

Cisco IQ Virtual Appliance - Betriebshandbuch

v1.2.0

Einleitung

Cisco IQ™ bietet Ihnen Erweiterungen und Funktionen, die darauf ausgelegt sind, die Transparenz von Ressourcen zu verbessern, intelligentere Einblicke in die Umgebung zu liefern und das Fallmanagement zu optimieren. Darüber hinaus optimieren KI-Funktionen wie der Cisco IQ AI Assistant die Betriebsergebnisse und die Benutzererfahrung mit Cisco IQ, indem sie kontextbezogene Kenntnisse bereitstellen, die Sie in die Lage versetzen, proaktive, fundierte Entscheidungen zu treffen und Prozesse für Kundenengagement und Erfolg zu optimieren.

Cisco IQ On-Prem Air-Gapped ist einer der Bereitstellungsmodi von Cisco IQ für Kunden in stark regulierten Branchen mit strengen Compliance-, Datenhoheit- und Sicherheitsanforderungen. In diesem Modus wird Cisco IQ als eigenständiges virtuelles System (VM) bereitgestellt, das als Cisco IQ Virtual Appliance (VA) bezeichnet wird. Die VA läuft vollständig am Kundenstandort und ist vollständig von externen Netzwerken isoliert. Um diese Isolierung aufrecht zu erhalten, werden Software-Updates und Wartungspakete von Cisco IQ SaaS abgerufen und über einen genehmigten manuellen Prozess an die VA übertragen.

Cisco IQ On-Prem Air-Gapped erweitert wichtige Funktionen von Cisco IQ SaaS auf Air-Gap-Umgebungen und ermöglicht es geschäftskritischen Teams, mit Geschwindigkeits- und Diagnoseintelligenz zu arbeiten, die mit Cloud-basierten Unternehmen vergleichbar ist.

Um auf Cisco IQ VA zuzugreifen, öffnen Sie einen unterstützten Browser, und navigieren Sie zu <https://<fqdn-of-the-Appliance>>. Melden Sie sich mit dem Benutzernamen und dem Kennwort für den Administrator an, die während des Installationsvorgangs festgelegt wurden.

 Anmerkung: Die Cisco IQ VA ist derzeit auf Kunden beschränkt, die für das Programm "Controller Availability" registriert sind. Der Download-Zugriff für die VA-Systemsoftware und zusätzliche Betriebspakete (Module, Regeln und Berechtigungen) aus dem Cisco IQ-Portal steht ausschließlich ausgewählten Kunden zur Verfügung. Weitere Informationen erhalten Sie von Ihrem Kundenbetreuer.

Verbindungsverwaltung (Datensammlung)

Cisco IQ VA ist eine standortbasierte Lösung für die Erfassung von Netzwerkdaten und sorgt so

für umfassende Transparenz in Ihrer Infrastruktur. Es erfasst Daten über Catalyst Center und Direct Connection. Es vereinfacht das Management der Netzwerkauthentifizierung und Geräteerkennung. Die Konfiguration der Datenerfassung umfasst:

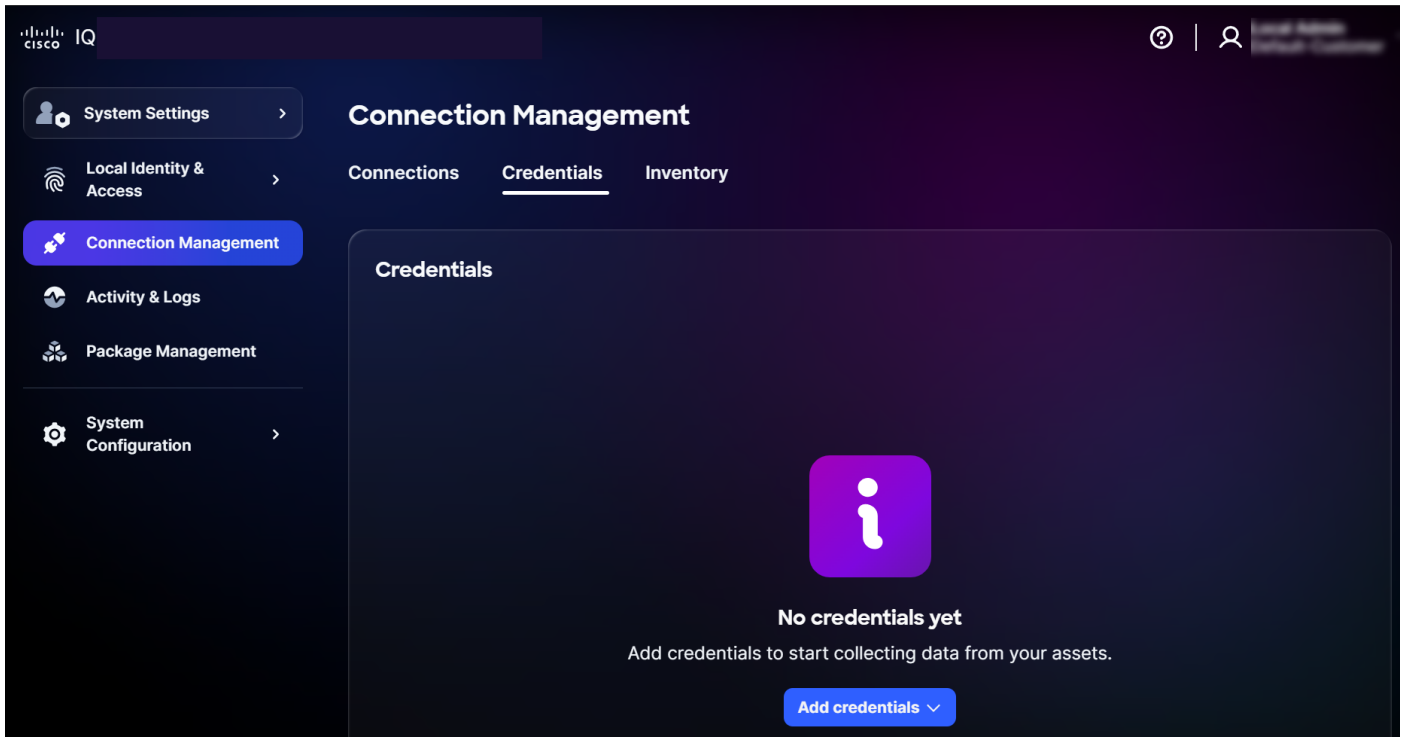
- Erstellen von Anmeldeinformationssätzen: Richten Sie die Authentifizierungsprotokolle (z. B. Simple Network Management Protocol (SNMP) v1/v2c/v3) für die Kommunikation mit den Netzwerkgeräten ein. Durch die Zentralisierung der Anmeldeinformationen nach Sicherheitszone oder Standort (z. B. "SanJose-SNMPv3") können Sie Kennwörter an einem Standort aktualisieren, wobei die Änderungen automatisch auf alle verbundenen Geräte übertragen werden.
- Zuordnen von Anmeldeinformationen zum Bestand: Ordnen Sie Ihre Berechtigungssätze den Bestands-Ressourcen zu, um den Authentifizierungsprozess zu automatisieren. Durch das Erstellen von Regeln, die bestimmte IP-Bereiche mit definierten Berechtigungssätzen verknüpfen, wendet das System während der Datenerfassung automatisch die richtige Authentifizierung an. So werden manuelle Eingabefehler vermieden und sichergestellt, dass die Konfiguration mit wachsendem Netzwerk immer fehlerfrei abläuft.

 Anmerkung: Für die Geräteerkennung sind SNMPv2c/SNMPv3 und SSH erforderlich, und vor der Konfiguration von Catalyst Center müssen HTTP/HTTPS-Anmeldeinformationen bereitgestellt werden.

Hinzufügen von Anmeldeinformationen

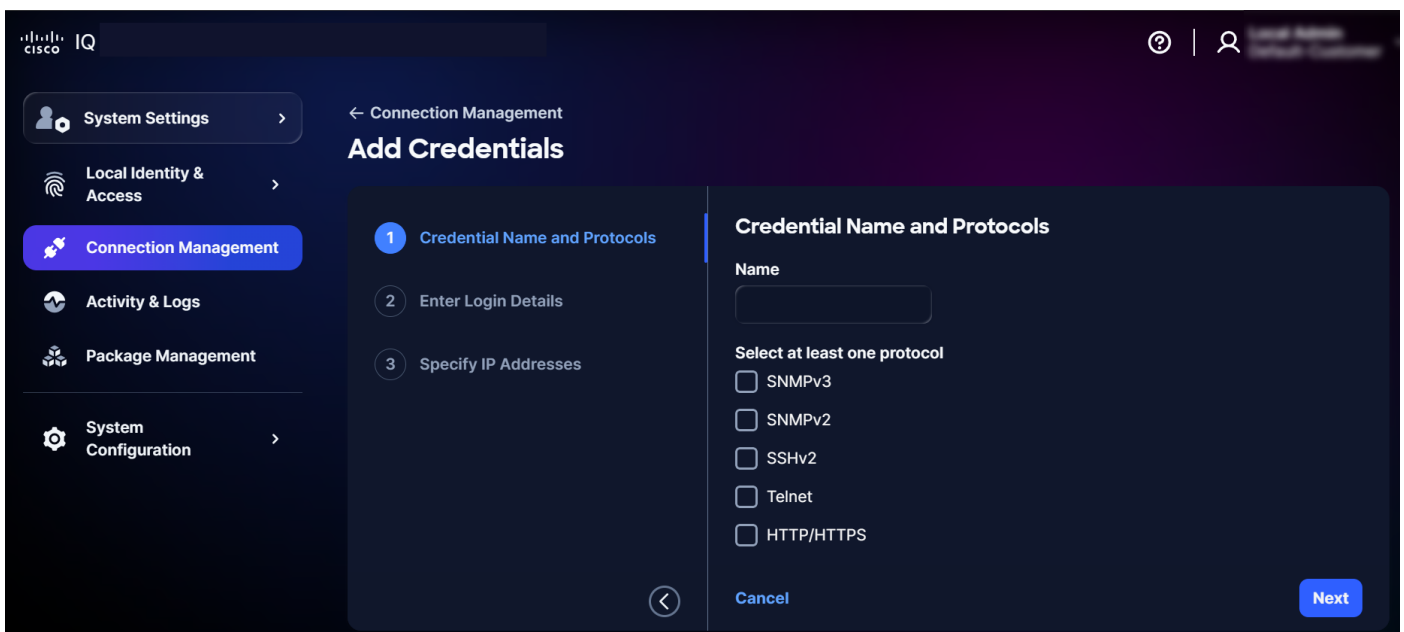
Sie müssen zunächst Anmeldeinformationen hinzufügen, um die Datensammlung durchzuführen. So fügen Sie Anmeldeinformationen hinzu:

1. Wählen Sie unter Systemeinstellungen die Option Verbindungsverwaltung aus. Die Seite Verbindungsverwaltung wird angezeigt.
2. Klicken Sie auf die Registerkarte Anmeldedaten.



Registerkarte "Anmeldeinformationen"

3. Klicken Sie auf Anmeldeinformationen hinzufügen.



Anmeldeinformationen hinzufügen

4. Geben Sie einen Namen ein.

5. Aktivieren Sie alle zutreffenden Kontrollkästchen für das Protokoll.

6. Klicken Sie auf Next (Weiter).

The screenshot shows the 'Add Credentials' wizard in Cisco IQ. The left sidebar contains navigation links: System Settings, Local Identity & Access, Connection Management (highlighted), Activity & Logs, Package Management, and System Configuration. The main area is titled 'Add Credentials' and shows three steps: 1. Credential Name and Protocols (checked), 2. Enter Login Details (active), and 3. Specify IP Addresses. The 'Enter Login Details' step is expanded, showing a form for 'SNMPv3'. The form includes fields for 'Username', 'Engine ID (optional)', 'Authorization algorithm' (dropdown), 'Authorization password' (with a 'Show' button), 'Privacy algorithm (optional)' (dropdown), and 'Privacy password' (with a 'Show' button'). At the bottom of the form are 'Cancel', 'Back', and 'Next' buttons.

Anmeldeinformationsdetails hinzufügen



Anmerkung: Für das obige Bild wird die Ansicht dargestellt, wenn alle Protokolle im vorherigen Schritt ausgewählt wurden. Ihre Schnittstelle zeigt nur die ausgewählten Protokolle an.

7. Geben Sie die Anmeldedetails für jedes ausgewählte Protokoll ein.

8. Klicken Sie auf Next (Weiter).

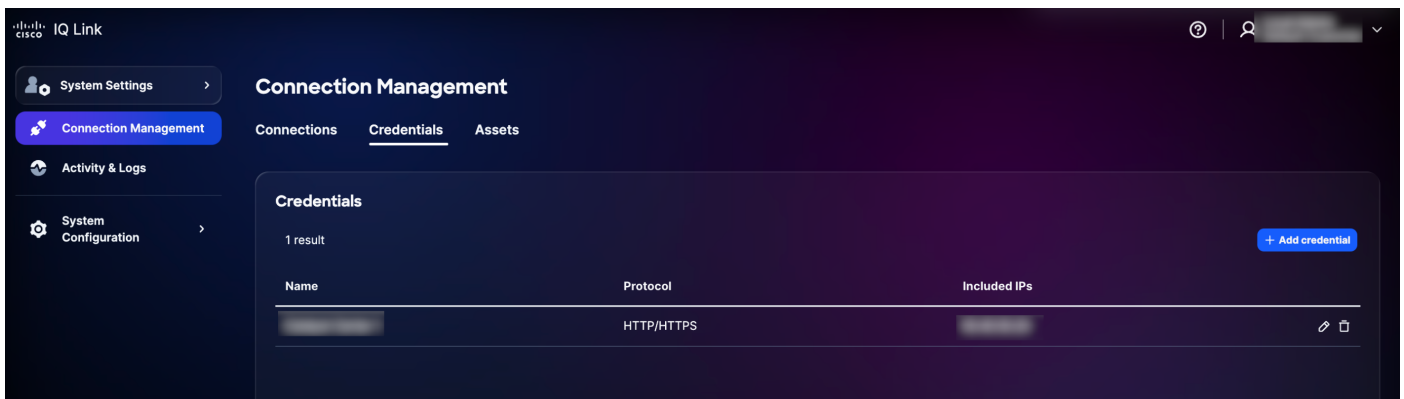
The screenshot shows the 'Add Credentials' wizard in Cisco IQ, step 3: Specify IP Addresses. The left sidebar is the same as in the previous screenshot. The main area shows the 'Specify IP Addresses' step, which is expanded. It includes a text area for 'Included IPs' with a placeholder example: 'e.g. *-*-*, 192.168.1.0/24, 172.16.*.*'. At the bottom of the form are 'Cancel', 'Back', 'Save and add another credential', and 'Save' buttons.

IP-Adressen angeben

9. Geben Sie die enthaltenen IPs ein.

 Anmerkung: Dieses Feld definiert die IP-Adressen oder IP-Bereiche, in denen die Anmeldeinformationen zum Herstellen einer Verbindung verwendet werden können. Es unterstützt eine Mischung aus IPs und IP-Masken (in der Schreibweise mit Platzhaltern). Ausführliche Informationen zu unterstützten Formaten finden Sie unter [Anrechnungsauswahl und Zuordnungslogik](#).

10. Klicken Sie auf Speichern. Eine Bestätigung wird angezeigt, und Sie werden zur Registerkarte Anmeldedaten weitergeleitet.



Anmeldeinformationen hinzugefügt

Sie können die Anmeldeinformationen bearbeiten, indem Sie auf das Symbol Bearbeiten klicken und sie löschen, indem Sie auf das Symbol Löschen klicken.

Logik für die Auswahl und den Abgleich von Anmeldeinformationen

Die Telemetrie-Engine verwendet eine priorisierungsbasierte Abgleichlogik, um zu bestimmen, welche Anmeldeinformationen bei der Erkennung und Erfassung angewendet werden sollen. Wenn Sie diese Hierarchie verstehen, wird sichergestellt, dass die richtigen Anmeldeinformationen für die beabsichtigten Geräte verwendet werden.

- Rangfolge der Prioritäten: Wenn für ein Gerät mehrere Berechtigungssätze gelten, werden diese von Cisco IQ auf der Grundlage der Übereinstimmung mit dem Gerät ausgewertet. Das System wendet die folgende Priorität an, wobei spezifischere Übereinstimmungen Vorrang haben:

- Genaue IP-Übereinstimmung: Höchste Priorität
- Trailing Wildcard Match: Priorität hängt von der Anzahl der nachlaufenden Sterne; Weniger Sterne stehen für eine spezifischere Übereinstimmung und daher für eine höhere Priorität.
- Platzhalterformatierungsregeln: Platzhalter (*) werden nur als nachfolgende Zeichen in einer IP-Adresse unterstützt. Sie müssen von rechts nach links angewendet werden.
 - Unterstützte Formate:
 - 1.2.3.* (höchste Priorität)
 - 1.2.*
 - 1.*.*
 - *.*.*.* (niedrigste Priorität)
 - Nicht unterstützte Formate:
 - Platzhalter (z. B. *.1.2.3)
 - Platzhalter zwischen Oktetten (z. B. 10.10.*.20)
 - Verwendung von Bindestrichen oder anderen nicht standardmäßigen Trennzeichen

Beispiel zur Auswahl von Anmeldeinformationen:

In der folgenden Tabelle wird veranschaulicht, wie die Telemetrie-Engine den am besten geeigneten Berechtigungssatz auswählt, wenn ein Gerät mehreren definierten Mustern entspricht.

Tabelle 1: Beispiel zur Auswahl von Anmeldeinformationen

Geräte-IP	Verfügbare Berechtigungssätze	Ausgewählter Berechtigungssatz
10.10.1.5	10.10.1.5, 10.10.1., 10.10.*	10.10.1.5 (Genaue Übereinstimmung)
10.10.2.15	10.10.2., 10.10.*	10.10.2.* (Näheres)
10.10.5.50	10.10.	10.10.. (Genauere Angaben)

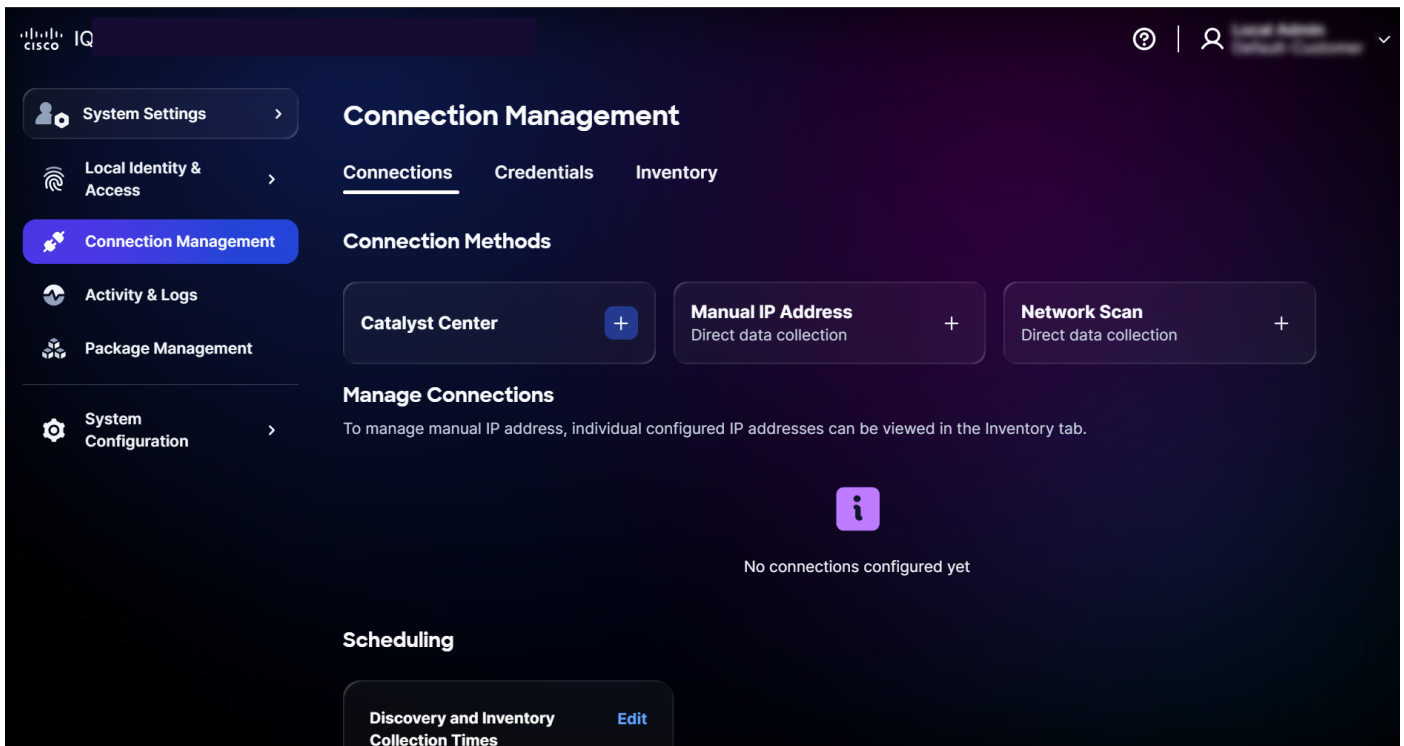
 Anmerkung: Fällt ein Gerät in mehrere sich überschneidende Kategorien, wählt das System immer den Berechtigungssatz mit der höchsten Spezifität aus (d. h. mit den wenigsten Platzhaltern am Ende).

Datenerfassung mit Catalyst Center

Sie können bis zu 20 Catalyst Center (nicht-Cluster) für jede Instanz von Cisco IQ VA anschließen.

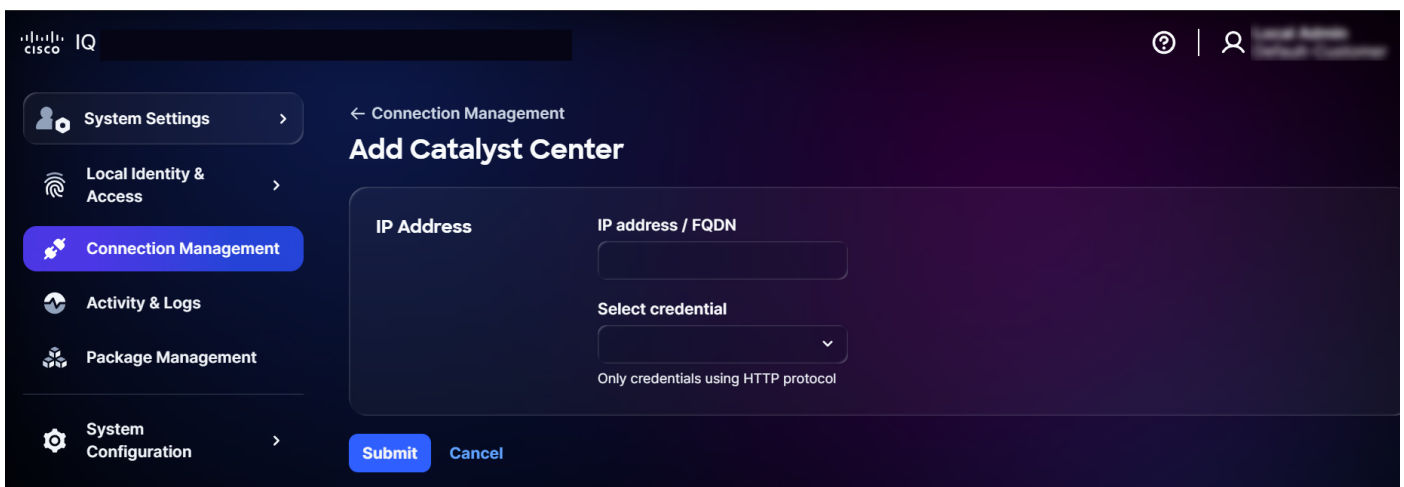
Datenerfassung mit Catalyst Center:

1. Wählen Sie unter Systemeinstellungen die Option Verbindungsverwaltung aus. Die Seite Verbindungsverwaltung wird angezeigt.



Verbindungsmanagement

2. Klicken Sie auf die Option Catalyst Center.



Catalyst Center hinzufügen

3. Geben Sie die IP-Adresse oder den FQDN ein.

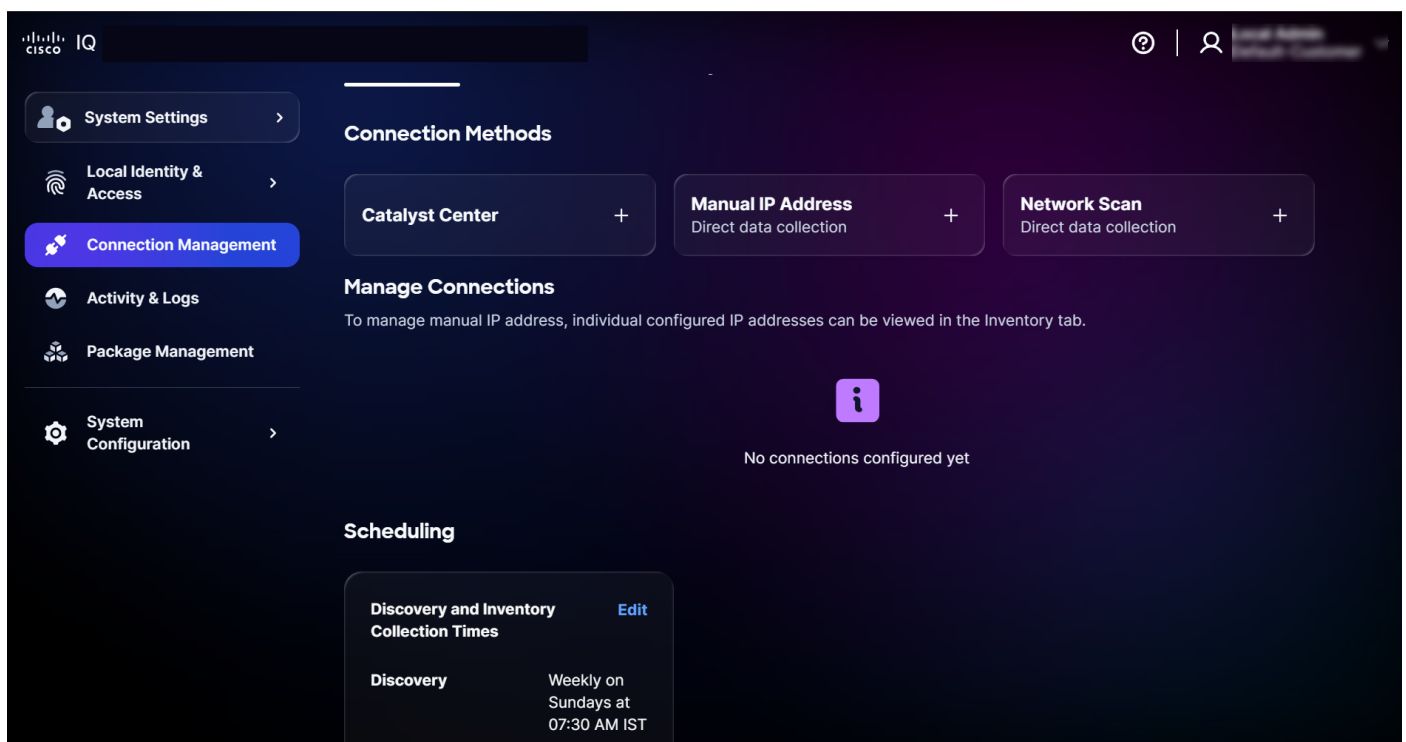
4. Wählen Sie in der Dropdown-Liste "Select credential" (Anmeldeinformationen auswählen) eine konfigurierte HTTP/HTTPS-Anmeldeinformation aus.
5. Klicken Sie auf Senden. Daraufhin wird eine Bestätigung angezeigt (kann bis zu 75 Minuten dauern). Sie können das neu hinzugefügte Catalyst Center unter Konfigurierte Verbindungen anzeigen.
6. Planen einer Sammlung. Weitere Informationen finden Sie unter [Planen](#).

 Anmerkung: Cisco IQ VA ist mit einer automatisierten Einrichtung für die Zeitplanung vorkonfiguriert, und das System initiiert einen standardmäßigen automatisierten Zeitplan für die Erfassung. Es wird dringend empfohlen, den Zeitplan an die Anforderungen und Wartungsfenster Ihres Unternehmens anzupassen.

Manuelle Datenerfassung

So fügen Sie Geräte für direkte Datenverbindungen hinzu:

1. Wählen Sie unter Systemeinstellungen die Option Verbindungsverwaltung aus. Die Seite Verbindungsverwaltung wird angezeigt.



Verbindungsmanagement

2. Klicken Sie auf Manuelle IP-Adresse. Die Seite "Direktverbindung" wird mit zwei (2)

Optionen zum Sammeln von Daten angezeigt.

System Settings >

Local Identity & Access >

Connection Management

Activity & Logs

Package Management

System Configuration >

← Connection Management

Direct Connection

Warning: Add credentials before form submission to ensure an immediate, successful discovery. Re-discovery will run on schedule until credentials are provided. [Add credentials](#)

Choose a Method of Entry

☒ Upload a file ☐ Specify individual devices

[Download the template](#) and add your device information. Then attach the file below.

Click or drag file to this area to upload

Only one CSV file can be uploaded. 50,000 assets maximum.

[Submit](#) [Cancel](#)

Datei hochladen

3. Klicken Sie unter Choose a Method of Entry (Eingabemethode auswählen) auf die bevorzugte Option, und geben Sie Ihre Geräteinformationen mit einer der folgenden Methoden an:

- Datei hochladen: Klicken Sie auf die Datei, oder ziehen Sie sie per Drag & Drop.

System Settings >

Local Identity & Access >

Connection Management

Activity & Logs

Package Management

System Configuration >

← Connection Management

Direct Connection

Warning: Add credentials before form submission to ensure an immediate, successful discovery. Re-discovery will run on schedule until credentials are provided. [Add credentials](#)

Choose a Method of Entry

☐ Upload a file ☒ Specify individual devices

Enter hostnames or IP addresses

e.g. 1.111.111.00.1.1, hostname.local, 1.1.1.1, hostname.dmz.local

[Submit](#) [Cancel](#)

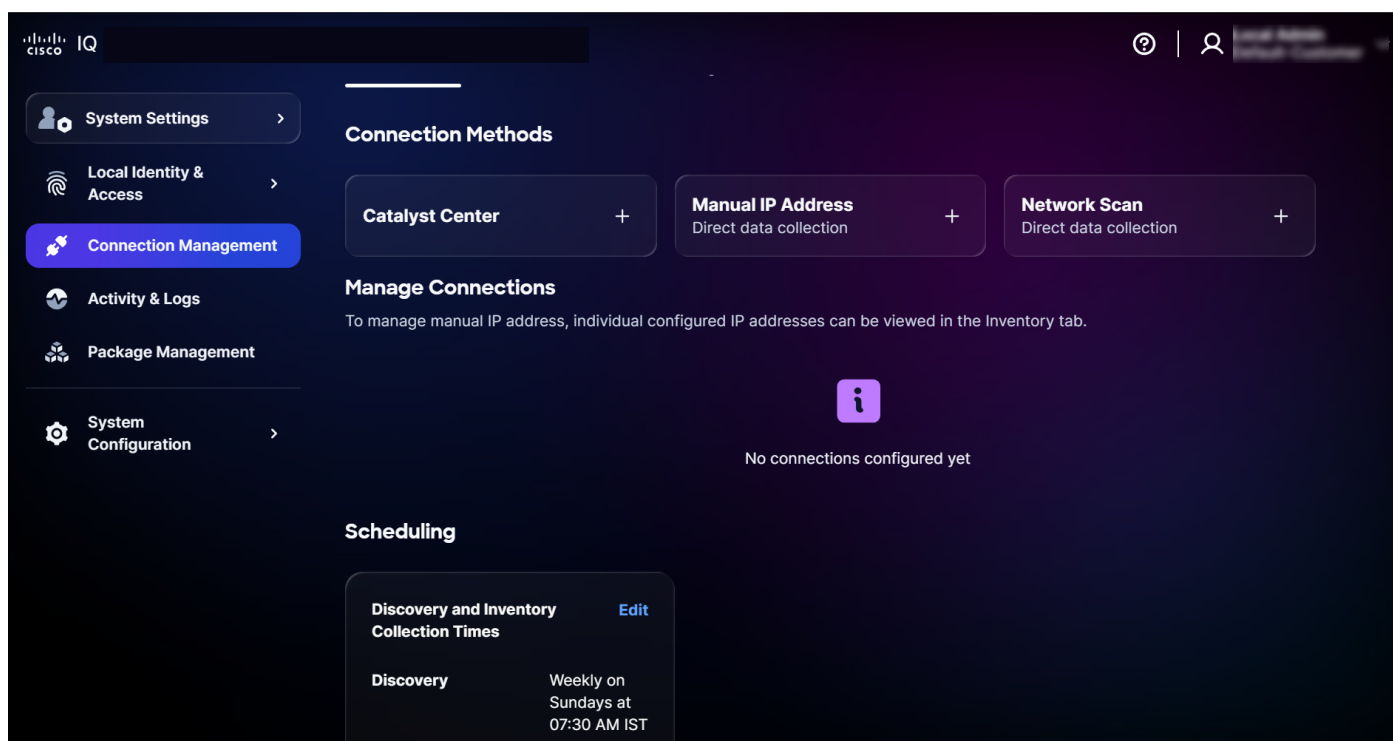
Individuelle Geräte angeben

- Geben Sie einzelne Geräte an: Geben Sie einen Hostnamen, eine IP-Adresse oder eine kommagetrennte Liste mit Hostnamen und/oder IP-Adressen ein.
4. Klicken Sie auf Senden. Nach erfolgreicher Einsendung werden Sie auf die Registerkarte Ressourcen weitergeleitet.
 5. Planen einer Sammlung. Weitere Informationen finden Sie unter [Planen](#).

 Anmerkung: Cisco IQ VA ist mit einer automatisierten Einrichtung für die Zeitplanung vorkonfiguriert, und das System initiiert einen standardmäßigen automatisierten Zeitplan für die Erfassung. Es wird dringend empfohlen, den Zeitplan entsprechend den Anforderungen und Wartungsfenstern Ihres Unternehmens zu bearbeiten.

Netzwerk-Scan

1. Wählen Sie unter Systemeinstellungen die Option Verbindungsverwaltung aus. Die Seite Verbindungsverwaltung wird angezeigt.



Netzwerk-Scan

2. Klicken Sie auf Netzwerksuche. Die Seite Assets nach Netzwerkscan verbinden wird mit drei

(3) Optionen angezeigt.

The screenshot shows the Cisco IQ web interface for 'Connect Assets by Network Scan'. The left sidebar contains navigation links: System Settings, Local Identity & Access, Connection Management (highlighted), Activity & Logs, Package Management, and System Configuration. The main content area is titled 'Connect Assets by Network Scan' and includes a 'Scan Method' section with three radio buttons: 'Specify IP Range' (selected), 'Specify Discovery Protocol (CDP/LLDP)', and 'File Upload'. Below this is a 'Name' text field. The 'Specify IP Range' method has 'IP Start' and 'IP End' text fields. A 'Schedule Scan' section contains a 'Frequency' dropdown menu and a 'Time' field with a clock icon and 'IST' label. At the bottom are 'Connect assets' and 'Cancel' buttons.

- IP-Bereich angeben: Definieren eines Bereichs von IP-Adressen, um Geräte innerhalb dieses Bereichs für Netzwerkerkennungs- oder -verwaltungsaufgaben zu adressieren
- Discovery Protocol (CDP/LLDP) angeben: Wählen Sie das zu verwendende Netzwerkerkennungsprotokoll aus.
- Datei hochladen: Laden Sie eine Datei hoch, z. B. Konfigurationsdateien oder Daten.

3. Geben Sie einen Namen ein.

4. Geben Sie IP Start und IP End ein.

5. Wählen Sie unter Zeitplansuche die Option Häufigkeit und Uhrzeit aus.

6. Klicken Sie auf Ressourcen verbinden.

Terminplanung

Mithilfe der Zeitplanung können Sie festlegen, wann Cisco IQ VA die automatisierte Datenerfassung durchführt. So planen Sie die Erfassung:

1. Klicken Sie im Abschnitt "Planung" auf der Seite "Verbindungsverwaltung" auf Bearbeiten, um den Zeitplan zu ändern. Die Seite "Zeitplan bearbeiten" wird angezeigt.

Zeitplan bearbeiten

2. Wählen Sie im Abschnitt Schedule Discovery aus den Dropdown-Listen Ihre bevorzugte Häufigkeit und Ihren gewünschten Tag aus, und geben Sie die gewünschte Startzeit ein.
3. Wählen Sie im Abschnitt "Schedule Inventory Collection" (Bestandserfassung planen) aus den Dropdown-Listen Ihre bevorzugte Häufigkeit aus, und geben Sie die gewünschte Startzeit ein.
4. Klicken Sie auf Senden.



Anmerkung: Bei Änderungen an Erkennungs- oder Erfassungsplänen dauert es 5-10 Minuten, bis diese innerhalb der virtuellen Appliance synchronisiert und korrekt wiedergegeben werden.

Installieren von Paketen (Module, Regeln und Berechtigungen)

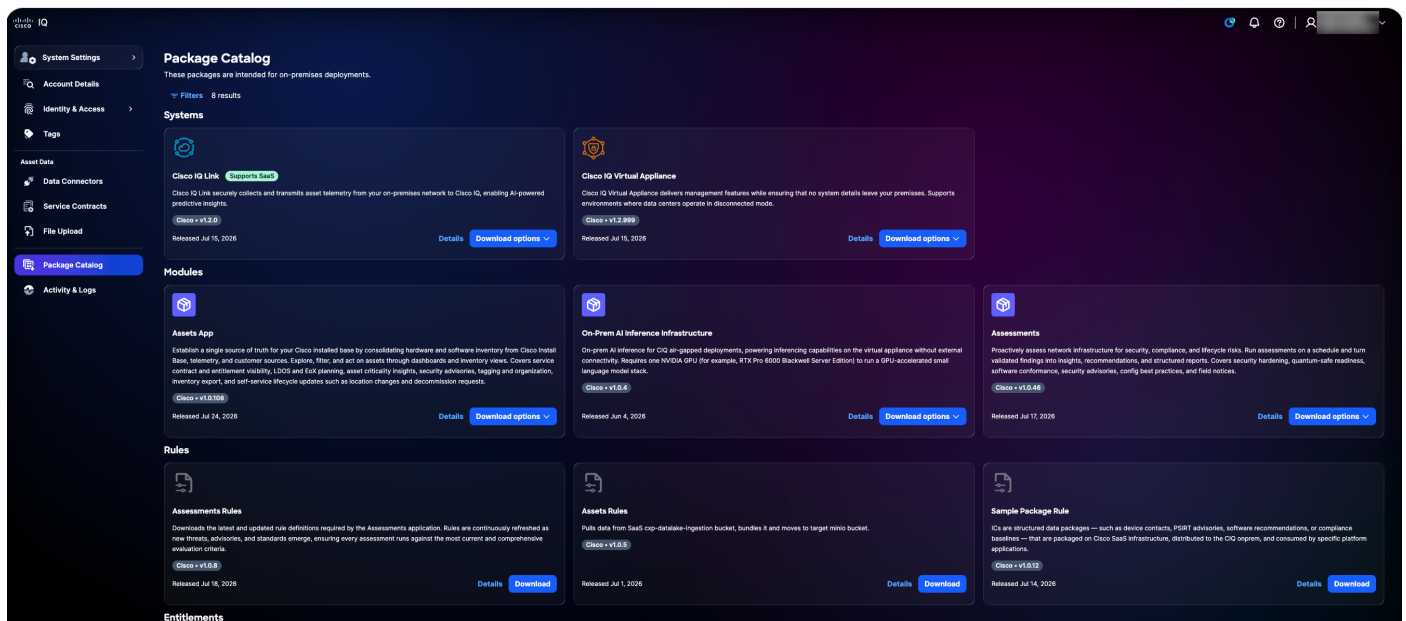
Sie können den Software-Lebenszyklus (d. h. Installation und Konfiguration) von Betriebsmodulen, Regeln, Berechtigungen und speziellen KI-gestützten Funktionen innerhalb der VA verwalten. Sie können sie installieren, indem Sie die neuesten Versionen von Cisco IQ (SaaS) herunterladen. Rufen Sie dazu den Paketkatalog auf. Im Paketkatalog werden die Softwareinstanzen angezeigt, die Ihnen zur Verfügung stehen. Es ermöglicht Ihnen, Updates nahtlos zu überwachen und zu verwalten, um eine effiziente Nachverfolgung und Verwaltung Ihrer Systeminstanzen sicherzustellen.

Hinzufügen von Modulen

Ein Modul ist ein eigenständiges Softwarepaket, das Kernfunktionen innerhalb der VA bereitstellt.

Hierbei handelt es sich um einen unabhängigen Service mit eigenem Lebenszyklus, der die Installation, Wartung und Größenanpassung ermöglicht. Die Ressourcenbelegung - einschließlich CPU, Grafikprozessor (GPU) und RAM - wird dynamisch auf Basis der bei der Erstinstallation ausgewählten Bereitstellungsgröße (klein, mittel oder groß) zugewiesen.

1. Melden Sie sich bei [Cisco IQ an](#).
2. Navigieren Sie zu Systemeinstellungen > Paketkatalog.

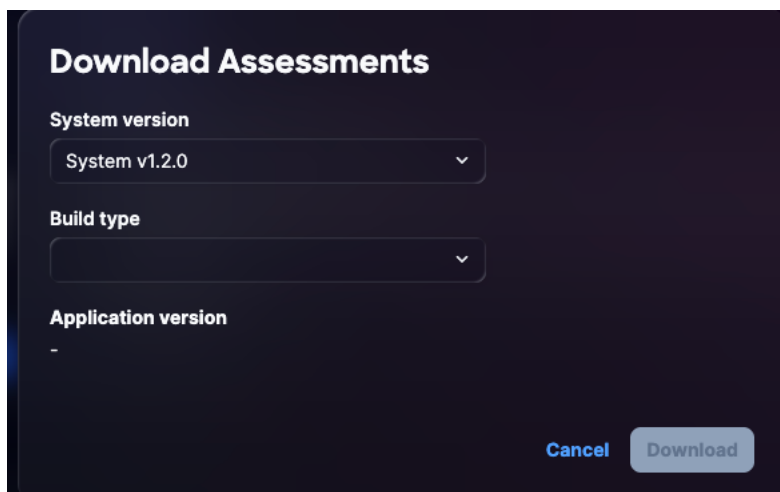


Paketkatalog

3. Klicken Sie auf der gewünschten Modulkarte auf Download options > Installation packages. Das Fenster Download wird geöffnet.



Anmerkung: Für die Beispiel-Images wird das Bewertungsmodul verwendet.



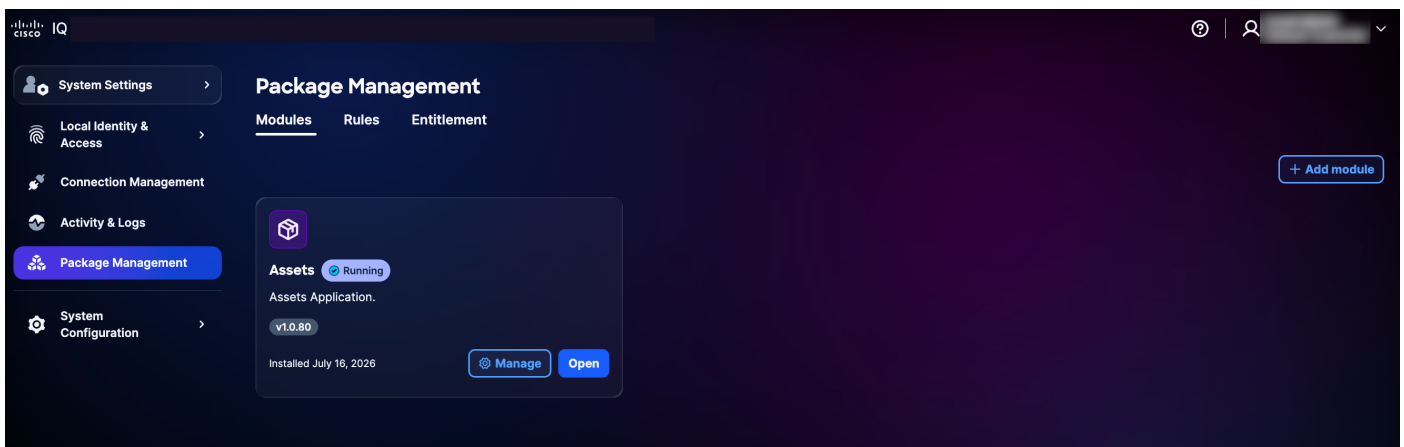
Herunterladen

4. Wählen Sie eine Systemversion aus der Dropdown-Liste aus.
5. Wählen Sie einen Buildtyp aus der Dropdown-Liste aus.
6. Klicken Sie auf Herunterladen, um die Datei lokal zu speichern.



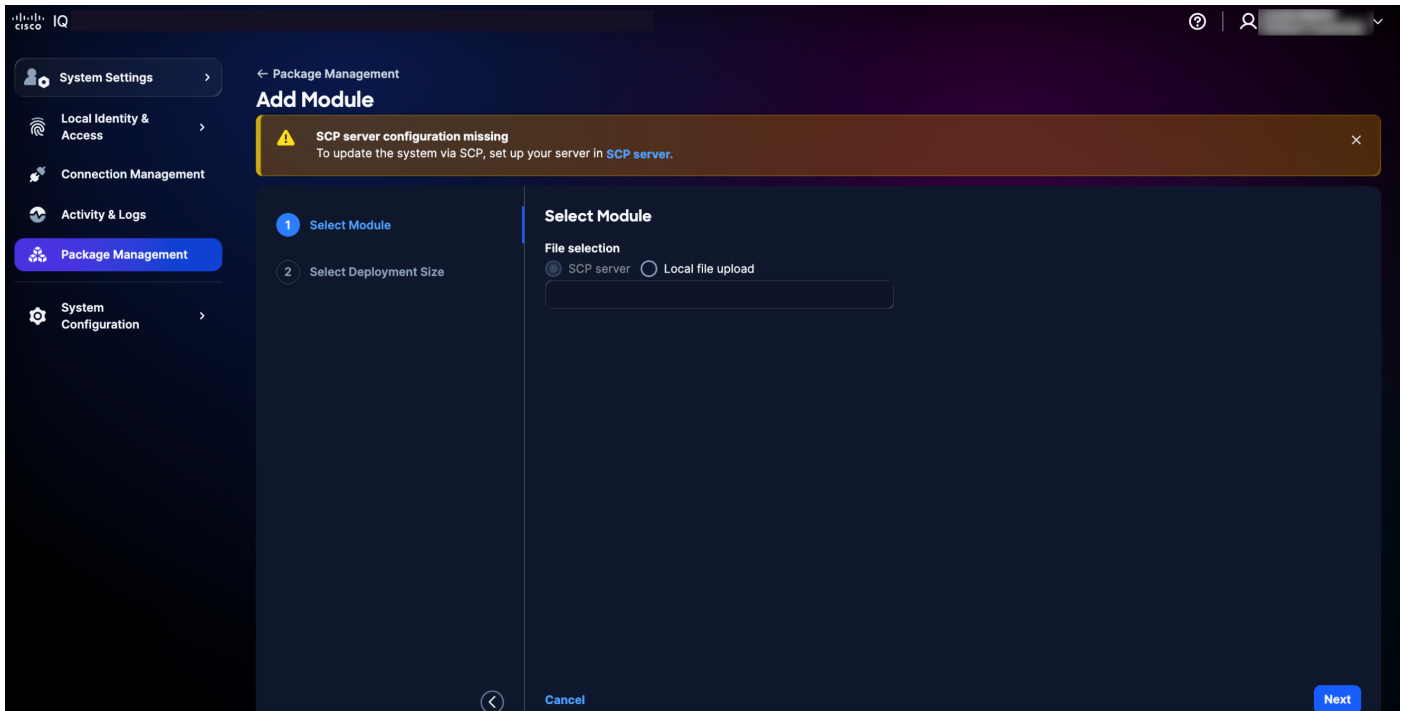
Anmerkung: Die Installationsdateien sind groß (10-25 GB). Stellen Sie vor dem Herunterladen sicher, dass Sie über ausreichend Speicherplatz verfügen.

7. Navigieren Sie zu VA.
8. Navigieren Sie zu Startseite > Systemeinstellungen > Paketverwaltung. Die Seite Paketverwaltung wird mit den folgenden Registerkarten angezeigt:
 - Module
 - Regeln
 - Ansprüche



Module

9. Klicken Sie auf Modul hinzufügen.

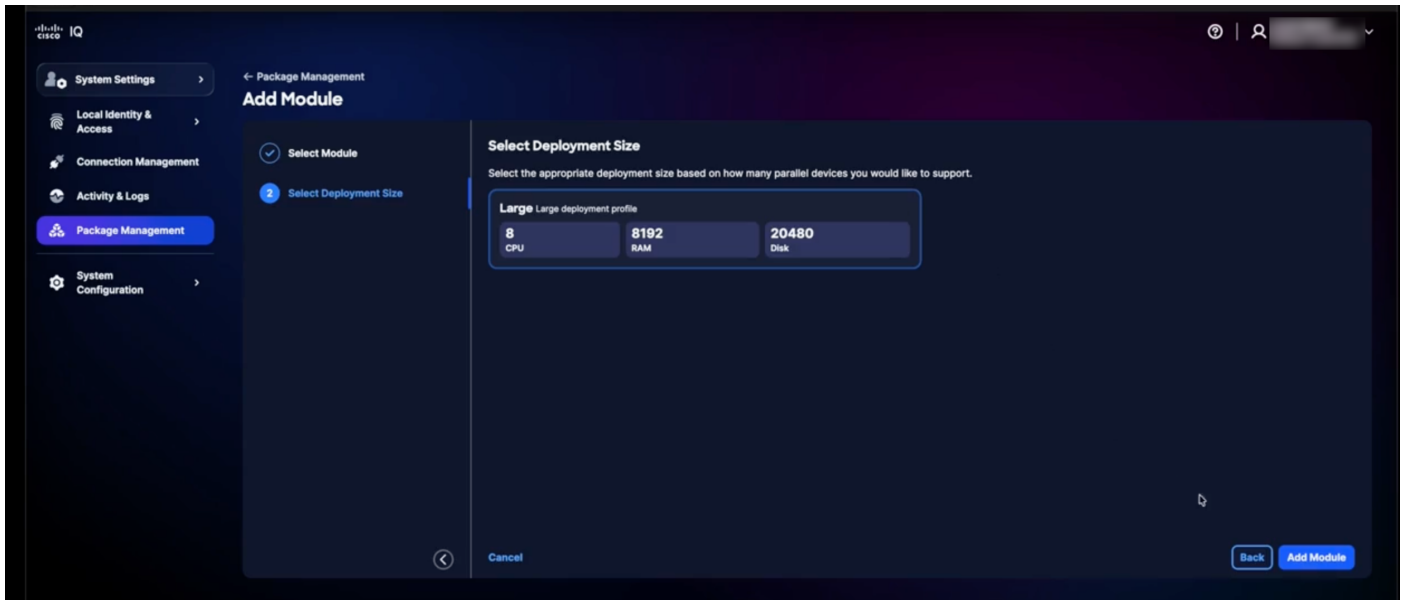


Modul hinzufügen

10. Wählen Sie Ihre bevorzugte Dateiauswahl-Option:

- SCP-Server: Geben Sie den genauen Dateinamen des Installationspakets ein (empfohlen für große Dateien).
- Upload der lokalen Datei: Ziehen Sie die heruntergeladene Installationsdatei per Drag-and-Drop (wird aufgrund der Uploadzeit für Dateien mit einer Größe von 30 GB oder mehr nicht empfohlen).

