inventory

Service Contracts

End of Life

Inventory

10.197.238.131

Cisco Catalyst Center Appliance (Gen 2) - 44 Core

Details

Product Alerts

Hardware

Software

Product

Product ID

Product type

Product family

Last Date of Support

Identity

Serial number

IP address

Hostname

Software version

Role

Importance

Tags

Sold by

Location

Install-at

Signals

Last signal

Last signal type

Telemetry

Telemetry status

Last data collection

Data connector

Warranty

Warranty type

Warranty end date

Coverage

Coverage status

Contract number

Support tier

Coverage end date

Ask AI

Dettagli asset

- Avvisi sui prodotti: Visualizza avvisi sui prodotti correlati, ad esempio consigli sulla sicurezza

e avvisi sui prodotti

- **Hardware:** Fornisce una visualizzazione dettagliata della tempistica per la fine del ciclo di vita dell'hardware (ad esempio, fine vendita, ultima spedizione e ultima data di data del supporto)
- **Software:** Fornisce una visualizzazione dettagliata della cronologia per la fine del ciclo di vita del software

Codici di matricola

I codici di matricola sono etichette personalizzate assegnate alle risorse di magazzino in Cisco IQ. Un tag è una coppia chiave:valore, ad esempio Ambiente:Prod o Etichetta:Campus, definita dall'utente. È possibile assegnare i cartellini a singoli asset o a più asset contemporaneamente e filtrare il magazzino in base ai cartellini per trovare rapidamente gli asset desiderati.



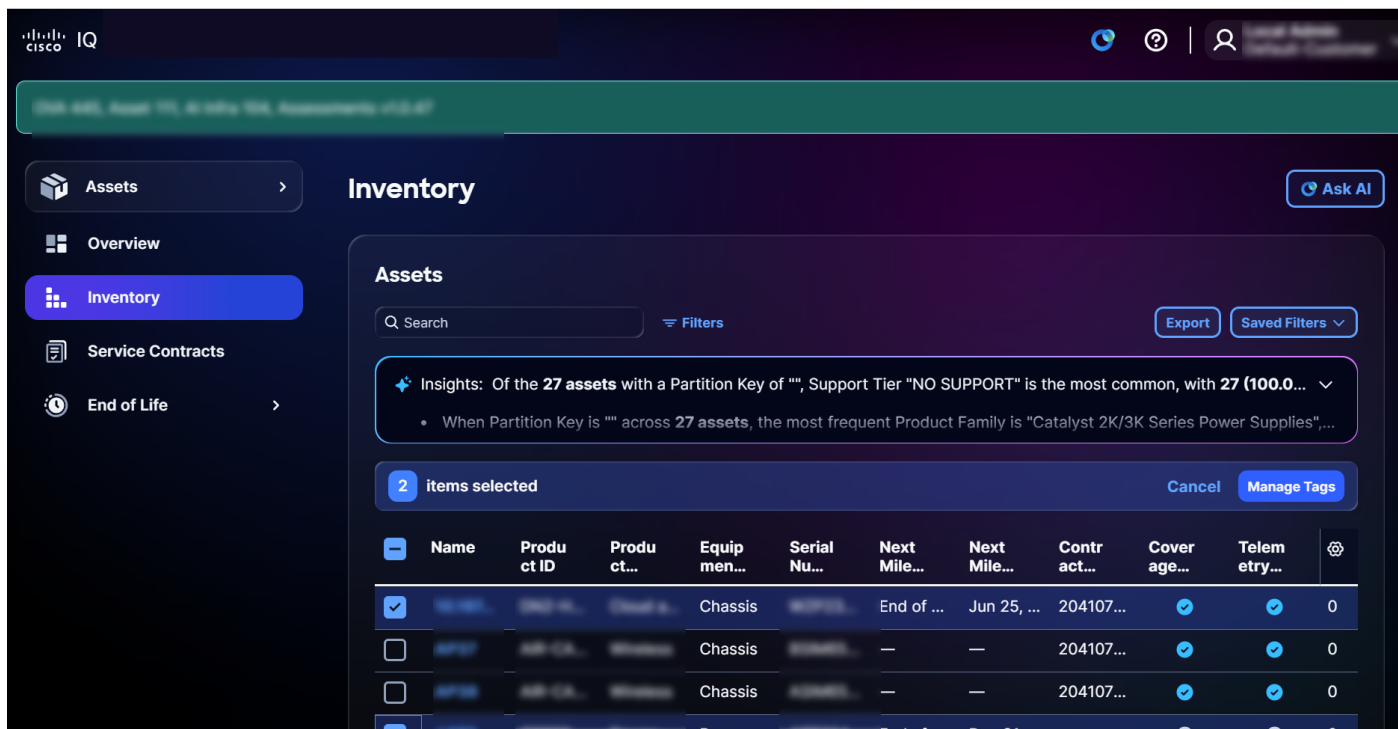
Nota: Una volta creato un tag da un amministratore dell'account, gli utenti possono assegnare un tag a una risorsa.

Assegnazione di tag

L'assegnazione dei cartellini ai cespiti selezionati nella vista Magazzino consente di organizzare e classificare i cespiti in modo da migliorare il filtraggio, la creazione di rapporti e la gestione.

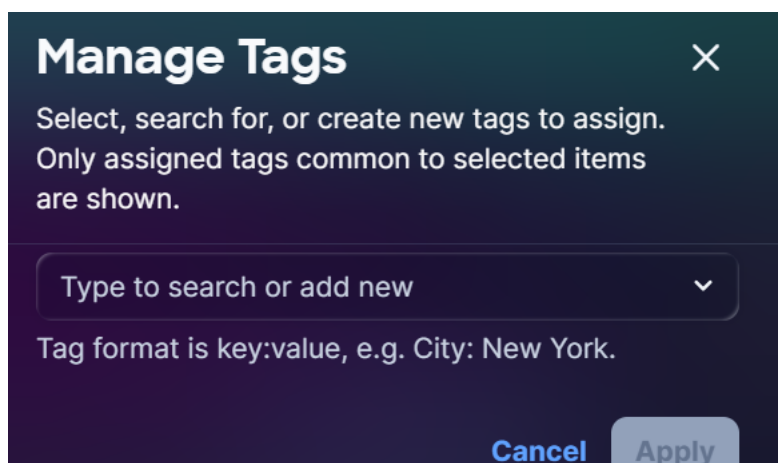
Per assegnare un'etichetta a un cespito:

1. Passare a Cespiti > Magazzino.



Applicazione di tag agli asset

2. Selezionare le caselle di controllo delle risorse desiderate.
3. Fare clic su Gestisci tag. Viene visualizzata la finestra Gestisci tag.



Assegnazione di tag

4. Nel campo di testo, immettere o selezionare il nome del tag dalle opzioni esistenti e premere Invio.



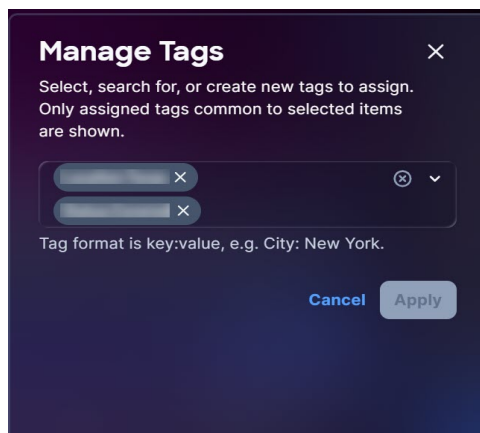
Nota: I tag sono nel formato chiave:valore (ad esempio, Città:NYC).

5. Fare clic su Apply (Applica).

Rimozione dei codici di matricola

Per rimuovere un tag da una o più risorse:

1. Passare a Cespiti > Magazzino.
2. Selezionare la casella di controllo accanto a una o più risorse.
3. Fare clic su Gestisci tag. Viene visualizzata la finestra Gestisci tag.



Rimozione di tag

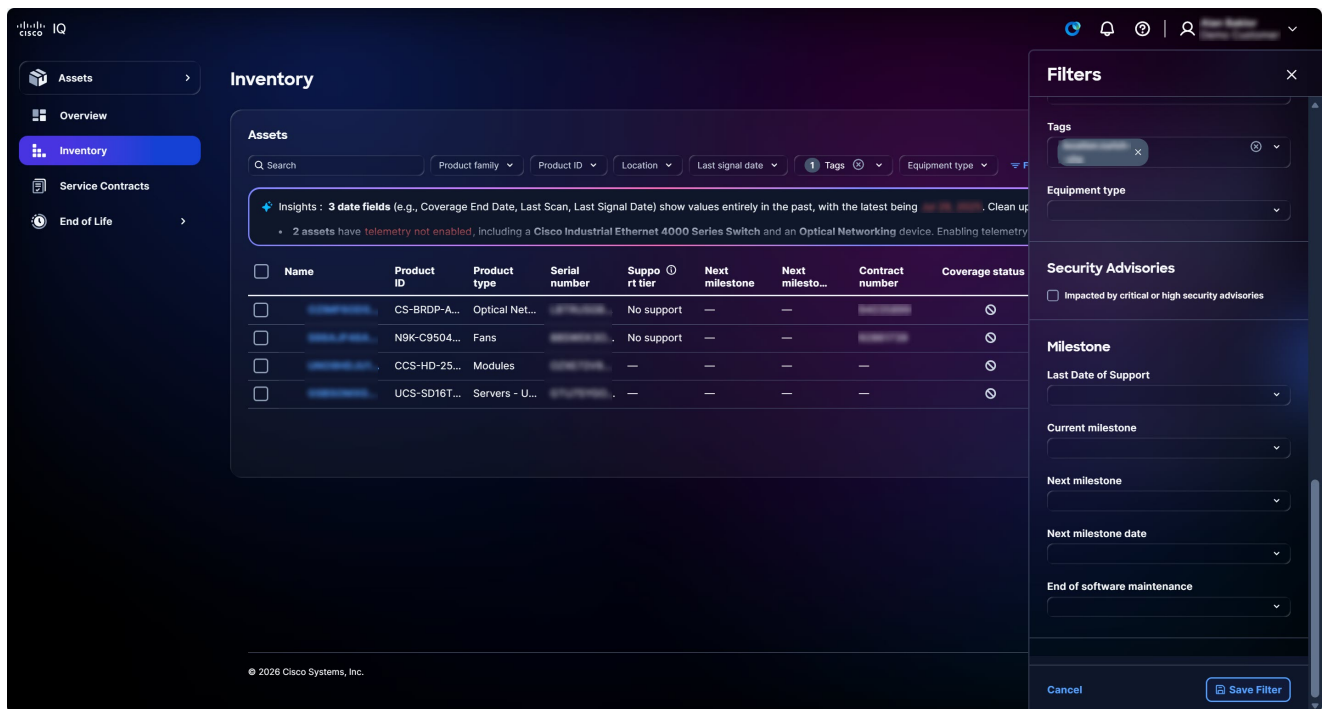
4. Fare clic sulla X su un tag qualsiasi per rimuoverlo dalla selezione.
5. Fare clic su Apply (Applica).

Utilizzo dei tag delle risorse come filtri

Dopo aver creato un tag, è possibile utilizzarlo come filtro.

Per utilizzare un tag come filtro:

1. Passare alla pagina Magazzino.
2. Fare clic su Filtri. Viene visualizzata la finestra Filtri.

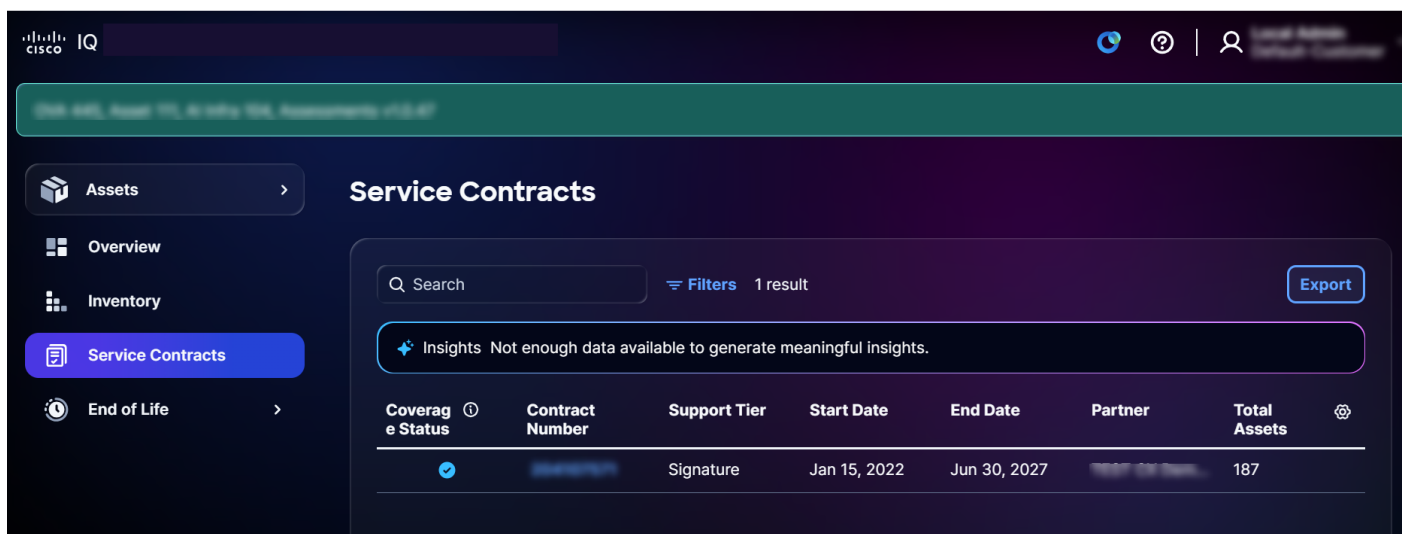


Utilizzo del tag come filtro

3. Dall'elenco a discesa Tag, selezionare le caselle di controllo dei tag desiderati. Dopo aver selezionato il cartellino, la vista nella pagina Inventario viene aggiornata alla vista filtrata.

Contratti di assistenza

La pagina Contratti di assistenza semplifica la supervisione dei contratti di assistenza fornendo riepiloghi e informazioni dettagliate sui contratti, supportando una pianificazione del rinnovo efficace e strategie di copertura.



Contratti di assistenza

Ricerca e filtraggio delle viste per i contratti di assistenza

È possibile filtrare la visualizzazione elenco scegliendo un filtro dagli elenchi a discesa. È inoltre possibile cercare contratti di assistenza immettendo il numero di contratto nel campo Cerca.

Esportazione dei contratti di assistenza

Fare clic su Esporta per salvare un elenco filtrato di contratti in formato xls o csv. Per ulteriori informazioni, vedere [Esportazione delle informazioni](#) nelle funzionalità comuni dei moduli.

Riepilogo EA servizi

La pagina Riepilogo del contratto EA (Services Enterprise Agreement) fornisce una vista consolidata della crescita della base installata nel portafoglio di asset. I dati provengono direttamente dai record della base installata di Cisco, offrendo all'utente e ai team responsabili degli account una visione coerente delle modifiche del portafoglio nel tempo.

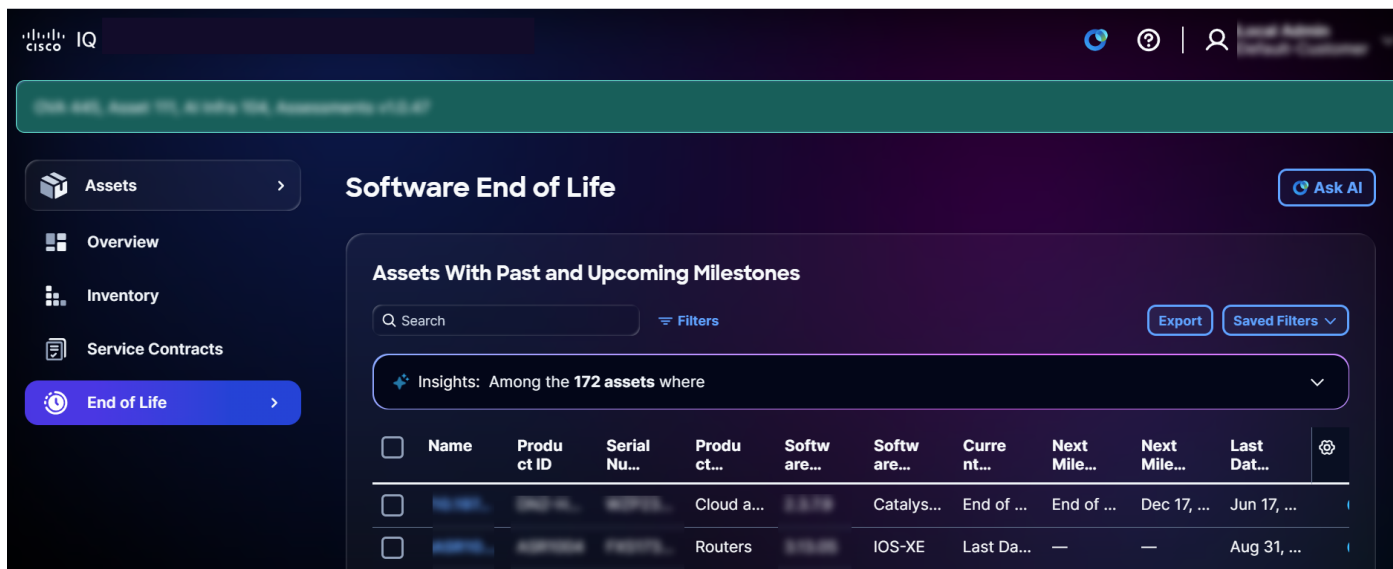
La pagina Riepilogo EA servizi visualizza le informazioni riportate di seguito.

- Risorse aggiunte: Nuove risorse aggiunte alla base installata durante il periodo di creazione rapporti
- Variazione netta: Modifica complessiva delle dimensioni della base installata per il periodo di creazione rapporti

 Nota: L'accesso alla pagina Riepilogo EA servizi può essere soggetto ai requisiti di ruolo e autorizzazione. Contattare l'amministratore dell'account se questa pagina non è visibile nella navigazione.

Fine del ciclo di vita

Le pagine Hardware End of Life e Software End of Life forniscono informazioni dettagliate sulla fine del ciclo di vita, fornendo agli utenti il supporto necessario per gestire in modo proattivo i cicli di aggiornamento dei prodotti e la copertura del supporto. Se si fa clic su una risorsa nella pagina Fine del ciclo di vita, si viene reindirizzati alla risorsa desiderata nella pagina Inventario.



Fine del ciclo di vita del software

Analisi alla fine del ciclo di vita

Il pannello Informazioni approfondite nella pagina Fine del ciclo di vita visualizza una panoramica delle risorse basata sull'IA con un ultimo giorno di supporto definito. Fare clic su Analisi completa per visualizzare visualizzazioni quali grafici, dashboard e grafici che forniscono ulteriori informazioni. Per ulteriori informazioni, vedere [Analisi dei dati](#) nelle funzionalità comuni dei moduli.

Esportazione della fine del ciclo di vita

Fate clic su Esporta (Export) per salvare un elenco filtrato di risorse di fine ciclo di vita in formato .xls o .csv. Per ulteriori informazioni, vedere [Esportazione delle informazioni](#) nelle funzionalità comuni dei moduli.

Modulo di valutazione

Il modulo Valutazioni fornisce una struttura di valutazione che consente di analizzare in modo proattivo e ridurre i rischi correlati a sicurezza, stabilità, capacità, conformità e invecchiamento, garantendo la sicurezza, la stabilità e l'affidabilità delle reti.

Concetti fondamentali

Il modulo Valutazioni è basato sui seguenti concetti fondamentali:

- **Valutazione:** una valutazione sistematica dei soggetti dell'infrastruttura sulla base di criteri predefiniti per misurare le prestazioni, la conformità, la sicurezza o la capacità operativa; Le valutazioni vengono attivate su richiesta, in base a un programma o da un evento
- **Esecuzione della valutazione:** un'istanza o un'unica esecuzione di una valutazione; Ogni esecuzione crea un nuovo record di esecuzione che tiene traccia dell'ambito, del meccanismo di attivazione, dell'indicatore orario e dei dati risultanti prodotti dalla valutazione
- **Ricerca di:** Osservazione convalidata e attivabile che identifica una lacuna, un rischio, un problema o uno stato degno di nota. I risultati rappresentano i dati a livello di suolo durante una valutazione
- **Insight:** Una conclusione analitica di livello superiore derivata da modelli o tendenze in più risultati. Le informazioni approfondite interpretano il significato dei risultati in un contesto aziendale o operativo più ampio
- **Consiglio:** una prescrizione specifica e praticabile collegata a constatazioni o conoscenze approfondite; Le raccomandazioni forniscono orientamenti chiari sulle misure necessarie per affrontare i problemi individuati o sfruttare le opportunità
- **Rapporto:** Un documento strutturato che raccoglie risultati, informazioni e raccomandazioni per un pubblico specifico; I report sono il principale strumento per comunicare i risultati delle valutazioni a clienti, dirigenti e team tecnici

Accesso al modulo Assessment

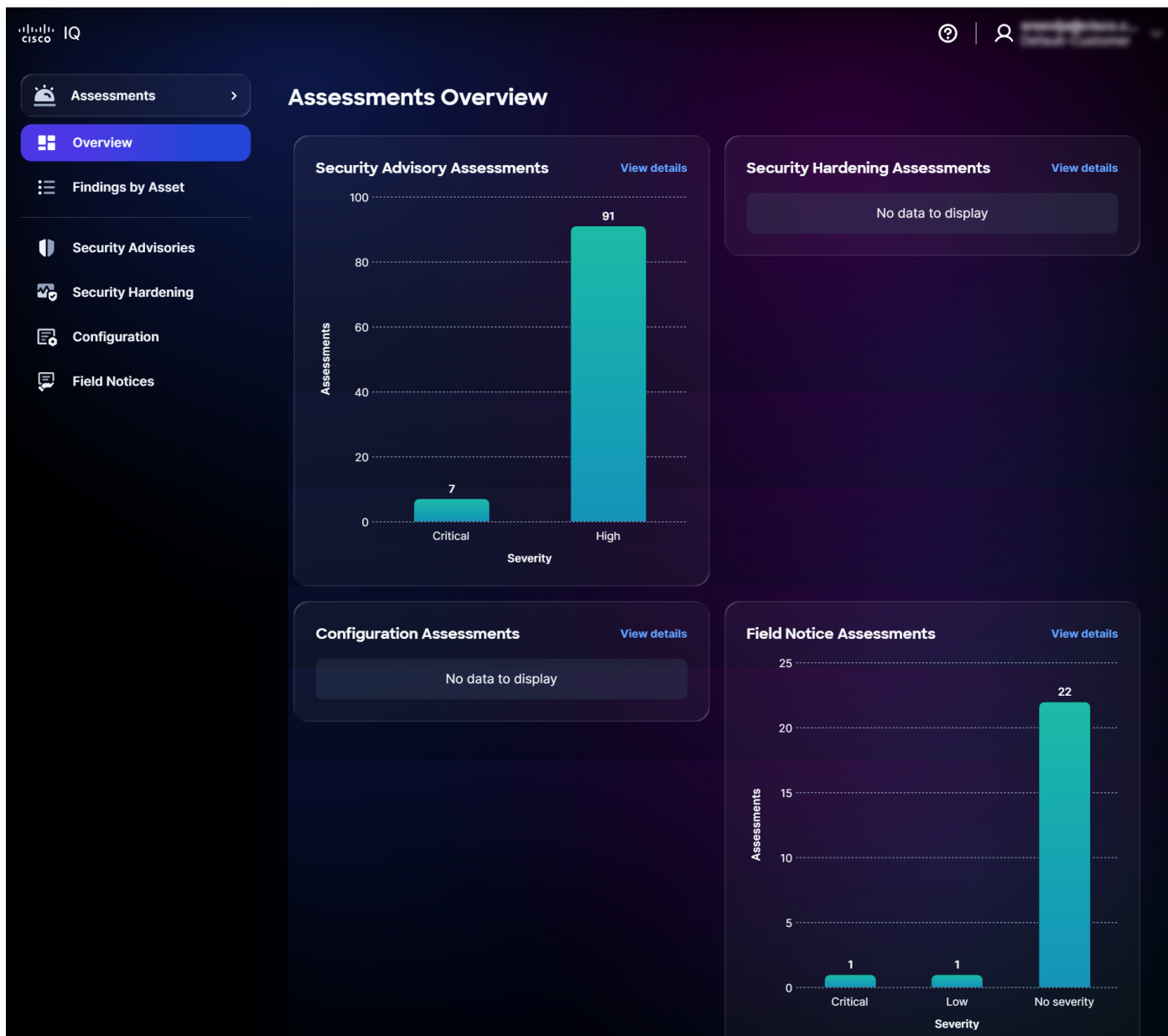
Per accedere alle funzioni di sicurezza e valutazione in Virtual Appliance, scegliere il menu Home > Valutazioni o fare clic su Valutazioni dalla sezione Applicazione della scheda Home page > Launchpad. Viene visualizzata la pagina Panoramica valutazioni.



Nota: Il modulo di valutazione può anche essere avviato da Configurazione di sistema > Gestione pacchetti.

Panoramica delle valutazioni

La pagina Panoramica valutazioni visualizza il dashboard riportato di seguito.



Panoramica delle valutazioni

Nel quadro comandi vengono visualizzate le informazioni riportate di seguito.

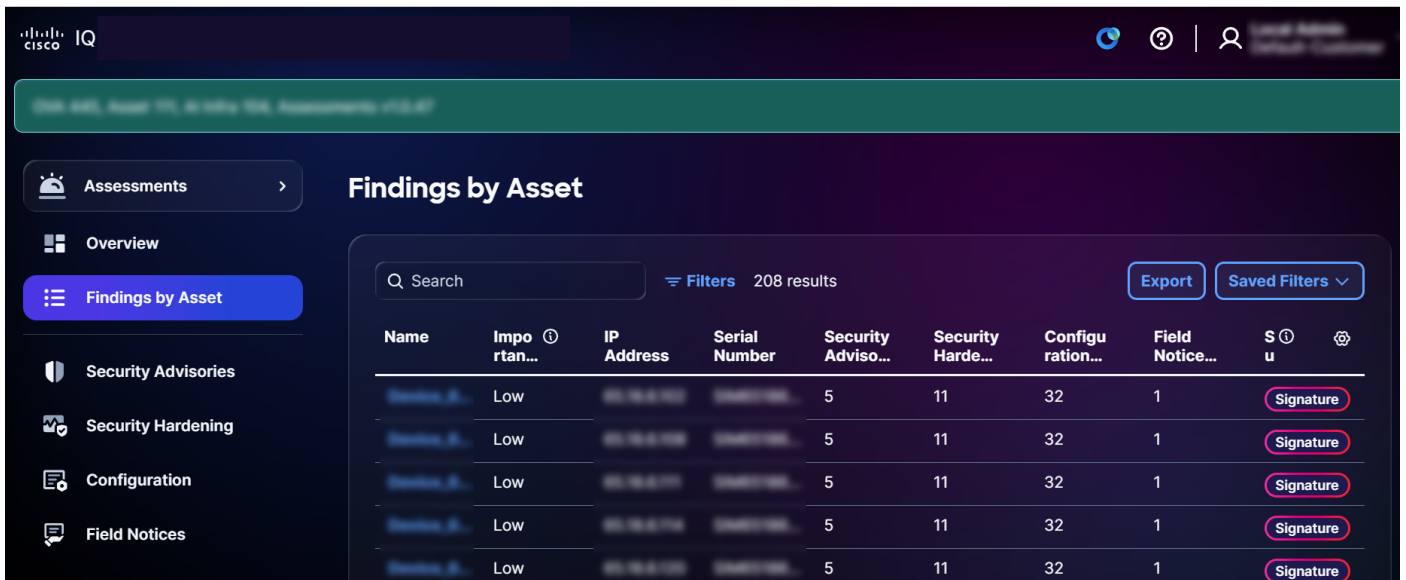
- **Valutazioni di Security Advisory:** Visualizza le valutazioni degli advisory della sicurezza, classificati in base alla criticità e all'alta gravità
- **Valutazioni della protezione avanzata:** Visualizza gli asset che non superano le regole di protezione avanzata, classificati in base alla gravità massima, media, bassa e informativa.
- **Valutazione della configurazione:** Visualizza gli asset che non soddisfano le regole di conformità della configurazione, suddivisi per livello di gravità critico, alto, medio, basso e informativo
- **Valutazioni delle notifiche sul campo:** Visualizza le valutazioni degli avvisi sui prodotti,

ordinati per livello di gravità Critico, Elevato e Non applicabile

 Nota: È possibile visualizzare solo gli asset a cui si è autorizzati ad accedere.

Risultati per cespiti

La pagina Risultati per cespiti fornisce un elenco di cespiti valutati utilizzando almeno una delle seguenti valutazioni: Consigli sulla sicurezza, protezione avanzata, configurazione e avvisi sui prodotti.



The screenshot shows the Cisco IQ interface for 'Findings by Asset'. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset (selected), Security Advisories, Security Hardening, Configuration, and Field Notices. The main content area displays a table of findings with columns: Name, Importance, IP Address, Serial Number, Security Advisories, Security Hardening, Configuration, Field Notices, and a Signature link. The table shows 208 results, all with a 'Low' importance level. The Signature column contains a 'Signature' link for each row.

Name	Importance	IP Address	Serial Number	Security Advisories	Security Hardening	Configuration	Field Notices	Signature
Security A...	Low	10.10.10.10	1000000000	5	11	32	1	Signature
Security A...	Low	10.10.10.10	1000000000	5	11	32	1	Signature
Security A...	Low	10.10.10.10	1000000000	5	11	32	1	Signature
Security A...	Low	10.10.10.10	1000000000	5	11	32	1	Signature
Security A...	Low	10.10.10.10	1000000000	5	11	32	1	Signature

Risultati per asset

Ricerca e filtro di viste per risultati per asset

È possibile filtrare la visualizzazione elenco scegliendo un filtro dagli elenchi a discesa oppure facendo clic su Filtri e scegliendo un'opzione dall'elenco dei filtri disponibili. È inoltre possibile cercare Risultati per cespiti nel campo Cerca.

 Nota:

- Alcuni filtri possono essere nascosti a seconda delle impostazioni di zoom.
- Sono disponibili diversi filtri a seconda dei ruoli e delle autorizzazioni.

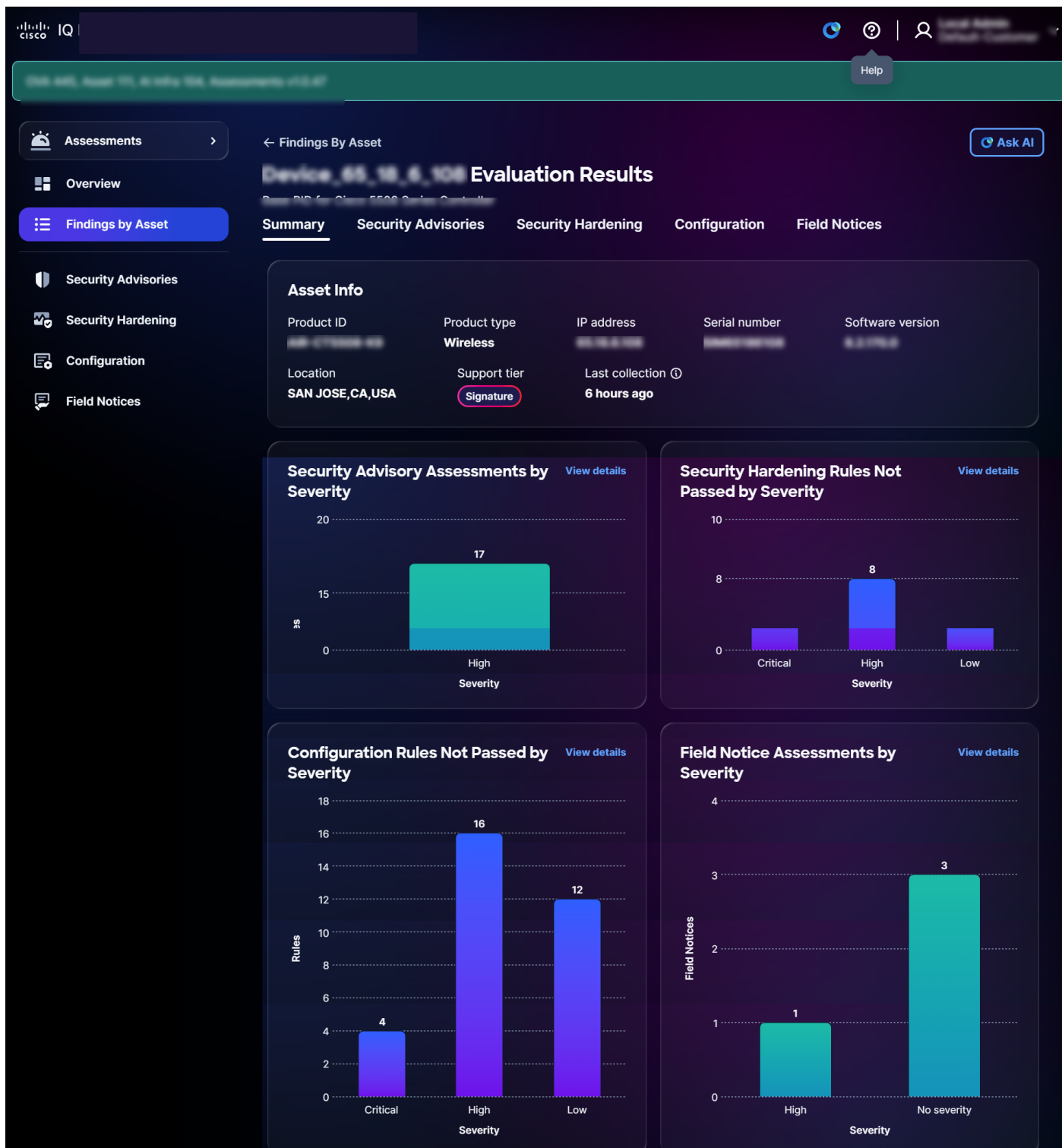
Esportazione dei risultati per asset

Per esportare la visualizzazione elenco Risultati per risorsa, fare clic su Esporta. Per ulteriori informazioni, vedere [Esportazione delle informazioni](#).

Visualizzazione dei risultati per dettagli cespiti

Per visualizzare i risultati per dettagli cespiti, fare clic su un cespiti. Nelle schede seguenti vengono visualizzati i dettagli relativi alla risorsa selezionata:

- **Riepilogo:** Fornisce informazioni dettagliate sugli asset, tra cui il numero di consigli sulla sicurezza, protezione avanzata, configurazione e avvisi sui prodotti
- **Consulenze sulla sicurezza:** Fornisce un elenco di valutazioni di Security Advisory correlate
- **Protezione avanzata:** Fornisce un elenco delle risorse che non superano le regole di protezione avanzata
- **Configurazione:** Fornisce un elenco di risorse che non superano le regole di best practice per la configurazione
- **Notifiche sul campo:** Fornisce un elenco di valutazioni di avvisi sui prodotti correlate



Risultati per dettagli cespite

Quando si fa clic su Visualizza dettagli in un riquadro, la pagina viene reindirizzata alla pagina appropriata all'interno del modulo.

Quando si fa clic su Visualizza dettagli completi asset, viene visualizzata la pagina di visualizzazione dei dettagli asset.

Consulenze sulla sicurezza

Le valutazioni dei servizi di consulenza per la sicurezza identificano le vulnerabilità e ne assegnano la priorità in base al rischio, alla gravità e alla criticità, migliorando in tal modo le capacità di gestione dei rischi dell'organizzazione. I consulenti per la sicurezza forniscono informazioni dettagliate sulle vulnerabilità, aiutano a ridurre i rischi e garantiscono l'allineamento con gli obiettivi aziendali e di conformità. Ciò rafforza la postura di sicurezza, ottimizza l'allocazione delle risorse e promuove la resilienza contro l'evoluzione delle minacce all'interno dell'azienda. Gli avvisi di sicurezza vengono aggiornati automaticamente in Cisco IQ non appena vengono pubblicati.

La pagina Consigli di sicurezza fornisce una lista di tutti gli avvisi di sicurezza con vulnerabilità rilevate all'interno dell'organizzazione. Se si fa clic su un advisory dall'elenco delle valutazioni degli advisory della sicurezza, viene visualizzata la vista dei dettagli corrispondente.

IQ

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Security Advisories

^

About the Assessments

These assessments compare your assets against Cisco Security Advisories. Security Advisories flag product security vulnerabilities that may need action to prevent incidents.

Security Advisory Assessments

Filters

98 results

Export

Saved Filters

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

Consulenze sulla sicurezza

Ricerca e filtraggio delle viste per i consigli sulla sicurezza

È possibile filtrare la visualizzazione elenco scegliendo un filtro dall'elenco a discesa. È inoltre possibile cercare le valutazioni di Security Advisory immettendo il nome della valutazione nel campo Cerca.



Nota:alcuni filtri potrebbero essere nascosti a seconda delle impostazioni di zoom dello schermo.Alcuni filtri potrebbero essere nascosti a seconda delle impostazioni di zoom dello schermo. Sono disponibili diversi filtri a seconda dei ruoli e delle autorizzazioni. I valori di severità mancanti vengono visualizzati come "-" con una descrizione comando descrittiva.

Esportazione degli avvisi di sicurezza

Per esportare le valutazioni di Security Advisory, fare clic su Esporta. Per ulteriori informazioni, vedere [Esportazione delle informazioni](#).

Visualizzazione dei dettagli della valutazione di Security Advisory

Fare clic su una valutazione per visualizzarne ulteriori dettagli. La pagina dei dettagli fornisce informazioni come il punteggio CVSS (Common Vulnerability Scoring System), le vulnerabilità e le esposizioni comuni (CVE), la gravità e un collegamento all'advisory della sicurezza Cisco a cui si fa riferimento.

Nella tabella Risultati della valutazione è possibile visualizzare i tipi di risultati riportati di seguito.

- **Interessato:** Indica che l'asset o il componente presenta una vulnerabilità confermata che può essere sfruttata da un utente non autorizzato e che richiede la risoluzione del problema
- **Potenzialmente interessati:** indica che l'attività o il componente presenta segni che possono portare a vulnerabilità, ma non è definitivamente confermato; potrebbero essere necessarie ulteriori indagini

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

← Security Advisories

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

About the Assessment

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

Show more

Severity

High

CVE

CVSS score

8.8

Version

1.1

First published

Sep 25, 2019

Last updated

Oct 4, 2019

References

[Security Advisory](#)

Asset Results

Q Search

Filters 12 results

Export

Saved Filters

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

Dettagli consigli di sicurezza

Ricerca e filtraggio delle viste per i risultati della valutazione degli asset

È possibile filtrare la visualizzazione elenco scegliendo un filtro dagli elenchi a discesa oppure facendo clic su Filtri e scegliendo un'opzione dall'elenco dei filtri disponibili. È inoltre possibile cercare le risorse immettendo il nome della risorsa nel campo Cerca.

Nota: Alcuni filtri potrebbero essere nascosti a seconda delle impostazioni di zoom dello schermo. Sono disponibili diversi filtri a seconda dei ruoli e delle autorizzazioni.

Visualizzazione dei risultati della valutazione dei cespiti

Per visualizzare i dettagli di un risultato della valutazione, fare clic su un cespite nella tabella Risultato valutazione. Viene visualizzata la pagina dei dettagli Risultato valutazione.

The screenshot displays the Cisco IQ interface for a security advisory. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories (highlighted), Security Hardening, Configuration, and Field Notices. The main content area shows the 'Result' for a 'Cisco Secure Boot Hardware Tampering Vulnerability' on device '65_10_4_108'. A status bar indicates 'Potentially affected'. The 'Evidence' section lists three matches: software type, chassis product ID, and module product ID. The 'Additional Verification Needed' section provides instructions for manual verification. The 'About the Assessment' section describes the vulnerability and includes a table with severity (High), CVE, CVSS score (6.7), first published date (May 13, 2019), and last updated date (Nov 20, 2019). The 'About the Asset' section shows details for the device, including product ID, product type (Switches), IP Address, serial number, software version, location (SAN JOSE, CA, USA), and support tier (Signature).

Security Advisories > Cisco Secure Boot Hardware Tampering Vulnerability

Device_65_10_4_108 Result [Ask AI](#)

Assessment: Cisco Secure Boot Hardware Tampering Vulnerability

Result Details Potentially affected

Evidence

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

Additional Verification Needed

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

About the Assessment

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

[Show more](#)

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

About the Asset [View evaluated asset](#)

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

Dettagli risultati

Esportazione dei risultati degli asset per i consigli sulla sicurezza

Per esportare i risultati delle risorse, fate clic su **Esporta (Export)**. Per ulteriori informazioni, vedere [Esportazione delle informazioni](#).

Protezione avanzata

La protezione avanzata offre una visibilità automatizzata in tempo reale sulla postura di sicurezza dell'infrastruttura di rete, grazie alla valutazione continua di router, switch e firewall rispetto ai benchmark standard del settore. Identifica le lacune nella configurazione e fornisce una guida attuabile per la risoluzione dei problemi, consentendo agli amministratori degli account di ridurre efficacemente la superficie di attacco e mantenere l'allineamento coerente con le rigorose best practice di Cisco in materia di sicurezza. Centralizzando il

monitoraggio della conformità e semplificando il processo di protezione, il modulo trasforma la gestione della sicurezza da un'attività reattiva in una strategia proattiva basata sui dati, garantendo una rete aziendale sicura e resiliente.

 **Nota:** Le valutazioni di protezione avanzata sono disponibili esclusivamente per gli asset con livelli di supporto standard.

Visualizzazione delle valutazioni di protezione avanzata

La pagina Valutazione protezione avanzata visualizza le informazioni riportate di seguito.

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Security Hardening Assessment

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

About the Assessment

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

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

Summary

Rule evaluations

179

Assets included

146

Rule evaluations

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

Q Search

Filters

179 results

Export

Saved Filters

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

Protezione avanzata

- **Valutazione:** Fornisce ulteriori dettagli riepillando lo scopo della valutazione
- **Risultato esecuzione:** Fornisce un riepilogo dei risultati della valutazione dei cespiti, incluso il numero totale di valutazioni delle regole e di cespiti inclusi
- **Valutazioni delle regole:** Fornisce informazioni dettagliate sulla regola, inclusi gravità, asset valutati, non superati, superati, non concludenti, non applicabili e tipo di software
- **Gravità:** Fornisce il livello di importanza o impatto della valutazione delle regole

- Cespiti valutati: Fornisce il numero totale di cespiti valutati in base ai criteri della regola
- Non superato: Fornisce le risorse che non hanno soddisfatto i criteri della regola durante la valutazione
- Superato: Fornisce le risorse che soddisfano i criteri della regola durante la valutazione
- Senza risultati: Fornisce le risorse per le quali la valutazione non ha potuto determinare l'errore
- Non applicabile: Indica le risorse o gli scenari in cui la regola non è applicabile o non è rilevante
- Tipo di software: Fornisce il tipo di software delle risorse

Ricerca e filtraggio delle viste per le regole

È possibile filtrare la visualizzazione elenco scegliendo un filtro dagli elenchi a discesa oppure facendo clic su Filtri e scegliendo un'opzione dall'elenco dei filtri disponibili. È inoltre possibile cercare una regola immettendo il nome della regola nel campo Cerca.



Nota:alcuni filtri potrebbero essere nascosti a seconda delle impostazioni di zoom dello schermo. Sono disponibili diversi filtri a seconda dei ruoli e delle autorizzazioni.

Visualizzazione dei dettagli di valutazione delle regole

Per visualizzare ulteriori dettagli sulla valutazione di una regola, fare clic su una regola. Viene visualizzata la pagina dei dettagli di valutazione della regola con le informazioni riportate di seguito.

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

About the Rule

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

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

Results Summary 31 assets

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

Asset Results

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

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

Visualizzazione regole

- Informazioni sulla regola: Fornisce dettagli sulla regola, ad esempio Gravità, Tipo di software, Versione e Asset valutati e include collegamenti descrittivi con etichetta alla documentazione di origine rilevante
- Riepilogo risultati: Fornisce un riepilogo dei risultati dei cespiti correlati alla regola, ad esempio Superato, Non superato, Non conclusivo e Non applicabile
- Risultati degli asset: Fornisce un elenco di asset con dettagli quali asset, risultato, ID prodotto, numero di serie, indirizzo IP e livello di supporto

 **Nota:** Cisco IQ fornisce una guida chiara quando un risultato della valutazione è "Non conclusivo", spiegando la causa (ad esempio, mancanza di dati di telemetria o sistema operativo non supportato) e consigliando procedure quali la verifica della raccolta dei dati, l'aggiornamento delle credenziali o l'aggiornamento dei dati. Per risolvere i problemi, sono inoltre disponibili collegamenti con etichetta alla documentazione pertinente.

Ricerca e filtraggio delle viste per le regole cespiti

È possibile filtrare la visualizzazione elenco scegliendo un filtro dagli elenchi a discesa oppure facendo clic su Filtri e scegliendo un'opzione dall'elenco dei filtri disponibili. È inoltre possibile cercare i risultati della valutazione dei cespiti immettendo il nome del cespite nel campo Cerca.



Nota:alcuni filtri potrebbero essere nascosti a seconda delle impostazioni di zoom dello schermo. Sono disponibili diversi filtri a seconda dei ruoli e delle autorizzazioni.

Esportazione dei risultati degli asset

Per esportare i risultati della valutazione per le regole, fare clic su Esporta. Per ulteriori informazioni, vedere [Esportazione delle informazioni](#).

Ricerca e filtraggio delle viste per i risultati degli asset

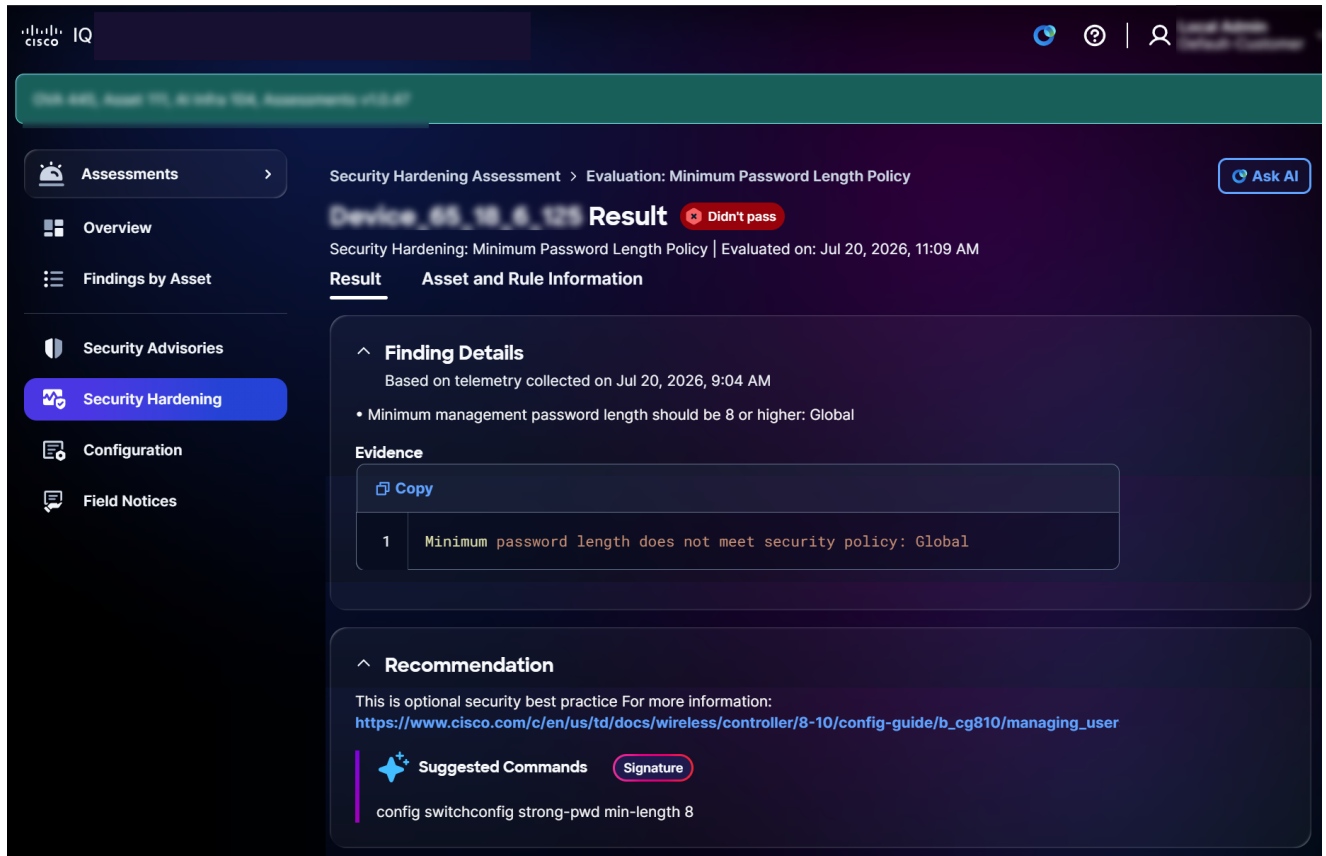
È possibile filtrare la visualizzazione elenco scegliendo un filtro dagli elenchi a discesa oppure facendo clic su Filtri e scegliendo un'opzione dall'elenco dei filtri disponibili. È inoltre possibile cercare i risultati dei cespiti immettendo il nome del cespite nel campo Cerca.