11. Klicken Sie auf Next (Weiter).

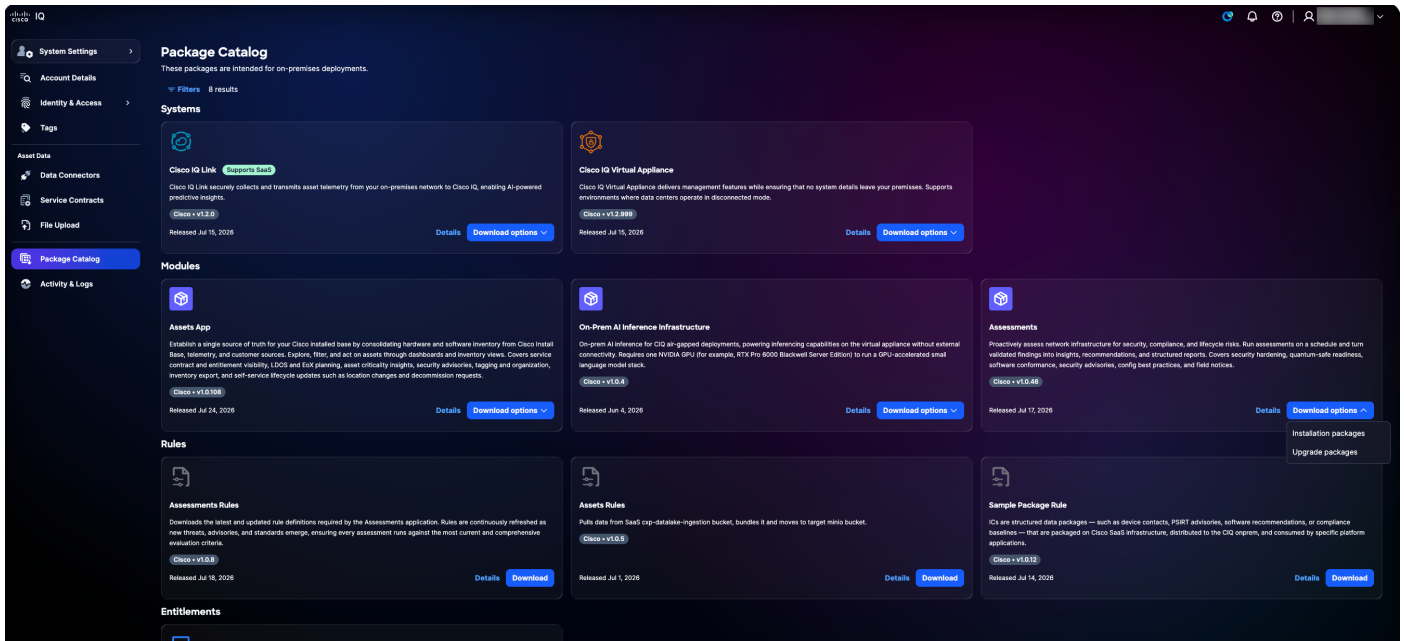


Bereitstellungsgröße

12. Wählen Sie die Bereitstellungsgröße (z. B. Klein, Mittel oder Groß) aus. Diese Größen sind vordefiniert und geben die Ressourcenanforderungen vor.
13. Klicken Sie auf Modul hinzufügen. Das neu installierte Modul wird auf der Registerkarte Module in der Paketverwaltung angezeigt. Nach Abschluss des Vorgangs ändert sich der Modulstatus in "Running" (Wird ausgeführt), und die Schaltfläche Open (Öffnen) wird verfügbar.

Modul-Upgrade

Die neuesten Module werden fortlaufend im Paketkatalog (in Cisco IQ) aktualisiert. Upgrade auf die neueste Version:



Vernetzung von Ressourcen durch Netzwerksuche

1. Klicken Sie auf der gewünschten Modulkarte auf Download options > Upgrade packages. Das Fenster Download wird geöffnet.



Anmerkung: Das Bewertungsmodul dient als Beispiel für die Images.

Upgrade Assessments

System version

System v1.2.0



Current app version



Build type



Application version

-

Cancel

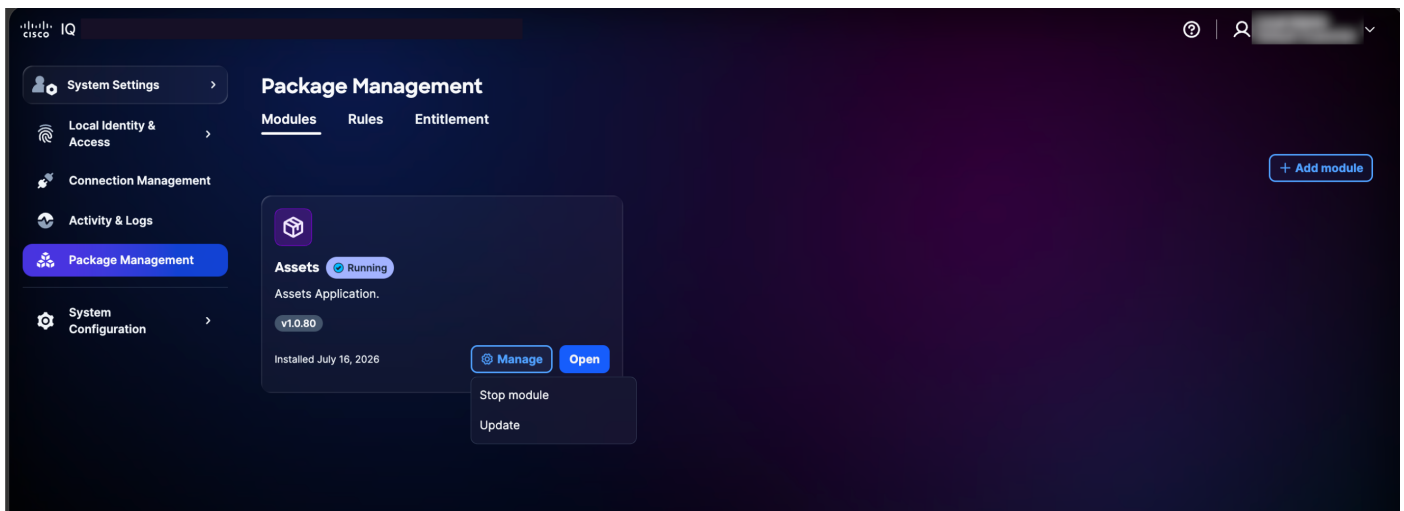
Download

Herunterladen

2. Wählen Sie eine Systemversion aus der Dropdown-Liste aus.
3. Wählen Sie eine aktuelle App-Version aus der Dropdown-Liste aus.
4. Wählen Sie einen Buildtyp aus der Dropdown-Liste aus.
5. Klicken Sie auf Herunterladen, um die Datei lokal zu speichern.
6. Navigieren Sie zu VA, und schließen Sie die Installation der heruntergeladenen Datei ab.

Verwalten von Modulen

Nachdem Sie ein Modul hinzugefügt haben, können Sie es auf der Seite Paketverwaltung ändern, indem Sie auf Verwalten klicken. Zu den verfügbaren Änderungsoptionen gehören die Größenänderung und das Upgrade auf eine höhere Version. So verwalten Sie Module:



Aktualisierungstyp

1. Klicken Sie auf der Seite Paketverwaltung auf Verwalten > Aktualisieren für das gewünschte Modul.
2. Wählen Sie den Aktualisierungstyp aus:
 - Nur Bereitstellungsgröße ändern
 - Version aktualisieren
3. Wenn die Option Bereitstellungsgröße ändern ausgewählt ist, klicken Sie auf Weiter, und wählen Sie auf der folgenden Seite die neue Bereitstellungsgröße aus.

ODER

Wenn Version aktualisieren ausgewählt ist, wird die Option Dateiauswahl angezeigt. Wählen Sie entweder SCP Server und geben Sie den genauen Dateinamen des Installationspakets ein, oder wählen Sie Lokaler Datei-Upload und ziehen Sie die heruntergeladene Installationsdatei per Drag-and-Drop.

4. Klicken Sie auf Next (Weiter). Die Seite "Aktualisierungszeitplan auswählen" wird angezeigt.
5. Wählen Sie eine der folgenden Optionen aus, um den Zeitplan zu aktualisieren:
 - Jetzt aktualisieren
 - Später aktualisieren



Anmerkung: Einige Module unterstützen Updates ohne Ausfallzeiten. Wenn Ausfallzeiten erforderlich sind, werden die Details in einem Banner angezeigt.

6. Wenn die Option Später aktualisieren ausgewählt ist, geben Sie Datum und Uhrzeit ein.

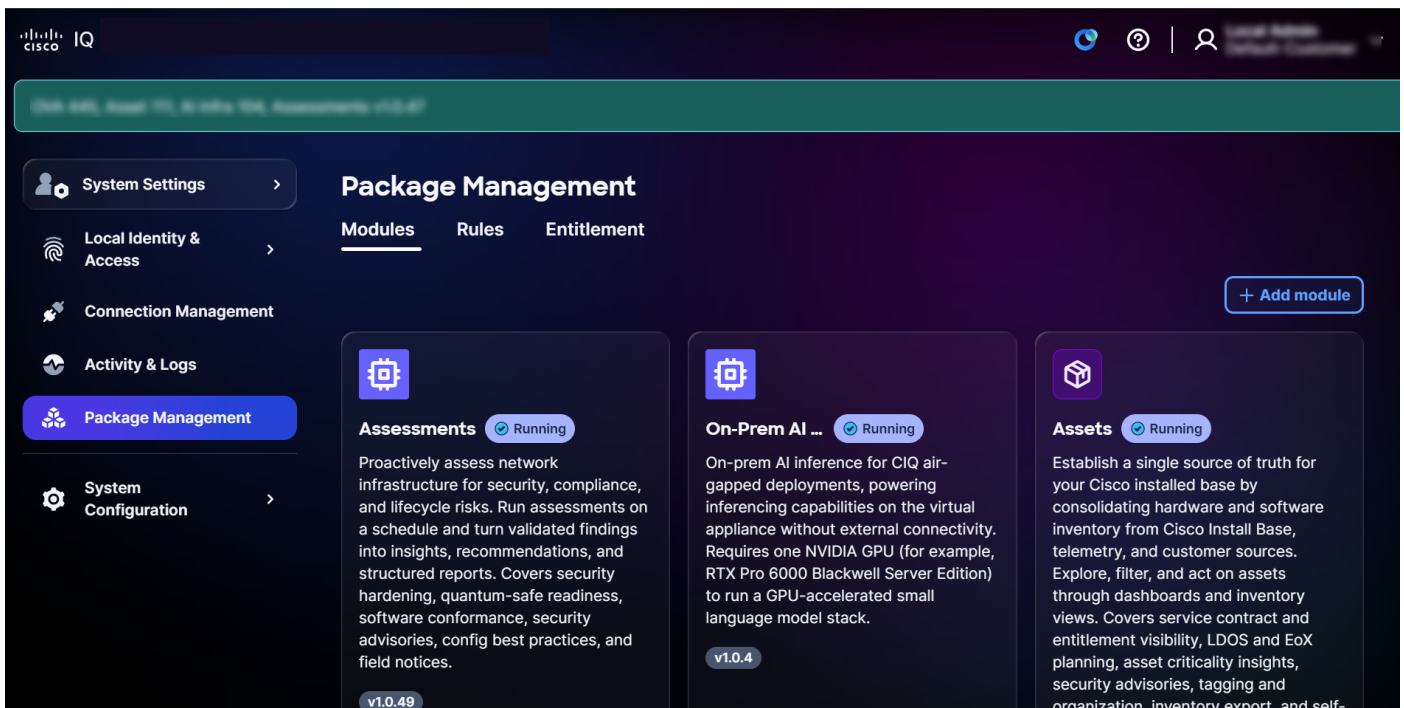
7. Klicken Sie auf Next (Weiter). Die Aktualisierungsübersicht wird angezeigt.

 Anmerkung: Über die Update Summary (Aktualisierungsübersicht) können Sie auf die Versionshinweise zugreifen.

8. Klicken Sie auf Modul aktualisieren, und navigieren Sie zur Registerkarte Modul. Das Modul zeigt den Status "Geplantes Update" an.

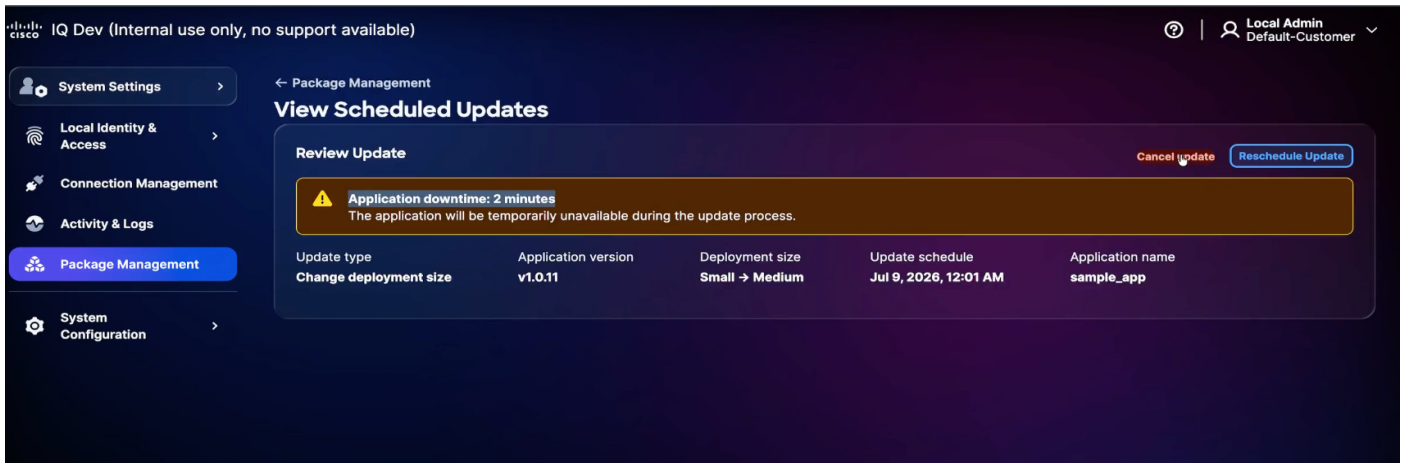
Zeitpläne bearbeiten

Sie können geplante Updates auch anzeigen, bearbeiten oder abbrechen. So bearbeiten oder stornieren Sie eine geplante Aktualisierung:



Bearbeitungszeitplan

1. Klicken Sie auf der Seite Paketverwaltung auf Verwalten > Geplante Aktualisierung des gewünschten Moduls anzeigen. Das Fenster "Geplante Updates anzeigen" wird angezeigt.



Updates planen

2. Klicken Sie ggf. auf Aktualisierung abbrechen oder Aktualisierung neu planen.
3. Befolgen Sie die Anweisungen auf dem Bildschirm, um die Vorgänge abzuschließen.

 Anmerkung: Wenn ein Modulvorgang (z. B. Installation, Upgrade oder Größenänderung) fehlschlägt, wählen Sie eine der folgenden Optionen aus:

Wiederholen: Die Benutzeroberfläche zeigt eine Schaltfläche zum Wiederholen an, mit der Sie den Vorgang wiederholen können. Protokolle: Wenn ein Fehler weiterhin auftritt, klicken Sie auf Protokolle, um detaillierte Diagnoseinformationen anzuzeigen. Dies ist die primäre Methode zur Identifizierung der Ursache von Installations- oder Laufzeitfehlern.

Installieren von Regeln

Eine Regel ist eine spezialisierte Komponente oder ein "Add-on", das die Funktionalität eines vorhandenen Moduls erweitert oder ändert. Regeln sind nicht für die Ausführung als eigenständige Programme konzipiert; Sie sind an ein Modul "angeschlossen", um bestimmte Regeln, Logik oder Funktionen bereitzustellen. Regeln sind an bestimmte Module gebunden. Wenn eine Regel installiert ist, wird sie mit dem Modul verknüpft, das sie unterstützt. Mit Regeln kann das System aktualisiert oder angepasst werden, ohne dass ein vollständiges Upgrade des Kernmoduls erforderlich ist. Wenn neue Regeln oder Funktionen benötigt werden, können Sie dem vorhandenen Modul einfach eine neue Regel hinzufügen.

So laden Sie eine Regel:

1. Melden Sie sich bei [Cisco IQ an](#).

2. Navigieren Sie zu Systemeinstellungen > Paketkatalog.
3. Klicken Sie auf der gewünschten Regelkarte auf Herunterladen.



Anmerkung: Das folgende Beispielbild zeigt eine Regel für Ressourcen.

Download Assets Rules

Target app version

assets v1.0.0



Cancel

Download

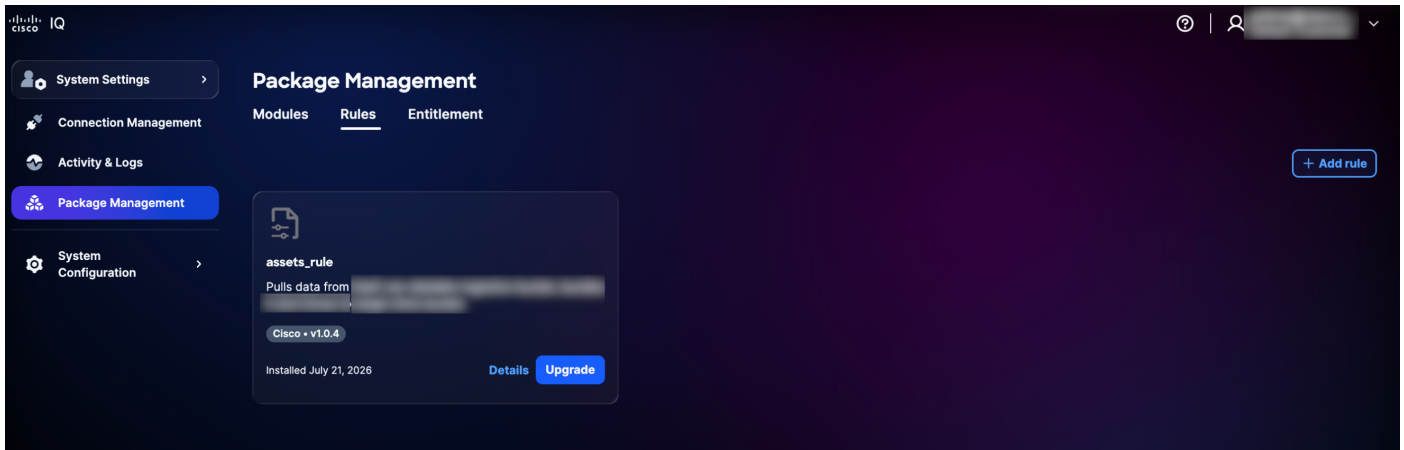
Herunterladen

4. Wählen Sie eine Ziel-App-Version aus der Dropdown-Liste aus.
5. Klicken Sie auf Herunterladen, um die Datei lokal zu speichern.



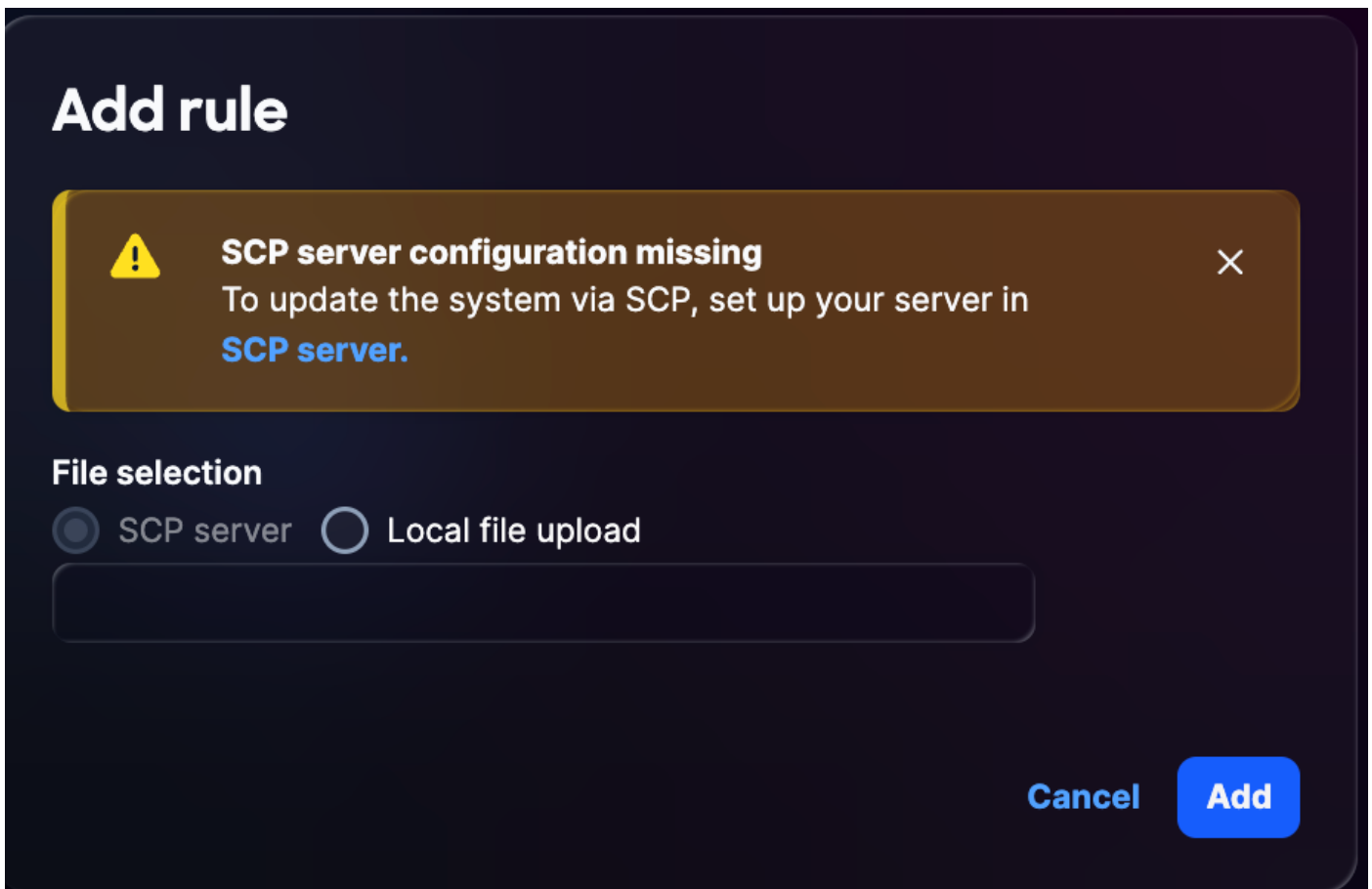
Anmerkung: Die Installationsdateien sind groß (10-25 GB). Stellen Sie vor dem Herunterladen sicher, dass Sie über ausreichend Speicherplatz verfügen.

6. Navigieren Sie zu VA.
7. Navigieren Sie zu Startseite > Systemeinstellungen > Paketverwaltung. Die Seite Paketverwaltung wird mit den folgenden Registerkarten angezeigt.
 - Module
 - Regeln
 - Ansprüche
8. Klicken Sie auf die Registerkarte Regeln.



Paketverwaltung

9. Klicken Sie auf Regel hinzufügen.



Regel hinzufügen

10. Wählen Sie Ihre bevorzugte Dateiauswahl-Option:

- SCP-Server (Secure Copy Protocol): Geben Sie den genauen Dateinamen des

Installationspakets ein. Diese Methode wird für große Dateien empfohlen.

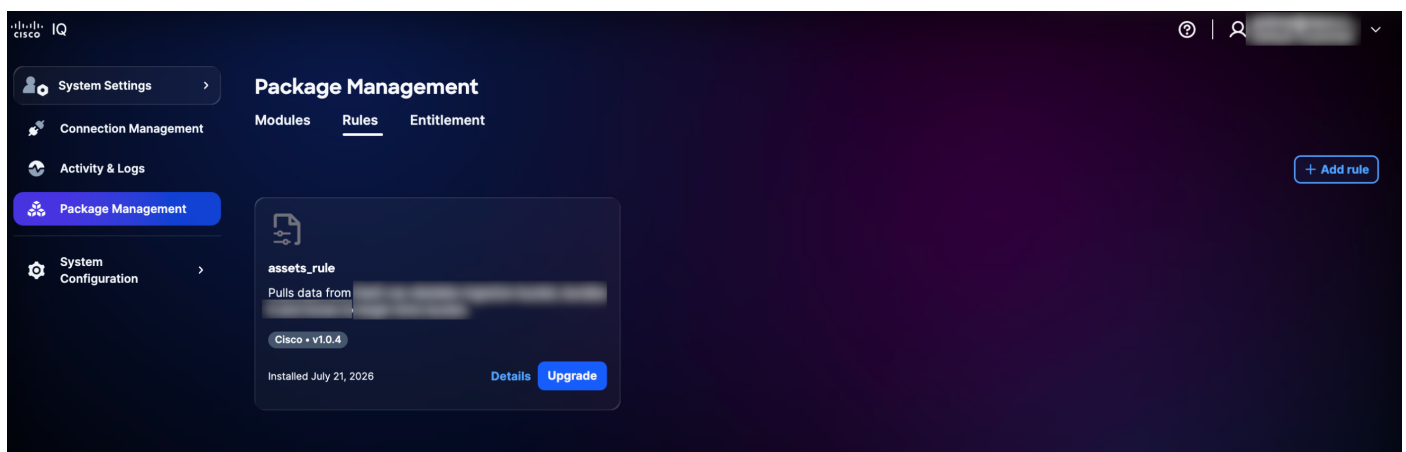
- Upload der lokalen Datei: Ziehen Sie die heruntergeladene Installationsdatei per Drag-and-Drop.

11. Klicken Sie auf Hinzufügen. Die hinzugefügte Regel wird in der Paketverwaltung angezeigt.

Regeln aktualisieren

So aktualisieren Sie Regeln:

1. Navigieren Sie zu Systemeinstellungen > Paketverwaltung in VA.



Upgrade

2. Klicken Sie in der gewünschten Regel auf Aktualisieren. Das Fenster Aktualisierungsregel wird geöffnet.

Upgrade Rule

File selection

☒ SCP server ☐ Local file upload

Cancel

Add

Aktualisierungsregel

3. Wählen Sie Ihre bevorzugte Dateiauswahl-Option:

- SCP-Server (Secure Copy Protocol): Geben Sie den genauen Dateinamen des Installationspakets ein. Diese Methode wird für große Dateien empfohlen.
- Upload der lokalen Datei: Ziehen Sie die heruntergeladene Installationsdatei per Drag-and-Drop.

4. Klicken Sie auf Hinzufügen.

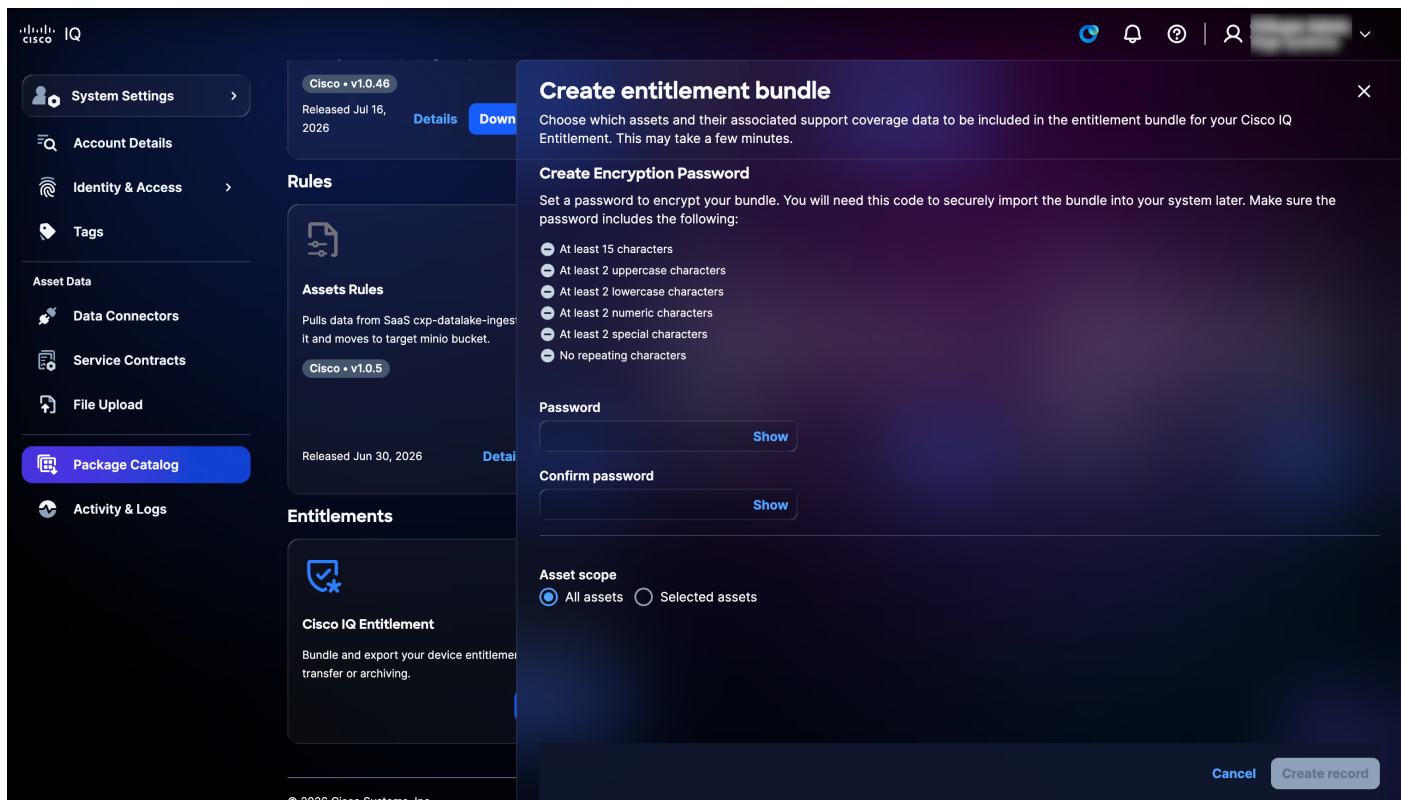
 Anmerkung: Diese Regeln werden bei der fortlaufenden Sammlung von Telemetriedaten für geplante Geräte angewendet. Für eine sofortige Anwendung können Sie die Erfassung der Gerätelemetrie manuell initiieren.

Installieren von Berechtigungen

Mit einer Berechtigung wird das Recht Ihres Unternehmens zur Verwendung bestimmter Softwarefunktionen, -module oder -services validiert. So installieren Sie eine Berechtigung:

1. Melden Sie sich bei [Cisco IQ an](#).
2. Navigieren Sie zu Systemeinstellungen > Paketkatalog.
3. Klicken Sie auf der Berechtigungskarte auf Datensatz erstellen. Das Fenster

"Berechtigungspaket erstellen" wird geöffnet.



Berechtigungspaket erstellen

4. Geben Sie ein Kennwort ein. Weitere Informationen finden Sie in den auf dem Bildschirm angezeigten Regeln zur Kennworterstellung.
5. Geben Sie das gleiche Kennwort unter Kennwort bestätigen erneut ein.
6. Wählen Sie das Optionsfeld für den bevorzugten Anlagenbereich.
 - Alle Ressourcen: Beinhaltet alle mit Ihnen verknüpften Ressourcen
 - Ausgewählte Ressourcen: Ermöglicht Ihnen die Auswahl bestimmter, auf Ihre Umgebung abgestimmter Geräte. Aktivieren Sie bei Aktivierung dieser Option die Kontrollkästchen aller zutreffenden Ressourcen.
7. Klicken Sie auf Datensatz erstellen, um die Datei lokal zu speichern.



Anmerkung: Navigieren Sie nach dem Erstellen des Anspruchspakets nicht vom aktuellen Bildschirm weg. Wenn Sie zu einer anderen Seite navigieren, wird das Paket ungültig, und Sie müssen es neu generieren, um die Download-Option zu aktivieren.



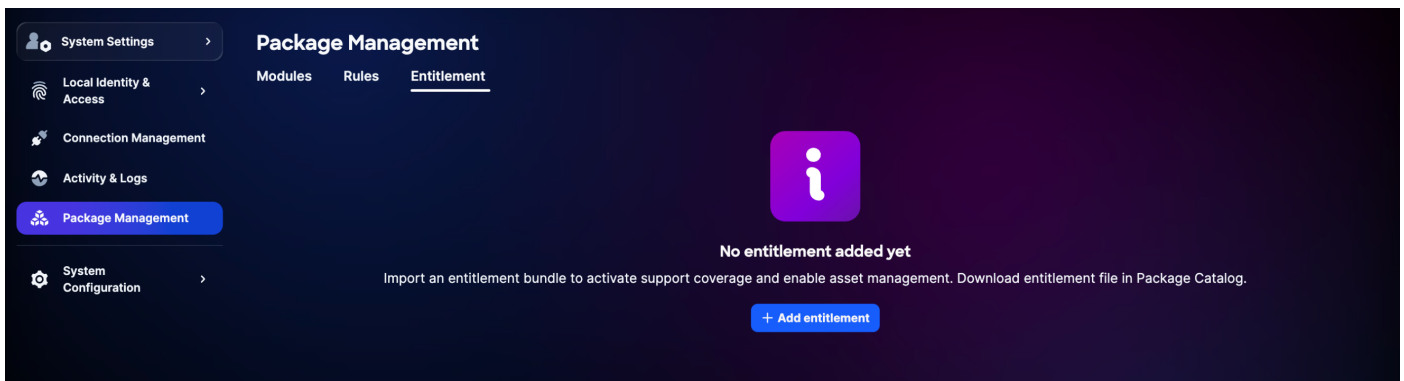
Anmerkung: Die Installationsdateien sind groß (10-25 GB). Stellen Sie vor dem Herunterladen sicher, dass Sie über ausreichend Speicherplatz verfügen.

8. Melden Sie sich bei VA an.

9. Navigieren Sie zu Startseite > Systemeinstellungen > Paketverwaltung. Die Seite Paketverwaltung enthält die folgenden Registerkarten:

- Module
- Regeln
- Ansprüche

10. Klicken Sie auf die Registerkarte Berechtigungen.



Registerkarte Berechtigung

11. Klicken Sie auf Berechtigung hinzufügen.

Add Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

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

Berechtigung hinzufügen

12. Wählen Sie Ihre bevorzugte Dateiauswahloption aus.

- SCP-Server (Secure Copy Protocol): Geben Sie den genauen Dateinamen des Installationspakets ein. Diese Methode wird für große Dateien empfohlen
- Upload der lokalen Datei: Ziehen und Ablegen der heruntergeladenen Installationsdatei

13. Geben Sie ein Kennwort ein.

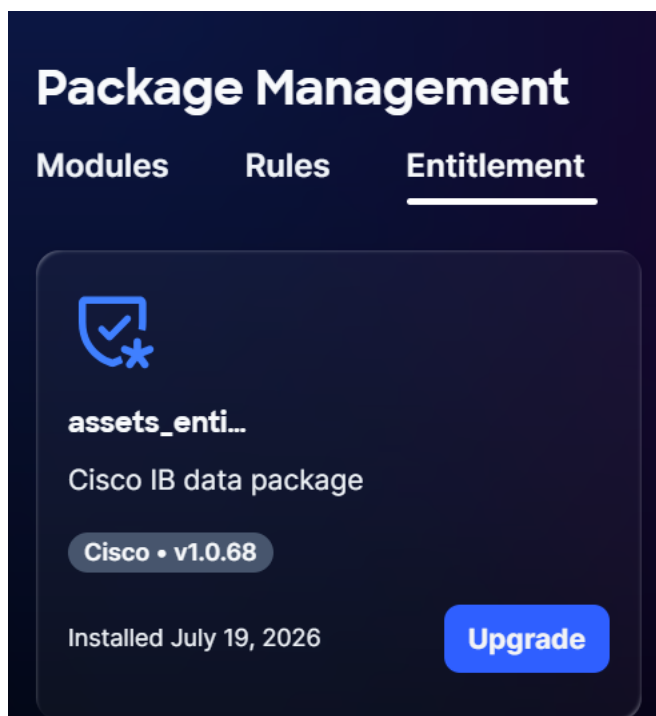
14. Klicken Sie auf Hinzufügen. Die neu installierte Berechtigung wird auf der Registerkarte Berechtigung in der Paketverwaltung angezeigt.

15. Um Berechtigungen zu aktivieren, warten Sie nach dem Hinzufügen 5 bis 10 Minuten, und starten Sie dann die Telemetriesammlung des Geräts.

 Anmerkung: Durch Hinzufügen eines Servicevertrags im Berechtigungsprozess werden alle mit diesem Vertrag verknüpften Geräte dem Inventar der Geräte vor Ort hinzugefügt. Sie haben die Möglichkeit, Geräte nach Seriennummer zu filtern, mehrere Konto-IDs zu verwenden oder bestimmte Geräte auszuwählen, um Berechtigungen zu verwalten.

Aktualisieren von Ansprüchen

So aktualisieren Sie einen Anspruch:



Berechtigungs-Upgrade

1. Klicken Sie unter der gewünschten Berechtigung auf Aktualisieren.

Upgrade Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

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

Upgrade-Berechtigung

2. Wählen Sie Ihre bevorzugte Dateiauswahl-Option:

- SCP-Server (Secure Copy Protocol): Geben Sie den genauen Dateinamen des Installationspakets ein. Diese Methode wird für große Dateien empfohlen
- Upload der lokalen Datei: Ziehen und Ablegen der heruntergeladenen Installationsdatei

3. Geben Sie ein Kennwort ein.

4. Klicken Sie auf Hinzufügen.

Funktionen mit KI

Das standortbasierte KI-Inferenzinfrastrukturmodul ermöglicht standortbasierte KI-gestützte Funktionen in VA. Es führt lokal ein Small Language Model (SLM) aus, das es dem System ermöglicht, auf KI-gestützte Aufforderungen zu reagieren. Nach der Installation können Sie direkt über die VA-Schnittstelle mit dem System interagieren.

Folgende Abfragetypen werden unterstützt:

- Ressourcen: Identifizierung von Ressourcen, die aufgrund von End-of-Life-Status, Softwarewährungen oder Nichtkonformität, Sicherheitslücken und Lücken in der Vertragsabdeckung gefährdet sind
- Bestand: Fordern Sie eine KI-gestützte Analyse der Bestände an.

Das Installationspaket für die standortbasierte KI-Inferenzinfrastruktur ist im Cisco IQ-Paketkatalog verfügbar und wird wie andere Module (z. B. Ressourcen) verteilt.

 Anmerkung: Es kann jeweils nur eine (1) standortbasierte KI-Inferenzinfrastruktur pro GPU ausgeführt werden. Die Installation dauert ca. 40-45 Minuten. Die Installationsdateien sind groß (ca. 30 GB). Stellen Sie vor dem Herunterladen sicher, dass Sie über ausreichend Speicherplatz verfügen.

Voraussetzungen für standortbasierte KI-Inferenzinfrastruktur

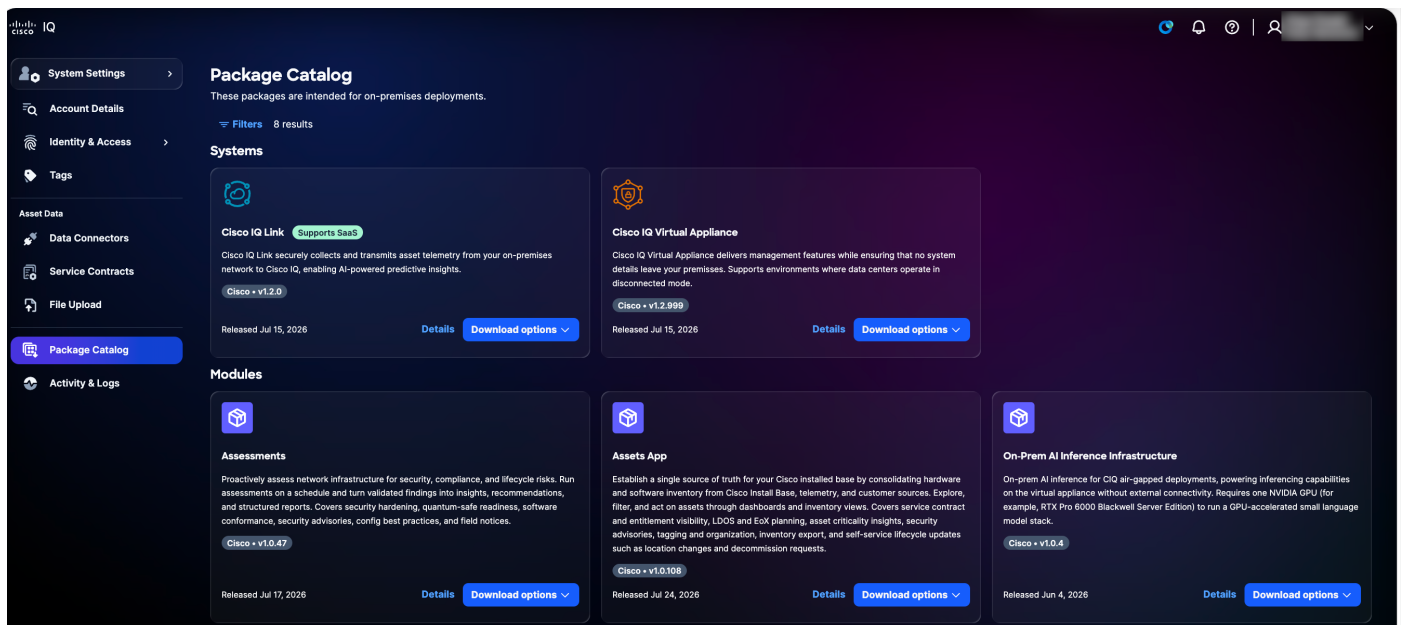
Vor der Installation der On-Prem AI Inference Infrastructure müssen folgende Voraussetzungen erfüllt sein:

- Die VA muss eine VM mit GPU-Zugang enthalten. Der SLM erfordert eine GPU und kann nicht ohne eine ausgeführt werden.
- Die GPU VM muss über mindestens 80 GB GPU VRAM verfügen.

Installation der Infrastruktur für KI-Inferenz am Standort

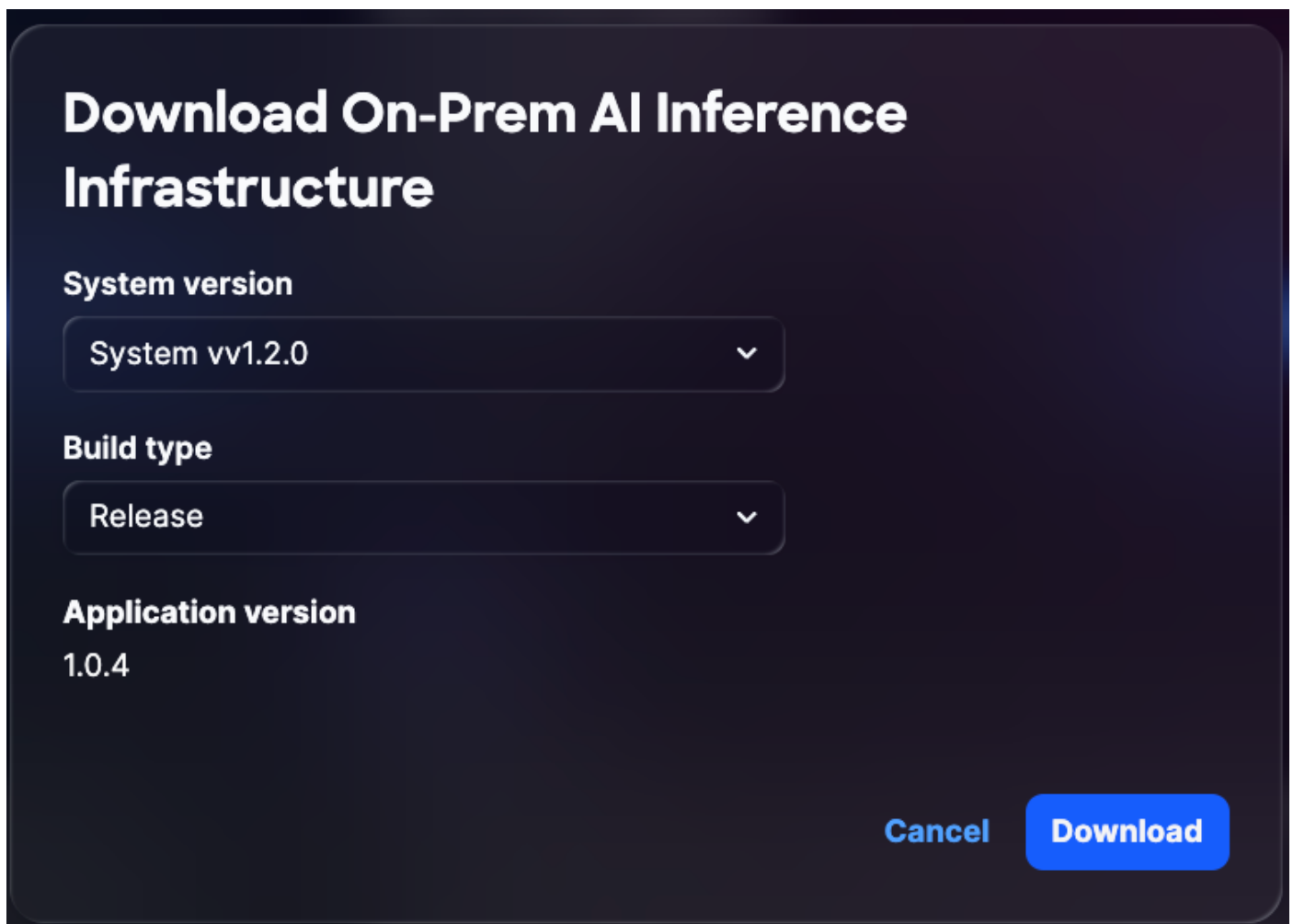
Um die standortbasierte KI-Inferenzinfrastruktur in der VA zu installieren, laden Sie das standortbasierte KI-Inferenzinfrastrukturmodul von Cisco IQ SaaS herunter:

1. Melden Sie sich bei [Cisco IQ an](#).
2. Navigieren Sie zu Systemeinstellungen > Paketkatalog.



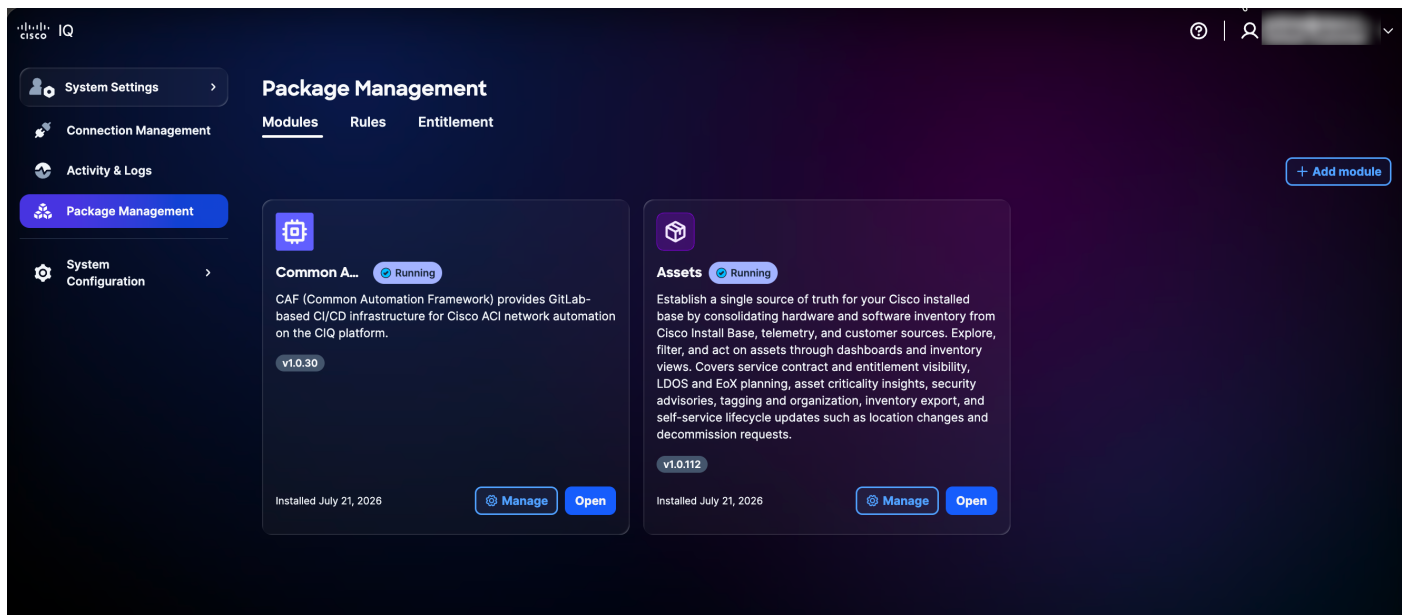
Paket installieren

-
-
3. Klicken Sie auf der Infrastruktur-Karte für standortbasierte KI-Inferenz auf Download options > Installation packages. Das Fenster Anwendung herunterladen wird geöffnet.



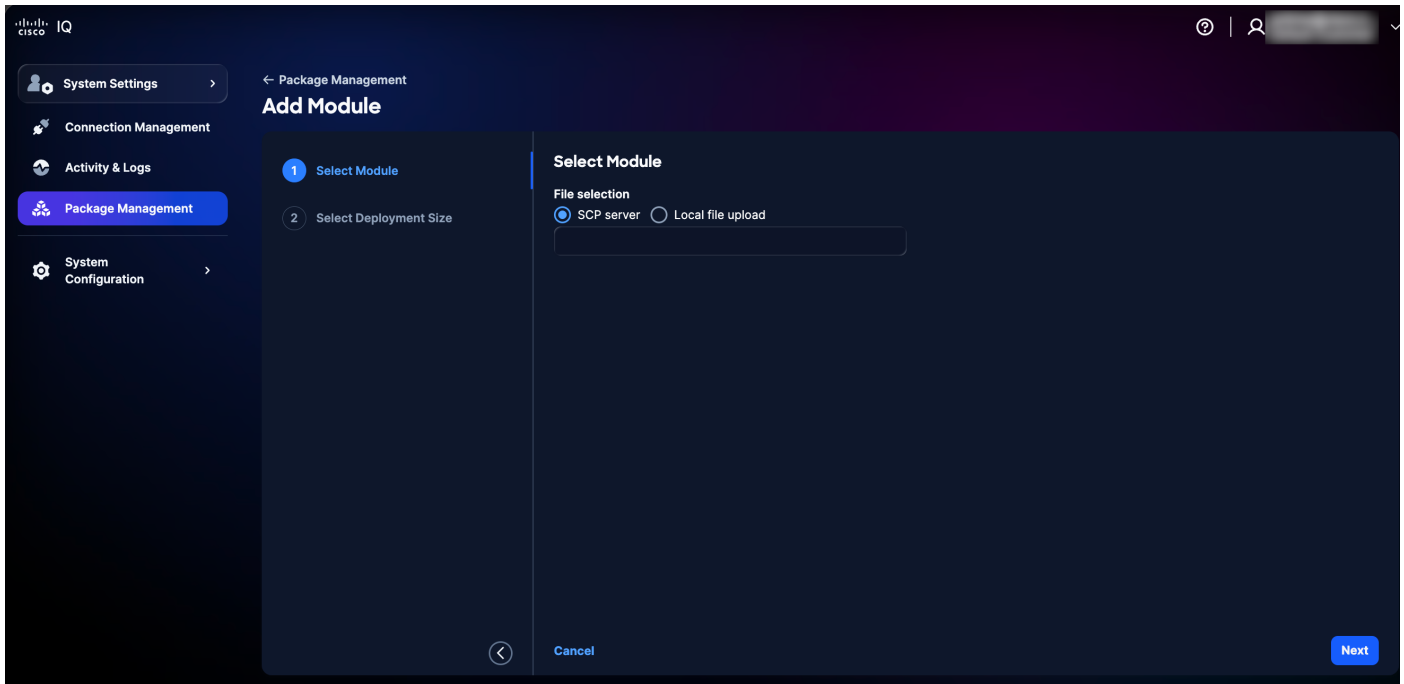
AI-Inferenzinfrastruktur herunterladen

4. Wählen Sie eine Systemversion aus der Dropdown-Liste aus.
5. Wählen Sie einen Buildtyp aus der Dropdown-Liste aus.
6. Klicken Sie auf Download (Herunterladen).
7. Navigieren Sie zu VA.