Nota: Alcuni filtri possono essere nascosti a seconda delle impostazioni di zoom. Sono disponibili diversi filtri a seconda dei ruoli e delle autorizzazioni.

Visualizzazione dei risultati degli asset per la protezione avanzata

Fare clic su un cespite in Risultati cespiti per visualizzarne i dettagli. Nella pagina dei dettagli del risultato del cespite vengono visualizzate le informazioni in base al livello o al livello di diritto.



Livello standard protezione avanzata

- Livello standard
- Dettagli ricerca: Fornisce informazioni sulle deviazioni della configurazione identificate durante la valutazione, insieme ai registri delle prove
- Consigli: Fornisce indicazioni per risolvere i problemi e garantire la coerenza della configurazione

Visualizzazione delle informazioni sugli asset e sulle regole per la protezione avanzata

Per visualizzare i dettagli di un cespite e le relative regole, fate clic sulla scheda Info cespite e regola (Asset and Rule Info). Viene visualizzata la pagina Informazioni su cespiti e regole.

Informazioni sulla risorsa: Fornisce i dettagli della risorsa, quali ID prodotto, tipo di prodotto, indirizzo IP, numero di serie, versione software, ubicazione e livello di supporto

- Informazioni sulla regola: Fornisce i dettagli della regola (tra cui gravità e tipo di software) e l'importanza di quel particolare controllo di protezione avanzata

Configurazione

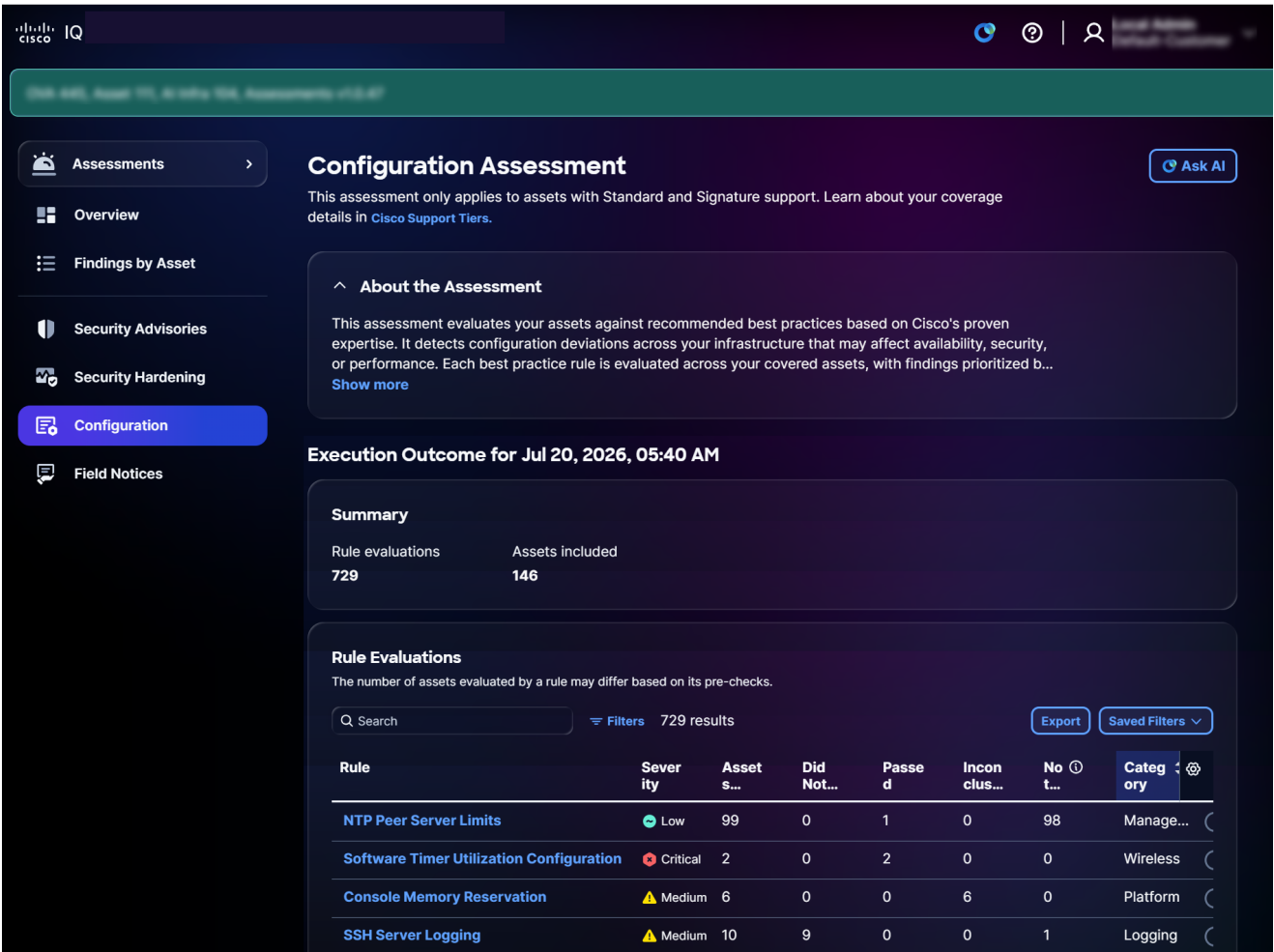
Le valutazioni della configurazione confrontano le risorse con le best practice consigliate sulla base dell'esperienza consolidata di Cisco nel rilevare le deviazioni della configurazione che possono influire sulla disponibilità, la sicurezza o le prestazioni dell'infrastruttura.

Ciascuna regola delle procedure ottimali viene valutata a livello delle risorse coperte e i risultati vengono classificati in base alla gravità per garantire la coerenza della configurazione, una migliore resilienza e una riduzione del rischio operativo.

 **Nota:** Le valutazioni della configurazione sono disponibili esclusivamente per gli asset con livelli di supporto standard.

Visualizzazione delle valutazioni della configurazione

La pagina Valutazione della configurazione visualizza le informazioni riportate di seguito.



Configuration Assessment

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

About the Assessment

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

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

Summary

Rule evaluations	Assets included
729	146

Rule Evaluations

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

Search: Filters 729 results [Export](#) [Saved Filters](#)

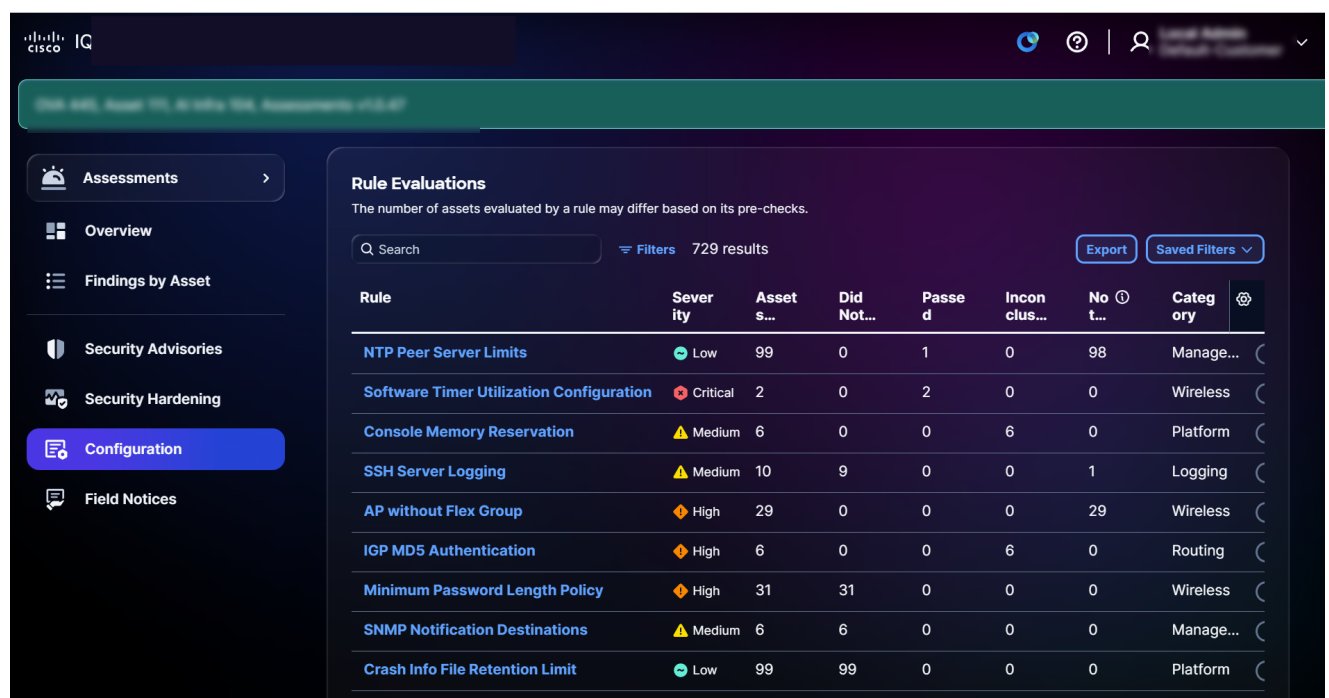
Rule	Severity	Asset s...	Did Not...	Passe d	Incon clus...	No t...	Categ ory
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless
Console Memory Reservation	Medium	6	0	0	6	0	Platform
SSH Server Logging	Medium	10	9	0	0	1	Logging

Valutazione della configurazione

- **Valutazione:** Fornisce ulteriori dettagli riempiendo lo scopo della valutazione
- **Riepilogo:** Fornisce un riepilogo dell'esecuzione della configurazione, ad esempio regole valutate e asset valutati
- **Informazioni approfondite:** Fornisce informazioni dettagliate sulle lacune di configurazione individuate generate mediante l'analisi dei modelli e una correlazione dei risultati. vengono visualizzate come schede principali raggruppate in modo intelligente per evidenziare le aree più critiche che richiedono attenzione

- **Valutazioni regole:** Fornisce informazioni dettagliate sulla regola, tra cui Gravità, Asset valutati, Non superato, Superato, Non conclusivo, Non applicabile, Categoria e Tipo di software
- **Gravità:** Fornisce il livello di importanza o impatto della valutazione delle regole
- **Cespiti valutati:** Fornisce il numero totale di cespiti valutati in base ai criteri della regola
- **Non superato:** Fornisce il numero totale di asset che non hanno soddisfatto i criteri della regola durante la valutazione
- **Senza risultati:** Indica il numero totale di asset per i quali non è stato possibile eseguire la valutazione
- **Superato:** Fornisce le risorse che soddisfano i criteri della regola durante la valutazione
- **Non applicabile:** Indica le risorse o gli scenari in cui la regola non è applicabile o non è rilevante
- **Categoria:** Fornisce l'area di dominio a cui appartiene la regola
- **Tipo di software:** Indica il tipo di risorse software a cui si applica la regola

Ricerca e filtraggio delle viste per le regole



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

Search: Filters: 729 results Export Saved Filters

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

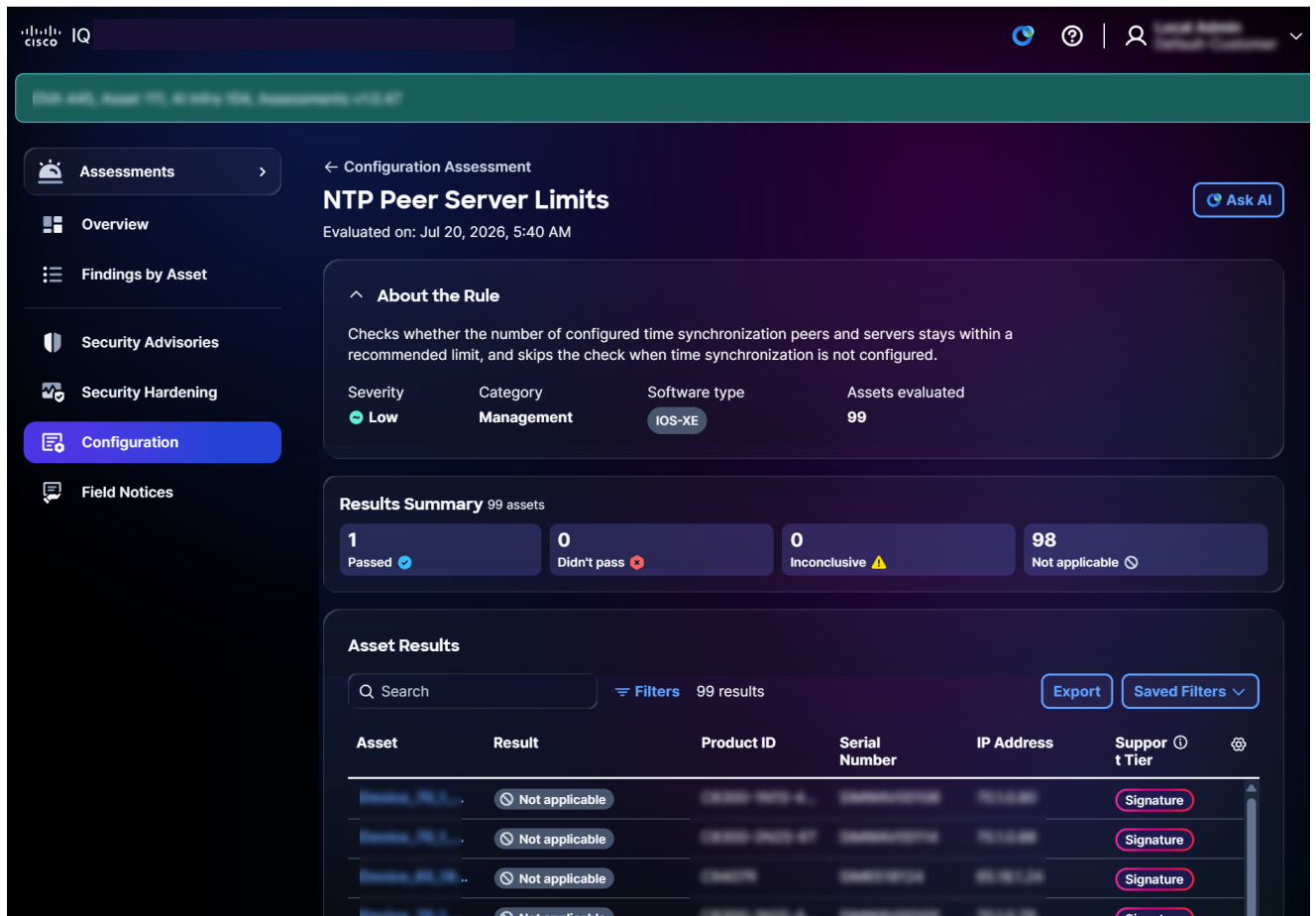
Valutazioni regole

È possibile filtrare la visualizzazione elenco scegliendo un filtro dagli elenchi a discesa oppure facendo clic su Filtri e scegliendo un'opzione dall'elenco dei filtri disponibili. È inoltre possibile cercare una regola immettendo il nome della regola nel campo Cerca.

 Nota: Alcuni filtri possono essere nascosti a seconda delle impostazioni di zoom. Sono disponibili diversi filtri a seconda dei ruoli e delle autorizzazioni.

Visualizzazione dei dettagli di valutazione delle regole

Per visualizzare ulteriori dettagli sulla valutazione di una regola, fare clic su qualsiasi regola. Viene visualizzata la pagina dei dettagli di valutazione della regola con le informazioni riportate di seguito.



The screenshot shows the Cisco IQ interface for a Configuration Assessment. The main heading is "NTP Peer Server Limits", evaluated on Jul 20, 2026, at 5:40 AM. The left sidebar contains navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (selected), and Field Notices. The main content area includes an "About the Rule" section, a "Results Summary" for 99 assets, and an "Asset Results" table.

About the Rule

Checks whether the number of configured time synchronization peers and servers stays within a recommended limit, and skips the check when time synchronization is not configured.

Severity	Category	Software type	Assets evaluated
Low	Management	IOS-XE	99

Results Summary 99 assets

Passed	Didn't pass	Inconclusive	Not applicable
1	0	0	98

Asset Results

Search: Filters 99 results Export Saved Filters

Asset	Result	Product ID	Serial Number	IP Address	Support Tier
Router, 78.1.1...	Not applicable	CISCO-7810-4...	00000000000000000000	78.1.1.1	Signature
Router, 78.1.1...	Not applicable	CISCO-7810-4...	00000000000000000000	78.1.1.2	Signature
Router, 78.1.1...	Not applicable	CISCO-7810-4...	00000000000000000000	78.1.1.3	Signature
Router, 78.1.1...	Not applicable	CISCO-7810-4...	00000000000000000000	78.1.1.4	Signature

Valutazione

- Informazioni sulla regola: Fornisce dettagli su una regola come Gravità, Categoria, Tipo di software e Asset valutati e include collegamenti descrittivi con etichetta alla documentazione di origine rilevante
- Riepilogo risultati: Fornisce i risultati globali dei cespiti visualizzando il numero di cespiti negli stati Superato, Non superato, Non conclusivo e Non applicabile
- Risultati degli asset: Fornisce un elenco degli asset interessati dalla regola selezionata con stato del risultato

 Nota: Cisco IQ fornisce una guida chiara quando un risultato della valutazione è "Non conclusivo", spiegando la causa (ad esempio, mancanza di dati di telemetria o sistema

 operativo non supportato) e consigliando procedure quali la verifica della raccolta dei dati, l'aggiornamento delle credenziali o l'aggiornamento dei dati. Per risolvere i problemi, sono inoltre disponibili collegamenti con etichetta alla documentazione pertinente. Il modulo di valutazione supporta la selezione di più categorie per le regole, consentendo l'elaborazione e la valutazione simultanee tra più categorie di regole.

Esportazione dei risultati degli asset

Per esportare i risultati delle risorse per le regole, fate clic su Esporta (Export). Per ulteriori informazioni, vedere [Esportazione delle informazioni](#).

Ricerca e filtraggio delle viste per i risultati degli asset

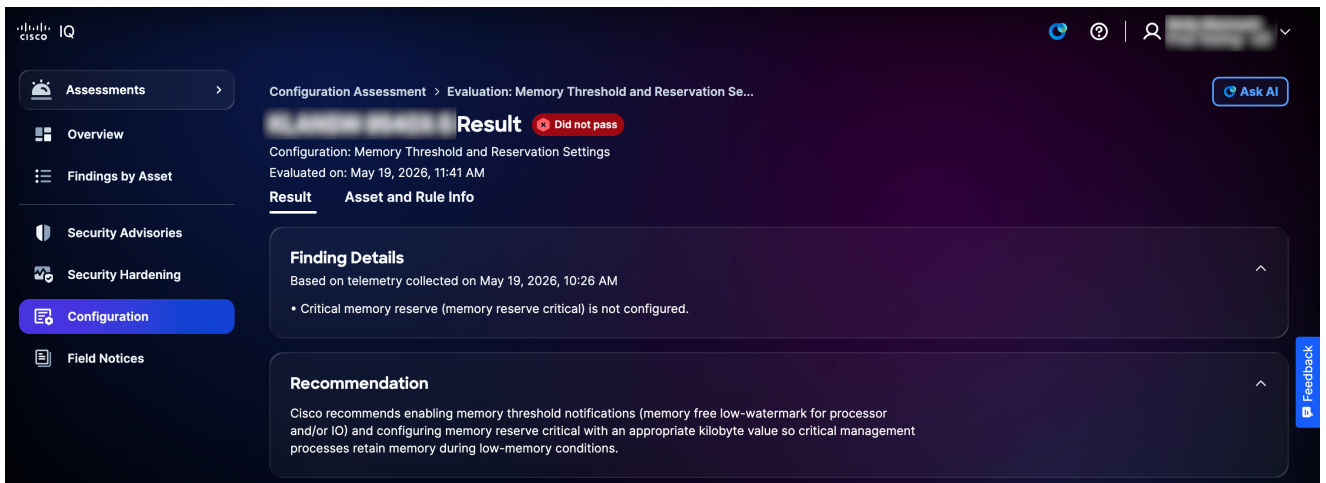
È possibile filtrare la visualizzazione elenco scegliendo un filtro dagli elenchi a discesa oppure facendo clic su Filtri e scegliendo un'opzione dall'elenco dei filtri disponibili. È inoltre possibile cercare i risultati dei cespiti immettendo il nome del cespite nel campo Cerca.

 Nota: Alcuni filtri possono essere nascosti a seconda delle impostazioni di zoom. Sono disponibili diversi filtri a seconda dei ruoli e delle autorizzazioni.

Visualizzazione dei risultati degli asset per le valutazioni della configurazione

Per visualizzare i dettagli dei risultati dei cespiti, fare clic su un cespite dai risultati dei cespiti.

Nella pagina dei dettagli del risultato del cespite vengono visualizzate le informazioni in base al livello o al livello di diritto.



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

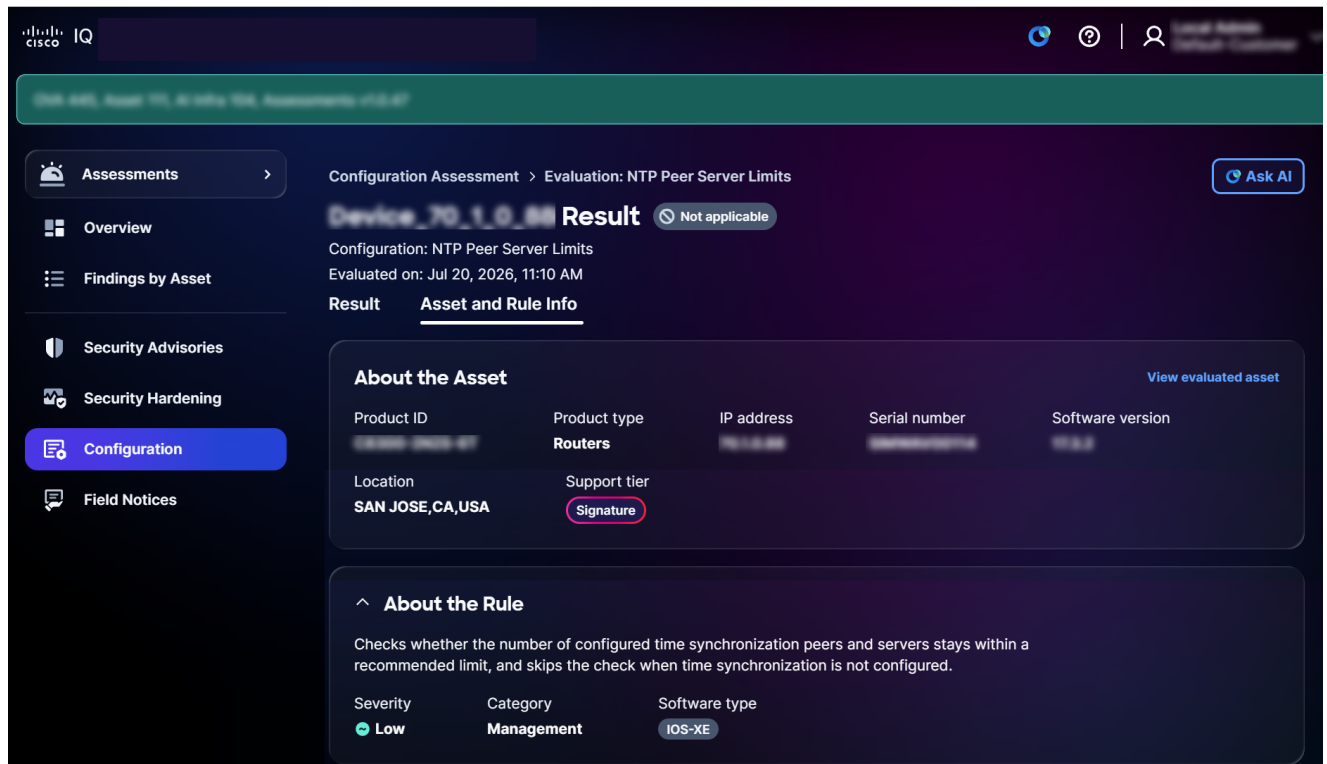
Livello standard di configurazione

- Livello standard
- Dettagli ricerca: Fornisce informazioni sulle deviazioni della configurazione identificate durante la valutazione, insieme ai registri delle prove

- Consigli: Fornisce indicazioni per risolvere i problemi e garantire la coerenza della configurazione

Visualizzazione delle informazioni sugli asset e sulle regole per le valutazioni della configurazione

Per visualizzare i dettagli relativi alle informazioni su cespiti e regole, fate clic sulla scheda Informazioni su cespiti e regole (Asset and Rule Info).