Paketverwaltung

8. Navigieren Sie zu Startseite > Systemeinstellungen > Paketverwaltung. Die Seite Paketverwaltung wird mit den folgenden Registerkarten angezeigt:
 - Module
 - Regeln
 - Ansprüche
9. Klicken Sie auf der Registerkarte Module auf Module hinzufügen.



Modul auswählen

10. Wählen Sie Ihre bevorzugte Dateiauswahl-Option:

- SCP-Server: Geben Sie den genauen Dateinamen des Installationspakets ein (empfohlen für große Dateien).
- Upload der lokalen Datei: Ziehen Sie die heruntergeladene Installationsdatei per Drag-and-Drop (wird aufgrund der Uploadzeit für Dateien mit einer Größe von 30 GB oder mehr nicht empfohlen). Anmerkung: Die lokale Datei-Upload-Methode hat einen Schwellenwert von 20 Minuten. Wenn der Uploadvorgang diese Dauer überschreitet, schlägt die Installation fehl. Die Verwendung eines SCP-Servers stellt die bevorzugte Methode für eine erfolgreiche und stabile Installation dar.

11. Klicken Sie auf Next (Weiter). Das System beginnt mit dem Hochladen der Datei.

12. Wählen Sie eine Bereitstellungsgröße (z. B. Klein, Mittel oder Groß).

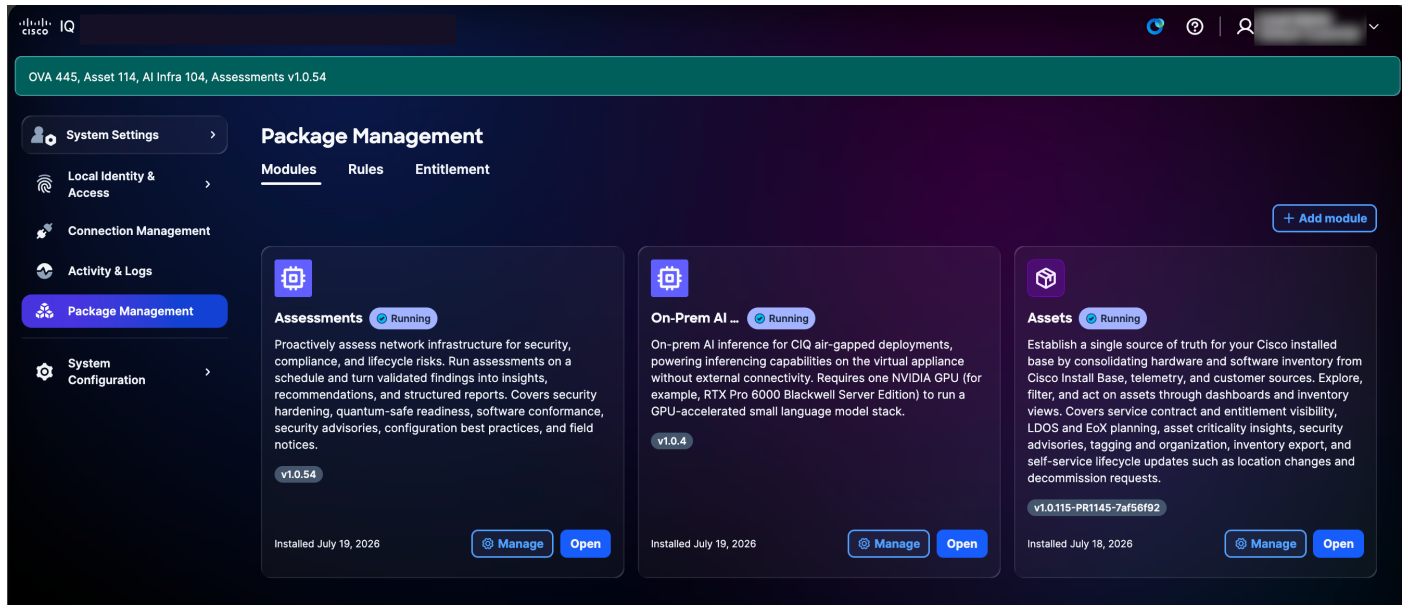
13. Klicken Sie auf Modul hinzufügen. Die Installation beginnt und dauert ca. 40-45 Minuten.

Nach Abschluss der Installation wird auf der Registerkarte Module (Module) im Paketmanagement die Infrastruktur für lokale KI-Inferenz angezeigt.

 Anmerkung: Pro GPU kann nur ein lokales KI-Inferenzinfrastrukturmodul ausgeführt werden. Das Modul verwendet ca. 90 % des GPU-VRAM. Es wird nicht unterstützt, eine zusätzliche Instanz auf derselben GPU zu installieren.

Management des standortbasierten KI-Inferenzinfrastrukturmoduls

Nach der Installation kann das On-Prem AI Inference Infrastructure-Modul über die Registerkarte Anwendungen im Paketmanagement verwaltet werden.



Bearbeiten der AI-Inferenzinfrastruktur

Um das Modul zu verwalten, klicken Sie neben dem Modul "On-Prem AI Inference Infrastructure" auf Manage (Verwalten). Weitere Informationen finden Sie unter [Module verwalten](#).

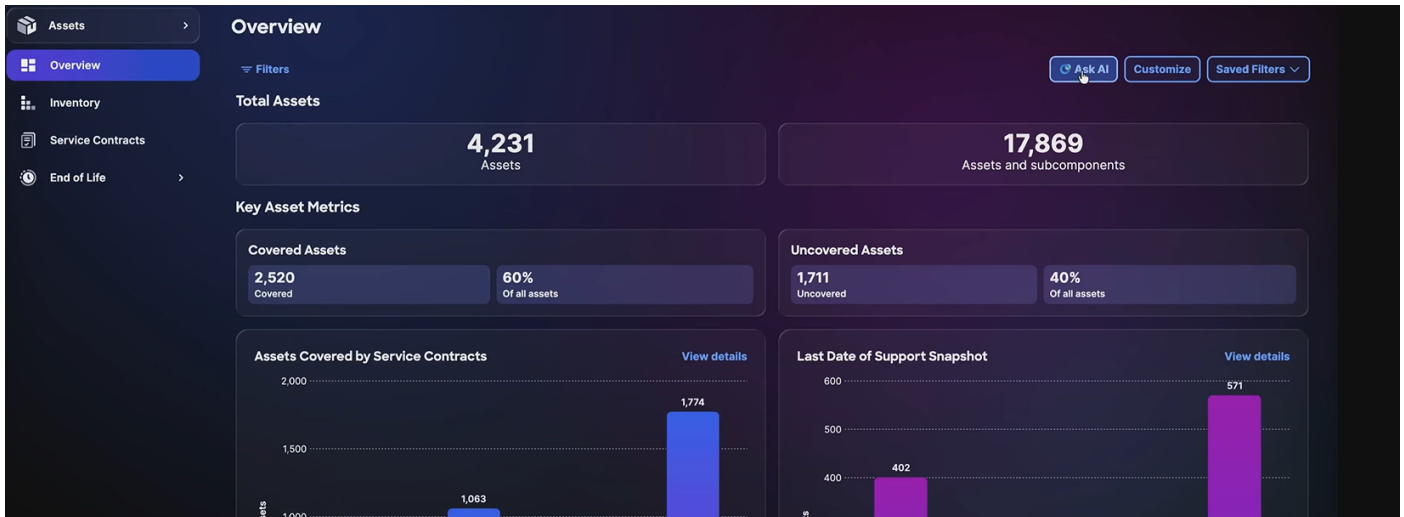
Verwenden von KI-basierten Funktionen

Nach der erfolgreichen Installation des On-Prem AI Inference Infrastructure-Moduls wird die Schaltfläche Ask AI (AI fragen) in der VA-Schnittstelle verfügbar.

Fragen Sie KI in Ressourcen

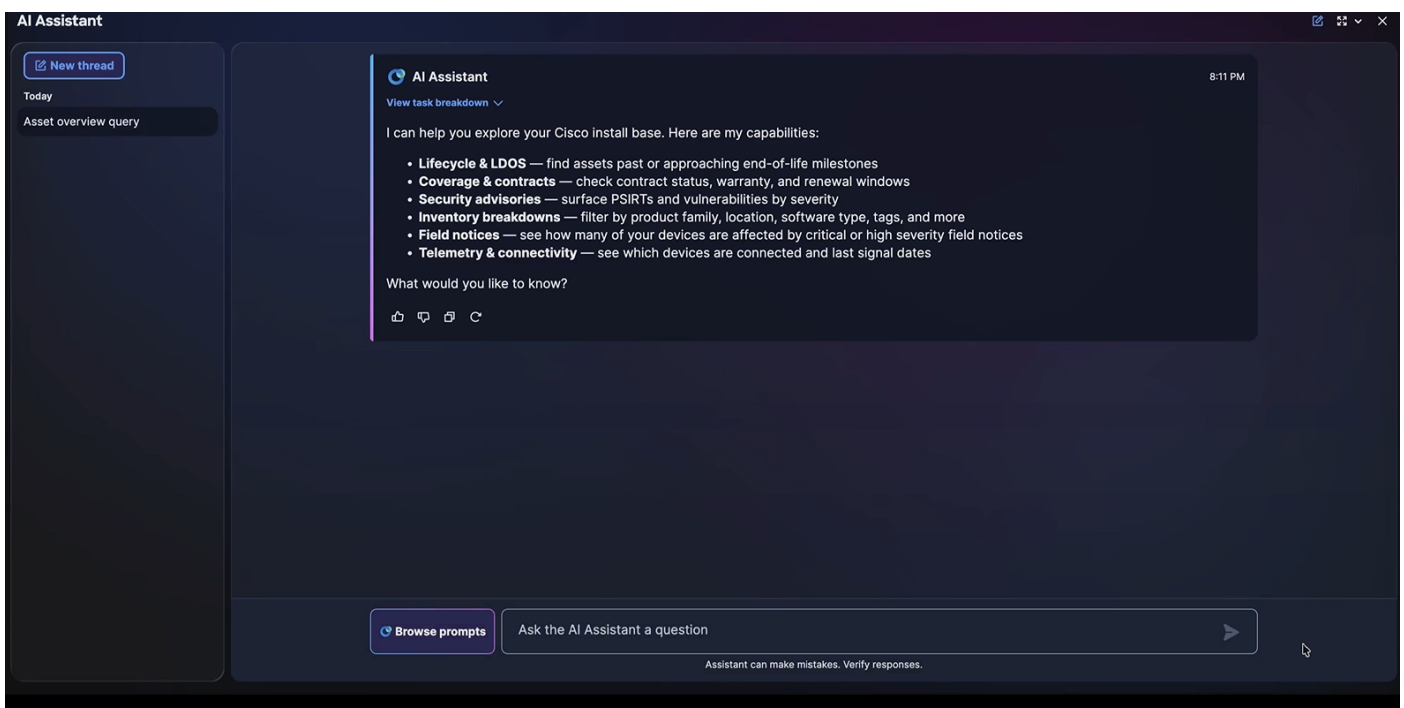
So verwenden Sie Ask AI in Ressourcen:

1. Wählen Sie das Menü Home (Startseite) > Assets (Ressourcen). Die Seite "Anlagen" wird angezeigt.



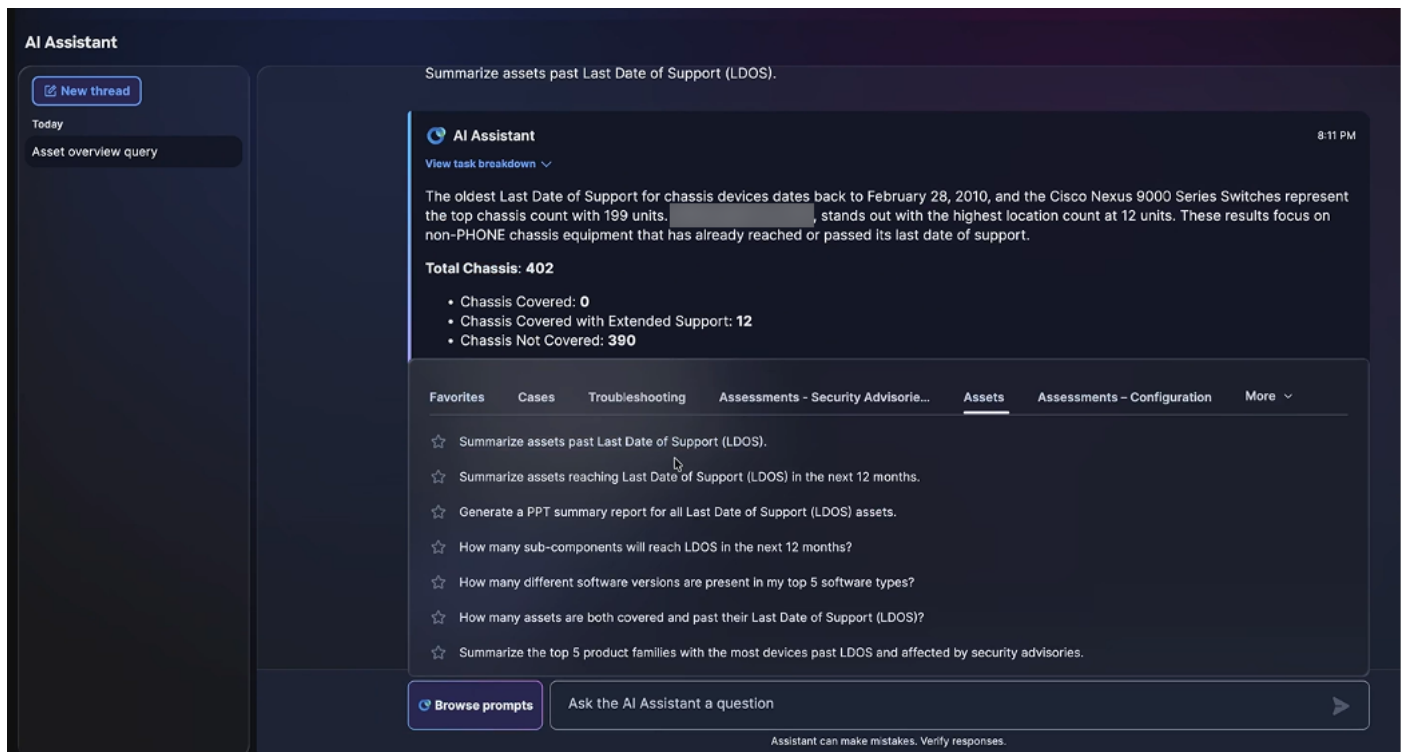
Seite "Ressourcen"

2. Klicken Sie auf AI fragen. Die standortbasierte KI-Inferenzinfrastruktur wird gestartet.



Aufforderungen durchsuchen

3. Klicken Sie entweder auf Aufforderungen durchsuchen, um verfügbare Aufforderungen anzuzeigen, oder geben Sie eine benutzerdefinierte Frage in das Feld Ask the AI Assistant a question (Fragen an den KI-Assistenten) ein.



Aufforderungen

4. Klicken Sie auf die gewünschte Eingabeaufforderung, oder drücken Sie die Eingabetaste.
Das standortbasierte SLM generiert eine Antwort.

AI-Analyse im Bestand

Das Modul der standortbasierten KI-Inferenz-Infrastruktur bietet eine automatisierte KI-gestützte Analyse im Abschnitt "Inventar". Die Analyseergebnisse werden automatisch angezeigt, sobald die Bestandsdaten eingegeben wurden.

So zeigen Sie die KI-Analyse im Bestand an:

1. Wählen Sie Home menu > Inventory. Die Seite "Bestand" wird angezeigt.

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	

Bestand

- Die KI-generierte Analyse anzeigen. Die Ergebnisse werden in der Inventaransicht angezeigt, sobald Daten verfügbar sind.



Anmerkung: Klicken Sie auf Vollständige Analyse, um Visualisierungen wie Diagramme, Dashboards und Diagramme anzuzeigen, die zusätzliche Einblicke bieten.

Allgemeine Funktionen für Module

In diesem Abschnitt werden die Kernfunktionen beschrieben, die von allen Modulen gemeinsam genutzt werden. Diese Funktionen sorgen für ein konsistentes Anwendererlebnis, optimieren die Systemleistung und straffen die administrativen Arbeitsabläufe

Datenanalyse

Das Bedienfeld Insights bietet eine KI-gestützte Analyse der Daten auf dieser Seite und liefert aussagekräftige Informationen zur Verbesserung der Sicherheit und des Zustands Ihrer Netzwerkumgebung.



Anmerkung: Das Analyse-Feature ist nur auf ausgewählten Seiten verfügbar.

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](#)

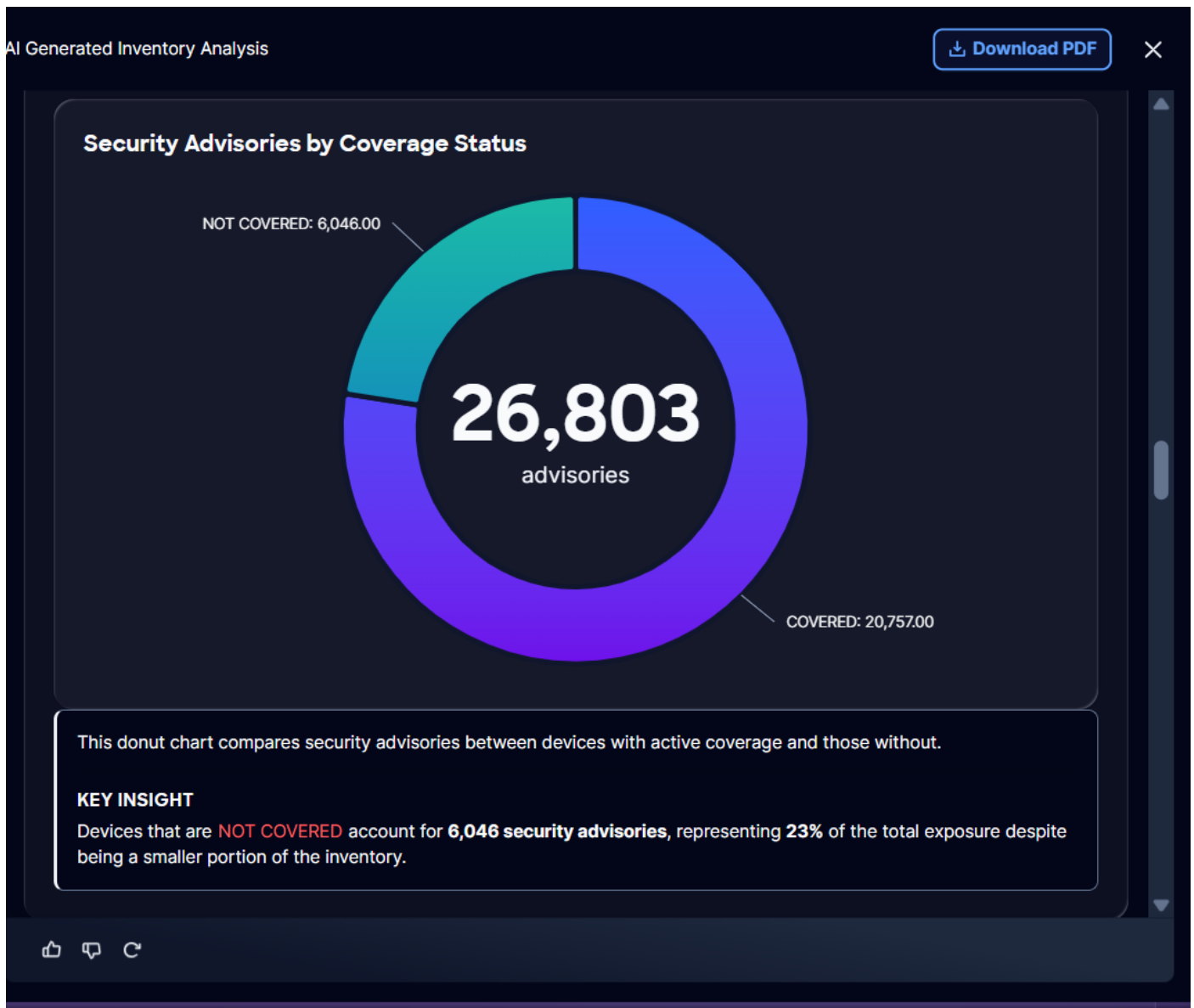
Full Analysis

Name	Product ID	Product Type	Serial Number	Next Milestone	Next Milestone Date	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

Einblicke-Panel

Folgende Optionen sind im Einblicke-Panel verfügbar:

- Klicken Sie auf das Symbol Erweitern, um den Bereich zu erweitern und zusätzliche Einblicke anzuzeigen.
- Klicken Sie auf das Symbol Daumen hoch oder Daumen runter, um Feedback zu den von der KI generierten Informationen abzugeben.
- Klicken Sie auf Vollständige Analyse, um zusätzliche Informationen, tiefere Analysen und Visualisierungen wie Diagramme, Dashboards und Diagramme anzuzeigen.



Vollständige Analyse

Die folgenden Optionen sind im Rahmen einer vollständigen Analyse verfügbar:

- Klicken Sie auf PDF herunterladen, um eine Offline-Kopie der Analyse für Ihre Unterlagen oder für die Zusammenarbeit zu speichern.

Exportieren von Informationen

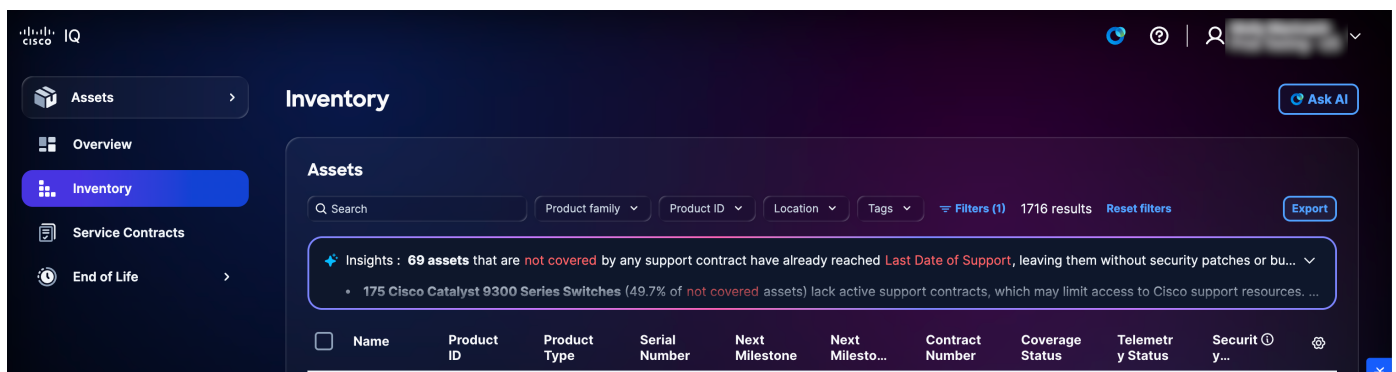
Mit der Exportfunktion können Sie benutzerdefinierte Ansichten für Ressourcen und Sicherheitsinformationen im XLS- oder CSV-Format exportieren.



Anmerkung: Die Exportfunktion ist nur für ausgewählte Seiten verfügbar.

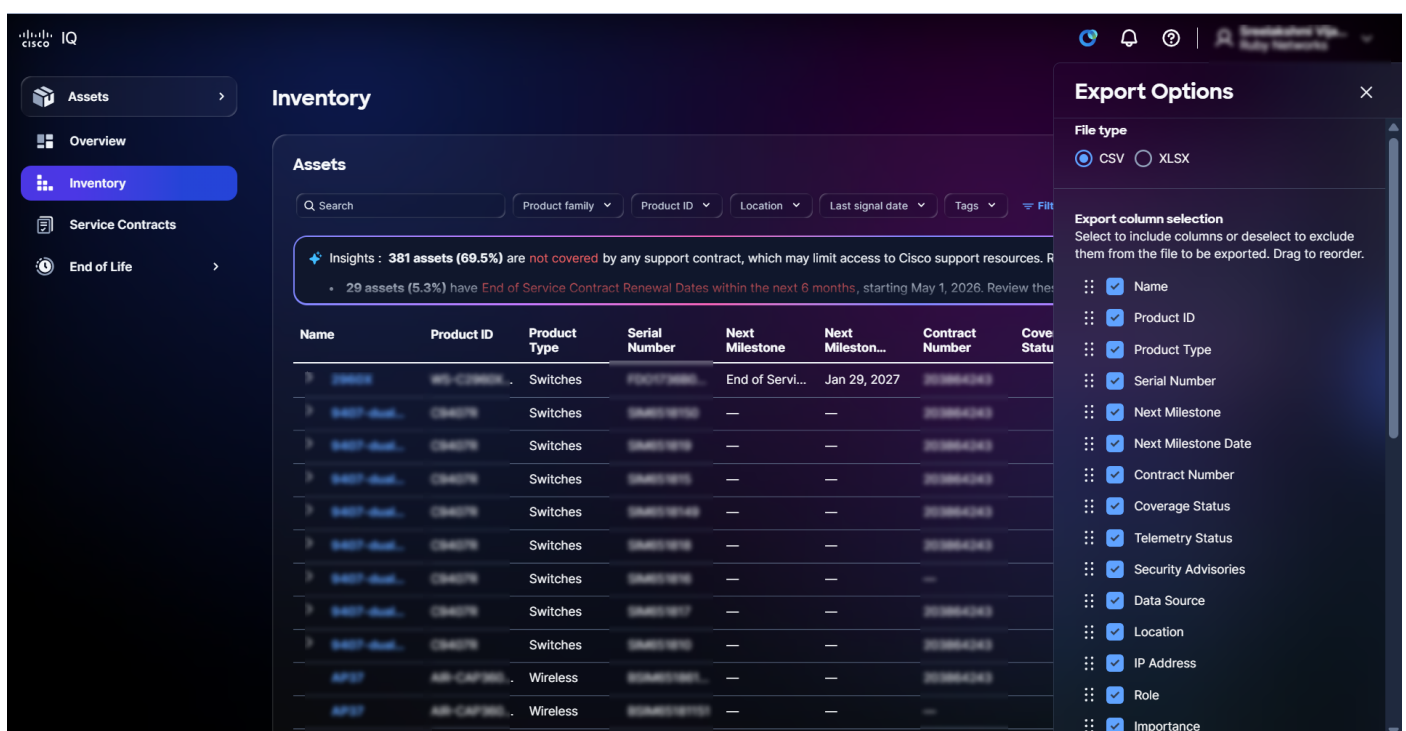
So exportieren Sie Informationen von einer Seite:

1. Navigieren Sie zur Seite.



Exportieren von Beständen im Modul "Ressourcen"

2. Klicken Sie auf Exportieren. Die Exportoptionen werden angezeigt.



Exportoptionen

3. Wählen Sie einen Dateityp aus.

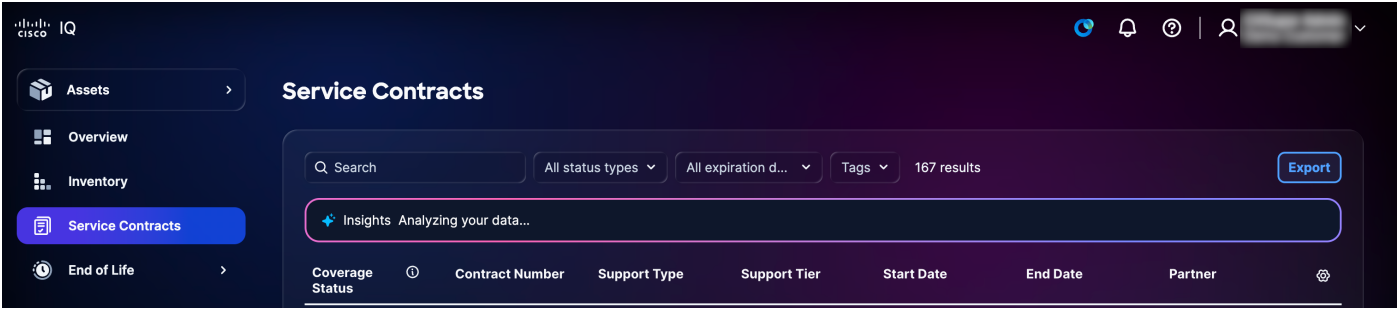
4. Aktivieren Sie das bzw. die Kontrollkästchen in der bzw. den gewünschten Spalten.

5. Klicken Sie auf Exportieren. Die Datei wird in den lokalen Downloadordner des Browsers

heruntergeladen.

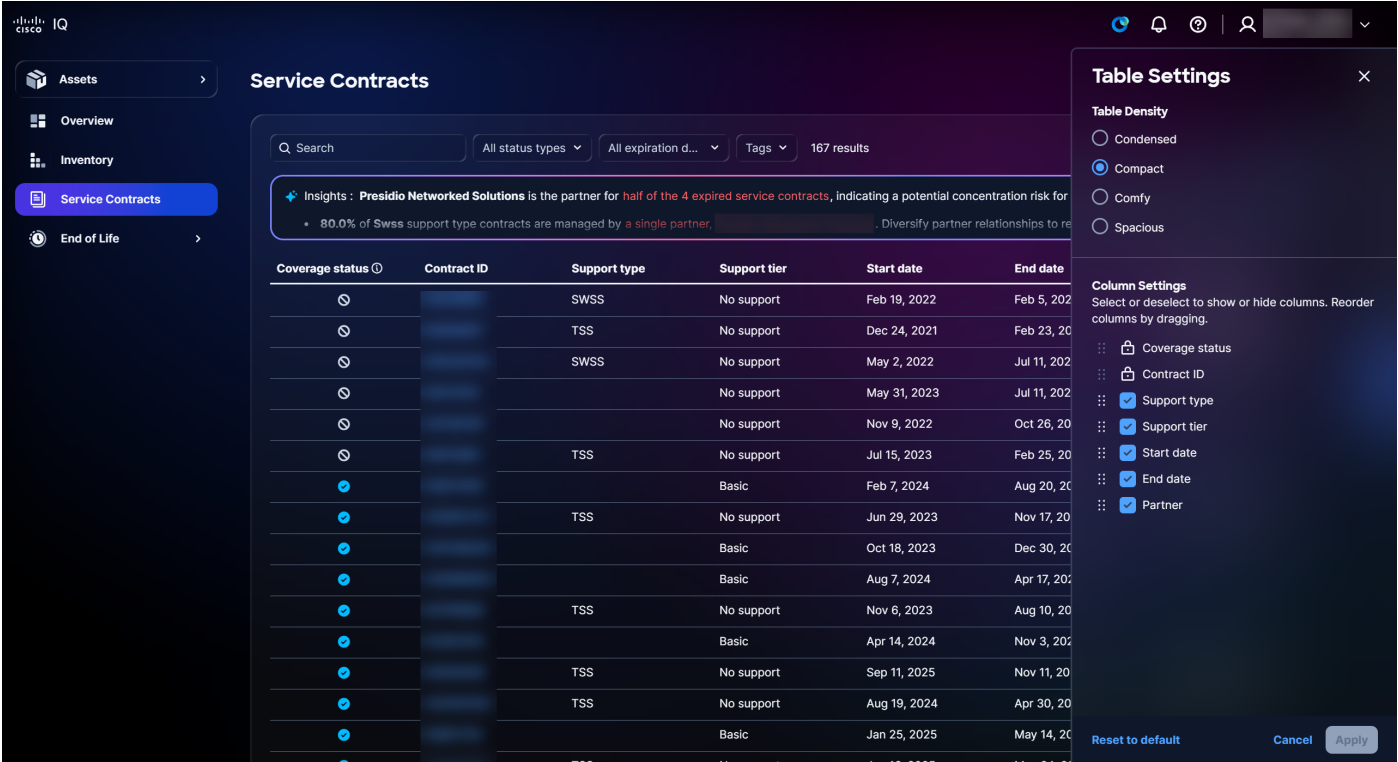
Tabelleneinstellungen

Sie können Tabelleneinstellungen konfigurieren, um benutzerdefinierte und verfeinerte Ansichten für verschiedene Modulfeatures zu erstellen.



Tabelleneinstellungen

Um die Spalten zu ändern, die auf ausgewählten Seiten angezeigt werden, klicken Sie auf das Symbol Tabelleneinstellungen. Die Tabelleneinstellungen werden angezeigt.



Optionen für Tabelleneinstellungen

Tabellenansicht ändern

So ändern Sie die Tabellenansicht:

1. Wählen Sie eine der folgenden Optionen für die Tabellendichte aus:

- Zusammengefasst: Minimiert visuelle Elemente und Abstände zur Anzeige weiterer Informationen
- Kompakt: Verringert Leerzeichen und verringert den Abstand zwischen den Elementen der Benutzeroberfläche
- Komfort: Nutzt mehr Leerraum und größeren Abstand zwischen den Elementen
- Geräumig: Betont eine große Zahl von Leerzeichen und größeren Benutzeroberflächenelementen

2. Klicken Sie auf Apply (Anwenden).

Hinzufügen und Entfernen von Spalten

So fügen Sie Spalten hinzu oder entfernen sie:

1. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen Spalteneinstellungen.

2. Klicken Sie auf Apply (Anwenden).



Anmerkung: Die Spalte Name kann nicht aus der Tabellenansicht entfernt werden.

Ändern der Spaltenreihenfolge

So ändern Sie die Reihenfolge der Spalten:

1. Ziehen Sie den Spaltennamen per Drag-and-Drop, um die Elemente in der gewünschten Reihenfolge anzuordnen.

2. Klicken Sie auf Apply (Anwenden).

Anpassen von Dashboards

Mit der Funktion "Benutzerdefiniertes Dashboard" können Sie Standard-Dashboards durch eine Reihe intuitiver Anpassungsoptionen personalisieren:

- Neuordnung von Dashboard-Widgets oder -Panels mithilfe der Drag-and-Drop-Funktion
- Entfernen Sie alle Komponenten, die für Ihren Workflow nicht relevant sind.
- Ihr persönliches Dashboard-Layout wird sicher in Ihrem Benutzerprofil gespeichert und automatisch auf alle Sitzungen und Geräte angewendet.
- Das ursprüngliche Dashboard-Layout mit einer einfachen Rücksetzoption wiederherstellen

So passen Sie ein Dashboard an:

1. Navigieren Sie zum Dashboard.



Anpassen

2. Klicken Sie auf Anpassen.



Dashboard bearbeiten

3. Ändern Sie das Dashboard wie gewünscht:

- Neu anordnen: Widgets per Drag-and-Drop in das gewünschte Layout verschieben
- Entfernen: Klicken Sie auf das Symbol Löschen, um ein Widget zu entfernen.
- Zurücksetzen: Klicken Sie auf Reset to default (Auf Standard zurücksetzen), um das Dashboard auf das ursprüngliche Layout zurückzusetzen.

4. Klicken Sie auf Speichern. Eine Meldung Gespeichertes Dashboard wird angezeigt.

Das Dashboard-Layout wird automatisch auf alle Sitzungen und Geräte angewendet.

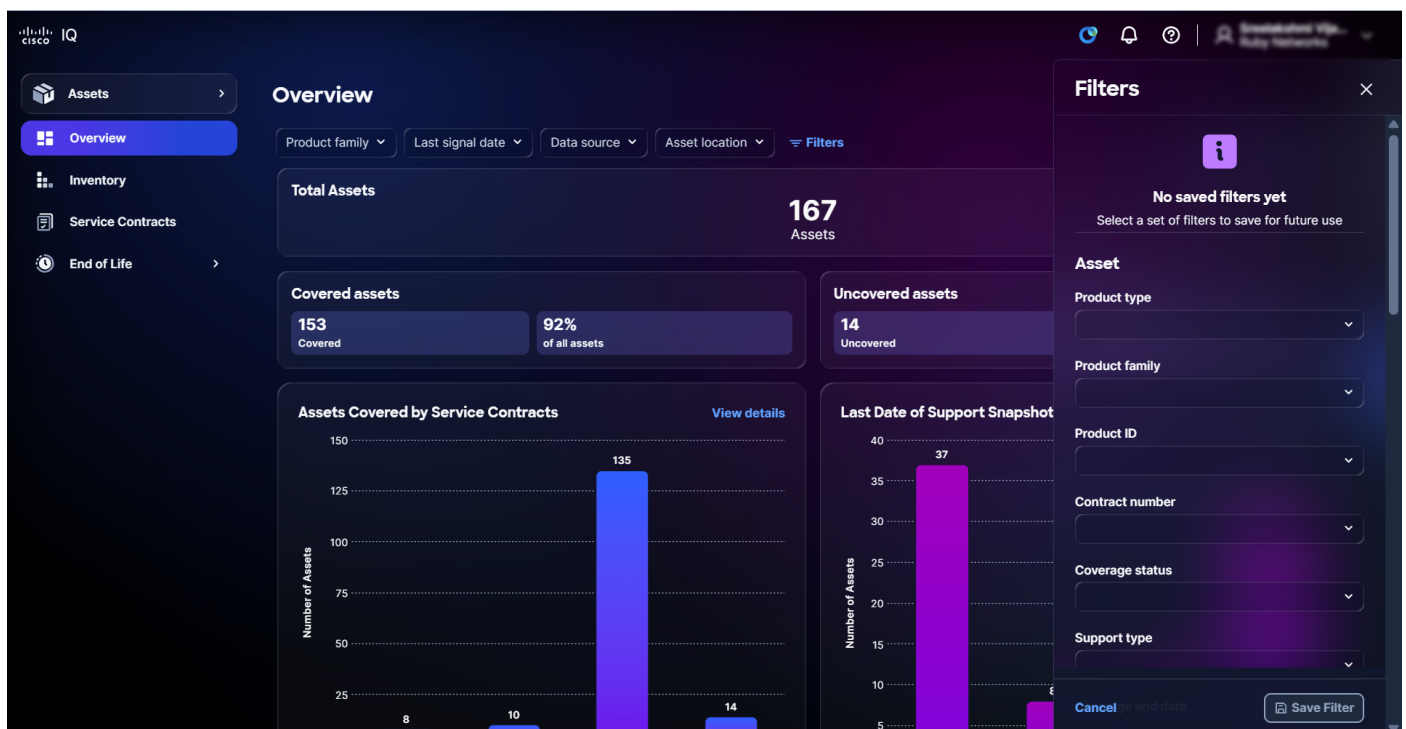
Anpassen von Filtern

Sie können benutzerdefinierte Filterkonfigurationen für jede Dashboard-Ansicht speichern, sodass Sie ganz einfach nach Bedarf zu Ihren bevorzugten Einstellungen zurückkehren können. Alle Filtereinstellungen werden auf sichere Weise für jeden Benutzer und jedes Konto gespeichert. Dadurch wird bei jedem Zugriff auf Cisco IQ eine personalisierte und konsistente Benutzerumgebung sichergestellt.

Erstellen eines Filters

So erstellen Sie einen benutzerdefinierten Filter:

1. Navigieren Sie zum Dashboard.
2. Klicken Sie auf Filter.



Filter

3. Wählen Sie die gewünschten Filter aus den Dropdown-Listen aus.
4. Klicken Sie auf Filter speichern. Das Fenster Gespeicherter Filter wird geöffnet.

Name saved Filter

Filter name *

Custom Filter |

Cancel

Save Filter

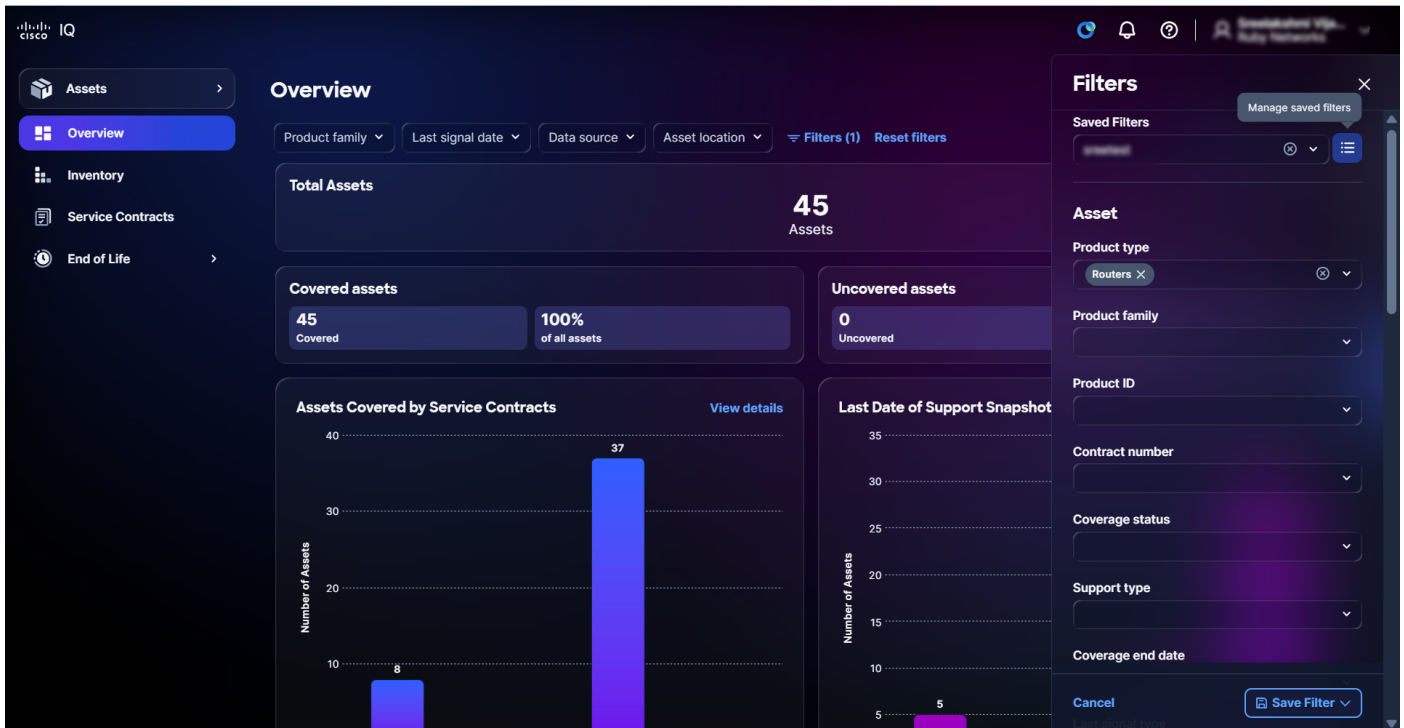
Filtername

5. Geben Sie einen Filternamen ein.
6. Klicken Sie zur Bestätigung auf Filter speichern.

Bearbeiten eines Filternamens

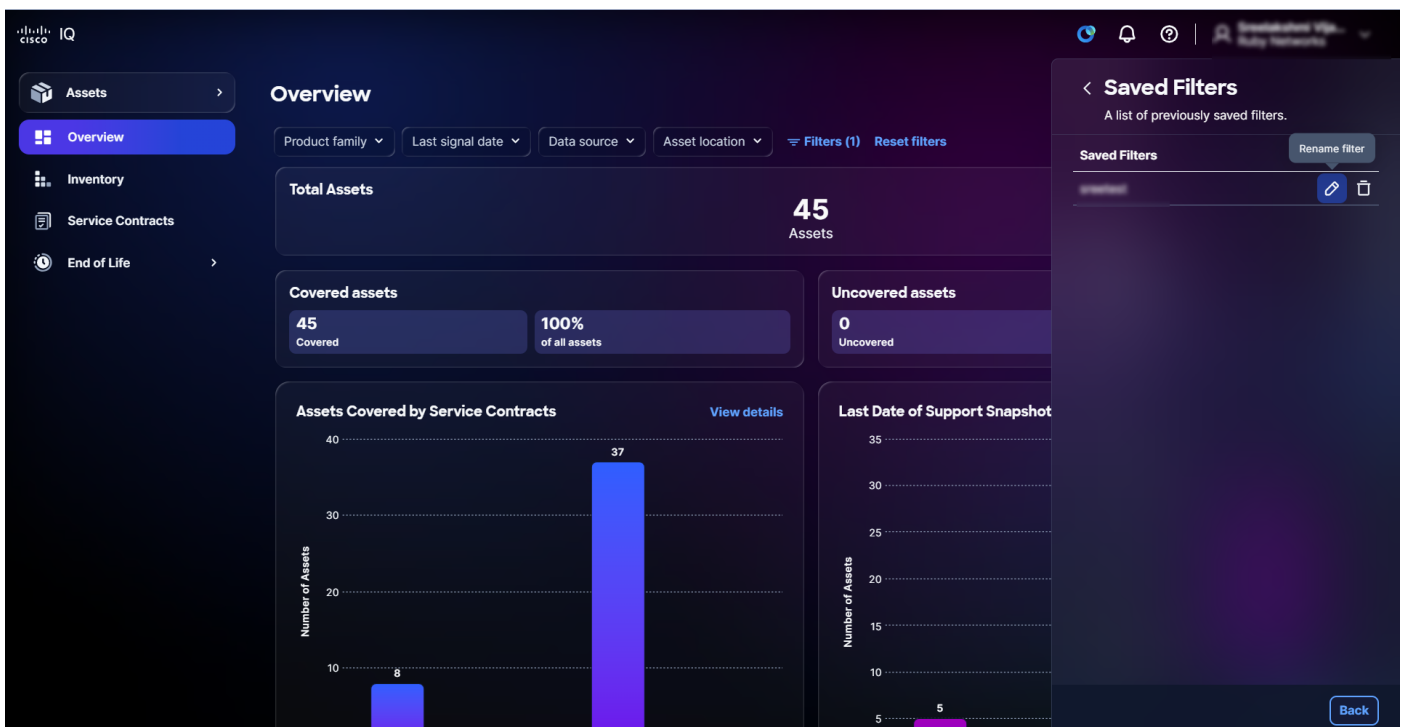
So bearbeiten Sie einen benutzerdefinierten Filter:

1. Klicken Sie auf Filter.



Gespeicherte Filter verwalten

2. Klicken Sie auf das Symbol Gespeicherte Filter verwalten.
3. Navigieren Sie zum Filter.



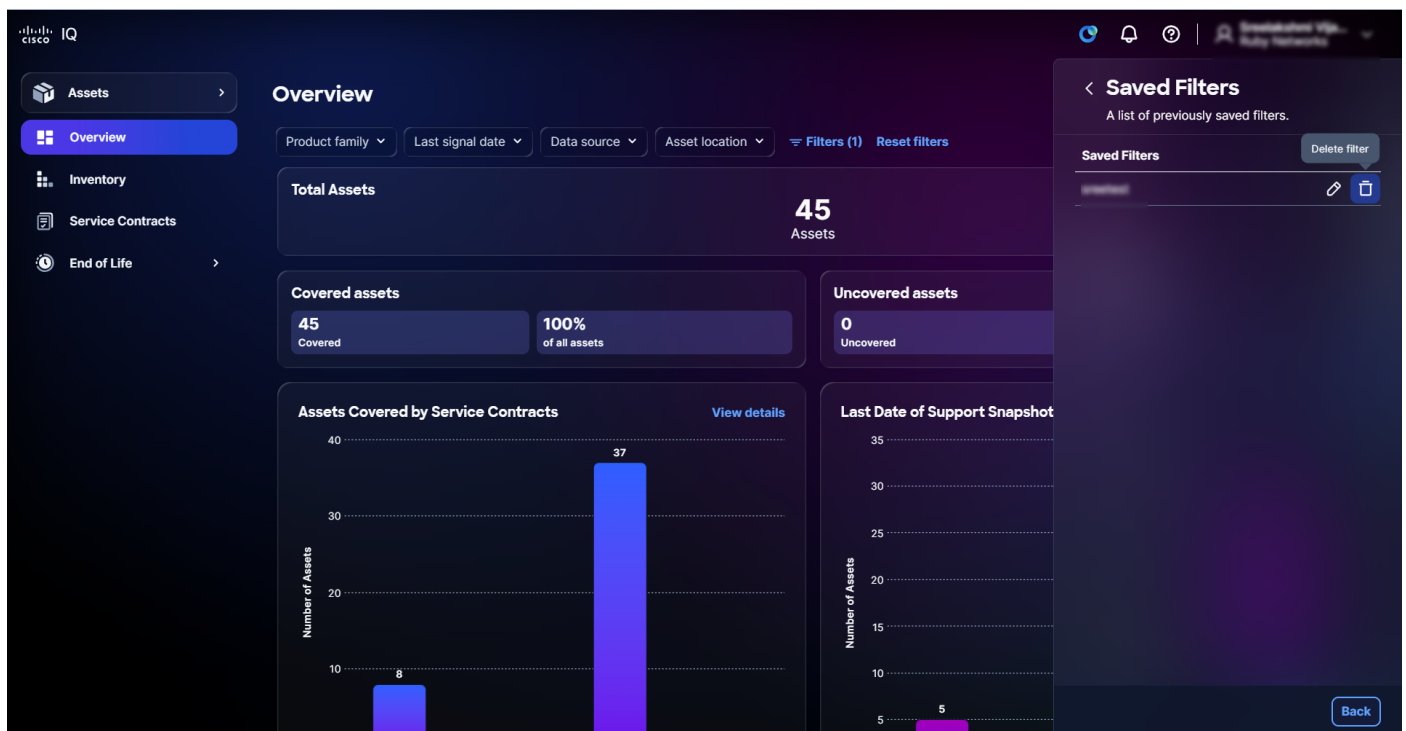
Filter bearbeiten

4. Klicken Sie auf das Symbol Bearbeiten. Das Fenster Name saved Filter wird geöffnet.
5. Bearbeiten Sie den Filternamen.
6. Klicken Sie zur Bestätigung auf Filter speichern.

Löschen eines Filters

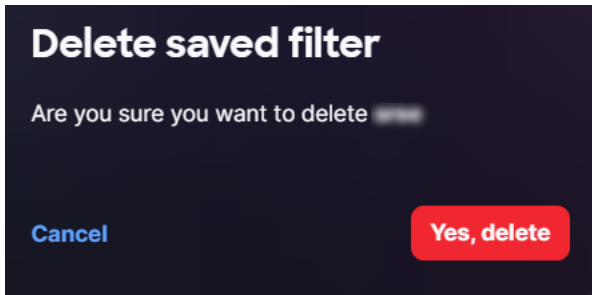
So löschen Sie einen benutzerdefinierten Filter:

1. Klicken Sie auf Filter.
2. Klicken Sie auf das Symbol Verwaltete gespeicherte Filter.
3. Navigieren Sie zum Filter.



Gespeicherten Filter löschen

4. Klicken Sie auf das Symbol Löschen. Das Fenster Gespeicherten Filter löschen wird geöffnet.



Löschen des gespeicherten Filters bestätigen

5. Klicken Sie zur Bestätigung auf Ja, löschen.

Ressourcen-Modul

Das Assets-Modul bietet umfassende Transparenz- und Managementfunktionen für Cisco Ressourcen und dient als Grundlage für den Cisco IQ. Es bietet eine zentralisierte Liste aller Geräte in einer Organisation. Durch das Sammeln von Informationen aus mehreren Quellen wird der Gerätebestand als einheitliche Datenquelle genutzt. Die Pflege einer vollständigen und präzisen Ressourcenliste ist von entscheidender Bedeutung, da sich andere Module von Cisco IQ - wie z. B. das Assessments-Modul - bei der Beurteilung des Zustands und der Sicherheit Ihrer Geräte auf diese Daten verlassen.

Kernkonzepte

Das Modul "Ressourcen" basiert auf den folgenden Kernkonzepten:

- **Ressource:** Alle physischen Geräte, Hardware oder Software, die im Rahmen der Servicebereitstellung von Cisco inventarisiert und verwaltet werden, mit detaillierter Nachverfolgung von Identität, Funktion, Serviceabdeckung und Lebenszyklus
- **Vertragsbezogene Ressourcen:** Ressourcen, die direkt aus verknüpften Servicevertragsdaten und nicht über Telemetrie in den Bestand aufgenommen werden. Cisco IQ bezieht die folgenden Gerätetypen aus Vertragsdaten ein: Chassis, Module, Netzteile und Lüfter. Diese Ressourcen sind im Bestand sichtbar, selbst wenn keine Telemetrierbindung besteht.
- **Support-Ende (LDOS):** Verfolgung von End-of-Life- und End-of-Support-Meilensteinen für Cisco Produkte
- **Serviceabdeckung:** Aktive Support-Verträge, Garantien und Berechtigungsstufen für eine bestimmte Hardware oder Software

- Ressourcen-Tag: Benutzerdefiniertes Label, das einer Ressource für Organisations-, Filter- und betriebliche Workflows zugewiesen wird
- Gerätesignal: bezieht sich auf die letzte Beobachtung eines Geräts (anhand seiner Seriennummer) durch Cisco, basierend auf Gerätetelemetrie, Supportfällen und Vertragsverlängerungen. Die Telemetriedaten der Ressourcen werden über eine mehrschichtige Daten-Pipeline aufgenommen und angereichert.

Modul Zugriff auf Ressourcen

Um auf die Bestandsverwaltungsfunktionen in Cisco IQ zuzugreifen, wählen Sie im Menü Home (Startseite) > Assets (Ressourcen) aus, oder klicken Sie im Abschnitt Application (Anwendung) der Startseite > Launchpad-Registerkarte auf Assets (Ressourcen). Die Seite Übersicht wird angezeigt.

Übersicht über Ressourcen

Auf der Seite Overview (Übersicht) wird ein Dashboard angezeigt, mit dem Sie den Status und Status von Geräten schnell bewerten können.

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

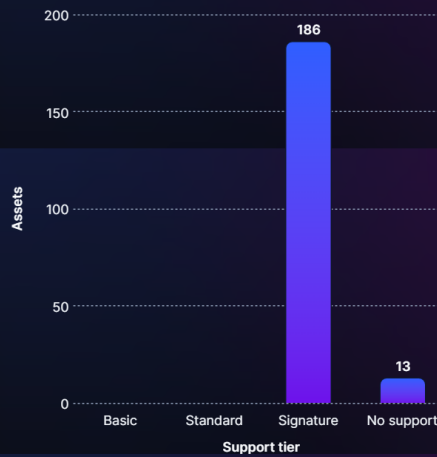
13

Uncovered

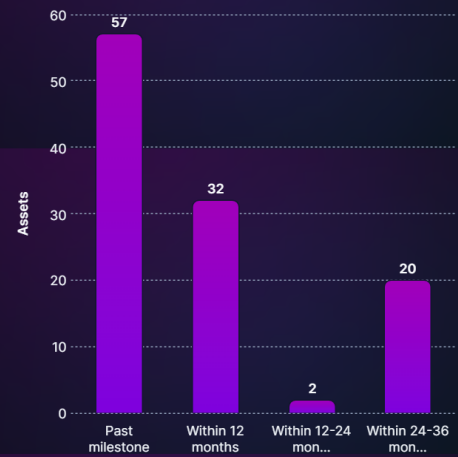
7%

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

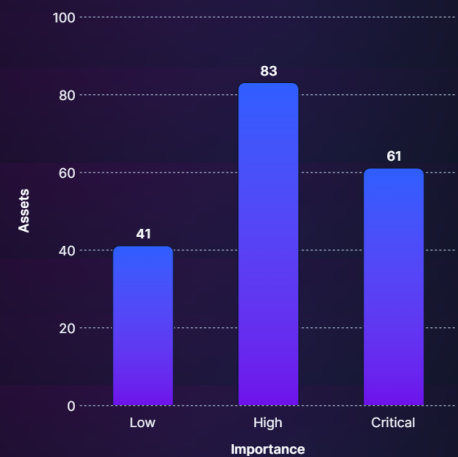
Assets With Critical or High Security Advisories [View details](#)



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.

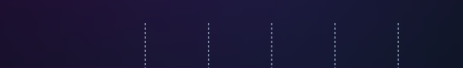


Asset Breakdown

Top 5 Product Families [View details](#)



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



Übersicht über Ressourcen

Das Dashboard zeigt die folgenden Informationen an:

- **Aktiva insgesamt:** Die Gesamtzahl der Ressourcen des Cisco IQ-Kontos
- **Wichtige Ressourcenmetriken:** Zusätzliche wichtige Kennzahlen wie Telemetriestatus, wichtige Sicherheitsempfehlungen und LDOS-Informationen
- **Abgedeckte Aktiva:** Gesamtzahl und Prozentsatz der durch Serviceverträge abgedeckten Ressourcen
- **Nicht abgedeckte Ressourcen:** Gesamtzahl und Prozentsatz der nicht durch Serviceverträge abgedeckten Ressourcen
- **Von Serviceverträgen abgedeckte Ressourcen:** Aufschlüsselung der Anzahl der von Serviceverträgen abgedeckten Ressourcen (Hardware oder Software), kategorisiert nach Berechtigungsstufe
- **Letztes Datum für Support-Snapshot:** Eine Aufschlüsselung der Anzahl an Ressourcen, die über LDOS hinausgehen oder LDOS erreichen
- **Ressourcen mit aktivierter Telemetrie:** Gesamtzahl und Prozentsatz der Ressourcen mit aktivierter Telemetrie
- **Ressourcen ohne aktivierte Telemetrie:** Gesamtzahl und Prozentsatz der Ressourcen ohne aktivierte Telemetrie
- **Ressourcen mit kritischen oder hohen Sicherheitsempfehlungen:** Prozentualer Anteil der Gesamtr Ressourcen mit aktivierter Telemetrie, die kritische oder hohe Sicherheitsempfehlungen enthalten
- **Vermögenswerte nach Wichtigkeit:** Eine Aufteilung der einem Gerät zugewiesenen Priorität im Vergleich zu anderen Geräten im Netzwerk.
- **Aufschlüsselung der Ressourcen:** Detaillierte Anzeige von Anlagendaten, z. B. Produktfamilien, Installationsstandorte, Softwareversionen und Ressourcenrollen

Filtern von Ansichten für Ressourcen

Sie können die Dashboard-Ansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen oder auf Filter klicken und eine Option aus der Liste der verfügbaren Filter auswählen.



Anmerkung: Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet. Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung.

Anzeigen von Details zu Ressourcen

Wenn Sie auf Details anzeigen klicken, wird die Seite zur Seite Inventar umgeleitet. Weitere Informationen finden Sie unter [Bestand](#).

Einblicke in kritische Ressourcen

Cisco IQ beinhaltet Asset Criticality Insights, eine neue Funktion im Assets-Modul, die die funktionale Rolle und die geschäftliche Bedeutung von Netzwerkgeräten vorhersagt. Durch die Analyse von Gerätekonfigurationen und aktivierten Funktionen unterstützen Asset Criticality Insights Sie dabei, die Ressourcen mit den größten Auswirkungen auf Ihr Netzwerk zu identifizieren. So können Sie sie priorisieren, um Sicherheitskorrekturen, Software-Upgrades, EOL-Planung (End-of-Life) und Abdeckungsentscheidungen zu treffen.



Anmerkung: Ressourcen-Criticality-Informationen sind nur für Ressourcen mit Standard- oder Signaturstufen verfügbar, die über aktive Telemetrieverbindungen verfügen. Stellen Sie sicher, dass Ihre Ressourcen die Konfigurationsanforderungen erfüllen, um diese Informationen im Dashboard anzugeben.

Erkenntnisse zu Asset Criticality sind in der Ressourcen-App in den folgenden Bereichen verfügbar:

- Übersicht über Ressourcen: Filtern und Anzeigen von Zusammenfassungen nach Asset Criticality Insights-Attributen
- Bestand an Ressourcen: Anzeigen, Suchen, Filtern und Sortieren von Geräten nach Rolle und Bedeutung
- Ressourcendetails: Rolle und Bedeutung für einzelne Geräte anzeigen, mit informativen QuickInfos zu jedem Wert

Überschreiben von Rollen- und Wichtigkeitsklassifizierungen

Der Cisco IQ prognostiziert automatisch die Rolle und die Bedeutung der einzelnen Ressourcen anhand von Telemetriedaten. Account-Administratoren können diese Klassifizierungen manuell korrigieren, wenn die automatisierte Prognose die Funktion oder Wichtigkeit der Ressource im

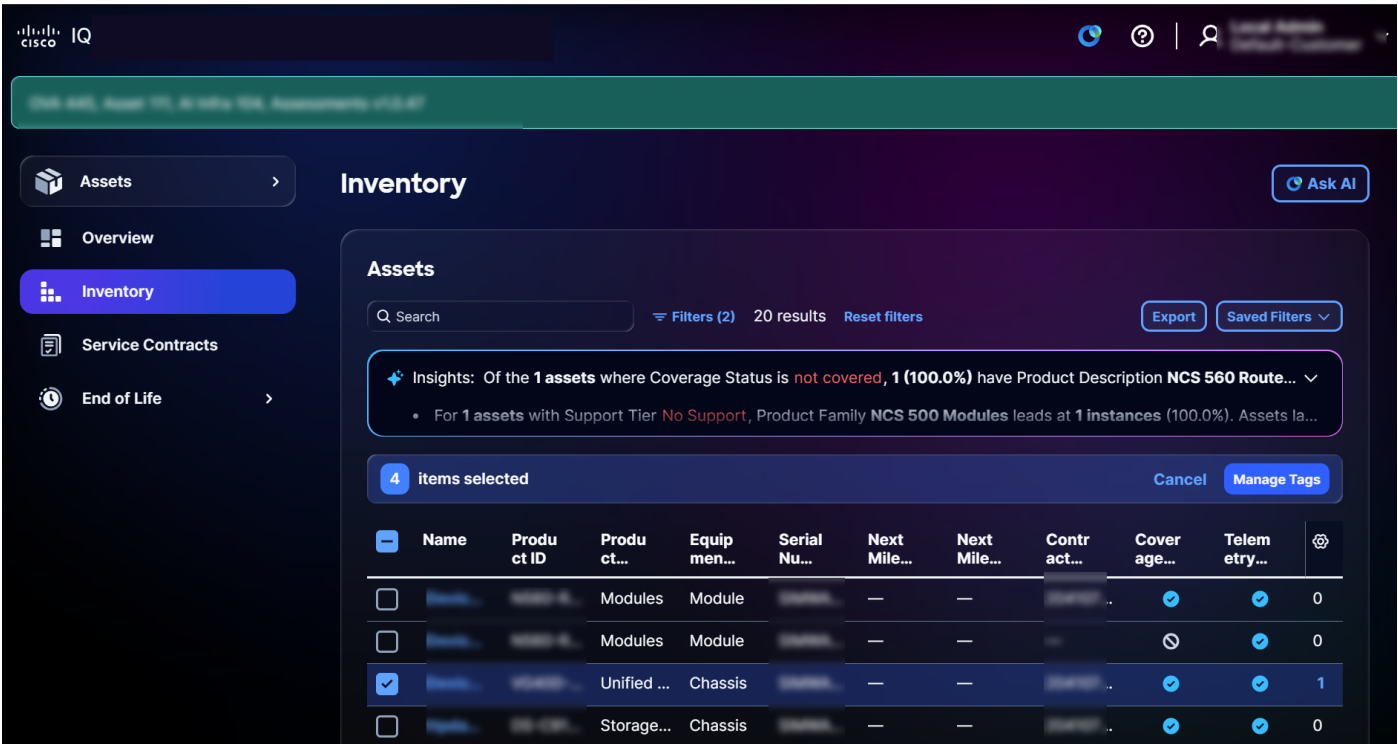
Netzwerk nicht genau widerspiegelt.

 Anmerkung: Außerkraftsetzungssteuerelemente stehen nur Kontoadministratoren zur Verfügung. Die Werte für Rolle und Wichtigkeit sind für alle anderen Benutzerrollen schreibgeschützt.

Klassifizierungen aus der Inventartabelle überschreiben

So überschreiben Sie die Rolle oder die Bedeutung für eine oder mehrere Ressourcen:

- 1. Navigieren Sie zu Anlagen > Lager.
- 2. Aktivieren Sie das Kontrollkästchen der gewünschten Zeile mit der Ressource. Um mehrere Ressourcen gleichzeitig zu aktualisieren, aktivieren Sie mehrere Kontrollkästchen.



Rolle und Bedeutung

- 3. Wählen Sie in der Spalte Rolle oder Wichtigkeit den richtigen Wert aus der Dropdown-Liste für die Zeile Ressource aus.
- 4. Klicken Sie auf Apply, um die Außerkraftsetzung zu bestätigen.

Anlagen mit manuell überschriebenen Werten zeigen einen visuellen Indikator in der Spalte Rolle

oder Wichtigkeit an.

 Anmerkung: Um eine zuvor konfigurierte Überschreibung zu entfernen und zur automatisierten Vorhersage zurückzukehren, wählen Sie in der Dropdown-Liste Rolle oder Wichtigkeit die Option Bindestrich (—) aus.

Klassifizierungen aus Ressourcendetails überschreiben

So überschreiben Sie die Rolle oder die Bedeutung in der Ansicht "Asset-Details":

1. Navigieren Sie zu Anlagen > Bestand, und klicken Sie auf eine Anlage.
2. Suchen Sie im Bereich mit den Ressourcendetails die Felder Rolle und Wichtigkeit.
3. Klicken Sie auf das Dropdown-Menü für das Feld, das Sie aktualisieren möchten, und wählen Sie den korrekten Wert aus.
4. Klicken Sie zur Bestätigung auf Apply.

In der Detailansicht einer Ressource werden auch die Telemetrieattribute aufgeführt, die der ursprünglichen automatisierten Prognose zugrunde lagen. So kann leichter ermittelt werden, ob eine Außerkraftsetzung angemessen ist.

Anzeigen des Prüfpfads für Außerkraftsetzung

Alle Überschreibungen auf Rolle und Bedeutung werden in einem Prüfpfad auf Account-Ebene erfasst. So greifen Sie auf den Prüfpfad zu:

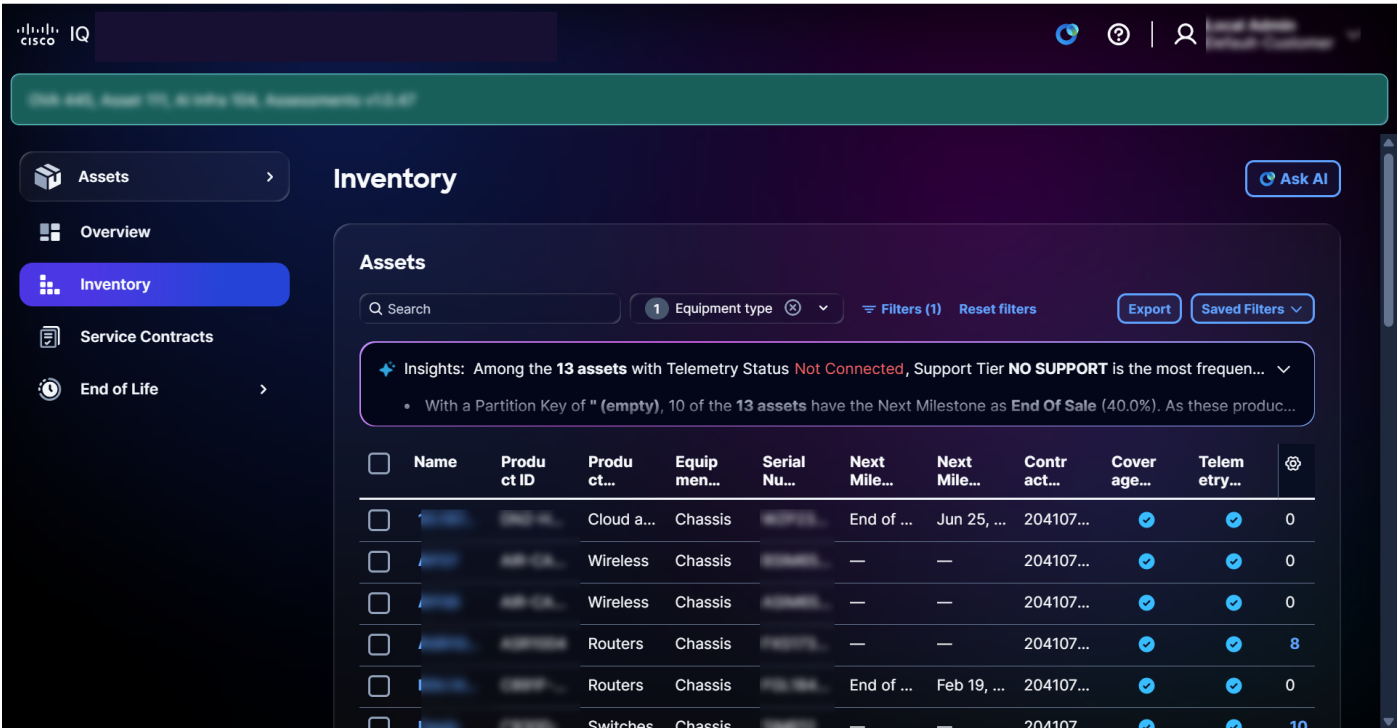
1. Wählen Sie Home > System Settings > Activity & Logs (Startseite > Systemeinstellungen > Aktivität und Protokolle).
2. Wählen Sie Filter > Aktionstyp > überschreiben, um nur überschreibende Ereignisse anzuzeigen.

Der Prüfpfad zeigt den Namen der Ressource, den vorherigen und den neuen Wert, den Benutzer, der die Änderung vorgenommen hat, sowie Datum und Uhrzeit der Änderung an. Der Prüfpfad kann mit der Option Exportieren exportiert werden.

 Anmerkung: Der Prüfpfad kann nach Datumsbereich, Benutzer und Ressourcenname gefiltert werden.

Bestand

Die Seite "Inventory" (Bestand) enthält eine Liste aller Cisco Ressourcen des Cisco IQ-Kontos.



Bestand

Ansichten für Ressourcenbestand durchsuchen und filtern

Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen oder auf Filter klicken und eine Option aus der Liste der verfügbaren Filter auswählen. Sie können auch nach Ressourcen suchen, indem Sie den Namen der Ressource in das Feld Suchen eingeben.

 Anmerkung:

- Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet.
- Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung.

Bestandsanalyse

Im Bereich Einblicke auf der Seite Inventar wird eine KI-gestützte Analyse angezeigt, die eine Zusammenfassung der Ressourcen mit Schwerpunkt auf Support-Abdeckung, Konnektivität und Meilensteinen liefert. Klicken Sie auf Vollständige Analyse, um Visualisierungen wie Diagramme, Dashboards und Diagramme anzuzeigen, die zusätzliche Einblicke bieten. Weitere Informationen finden Sie unter [Analysieren von Daten](#) in allgemeinen Modulfunktionen.

Exportieren des Bestands

Klicken Sie auf Exportieren, um eine gefilterte Inventarliste im XLS- oder CSV-Format zu speichern. Weitere Informationen finden Sie unter [Exportieren von Informationen](#) unter Allgemeine Modulfunktionen.

Ressourcendetails anzeigen

Klicken Sie auf eine Ressource, um Details anzuzeigen. Die Detailansicht einer Ressource wird mit den folgenden Registerkarten angezeigt:

- Details: Zeigt Ressourcendetails an, z. B. Produkt-, Signal-, Identitäts-, Standort-, Garantie- und Abdeckungsinformationen.

Assets

Overview

Inventory

Service Contracts

End of Life

← Inventory

10.197.236.131

Ask AI

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

Ressourcendetails

- **Produktwarnungen:** Zeigt Produktwarnungen wie Sicherheitsempfehlungen und

Problemhinweise an.

- Hardware: Detaillierte Zeitplanansicht für das EOL der Hardware (z. B. End-of-Sale, Last Ship und Last Date of Support)
- Software: Detaillierte Zeitplanansicht für den EOL der Software

Ressourcen-Tags

Asset-Tags sind benutzerdefinierte Labels, die Sie Inventarressourcen im Cisco IQ zuweisen. Ein Tag ist ein Schlüssel-Wert-Paar, das Sie definieren, z. B. Environment:Prod oder Label:Campus. Sie können einzelnen oder vielen Ressourcen gleichzeitig Tags zuweisen, und Sie können Ihren Bestand nach Tags filtern, um die für Sie wichtigen Ressourcen schnell zu finden.



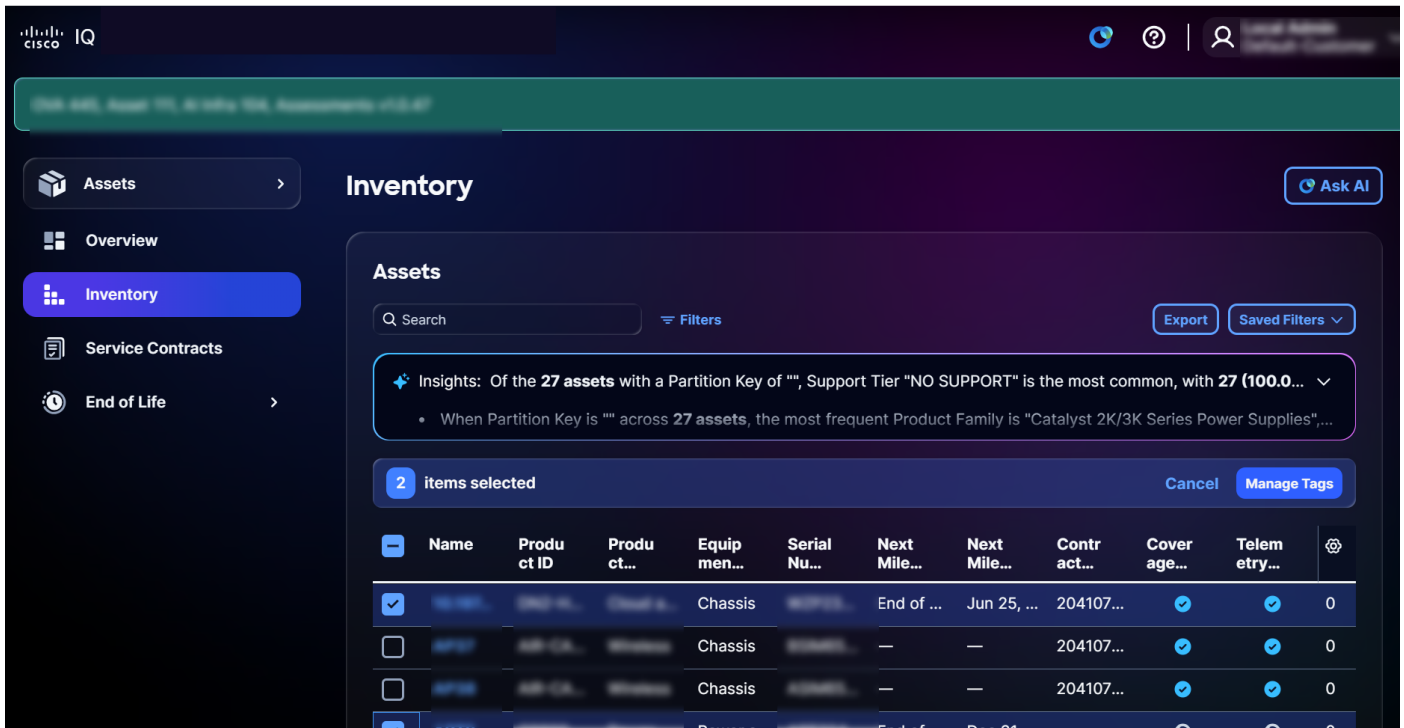
Anmerkung: Nachdem ein Tag von einem Kontoadministrator erstellt wurde, können Benutzer einem Asset einen Tag zuweisen.

Tags zuweisen

Durch das Zuweisen von Tags zu ausgewählten Ressourcen in der Inventaransicht können Ressourcen organisiert und kategorisiert werden, um eine bessere Filterung, Berichterstellung und Verwaltung zu ermöglichen.

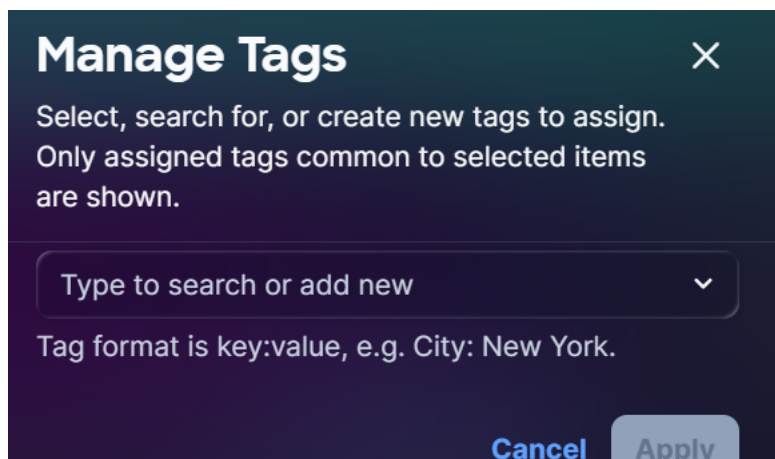
So ordnen Sie einer Anlage ein Tag zu:

1. Navigieren Sie zu Anlagen > Lager.



Tagging von Ressourcen

2. Aktivieren Sie die Kontrollkästchen der gewünschten Ressourcen.
3. Klicken Sie auf Tags verwalten. Das Fenster Tags verwalten wird geöffnet.



Tags zuweisen

4. Geben Sie im Textfeld den Tag-Namen ein, oder wählen Sie ihn aus den vorhandenen Optionen aus, und drücken Sie die Eingabetaste.

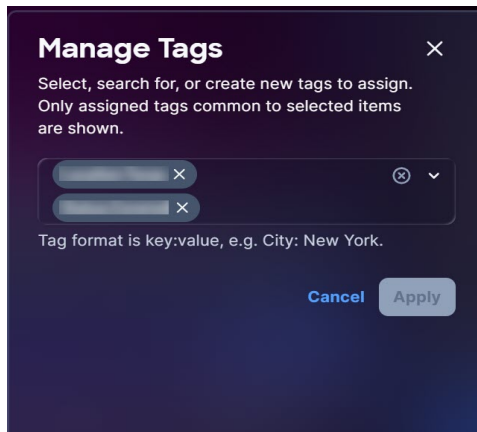
 Anmerkung: Tags haben das Format key:value (beispielsweise City:NYC).

5. Klicken Sie auf Apply (Anwenden).

Entfernen von Asset-Tags

So entfernen Sie ein Tag aus einer oder mehreren Ressourcen:

1. Navigieren Sie zu Anlagen > Lager.
2. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Ressourcen.
3. Klicken Sie auf Tags verwalten. Das Fenster Tags verwalten wird geöffnet.



Tags entfernen

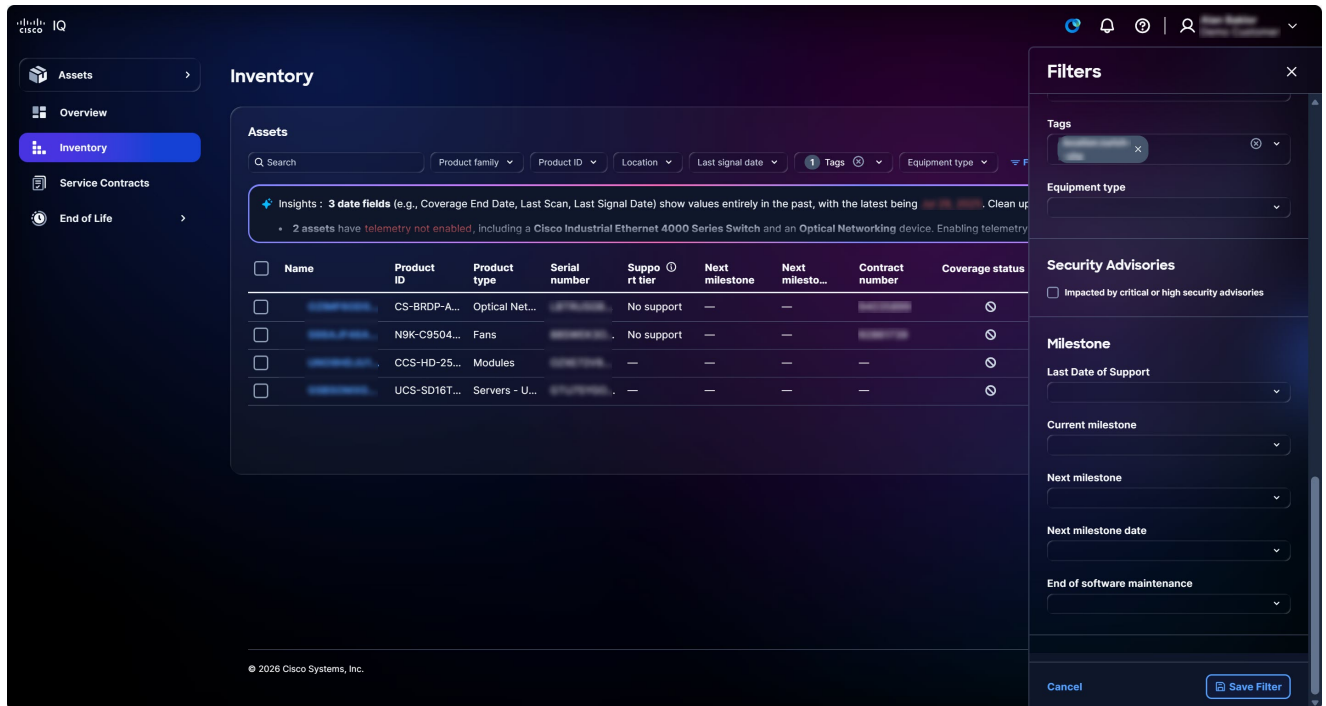
4. Klicken Sie auf das X für ein beliebiges Tag, um es aus der Auswahl zu entfernen.
5. Klicken Sie auf Apply (Anwenden).

Verwenden von Asset-Tags als Filter

Nachdem Sie ein Tag erstellt haben, können Sie das Tag als Filter verwenden.

So verwenden Sie ein Tag als Filter:

1. Navigieren Sie zur Seite "Bestand".
2. Klicken Sie auf Filter. Das Fenster Filter wird geöffnet.

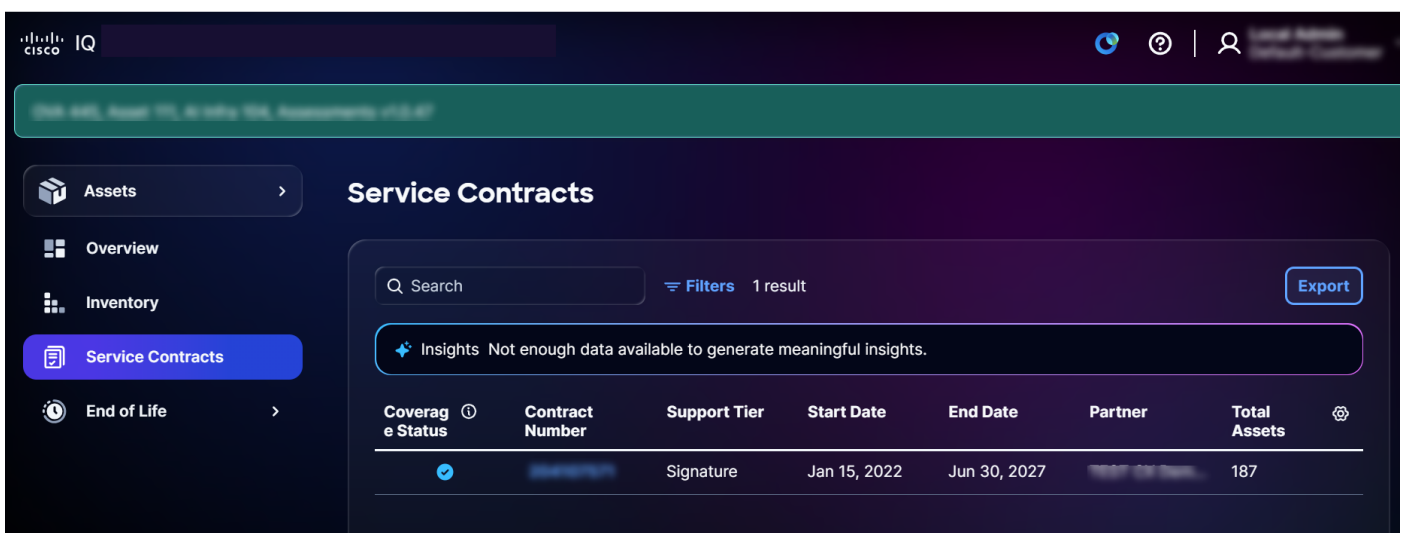


Tag als Filter verwenden

- Aktivieren Sie in der Dropdown-Liste Tags die Kontrollkästchen der gewünschten Tags. Nach der Auswahl des Tags wird die Ansicht auf der Seite "Inventar" auf die gefilterte Ansicht aktualisiert.

Serviceverträge

Auf der Seite für Serviceverträge wird die Überwachung von Supportverträgen optimiert. Sie enthält Zusammenfassungen und detaillierte Vertragsinformationen, die eine effektive Planung von Vertragsverlängerungen und Abdeckungsstrategien unterstützen.



Serviceverträge

Ansichten für Serviceverträge suchen und filtern

Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen. Sie können auch nach Serviceverträgen suchen, indem Sie die Vertragsnummer in das Feld Suchen eingeben.

Exportieren von Serviceverträgen

Klicken Sie auf Exportieren, um eine gefilterte Liste von Verträgen im XLS- oder CSV-Format zu speichern. Weitere Informationen finden Sie unter [Exportieren von Informationen](#) unter Allgemeine Modulfunktionen.

Services EA-Zusammenfassung

Die Seite Services Enterprise Agreement (EA)-Übersicht bietet eine konsolidierte Übersicht über das Wachstum der vorhandenen Installationen in Ihrem Portfolio. Die Daten stammen direkt aus den Aufzeichnungen der vorhandenen Cisco Installationen. So erhalten Sie und Ihre Account Teams eine konsistente Übersicht über Portfolioänderungen im Laufe der Zeit.

Auf der Seite "Services EA-Übersicht" werden folgende Informationen angezeigt:

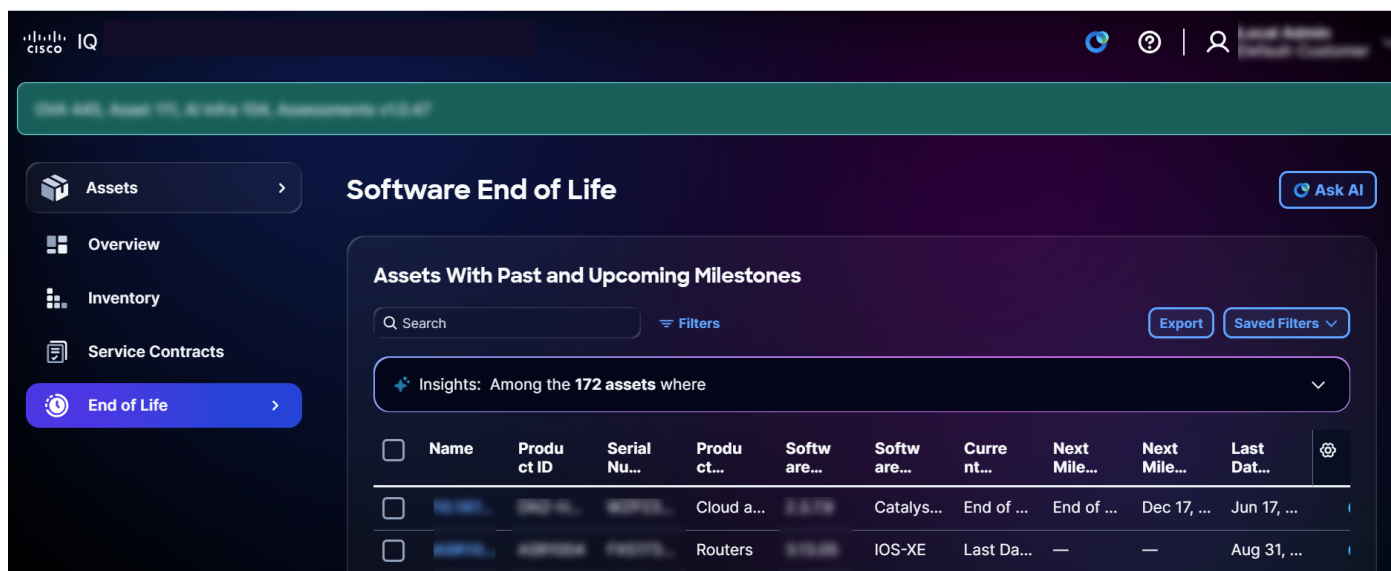
- Hinzugefügte Ressourcen: Neue Ressourcen, die während des Berichtszeitraums zur vorhandenen Installationen hinzugefügt wurden
- Nettoänderung: Die Gesamtänderung der Anzahl vorhandener Installationen für den Berichtszeitraum.

 Anmerkung: Der Zugriff auf die Übersichtsseite der Services-EA kann je nach Rolle und Berechtigungen erfolgen. Wenden Sie sich an Ihren Kontoadministrator, wenn diese Seite in Ihrer Navigation nicht angezeigt wird.

Ende des Lebenszyklus

Auf den Seiten End of Life für Hardware und End of Life für Software finden Sie detaillierte Informationen zum Lebenszyklusende, sodass Benutzer den erforderlichen Support erhalten, um Produktaktualisierungszyklen und Supportabdeckung proaktiv zu verwalten. Durch Klicken auf eine Ressource auf den Seiten zum Ende der Lebensdauer werden Sie zur entsprechenden

Ressource auf der Seite Bestand weitergeleitet.



Ende des Software-Lebenszyklus

Analyse am Ende des Lebenszyklus

Im Bereich Einblicke auf der Seite End of Life (Ende des Lebenszyklus) wird ein KI-gesteuerter Überblick über Ressourcen mit einem definierten Last Day of Support (Letzter Support-Tag) angezeigt. Klicken Sie auf Vollständige Analyse, um Visualisierungen wie Diagramme, Dashboards und Diagramme anzuzeigen, die zusätzliche Einblicke bieten. Weitere Informationen finden Sie unter [Analysieren von Daten](#) in allgemeinen Modulfunktionen.

Ende des Lebenszyklus exportieren

Klicken Sie auf Exportieren, um eine gefilterte Liste der EOL-Ressourcen im XLS- oder CSV-Format zu speichern. Weitere Informationen finden Sie unter [Exportieren von Informationen](#) unter Allgemeine Modulfunktionen.

Leistungsbeurteilungsmodul

Das Assessments-Modul bietet ein Bewertungs-Framework, mit dem Sie Risiken im Zusammenhang mit Sicherheit, Stabilität, Kapazität, Compliance und Alterung proaktiv untersuchen und mindern können, um die Sicherheit, Stabilität und Zuverlässigkeit von Netzwerken zu gewährleisten.

Kernkonzepte

Das Modul "Leistungsbeurteilungen" basiert auf den folgenden Kernkonzepten:

- **Leistungsbeurteilung:** eine systematische Bewertung von Infrastruktureinheiten anhand vordefinierter Kriterien zur Messung von Leistung, Compliance, Sicherheit oder Betriebsfähigkeit; Bewertungen werden bei Bedarf, nach einem Zeitplan oder durch ein Ereignis ausgelöst.
- **Durchführung der Leistungsbeurteilung:** eine Instanz oder ein einzelner Bewertungslauf; Bei jeder Ausführung wird ein neuer Ausführungsdatensatz erstellt, der den Bereich, den Triggermechanismus, den Zeitstempel und die von der Auswertung generierten Ergebnisdaten verfolgt.
- **Suche:** Eine validierte, aussagekräftige Beobachtung, die eine Lücke, ein Risiko, ein Problem oder einen bemerkenswerten Zustand identifiziert. Die Ergebnisse repräsentieren die grundlegenden Daten während einer Bewertung.
- **Erkenntnis:** Eine übergeordnete analytische Schlussfolgerung, die sich aus Mustern oder Trends über mehrere Befunde hinweg ableitet. Erkenntnisse interpretieren die Auswirkungen der Ergebnisse auf einen breiteren geschäftlichen oder betrieblichen Kontext
- **Empfehlung:** ein spezifisches, umsetzbares Rezept, das mit Befunden oder Erkenntnissen verknüpft ist; Die Empfehlungen enthalten klare Leitlinien für die erforderlichen Schritte zur Lösung der festgestellten Probleme oder zur Nutzung von Chancen.
- **Bericht:** Ein strukturiertes Dokument, das die Ergebnisse, Erkenntnisse und Empfehlungen für eine Zielgruppe zusammenfasst. In erster Linie liefern Berichte Informationen zu den Ergebnissen von Analysen an Kunden, Führungskräfte und technische Teams

Zugreifen auf Leistungsbeurteilungsmodule

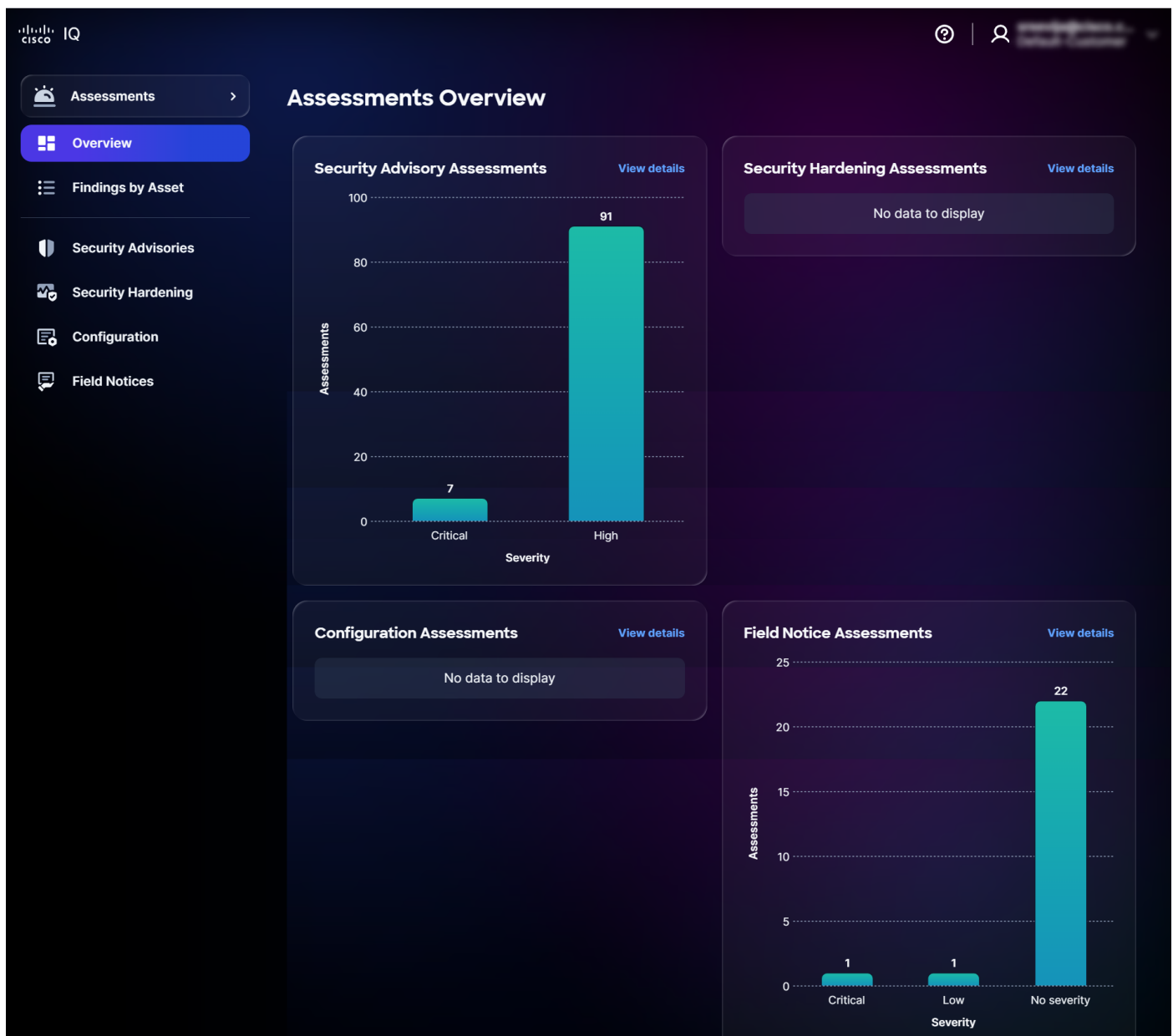
Um auf die Sicherheits- und Bewertungsfunktionen in der virtuellen Appliance zuzugreifen, wählen Sie Home menu > Assessments aus, oder klicken Sie auf Assessments im Abschnitt Application (Anwendung) der Startseite > Launchpad-Registerkarte. Die Seite "Übersicht Leistungsbeurteilungen" wird angezeigt.



Anmerkung: Das Leistungsbeurteilungsmodul kann auch über Systemkonfiguration > Paketverwaltung gestartet werden.

Leistungsbeurteilungen - Überblick

Auf der Seite Assessments Overview (Übersicht der Assessments) wird das folgende Dashboard angezeigt:



Leistungsbeurteilungen - Überblick

Das Dashboard zeigt die folgenden Informationen an:

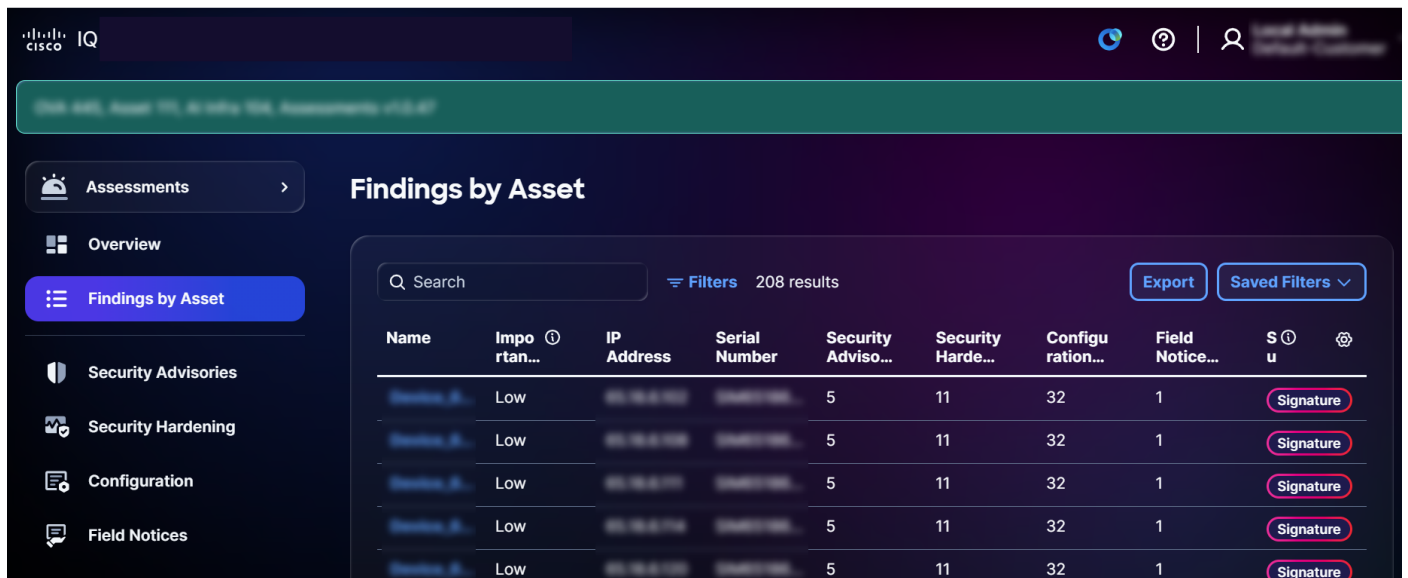
- Sicherheitsratgeber-Analysen: Zeigt Bewertungen von Sicherheitsempfehlungen an, die nach kritischem und hohem Schweregrad kategorisiert sind.
- Bewertungen zur Sicherheitssicherung: Zeigt Ressourcen an, die die Sicherheitshärtungsregeln nicht erfüllen, kategorisiert nach Schweregrad Hoch, Mittel, Niedrig und Informativ

- Konfigurationsanalysen: Zeigt Ressourcen an, die die Compliance-Regeln für Konfigurationen nicht erfüllen, kategorisiert nach dem Schweregrad Kritisch, Hoch, Mittel, Niedrig und Informativ
- Bewertungen von Problemhinweisen: Zeigt Bewertungen von Problemhinweisen an, die nach dem Schweregrad Kritisch, Hoch und Nicht zutreffend kategorisiert sind.

 Anmerkung: Sie können nur die Ressourcen anzeigen, auf die Sie zugreifen dürfen.

Ergebnisse nach Ressource

Auf der Seite Ergebnisse nach Ressource finden Sie eine Liste der Ressourcen, die mit mindestens einer der folgenden Bewertungen bewertet wurden: Sicherheitsempfehlungen, Sicherheitshärtung, Konfiguration und Problemhinweise.



Name	Importance	IP Address	Serial Number	Security Advisory	Security Hardening	Configuration	Field Notice	Signature
Device A	Low	10.10.10.1	1000000000	5	11	32	1	Signature
Device B	Low	10.10.10.2	1000000001	5	11	32	1	Signature
Device C	Low	10.10.10.3	1000000002	5	11	32	1	Signature
Device D	Low	10.10.10.4	1000000003	5	11	32	1	Signature
Device E	Low	10.10.10.5	1000000004	5	11	32	1	Signature

Ergebnisse nach Vermögenswerten

Suchen und Filtern von Ansichten nach Ergebnissen nach Ressource

Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen oder auf Filter klicken und eine Option aus der Liste der verfügbaren Filter auswählen. Sie können im Feld Suchen auch nach Ergebnissen nach Ressource suchen.

 Anmerkung:

- Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet.
- Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung.

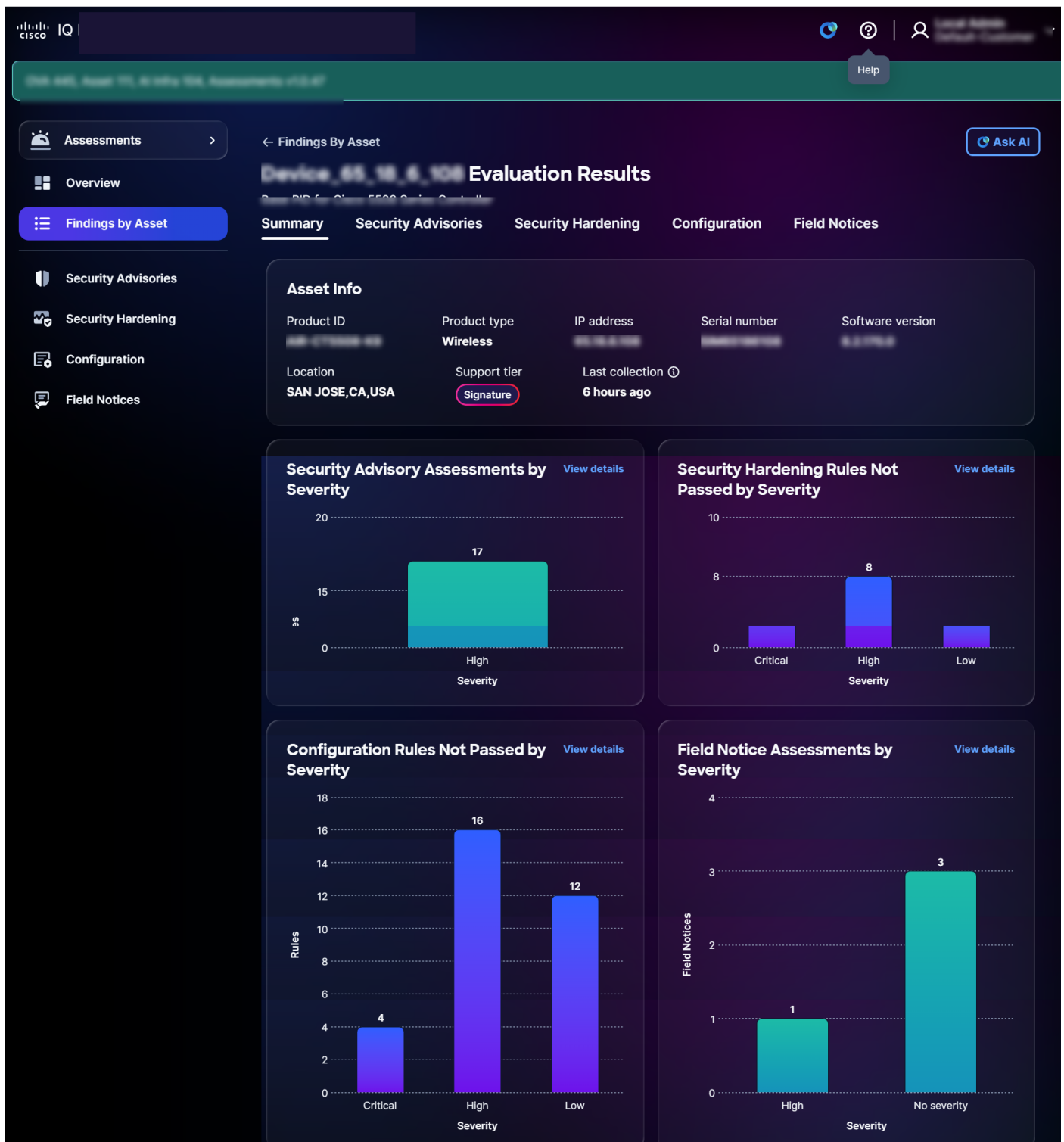
Exportieren der Ergebnisse nach Ressource

Zum Exportieren der Listenansicht Ergebnisse nach Ressource klicken Sie auf Exportieren. Weitere Informationen finden Sie unter [Exportieren von Informationen](#).