Informazioni su cespiti e regole

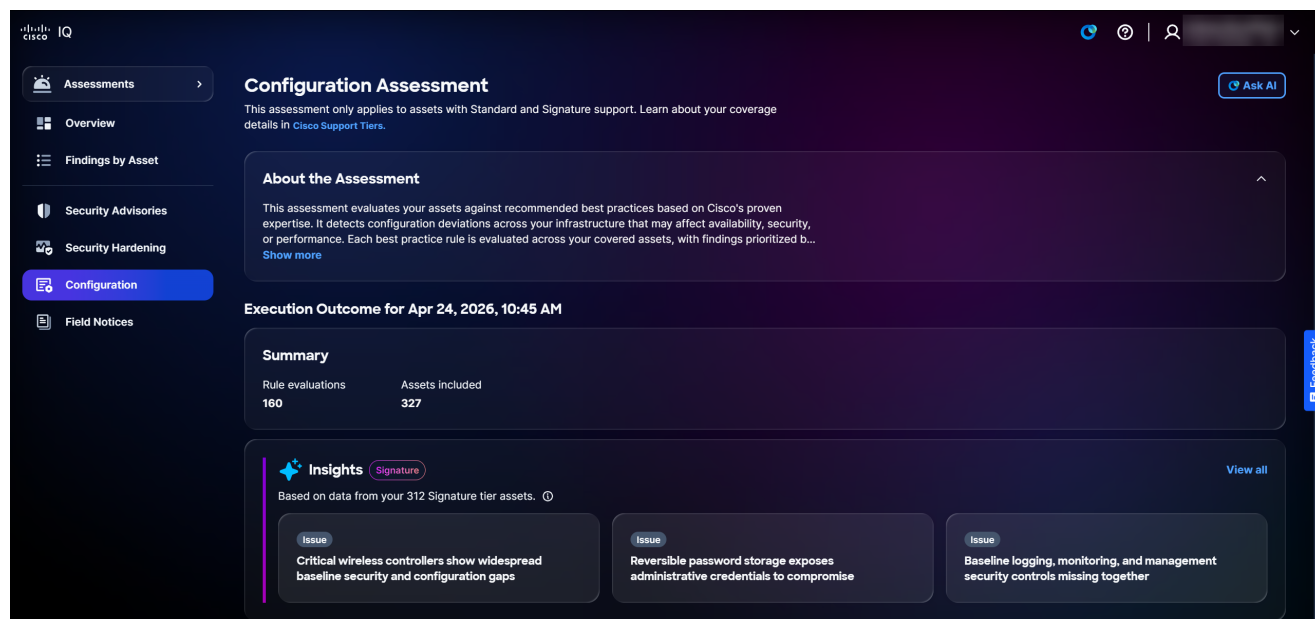
Viene visualizzata la pagina Informazioni su cespiti e regole con le informazioni riportate di seguito.

- Informazioni sulla risorsa: Fornisce i dettagli di una risorsa, ad esempio ID prodotto, tipo di prodotto, indirizzo IP, numero di serie, versione software, ubicazione e livello di supporto
- Informazioni sulla regola: Fornisce i dettagli di una regola, ad esempio Gravità, Categoria e Tipo di software

Visualizzazione di informazioni approfondite

Le informazioni approfondite sono generate dall'intelligenza artificiale e fungono da dashboard intelligente che sintetizza i dati di valutazione in schede chiave con priorità, evidenziando le differenze di configurazione critiche tra più risultati. Consente di affrontare in modo efficiente i rischi di infrastruttura più impattanti concentrandosi su queste aree urgenti. Vengono inoltre evidenziati i punti di forza identificando le aree in cui l'infrastruttura funziona

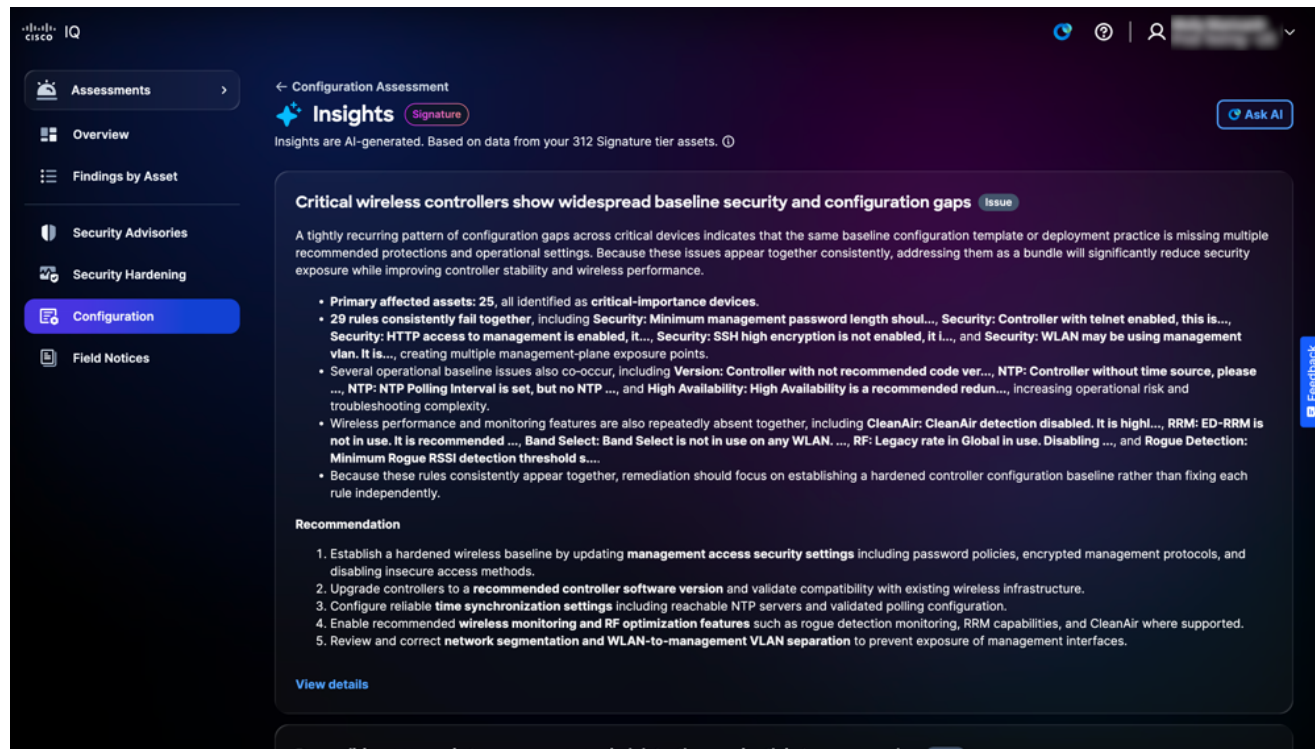
correttamente e le procedure ottimali.



Informazioni approfondite

Per visualizzare i dettagli di Insights:

1. Nel pannello Informazioni approfondite, fare clic su Visualizza tutto. La pagina Informazioni approfondite visualizza tutte le informazioni dettagliate.



Pagina Informazioni approfondite

2. Fare clic su Visualizza dettagli o su una scheda qualsiasi. Viene visualizzata la pagina Dettagli di Insights con le informazioni riportate di seguito.

Configuration Assessment > Insights

Critical wireless controllers show widespread baseline security and configuration gaps

Insights are AI-generated. Based on data from 312 assets with Signature support. ⓘ

[Signature](#) [Ask AI](#)

Details **Source Findings**

Insight

A tightly recurring pattern of configuration gaps across critical devices indicates that the same baseline configuration template or deployment practice is missing multiple recommended protections and operational settings. Because these issues appear together consistently, addressing them as a bundle will significantly reduce security exposure while improving controller stability and wireless performance.

- **Primary affected assets:** 25, all identified as **critical-importance devices**.
- **29 rules consistently fail together**, including **Security: Minimum management password length should be 12 characters or more**, **Security: Controller with telnet enabled, this is insecure**, **Security: HTTP access to management is enabled, it is insecure**, **Security: SSH high encryption is not enabled, it is insecure**, and **Security: WLAN may be using management vlan. It is insecure**, creating multiple management-plane exposure points.
- Several operational baseline issues also co-occur, including **Version: Controller with not recommended code version**, **NTP: Controller without time source, please use NTP**, **NTP: NTP Polling Interval is set, but no NTP server is configured**, and **High Availability: High Availability is a recommended redundancy feature**, increasing operational risk and troubleshooting complexity.
- Wireless performance and monitoring features are also repeatedly absent together, including **CleanAir: CleanAir detection disabled. It is highly recommended to enable it**, **RRM: ED-RRM is not in use. It is recommended to enable it**, **Band Select: Band Select is not in use on any WLAN. It is recommended to enable it**, **RF: Legacy rate in Global is in use. Disabling it is recommended**, and **Rogue Detection: Minimum Rogue RSSI detection threshold should be -90 dBm**.
- Because these rules consistently appear together, remediation should focus on establishing a hardened controller configuration baseline rather than fixing each rule independently.

Recommendation

1. Establish a hardened wireless baseline by updating **management access security settings** including password policies, encrypted management protocols, and disabling insecure access methods.
2. Upgrade controllers to a **recommended controller software version** and validate compatibility with existing wireless infrastructure.
3. Configure reliable **time synchronization settings** including reachable NTP servers and validated polling configuration.
4. Enable recommended **wireless monitoring and RF optimization features** such as rogue detection monitoring, RRM capabilities, and CleanAir where supported.
5. Review and correct **network segmentation and WLAN-to-management VLAN separation** to prevent exposure of management interfaces.

Affected Assets

Q Search Product type Product family Product ID 25 results

Name	Product ID	Serial Number	IP Address
WLC-1	WLC-1	WLC-1	WLC-1
WLC-2	WLC-2	WLC-2	WLC-2
WLC-3	WLC-3	WLC-3	WLC-3

Dettagli informazioni approfondite

- **Insight:** Fornisce un riepilogo che evidenzia i modelli ricorrenti di deviazioni della configurazione identificati attraverso un'analisi completa su più risultati, nonché le aree di eccellenza dell'infrastruttura in cui le configurazioni sono allineate alle best practice
 - **Consiglio:** Fornisce una serie di procedure per correggere le lacune di configurazione identificate
 - **Asset interessati:** Fornisce un elenco di dispositivi specifici in cui la deviazione di configurazione è stata identificata come definito nella sezione Insight
3. Fare clic su **Source Findings**. La pagina Risultati di origine visualizza i singoli risultati dettagliati che supportano le informazioni dettagliate dell'utente.

Configuration Assessment > Insights

Critical wireless controllers show widespread baseline security and configuration gaps

Insights are AI-generated. Based on data from 312 assets with Signature support. ⓘ

Details Source Findings

Q Search Severity Result 725 results Export

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

Risultati di origine

È possibile filtrare la vista tabella scegliendo un filtro dagli elenchi a discesa Gravità e Risultato.



Nota: I suggerimenti e le risorse interessate sono facoltativi a seconda dell'output di ciascuna analisi.

Notifiche sul campo

Gli avvisi sui prodotti identificano problemi significativi non correlati alla sicurezza e li organizzano in base alla gravità e alla criticità dell'impatto, migliorando la capacità dell'organizzazione di gestire i rischi dei prodotti. Gli avvisi sui prodotti forniscono informazioni utili sui difetti dei prodotti, riducono i tempi di attenuazione dei problemi tramite aggiornamenti consigliati o soluzioni alternative e garantiscono l'allineamento con gli obiettivi operativi e aziendali. In questo modo si rafforza l'affidabilità dei prodotti, si ottimizza l'allocazione delle risorse e si favorisce la resilienza contro le sfide in continua evoluzione dei prodotti all'interno dell'azienda.

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Field Notices

Ask AI

^

About the Assessments

These assessments compare your assets against Cisco Field Notices. Field Notices flag non-security product issues that may need action to prevent incidents.

Field Notice Assessments

Q Search

Filters 47 results

Export

Saved Filters

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

Notifiche sul campo

Ricerca e filtro di visualizzazioni per avvisi sui prodotti

È possibile filtrare la visualizzazione elenco scegliendo un filtro dagli elenchi a discesa. È inoltre possibile cercare le valutazioni delle notifiche sul campo immettendo il nome della valutazione nel campo Cerca.

Visualizzazione delle valutazioni per gli avvisi sui prodotti

Per visualizzare ulteriori dettagli su un avviso sui prodotti, fare clic su una valutazione. Vengono visualizzati i seguenti dettagli della valutazione:

- Informazioni sulle valutazioni: Fornisce ulteriori dettagli riepilogando lo scopo della valutazione
- Valutazioni delle notifiche sul campo: Visualizza un elenco di asset interessati dall'avviso di campo selezionato, inclusi gli asset con vulnerabilità rilevate

The screenshot shows the Cisco IQ interface for Field Notices. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration, and Field Notices (highlighted). The main content area displays a critical field notice titled 'FN74223 - Some Cisco NCS 540 Series Medium Density Routers May Become Unresponsive After Upgrade to Cisco IOS XR Software Release 7.11.1 or Later - Workaround Provided'. The notice is categorized as 'Critical' and was last updated on 'Dec 11, 2024'. Below the notice details, the 'Asset Results' section shows a table with 3 results, each marked as 'Potentially affected'.

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

Visualizzazione delle valutazioni per gli avvisi sui prodotti

Ricerca e filtraggio delle visualizzazioni per i risultati dei cespiti per gli avvisi sui prodotti

È possibile filtrare la visualizzazione elenco scegliendo un filtro dagli elenchi a discesa oppure facendo clic su Filtri e scegliendo un'opzione dall'elenco dei filtri disponibili. È inoltre possibile cercare i risultati dei cespiti immettendo il nome del cespite nel campo Cerca.



Nota: Alcuni filtri possono essere nascosti a seconda delle impostazioni di zoom. Sono disponibili diversi filtri a seconda dei ruoli e delle autorizzazioni.

Esportazione dei risultati degli asset per gli avvisi sui prodotti

Per esportare i risultati degli asset di valutazione per gli avvisi sui prodotti, fare clic su Esporta. Per ulteriori informazioni, vedere [Esportazione delle informazioni](#).

Visualizzazione dei risultati della valutazione dei cespiti per gli avvisi sui prodotti

Per visualizzare i dettagli dei risultati della valutazione di un cespite, fare clic su un cespite in Risultati valutazione cespiti. Viene visualizzata la pagina dei dettagli del risultato della valutazione del cespite.

È possibile visualizzare i seguenti tipi di risultati:

- Interessato: Indica le risorse che soddisfano tutti i criteri controllati automaticamente

per un avviso sui prodotti e che non richiedono ulteriori verifiche manuali per confermare l'impatto

- Potenzialmente interessati: Indica le risorse che soddisfano tutti i criteri controllati automaticamente per un avviso sui prodotti ma che richiedono ulteriori verifiche manuali per verificare se hanno un impatto reale

Nella scheda Valutazioni - Protezione avanzata sono disponibili i seguenti prompt:

- Quali sono le best practice di Cisco Security Hardening per i dispositivi di rete?
- Come fortificare i dispositivi Cisco IOS XE?
- Elencare le fasi di protezione avanzata per router e switch.
- Quali sono le impostazioni di protezione avanzata della linea di base consigliate per i dispositivi Cisco?
- Quanti asset violano le best practice per il rafforzamento della sicurezza?

Autenticazione locale

Per accedere correttamente a VA, gli amministratori account devono utilizzare le credenziali seguenti:

- Nome utente predefinito: admin
- Password predefinita: la password impostata durante il processo di installazione di VA. fare riferimento alla Guida introduttiva per ulteriori informazioni
- Contesto account predefinito: Default-Cliente

Al momento dell'accesso, l'utente predefinito, "admin", e il nome dell'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).

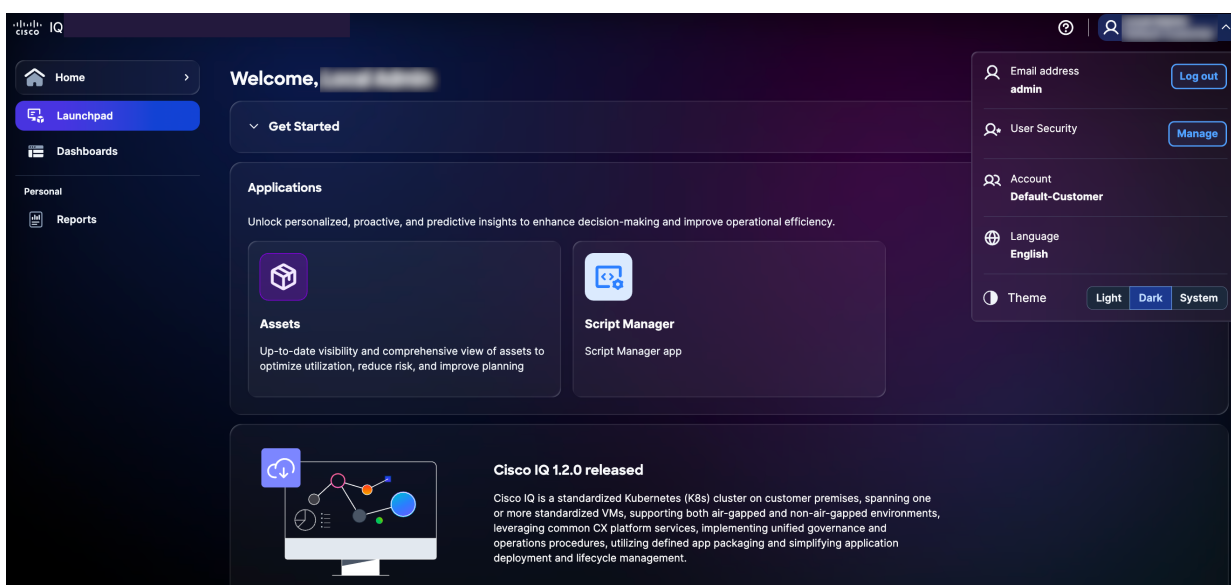
 **Nota:** Si hanno a disposizione tre (3) tentativi per immettere la password corretta entro un periodo di 15 minuti. Se tutti e tre (3) i tentativi hanno esito negativo, l'account viene temporaneamente bloccato per 30 minuti per proteggere la protezione. Non è possibile tentare l'accesso durante il 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.



Usa protezione

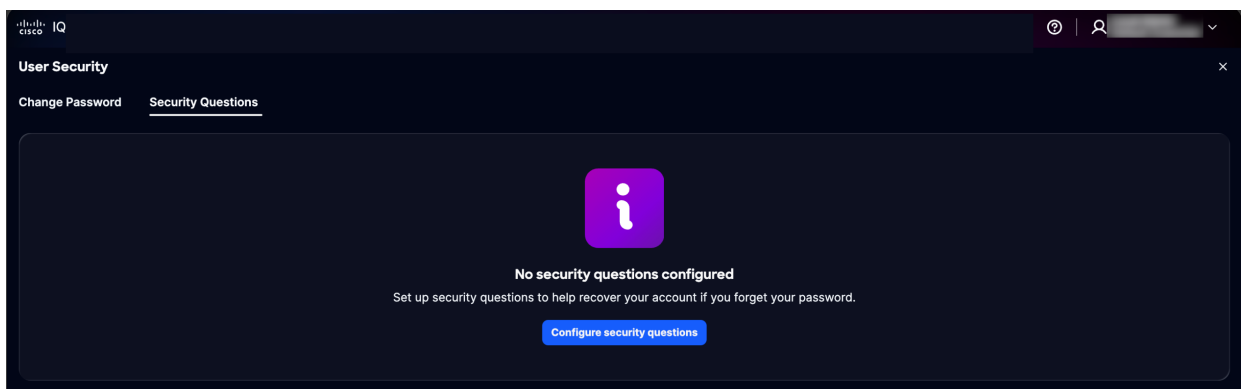
2. Fare clic su Gestisci in Protezione utente. Verrà visualizzata la pagina Sicurezza utente.



The screenshot shows the Cisco IQ User Security interface. The 'Change Password' tab is active. It displays a list of password requirements: At least 15 characters, At least 2 uppercase characters, At least 2 lowercase characters, At least 2 numeric characters, At least 2 special characters, and No repeating characters. Below these requirements are three input fields: 'Password', 'New password', and 'Confirm password', each with a 'Show' button. A 'Save' button is at the bottom left.

Domande di sicurezza

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



The screenshot shows the Cisco IQ User Security interface with the 'Security Questions' tab active. It features a large blue information icon (i) in the center. Below the icon, the text reads 'No security questions configured' and 'Set up security questions to help recover your account if you forget your password.' A blue button labeled 'Configure security questions' is positioned at the bottom center.

Scheda Domande di sicurezza

4. Fare clic su Configura domande di sicurezza.



User Security

[Change Password](#)[Security Questions](#)

Security Questions

Set up security questions to help recover your account if you forget your password. You must answer all questions.

Question 1 *

Select a security question

Answer *

Question 2 *

Select a security question

Answer *

Question 3 *

Select a security question

Answer *

Question 4 *

Select a security question

Answer *

Question 5 *

Select a security question

Answer *

Configura domande di sicurezza

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



Nota: Nelle risposte non viene fatta distinzione tra maiuscole e minuscole. Ad esempio, "SMITH" e "smith" vengono considerati uguali. Gli spazi aggiuntivi vengono ignorati, il che significa che "Smith" e "Smith" vengono trattati allo stesso modo. Ricordare come è stata immessa la risposta, ad esempio nomi completi o soprannomi. Usa risposte chiare che ti ricorderai



anni dopo. Scegliete le domande con risposte che non cambieranno nel tempo.



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 la 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, sarà necessario impostare una nuova password prima di poter accedere al sistema (se configurato su 0, la scadenza della password è disabilitata).

Prerequisiti

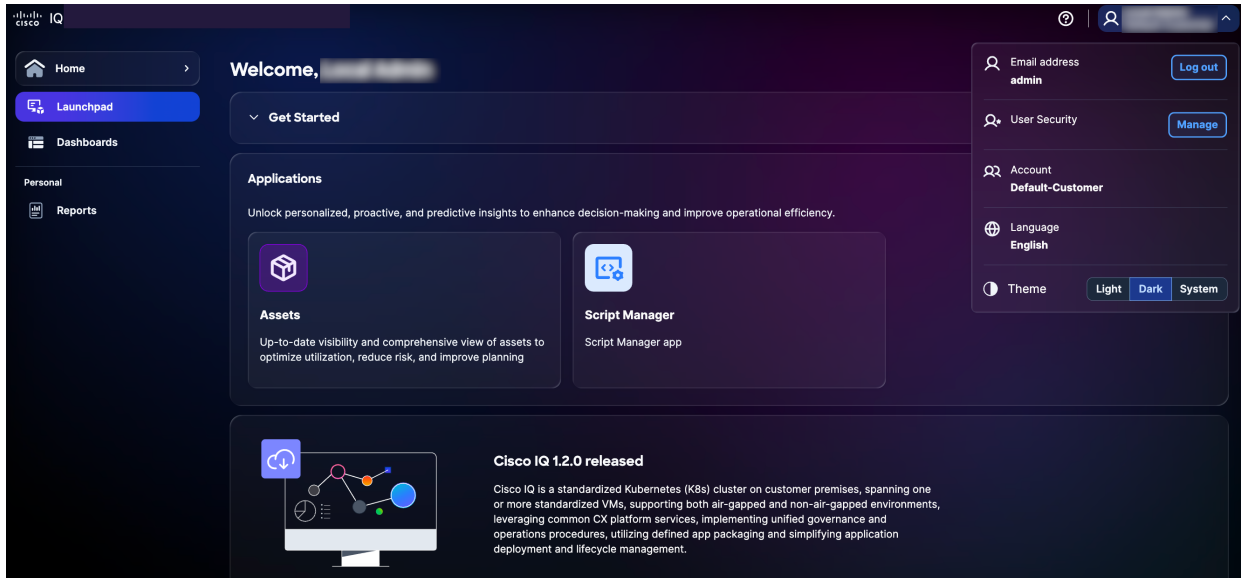
Per gestire le password, è necessario che siano soddisfatte le seguenti condizioni:

- 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)
- Sei connesso a Cisco IQ
- Si conosce la password corrente

Modifica delle password

Per modificare la password:

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



Gestisci protezione 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).