Ergebnisse nach Ressourcendetails anzeigen

Klicken Sie auf eine Ressource, um Ergebnisse nach Ressourcendetails anzuzeigen. Auf den folgenden Registerkarten werden Details zu der ausgewählten Ressource angezeigt:

- Zusammenfassung: Detaillierte Bestandsdaten, z. B. Anzahl der Sicherheitsempfehlungen, Sicherheitshärtung, Konfiguration und Problemhinweise
- Sicherheitsempfehlungen: Bietet eine Liste zugehöriger Bewertungen der Sicherheitsberatung
- Sicherheitssicherung: Liste der Ressourcen, die die Sicherheitshärtungsregeln nicht erfüllen
- Konfiguration: Liste der Ressourcen, die nicht mit den Best Practice-Regeln für die Konfiguration übereinstimmen
- Problemhinweise: Bietet eine Liste zugehöriger Analysen für Problemhinweise



Ergebnisse nach Ressourcendetails

Wenn Sie auf Details anzeigen auf einer Kachel klicken, wird die Seite zur entsprechenden Seite im Modul umgeleitet.

Wenn Sie auf Vollständige Anlagendetails anzeigen klicken, wird die Seite mit den Anlagendetails angezeigt.

Sicherheitsempfehlungen

Sicherheitsberatungs-Analysen identifizieren Schwachstellen und priorisieren sie basierend auf ihrem Risiko, Schweregrad und ihrer Wichtigkeit und verbessern so die Risikomanagementfunktionen des Unternehmens. Security Advisories bieten einen präzisen Einblick in Sicherheitslücken, beschleunigen die Eindämmung kritischer Bedrohungen und sorgen für die Abstimmung auf Compliance und Geschäftsziele. Dies stärkt die Sicherheit, optimiert die Ressourcenzuweisung und stärkt die Widerstandsfähigkeit gegen neue Bedrohungen im gesamten Unternehmen. Sicherheitsempfehlungen werden in Cisco IQ automatisch aktualisiert, sobald sie veröffentlicht werden.

Die Seite Security Advisories enthält eine Liste aller Security Advisories mit Sicherheitslücken, die in der Organisation entdeckt wurden. Durch Klicken auf eine Beratung aus der Liste der Sicherheitsberatungs-Einschätzungen wird die entsprechende Detailansicht angezeigt.

 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

Q Search

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

Sicherheitsempfehlungen

Suchen und Filtern von Ansichten nach Sicherheitsempfehlungen

Sie können die Listenansicht filtern, indem Sie einen Filter aus der Dropdown-Liste auswählen. Sie können auch nach Security Advisory-Bewertungen suchen, indem Sie den Namen der Bewertung in das Feld Suchen eingeben.



Hinweis: Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms ausgeblendet. Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms ausgeblendet. Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung. Fehlende Schweregrade werden mit einem beschreibenden Tooltip als "-" angezeigt.

Exportieren von Sicherheitsempfehlungen

Klicken Sie zum Exportieren von Sicherheitsberatungsbewertungen auf Exportieren. Weitere Informationen finden Sie unter [Exportieren von Informationen](#).

Anzeigen der Bewertungsdetails für Sicherheitsberatung

Klicken Sie auf eine Leistungsbeurteilung, um weitere Details anzuzeigen. Die Detailseite enthält Informationen wie Common Vulnerability Scoring System (CVSS) Score, Common Vulnerabilities and Exposures (CVE), Severity (Schweregrad) sowie einen Link zu dem angegebenen Cisco Security Advisory.

In der Tabelle mit den Leistungsbeurteilungsergebnissen können Sie die folgenden Arten von Ergebnissen anzeigen:

- **Betroffen:** Zeigt an, dass die Sicherheitslücke in der Ressource oder Komponente bestätigt wurde und von einem Angreifer ausgenutzt werden kann, sodass eine Behebung erforderlich ist.
- **Potenziell betroffen:** weist darauf hin, dass der Vermögenswert oder die Komponente Anzeichen aufweist, die zu Schwachstellen führen können, dies jedoch nicht definitiv bestätigt wird; Weitere Untersuchungen sind möglicherweise erforderlich

The screenshot shows the Cisco IQ interface for Security Advisories. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories (selected), Security Hardening, Configuration, and Field Notices. The main content area is titled 'Cisco IOS and IOS XE Software Session Initiation Protocol Denial of Service Vulnerability'. It includes an 'About the Assessment' section with a description of the vulnerability, severity (High), CVE, CVSS score, version (1.1), first published date (Sep 25, 2019), and last updated date (Oct 4, 2019). Below this is the 'Asset Results' section, which displays a table of affected assets. The table has columns for Asset, Result, Product ID, IP Address, Serial Number, and Support Tier. The results show several assets marked as 'Potentially Affected' with a yellow warning icon. A search bar and filter options are visible above the table.

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
ISR43...	Potentially Affected				Signature

Details zu Sicherheitsempfehlungen

Anzeigen nach Ergebnissen der Ressourcenbewertung suchen und filtern

Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen oder auf Filter klicken und eine Option aus der Liste der verfügbaren Filter auswählen. Sie können auch nach Ressourcen suchen, indem Sie den Namen der Ressource in das Feld Suchen eingeben.

 Anmerkung: Einige Filter werden je nach Bildschirmzooomeinstellungen möglicherweise ausgeblendet. Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung.

Anzeigen der Ergebnisse der Ressourcenbewertung

Um Details zu einem Bewertungsergebnis anzuzeigen, klicken Sie in der Tabelle Bewertungsergebnis auf eine Ressource. Die Detailseite des Leistungsbeurteilungsergebnisses der Anlage wird angezeigt.

The screenshot displays the Cisco IQ interface for a security advisory. The left sidebar contains navigation options: Assessments, Overview, Findings by Asset, Security Advisories (selected), Security Hardening, Configuration, and Field Notices. The main content area shows the 'Result' for the 'Cisco Secure Boot Hardware Tampering Vulnerability'. The device ID is 'Device_65_10_4_108'. The assessment is 'Cisco Secure Boot Hardware Tampering Vulnerability'. The result details indicate it is 'Potentially affected'. Evidence shows it matched on software type, chassis product ID, and module product ID. Additional verification needed includes checking software releases and module/chassis PID level automation. The 'About the Assessment' section describes a vulnerability in the logic that handles access control to hardware components. The severity is 'High' with a CVSS score of 6.7. The first published date is May 13, 2019, and the last updated date is Nov 20, 2019. The 'About the Asset' section shows the 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		

Ergebnisdetails

Exportieren von Ressourcenergebnissen für Sicherheitsempfehlungen

Zum Exportieren der Ressourcenergebnisse klicken Sie auf Exportieren. Weitere Informationen finden Sie unter [Exportieren von Informationen](#).

Sichern

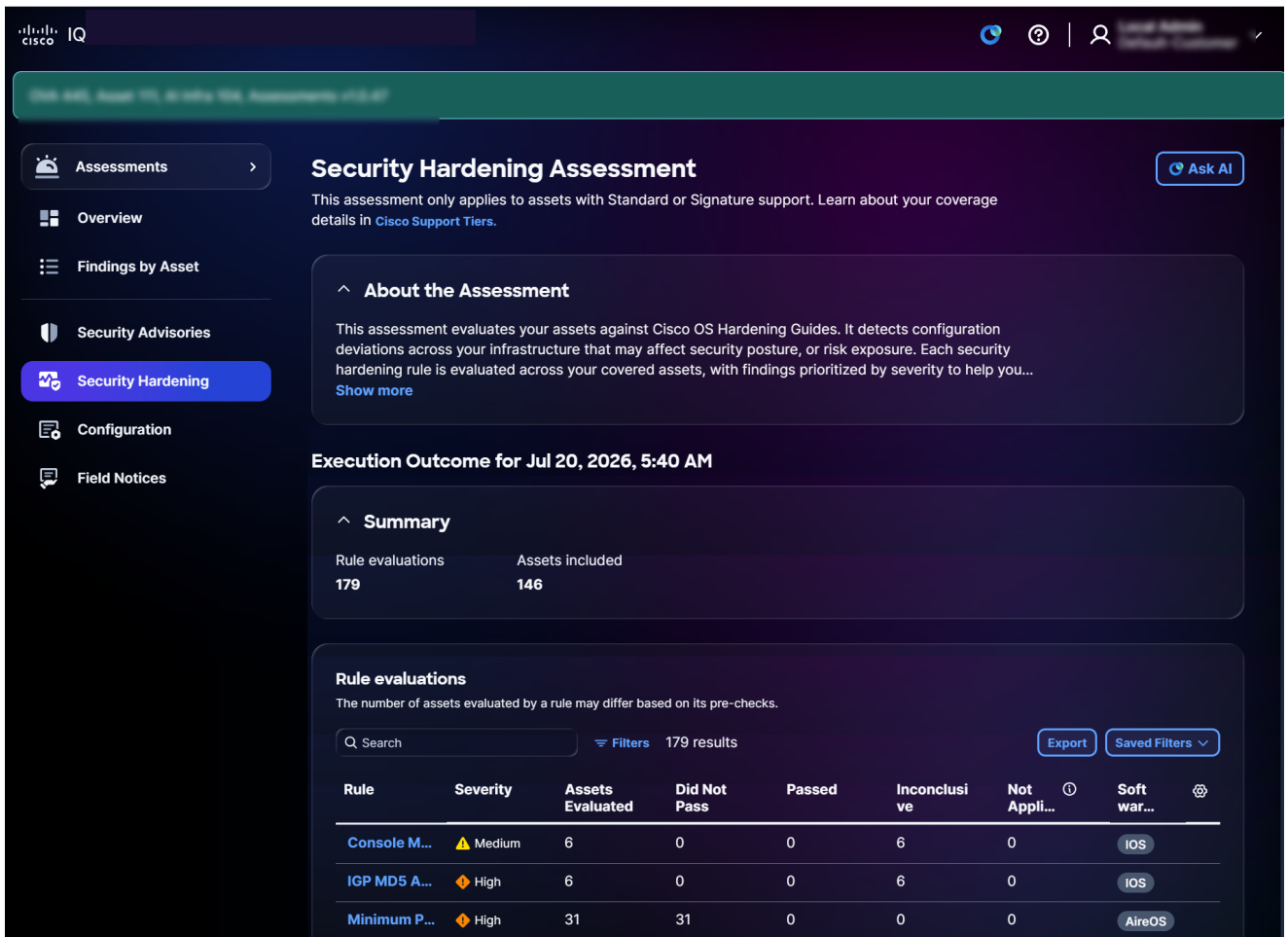
Die Sicherheitsfunktionen bieten einen automatisierten Überblick über den Sicherheitsstatus Ihrer Netzwerkinfrastruktur nahezu in Echtzeit, indem Router, Switches und Firewalls anhand von Branchenstandard-Benchmarks kontinuierlich evaluiert werden. Es identifiziert Konfigurationslücken und bietet Account-Administratoren praktische Anleitungen zur Problembehebung, mit denen sie die Angriffsfläche effektiv verringern und die konsistente Ausrichtung an den strikten Cisco Best Practices für die Sicherheit beibehalten können.

Durch die Zentralisierung der Compliance-Überwachung und die Vereinfachung des Härtungsprozesses verwandelt das Modul das Sicherheitsmanagement von einer reaktiven Aufgabe in eine proaktive, datengesteuerte Strategie, die ein ausfallsicheres und sicheres Unternehmensnetzwerk gewährleistet.

 Anmerkung: Bewertungen der Sicherheitsaushärtung sind ausschließlich für Ressourcen mit standardmäßigen Supportstufen verfügbar.

Sicherheitsbewertungen anzeigen

Auf der Seite Sicherheitsbewertung werden folgende Informationen angezeigt:



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	Assets included
179	146

Rule evaluations

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

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

Sichern

- Informationen zur Leistungsbeurteilung: Zusätzliche Details durch Zusammenfassung des Zwecks der Leistungsbeurteilung
- Ergebnis der Durchführung: Bietet eine Zusammenfassung der Ergebnisse der Ressourcenbewertung, einschließlich der Gesamtzahl der Regelbewertungen und der enthaltenen Ressourcen
- Regelbewertungen: Detaillierte Informationen zur Regel, einschließlich Schweregrad, bewertete Ressourcen, nicht bestanden, bestanden, nicht schlüssig, nicht zutreffend

und Softwaretyp

- Schweregrad: Legt den Grad der Bedeutung oder die Auswirkungen der Regelauswertung fest.
- Bewertete Ressourcen: Zeigt die Gesamtzahl der Ressourcen an, die anhand der Regelkriterien bewertet wurden.
- Nicht bestanden: Stellt die Ressourcen bereit, die während der Leistungsbeurteilung die Regelkriterien nicht erfüllt haben
- Bestanden: Stellt die Ressourcen bereit, die während der Leistungsbeurteilung die Regelkriterien erfüllt haben
- Nicht eindeutig: Stellt die Ressourcen bereit, für die die Analyse den Fehler nicht ermitteln konnte
- Nicht zutreffend: Angabe der Vermögenswerte oder Szenarien, bei denen die Regel nicht anwendbar oder nicht relevant ist
- Softwaretyp: Softwaretyp der Ressourcen

Suchen und Filtern von Ansichten nach Regeln

Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen oder auf Filter klicken und eine Option aus der Liste der verfügbaren Filter auswählen. Sie können auch nach einer Regel suchen, indem Sie den Namen der Regel in das Feld Suchen eingeben.



Hinweis: Je nach Vergrößerungseinstellung des Bildschirms können einige Filter ausgeblendet werden. Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung.

Anzeigen von Regelauswertungsdetails

Klicken Sie auf eine Regel, um weitere Details zu einer Regelauswertung anzuzeigen. Die Seite mit den Evaluierungsdetails der Regel wird mit den folgenden Informationen angezeigt:

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 v]

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

Regelansicht

- Über die Regel: Enthält Details zur Regel, z. B. Schweregrad, Softwaretyp, Version und bewertete Ressourcen, sowie beschreibende Links zur relevanten Quelldokumentation
- Zusammenfassung der Ergebnisse: Bietet eine Zusammenfassung der Anlagenergebnisse im Zusammenhang mit der Regel, z. B. Bestanden, Nicht bestanden, Nicht eindeutig und Nicht zutreffend
- Ergebnisse der Ressourcen: Bietet eine Liste der Ressourcen mit Details wie Ressource, Ergebnis, Produkt-ID, Seriennummer, IP-Adresse und Support-Stufe

 Anmerkung: Cisco IQ bietet klare Richtlinien für den Fall, dass eine Bewertung zu "nicht eindeutig" gelangt, erklärt die Ursache (z. B. fehlende Telemetrie oder nicht unterstütztes Betriebssystem) und empfiehlt Schritte wie die Überprüfung der Datenerfassung, die Aktualisierung von Anmeldedaten oder die Aktualisierung von Daten. Bezeichnete Links zu relevanten Dokumentationen unterstützen Sie ebenfalls bei der Problembehebung.

Suchen und Filtern von Ansichten nach Asset-Regeln

Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen oder auf Filter klicken und eine Option aus der Liste der verfügbaren Filter auswählen. Sie können auch nach Ergebnissen der Anlagenbewertung suchen, indem Sie den Namen der Anlage in das Feld Suchen eingeben.



Hinweis: Je nach Vergrößerungseinstellung des Bildschirms können einige Filter ausgeblendet werden. Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung.

Exportieren der Ressourcenergebnisse

Klicken Sie auf Exportieren, um die Bewertungsergebnisse für Regeln zu exportieren. Weitere Informationen finden Sie unter [Exportieren von Informationen](#).

Suchen und Filtern von Ansichten nach Ressourcenergebnissen

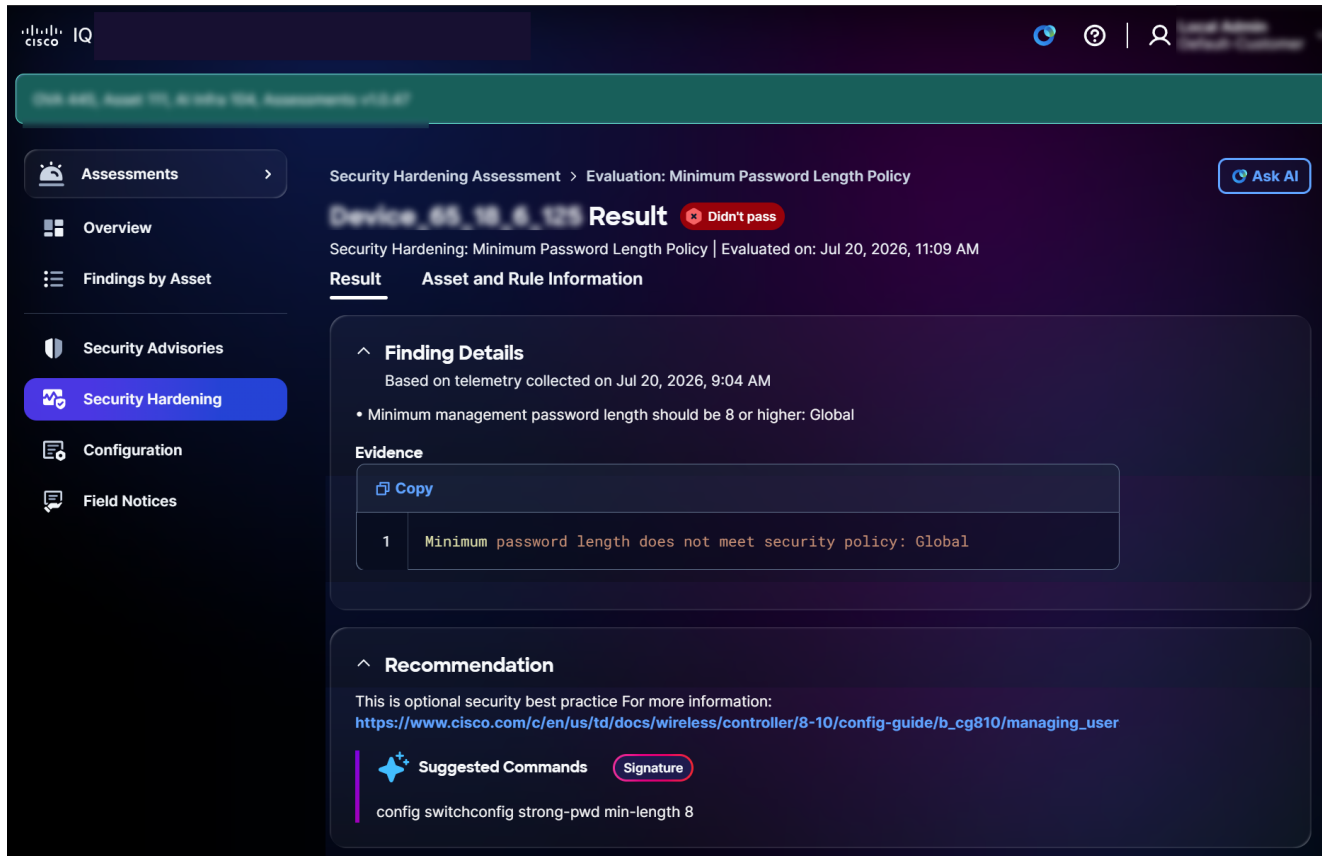
Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen oder auf Filter klicken und eine Option aus der Liste der verfügbaren Filter auswählen. Sie können auch nach Bestandsergebnissen suchen, indem Sie den Namen der Ressource in das Feld Suchen eingeben.



Anmerkung: Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet. Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung.

Anzeigen von Ressourcenergebnissen für die Sicherheitssicherung

Klicken Sie in Asset Results auf eine Ressource, um deren Details anzuzeigen. Auf der Seite mit den Ergebnisdetails der Ressource werden Informationen entsprechend Ihrer Berechtigungsstufe oder -stufe angezeigt.



Standardstufe zur Sicherheitssicherung

- Standard-Tier
- Details suchen: Stellt Informationen zu den bei der Bewertung identifizierten Konfigurationsabweichungen zusammen mit Evidenzprotokollen bereit
- Empfehlungen: Unterstützung bei der Auswertung der Ergebnisse und Sicherstellung konsistenter Konfigurationen

Anzeigen von Ressourcen- und Regelinformationen zur Sicherheitssicherung

Klicken Sie auf die Registerkarte Asset and Rule Info (Asset- und Regelinformationen), um die Details einer Ressource und ihrer Regeln anzuzeigen. Die Seite Asset and Rule Info (Ressourcen- und Regelinformationen) wird angezeigt.

Informationen zum Asset: Beschreibt Details der Ressource wie Produkt-ID, Produkttyp, IP-Adresse, Seriennummer, Softwareversion, Standort und Support-Stufe

- Über die Regel: Enthält Regeldetails (einschließlich Schweregrad und Softwaretyp) und die Bedeutung dieser speziellen Härtingsprüfung

Konfiguration

Bei Konfigurationsanalysen werden Ihre Ressourcen anhand empfohlener Best Practices bewertet, die auf dem bewährten Know-how von Cisco basieren, um

Konfigurationsabweichungen zu erkennen, die sich auf die Verfügbarkeit, die Sicherheit oder die Leistung in der gesamten Infrastruktur auswirken können. Jede Best Practice-Regel wird für alle abgedeckten Ressourcen bewertet, und die Ergebnisse werden nach Schweregrad priorisiert, um eine konsistente Konfiguration, eine erhöhte Ausfallsicherheit und ein geringeres betriebliches Risiko zu gewährleisten.



Anmerkung: Konfigurationsbewertungen sind ausschließlich für Ressourcen mit standardmäßigen Supportstufen verfügbar.

Anzeigen von Konfigurationsanalysen

Auf der Seite Konfigurationsbewertung werden folgende Informationen angezeigt:

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

Konfigurationsbewertung

- Informationen zur Leistungsbeurteilung: Zusätzliche Details durch Zusammenfassung des Zwecks der Leistungsbeurteilung
- Zusammenfassung: Bietet eine Zusammenfassung der Konfigurationsausführung wie evaluierte Regeln und evaluierte Ressourcen
- Insights: bietet Einblicke in identifizierte Konfigurationslücken, die durch eine

Musteranalyse und eine Korrelation der Ergebnisse generiert wurden; Sie werden als intelligent gruppierte Schlüsselkarten angezeigt, um die wichtigsten Bereiche hervorzuheben, die Aufmerksamkeit erfordern.

- Regelauswertungen: Ausführliche Informationen zur Regel, einschließlich Schweregrad, bewertete Ressourcen, nicht bestanden, bestanden, nicht schlüssig, nicht zutreffend, Kategorie und Softwaretyp
- Schweregrad: Legt den Grad der Bedeutung oder die Auswirkungen der Regelauswertung fest.
- Bewertete Ressourcen: Zeigt die Gesamtzahl der Ressourcen an, die anhand der Regelkriterien bewertet wurden.
- Nicht bestanden: Zeigt die Gesamtzahl der Ressourcen an, die während der Leistungsbeurteilung die Regelkriterien nicht erfüllt haben.
- Nicht eindeutig: Zeigt die Gesamtzahl der Ressourcen an, für die die Leistungsbeurteilung nicht ausgeführt werden konnte.
- Bestanden: Stellt die Ressourcen bereit, die während der Leistungsbeurteilung die Regelkriterien erfüllt haben
- Nicht zutreffend: Angabe der Vermögenswerte oder Szenarien, bei denen die Regel nicht anwendbar oder nicht relevant ist
- Kategorie: Stellt den Domänenbereich bereit, zu dem die Regel gehört
- Softwaretyp: Gibt den Typ der Softwareressourcen an, auf die die Regel angewendet wird.

Suchen und Filtern von Ansichten nach Regeln

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

Regelauswertungen

Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen oder auf Filter klicken und eine Option aus der Liste der verfügbaren Filter auswählen. Sie können auch nach einer Regel suchen, indem Sie den Namen der Regel in das Feld Suchen eingeben.



Anmerkung: Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet. Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung.

Anzeigen von Regelauswertungsdetails

Klicken Sie auf eine beliebige Regel, um weitere Details zu einer Regelauswertung anzuzeigen. Die Seite mit den Evaluierungsdetails der Regel wird mit den folgenden Informationen angezeigt:

The screenshot shows the Cisco IQ Configuration Assessment interface. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (highlighted), and Field Notices. The main content area is titled 'Configuration Assessment' and 'NTP Peer Server Limits', evaluated on Jul 20, 2026, at 5:40 AM. It includes an 'Ask AI' button. The 'About the Rule' section explains the rule's purpose and lists its attributes: Severity (Low), Category (Management), Software type (IOS-XE), and Assets evaluated (99). The 'Results Summary' for 99 assets shows: 1 Passed, 0 Didn't pass, 0 Inconclusive, and 98 Not applicable. The 'Asset Results' section features a search bar, filters, and a table of results. The table has columns for Asset, Result, Product ID, Serial Number, IP Address, and Support Tier. The first four rows all show 'Not applicable' results.

Evaluierung

- Über die Regel: Enthält Details zu einer Regel wie Schweregrad, Kategorie, Softwaretyp und bewertete Ressourcen sowie beschreibende Links zur relevanten Quelldokumentation
- Zusammenfassung der Ergebnisse: Zeigt die Gesamtergebnisse der Ressource an, indem die Anzahl der Ressourcen in den Status Bestanden, Nicht bestanden, Nicht schlüssig und Nicht zutreffend angezeigt wird.
- Ressourcenergebnisse: Bietet eine Liste der von der ausgewählten Regel betroffenen Ressourcen mit dem Ergebnisstatus

 Anmerkung: Cisco IQ bietet klare Richtlinien für den Fall, dass eine Bewertung zu "nicht eindeutig" gelangt, erklärt die Ursache (z. B. fehlende Telemetrie oder nicht unterstütztes Betriebssystem) und empfiehlt Schritte wie die Überprüfung der Datenerfassung, die Aktualisierung von Anmeldedaten oder die Aktualisierung von Daten. Bezeichnete Links zu relevanten Dokumentationen unterstützen Sie ebenfalls bei der Problembehebung. Das Bewertungsmodul unterstützt die Auswahl verschiedener Kategorien für Regeln und ermöglicht die gleichzeitige Verarbeitung und Bewertung über mehrere Regelkategorien hinweg.

Exportieren der Ressourcenergebnisse

Zum Exportieren der Ressourcenergebnisse für Regeln klicken Sie auf Exportieren. Weitere Informationen finden Sie unter [Exportieren von Informationen](#).

Suchen und Filtern von Ansichten nach Ressourcenergebnissen

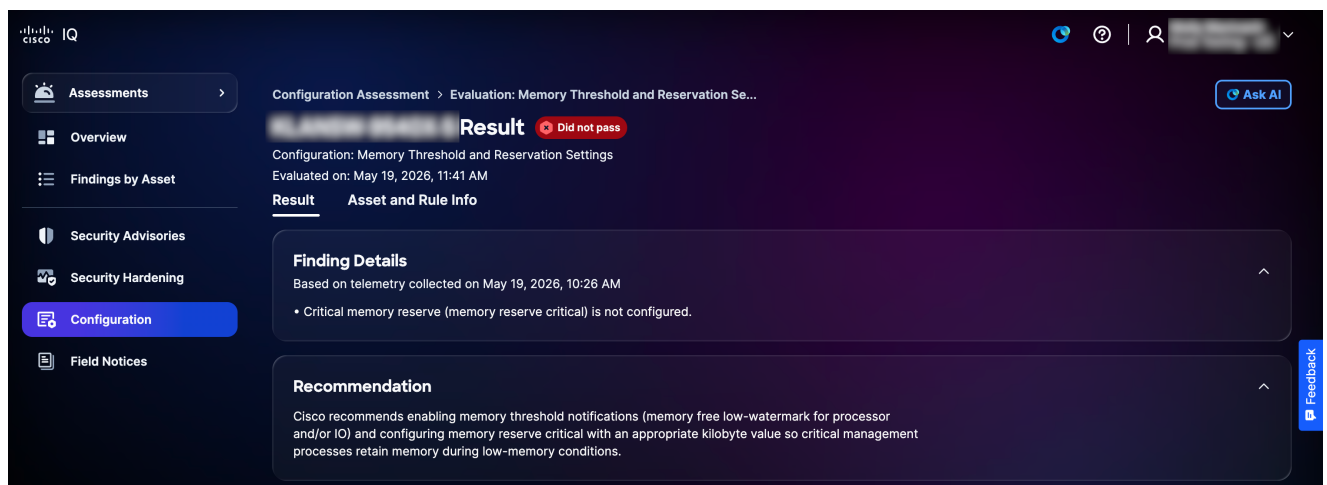
Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen oder auf Filter klicken und eine Option aus der Liste der verfügbaren Filter auswählen. Sie können auch nach Bestandsergebnissen suchen, indem Sie den Namen der Ressource in das Feld Suchen eingeben.

 Anmerkung: Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet. Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung.

Anzeigen von Ressourcenergebnissen für Konfigurationsanalysen

Um Details der Asset-Ergebnisse anzuzeigen, klicken Sie in den Asset-Ergebnissen auf eine Ressource.

Auf der Seite mit den Ergebnisdetails der Ressource werden Informationen entsprechend Ihrer Berechtigungsstufe oder -stufe angezeigt.

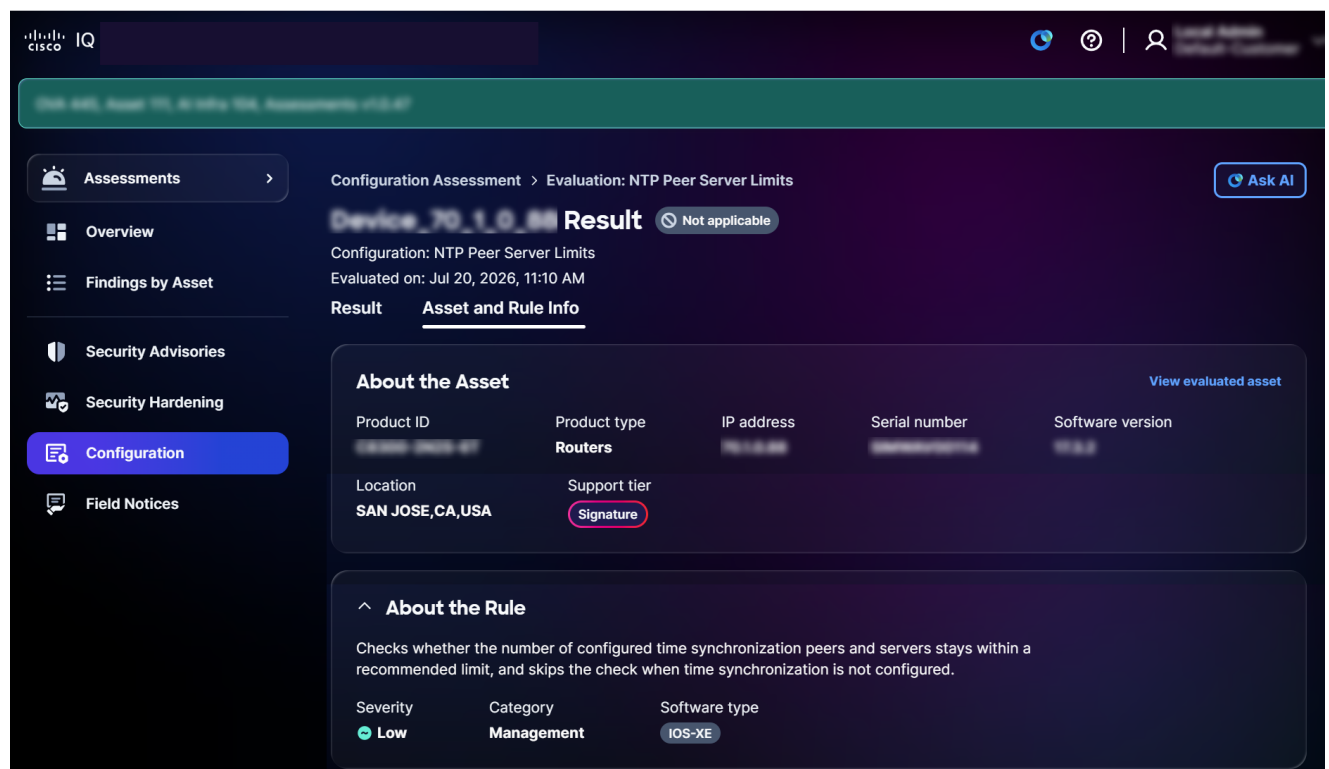


Konfiguration der Standardstufe

- Standard-Tier
- Details suchen: Stellt Informationen zu den bei der Bewertung identifizierten Konfigurationsabweichungen zusammen mit Evidenzprotokollen bereit
- Empfehlungen: Unterstützung bei der Auswertung der Ergebnisse und Sicherstellung konsistenter Konfigurationen

Anzeigen von Ressourcen- und Regelinformationen für Konfigurationsbewertungen

Klicken Sie auf die Registerkarte Asset and Rule Info (Asset- und Regelinformationen), um Details zu Ressourcen und Regeln anzuzeigen.



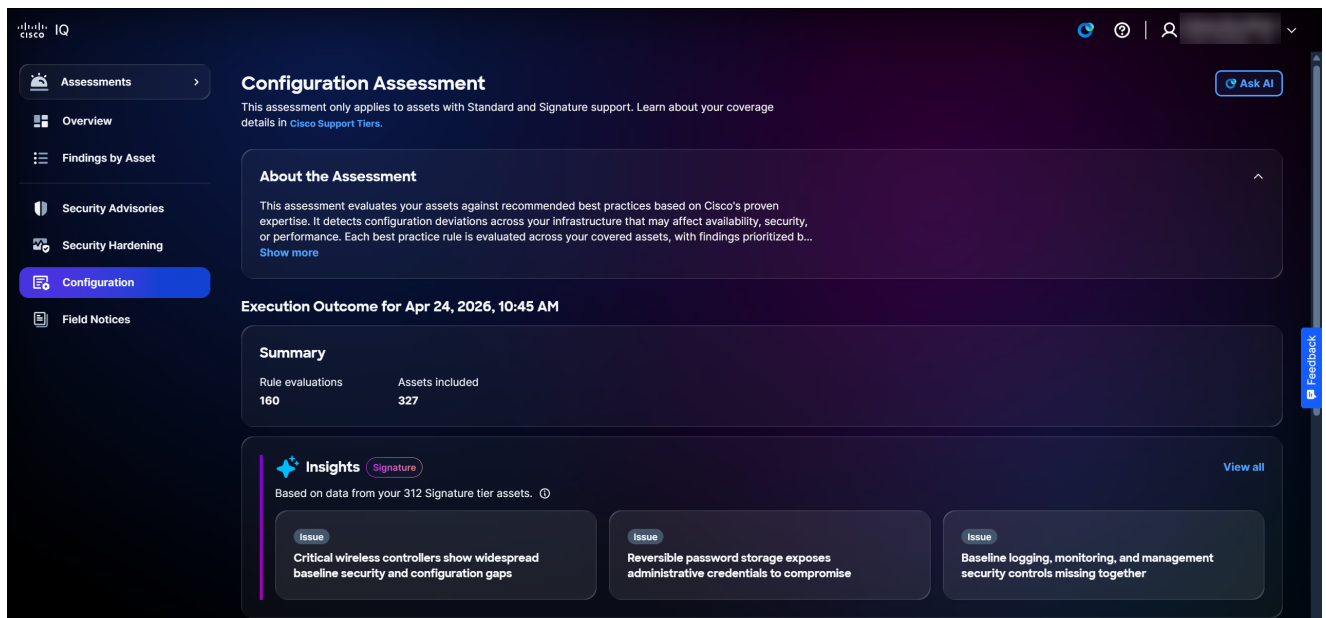
Ressourcen- und Regelinformationen

Die Seite Asset and Rule Info (Ressourcen- und Regelinformationen) wird mit den folgenden Informationen angezeigt:

- Informationen zum Asset: Enthält Details zu Ressourcen wie Produkt-ID, Produkttyp, IP-Adresse, Seriennummer, Softwareversion, Standort und Support-Stufe
- Über die Regel: Enthält Details zu einer Regel wie Schweregrad, Kategorie und Softwaretyp

Einblicke anzeigen

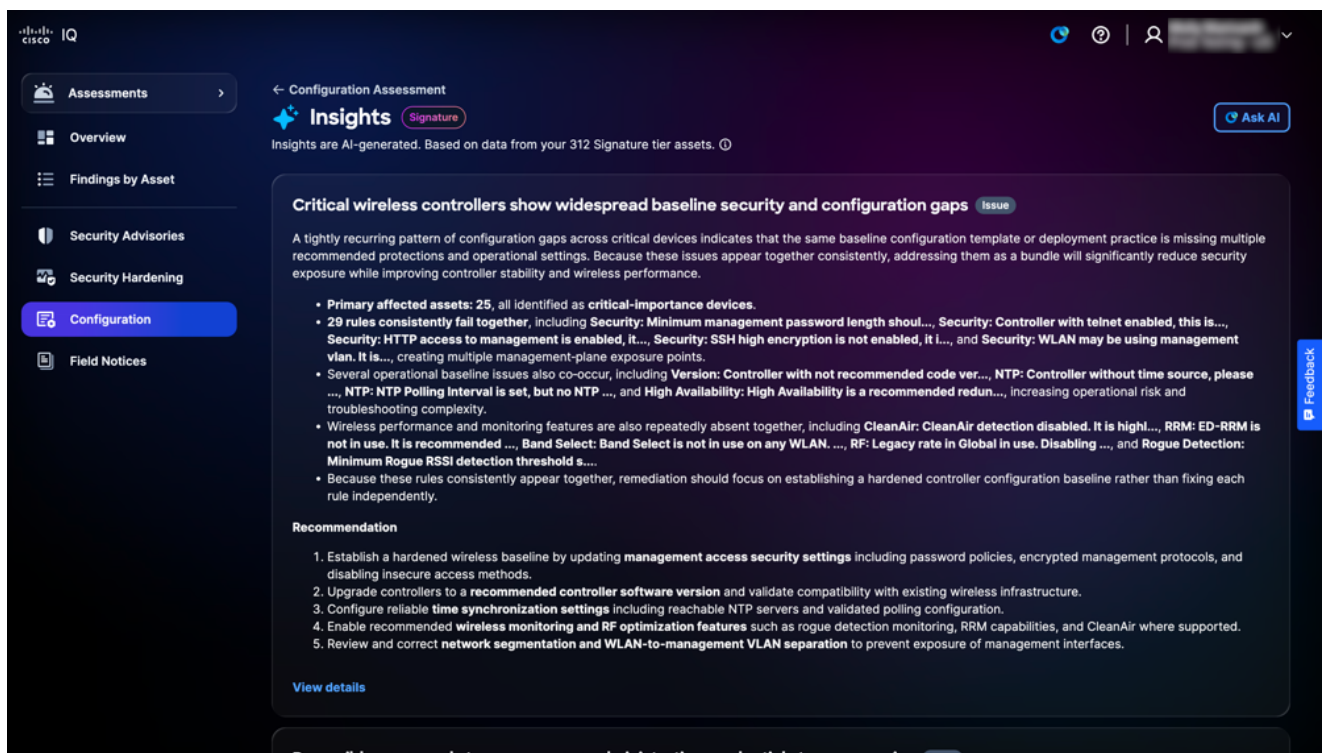
Die Erkenntnisse werden durch KI generiert und dienen als intelligentes Dashboard, das Bewertungsdaten in priorisierte Schlüsselkarten integriert und so wichtige Konfigurationsunterschiede zwischen verschiedenen Ergebnissen aufzeigt. Mit der Lösung können Sie die größten Infrastrukturrisiken effizient angehen, indem Sie sich auf diese dringenden Bereiche konzentrieren. Außerdem werden Stärken hervorgehoben, indem Bereiche ermittelt werden, in denen Ihre Infrastruktur gute Leistung bringt, sowie Best Practices.



Insights

So zeigen Sie Details zu Einblicken an:

1. Klicken Sie im Bereich "Einblicke" auf Alle anzeigen. Auf der Seite Einblicke werden alle Einblicke angezeigt.



Einblicke

2. Klicken Sie auf Details anzeigen, oder klicken Sie auf eine Karte. Die Detailseite "Einblicke" wird mit den folgenden Informationen angezeigt:

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**

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 16 characters**, **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 high priority**, **RRM: ED-RRM is not in use. It is recommended**, **Band Select: Band Select is not in use on any WLAN**, **RF: Legacy rate in Global is in use**, **Disabling Rogue Detection: Minimum Rogue RSSI detection threshold should be -90 dBm**, 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 Filters 25 results Export

Name	Product ID	Serial Number	IP Address
WLC-3850-1	WLC-3850-1	WLC-3850-1	10.10.10.1
WLC-3850-2	WLC-3850-2	WLC-3850-2	10.10.10.2
WLC-3850-3	WLC-3850-3	WLC-3850-3	10.10.10.3

Einblicke - Details

- **Erkenntnis:** Bietet eine Zusammenfassung, in der wiederkehrende Muster von Konfigurationsabweichungen hervorgehoben werden, die durch eine umfassende Analyse verschiedener Ergebnisse ermittelt wurden, sowie Bereiche Ihrer Infrastruktur, in denen Konfigurationen mit Best Practices übereinstimmen
 - **Empfehlung:** Aussagekräftige Schritte zur Beseitigung der festgestellten Konfigurationslücken
 - **Betroffene Ressourcen:** Bietet eine Liste spezifischer Geräte, bei denen die Konfigurationsabweichung gemäß den Definitionen im Abschnitt Insight identifiziert wurde.
3. Klicken Sie auf Quellenergebnisse. Auf der Seite "Source Findings" (Quellenergebnisse) werden die detaillierten individuellen Ergebnisse angezeigt, die Ihre Erkenntnisse unterstützen.

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

Ergebnisse

Sie können die Tabellenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen Schweregrad und Ergebnis auswählen.



Anmerkung: Empfehlungen und "Affected Assets" (Betroffene Ressourcen) sind je nach Ergebnis der einzelnen Erkenntnisse optional.

Problemhinweise

In den Problemhinweisen werden erhebliche nicht sicherheitsrelevante Produktprobleme identifiziert und nach Schweregrad und Bedeutung der Auswirkungen geordnet, sodass Produktrisiken besser gehandhabt werden können. Problemhinweise liefern aussagekräftige Informationen zu Produktfehlern, beschleunigen die Risikominderung durch empfohlene Upgrades oder Workarounds und sorgen für die Abstimmung auf Betriebs- und Geschäftsziele. Dies erhöht die Produktzuverlässigkeit, optimiert die Ressourcenzuweisung und stärkt die Widerstandsfähigkeit gegen neue Produktherausforderungen im gesamten Unternehmen.

IQ Dev (Internal use only, no support available)

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

Problemhinweise

Suchen und Filtern von Ansichten nach Feldbenachrichtigungen

Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen. Sie können auch nach Leistungsbeurteilungen für Feldanmerkungen suchen, indem Sie den Namen der Leistungsbeurteilung in das Feld Suchen eingeben.

Anzeigen von Leistungsbeurteilungen für Problemhinweise

Klicken Sie auf eine Leistungsbeurteilung, um weitere Details zu einem Problemhinweis anzuzeigen. Die folgenden Leistungsbeurteilungsdetails werden angezeigt:

- Über die Leistungsbeurteilungen: Zusätzliche Details durch Zusammenfassung des Zwecks der Leistungsbeurteilung
- Bewertung von Problemhinweisen: Zeigt eine Liste der Ressourcen an, die von der ausgewählten Problemmeldung betroffen sind, einschließlich Ressourcen mit erkannten Schwachstellen.

Field Notices

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

About the assessment

Some medium density Cisco Network Convergence System (NCS) 540 Series Routers may not boot when subjected to a field programmable device (FPD) upgrade during installation of Cisco IOS XR Software Release 7.11.1 or later.

Severity: **Critical** | Last updated: **Dec 11, 2024** | Bugs: [Redacted]

References: [Field Notice](#)

Asset Results

Search: [Input] | Filters: 3 results | Export | Saved Filters

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

Anzeigen von Leistungsbeurteilungen für Problemhinweise

Suchen und Filtern von Ansichten nach Ressourcenergebnissen für Feldbenachrichtigungen

Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen oder auf Filter klicken und eine Option aus der Liste der verfügbaren Filter auswählen. Sie können auch nach Bestandsergebnissen suchen, indem Sie den Namen der Ressource in das Feld Suchen eingeben.



Anmerkung: Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet. Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung.

Exportieren von Ressourcenergebnissen für Feldbenachrichtigungen

Klicken Sie auf Exportieren, um die Ergebnisse der Leistungsbeurteilung für Feldhinweise zu exportieren. Weitere Informationen finden Sie unter [Exportieren von Informationen](#).

Anzeigen der Ergebnisse der Ressourcenbewertung für Problemhinweise

Um die Bewertungsergebnisdetails einer Ressource anzuzeigen, klicken Sie in den Anlagenbewertungsergebnissen auf eine Ressource. Die Seite mit den Analyseergebnissen der Anlage wird angezeigt.

Sie können die folgenden Ergebnistypen anzeigen:

- Betroffen: Gibt Ressourcen an, die alle Kriterien erfüllen und automatisch auf eine Problembeschreibung hin geprüft werden und keine zusätzliche manuelle Überprüfung erfordern, um sicherzustellen, dass sie betroffen sind.
- Potenziell betroffen: Gibt Ressourcen an, die alle automatisch geprüften Kriterien für eine Problembeschreibung erfüllen, aber zusätzliche manuelle Prüfungen erfordern, um sicherzustellen, dass sie tatsächlich betroffen sind.

Die folgenden Aufforderungen sind auf der Registerkarte Assessments - Security Hardening verfügbar:

- Was sind Cisco Best Practices zur Erhöhung der Sicherheit für Netzwerkgeräte?
- Wie härte ich meine Cisco IOS XE-Geräte aus?
- Führen Sie die wichtigsten Schritte zur Sicherung von Routern und Switches auf.
- Welche grundlegenden Härtungseinstellungen werden für Cisco Geräte empfohlen?
- Wie viele Ressourcen verstoßen gegen Best Practices zur Sicherheitssicherung?

Lokale Authentifizierung

Kontoadministratoren sollten die folgenden Anmeldeinformationen verwenden, um sich erfolgreich bei der VA anzumelden:

- Standard-Benutzername: admin
- Default Password (Standardkennwort): Das Kennwort, das während der VA-Installation festgelegt wird. Weitere Informationen finden Sie im Handbuch "Erste Schritte".
- Standard-Kontenkontext: Standard-Kunde

Nach der Anmeldung werden auf der Startseite der Standardbenutzer "admin" und der Kontoname "Default-Customer" angezeigt.

Festlegen der lokalen Administratorsicherheit

Sie können Ihr Kennwort ändern und Sicherheitsfragen über das Menü Benutzerprofil auf der Startseite einrichten.

Sperreinstellungen

Die folgenden Kontosperrungseinstellungen können während der Bereitstellung konfiguriert werden:

- Lockout Status (Sperrstatus): Aktiviert oder deaktiviert die Kontosperrungsfunktion.
- Maximum Login Attempts (Maximale Anmeldeversuche): Legt die maximale Anzahl der

aufeinander folgenden fehlgeschlagenen Anmeldeversuche fest, die vor dem Sperren eines Kontos zulässig sind (Standard: 3; Bereich: 0–10).

- Rolling Time Window: Definiert den Zeitraum für die Nachverfolgung fehlgeschlagener Versuche (Standard: 15 Minuten; Bereich: 0-60 Minuten).
- Duration (Dauer): Legt die Dauer fest, für die ein Konto gesperrt bleibt, nachdem die maximale Anzahl von Versuchen erreicht wurde (Standard: 30 Minuten; Bereich: 0-60 Minuten).

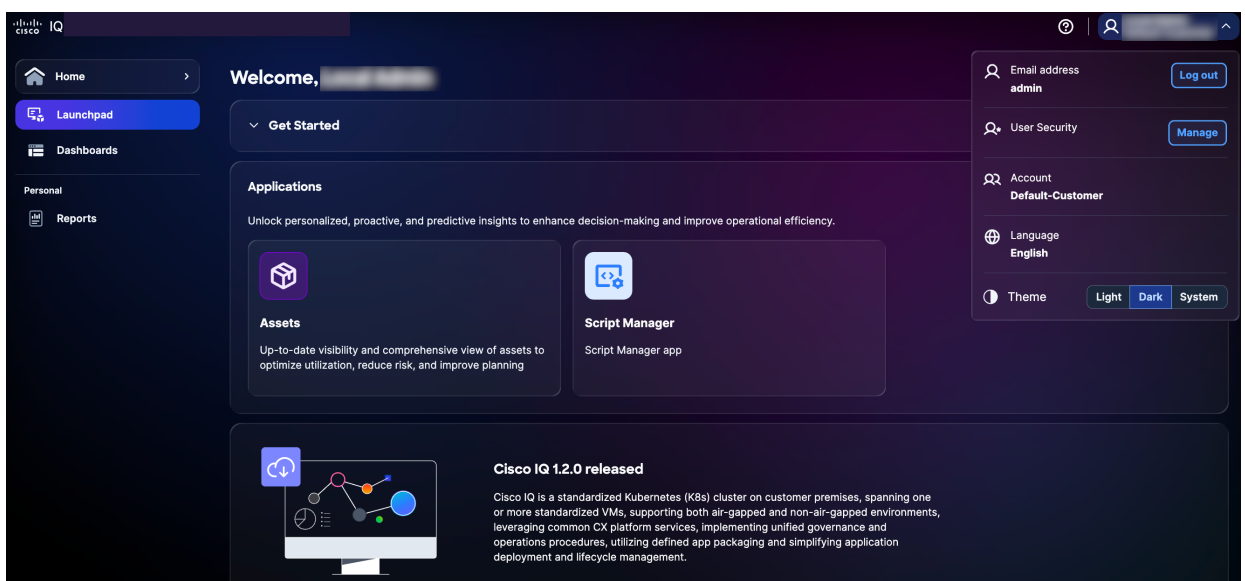
 Anmerkung: Sie haben drei (3) Versuche, innerhalb von 15 Minuten das richtige Kennwort einzugeben. Wenn alle drei (3) Versuche nicht erfolgreich sind, wird Ihr Konto vorübergehend für 30 Minuten gesperrt, um Ihre Sicherheit zu schützen. Sie können nicht versuchen, sich während der Sperrzeit anzumelden. Das System zeigt folgende Meldung an: "Das Konto wurde aufgrund zu vieler fehlgeschlagener Versuche gesperrt. Versuchen Sie es später erneut.", einschließlich der Zeit, zu der die Sperre abläuft. Nach 30 Minuten wird Ihr Konto automatisch entsperrt. Sie können dann versuchen, sich anzumelden oder Ihr Kennwort zurückzusetzen.

Einrichten von Sicherheitsfragen und -antworten

Sicherheitsfragen helfen dabei, Ihre Identität zu verifizieren, wenn Sie Ihr Kennwort vergessen haben. Kontoadministratoren müssen Antworten auf fünf (5) Sicherheitsfragen einrichten, um die Funktion zum Zurücksetzen des Kennworts zu aktivieren. Dies ist eine einmalige Konfiguration.

So richten Sie Sicherheitsfragen ein:

1. Klicken Sie auf der Startseite auf das Symbol Benutzerprofil. Das Dropdown-Menü wird geöffnet.



Sicherheit verwenden

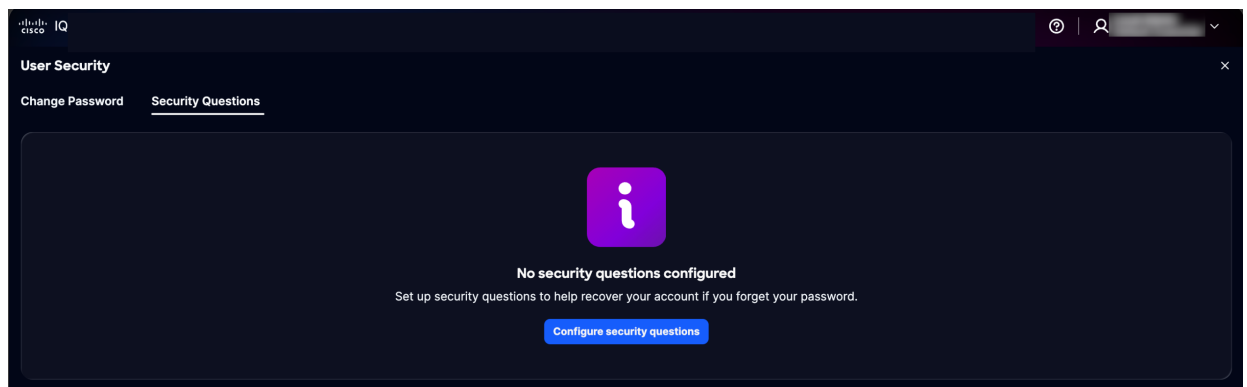
2. Klicken Sie auf Verwalten in der Benutzersicherheit. Die Seite User Security (Benutzersicherheit) wird angezeigt.



The screenshot shows the Cisco IQ User Security interface. The top navigation bar includes the Cisco IQ logo and a user profile icon. The main header is "User Security" with a close button. Below the header, there are two tabs: "Change Password" (active) and "Security Questions". The "Change Password" section contains 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.

Sicherheitsfragen

3. Klicken Sie auf Sicherheitsfragen, um die Registerkarte zu öffnen.



The screenshot shows the Cisco IQ User Security interface with the "Security Questions" tab selected. The main content area displays a large blue information icon. 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 at the bottom.

Registerkarte "Sicherheitsfragen"

4. Klicken Sie auf Sicherheitsfragen konfigurieren.



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 *

Sicherheitsfragen konfigurieren

5. Wählen Sie aus den Dropdown-Listen fünf (5) Sicherheitsfragen aus.
6. Geben Sie Ihre Antwort für jede Frage ein.
7. Klicken Sie auf Speichern.



Anmerkung: Bei den Antworten wird nicht zwischen Groß- und Kleinschreibung unterschieden. Zum Beispiel werden "SMITH" und "Smith" als identisch betrachtet. Zusätzliche Leerzeichen werden ignoriert, was bedeutet, dass "Smith" und "Smith" identisch behandelt werden. Denken Sie daran, wie Sie Ihre Antwort eingegeben haben (z. B. vollständige

 Namen und Spitznamen). Verwenden Sie einfache Antworten, an die Sie sich Jahre später erinnern werden. Wählen Sie Fragen mit Antworten aus, die sich im Laufe der Zeit nicht ändern.

 Anmerkung: Sie können Ihre Antworten bei Bedarf später aktualisieren. Wenn Sie Ihre Antworten aktualisieren, werden alle vorherigen Antworten ersetzt. Sie müssen daher alle fünf (5) Fragen erneut beantworten und nicht nur die, die Sie ändern möchten.

Verwalten von Kennwörtern

Kontoadministratoren und lokale Benutzer können das Kennwort für Cisco IQ verwalten.

Um die Sicherheit Ihres Kontos zu gewährleisten, werden die folgenden Kennwortrichtlinien durchgesetzt:

- Einschränkung der Wiederverwendung: Ihr neues Kennwort kann mit keinem Ihrer vorherigen fünf (5) Kennwörter übereinstimmen. Diese Richtlinie gilt für die Abläufe "Anmeldung", "Kennwort vergessen" und "Kennwort ändern".
- Zeichenvarianz: Wenn Sie Ihr Kennwort ändern, während Sie authentifiziert sind, müssen sich mindestens acht (8) Zeichen von Ihrem aktuellen Kennwort in Ihrem neuen Kennwort unterscheiden.
- Minimales Änderungsintervall: Standardmäßig müssen Sie 24 Stunden warten, bevor Sie Ihr Kennwort erneut ändern können. Wenn ein anderes Intervall konfiguriert wird, können Sie Ihr Kennwort erst nach Ablauf dieses Zeitraums aktualisieren.
- Kennwort läuft ab: Kennwörter laufen alle 60 Tage ab. Bei Ihrer ersten Anmeldung nach dem Ablaufdatum müssen Sie ein neues Kennwort festlegen, bevor Sie auf das System zugreifen können (wenn Sie für 0 konfiguriert sind, ist die Kennwortablaufzeit deaktiviert).

Voraussetzungen

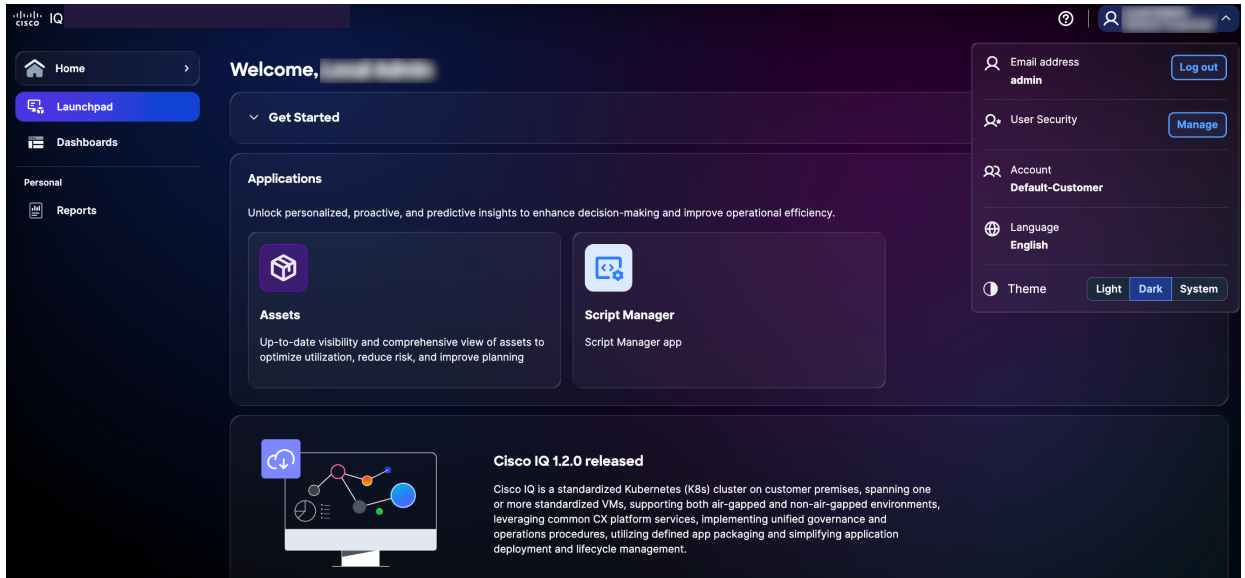
Um Kennwörter zu verwalten, müssen die folgenden Bedingungen erfüllt sein:

- Sie sind ein lokaler Kontoadministrator oder Benutzer.
- Sie verwenden ein lokales Konto (kein Single Sign-On (SSO) oder externe Authentifizierung).
- Sie sind bei Cisco IQ angemeldet.
- Sie kennen das aktuelle Kennwort.

Kennwörter ändern

So ändern Sie das Kennwort:

1. Klicken Sie auf der Startseite auf das Symbol für Ihr Benutzerprofil. Das Dropdown-Menü wird geöffnet.



Benutzersicherheit verwalten

2. Klicken Sie auf Verwalten in der Benutzersicherheit. Die Seite User Security (Benutzersicherheit) wird angezeigt.



Kennwort ändern

3. Geben Sie das aktuelle Kennwort ein.
4. Geben Sie das neue Kennwort ein.
5. Geben Sie zur Bestätigung erneut das neue Kennwort ein.

6. Klicken Sie auf Speichern.

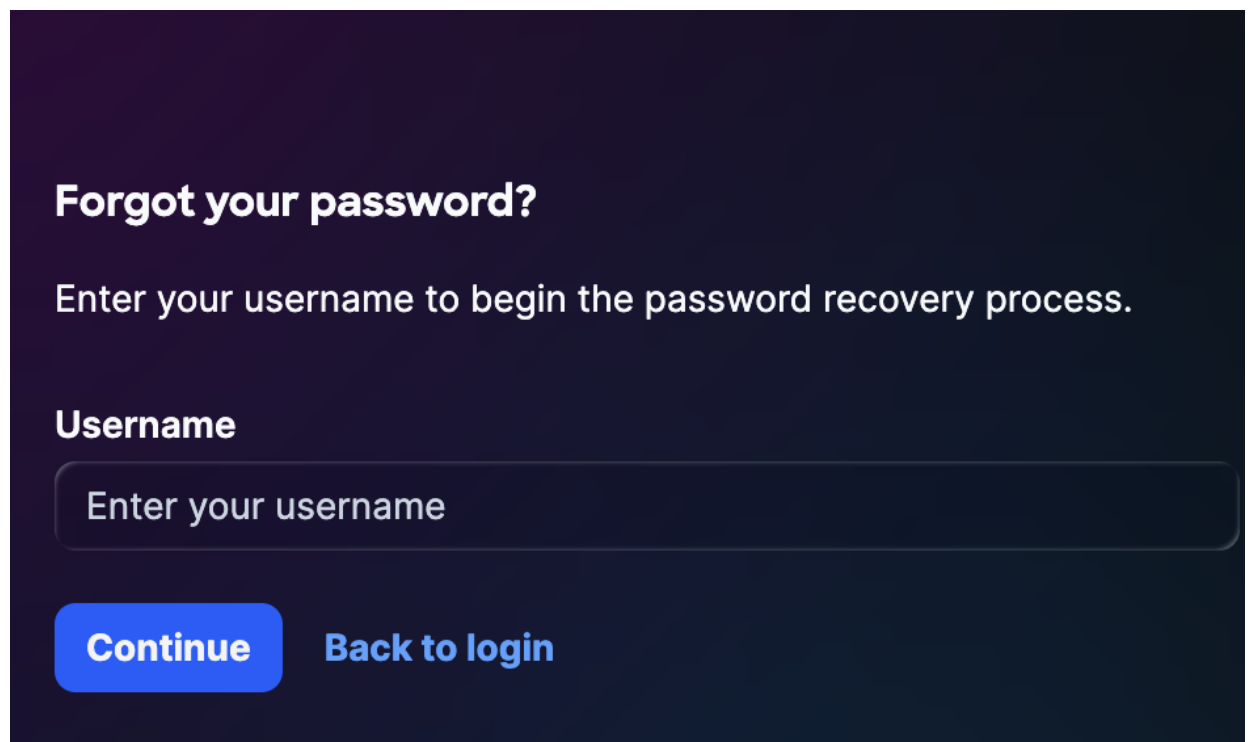
Das Kennwort wird im Cisco IQ-System einschließlich des Cisco IQ VM aktualisiert.

Zurücksetzen eines vergessenen Kennworts

Sie können ein Kennwort zurücksetzen, indem Sie die Sicherheitsfrage überprüfen.

So setzen Sie ein vergessenes Kennwort zurück:

1. Navigieren Sie zur Anmeldeseite von Cisco IQ VA.
2. Klicken Sie auf Kennwort vergessen.



Forgot your password?

Enter your username to begin the password recovery process.

Username

Enter your username

Continue [Back to login](#)

Passwort vergessen

3. Geben Sie den Benutzernamen ein.
4. Klicken Sie auf Continue (Weiter). Auf der Seite Identität überprüfen werden drei (3) zufällige Sicherheitsfragen von den fünf (5) Fragen angezeigt, die zuvor konfiguriert wurden.

Verify Identity

Answer the following security questions to verify your identity.

What city were you born in?

[Show](#)

What is your mother's maiden name?

[Show](#)

What was the name of your elementary school?

[Show](#)[Verify and continue](#)[Back to login](#)

Identität überprüfen

5. Geben Sie die Antworten für alle drei (3) angezeigten Fragen ein.
6. Klicken Sie auf Verifizieren, und fahren Sie fort. Wenn die eingesendete Antwort mit den zuvor gespeicherten Antworten übereinstimmt, werden Sie aufgefordert, ein neues Kennwort einzugeben.

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

Kennwort zurücksetzen

 Anmerkung: Sie haben drei (3) Versuche, innerhalb von 15 Minuten das richtige Kennwort einzugeben. Wenn alle drei (3) Versuche nicht erfolgreich sind, wird Ihr Konto vorübergehend für 30 Minuten gesperrt, um Ihre Sicherheit zu schützen. Sie können nicht versuchen, sich während der Sperrzeit anzumelden. Das System zeigt folgende Meldung an: "Das Konto wurde aufgrund zu vieler fehlgeschlagener Versuche gesperrt. Versuchen Sie es später erneut.", einschließlich der Zeit, zu der die Sperre abläuft. Nach 30 Minuten wird Ihr Konto automatisch entsperrt. Sie können dann versuchen, sich anzumelden oder Ihr Kennwort zurückzusetzen.

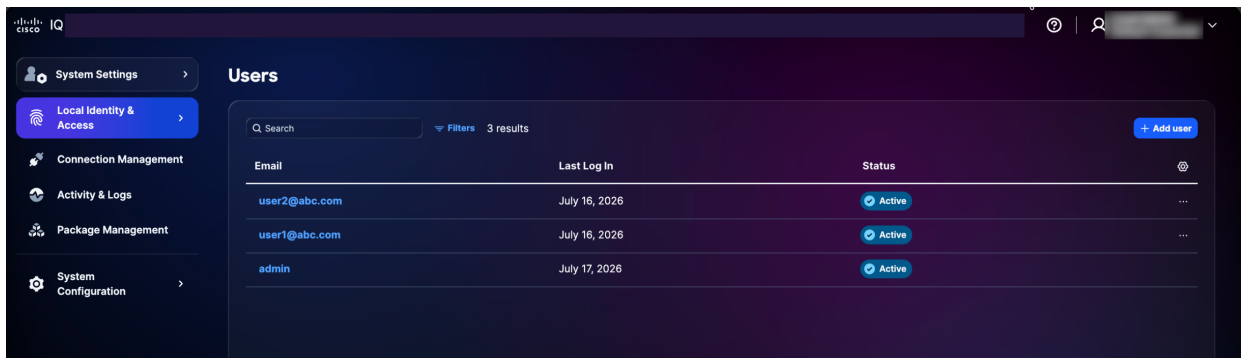
- Geben Sie das neue Kennwort ein.
- Geben Sie zur Bestätigung erneut das Kennwort ein.
- Klicken Sie auf Senden.

Hinzufügen von lokalen Benutzern

Kontoadministratoren können Benutzer zum Cisco IQ-Konto hinzufügen. So fügen Sie

einen neuen Benutzer hinzu

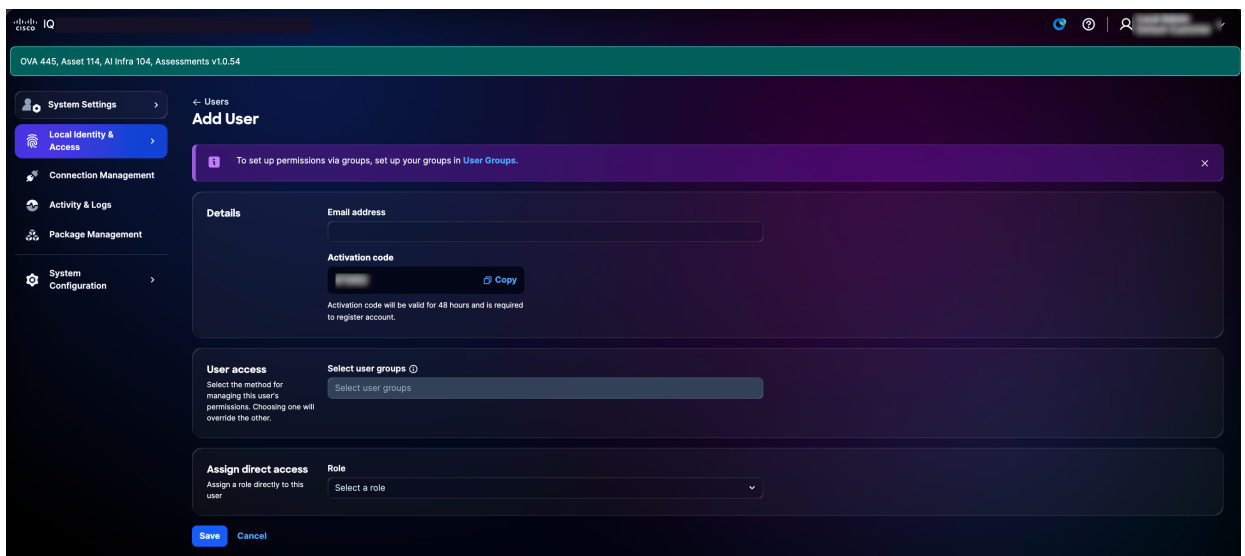
1. Navigieren Sie zu Systemeinstellungen > Lokale Identität und Zugriff > Benutzer. Die Seite Benutzer wird angezeigt. Es listet alle vorhandenen lokalen Benutzer zusammen mit ihrem Status auf.



Seite Benutzer

 Anmerkung: Geben Sie den Aktivierungscode nicht über unsichere Kanäle frei. Wenn der Code verloren geht oder kompromittiert wurde, verwenden Sie das Menü-Symbol, um einen neuen Aktivierungscode zu generieren, der den vorherigen ungültig macht. Aktivierungscodes sind 48 Stunden gültig. Wenn Ihr Code abläuft, wenden Sie sich an Ihren Kontoadministrator, um einen neuen Code anzufordern.

- Klicken Sie auf Benutzer hinzufügen. Die Seite Benutzer hinzufügen wird angezeigt.



Benutzer hinzufügen

3. Geben Sie die E-Mail-Adresse ein.
4. Geben Sie den Aktivierungscode ein.



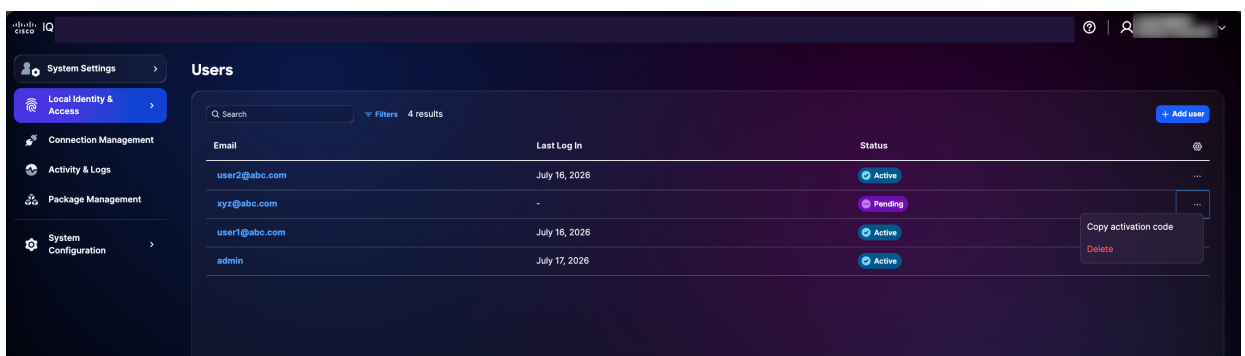
Anmerkung: Der Aktivierungscode wird standardmäßig angezeigt. Teilen Sie den angezeigten Aktivierungscode mit dem Benutzer, wie er für die Registrierung erforderlich ist.

- Wählen Sie in User access die Benutzergruppe aus der Dropdown-Liste Select user groups (Benutzergruppen auswählen) aus.



Anmerkung: Benutzer erben den Zugriff der ausgewählten Gruppe.

- Wählen Sie in Assign direct access (Direktzugriff zuweisen) in der Dropdown-Liste Role (Rolle) die Option role aus. Es sind zwei (2) Rollen verfügbar:
 - Viewer: Anzeigen und Zugreifen auf Anwendungen
 - Kontoadministrator: Zugriff auf Module und Verwaltung von Systemeinstellungen mit Ausnahme von System Management und Identity Provider (IDP)
- Klicken Sie auf Speichern. Der neue Benutzer wird erstellt und in der Benutzerliste im Status Ausstehend angezeigt. Pending (Ausstehend): Der Benutzer hat die Selbstaktivierung noch nicht abgeschlossen.
- Suchen Sie den neu erstellten Benutzer in der Liste, und stellen Sie sicher, dass in der Spalte Status die Meldung Pending (Ausstehend) angezeigt wird.
- Klicken Sie auf das Symbol Weitere Optionen neben dem neu erstellten Benutzer.



Aktivierungscode kopieren

- Wählen Sie den Aktivierungscode kopieren aus der Dropdown-Liste aus. Der Aktivierungscode wird in die Zwischenablage kopiert.
- Geben Sie diesen Code sicher für den Benutzer frei (z. B. über einen sicheren internen Kanal). Der Aktivierungscode ist nur einmal verwendbar und für die vollständige Registrierung erforderlich.

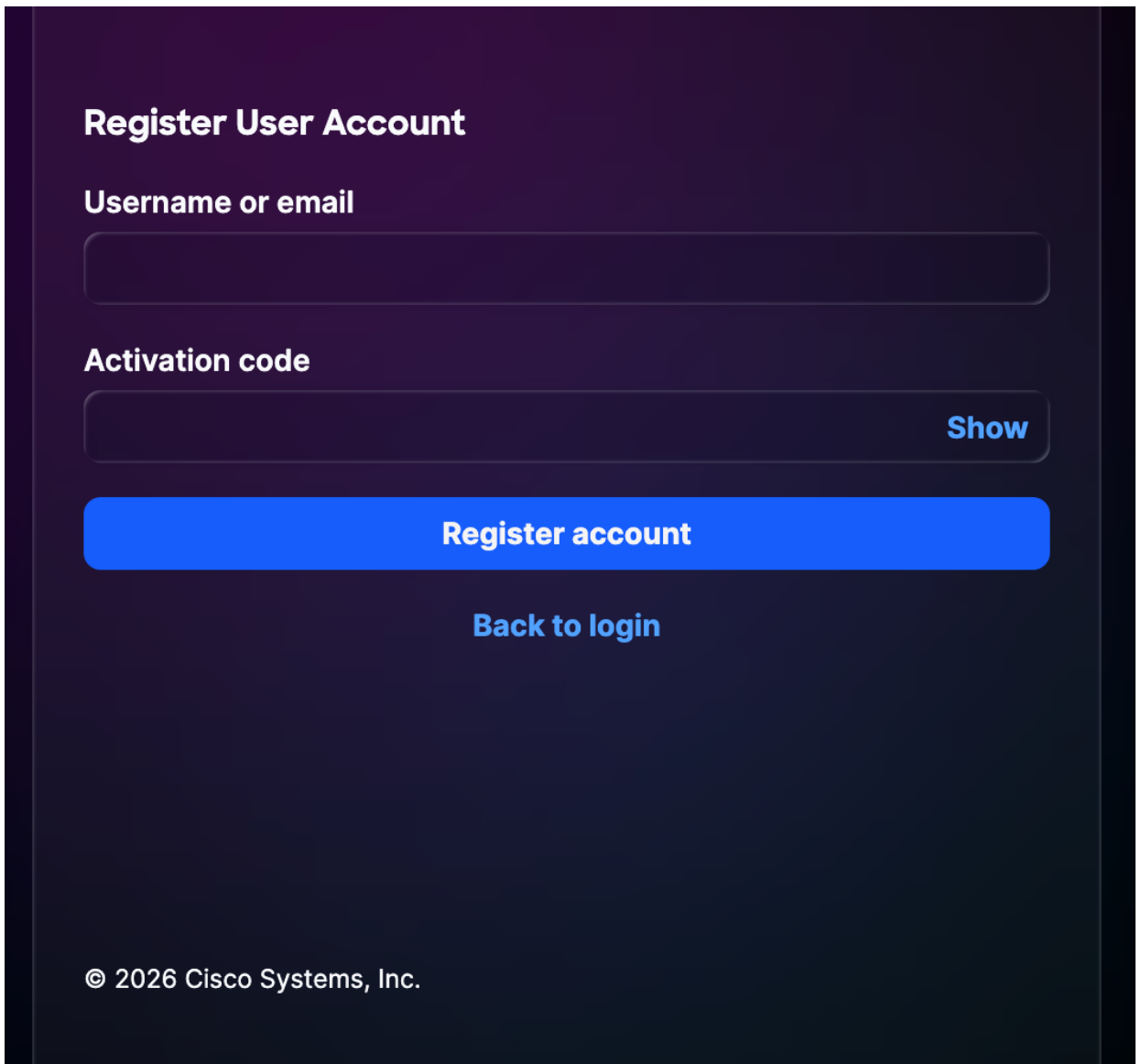
 Anmerkung: Geben Sie den Aktivierungscode nicht über unsichere Kanäle frei. Wenn der Code verloren geht oder kompromittiert wurde, verwenden Sie das Menü-Symbol, um einen neuen Aktivierungscode zu generieren, der den vorherigen ungültig macht. Aktivierungscodes sind 48 Stunden gültig. Wenn Ihr Code abläuft, wenden Sie sich an Ihren Kontoadministrator, um einen neuen Code anzufordern.

12. Um sich abzumelden, klicken Sie auf das Symbol Benutzerprofil in der rechten oberen Ecke, und wählen Sie Abmelden aus. Sie kehren zur Cisco IQ-Anmeldeseite zurück.

Registrieren neuer Benutzerkonten

So registrieren Sie das neue Benutzerkonto:

1. Klicken Sie auf der Anmeldeseite auf den Link Neues Benutzerkonto registrieren.



Register User Account

Username or email

Activation code

 Show

Neues Benutzerkonto

2. Geben Sie den Benutzernamen oder die E-Mail-Adresse ein, die bei der Erstellung des Benutzers verwendet wurde (z. B. user1@abc.com).
3. Geben Sie den vom Kontoadministrator freigegebenen Aktivierungscode ein.
4. Klicken Sie auf Konto registrieren. Das Fenster Neues Kennwort festlegen wird angezeigt.

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](#)

Kennwort für neues Benutzerkonto

5. Geben Sie ein neues Kennwort ein.
6. Geben Sie das Kennwort unter Kennwort bestätigen erneut ein.
7. Bei der ersten erfolgreichen Anmeldung wird der Benutzer aufgefordert, fünf (5) Sicherheitsfragen zu konfigurieren. (Siehe [Sicherheitsfragen einrichten](#)).

Verwalten lokaler Benutzergruppen

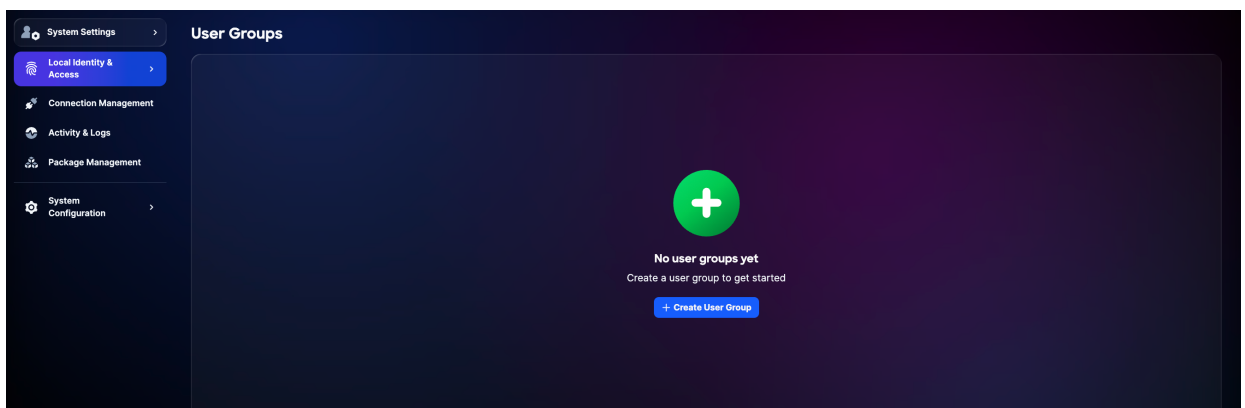
Benutzergruppen ermöglichen es dem Kontoadministrator, Rollen für mehrere lokale Benutzer gleichzeitig zu verwalten. Anstatt jedem Benutzer einzeln eine Rolle zuzuweisen, können Sie eine Gruppe erstellen, eine Rolle und eine Gruppe von Benutzern hinzufügen und die Rolle oder Mitgliedschaft an einem Ort aktualisieren. Die gesamte Benutzergruppenverwaltung erfolgt über die Seite Lokale Identität und Zugriff.

 Anmerkung: Nur ein Kontoadministrator kann Benutzergruppen erstellen, bearbeiten oder löschen. Gruppen bestehen aus vorhandenen lokalen Benutzern; Benutzer müssen erstellt werden, bevor sie einer Gruppe hinzugefügt werden können. Weitere Informationen finden Sie unter [Hinzufügen lokaler Benutzer](#).

Erstellen einer Benutzergruppe

Erstellen einer Benutzergruppe:

1. Wählen Sie in den Systemeinstellungen die Option Lokale Identität und lokaler Zugriff > Benutzergruppen aus. Die Seite Benutzergruppen wird angezeigt.



Benutzergruppen

2. Klicken Sie auf Benutzergruppe erstellen. Die Seite Benutzergruppe erstellen wird angezeigt.

Benutzergruppe erstellen

3. Füllen Sie die folgenden Abschnitte aus:

- Details
 - Name: Geben Sie einen eindeutigen Namen für die Gruppe ein (z. B. Schreibgeschützte Operatoren).
 - Beschreibung (optional): Eine kurze Beschreibung der Gruppe (maximal 50 Zeichen; alphanumerische Zeichen und + = @ - \ _ Zeichen sind zulässig)
 - Benutzer zuweisen: Suchen Sie nach einem oder mehreren vorhandenen lokalen Benutzern, die der Gruppe hinzugefügt werden sollen, und wählen Sie sie aus. Anmerkung: Um noch nicht aufgelistete Benutzer hinzuzufügen, klicken Sie auf Benutzer verwalten.
- Zugriff zuweisen
 - Rolle: Wählen Sie die Systemrolle aus, die allen Mitgliedern dieser Gruppe zugewiesen werden soll. Folgende Rollen sind verfügbar:
 - Viewer: Anzeigen und Zugreifen auf Module (schreibgeschützt)
 - Administrator: Zugriff auf Module und Verwaltung von Systemeinstellungen

4. Klicken Sie auf Speichern.

Die neue Benutzergruppe wird in der Liste Benutzergruppen zusammen mit der zugewiesenen Rolle und der Mitgliederanzahl angezeigt.

Bearbeiten einer Benutzergruppe

So bearbeiten Sie eine Benutzergruppe:

1. Suchen Sie in der Liste Benutzergruppen die Gruppe, die Sie ändern

möchten.

2. Wählen Sie das Symbol Weitere Optionen > Bearbeiten der gewünschten Gruppe. Die Seite Benutzergruppe bearbeiten wird angezeigt.

System Settings > Local Identity & Access > Connection Management > Activity & Logs > System Configuration >

Edit user group

Details

Name: UserGp1
Maximum 50 characters. Use alphanumeric and '+-@._' characters.

Description (optional):
Maximum 50 characters. Use alphanumeric and '+-@._' characters.

Assign users

Search: 1 result [+ Manage users](#)

Name	Email
—	user1@abc.com

Assign access

Role: Administrator

[Save](#) [Cancel](#)

Benutzergruppe bearbeiten

3. Nehmen Sie die gewünschten Änderungen vor.
4. Klicken Sie auf Speichern.

Die aktualisierte Gruppe wird in der Liste Benutzergruppen angezeigt. Die neue Rolle tritt für alle Mitglieder der Gruppe in Kraft.

Löschen einer Benutzergruppe

So löschen Sie eine Benutzergruppe:

1. Suchen Sie in der Liste Benutzergruppen nach der Gruppe, die Sie löschen möchten.
2. Klicken Sie auf das Symbol Weitere Optionen neben der Gruppe, und wählen Sie Löschen aus.

⚠ Delete user group?

User group will be permanently removed from the platform.

[Cancel](#) [Delete user group](#)

Benutzergruppe löschen

3. Bestätigen Sie den Löschvorgang, wenn Sie dazu aufgefordert werden.

Die Gruppe wird aus der Liste Benutzergruppen entfernt.



Anmerkung: Beim Löschen einer Benutzergruppe wird die gruppenbasierte Rollenzuweisung von allen Mitgliedern entfernt. Die einzelnen Benutzerkonten werden nicht gelöscht.

Identitätsanbieter konfigurieren

Nach der Anmeldung bei der VA können Kontoadministratoren verschiedene Einstellungen konfigurieren. Kontoadministratoren können sich über die lokale Administration oder die IDP-Konfiguration anmelden.

Okta IDP SAML-Konfiguration für SSO

Voraussetzungen für die Konfiguration von IDP SAML

- Lokaler Administratorzugriff auf Cisco IQ
- Zugang zum IDP-Portal

IDP SAML-Konfiguration für SSO

So konfigurieren Sie die IDP Security Assertion Markup Language (SAML) für SSO:

1. Navigieren Sie zu Ihrem IDP-Portal.

Tabelle 2: Cisco IQ-Attribute

Feld	Wert
Anwendungsname	<Anwendungsname>
Umwelt	ESP-Geschäftsanwendung
Anwendungsbesitzergruppen	Eigentümer der IDP-Einstellungen
Team-Mailer	Mailer für das Team
Zielgruppe	Nicht erwerbstätig
Onboarding-Kategorie	Wählen Sie "New Onboarding".

Tabelle 3: SAML-Konfigurationsparameter

Parameter	Konfiguration	Beispiel
	Vollqualifizierter Domänenname (FQDN)	
Zielgruppe (Element-ID)		mymanagementhost.mydomain.com
URL für einmalige	SAML	https://mymanagementhost.mydomain.com

Parameter	Konfiguration	Beispiel
Anmeldung	Assertion Customer Service (ACS)- Endpunkt	/saml/acs
Name ID-Format	E-Mail-Adresse	NA
Anwendungsbenutzername	Benutzername	NA

5. Konfigurieren der Attributanweisungen



Anmerkung: Änderungen der IDP-Attribute hängen vom jeweiligen Anbieter und der jeweiligen Konfiguration ab. Cisco IDP und seine Attribute werden nachfolgend als Beispiel genannt.

- Erster Eintrag
 - Name: Benutzername
 - Wert: user.login
- Zweiter Eintrag
 - Name: Primäre E-Mail
 - Wert: Benutzer.E-Mail
- Gruppenattribut-Anweisungen
 - Name: Gruppen
 - Filter: REGELN
 - Wert: .*

6. Konfigurieren der SLO-Einstellungen (Single Logout) in der Anwendung

Tabelle 4: SLO-Konfigurationseinstellungen

Feld	Wert
Signaturzertifikat	Für Okta ist dieses Zertifikat nur erforderlich, wenn Sie SLO aktivieren. Laden Sie das Signaturzertifikat mithilfe von Download SP Certificate in Identity Providers herunter. Speichern Sie die Datei unter dem Namen sp-public-key.crt. Weitere Informationen finden Sie unter Single Logout Configuration (Einzelabmeldekonfiguration).
SP-Metadaten	Die Service Provider (SP)-Metadaten sind nur für ADFS-IDP (und nicht für Okta) erforderlich.
Möchten Sie Single Logout aktivieren?	Ja oder Nein
URL für einzelne Abmeldung	https://mymanagementhost.mydomain.com/saml/logout
SP-Aussteller (Zielgruppe/Objektkennung)	https://mymanagementhost.mydomain.com

Feld	Wert
oder ACS-URL)	

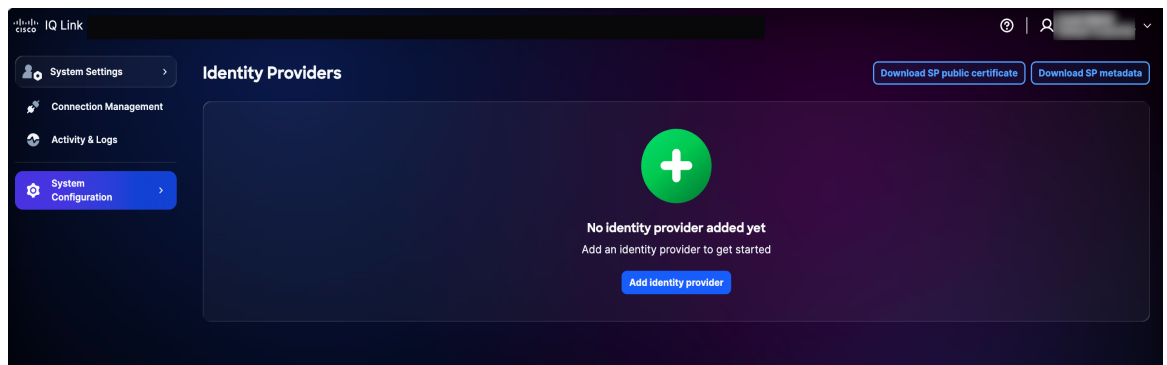
8. Klicken Sie auf das Symbol Download, um die Datei "IDP Metadata XML" herunterzuladen.

9. Stellen Sie die Anwendung gemäß den Anforderungen des Anbieters bereit, oder erstellen Sie sie.

Hinzufügen von Okta IDP

So fügen Sie einen IDP in Cisco IQ hinzu:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Identitätsanbieter aus. Die Seite "Identitätsanbieter" wird angezeigt.



IDP-Startseite



Anmerkung: Es kann jeweils nur ein (1) IDP hinzugefügt werden.

2. Klicken Sie auf Identitätsanbieter hinzufügen. Die Seite Identitätsanbieter hinzufügen wird angezeigt.

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 'Identity Providers' and 'Add Identity Provider'. It contains three main sections: 'Identity provider name' with a text input field; 'Domains' with a text input field and an 'Add' button; and 'Organization IDP metadata' with a dashed box for file upload and an upload icon. Below these is a toggle switch for 'Enable single log out (SLO)' and 'Save'/'Cancel' buttons at the bottom.

Identitätsanbieter hinzufügen

3. Geben Sie den Namen des Identitätsanbieters ein.
4. Klicken Sie auf Add (Hinzufügen), um dem Feld Domain(s) einen von Cisco IQ konfigurierten Domännennamen hinzuzufügen.
5. Ziehen Sie die aus der IDP-Anwendung erhaltene SAML-Metadatendatei per Drag-and-Drop in das Feld Organization IDP-Metadaten, oder laden Sie sie hoch. Diese Datei enthält Zertifikatdetails und SP-Entitätsdetails.
6. (Optional) Aktivieren Sie die Umschaltfläche Einzelnes Abmelden aktivieren. Sie können das SLO auch später aktivieren.
7. Klicken Sie auf Speichern.

Konfiguration der Rollenzuordnung

1. Wählen Sie aus dem hinzugefügten IDP das Symbol More Options (Weitere Optionen) > Map Roles (Rollen zuordnen). Die Seite Benutzerrollen zuordnen wird angezeigt.

×

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

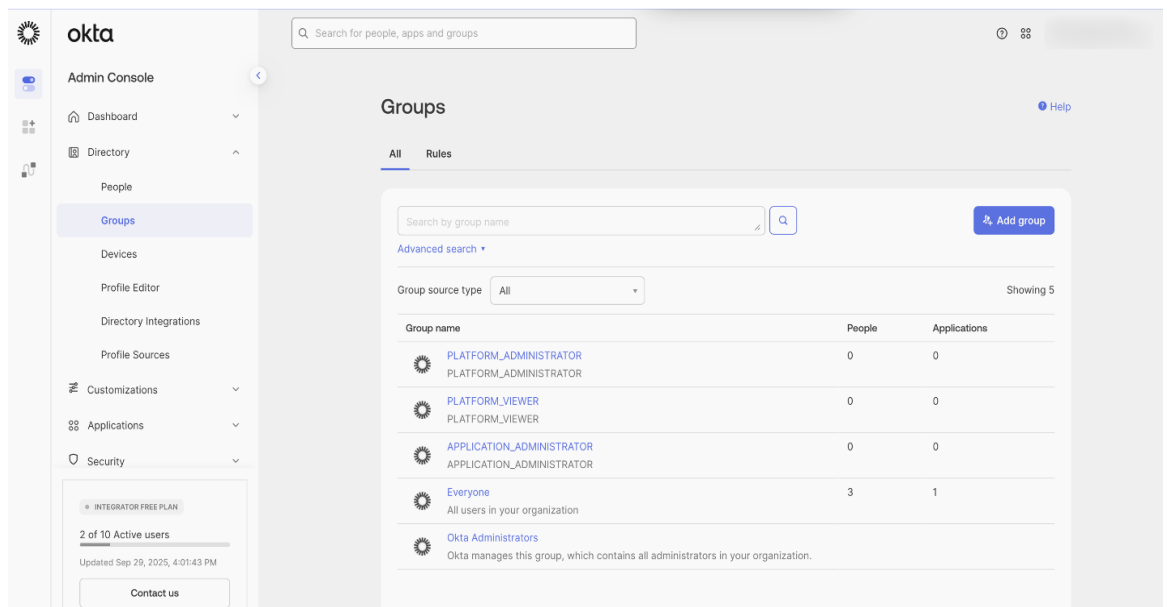
Benutzerrollen zuordnen

2. Geben Sie eine IDP-Rolle für die ausgewählte Systemrolle ein. Folgende Systemrollen werden unterstützt:

- Allgemeiner Kontoadministrator: Der allgemeine Kontoadministrator verfügt über die vollen Berechtigungen zum Ausführen aller Aktionen im Produkt.
- Allgemeine Kontoanzeige: Die allgemeine Kontoanzeige verfügt über schreibgeschützten Zugriff.



Anmerkung: Die IDP-Rolle ist ein offenes Feld. Er muss genau mit dem Gruppen- oder Rollennamen übereinstimmen, der im IDP Ihrer Organisation konfiguriert wurde. Ein Beispiel für Okta-Gruppen finden Sie weiter unten.



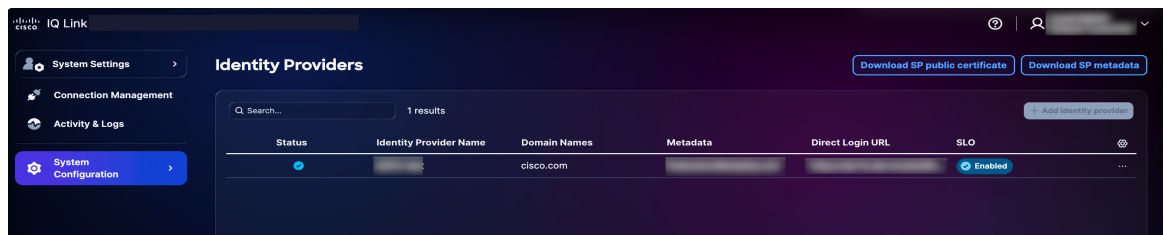
Referenz zur Rollenzuordnung

3. Ordnen Sie ggf. weitere Rollen zu, indem Sie auf Identitätsanbieterrolle hinzufügen klicken.
4. Klicken Sie auf Speichern. Nach der Konfiguration wird auf der Anmeldeseite eine Option zur Anmeldung mit SSO (über IDP) angezeigt.

Konfiguration für einmaliges Abmelden

Wenn Sie SLO aktivieren, müssen Sie Metadaten hochladen, die die SLO-URL enthalten. Sie können dies konfigurieren, indem Sie die Einstellungen für den Identitätsanbieter bearbeiten und den Umschalter für einmaliges Abmelden aktivieren aktivieren. SLO-Konfiguration abschließen:

1. Klicken Sie auf der Homepage der Identitätsanbieter auf Öffentliches SP-Zertifikat herunterladen.



Öffentliches SP-Zertifikat

2. Speichern Sie die heruntergeladene Datei als sp-public-key.crt.
3. Navigieren Sie zu Ihrem IDP-Portal.
4. Laden Sie die Signaturzertifikatdatei hoch, die in der [IDP SAML-Konfiguration für SSO](#) generiert wurde.
5. Geben Sie die SLO-URL ein (z. B. https://ciq-xxx-xxx-37-160.cx-hub-rtп.cisco.com/saml/logout).
6. Geben Sie den SP-Aussteller ein (z. B. ciq-xxx-xxx-37-160.cx-hub-rtп.cisco.com).
7. Klicken Sie auf Senden.
8. Laden Sie die IDP-Metadatendatei erneut herunter.
9. Wählen Sie auf der Seite Identity Providers (Identitätsanbieter) das Symbol More Options (Weitere Optionen) des hinzugefügten IDP aus > Edit (Bearbeiten).
10. Aktivieren Sie die Umschaltfläche Enable single log out (SLO).
11. Laden Sie die neu heruntergeladene Metadatendatei hoch.
12. Verwenden Sie die folgende Checkliste, um die SSO- und SLO-Funktionalität zu überprüfen:

Verifizierungs-Checkliste:

- Anmeldung beim lokalen Administrator erfolgreich
- IDP-Portal wird konfiguriert und bereitgestellt
- IDP wird dem Cisco IQ mit dem Status "Success" hinzugefügt
- Rollenzuordnungen werden konfiguriert und getestet.
- SP-Metadaten werden heruntergeladen, und das Zertifikat wird extrahiert.

- Wenn SLO aktiviert ist, ist die SLO-Konfiguration mit dem echten Signaturzertifikat abgeschlossen
- Der gesamte SSO- und SLO-Fluss wurde erfolgreich getestet.

Fehlerbehebung bei IDP-Problemen

In den folgenden Tabellen sind häufige Probleme und mögliche Lösungen aufgeführt, die bei der schnellen Identifizierung und Behebung von Problemen im Zusammenhang mit dem IDP-Status, Zertifikatfehlern, SSO-Anmeldefehlern und der SLO-Konfiguration helfen:

Tabelle 5: Fehlerbehebung

Problem	Lösung
Der IDP-Status wird als "Incomplete" (Unvollständig) angezeigt.	Überprüfen der Konfigurationen für die Rollenzuordnung
Zertifikatfehler	Format und Gültigkeit des Zertifikats überprüfen
SSO-Anmeldefehler	Attributzuordnung und Gruppenzuweisungen validieren
SLO funktioniert nicht wie erwartet	Stellen Sie sicher, dass das Zertifikat ordnungsgemäß hochgeladen und SLO-URLs konfiguriert wurden.

ADFS IDP SAML-Konfiguration für SSO

Dieser Abschnitt enthält Anleitungen zur Konfiguration von Microsoft Active Directory (AD) Federation Services (FS) als SAML IDP für Cisco IQ mit Unterstützung passwortbasierter und PKI- (Public Key Infrastructure) oder zertifikatbasierter Authentifizierung.

Voraussetzungen für die Konfiguration von ADFS IDP SAML für SSO

- ADFS 6.0+ wird empfohlen
- Windows Server 2016 + (empfohlen 2019)
- Konfigurierte AD-Integration mit Benutzerkonten
- SSL/TLS-Zertifikate auf dem ADFS-Server
- Administratorzugriff auf Cisco IQ
- Administratorzugriff auf den ADFS-Server (Windows Server)

- PowerShell-Zugriff auf ADFS-Server
- Netzwerkverbindung zwischen ADFS und Cisco IQ
- Enterprise Certificate Authority (CA) (installiert oder erreichbar)
- Domain Administrator- oder Enterprise Administrator-Berechtigungen (nur für PKI erforderlich)
- Details zur ADFS-Serverkonfiguration (wie in der unten stehenden Tabelle aufgeführt)

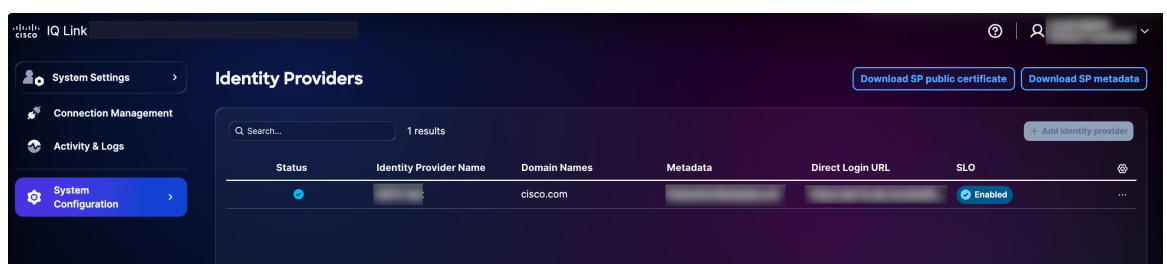
Tabelle 6: Übersicht über den Authentifizierungsfluss

Posten	Beschreibung	Beispiel
Cisco IQ-FQDN	Hostname der Benutzerbereitstellung	<Ihr-CIQ-FQDN> Beispiel: dev35-23.cx-xxx-xxx.cisco.com
ADFS-Server-URL	Benutzer ADFS-Serveradresse	https://<Ihr-ADFS-HOSTNAME> Beispiel: https://ad-fs.dev.local
Firmendomäne	E-Mail-Domäne	<Ihre Domäne>
AD-Gruppen	Domänennamen (DN) der Active Directory-Gruppe	CN=Rolle - CXIQ-Entwickler OU = Gruppen, DC = dev, DC = lokal
Zertifizierungsstellenname (PKI)	Name der Enterprise CA	<Ihr-Zertifizierungsstellenname>
Zertifikatauthentifizierungs-Port (PKI)	ADFS alternativer TLS-Port	49443
SSL-Zertifikatfingerabdruck	ADFS-Server SSL-Zertifikat	<Ihr SSL-CERT-THUMBPRINT>

Basiskonfiguration von ADFS-SAML

ADFS konfigurieren:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Identitätsanbieter aus. Die Seite "Identitätsanbieter" wird angezeigt.



Download-Optionen

2. Klicken Sie auf Öffentliches SP-Zertifikat herunterladen und auf SP-Metadaten herunterladen, um diese Dateien herunterzuladen.
3. Kopieren Sie die Dateien service-provider-metadaten.xml und service-provider-certificate.crt auf den ADFS-Server (z. B. C:\), und speichern Sie sie.
4. Melden Sie sich beim ADFS-Server an.
5. Klicken Sie im Menü ADFS Management (ADFS-Verwaltung) auf Relying Party Trusts (Vertrauenswürdige Partei).
6. Klicken Sie im Menü Vertrauenswürdige Partei auf Vertrauenswürdige Partei hinzufügen. Der neue Assistent wird geöffnet.
7. Klicken Sie auf das Optionsfeld Claims Aware (Ansprüche bekannt).
8. Klicken Sie auf Start, um die Konfiguration fortzusetzen.
9. Klicken Sie auf Daten über die vertrauende Partei aus einer Datei importieren, um Details aus der Datei abzurufen, die als Teil von Schritt 3 gespeichert wird.
10. Klicken Sie auf Durchsuchen, um die Metadatendatei des Dienstanbieters auszuwählen und den Dateiupload abzuschließen.
11. Klicken Sie auf Next (Weiter).
12. Geben Sie einen Anzeigenamen ein (z. B. "Cisco IQ"), fügen Sie relevante Anmerkungen hinzu, und klicken Sie auf "Weiter".
13. Klicken Sie auf der Seite Choose Access Control Policy (Zugriffskontrollrichtlinie auswählen) auf Permit everyone (Alle zulassen) (oder auf die Richtlinie, die für die Sicherheitskonfiguration Ihres Unternehmens erforderlich ist).
14. Klicken Sie durch die übrigen Bildschirme auf Weiter.
15. Klicken Sie auf Schließen, um die Vertrauensstellungskonfiguration für die vertrauende Seite abzuschließen.



Anmerkung: Wählen Sie nicht "Jeden mit MFA zulassen" aus, es sei denn, Ihr ADFS-Server verfügt über einen registrierten MFA-Adapter (Multi-Factor Authentication) (z. B. Azure MFA, Konfiguration eines zeitbasierten einmaligen Kennworts (TOTP)).