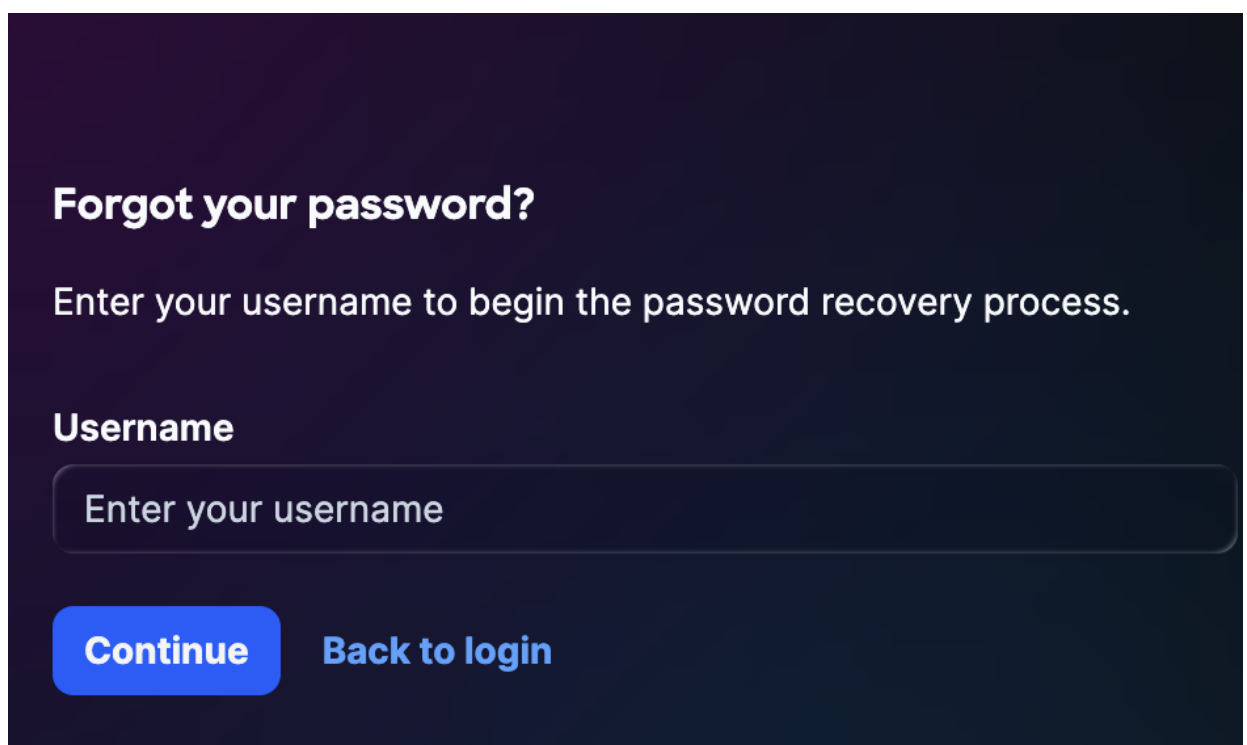
La password viene aggiornata nel sistema Cisco IQ, inclusa la VM Cisco IQ.

Reimpostazione di una password dimenticata

È possibile reimpostare una password utilizzando il processo di verifica delle domande di sicurezza.

Per reimpostare una password dimenticata:

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



Forgot your password?

Enter your username to begin the password recovery process.

Username

Enter your username

Continue [Back to login](#)

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.

Verify Identity

Answer the following security questions to verify your identity.

What city were you born in?

Enter your answer

Show

What is your mother's maiden name?

Enter your answer

Show

What was the name of your elementary school?

Enter your answer

Show

Verify and continue

Back to login

Verifica identità

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.

Set New Password

Choose a strong password that contains the following:

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

New password

Show

Confirm password

Show

Reset password

Back to login

Reimposta password

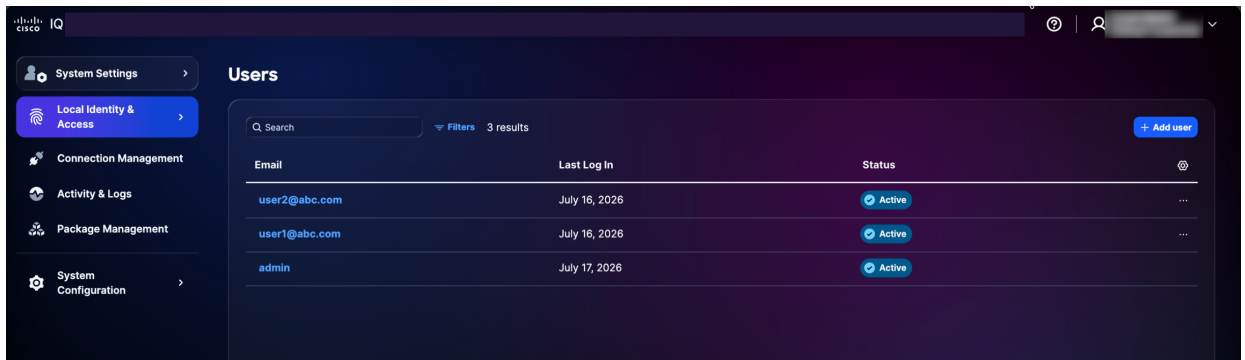
 Nota: Si hanno a disposizione tre (3) tentativi per immettere la password corretta entro un periodo di 15 minuti. Se tutti e tre (3) i tentativi hanno esito negativo, l'account viene temporaneamente bloccato per 30 minuti per proteggere la protezione. Non è possibile tentare l'accesso durante il periodo 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.

- Immettere la nuova password.
- Immettere nuovamente la password per confermarla.
- Fare clic su Invia.

Aggiunta di utenti locali

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

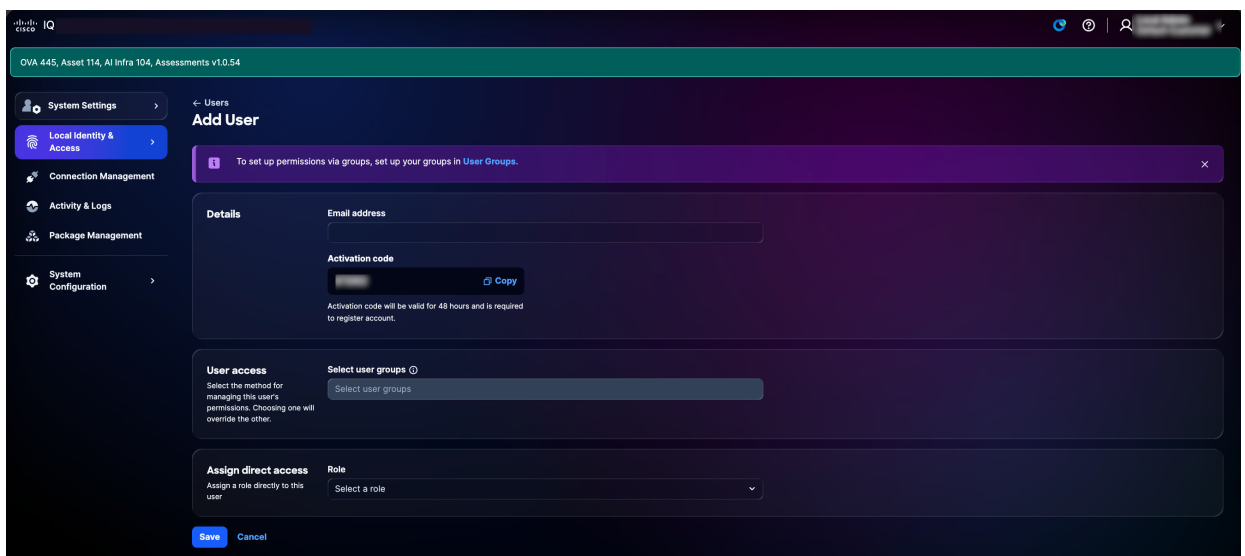
1. Passare a Impostazioni di sistema > Identità locale e accesso > Utenti. Verrà visualizzata la pagina Utenti. Vengono elencati tutti gli utenti locali esistenti con il relativo stato.



Pagina Utenti

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

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



Aggiungi utente

3. Immettere l'indirizzo e-mail.
4. Immettere il codice di attivazione.

 **Nota:** Il codice di attivazione viene visualizzato per impostazione predefinita. Condividere il codice di attivazione visualizzato con l'utente, in quanto necessario per la registrazione.

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



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

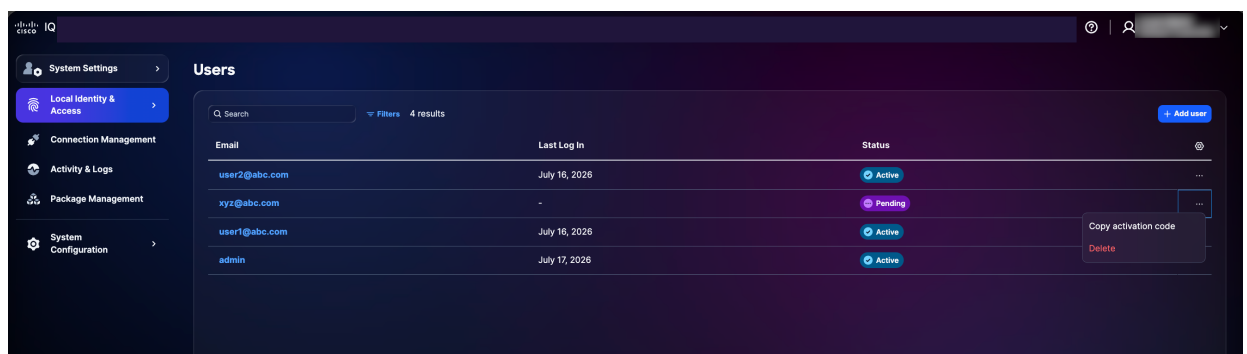
6. In Assegna accesso diretto, scegliere il ruolo dall'elenco a discesa Ruolo. Sono disponibili due (2) ruoli:

- Visualizzatore: Visualizza e accedi alle applicazioni
- Amministratore account: Accedere ai moduli e gestire le impostazioni di sistema, ad eccezione di IDP (System Management and Identity Provider)

7. Fare clic su Save (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.

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

9. Fare clic sull'icona Altre opzioni accanto all'utente appena creato.



Copia codice di attivazione

10. Selezionare il codice di attivazione Copia dall'elenco a discesa. Il codice di attivazione viene copiato negli Appunti.
11. Condividere questo codice con l'utente in modo protetto, 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. I codici di attivazione sono validi per 48 ore. Se il codice scade, contattare l'amministratore dell'account per richiederne uno nuovo.

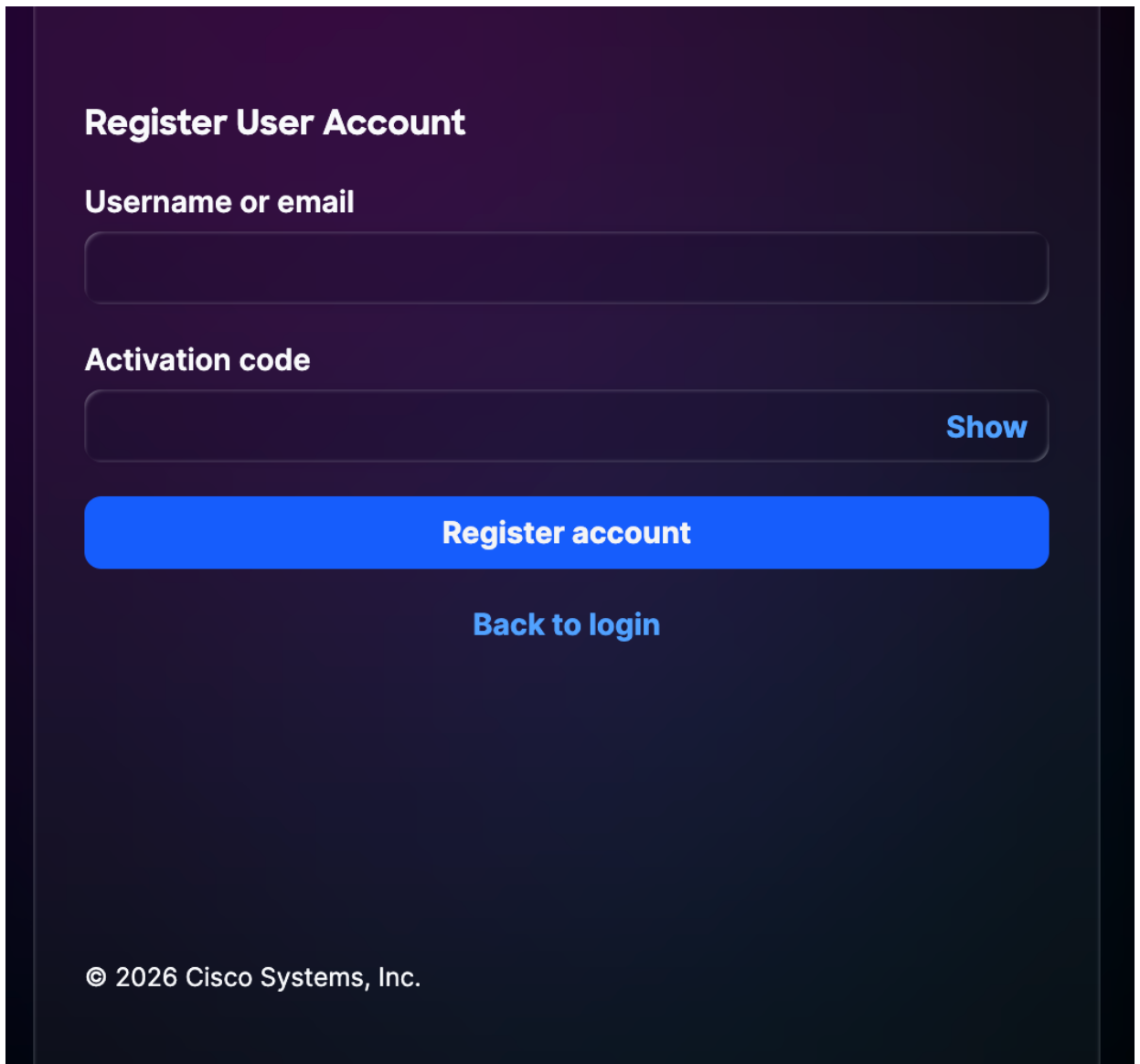
12. Per disconnettersi, fare clic sull'icona Profilo utente nell'angolo superiore destro e

selezionare Disconnetti. Viene visualizzata di nuovo la pagina di accesso di Cisco IQ.

Registrazione di nuovi account utente

Per registrare il nuovo account utente:

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



The screenshot shows a dark-themed registration form titled "Register User Account". It contains two input fields: "Username or email" and "Activation code". The "Activation code" field has a "Show" button on its right side. Below the input fields is a large blue button labeled "Register account". Underneath this button is a link labeled "Back to login". At the bottom left of the form, the copyright notice "© 2026 Cisco Systems, Inc." is displayed.

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.

Set New Password

Choose a strong password that contains the following:

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

New password

Show

Confirm password

Show

[Reset password](#)

[Back to login](#)

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. (Vedere [Impostazione delle domande di sicurezza](#)).

Gestione dei gruppi di utenti locali

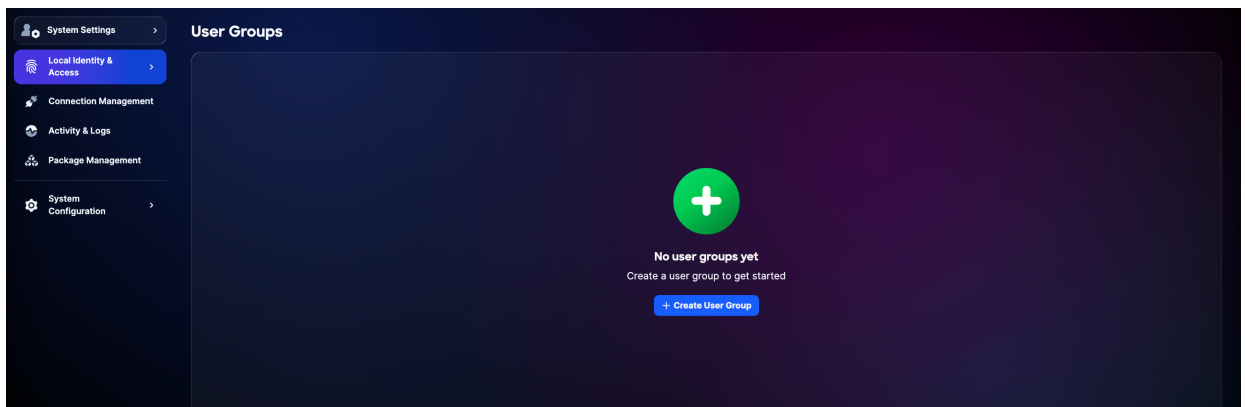
I gruppi di utenti consentono all'amministratore dell'account di gestire i ruoli per più utenti locali contemporaneamente. Anziché assegnare un ruolo a ogni singolo utente, è possibile creare un gruppo, associarvi un ruolo e un set di utenti e aggiornare il ruolo o l'appartenenza in un'unica posizione. 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. per ulteriori informazioni, fare riferimento a [Aggiunta di utenti locali](#).

Creazione di un gruppo di utenti

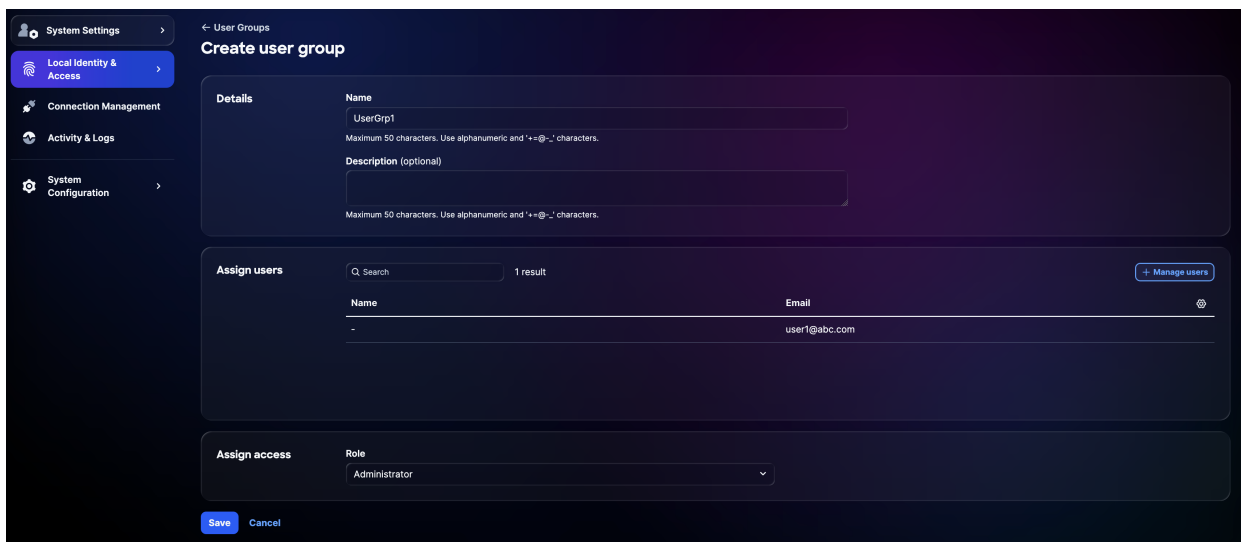
Per creare un gruppo di utenti:

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; alfanumerico e + = @ - _ caratteri 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 ai moduli (sola lettura)
- Amministratore: Accedere ai moduli e gestire le impostazioni di sistema

4. Fare clic su Save (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. Scegliere l'icona Altre opzioni > Modifica del gruppo desiderato. Viene visualizzata la pagina Modifica gruppo di utenti.

The screenshot shows the 'Edit user group' page. On the left is a sidebar with navigation links: System Settings, Local Identity & Access (highlighted), Connection Management, Activity & Logs, and System Configuration. The main content area has a header 'User Groups' and 'Edit user group'. Below this are three sections: 'Details' with input fields for 'Name' (containing 'UserGp1') and 'Description (optional)'; 'Assign users' with a search bar showing '1 result' and a table with one user 'user1@abc.com'; and 'Assign access' with a 'Role' dropdown menu set to 'Administrator'. At the bottom are 'Save' and 'Cancel' buttons.

Modifica gruppo di utenti

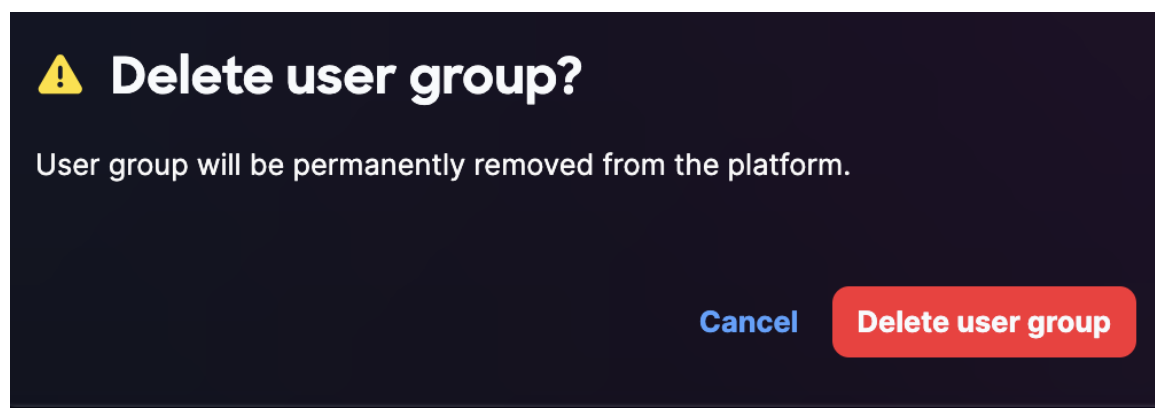
3. Apportare le modifiche desiderate.
4. Fare clic su Save (Salva).

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

Una volta effettuato l'accesso a VA, gli amministratori account possono configurare varie impostazioni. Gli amministratori degli account possono eseguire l'accesso utilizzando l'amministrazione locale o la configurazione IDP.

Configurazione SAML IDP Okta per SSO

Prerequisiti per la configurazione di SAML IDP

- Accesso come amministratore locale a 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.

Tabella 2: Attributi 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 3. Parametri di configurazione SAML

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

5. Configurare le istruzioni degli attributi.



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: .*

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

Tabella 4. 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 del provider di servizi (SP) sono necessari solo per 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

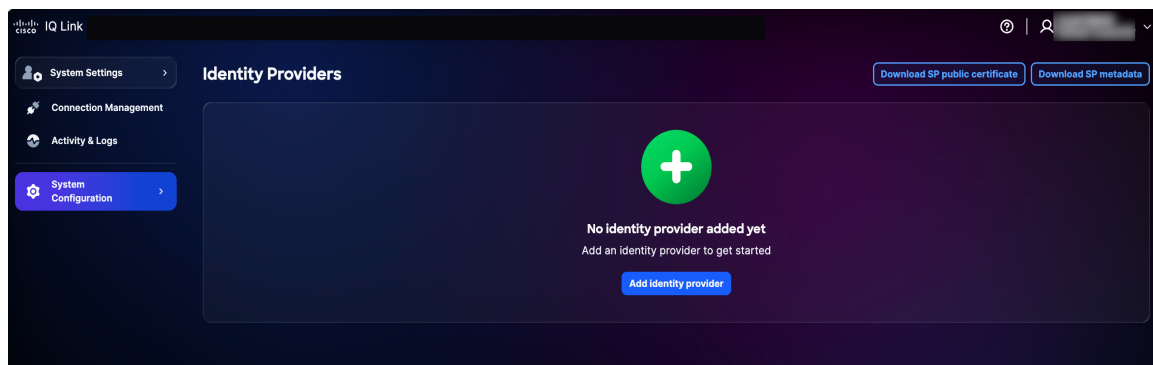
8. Fare clic sull'icona Download per scaricare il file "IDP Metadata XML".

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

Aggiunta di IDP Okta

Per aggiungere un IDP in Cisco IQ:

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



Home page di IDP



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

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

The screenshot shows the Cisco IQ Link interface for adding an identity provider. On the left is a sidebar with navigation options: 'System Settings', 'Connection Management', 'Activity & Logs', and 'System Configuration' (highlighted in blue). The main content area is titled 'Add Identity Provider' and includes a back arrow and the text 'Identity Providers'. The form contains three main sections: 1. 'Identity provider name' with a text input field and a red asterisk indicating it is required. 2. 'Domains' with a text input field for domain names and an 'Add' button. 3. 'Organization IDP metadata' with a red asterisk, a dashed box containing an upload icon and the text 'Select or drag file to this area to upload' and 'Only one file can be uploaded at 5 MB or less'. At the bottom, there is a toggle switch for 'Enable single log out (SLO)' and two buttons: 'Save' (blue) and 'Cancel'.