Wenn diese Richtlinie ohne einen konfigurierten MFA-Anbieter aktiviert ist,

authentifiziert ADFS den Benutzer, verweigert jedoch die Anforderung mit dem Status urn:oasis:names:tc:SAML:2.0:status:RequestDenied. Da die SAML-Antwort keine Assertion enthält, schlägt das Plugin fehl und meldet einen "Missing Email"-Fehler.

Problem: Wählen Sie "Jeden Benutzer mit MFA zulassen" aus.

Problemumgehung: Überprüfen Sie in PowerShell die aktuelle Richtlinie, indem Sie den folgenden Befehl ausführen.

```
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”);
```

ADFS-Anspruchsregeln konfigurieren

Führen Sie zum Konfigurieren der ADFS-Anspruchsregeln die in den folgenden Abschnitten aufgeführten Schritte aus.

Erforderliche Forderungen

Die erforderlichen Ansprüche finden Sie in der folgenden Tabelle.

Tabelle 7: Erforderliche Forderungen

Forderung	Zweck	Quelle
E-Mail	Benutzer-ID	AD-Mail
Anzeigename	Vollständiger Name des Benutzers	AD-Anzeigename
UPN	PKI/Zertifikatauthentifizierung	ADFS ordnet das Clientzertifikat einem AD-Benutzer über UPN zu.
NameID	SAML-Betreff	Aus E-Mail umgewandelt
Gruppen	Rollenbasierter Zugriff	AD-Gruppenmitgliedschaft (Mitglied von)

Anspruchsregeln anwenden

1. Definieren Sie den Namen Ihres Vertrauens der vertrauenden Partei (z. B. "Cisco IQ - Production").

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

2. Definieren Sie Anspruchsregeln, um Benutzerinformationen und die Gruppenmitgliedschaft an Cisco IQ zu senden.

```
$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"] = '
@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. Wenden Sie die Anspruchsregeln an, indem Sie den folgenden Befehl ausführen:

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

Write-Host "Anspruchsregeln erfolgreich konfiguriert!" -ForegroundColor Grün

Warnung: Für jedes AD-Benutzerkonto muss das E-Mail-Attribut ausgefüllt werden. Wenn dieses Attribut fehlt, enthält die SAML-Assertion keinen E-Mail-Anspruch, was zu einer Ablehnung der Authentifizierung führt.

Um die E-Mail-Adresse eines Benutzers zu aktualisieren, führen Sie den folgenden PowerShell-Befehl aus:

```
Set-ADUser -Identity "
" -EmailAddress
"
"
```

Überprüfen von Benutzergruppen

1. Geben Sie den folgenden Befehl ein, um die Gruppenmitgliedschaft des Benutzers zu überprüfen:

```
$username = "username"
```

2. Führen Sie die folgenden Befehle aus, um das Benutzerkonto zu finden:

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

3. Anzeigen der Gruppen, zu denen der Benutzer gehört, mithilfe des folgenden Befehls:

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

Beispiel:

CN=Role - CXIQ Entwickler,OU=Rollengruppen,DC=dev,DC=local

Konfigurieren von ADFS, um dem SP-Signaturzertifikat zu vertrauen

1. Importieren Sie das SP-Zertifikat im ADFS-Server in den TrustedPeople-Speicher:

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

2. Wählen Sie eine der folgenden Optionen aus:



Anmerkung: Das SP-Zertifikat wird von einer internen Zertifizierungsstelle ausgestellt, die von ADFS nicht über die standardmäßige Vertrauenskette validiert werden kann.

- Globale Kettenvalidierung für diese vertrauende Partei deaktivieren

```
Set-AdfsRelyingPartyTrust `  
-TargetIdentifier "
```

","`

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

- Wenn das SP-Zertifikat von einer Zertifizierungsstelle ausgestellt wurde (nicht selbstsigniert), importieren Sie das ausstellende

Zertifizierungsstellenzertifikat in den Stammzertifikatspeicher.

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

3. Wenden Sie die Änderungen an, indem Sie den ADFS-Dienst neu starten.

ADFSrv für Neustart-Service

PKI-/Zertifikatauthentifizierung einrichten

In diesem Abschnitt wird beschrieben, wie Sie zertifikatbasierte (d. h. Smartcard- oder Softwarezertifikate) Authentifizierung neben Kennwörtern hinzufügen. Dieser Abschnitt kann übersprungen werden, wenn eine nur mit einem Kennwort durchgeführte Authentifizierung ausreichend ist.

Installieren der AD CS CA-Rolle

So installieren Sie die Zertifizierungsstellenrolle "AD Certificate Services (CS)":

1. Überprüfen Sie, ob in Ihrer Domäne bereits eine Enterprise CA vorhanden ist, indem Sie den folgenden Befehl ausführen:

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

Wenn der Befehl eine gültige Antwort zurückgibt, können Sie den Rest dieses Abschnitts überspringen. Ihre Umgebung ist bereits konfiguriert. Wenn der Befehl anzeigt, dass keine CA gefunden wurde, fahren Sie mit Schritt 2 fort.

2. Installieren Sie die Zertifizierungsstellenrolle, indem Sie den folgenden Befehl ausführen:

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

3. Konfigurieren Sie die CA-Rolle mit dem folgenden Befehl:

```
install-AdcsCertificationAuthority `
-CAType EnterpriseRootCA `
-CACommonName "
```

```
`,
-KeyLength 2048 `
-HashAlgorithmName SHA256 `
```

```
-CryptoProviderName "RSA#Microsoft Software Key Storage Provider" `
-ValidityPeriod Years `
-ValidityPeriodUnits 10 `
-Force
```

4. Überprüfen Sie die Installation, indem Sie den folgenden Befehl ausführen:

```
certutil -ca
```

5. Bestätigen Sie mit dem folgenden Befehl, dass der Dienst aktiv und erreichbar ist:

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

Konfigurieren einer Zertifikatvorlage

So konfigurieren Sie eine Zertifikatvorlage mit der erweiterten Clientauthentifizierungsschlüsselverwendung (Client Authentication Enhanced Key Usage, EKU):

1. Öffnen Sie `certsrv.msc`, und erweitern Sie den CA-Knoten.
2. Klicken Sie mit der rechten Maustaste auf Zertifikatvorlagen > Verwalten.
3. Duplizieren Sie die Benutzervorlage.



Anmerkung: Die integrierte Benutzervorlage ist nur dann funktionsfähig oder gültig, wenn das von ihr ausgestellte Zertifikat die Clientauthentifizierungs-EKU enthält.

4. Konfigurieren Sie die Einstellungen auf den folgenden Registerkarten:

- Allgemein: Geben Sie "CIQ User Authentication" in das Feld Name mit einer Gültigkeitsdauer von einem (1) Jahr ein.
- Anforderungsverarbeitung: Wählen Sie Signatur und Verschlüsselung aus der Dropdown-Liste Zweck aus, und aktivieren Sie das Kontrollkästchen Privaten Schlüssel exportieren zulassen.
- Betreffname: Wählen Sie Aus Active Directory-Informationen erstellen aus, und fügen Sie eine E-Mail in die Felder Betreff und SAN ein.

Warnung: Die Felder Betreff und SAN müssen den Benutzerprinzipalnamen (User Principal Name, UPN) oder eine E-Mail enthalten, die mit einem AD-Konto übereinstimmt. ADFS ordnet das Zertifikat mithilfe dieser Felder einem AD-Benutzer zu.

- Durchwahlen: Stellen Sie sicher, dass die Anwendungsrichtlinien "Client Authentication (1.3.6.1.5.5.7.3.2)" enthalten.
- Sicherheit: Hinzufügen von Domänenbenutzern und Gewähren von Lese- und Registrierungsberechtigungen

5. Veröffentlichen Sie die Vorlage mit dem folgenden Befehl:

```
Add-CATemplate -Name "CIQUserAuthentication" -Force
```

Registrieren eines Benutzerzertifikats

1. Melden Sie sich als Zielbenutzer an.

2. Registrieren Sie das Zertifikat mit dem folgenden Befehl:

```
certreq -enroll -user "CIQUserAuthentication"
```

3. Überprüfen Sie die Zertifikatinstallation, indem Sie den folgenden Befehl ausführen:

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

Exportieren eines Benutzerzertifikats aus Windows und Installieren auf dem Client (Mac)

So exportieren Sie ein Benutzerzertifikat von Windows nach Mac:

1. Exportieren Sie das Zertifikat von Windows als PFX-Datei, indem Sie die folgenden Befehle ausführen:

```
$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. Übertragen Sie die Datei user-cert.pfx auf Ihr Mac-Gerät.
3. Importieren Sie das Zertifikat in die Mac Keychain, indem Sie den folgenden Befehl ausführen:

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

”



Anmerkung: Nach dem Importieren des Zertifikats muss der Browser geschlossen und erneut geöffnet werden, damit das Zertifikat erkannt werden kann.

4. Vertrauen Sie der Zertifizierungsstelle auf dem Mac, indem Sie Folgendes ausführen:

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

Endpunkte für die Authentifizierung mit ADFS-Zertifikaten aktivieren

So aktivieren Sie Endpunkte für die ADFS-Zertifikatauthentifizierung:

1. Aktivieren Sie die erforderlichen ADFS-Zertifikatendpunkte, indem Sie die folgenden Befehle ausführen:

```
EEnable-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. Stellen Sie sicher, dass alle Endpunkte aktiviert sind, indem Sie den folgenden Befehl ausführen:

```
Get-AdfsEndpoint | Where-Object { $_.AddressPath -like "*cert*" } | Format-Table Address
```

Aktivieren der Zertifikatauthentifizierung als primäres Kriterium

So aktivieren Sie die Zertifikatsauthentifizierung als primäre Authentifizierung:

1. Konfigurieren Sie die primären Authentifizierungsanbieter für den Intranet- und Extranet-Zugriff mithilfe des folgenden Befehls:

```
Set-AdfsGlobalAuthenticationPolicy `
-PrimaryIntranetAuthenticationProvider @"CertificateAuthentication", "WindowsAuthenticat
-PrimaryExtranetAuthenticationProvider @"CertificateAuthentication", "FormsAuthenticat
```

2. Stellen Sie mithilfe der folgenden Befehle sicher, dass beide Listen CertificateAuthentication und FormsAuthentication enthalten:

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

3. Überprüfen Sie die aktuelle TLS-Client-Port-Konfiguration mit dem folgenden Befehl:

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

4. Wenn TlsClientPort nicht 49443 ist, aktualisieren Sie den Port, und starten Sie den ADFS-Dienst mithilfe der folgenden Befehle neu:

```
Set-AdfsProperties -TlsClientPort 49443
Restart-Service adfssrv
```

SChannel/TLS-Korrekturen (WICHTIG für PKI)

Mit den Schritten in den folgenden Abschnitten werden CERT_E_UNTRUSTEDROOT-Fehler (0x800B0109) behoben, die die Zertifikatauthentifizierung verhindern.

Binden von SSL-Zertifikaten an Port 49443

SSL-Zertifikate an Port 49443 binden:

1. Entfernen Sie alle vorhandenen SSL-Zertifikatsbindungen auf Port 49443, indem Sie den folgenden Befehl verwenden:

```
>netsh http delete sslcert  
hostnameport=
```

:49443

2. Erstellen Sie eine neue Bindung mit aktivierter Clientzertifikataushandlung, indem Sie den folgenden Befehl verwenden:

```
netsh http add sslcert hostnameport=
```

```
:49443 `  
certhash=
```

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

3. Überprüfen Sie, ob die Client-Zertifikataushandlung mit dem folgenden Befehl aktiviert ist:

```
http show sslcert  
hostnameport=
```

:49443

Löschen des Zertifikatspeichers (KRITISCH)

So bereinigen Sie den Zertifikatspeicher:

Warnung: Windows SChannel lehnt alle Clientzertifikate ab, wenn im vertrauenswürdigen Stammspeicher nicht selbstsignierte Zertifikate vorhanden sind. Dies ist die Hauptursache für PKI-Fehler.

1. Identifizieren Sie nicht selbstsignierte Zertifikate im Speicher für vertrauenswürdige Stammverzeichnisse, indem Sie den folgenden Befehl ausführen:

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

2. Verschieben Sie diese Zertifikate in den Zwischenspeicher der Zertifizierungsstelle, indem Sie den folgenden Befehl ausführen:

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

3. Vergewissern Sie sich, dass keine nicht selbstsignierten Zertifikate im Speicher für vertrauenswürdige Stammverzeichnisse verbleiben, indem Sie den folgenden Befehl ausführen:

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

SChannel-Registrierungsreparaturen (KRITISCH)

So konfigurieren Sie die SChannel-Registrierungseinstellungen, um eine ordnungsgemäße Zertifikatsauthentifizierung sicherzustellen:

1. Definieren Sie die Registrierungspfadvariable mit dem folgenden Befehl:

```
$regPath = "HKLM:"
```

2. Wenden Sie die in der Tabelle unten definierten Registrierungseinstellungen mithilfe der folgenden Befehle an:

```
Set-ItemProperty -Path $regPath -Name "ClientAuthTrustMode" -Value 2 -Type DWord  
Set-ItemProperty -Path $regPath -Name "SendTrustedIssuerList" -Value 0 -Type DWord
```

Tabelle 8: SChannel-Registrierungseinstellungen

Einstellung	Wert	Zweck
ClientAuthTrustMode	2	Aktiviert exklusive Zertifizierungsstellenvertrauensstellung, um den Standardüberprüfungspfad zu korrigieren.
VertrauenswürdigeAusstellerlisteSenden	0	Verhindert, dass der Server während des TLS-Handshakes die vollständige Liste vertrauenswürdiger Aussteller sendet.

Überprüfen des Zertifizierungsstellen-Zertifikatspeichers

So überprüfen Sie den Zertifikatspeicher der Zertifizierungsstelle:



Anmerkung: Das Zertifizierungsstellenzertifikat, das Benutzerzertifikate ausstellt, muss sich im SystemCertificatesStore befinden, um sicherzustellen, dass es richtig erkannt wird.

1. Definieren Sie den Fingerabdruck Ihres Zertifizierungsstellenzertifikats mit dem folgenden Befehl:

```
$caThumbprint = "
```

```
"
```

2. Stellen Sie sicher, dass das Zertifizierungsstellenzertifikat bereits im LocalMachineStore* vorhanden ist. Verwenden Sie hierzu den folgenden Befehl:

```
$exists = Test-Path "HKLM:\caThumbprint"
```

Wenn das Zertifikat nicht gefunden wird, importieren Sie es in den LocalMachine-Speicher:

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

Neustarten des ADFS-Servers (OBLIGATORISCH)

Starten Sie den ADFS-Server mit dem folgenden Befehl neu:

`Restart-Computer -Force`



Anmerkung: Die Registrierungsänderung von ClientAuthTrustMode wird erst nach dem Neustart des Servers wirksam.

ADFS-Metadaten exportieren

Sie können Ihre ADFS-Metadaten entweder über PowerShell oder Ihren Webbrowser herunterladen.

PowerShell

So exportieren Sie ADFS-Metadaten mit PowerShell:

1. Öffnen Sie PowerShell auf Ihrem ADFS-Server.
2. Führen Sie die folgenden Befehle aus, um die Metadaten-datei herunterzuladen.

```
$metadataUrl = (Get-AdfsEndpoint | Where-Object {$_.Protocol -eq "Federation Meta  
Invoke-WebRequest -Uri $metadataUrl.AbsoluteUri -OutFile "C:-metadata.xml"  
Write-Host "ADFS metadata exported to C:-metadata.xml" -ForegroundColor Green
```

Nach der Ausführung der Befehle wird die Metadaten-datei in C:-
metadaten.xml gespeichert.

Webbrowser

So exportieren Sie ADFS-Metadaten mit einem Webbrowser:

1. Navigieren Sie zu <https://<your-adfs-server>/FederationMetadata/2007-06/FederationMetadata.xml>, und ersetzen Sie "<your-adfs-server>" durch den Hostnamen Ihres ADFS-Servers.
2. Speichern Sie die XML-Metadaten-datei auf Ihrem Computer, wenn

Sie dazu aufgefordert werden.

Konfiguration im Cisco IQ

Konfiguration auf Cisco IQ:

1. Übertragen Sie adfs-metadaten.xml auf Ihre Workstation.
2. Navigieren Sie in Cisco IQ zu Systemeinstellungen > Systemkonfiguration > Identitätsanbieter.
3. Laden Sie die ADFS-Metadatendatei hoch, um das IDP-Zertifikat, die Element-ID und die SSO-URL automatisch zu extrahieren.
4. Speichern Sie die Konfiguration.



Anmerkung: Wenn ADFS einen automatischen Rollover für Tokensignaturzertifikate durchführt, müssen Sie die Metadatendatei erneut exportieren und in Cisco IQ hochladen, um eine kontinuierliche Authentifizierung sicherzustellen.

Hinzufügen von ADFS IDP

1. Klicken Sie auf der Seite Identitätsanbieter auf Identitätsanbieter hinzufügen.
2. Geben Sie den Namen des Identitätsanbieters ein.
3. Geben Sie die Domäne(n) ein (z. B. company.com).
4. (Optional) Aktivieren Sie ggf. die Umschalttaste Enable single logout (Einmaliges Abmelden aktivieren).
5. Ziehen Sie die aus der IDP-Anwendung erhaltene SAML-Metadatendatei per Drag-and-Drop in das Feld Upload IDP Metadata (IDP-Metadaten hochladen).
6. Klicken Sie auf Speichern.



Anmerkung: Der Status wird als "Incomplete" (Unvollständig) angezeigt, bis die Rollenzuordnung abgeschlossen ist. Dies ist ein erwartungsgemäßes Verhalten.

Konfigurieren der Rollenzuordnung

Bevor Sie mit der Konfiguration der Rollenzuordnung fortfahren, stellen Sie sicher, dass Sie Gruppen von AD finden, die für die Zuordnung verwendet

werden sollen. Führen Sie den folgenden PowerShell-Befehl aus, um Gruppen aus AD zu suchen:

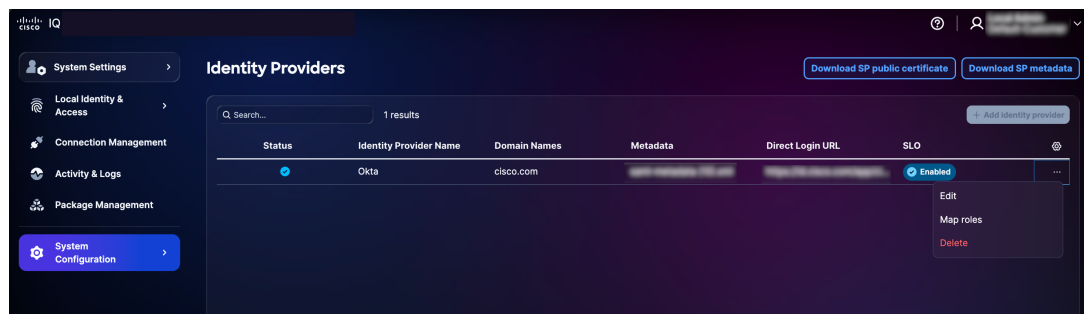
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = "(&(objectClass=group)(cn=Role - CXIQ*))"
$searcher.PropertiesToLoad.Add("distinguishedName") | Out-Null
$searcher.PropertiesToLoad.Add("cn") | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties["distinguishedname"]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

Das System fragt AD direkt über das Lightweight Directory Access Protocol (LDAP) ab und benötigt keine zusätzlichen Module. Die Gruppeninformationen werden im vollständigen Distinguished Name-Format zurückgegeben, z. B.:

CN=Role - CXIQ Developers, OU=Groups, DC=dev, DC=example, DC=com
CN=Role - CXIQ Viewers, OU=Groups, DC=dev, DC=example, DC=com

Wenn die erforderlichen Gruppen nicht aufgeführt sind, müssen sie von einem Kontoadministrator in AD erstellt werden, bevor Sie die ADFS-Rollenzuordnung abschließen können.

So konfigurieren Sie die Rollenzuordnung:



Rollenzuordnung

1. Wählen Sie aus dem hinzugefügten IDP das Symbol More Options (Weitere Optionen) > Map Roles (Rollen zuordnen). Die Seite Benutzerrollen zuordnen wird angezeigt.

Cisco IQ Link_IDP

X

Map identity provider roles to system roles to assign permissions.

Map user roles

IDP role	System role
	General Account...
	General Account...
	Select option
	Select option
	Select option

+ Add identity provider role

Save

Rollenzuordnung

2. Geben Sie eine IDP-Rolle für die ausgewählte Systemrolle ein.

Folgende Systemrollen werden unterstützt:

- Allgemeiner Kontoadministrator: Der allgemeine Kontoadministrator verfügt über alle Berechtigungen zum Ausführen aller Aktionen im Produkt. Die IDP-Rolle (analysierter Name) lautet CXIQ Admins.
- Allgemeine Kontoanzeige: Die allgemeine Kontoanzeige verfügt über schreibgeschützten Zugriff. Die IDP-Rolle (analysierter Name) ist CXIQ-Entwickler und CXIQ-Viewer.



Anmerkung: Verwenden Sie analysierte Namen (z. B. CXIQ-Entwickler) und keine vollständigen DNS.

3. Klicken Sie auf Speichern. Der Status wird auf Erfolgreich aktualisiert.

SChannel-Clientzertifikatstest

Öffnen Sie ein neues PowerShell-Fenster, und führen Sie den folgenden Befehl aus, um zu überprüfen, ob SChannel ordnungsgemäß für die Annahme von Client-Zertifikaten konfiguriert ist:

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

```
:49443/adfs/ls/"
```

Die erwartete Ausgabe ist eine HTTP-Antwort (z. B. eine Umleitung oder die ADFS-Seite). Tritt ein TLS-Handshake-Fehler auf, ist die Verbindung fehlgeschlagen.

End-to-End-Browsertest für PKI-Fluss

Bevor Sie mit End-to-End-Browser-Tests für den PKI-Fluss beginnen, stellen Sie sicher, dass das Benutzerzertifikat in MacOS Keychain installiert ist (siehe [Importieren des Benutzerzertifikats auf dem Client-Computer \(MacOS\)](#)). So testen Sie:

1. Navigieren Sie zur SAML-Anmelde-URL der Anwendung. Das ADFS stellt die Zertifikat- und Kennwortoptionen dar.
2. Wählen Sie Zertifikatsauthentifizierung aus. Der Browser fordert Sie zur Eingabe des Zertifikats auf.
3. Zertifikat hochladen Das ADFS authentifiziert den Benutzer, leitet die Anforderung mit einer SAML-Antwort um und erstellt eine neue Sitzung.

End-to-End-Browser-Tests auf Passwortfluss

Bevor Sie mit dem End-to-End-Browser-Testen des Kennwortflusses

beginnen:

1. Navigieren Sie zur SAML-Anmelde-URL der Anwendung. Das ADFS stellt die Zertifikat- und Kennwortoptionen dar.
2. Wählen Sie Kennwort/Formularauthentifizierung aus.
3. Geben Sie einen Benutzernamen ein.
4. Geben Sie ein Passwort ein.
5. Überprüfen Sie, ob die Anmeldung erfolgreich war.



Anmerkung: Beide Datenflüsse müssen gleichzeitig funktionieren.

Fehlerbehebung bei ADFS-Problemen

In der folgenden Liste werden häufige Probleme und mögliche Lösungen beschrieben, um Probleme im Zusammenhang mit dem ADFS-Status, Zertifikatfehlern, SSO-Anmeldefehlern und der SLO-Konfiguration schnell zu identifizieren und zu beheben.

Tabelle 9: ADFS-Probleme

Problem	Symptome / Beschreibung	Ursachen/Prüfungen/Problemumgehungen und Korrekturen
Nicht extrahierte Gruppen	Keine Rollen nach der Anmeldung	◦ Anspruchsregel fehlt: Führen Sie die Anweisungen unter Konfigurieren der ADFS-Anspruchsregeln erneut aus.
Entschlüsselung fehlgeschlagen	Fehler beim Entschlüsseln der Assertion in Protokollen.	Konfiguration der ADFS-Zertifikatkonfiguration überprüfen
Anmelde-Schleife	In Authentifizierungs- oder Anmelde-Schleife feststecken	◦ Ungültige ACS-URL: Überprüfung: https://your-fqdn/saml/acs ◦ Cookie-Konflikt: Browser-Cookies auf die richtige Domain überprüfen

Diagnosebefehle zur Fehlerbehebung

Um eine erfolgreiche Integration zwischen Ihrer ADFS-Umgebung und Cisco IQ sicherzustellen, verwenden Sie die folgenden Diagnosebefehle. Mit diesen Befehlen können der Zugriff auf Metadaten, die Zertifikatkonfigurationen und die Endpunkteinstellungen überprüft werden.

- Zugänglichkeit von ADFS-Metadaten überprüfen: bestätigt, dass die ADFS-Verbundmetadaten erreichbar und öffentlich zugänglich sind; Dies ist ein wichtiger Schritt zur Einrichtung des anfänglichen Vertrauens.

```
curl -k https://
```

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

- Validieren Sie das Verschlüsselungszertifikat: Stellt sicher, dass das richtige Verschlüsselungszertifikat mit dem Cisco IQ Relying Party Trust verknüpft ist

```
Get-AdfsRelyingPartyTrust -Name "Cisco IQ - Production" |  
Select-Object EncryptionCertificate | Format-List
```

- Überprüfen der SAML-Endpunktkonfiguration: Überprüft, ob die SAML-Endpunkte für die Cisco IQ-Vertrauensstellung richtig konfiguriert sind und Authentifizierungsanforderungen und -assertionen an die erwarteten URLs weitergeleitet werden

```
Get-AdfsRelyingPartyTrust -Name "Cisco IQ - Production" |  
Select-Object SamlEndpoints
```

Microsoft Entra ID SAML-Konfiguration für SSO

In diesem Abschnitt wird erläutert, wie Sie Microsoft Entra ID (Entra ID) als SAML IDP für Cisco IQ konfigurieren. Dabei werden sowohl kennwortbasierte als auch PKI- oder Certificate-Based Authentication (CBA) unterstützt.

Voraussetzungen für die Konfiguration von Entra ID SAML für SSO

- Entra ID-Tenant (z. B. "cigttestdev.onmicrosoft.com")
- Globaler Administrator oder Anwendungsadministrator mit Rollenzugriff auf Cisco IQ
- Verbindung zwischen Entra ID (Cloud) und Cisco IQ
- Enterprise CA installiert oder erreichbar (nur für PKI erforderlich)

- Der CRL-Verteilungspunkt (Certificate Revocation List) ist über das Internet erreichbar (nur für PKI erforderlich).

Tabelle 10: Konfiguration des Entra-ID-Servers

Posten	Beschreibung	Beispiel
Tenant-ID	Tenant-ID (Eingabe)	37352d8f-0ebe-4762-8161-8775ffe897cb
Cisco IQ-FQDN	Bereitstellungs- Hostname	<IHR CIQ-FQDN>
ID der IDP-Einheit	URL des Einwahl- Ausstellers	https://sts.windows.net/<TENANT-ID>/
IDP SSO-URL	SAML- Anmeldeendpunkt	https://login.microsoftonline.com/<TENANT-ID>/saml2
Firmendomäne	E-Mail-Domäne für Benutzer	<IHRE-DOMÄNE>

Konfiguration der Entra ID SAML-Anwendung

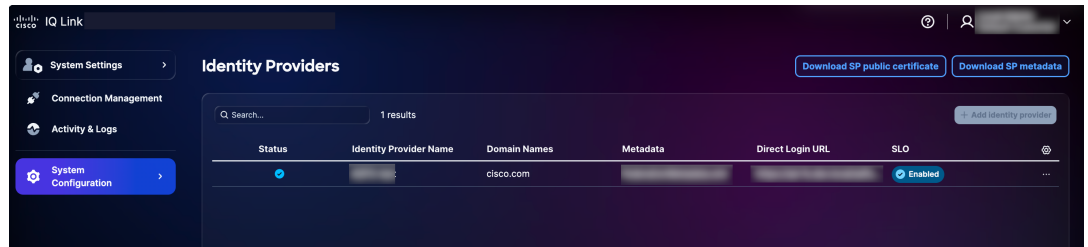
Erstellen einer Unternehmensanwendung

1. Melden Sie sich beim [Microsoft Entra Admin Center an](#).
2. Navigieren Sie zu Identität > Anwendungen > Unternehmensanwendungen.
3. Klicken Sie auf Neue Anwendung > Eigene Anwendung erstellen.
4. Geben Sie den Namen ein (z. B. "Cisco IQ").
5. Wählen Sie Alle anderen Anwendungen integrieren, die Sie nicht in der Galerie finden (nicht in der Galerie).
6. Klicken Sie auf Erstellen.

Konfigurieren der SAML-einmaligen Anmeldung

Um die SAML Single Sign-On zu konfigurieren, müssen Sie die SP-Metadatenfile hochladen. Sie können es erhalten, indem Sie die folgenden Schritte von VA ausführen:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Identitätsanbieter aus. Die Seite "Identitätsanbieter" wird angezeigt.



Download-Optionen

2. Klicken Sie auf SP-Metadaten herunterladen, um sie herunterzuladen. Diese heruntergeladene SP-Metadatendatei wird hochgeladen, um die Konfiguration der einmaligen Anmeldung (Single Sign-on, SAML) abzuschließen.
3. Klicken Sie auf die Schaltfläche Metadatendatei hochladen, um die SP-Metadatendatei hochzuladen. Die Daten aus der Metadatendatei des SP werden nach dem erfolgreichen Upload automatisch im SAML-basierten Bildschirm für einmalige Anmeldung angezeigt.

Sie können diese Angaben auch manuell eingeben, um die Einstellungen für die einmalige Anmeldung zu konfigurieren. So konfigurieren Sie die SAML-einmalige Anmeldung manuell:

4. Navigieren Sie in der Enterprise-Anwendung zu Single Sign-On, und wählen Sie SAML.
5. Klicken Sie im Abschnitt SAML-Basiskonfiguration auf Bearbeiten, und geben Sie Folgendes ein:
 - Kennung (Element-ID): <IHR CIQ-FQDN>
 - Antwort-URL (ACS-URL): https://<YOUR-CIQ-FQDN>/saml/acs
 - Anmelde-URL: https://<YOUR-CIQ-FQDN>/saml/login
 - Abmelde-URL: https://<YOUR-CIQ-FQDN>/saml/abmelden
6. Klicken Sie auf Speichern.



Anmerkung: Die Element-ID muss genau der von Cisco IQ als SP-Element-ID verwendeten ID entsprechen. Hierbei handelt es sich in der Regel um den FQDN der Bereitstellung.

7. Um SAML-Attribute und -Ansprüche zu konfigurieren, klicken Sie im Abschnitt Attribute und Ansprüche auf Bearbeiten.
8. Konfigurieren Sie die folgenden Ansprüche:

Tabelle 11: Erforderliche SAML-Ansprüche

Forderung	Quellattribut	Namespace
Eindeutige Benutzererkennung (NameID)	user.userprincipalname (standard)	
Email-Adresse	Benutzer.Mail	http://schemas.xmlsoap.org/ws/2005/05
Givenname	user.givenname	http://schemas.xmlsoap.org/ws/2005/05
Nachname	Benutzer.Nachname	http://schemas.xmlsoap.org/ws/2005/05
name	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05
Gruppen	user.assignedroles	(LEER — leerer Namespace)



Anmerkung: Für die Gruppen Anspruch:

- Verwenden Sie user.assignedroles als Quelle - nicht user.groups.
- Das Feld Namespace muss leer sein. Dadurch wird sichergestellt, dass der Attributname in der SAML-Assertion einfach Gruppen anstatt eines vollständigen URI (Uniform Resource Identifier) ist
- Fügen Sie keinen doppelten Gruppenanspruch mit user.groups hinzu, da dies Konflikte verursacht.

Konfigurieren von App-Rollen

App-Rollen werden in der App-Registrierung konfiguriert (nicht in der Enterprise-Anwendung). So konfigurieren Sie Anwendungsrollen:

1. Navigieren Sie zu Identität > Anwendungen > App-Registrierungen.
2. Suchen Sie Ihre Anwendung aus und wählen Sie sie aus.
3. Gehen Sie zu App-Rollen > App-Rolle erstellen.
4. Konfigurieren Sie für jede erforderliche Rolle Folgendes:
 - Anzeigename: Cisco IQ-Administratoren beispielsweise
 - Zulässige Membertypen: Benutzer/Gruppen
 - Wert: Cisco IQ-Administratoren beispielsweise
 - Beschreibung: Beispielsweise Cisco IQ-Administratoren
5. Klicken Sie auf Apply (Anwenden).



Anmerkung: Erstellen Sie Rollen, die Ihren Cisco IQ-Rollenzuordnungsanforderungen entsprechen (z. B. CXIQ-



Administratoren, CXIQ-Entwickler oder CXIQ-Viewer).

Anstelle von Gruppenansprüchen werden aus folgenden Gründen App-Rollen verwendet:

- Nur-Cloud-Tenants können Gruppen-Anzeigenamen ohne P1- oder P2-Lizenz nicht senden.
- sAMAccountName funktioniert nur für Gruppen, die von lokalen AD synchronisiert werden
- Die Group ID-Quelle sendet UUIDs (Universally Unique Identifier), deren Zuordnung schwierig ist.
- App-Rollen senden exakte Zeichenfolgenwerte, die den Erwartungen der Cisco IQ-Rolle entsprechen

Zuweisen von Benutzern zu Anwendungsrollen

So weisen Sie Benutzern App-Rollen zu:

1. Gehen Sie zurück zu Enterprise Application > Users and groups.
2. Klicken Sie auf Benutzer/Gruppe hinzufügen.
3. Wählen Sie die Benutzer aus, und weisen Sie die entsprechende App-Rolle zu.
4. Klicken Sie auf Zuweisen. Rollenwerte werden im SAML-Assertiongruppenattribut als lesbare Zeichenfolgen angezeigt.

IDP-Metadaten und -Zertifikat herunterladen

IDP-Metadaten und -Zertifikate herunterladen:

1. Wählen Sie in der Enterprise-Anwendung Single Sign-On > SAML Signing Certificate aus.
2. Verbundmetadaten-XML herunterladen (als entra-id-metadaten.xml speichern).

ODER

Laden Sie das Zertifikat (Base64) für die manuelle Zertifikatseingabe herunter.

3. Beachten Sie die folgenden Werte aus dem Abschnitt Einrichtung:
 - Anmelde-URL (IDP SSO-URL)

- Azure AD Identifier (IDP Entity ID)
- Abmelde-URL (IDP SLO-URL)



Anmerkung: Da die Entra-ID sich regelmäßig dreht, müssen Sie die Metadaten erneut herunterladen und bei jeder Änderung des aktiven Zertifikats in die VA hochladen, um einen unterbrechungsfreien SSO-Dienst sicherzustellen.

Hinzufügen von Entra ID IDP



Anmerkung: APISIX-Routen für SAML werden automatisch erstellt, wenn ein IDP im Cisco IQ hinzugefügt wird. Somit ist keine manuelle Routenkonfiguration erforderlich.

So fügen Sie Entra ID IDP hinzu:

1. Melden Sie sich bei VA als Kontoadministrator an.
2. Navigieren Sie zu Systemeinstellungen > Systemkonfiguration > Identitätsanbieter.
3. Klicken Sie auf Identitätsanbieter hinzufügen.
4. Geben Sie den Namen des IDP ein (z. B. "Entra ID").
5. Geben Sie die Domäne(n) ein (z. B. "ciqtestdev.onmicrosoft.com" oder Ihre Unternehmensdomäne).
6. (Optional) Aktivieren Sie ggf. die Umschalttaste Enable single logout (Einmaliges Abmelden aktivieren).
7. Ziehen Sie die Datei entra-id-metadates.xml, die von Entra ID abgerufen wurde, per Drag-and-Drop in das Feld Upload IDP Metadata (IDP-Metadaten hochladen).
8. Klicken Sie auf Speichern.



Anmerkung: Der Status bleibt "Incomplete" (Unvollständig), bis die Rollenzuordnung abgeschlossen ist. Dies ist das erwartete Verhalten.

Konfigurieren der Rollenzuordnung

So konfigurieren Sie die Rollenzuordnung:

1. Wählen Sie aus dem hinzugefügten IDP das Symbol More Options

(Weitere Optionen) > Map Roles (Rollen zuordnen). Die Seite Benutzerrollen zuordnen wird angezeigt.

2. Geben Sie eine IDP-Rolle für jede Systemrolle ein. Folgende Systemrollen werden unterstützt:

Tabelle 12: Systemrollen

Systemrolle	IDP-Rolle (Wert der App-Rolle)	Beschreibung
Allgemeiner_Account_Administrator	CXIQ-Administratoren	Vollständige Berechtigungen für alle Aktionen
Allgemeiner_Account_Viewer	CXIQ-Entwickler	Schreibgeschützter Zugriff
Allgemeiner_Account_Viewer	CXIQ-Viewer	Schreibgeschützter Zugriff



Anmerkung: Verwenden Sie die Zeichenfolgen für den Wert der App-Rolle genau so, wie in Entra ID konfiguriert (weitere Informationen finden Sie unter [Konfigurieren von App-Rollen](#)).

4. Klicken Sie auf Speichern. Der Status wird auf Erfolgreich aktualisiert.

Überprüfen des SAML-Ablaufs (Kennwortauthentifizierung)

So überprüfen Sie den SAML-Fluss:

1. Öffnen Sie einen Browser im Inkognito- oder Privat-Modus.
2. Navigieren Sie zu `https://<YOUR-CIQ-FQDN>/saml/login`.
3. Stellen Sie sicher, dass Sie zur Microsoft-Anmeldeseite weitergeleitet werden.
4. Authentifizieren Sie sich mit Ihren Anmeldeinformationen (und MFA, wenn konfiguriert).
5. Überprüfen Sie nach der Authentifizierung, ob Sie zurück zu `/saml/acs` geleitet werden und die Cisco IQ-Anwendung angezeigt wird.
6. Überprüfen Sie die Gruppenextraktion, indem Sie den folgenden Befehl ausführen:

```
kubectl -ncxue logs deployment/apisix -since=5m | grep -E "authentication success"
```

Erwartete Ausgabe

SAML 2.0-kompatible Authentifizierung erfolgreich für Benutzer:
user@domain.com mit vollständigem Namen: K/A und 1 Gruppe

Extrahierte Gruppe: CXIQ-Administratoren (ursprünglich: CXIQ-Administratoren)

Insgesamt extrahierte Gruppen: 1

Konfigurieren der zertifikatbasierten Authentifizierung

In diesem Abschnitt wird beschrieben, wie Sie neben Kennwörtern auch eine CBA hinzufügen. Dieser Abschnitt kann übersprungen werden, wenn eine nur mit einem Kennwort durchgeführte Authentifizierung ausreichend ist.

Voraussetzungen für CBA

- Windows Server mit AD CS mit konfigurierter Enterprise-CA (z. B. "DEV-ADCS-CA")
- PowerShell-Administratorzugriff auf dem CA-Server
- Das Zertifikat-UPN muss mit der Entra-ID userPrincipalName übereinstimmen.
- Der Zugriff auf den CRL Distribution Point muss über das Internet möglich sein.

Erstellen einer Zertifikatvorlage in AD CS

1. Öffnen Sie certtmpl.msc auf dem Zertifizierungsstellenserver.
2. Duplizieren Sie die Benutzervorlage, und nennen Sie sie "EntraUserCert".
3. Konfigurieren Sie die Vorlage:
 - Allgemein: Anzeigename EntraUserCert, Gültigkeit 1-2 Jahre
 - Anforderungsverarbeitung: Zweck = Signatur und Verschlüsselung
 - Betreffname: Wählen Sie in der Anforderung "Bedarfsdeckung"
 - Durchwahlen: Die Anwendungsrichtlinien müssen die Clientauthentifizierung (1.3.6.1.5.5.7.3.2) umfassen.

- Sicherheit: Authentifizierten Benutzern Lese- und Registrierungsberechtigungen gewähren

4. Veröffentlichen Sie die Vorlage mit dem folgenden Befehl:

```
Add-CATemplate -Name "EntraUserCert" -Force
```

Anfordern und Ausstellen eines Benutzerzertifikats

1. Erstellen Sie eine Zertifikatskonfigurationsdatei (INF) (z. B. C:-cert.inf) mithilfe des folgenden PowerShell-Skripts:

```
@"
[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. Ersetzen Sie <USER-UPN> durch Ihre Entra-ID UPN (z. B. user@ciqtestdev.onmicrosoft.com).

3. Führen Sie zum Generieren des Zertifikats die folgenden Befehle aus:

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

4. Führen Sie den folgenden Befehl aus, um die Anforderung an die Zertifizierungsstelle zu senden:

```
certreq -submit -config “
```

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

5. Führen Sie den folgenden Befehl aus, um das Zertifikat in der Zertifizierungsstelle zu installieren:

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

Exportieren von Zertifikaten

Führen Sie das folgende Skript aus, um das Benutzerzertifikat als PFX-Datei (für den Client) zu exportieren:

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

```
  *” }
```

```
$password = ConvertTo-SecureString -String “
```

```
  ” -Force -AsPlainText
```

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

Führen Sie das folgende Skript aus, um das Zertifikat für den

Zertifizierungsstellen-Stamm (für die Entra-ID) zu exportieren:

```
Get-ChildItem Cert: | Where-Object { $_.Subject -like "*"
    *"} } |
Select-Object -First 1 | Export-Certificate -FilePath C:-root.cer -Type CERT
```

Benutzerzertifikat auf Client-Computer (MacOS) importieren

Führen Sie den folgenden Befehl aus, um das Benutzerzertifikat (PFX) zu importieren:

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

"
```

Führen Sie den folgenden Befehl aus, um das CA-Stammzertifikat zu importieren:

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

So legen Sie das Zertifizierungsstellenzertifikat auf Always Trust in Keychain Access fest:

1. Öffnen Sie Keychain Access.
2. Suchen Sie das Zertifizierungsstellenzertifikat, und klicken Sie auf Informationen abrufen.
3. Wählen Sie unter Vertrauenswürdig die Option Immer vertrauen aus.

 Anmerkung: Beenden Sie nach dem Importieren den Browser, und öffnen Sie ihn erneut, damit das Zertifikat erkannt wird.

Hochladen des CA-Stammzertifikats in die Entra-ID

1. Melden Sie sich beim [Microsoft Entra Admin Center](#) an.
2. Navigieren Sie zu Schutz > Sicherheit > Zertifizierungsstellen.
3. Klicken Sie auf Hochladen, und wählen Sie die Datei ca-root.cer aus.
4. Markieren Sie es als Stammzertifikat der Zertifizierungsstelle.
5. Geben Sie die URL des Zertifikatssperrlisten-Verteilungspunkts ein (muss öffentlich erreichbar sein).

Aktivieren von CBA bei Entra-ID-Authentifizierungsmethoden

1. Navigieren Sie zu Schutz > Authentifizierungsmethoden > Richtlinien.
2. Klicken Sie auf Zertifikatsbasierte Authentifizierung, um sie zu konfigurieren.
3. Aktivieren Sie CBA, und fügen Sie die Zielbenutzer oder -gruppen hinzu.
4. Legen Sie unter Konfigurieren die Schutzstufe auf Einzelfaktor-Authentifizierung fest.

Konfigurieren der Benutzernamenbindung

Wechseln Sie in der CBA-Konfiguration zur Registerkarte Username binding, und legen Sie die folgende Bindung fest:

- Zertifikatfeld: PrincipalName
- Benutzerattribut: BenutzerPrincipalName

Dadurch wird der UPN im SAN des Zertifikats (Subject Alternative Name) dem Entra-ID-Benutzer zugeordnet.

Überprüfen des CBA-Datenflusses

1. Öffnen Sie einen Browser im Inkognito- oder Privat-Modus.
2. Navigieren Sie zu <https://<YOUR-CIQ-FQDN>/saml/login>.
3. Geben Sie auf der Microsoft-Anmeldeseite die E-Mail-Adresse des Benutzers ein, und klicken Sie auf Weiter.
4. Wählen Sie Zertifikat oder Smartcard verwenden (oder Sie werden automatisch dazu aufgefordert).

5. Wählen Sie das entsprechende Benutzerzertifikat aus, wenn der Browser zur Zertifikatauswahl auffordert.
6. Überprüfen Sie, ob die Entra-ID das Zertifikat validiert, mit einer SAML-Antwort umleitet und eine Sitzung erstellt.

 **Anmerkung:** Stellen Sie sicher, dass Sie das richtige Clientzertifikat auswählen. Wenn Sie ein falsches Zertifikat auswählen (z. B. ein Zertifikat eines anderen Benutzers oder ein abgelaufenes Zertifikat), tritt ein Authentifizierungsfehler auf.

Fehlerbehebung bei Entra-ID-Problemen

Die folgende Liste enthält allgemeine Probleme und mögliche Lösungen, um Probleme im Zusammenhang mit der Entra ID SAML-Konfiguration schnell zu identifizieren und zu beheben.

Tabelle 13: Fehlerbehebung

Problem	Ursache	Beheben
Ungültige SAML-Antwort - fehlende E-Mail	SAML-Assertion hat keine NameID oder kein E-Mail-Attribut	Überprüfen Sie die Entra ID-Anspruchskonfiguration (weitere Informationen finden Sie unter Konfigurieren der SAML-einmaligen Anmeldung). Überprüfen Sie, ob das E-Mail-Attribut des Benutzers ausgefüllt ist. Verwenden Sie <code>user.assignedroles</code> als Quelle.
Insgesamt extrahierte Gruppen: 0	Gruppenansprüche nicht konfiguriert oder falsche Quelle	Stellen Sie sicher, dass der Benutzer einer App-Rolle zugewiesen ist (weitere Informationen finden Sie unter Zuweisen von Benutzern zu App-Rollen).
Doppelte Gruppenansprüche	Sowohl <code>user.groups</code> als auch <code>user.assignedroles</code> aktiv	Entfernen Sie den <code>user.groups</code> -Anspruch. Behalten Sie nur <code>user.assignedroles</code> bei.
Gruppen werden als UUIDs angezeigt	Quellattribut ist "Gruppen-ID"	Verwenden Sie den Ansatz "Anwendungsrollen" (weitere Informationen finden Sie unter Konfigurieren von

Problem	Ursache	Beheben
Attributname zeigt langen URI an	Namespace-Feld ist nicht leer.	Anwendungsrollen). Löschen Sie das Feld Namespace in den Gruppenanspruchseinstellungen.
Ungültige SAML-Signatur	IdP-Zertifikat gedreht oder stimmt nicht überein	Laden Sie die Metadaten erneut von der Entra-ID herunter, und laden Sie sie erneut in Cisco IQ hoch. Veröffentlichen Sie die Zertifikatsperrliste unter einer öffentlich zugänglichen URL, oder verwenden Sie den selbstsignierten Zertifizierungsstellenansatz (weitere Informationen finden Sie unter CRL Workaround for Reachability Issues (Umgehung der Verfügbarkeit)).
ADSTS500191	CRL vom Internet aus nicht erreichbar	Vergewissern Sie sich, dass das Benutzerzertifikat in MacOS Keychain Access importiert wird (weitere Informationen finden Sie unter Import the User Certificate on Client Machine (MacOS)), CBA wird in Entra ID mit den erforderlichen Einstellungen aktiviert (weitere Informationen finden Sie unter Entra ID Authentication Methods unter Entra ID Authentication Methods) und Chrome wird neu gestartet, um Änderungen anzuwenden.
Zertifikat nicht angefordert	Zertifikat nicht in Schlüsselbund, CA auf Client nicht vertrauenswürdig oder CBA nicht aktiviert	Erhöhen Sie clock_skew_seconds in der Plugin-Konfiguration (der Standardwert ist 300; 30000 für die Übung verwenden)
SAML-Assertion abgelaufen	Schrägstellung der Uhr zwischen den Systemen	Vollständige Rollenzuordnung (weitere Informationen finden Sie unter Konfigurieren der Rollenzuordnung).
Status "Unvollständig" in virtueller Appliance	Rollenzuordnung noch nicht konfiguriert	

Umgehung der Sperrliste für Probleme mit der Erreichbarkeit

Wenn der CRL Distribution Point Ihrer Zertifizierungsstelle nicht über das Internet erreichbar ist (was in Laborumgebungen üblich ist), verwenden Sie eine selbstsignierte Zertifizierungsstelle ohne die Anforderungen für die Sperrliste:

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

", `
-CertStoreLocation "Cert:" `
-Signer $rootCA `
-KeyUsage DigitalSignature `
-KeyLength 2048 `
-NotAfter (Get-Date).AddYears(2) `
-TextExtension @(
"2.5.29.37={text}1.3.6.1.5.5.7.3.2",
"2.5.29.17={text}upn=

&email=

"
)
)
```

Laden Sie nur das Zertifikat der Stammzertifizierungsstelle in die Entra-ID hoch. Da es selbstsigniert ist und über kein Cisco Discovery Protocol (CDP) verfügt, wird für Entra ID keine CRL-Validierung versucht.

Abschließen der Setup-Checkliste

In diesem Abschnitt wird eine vollständige Setup-Checkliste für die Konfiguration der VA mit der Microsoft Entra ID SAML-Anwendung und der optionalen CBA beschrieben.

Setup der Eingangs-ID-SAML-Anwendung

- Enterprise-Anwendung (ohne Galerie) in Entra-ID erstellen
- Konfigurieren einer SAML-Basiskonfiguration durch manuelle Eingabe von SP-Metadaten
- Konfigurieren von Attributen und Ansprüchen (einschließlich E-Mail, Name und Gruppen mit user.assignedroles)
- App-Rollen bei der App-Registrierung erstellen
- Zuweisen von Benutzern zu Anwendungsrollen
- Verbundmetadaten-XML herunterladen

Cisco IQ-Konfiguration

- Hinzufügen eines IDP in Cisco IQ durch Hochladen von Entra ID-Metadaten
- Konfigurieren Sie die Rollenzuordnung, um den Cisco IQ-Systemrollen App-Rollenwerte zuzuordnen.
- Überprüfung, ob die kennwortbasierte Anmeldung durchgängig funktioniert
- Überprüfen, ob Gruppen in Protokollen richtig extrahiert wurden

Zertifikatbasierte Authentifizierung (optional)

- Zertifikatvorlage auf AD CS mit Clientauthentifizierungs-EKU erstellen
- Geben Sie ein Benutzerzertifikat mit einer UPN aus, die mit dem Entra-ID-Benutzer übereinstimmt.
- Exportieren eines Benutzerzertifikats als PFX-Datei und Installation auf dem Client-Computer
- Vertraut dem Zertifizierungsstellenzertifikat auf dem Clientcomputer
- Laden Sie das CA-Stammzertifikat unter Schutz > Zertifizierungsstellen in die Entra-ID hoch.
- Aktivieren des CBA in den Authentifizierungsmethoden

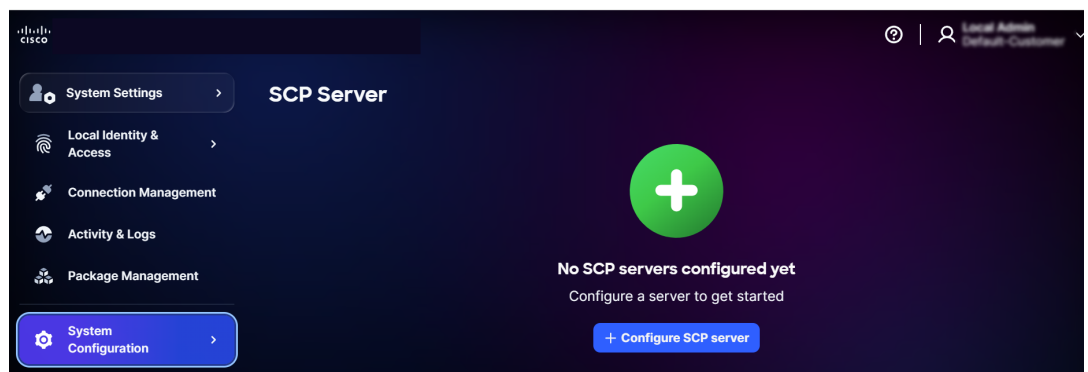
- Konfigurieren der Bindung des Benutzernamens (PrincipalName und userPrincipalName)
- Überprüfung, ob die CBA-Anmeldung durchgängig funktioniert

SCP-Server hinzufügen

Ein SCP-Server ist eine Voraussetzung für den Import von Upgrade-Dateien, die zum Hinzufügen, Aktualisieren oder Reparieren der Cisco IQ-Installation erforderlich sind.