Aggiungi provider di identità

3. Immettere il nome del provider di identità.
4. Fare clic su Add (Aggiungi) per aggiungere un nome di dominio configurato da Cisco IQ al campo Domain(s).
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 dell'entità SP.
6. (Facoltativo) attivare il pulsante Abilita disconnessione singola. È possibile attivare lo SLO anche in un secondo momento.
7. Fare clic su Save (Salva).

Configurazione mapping ruoli

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

×

Map identity provider roles to system roles to assign permissions.

Map User Roles

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

+ Add identity provider role

Save

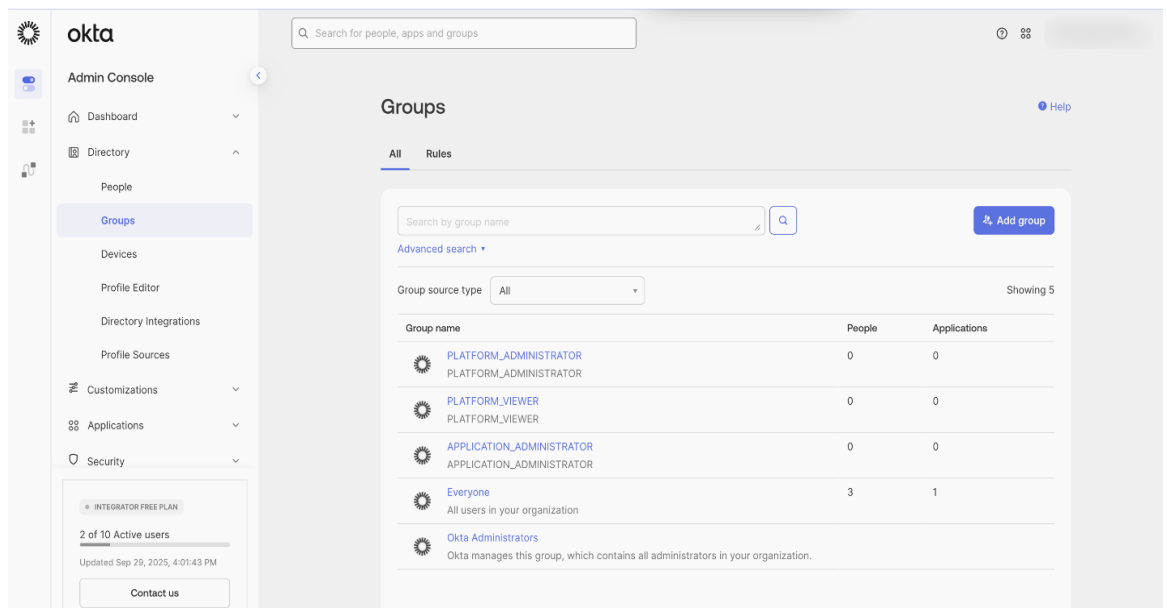
Mapping ruoli utente

- 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.



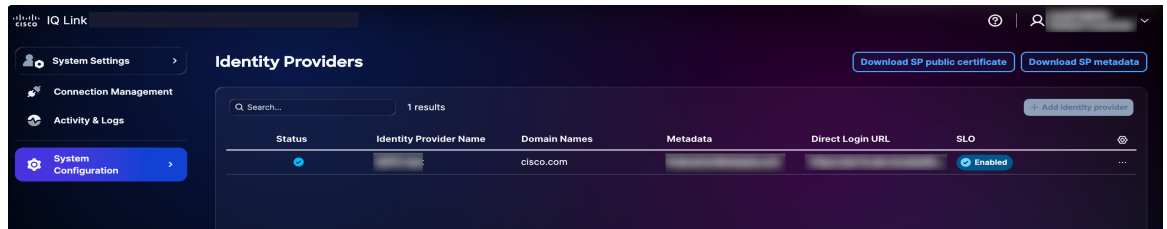
Riferimento mapping ruoli

3. Eseguire il mapping di ruoli aggiuntivi in base alle esigenze facendo clic su Aggiungi ruolo provider di identità.
4. Fare clic su Save (Salva). Una volta configurata, la pagina di login visualizza un'opzione per eseguire il login con SSO (tramite IDP).

Configurazione disconnessione singola

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

1. Dalla home page dei provider di identità, fare clic su Scarica certificato pubblico SP.



Certificato pubblico SP

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. Immettere l'URL SLO (ad esempio, https://ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com/saml/logout).
6. Immettere l'autorità emittente SP (ad esempio, ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com).
7. Fare clic su Invia.
8. Scaricate nuovamente il file di metadati IDP.
9. Nella pagina Provider di identità, scegliere l'icona Altre opzioni dell'IDP aggiunto > Modifica.
10. Attivare il pulsante Attiva disconnessione singola (SLO).
11. Caricare il file di metadati appena scaricato.
12. Utilizzare l'elenco di controllo seguente per verificare la funzionalità SSO e SLO:

Elenco di controllo per la verifica:

- Accesso dell'amministratore locale riuscito
- Il portale IDP è configurato e sottoposto a provisioning
- L'IDP viene aggiunto a Cisco IQ con lo stato "Operazione riuscita"
- I mapping dei ruoli vengono configurati e testati
- I metadati SP vengono scaricati ed estratti
- Se SLO è abilitato, la configurazione SLO è completata con il certificato di firma reale
- Test del flusso di SSO e SLO end-to-end completato

Risoluzione dei problemi relativi a IDP

Nella tabella seguente vengono elencati 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 5. 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 (FS) come provider di identità SAML per Cisco IQ, supportando l'autenticazione basata su password e PKI (Public Key Infrastructure) o basata su certificati.

Prerequisiti per configurare SAML IDP ADFS per SSO

- Si consiglia ADFS 6.0+
- Windows Server 2016 + (consigliato 2019)
- Integrazione di Active Directory configurata con gli account utente
- Certificati SSL/TLS sul server ADFS
- Accesso come amministratore a Cisco IQ
- Accesso amministrativo al server ADFS (Windows Server)
- Accesso PowerShell al server ADFS
- Connettività di rete tra ADFS e Cisco IQ
- CA (Certification Authority) Enterprise (installata o raggiungibile)
- Privilegi di amministratore di dominio o di amministratore dell'organizzazione (necessari solo per PKI)

- Dettagli di configurazione del server ADFS (come indicato nella tabella seguente)

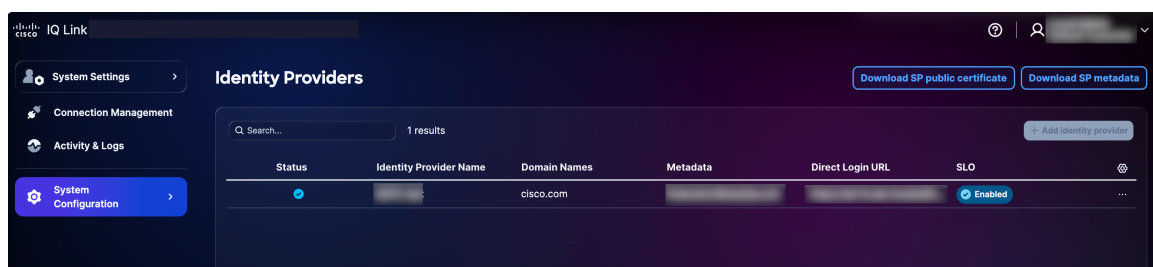
Tabella 6. Panoramica sul flusso di autenticazione

Articolo	Descrizione	Esempio
FQDN Cisco IQ	Nome host distribuzione utente	<FQDN-CIQ-utente> Ad esempio, dev35-23.cx-xxx-xxx.cisco.com
URL server ADFS	Indirizzo server ADFS utente	https://<Nome-HOST-ADFS> Ad esempio, https://ad-fs.dev.local
Dominio società	Dominio e-mail	<Dominio-Utente> CN=Ruolo - Sviluppatori
Gruppi AD	Nomi di dominio (DN) del gruppo Active Directory	CXIQ OU=Gruppi, DC=dev, DC=locale
Nome CA (PKI)	Nome CA organizzazione	<Nome-CA-utente>
PKI (Cert Auth Port)	Porta TLS alternativa ADFS	49443
Identificazione personale certificato SSL	Certificato SSL del server ADFS	<IDENTIFICAZIONE PERSONALE-SSL-CERT>

Configurazione di SAML ADFS di base

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 nel server ADFS, ad esempio C:\.

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 dei metadati del provider di servizi e completare il caricamento del file.
11. Fare clic su Next (Avanti).
12. Immettere un nome visualizzato (ad esempio, "Cisco IQ"), 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 autenticazione a più fattori" a meno che il server ADFS non disponga di una scheda di rete Multi-Factor Authentication (MFA) registrata, ad esempio Azure MFA, Totp (Time-Based One-Time Password) configurato.

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

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

Set-AdfsRelyingPartyTrust -TargetName “

”

-AccessControlPolicyName “Permit everyone”

You can also create the trust through PowerShell:

-Add-AdfsRelyingPartyTrust `

=Name “

” `

-Identifier “

” `

-SamlEndpoint (New-AdfsSamlEndpoint -Binding POST -Protocol

SAMLAssertionConsumer -Uri “

”) `

-AccessControlPolicyName “Permit everyone” `

-IssuanceAuthorizationRules '=> issue(Type =

“http://schemas.microsoft.com/authorization/claims/permit”, Value =

“true”);

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 7. Richieste di rimborso necessarie

Richiesta di rimborso	Scopo	Origine
Email	Identificatore utente	Posta elettronica
Nome visualizzato	Nome completo dell'utente	Nome visualizzato AD
UPN	Autenticazione PKI/certificati	ADFS mappa il certificato client a un utente AD tramite 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 - Produzione".

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

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

3. Applicare le regole attestazione eseguendo il comando seguente:

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

Write-Host "Regole attestazione configurate correttamente" -ColorePrimoPiano Verde

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 verificare l'appartenenza dell'utente ai gruppi eseguendo il comando seguente:

```
$username = “username”
```

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

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

3. Per visualizzare i gruppi a cui appartiene l'utente, utilizzare il comando seguente:

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

Output di esempio:

CN=Ruolo - Sviluppatori CXIQ,OU=Gruppi di ruoli,DC=dev,DC=locale

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 opzioni seguenti:



Nota: Il certificato SP è rilasciato da una 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
```

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

```
Import-Certificate -FilePath "C:-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. Verificare l'installazione eseguendo il comando seguente:

```
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 il nome dell'entità utente (UPN) di un utente o un indirizzo 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 comando seguente:

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

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. Trasferite il file user-cert.pfx sul dispositivo Mac.
3. Importare il certificato nel portachiavi Mac eseguendo il comando seguente:

```
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. Affidare la 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 Address
```

Abilitazione dell'autenticazione del certificato come principale

Per abilitare l'autenticazione del 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", "WindowsAuthenticat  
-PrimaryExtranetAuthenticationProvider @"CertificateAuthentication", "FormsAuthenticat
```


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

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

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

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

4. Se TlsClientPort non è 4943, aggiornare la porta e riavviare il servizio ADFS utilizzando i comandi seguenti:

```
Set-AdfsProperties -TlsClientPort 4943  
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 una nuova associazione 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:

```
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)" -Fore
```

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

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

3. Verificare che nessun certificato non autofirmato rimanga nell'archivio radice attendibile 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 8. Impostazioni Registro di sistema 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 SystemCertificatesper essere certi 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 nell'archivio LocalMachine:

```
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 Meta  
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://<server-adfs>/FederationMetadata/2007-06/FederationMetadata.xml>, sostituendo "<server-adfs>" con il nome host del server ADFS.
2. 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:

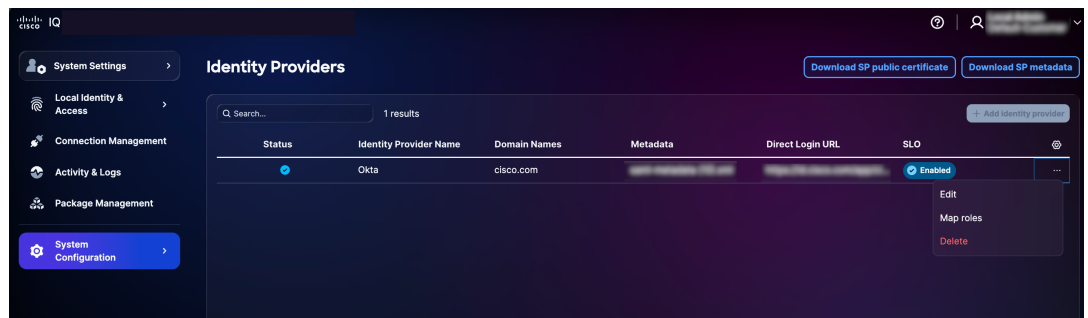
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = "(&(objectClass=group)(cn=Role - CXIQ*))"
$searcher.PropertiesToLoad.Add("distinguishedName") | Out-Null
$searcher.PropertiesToLoad.Add("cn") | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties["distinguishedname"]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

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

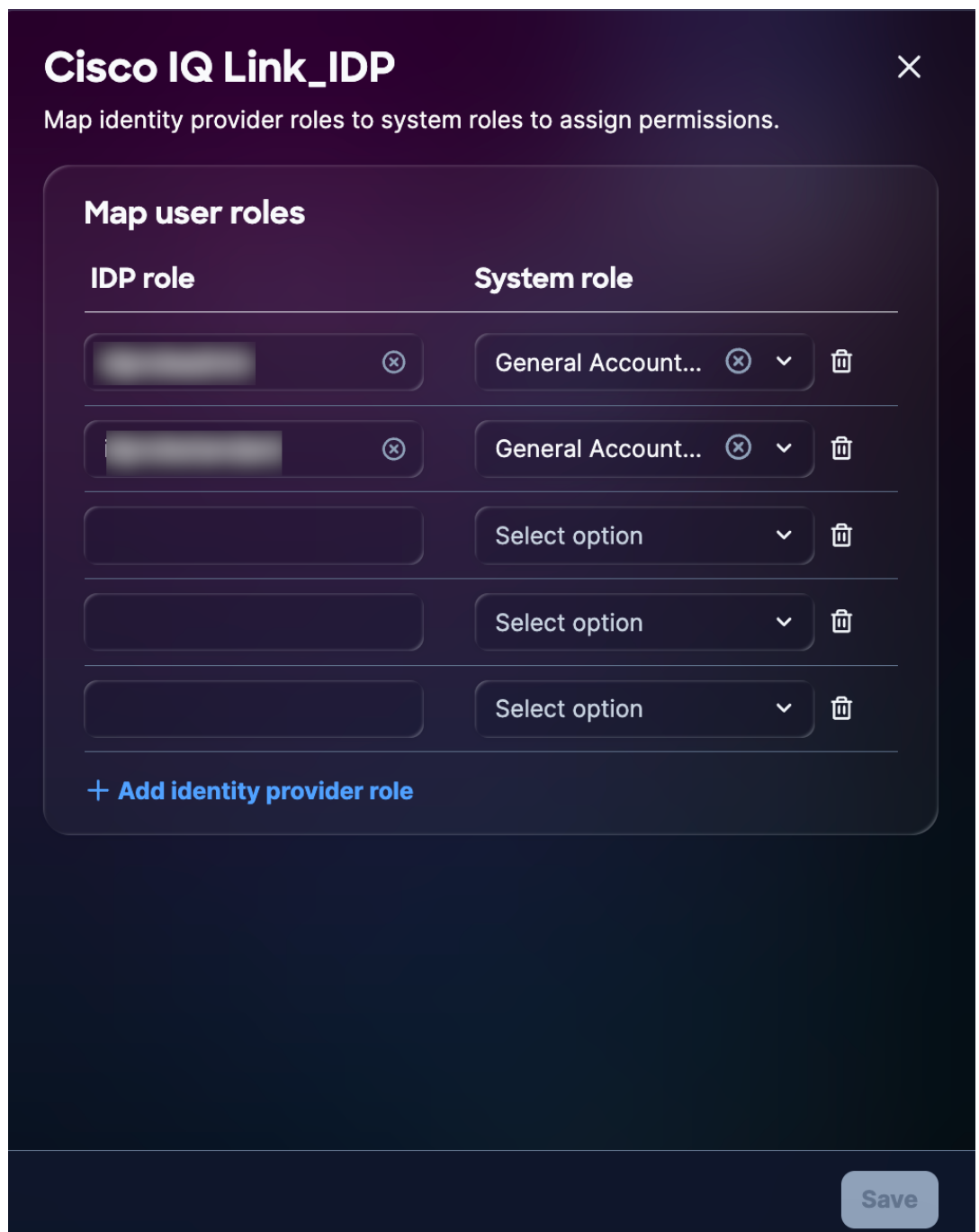
Se i gruppi richiesti non sono elencati, è necessario crearli in AD da un amministratore account prima di poter completare il mapping dei ruoli ADFS.

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 DN completi.

3. Fare clic su Save (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 finale del browser per il flusso PKI, assicurarsi che il certificato utente sia installato nel portachiavi di MacOS (vedere [Importazione del certificato utente sul computer client \(MacOS\)](#)). 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 9. 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
Decrittografia non	"Impossibile	Controllare la

Problema	Sintomi / Descrizione	Cause / Controlli / Soluzioni alternative e correzioni
riuscita	decrittografare l'asserzione" nei log	configurazione del certificato ADFS ◦ URL ACS non valido: Verifica: https://your-fqdn/saml/acs ◦ Mancata corrispondenza cookie: Verificare i cookie del browser per il dominio corretto
Loop di accesso	Bloccato nell'autenticazione o nel loop di accesso	

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 - Production" |  
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 - Production" |  
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 PKI o basata su certificato (CBA).

Prerequisiti per configurare Entra ID SAML per SSO

- Tenant ID Entra (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 10. 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

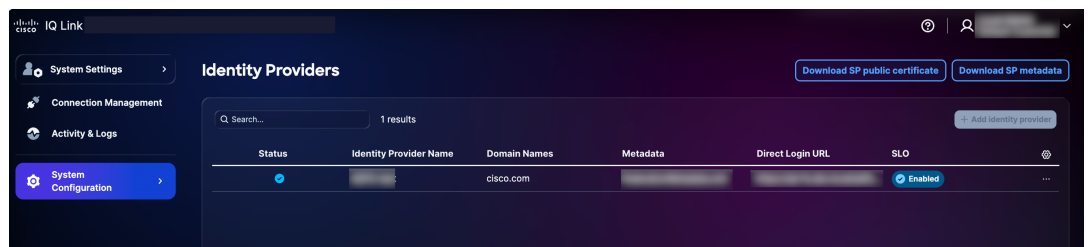
1. Accedere all'[interfaccia di amministrazione di Microsoft Entra](#).
2. Passare a Identità > Applicazioni > Applicazioni aziendali.

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 inclusa nella raccolta).
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. È possibile ottenerlo eseguendo le seguenti operazioni da 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 per caricare il file di metadati SP. Dopo il caricamento, i dati del file di metadati SP verranno automaticamente inseriti nella schermata Single Sign-on basata su SAML.

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:

4. Nell'applicazione enterprise, passare a Single Sign-On e scegliere SAML.
5. Nella sezione Configurazione SAML di base, fare clic su Modifica e immettere quanto segue:
 - Identificatore (ID entità): <FQDN-CIQ-UTENTE>
 - URL risposta (URL ACS): https://<FQDN-CIQ-UTENTE>/saml/acs

- URL di accesso: <https://<FQDN-CIQ-UTENTE>/saml/login>
- URL di disconnessione: <https://<FQDN-CIQ-UTENTE>/saml/logout>

6. 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.

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

8. Configurare le attestazioni seguenti:

Tabella 11. 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/emailaddress-1
nome dato	user.nomedato	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname-1
cognome	user.cognome	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname-1
nome	user.nomeprincipaleutente	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name-1
gruppi	user.assignedroles	(VUOTO — cancella lo spazio dei nomi)



Nota: Per l'affermazione dei gruppi:

- Utilizzare user.assignedroles come origine, non user.groups
- 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 Apply (Applica).



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

Per scaricare i metadati e il certificato IDP:

1. Dall'applicazione Enterprise, scegliere 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. Osservate i seguenti valori dalla sezione Imposta (Set up):
 - 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 12. 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: Usare le stringhe dei valori del ruolo app esattamente come configurato in Entra ID (per ulteriori dettagli, vedere [Configurazione dei ruoli app](#))

4. Fare clic su Save (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 success"
```

Output previsto

Autenticazione conforme a SAML 2.0 riuscita per l'utente:
user@domain.com con nome completo: N/D e 1 gruppo

Gruppo estratto: CXIQ Admins (originale: Amministratori CXIQ)

Totale gruppi estratti: 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 seguente comando:

```
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 i comandi seguenti:

```
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 il 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  
”
```

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 Attendibilità, impostare su "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 > Sicurezza > 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 CBA 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 (SAN) 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'indirizzo 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 13. 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). Verificare che l'attributo mail dell'utente sia compilato.
Totale gruppi estratti: 0	Attestazione basata su gruppi non configurata o origine errata	Utilizzate user.assignedroles come origine. Verificare che l'utente sia assegnato a un ruolo applicazione (per ulteriori informazioni, vedere Assegnazione di utenti ai ruoli applicazione).
Attestazioni gruppi duplicati	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).

Problema	Causa	Fix
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 dall'ID Entra e caricarli nuovamente in Cisco IQ.
ADSTS500191	CRL non raggiungibile da Internet	Pubblicare il CRL su un URL accessibile pubblicamente o utilizzare l'approccio CA autofirmato (per ulteriori informazioni, vedere Risoluzione dei problemi di raggiungibilità del CRL).
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) per ulteriori dettagli), CBA è abilitato in Entra ID con le impostazioni richieste (vedere Abilitazione di CBA in Entra ID Authentication Methods per ulteriori dettagli) e Chrome è 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 il lab).
Stato "Incompleto" in Virtual Appliance	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:

```
# 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 (Cisco Discovery Protocol), 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 un'applicazione enterprise (diversa dalla raccolta) in Entra ID
- Configurare una 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

- Aggiungere un IDP in Cisco IQ caricando i metadati Entra ID
- Configurare il mapping dei 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)

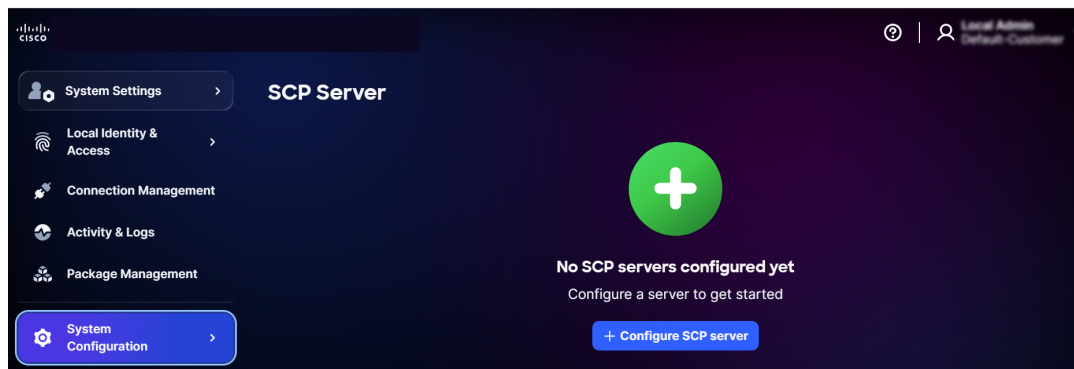
- Crea modello di certificato in Servizi certificati Active Directory con utilizzo chiavi avanzato di autenticazione client
- Rilasciare un certificato utente con un UPN corrispondente all'ID utente Entra
- Esportare un certificato utente come file PFX e installarlo nel computer client
- Considera attendibile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

Aggiunta del server SCP

Un server SCP è un prerequisito per l'importazione dei file di aggiornamento essenziali per aggiungere, aggiornare o correggere l'installazione di Cisco IQ.

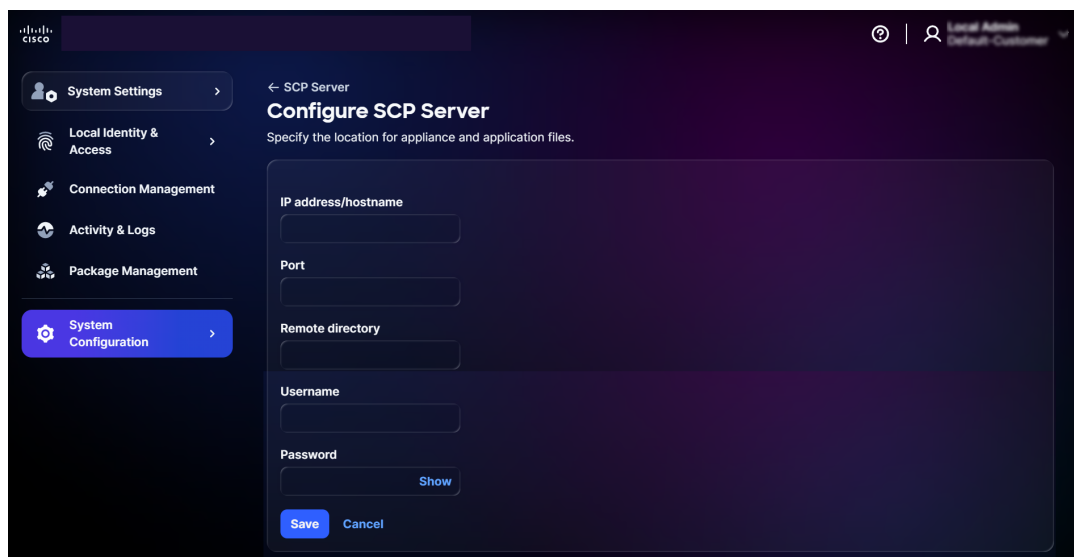
Per aggiungere un server SCP:

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). Viene visualizzata la pagina Configura server SCP.



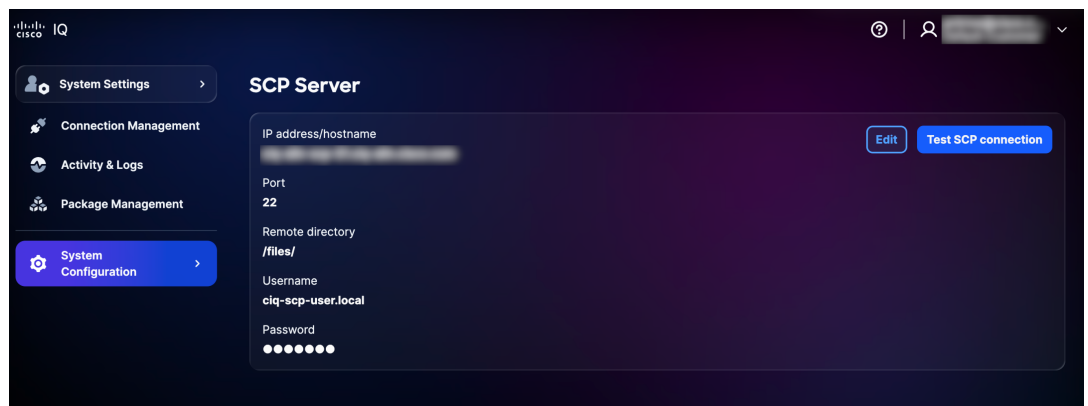
Configura server SCP

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

Modifica di un server SCP esistente

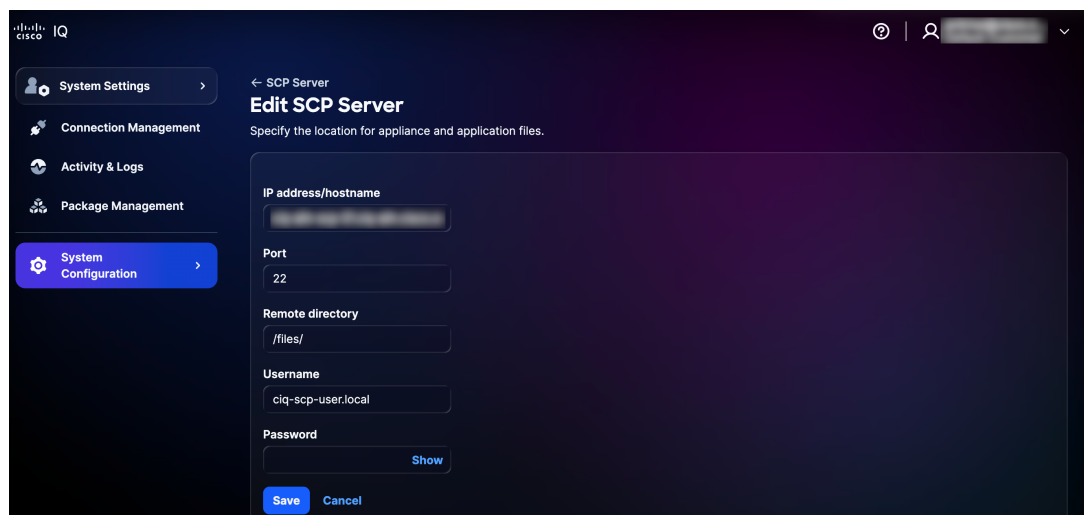
Per modificare un server SCP esistente:

1. Passare alla pagina SCP Server.



Server SCP aggiunto

2. Fare clic su Edit (Modifica) del server SCP desiderato esistente.



Modifica del server SCP

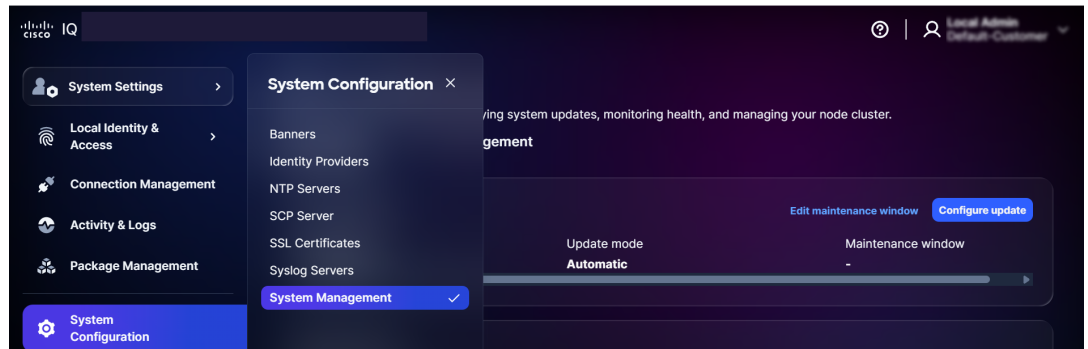
3. Modificare i dettagli in base alle esigenze.
4. Fare clic su Save (Salva).

Gestione del sistema

È possibile eseguire l'aggiornamento alla versione più recente di Cisco IQ VA tramite l'interfaccia utente. È possibile effettuare la verifica anche dalla pagina Cisco IQ Data Connector.

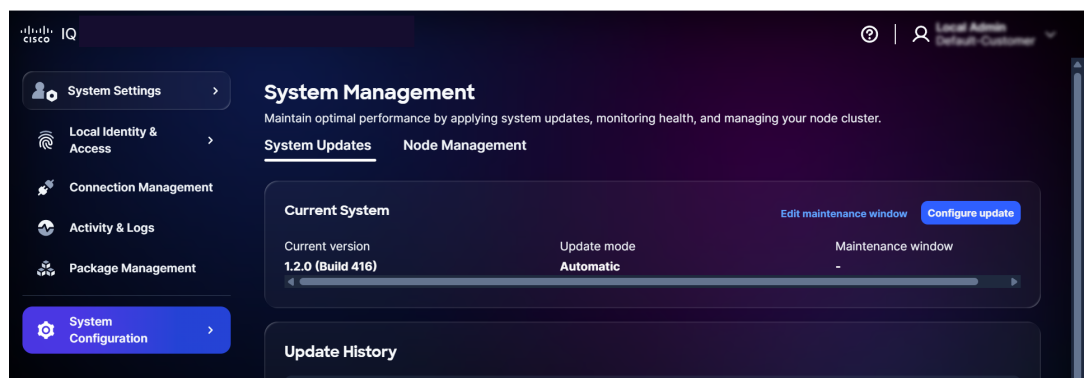
Riprogrammazione dell'aggiornamento del sistema

Per riprogrammare l'aggiornamento del sistema:



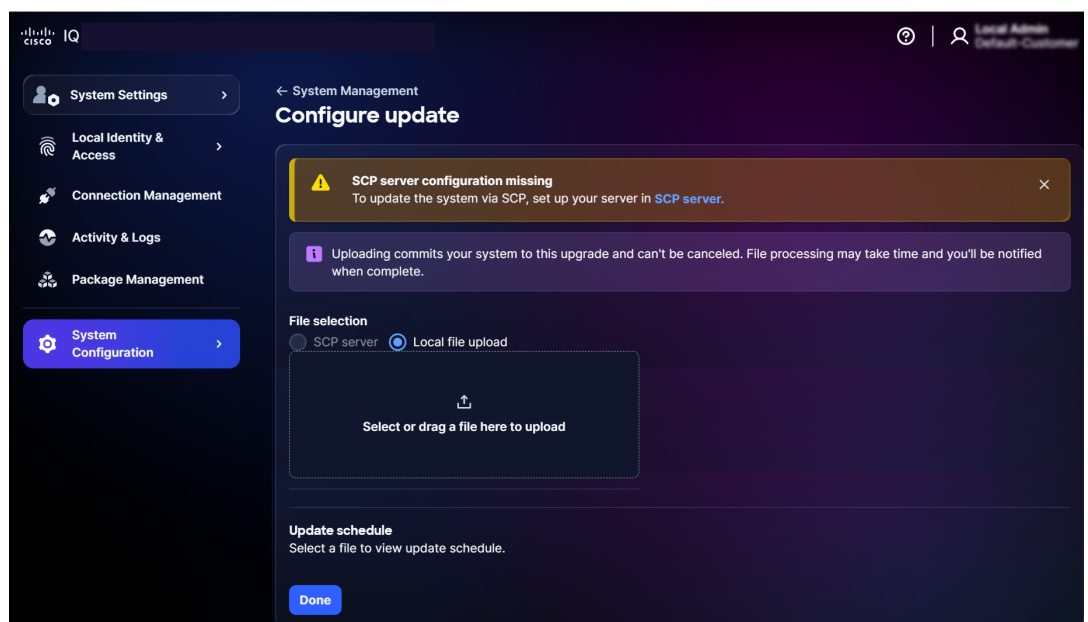
Gestione del sistema

1. Da Impostazioni di sistema, scegliere Configurazione di 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 Configura aggiornamento. Viene visualizzata la pagina Configura aggiornamento.



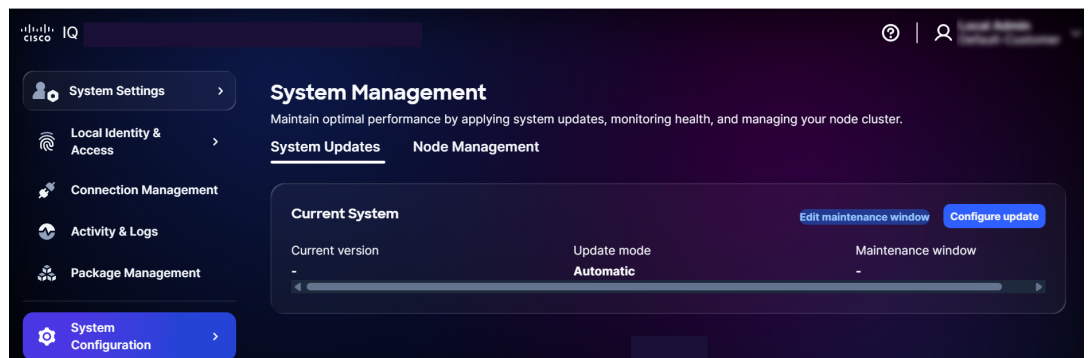
Configura aggiornamento

3. Scegliere la pianificazione di aggiornamento per pianificare un'altra pianificazione.
4. Attendere il completamento del caricamento del file; la durata dipende dalle dimensioni del bundle e dalla velocità della rete.

Confermare l'esito positivo dell'aggiornamento verificando l'icona con il segno di spunta visualizzato nella colonna Aggiorna stato.

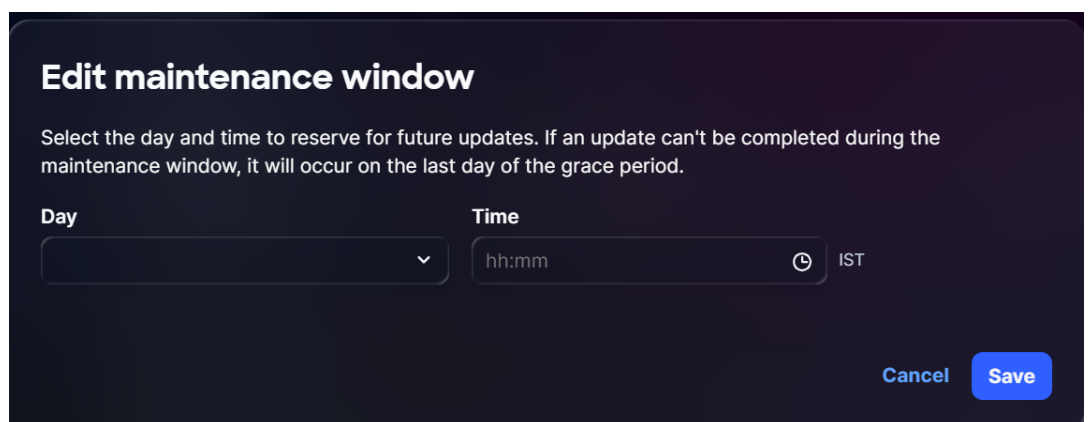
Modifica delle pianificazioni di aggiornamento del sistema

È possibile creare una pianificazione personalizzata per gli aggiornamenti del sistema. Se è stata configurata una pianificazione personalizzata, gli aggiornamenti vengono eseguiti alle date definite dall'utente purché rimangano entro il periodo di tolleranza massimo. Per creare una pianificazione di aggiornamento del sistema:



Modifica manutenzione

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



Modifica finestra di manutenzione

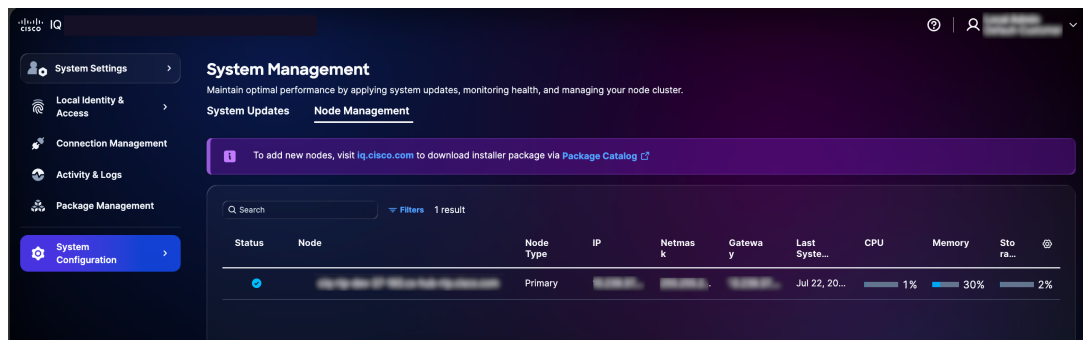
2. Selezionare un'opzione dagli elenchi a discesa Giorno e Ora.

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 configurata alcuna pianificazione di aggiornamento, per impostazione predefinita il sistema prevede periodi di tolleranza di due (2) settimane per gli aggiornamenti senza riavvio e di quattro (4) settimane per gli aggiornamenti che richiedono un riavvio. Al termine di questi periodi di prova, gli aggiornamenti devono essere eseguiti manualmente. In caso di errore di aggiornamento, il sistema esegue fino a due (2) tentativi automatici. Un terzo tentativo è pianificato ma richiede l'avvio manuale.

Gestione dei nodi

1. Passare a Configurazione di sistema > Gestione sistema > Gestione nodi per visualizzare e gestire i nodi nel cluster.



Status	Node	Node Type	IP	Netmask	Gateway	Last System Update	CPU	Memory	Storage
	10.10.10.10	Primary	10.10.10.10	255.255.255.0	10.10.10.1	Jul 22, 20...	1%	30%	2%

Gestione dei nodi

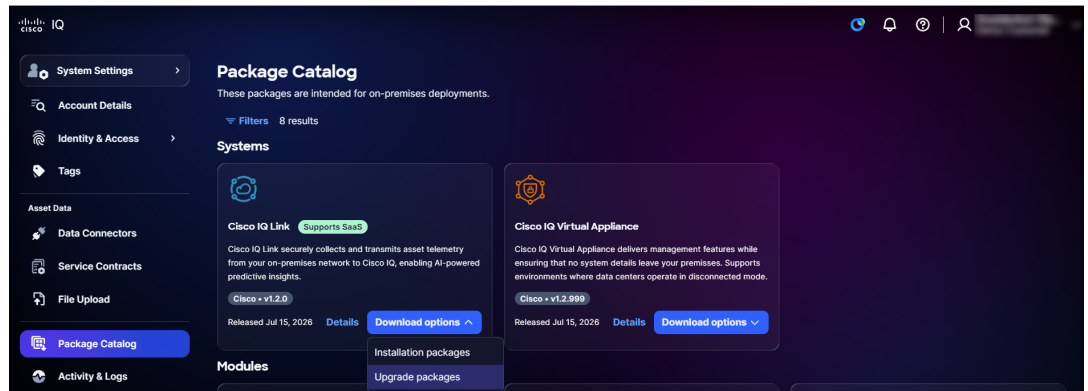
2. Nell'elenco dei nodi vengono visualizzati lo stato, il nome host, il tipo di nodo, l'indirizzo IP, la netmask, il gateway e l'ora dell'ultima sincronizzazione di ogni nodo.

 Nota: Un segno di spunta blu nella colonna Stato indica che il nodo è attivo.

Aggiornamento manuale del sistema

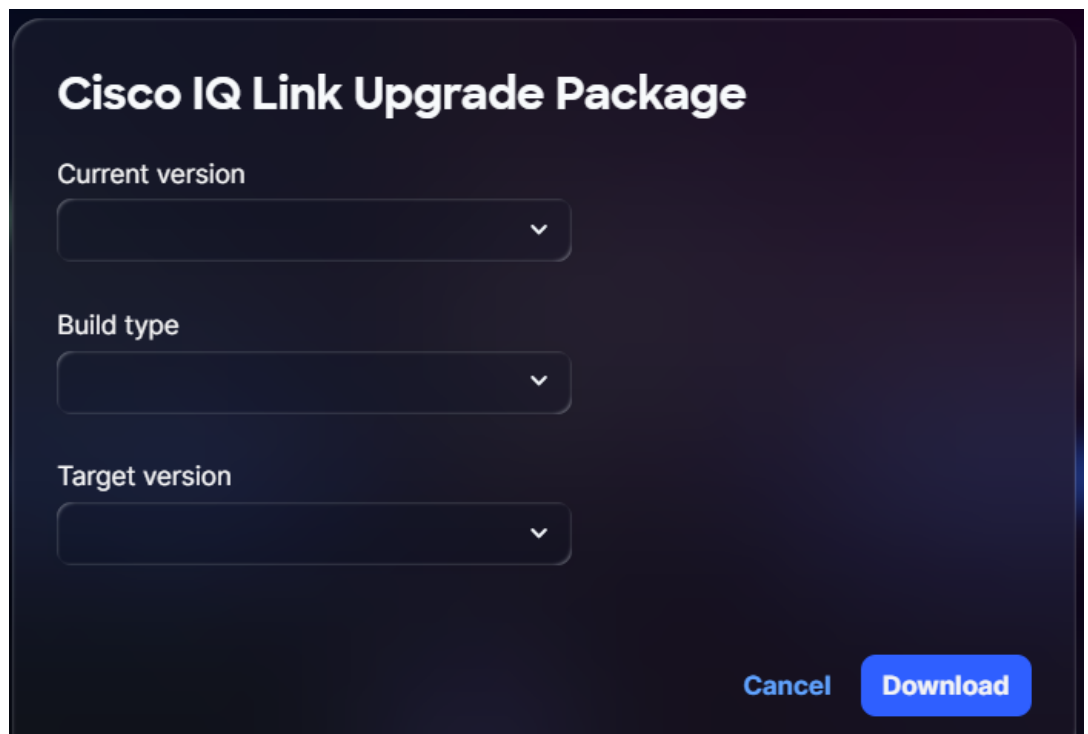
Negli scenari in cui la distribuzione automatica da Cisco IQ SaaS non è disponibile o è ritardata, è possibile eseguire manualmente un aggiornamento del sistema scaricando il bundle di aggiornamento direttamente da Cisco IQ SaaS. Per aggiornare manualmente il sistema:

1. Accedere a [Cisco IQ SaaS](#).
2. Passare a Home > Impostazioni di sistema > Catalogo package.



Catalogo software

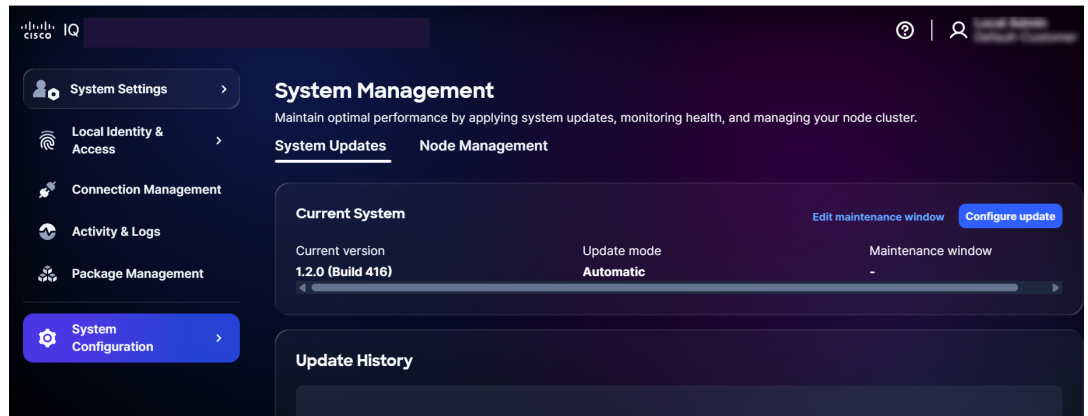
3. Nella scheda Cisco IQ Virtual Appliance, fare clic su Download options (Opzioni di download) > Upgrade packages (Pacchetti di aggiornamento).



Pacchetto di aggiornamento

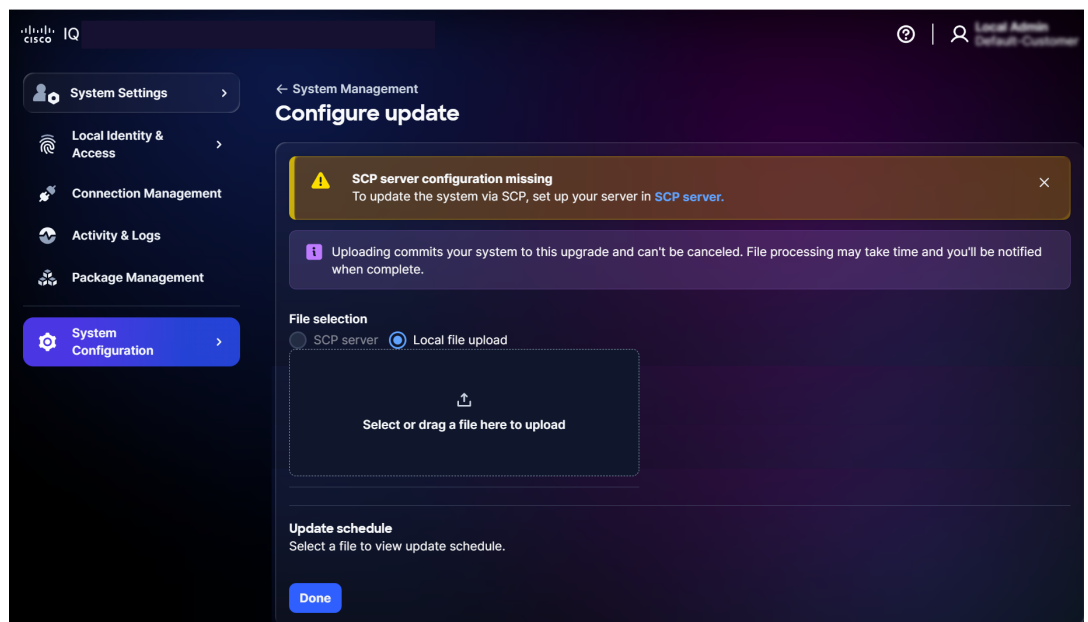
4. Selezionare la versione corrente dall'elenco a discesa.
5. Selezionare il tipo di generazione dall'elenco a discesa.
6. Selezionare la versione di destinazione dall'elenco a discesa.
7. Fare clic su Download (Scarica). Il bundle di aggiornamento viene scaricato.
8. Passare a Cisco IQ VA.
9. Da Impostazioni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

Gestione sistema.



Configura aggiornamento

10. Fare clic su Configura aggiornamento.



Caricamento file locale

11. Fare clic sul pulsante di opzione Caricamento file locale.

12. Selezionare o trascinare il file del bundle di aggiornamento scaricato nel campo di caricamento.

13. Attendere il completamento del caricamento del file; la durata dipende dalle dimensioni del bundle e dalla velocità della rete.

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;

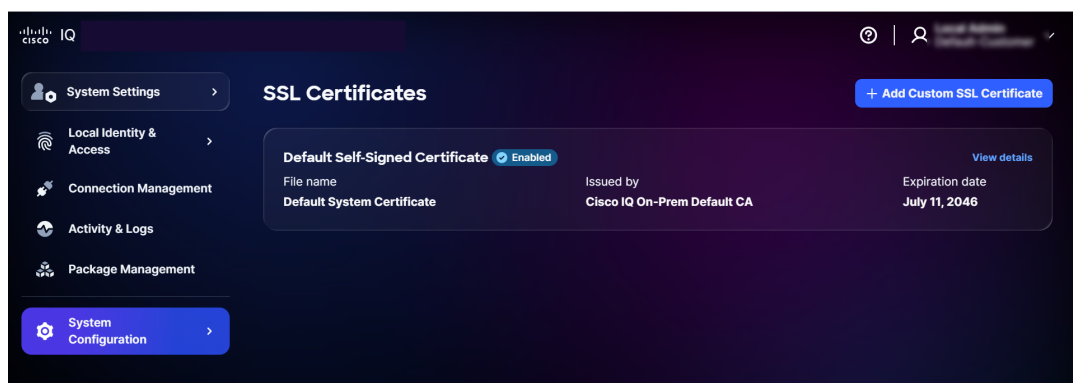
se il certificato viene disabilitato o eliminato, il sistema ripristina automaticamente il certificato predefinito. Impossibile modificare o eliminare il certificato SSL predefinito.

 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 [Completamento della configurazione SLO](#) per l'IDP Okta o l'IDP ADFS.

Aggiunta del certificato SSL personalizzato

Per aggiungere un certificato SSL personalizzato:

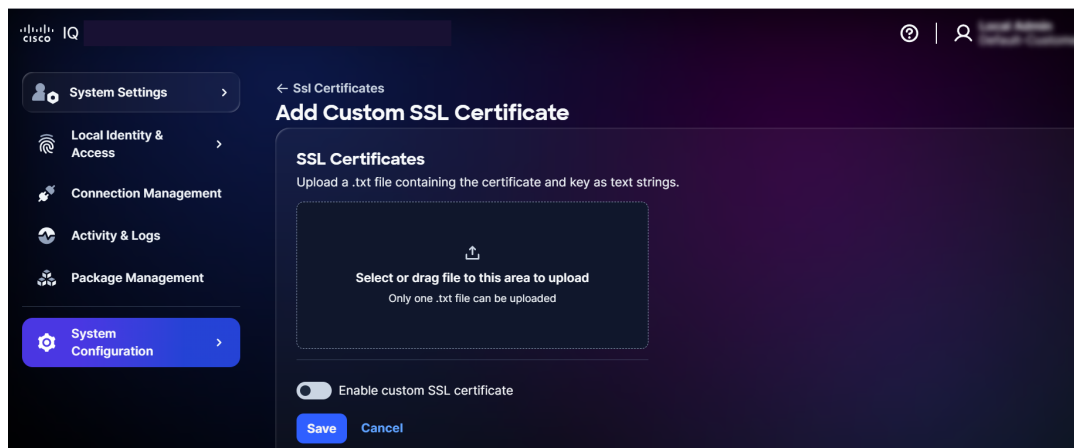
1. Da Impostazioni di sistema, scegliere Configurazione di sistema > Certificati SSL. Viene visualizzata la pagina Certificati SSL, in cui sono elencati tutti i certificati SSL per il sistema in uso.



Aggiunta del certificato SSL

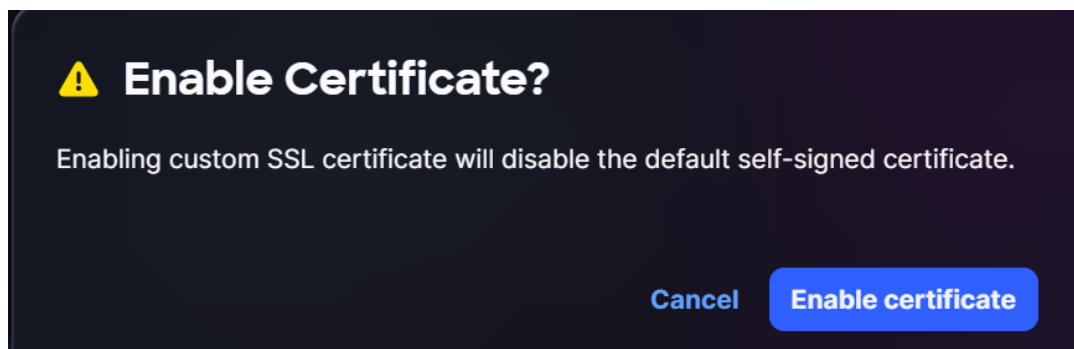
2. Fare clic su Aggiungi certificato SSL personalizzato.

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



Carica certificato SSL

3. Trascinare o caricare il certificato SSL personalizzato nella sezione Certificato SSL.
4. Attivare il pulsante Attiva/disattiva certificato SSL personalizzato.



Abilita certificato



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

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

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

Modifica del certificato SSL personalizzato

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.

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 del certificato SSL personalizzato

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

Per eliminare:

1. Passare al certificato SSL personale desiderato.
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.

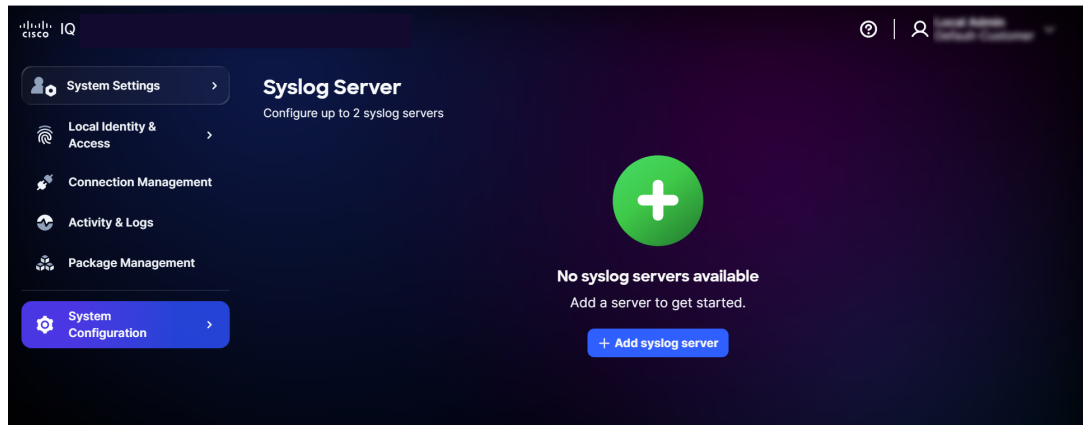


Nota: Il server Syslog deve essere specificato come indirizzo IP e non come nome di dominio completo (FQDN).

Aggiunta del server syslog

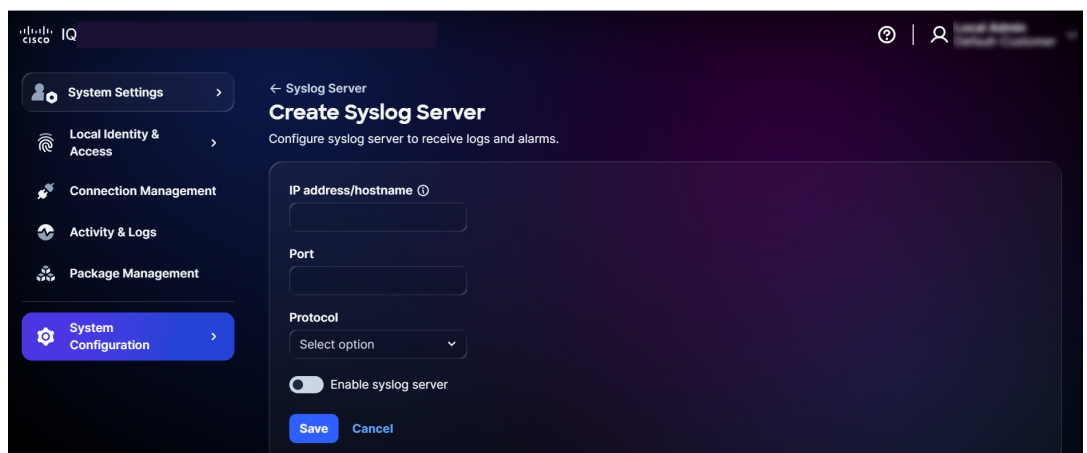
Per aggiungere un server syslog:

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. Accedere a Port.
5. Selezionare il protocollo desiderato dall'elenco a discesa Protocollo (ad esempio, UDP, 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 del server syslog configurato

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

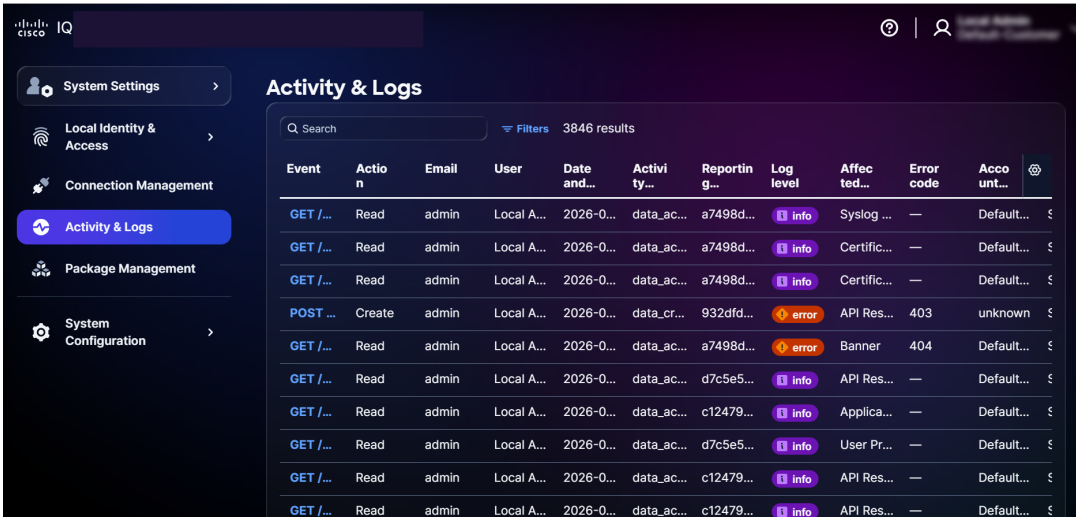
Eliminazione del server syslog configurato

Per eliminare un server syslog configurato:

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



The screenshot shows the 'Activity & Logs' section of the Cisco IQ interface. On the left is a sidebar with navigation links: System Settings, Local Identity & Access, Connection Management, Activity & Logs (highlighted), Package Management, and System Configuration. The main area displays a table of activity logs with 3846 results. The table has columns for Event, Action, Email, User, Date and time, Activity ID, Reporting ID, Log level, Affected resource, Error code, and Account. The data rows show various system events like 'GET /...' (Read) and 'POST /...' (Create) performed by 'admin' on 'Local A...' at '2026-0...'. Some events have status icons (info or error) and error codes (403, 404).

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

Registri attività

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

Log attività:

- Registra tutte le operazioni API a livello di gateway

- Supporta filtri, impaginazione e funzionalità di ricerca per semplificare l'individuazione e la gestione delle informazioni

Sono disponibili le seguenti opzioni di filtro:

- Data ultimo accesso: 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: Filtri per un codice di errore specifico

Banner

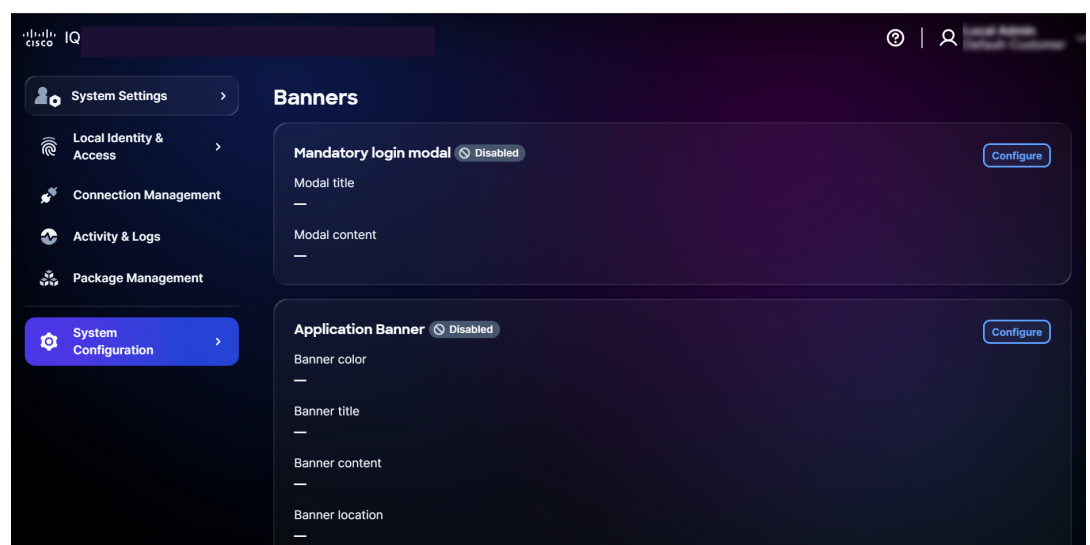
Gli amministratori degli account possono configurare banner a livello di sistema per soddisfare gli standard di sicurezza e conformità.

- 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

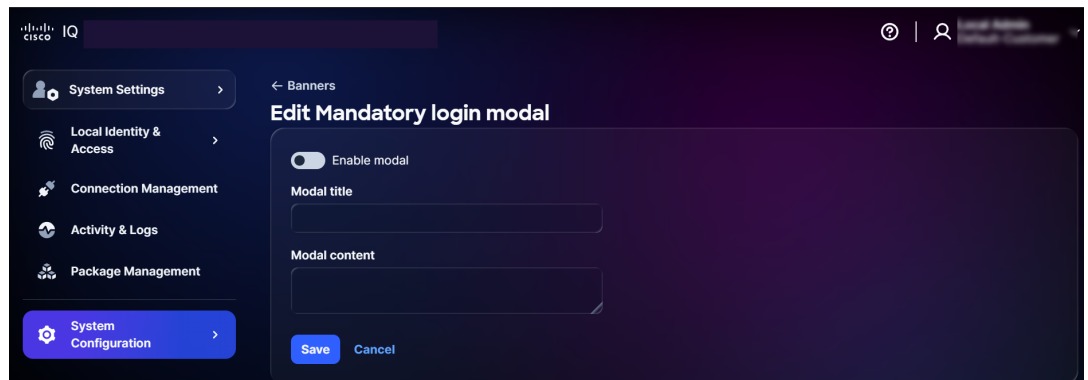
Per configurare un banner obbligatorio:

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.



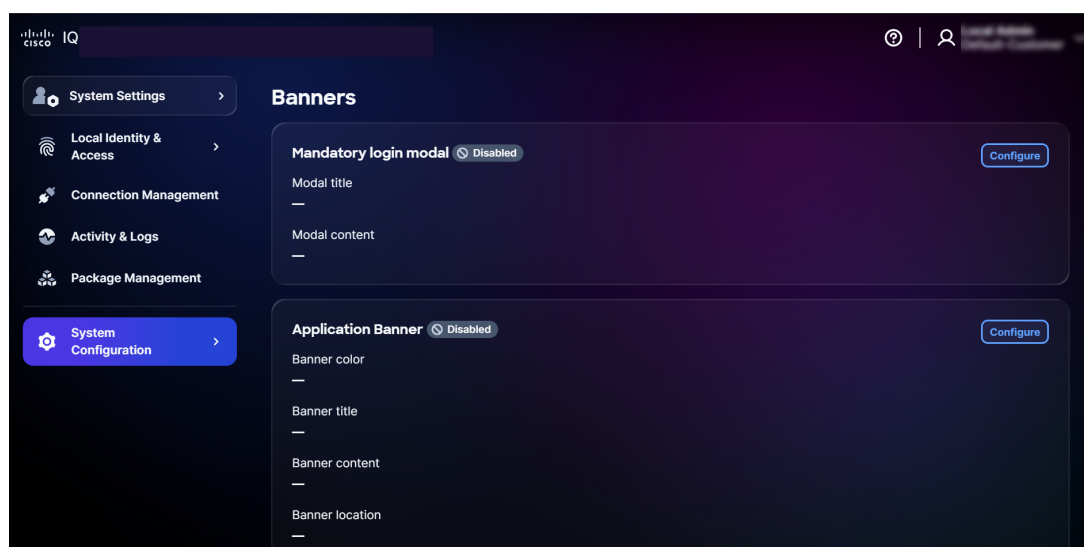
Modifica banner modale di accesso obbligatorio

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

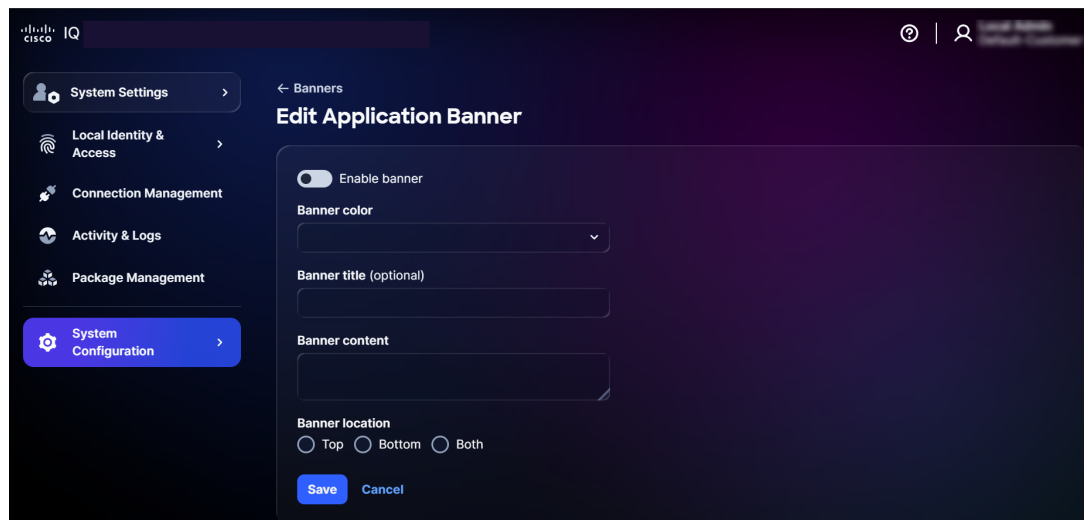
Per configurare un banner applicazione:

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.



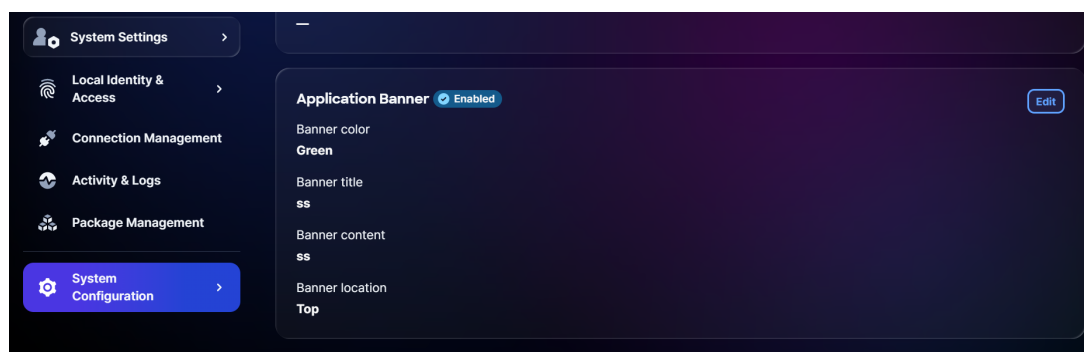
Modifica banner applicazione

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

Modifica dei banner

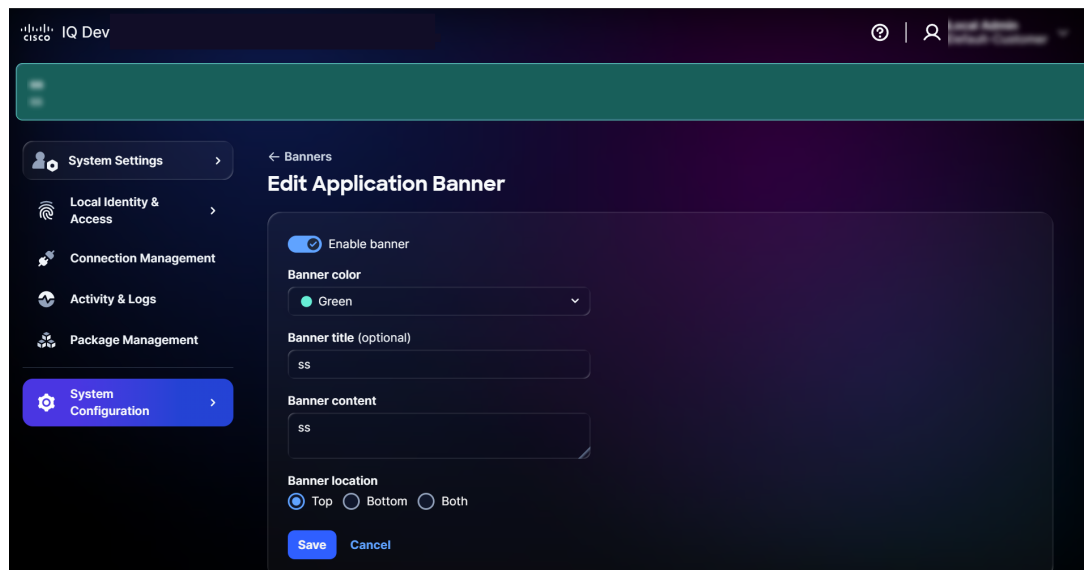
Per modificare uno striscione:

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



Modifica banner

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



Modifica banner applicazione

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

Risoluzione dei problemi

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.

```
CISCO IQ

Navigation Main Menu

SYSTEM STATUS
Cisco IQ On-Prem Installed

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

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

Menu principale

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

```
CISCO IQ

Navigation Main Menu > System Diagnostics

Please provide the following server connection details:

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

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

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

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

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.



```
Navigation Main Menu > System Diagnostics

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

Press Enter to return to main menu...█
```

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.

Modulo di supporto

È possibile creare richieste di supporto per VA e moduli specifici da Cisco IQ SaaS. Il modulo di supporto è disponibile in Cisco IQ SaaS e offre una visualizzazione consolidata delle richieste di supporto. Consente di filtrare,

ordinare e personalizzare la visualizzazione dell'elenco di richieste, fornendo visibilità sia sulle richieste aperte che su quelle chiuse a cui si è autorizzati ad accedere. Per informazioni più dettagliate sul modulo di supporto in Cisco IQ SaaS, vedere la [guida introduttiva a Cisco IQ SaaS](#).



Nota: I clienti Cisco IQ VA possono accedere alla maggior parte delle funzionalità del modulo di supporto SaaS per Cisco IQ, tra cui l'apertura di richieste TAC (Technical Assistance Center) relative a Cisco IQ VA e ai relativi moduli, nonché la creazione e la gestione di richieste di prodotti.

Creazione di una richiesta di assistenza

È possibile creare richieste VA e specifiche per il modulo in Cisco IQ SaaS. Per creare una richiesta:

1. Accedere a [Cisco IQ \(SaaS\)](#).
2. Fare clic sull'icona Guida > Segnala un problema. Viene visualizzata la finestra Segnala un problema.

Report an Issue

Experiencing an issue with Cisco IQ? Let us know what's going on and we'll open a support case for you.

Issue type

☐ Portal login issues ☐ Error message ☐ Data discrepancy ☐ Other

Issue description

Describe what happened.

The more detail you give, the faster we can help.

Preferred contact method

☐ Telephone ☐ Email ☐ Virtual space via Webex

Include recipients (optional)

Select or add email addresses

Select or enter email addresses to include.

Cancel Submit

Segnala un problema

3. Fornire i dettagli richiesti.
4. Fare clic su Invia.

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).