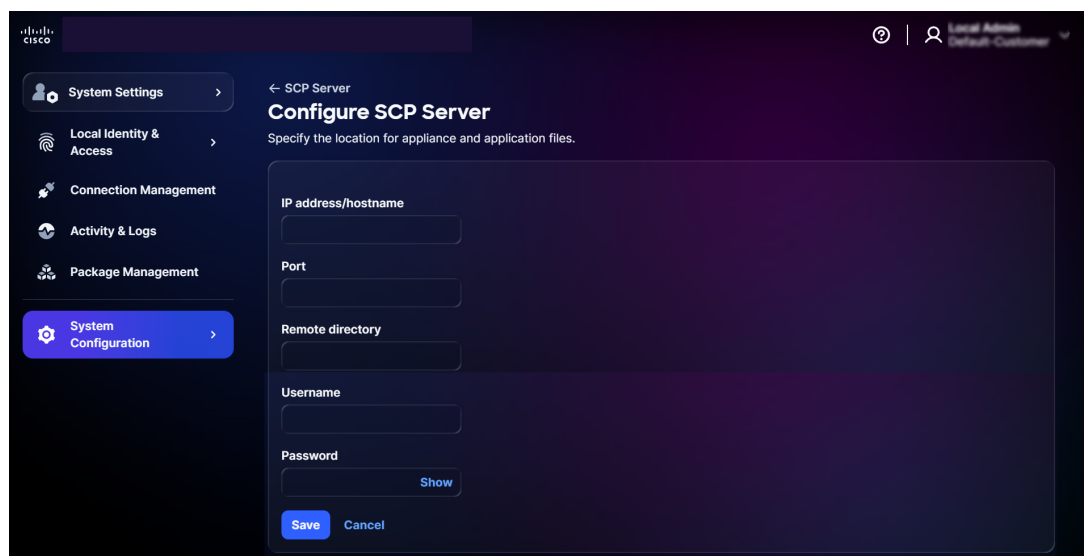
SCP-Server hinzufügen:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > SCP-Server aus. Die Seite SCP Server wird angezeigt.



SCP-Server-Startseite

2. Klicken Sie auf SCP-Server konfigurieren. Die Seite "SCP-Server konfigurieren" wird angezeigt.



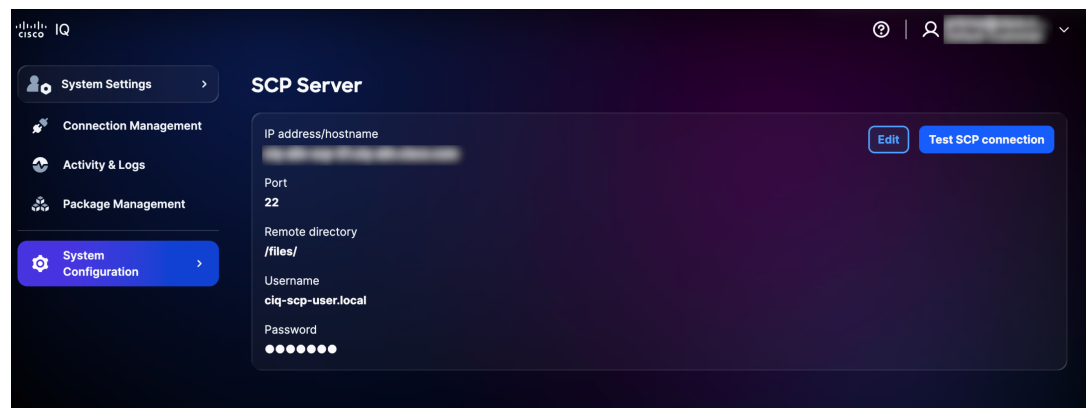
SCP-Server konfigurieren

3. Geben Sie eine IP-Adresse/einen Hostnamen ein.
4. Geben Sie einen Port ein.
5. Geben Sie ein Remote-Verzeichnis ein.
6. Geben Sie einen Benutzernamen ein.
7. Geben Sie ein Kennwort ein.
8. Klicken Sie auf Speichern. Es wird eine Bestätigung angezeigt.

Bearbeiten eines vorhandenen SCP-Servers

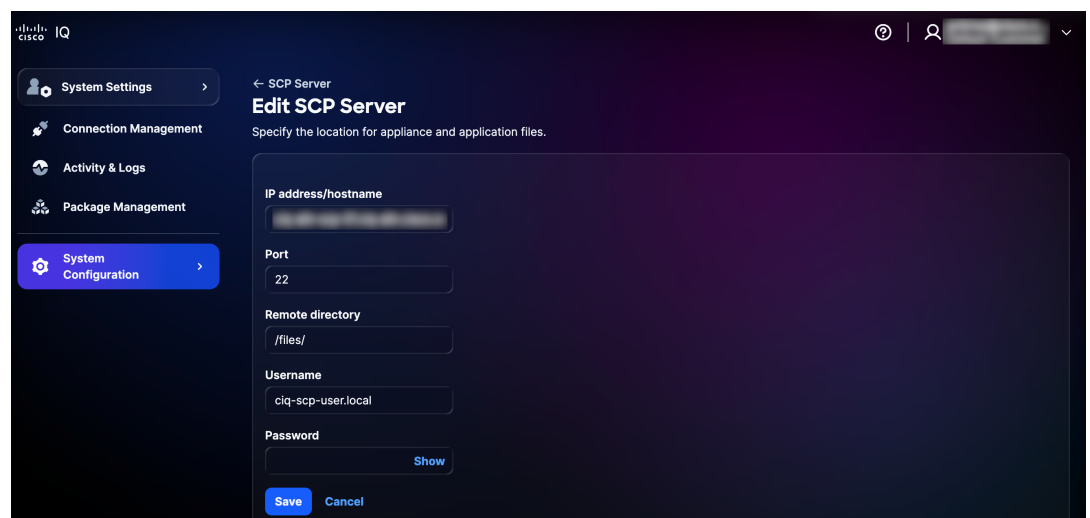
So bearbeiten Sie einen vorhandenen SCP-Server:

1. Navigieren Sie zur Seite SCP-Server.



SCP-Server hinzugefügt

2. Klicken Sie auf Edit (Bearbeiten) des gewünschten vorhandenen SCP-Servers.



SCP-Server bearbeiten

3. Ändern Sie die Details nach Bedarf.

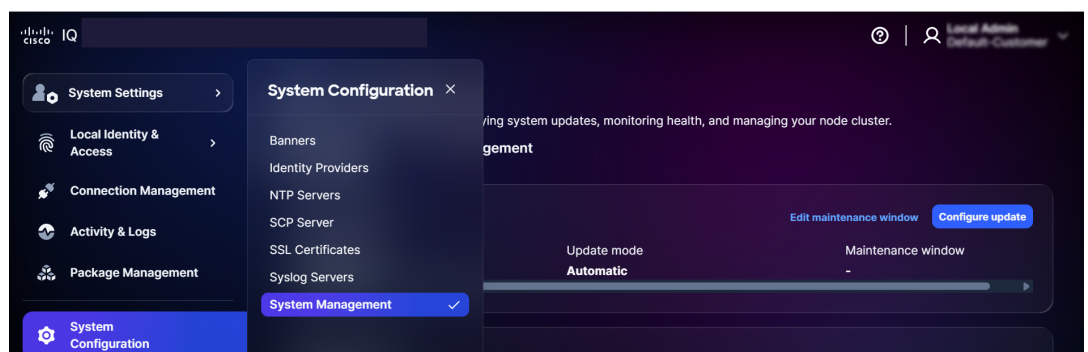
4. Klicken Sie auf Speichern.

Systemverwaltung

Sie können über die Benutzeroberfläche ein Upgrade auf die neueste Cisco IQ VA-Version durchführen. Sie können dies auch auf der Seite Cisco IQ Data Connectors überprüfen.

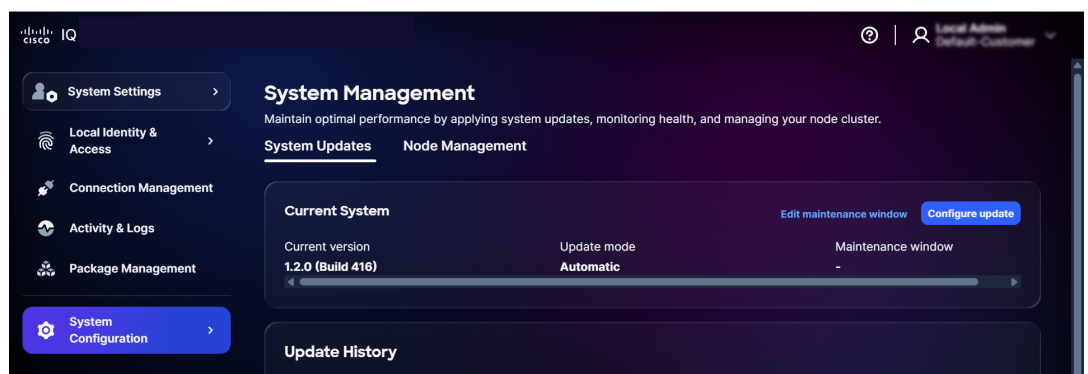
Neuplanung der Systemaktualisierung

So planen Sie die Systemaktualisierung neu:



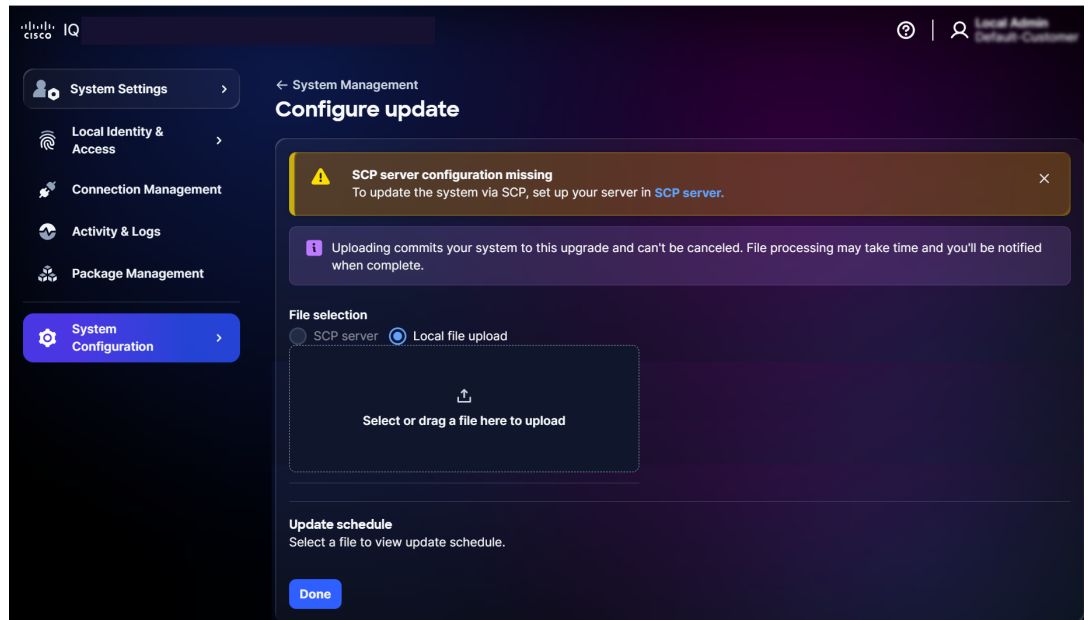
Systemverwaltung

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Systemverwaltung aus. Die Seite Systemverwaltung wird angezeigt. Auf dieser Seite wird die Systemversion angezeigt, die derzeit ausgeführt wird. Wenn keine Updates konfiguriert wurden, ist der Abschnitt Aktualisierungsverlauf leer.



System-Upgrade

2. Klicken Sie auf Update konfigurieren. Die Seite Update konfigurieren wird angezeigt.



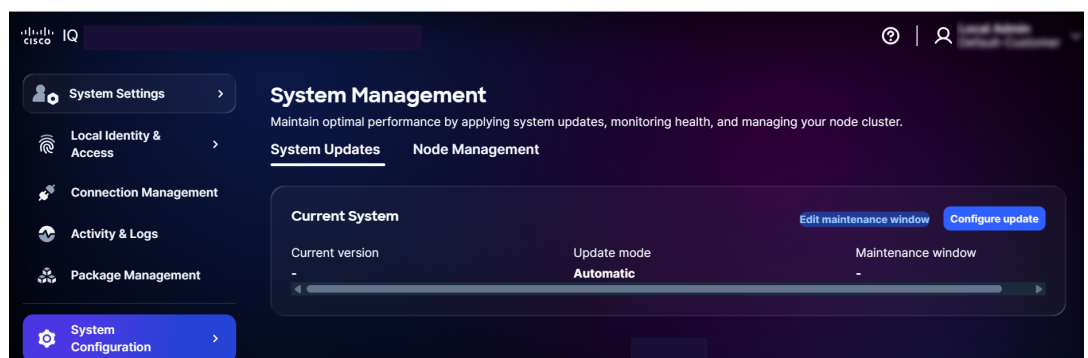
Upgrade konfigurieren

3. Wählen Sie den Aktualisierungszeitplan aus, um einen anderen Zeitpunkt zu planen.
4. Warten Sie, bis der Datei-Upload abgeschlossen ist. Die Dauer hängt von der Paketgröße und der Netzwerkgeschwindigkeit ab.

Bestätigen Sie die erfolgreiche Aktualisierung, indem Sie das Häkchen in der Spalte Update Status (Aktualisierungsstatus) überprüfen.

Bearbeiten von Systemaktualisierungsplänen

Sie können einen benutzerdefinierten Zeitplan für System-Upgrades erstellen. Wenn ein benutzerdefinierter Zeitplan konfiguriert wird, erfolgen Upgrades zu benutzerdefinierten Daten, sofern sie innerhalb der maximalen Kulanzfrist erfolgen. So erstellen Sie einen Zeitplan für das System-Upgrade:



Wartung bearbeiten

1. Klicken Sie im Abschnitt Aktuelles System auf der Seite Systemverwaltung auf Wartungsfenster bearbeiten.

Edit maintenance window

Select the day and time to reserve for future updates. If an update can't be completed during the maintenance window, it will occur on the last day of the grace period.

Day

Time

▼

hh:mm

⌚

IST

Cancel

Save

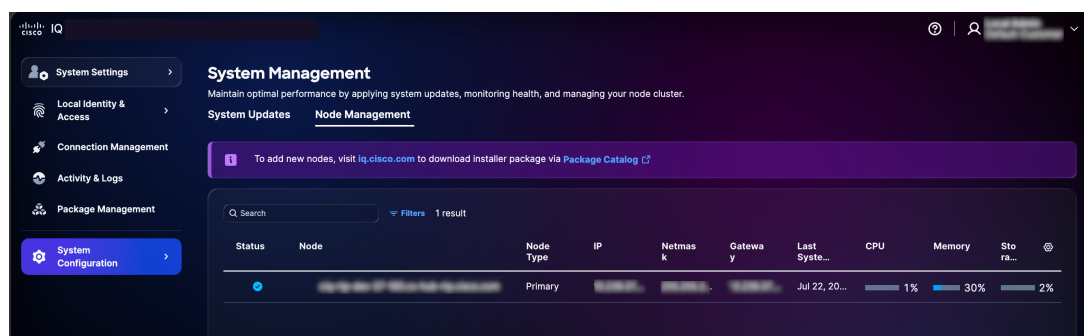
Wartungsfenster bearbeiten

2. Wählen Sie eine Option aus den Dropdown-Listen Tag und Uhrzeit aus.
3. Klicken Sie auf Speichern. Das Wartungsfenster wurde erfolgreich geplant. Die Aktualisierung wird entsprechend dem angezeigten Zeitplan ausgelöst.

 Anmerkung: Wenn kein Aktualisierungszeitplan konfiguriert ist, beträgt die Frist für Upgrades ohne Neustart standardmäßig zwei (2) Wochen und für Upgrades ohne Neustart vier (4) Wochen. Nach diesen Kulanzperioden müssen die Updates manuell durchgeführt werden. Bei einem Upgrade-Fehler führt das System bis zu zwei (2) automatische Wiederholungsversuche durch. Ein dritter Versuch ist geplant, erfordert jedoch die manuelle Initiierung.

Knotenverwaltung

1. Navigieren Sie zu Systemkonfiguration > Systemverwaltung > Knotenverwaltung, um die Knoten im Cluster anzuzeigen und zu verwalten.



The screenshot shows the 'System Management' interface with the 'Node Management' tab selected. A message at the top states: 'To add new nodes, visit iq.cisco.com to download installer package via Package Catalog'. Below this is a table with 11 columns: Status, Node, Node Type, IP, Netmask, Gateway, Last System Update, CPU, Memory, Storage, and Actions. One node is listed with a status of 'Online' (blue dot) and a node type of 'Primary'.

Status	Node	Node Type	IP	Netmask	Gateway	Last System Update	CPU	Memory	Storage	Actions
Online	10.10.10.10	Primary	10.10.10.10	255.255.255.0	10.10.10.1	Jul 22, 2023	1%	30%	2%	

Knotenverwaltung

2. In der Knotenliste werden der Status, der Hostname, der Knotentyp, die IP-Adresse, die Netzmaske, das Gateway und die Uhrzeit der

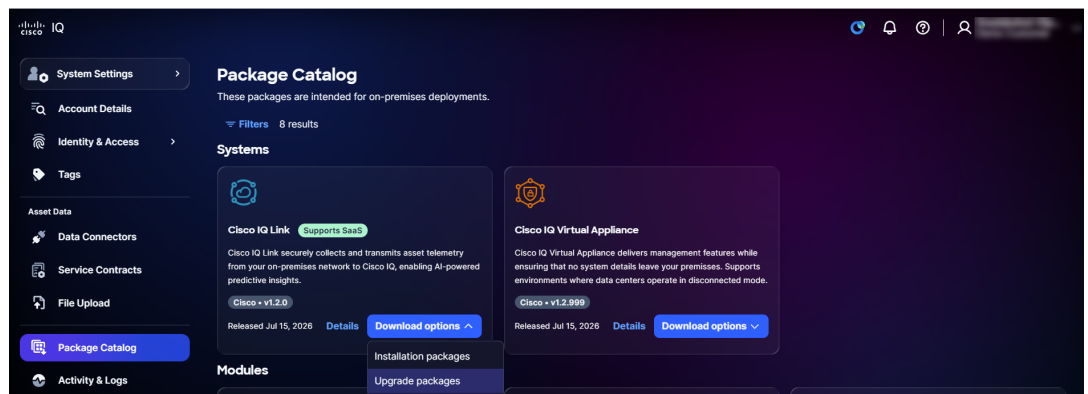
letzten Synchronisierung jedes Knotens angezeigt.

 Anmerkung: Ein blaues Häkchen in der Spalte Status zeigt an, dass der Knoten aktiv ist.

Manuelles Aktualisieren des Systems

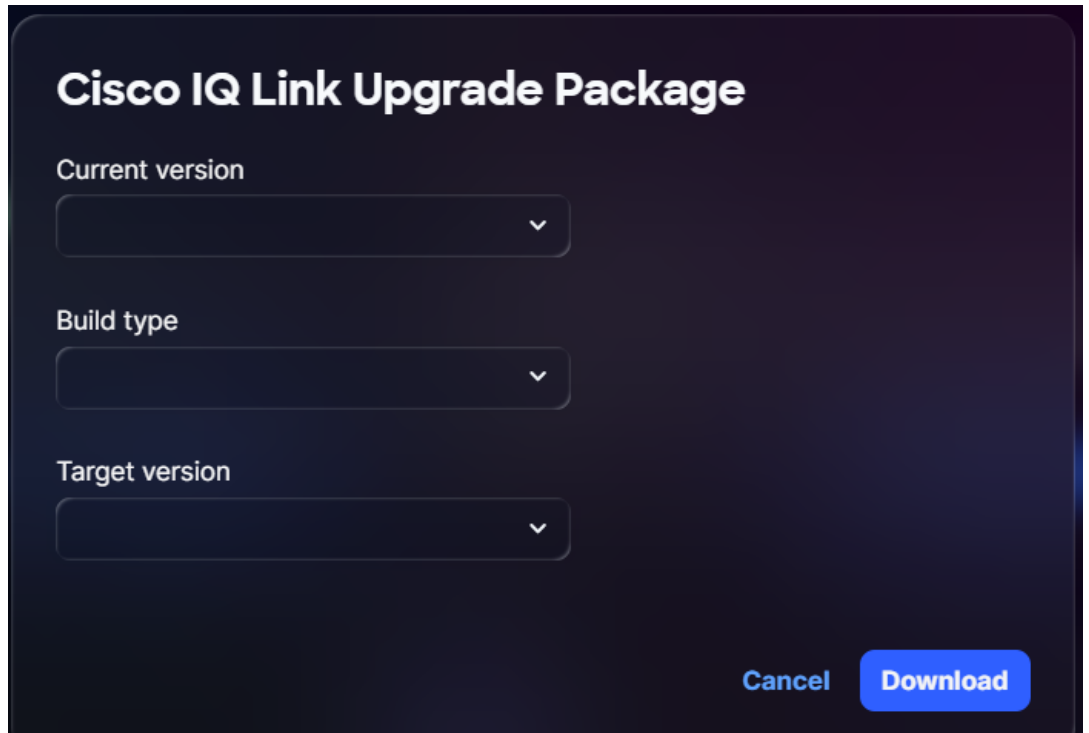
In Szenarien, in denen die automatische Verteilung über Cisco IQ SaaS entweder nicht verfügbar ist oder verzögert wird, können Sie ein System-Upgrade manuell durchführen, indem Sie das Upgrade-Paket direkt von Cisco IQ SaaS herunterladen. So aktualisieren Sie das System manuell:

1. Melden Sie sich bei [Cisco IQ SaaS an](#).
2. Navigieren Sie zu Startseite > Systemeinstellungen > Paketkatalog.



Softwarekatalog

3. Klicken Sie in der Cisco IQ Virtual Appliance Card auf Download options > Upgrade packages.

A dark-themed dialog box titled "Cisco IQ Link Upgrade Package". It contains three dropdown menus: "Current version", "Build type", and "Target version". At the bottom right, there are two buttons: "Cancel" and "Download".

Cisco IQ Link Upgrade Package

Current version

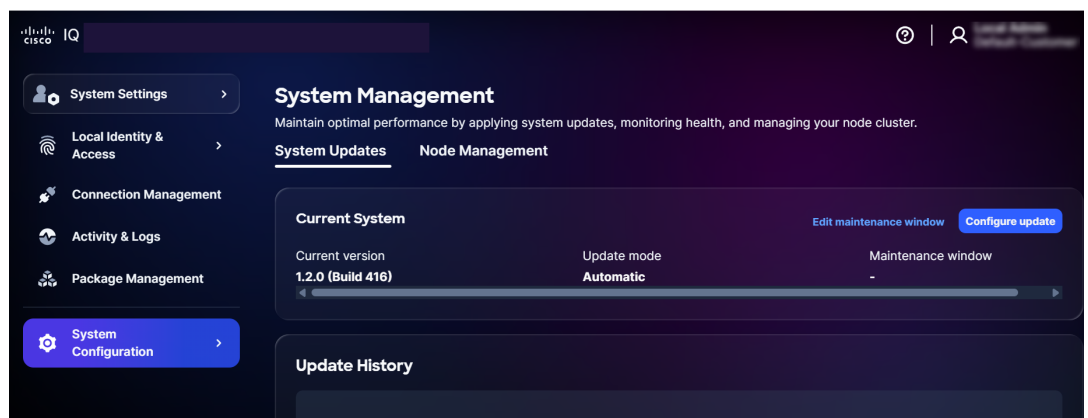
Build type

Target version

Cancel Download

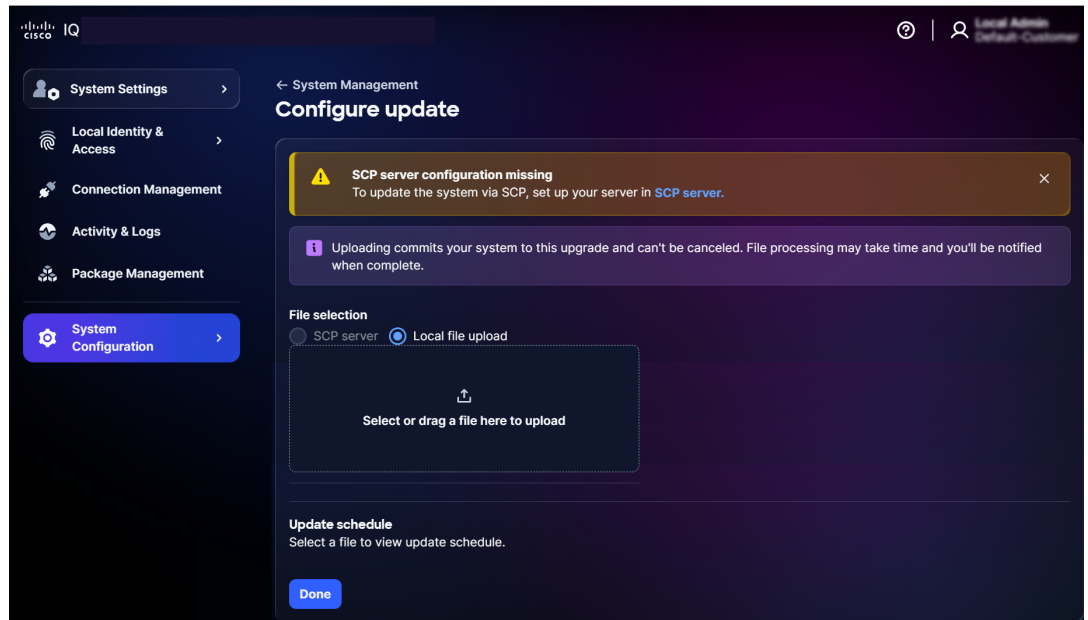
Upgrade-Paket

4. Wählen Sie die aktuelle Version aus der Dropdown-Liste aus.
5. Wählen Sie den Buildtyp aus der Dropdown-Liste aus.
6. Wählen Sie die Zielversion aus der Dropdown-Liste aus.
7. Klicken Sie auf Download (Herunterladen). Das Upgrade-Paket wird heruntergeladen.
8. Navigieren Sie zur Cisco IQ VA.
9. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Systemverwaltung aus.



Update konfigurieren

10. Klicken Sie auf Update konfigurieren.



Hochladen lokaler Dateien

11. Klicken Sie auf das Optionsfeld Lokaler Datei-Upload.
12. Wählen Sie die heruntergeladene Upgrade-Paketdatei aus, oder ziehen Sie sie in das Uploadfeld.
13. Warten Sie, bis der Datei-Upload abgeschlossen ist. Die Dauer hängt von der Paketgröße und der Netzwerkgeschwindigkeit ab.

Konfiguration von SSL-Zertifikaten

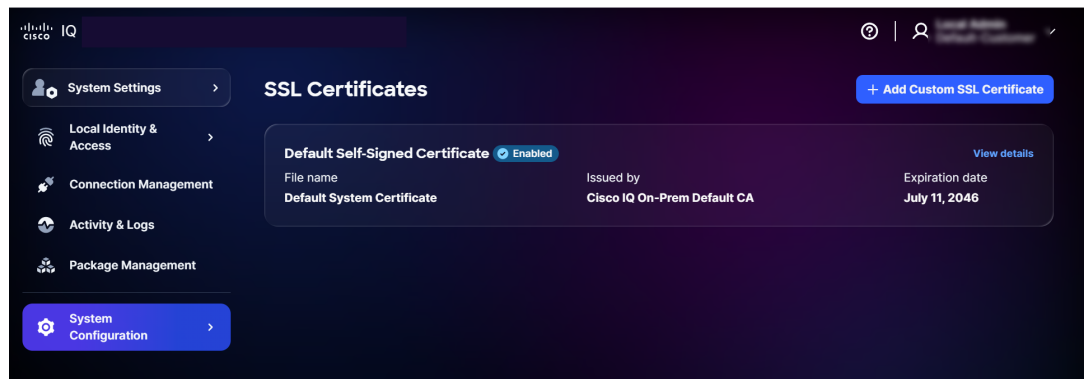
Ein standardmäßig selbst signiertes Zertifikat ist vorinstalliert und in Cisco IQ aktiviert. Sie können jedoch optional benutzerdefinierte SSL-Zertifikate hochladen. Wenn ein benutzerdefiniertes SSL-Zertifikat aktiviert ist, wird es für HTTPS-Verbindungen verwendet. Wenn das Zertifikat deaktiviert oder gelöscht wird, wird automatisch das Standardzertifikat wiederhergestellt. Das SSL-Standardzertifikat kann nicht bearbeitet oder gelöscht werden.

 Anmerkung: Das Zertifikat muss noch mindestens 90 Tage gültig sein. Ein Zertifikat gilt als "bald abgelaufen", wenn es weniger als 90 Tage bis zum Ablauf hat. Nachdem Sie ein SSL-Zertifikat hinzugefügt, bearbeitet oder gelöscht haben, müssen Sie das neue SSL-Zertifikat hochladen, wie unter [SLO-Konfiguration abschließen](#) für den Okta IDP oder den ADFS IDP beschrieben.

Hinzufügen eines benutzerdefinierten SSL-Zertifikats

So fügen Sie ein benutzerdefiniertes SSL-Zertifikat hinzu

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > SSL-Zertifikate aus. Die Seite SSL-Zertifikate wird angezeigt, auf der alle SSL-Zertifikate für Ihr System aufgeführt sind.

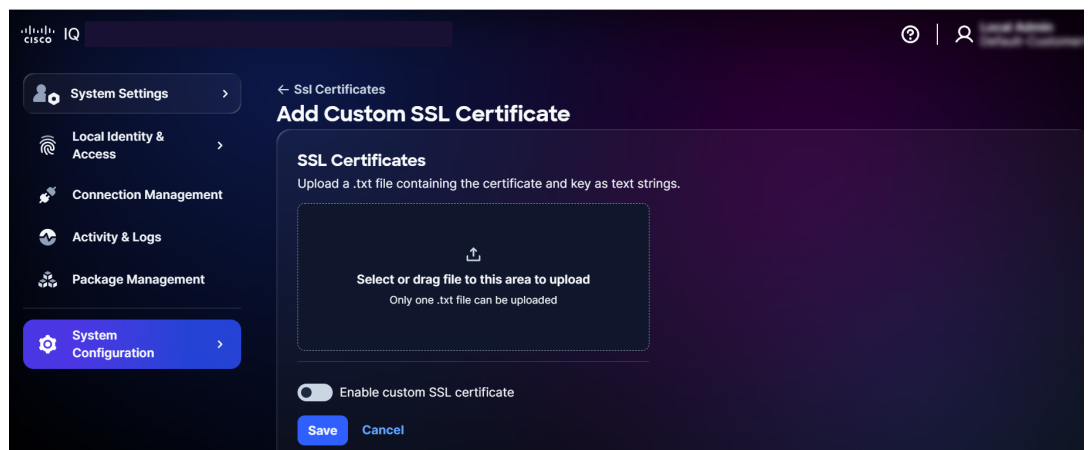


Hinzufügen eines SSL-Zertifikats

2. Klicken Sie auf Benutzerdefiniertes SSL-Zertifikat hinzufügen.



Anmerkung: Laden Sie eine TXT-Datei hoch, die sowohl das Privacy-Enhanced Mail-codierte Zertifikat als auch den Schlüssel als Textzeichenfolgen enthält. Es kann jeweils nur eine TXT-Datei hochgeladen werden. Die Datei muss sowohl das Zertifikat als auch den privaten Schlüssel enthalten.



SSL-Zertifikat hochladen

3. Ziehen Sie das benutzerdefinierte SSL-Zertifikat per Drag-and-Drop oder laden Sie es unter dem Abschnitt SSL-Zertifikat hoch.
4. Aktivieren Sie die Schaltfläche Benutzerdefiniertes SSL-Zertifikat aktivieren.

Enable Certificate?

Enabling custom SSL certificate will disable the default self-signed certificate.

Cancel

Enable certificate

Zertifikat aktivieren



Anmerkung: Lassen Sie den Schalter AUS, wenn Sie das Zertifikat hochladen möchten, ohne es sofort zu aktivieren.

5. Klicken Sie auf Zertifikat aktivieren.

6. Klicken Sie auf Speichern.

Das benutzerdefinierte SSL-Zertifikat ist aktiviert und aktiv. Das Standard-Systemzertifikat wird automatisch deaktiviert.

Bearbeiten des benutzerdefinierten SSL-Zertifikats

Sie können das benutzerdefinierte SSL-Zertifikat bearbeiten, um ein neues Zertifikat hochzuladen oder das aktuell aktivierte Zertifikat zu deaktivieren. So bearbeiten Sie:

1. Navigieren Sie zum gewünschten benutzerdefinierten SSL-Zertifikat.
2. Wählen Sie das Symbol Weitere Optionen > Bearbeiten aus. Die Seite SSL-Zertifikat bearbeiten wird angezeigt.
3. Bearbeiten Sie die Zertifikatdetails nach Bedarf.
4. Klicken Sie auf Speichern.

Benutzerdefiniertes SSL-Zertifikat wird gelöscht

Warnung: Ein benutzerdefiniertes SSL-Zertifikat kann jederzeit gelöscht werden, es handelt sich jedoch um eine unumkehrbare Aktion. Sie können jederzeit nach dem Löschen ein neues benutzerdefiniertes Zertifikat hochladen.

So löschen:

1. Navigieren Sie zum gewünschten persönlichen SSL-Zertifikat.

2. Wählen Sie das Symbol Weitere Optionen > Löschen aus.
3. Klicken Sie auf Zertifikat löschen. Das benutzerdefinierte Zertifikat wird gelöscht, und das Standardzertifikat wird automatisch wieder aktiviert.

Syslog-Serverkonfiguration

Benutzer mit der Kontoadministratorrolle können externe Syslog-Server für den Export von Systemprotokollen konfigurieren. Es können bis zu zwei (2) Syslog-Server konfiguriert werden.

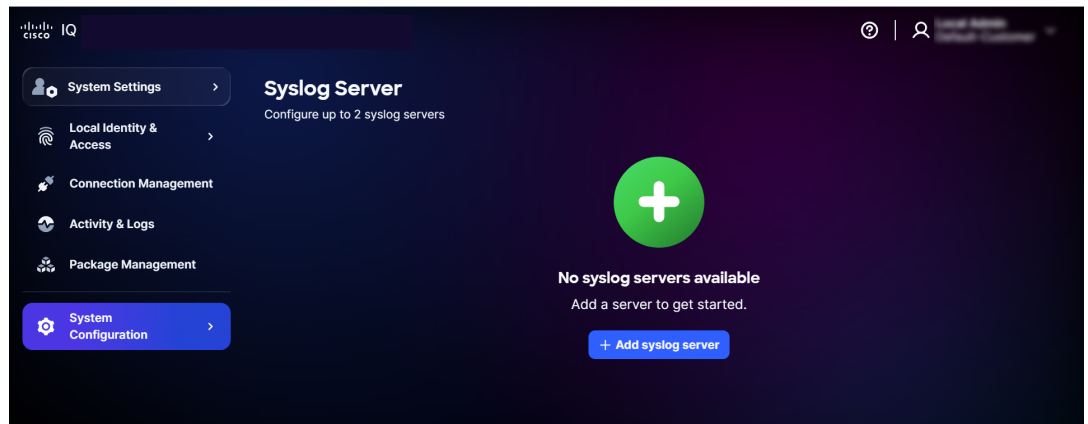


Anmerkung: Der Syslog-Server muss als IP-Adresse und nicht als FQDN (Fully Qualified Domain Name) angegeben werden.

Syslog-Server hinzufügen

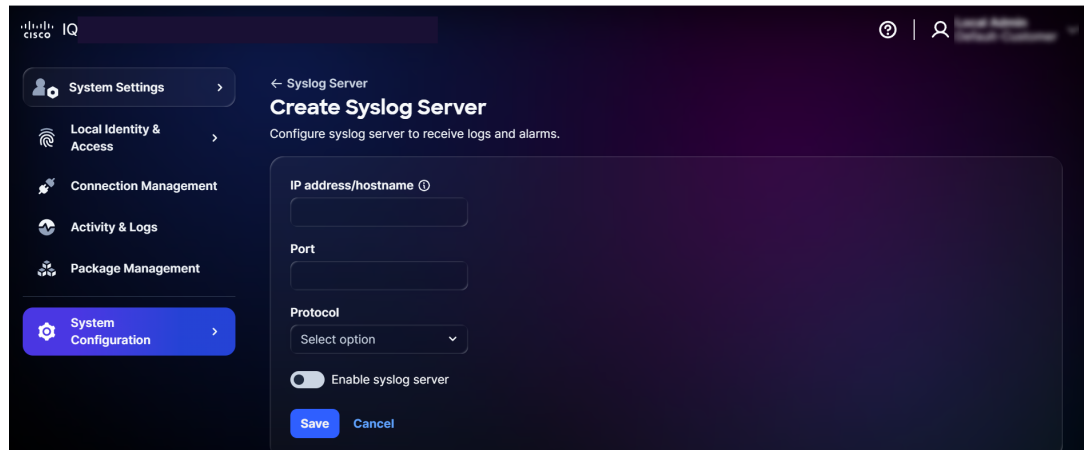
Syslog-Server hinzufügen:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Syslog-Server aus. Die Seite Syslog-Server wird angezeigt.



Syslog-Server hinzufügen

2. Klicken Sie auf Syslog-Server hinzufügen. Die Seite Syslog-Server erstellen wird angezeigt.



Syslog-Server erstellen

3. Geben Sie die IP-Adresse/den Hostnamen ein.
4. Geben Sie Port ein.
5. Wählen Sie das entsprechende Protokoll aus der Dropdown-Liste "Protocol" (Protokoll) aus (z. B. UDP, TCP).
6. Aktivieren Sie die Umschaltfläche Syslog-Server aktivieren.
7. Klicken Sie auf Speichern. Es wird eine Bestätigung angezeigt, und der neu hinzugefügte Syslog-Server wird auf der Syslog-Server-Startseite angezeigt.

Bearbeiten des konfigurierten Syslog-Servers

So bearbeiten Sie einen konfigurierten Syslog-Server:

1. Navigieren Sie zum gewünschten Syslog-Server.
2. Wählen Sie das Symbol Weitere Optionen > Bearbeiten aus. Die Seite "Syslog-Server bearbeiten" wird angezeigt.
3. Bearbeiten Sie nach Bedarf Details, oder deaktivieren Sie den Umschalter Syslog-Server aktivieren.
4. Klicken Sie auf Speichern.

Konfigurierten Syslog-Server löschen

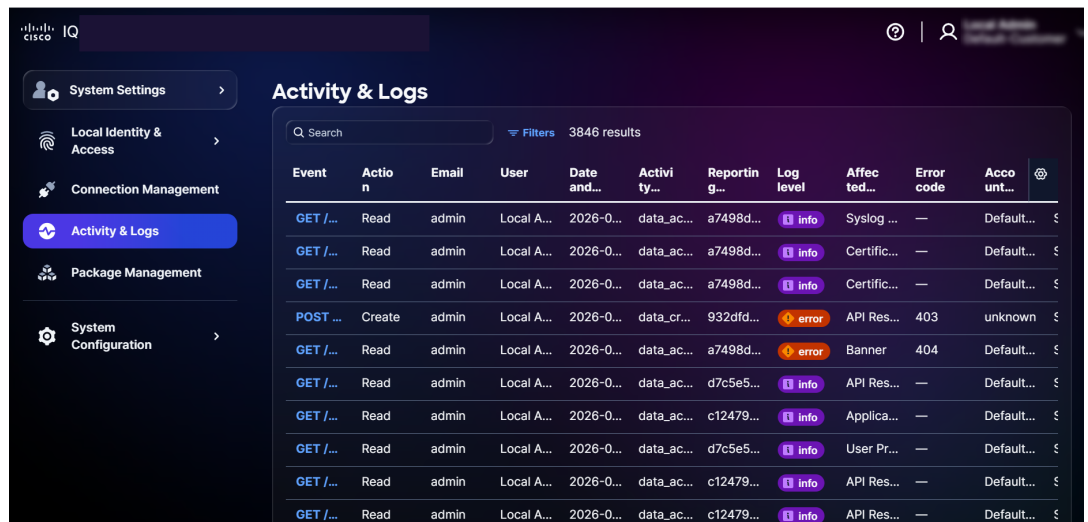
Einen konfigurierten Syslog-Server löschen:

1. Navigieren Sie zum gewünschten Syslog-Server.
2. Wählen Sie das Symbol Weitere Optionen > Löschen aus. Es wird eine Bestätigung angezeigt.

3. Klicken Sie auf Syslog-Server löschen.

Aktivität und Protokolle

Aktivität und Protokolle bieten eine detaillierte Aufzeichnung von Benutzeraktionen und Änderungen in Cisco IQ, sodass Kontoadministratoren Benutzeraktivitäten nachverfolgen und die Transparenz aufrechterhalten können.



Event	Action	Email	User	Date and time	Activity ID	Report 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...

Aktivität und Protokolle

Um Aktivitäten und Protokolle anzuzeigen, wählen Sie Aktivität und Protokolle aus dem Menü Systemeinstellungen.

Aktivität und Protokolle:

- Protokolliert alle API-Vorgänge auf Gateway-Ebene
- Unterstützt Filter, Paginierungs- und Suchfunktionen, die Ihnen das Auffinden und Verwalten von Informationen erleichtern

Folgende Filteroptionen sind verfügbar:

- Letztes Protokollierungsdatum: Filtert Protokolle auf einen bestimmten Zeitraum
- Protokollstufe: Filtert Protokolle nach Schweregrad (z. B. Fehler, Warnungen und Informationen)
- Aktivitätstyp: Filtert Protokolle nach Art der Systemaktivität
- Fehlercode: Filtert nach einem bestimmten Fehlercode

Banner

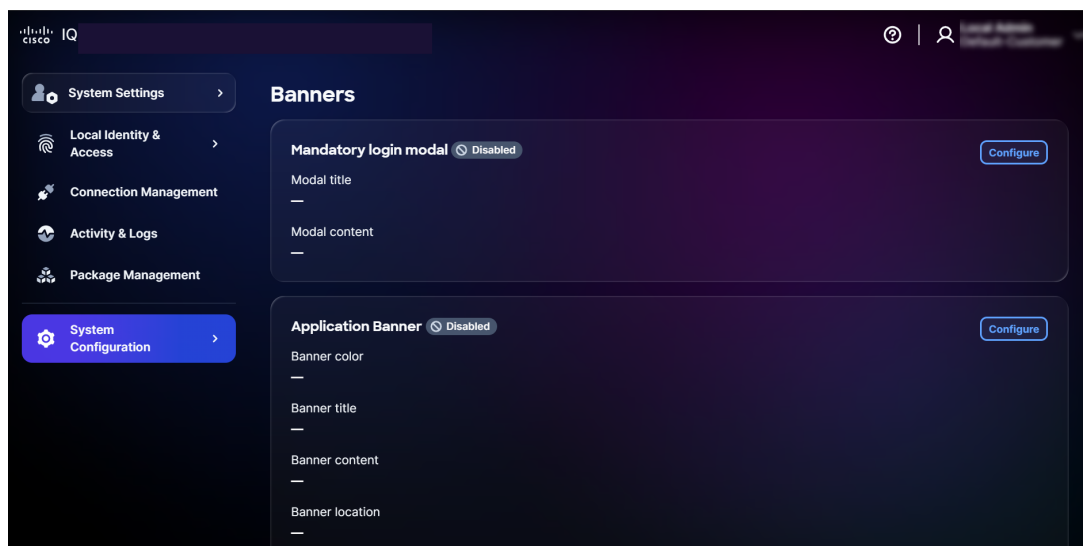
Kontoadministratoren können systemweite Banner konfigurieren, um Sicherheits- und Compliance-Standards zu erfüllen.

- Obligatorischer Anmeldemodus: Sie müssen das erforderliche Banner bestätigen, bevor Sie zum Anmeldebildschirm wechseln.
- Anwendungs-Banner: Hierbei handelt es sich um angepasste Banner, die nach der erfolgreichen Authentifizierung in der gesamten Anwendung angezeigt werden.

Konfigurieren von Modal-Bannern für obligatorische Anmeldung

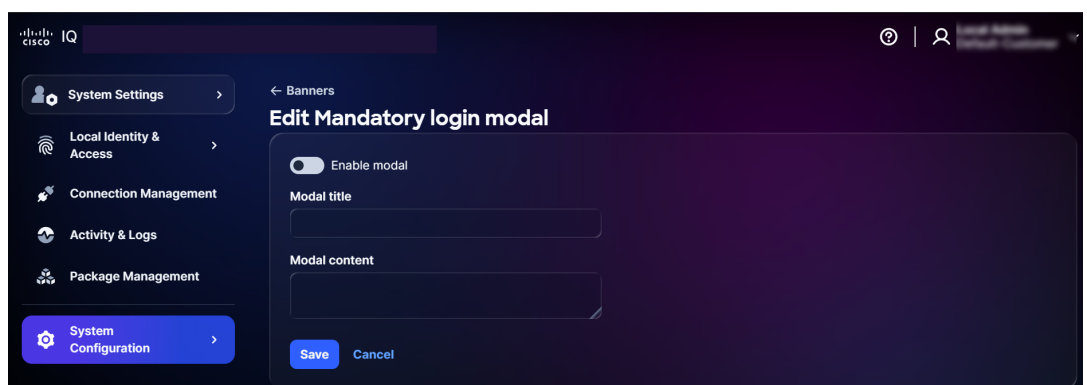
So konfigurieren Sie ein obligatorisches Banner:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Banner aus. Die Seite Banner wird angezeigt.



Pflichtbanner konfigurieren

2. Klicken Sie im Modus für obligatorische Anmeldung auf Konfigurieren. Die Seite "Obligatorische Anmeldung bearbeiten" wird angezeigt.



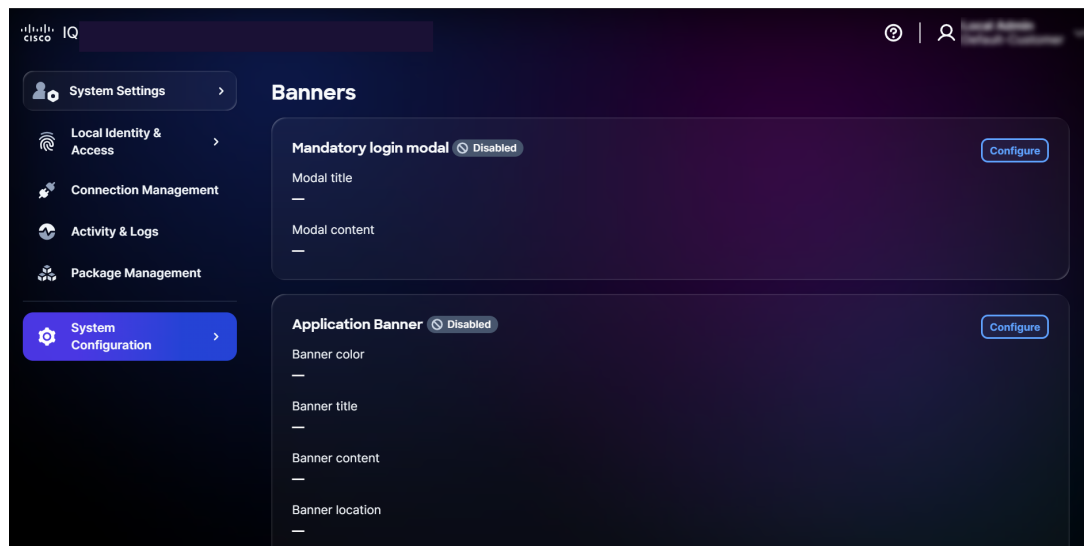
Bearbeiten Modales Banner für obligatorische Anmeldung

3. Klicken Sie auf den Umschalter, um den Banner zu aktivieren oder zu deaktivieren.
4. Geben Sie den Titel Modal (Modal) ein.
5. Geben Sie den Modal-Inhalt ein.
6. Klicken Sie auf Speichern. Der Modus für die obligatorische Anmeldung wird gespeichert.

Konfigurieren von Anwendungsbannern

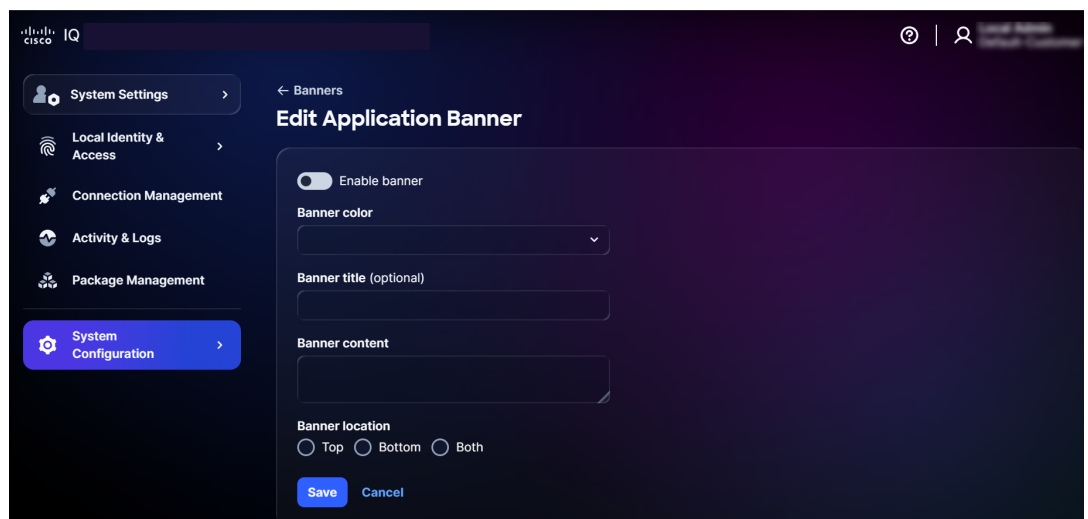
So konfigurieren Sie ein Anwendungsbanner:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Banner aus. Die Seite Banner wird angezeigt.



Banner konfigurieren

2. Klicken Sie auf In Anwendungs-Banner konfigurieren. Die Seite Bewerbungsbanner bearbeiten wird angezeigt.



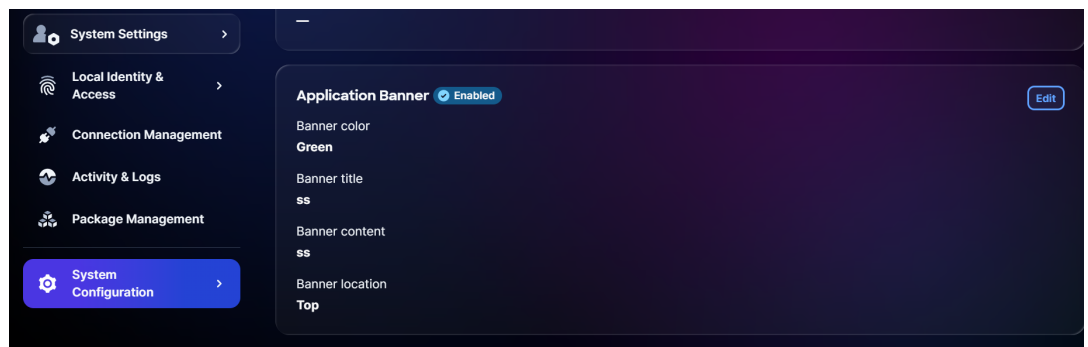
Anwendungsbanner bearbeiten

3. Klicken Sie auf den Umschalter, um den Banner zu aktivieren oder zu deaktivieren.
4. Wählen Sie eine Bannerfarbe aus.
5. Geben Sie den Bannertitel ein.
6. Geben Sie den Bannerinhalt ein.
7. Wählen Sie einen Bannerstandort aus.
8. Klicken Sie auf Speichern. Das Banner wird in der gesamten Anwendung angezeigt.

Banner bearbeiten

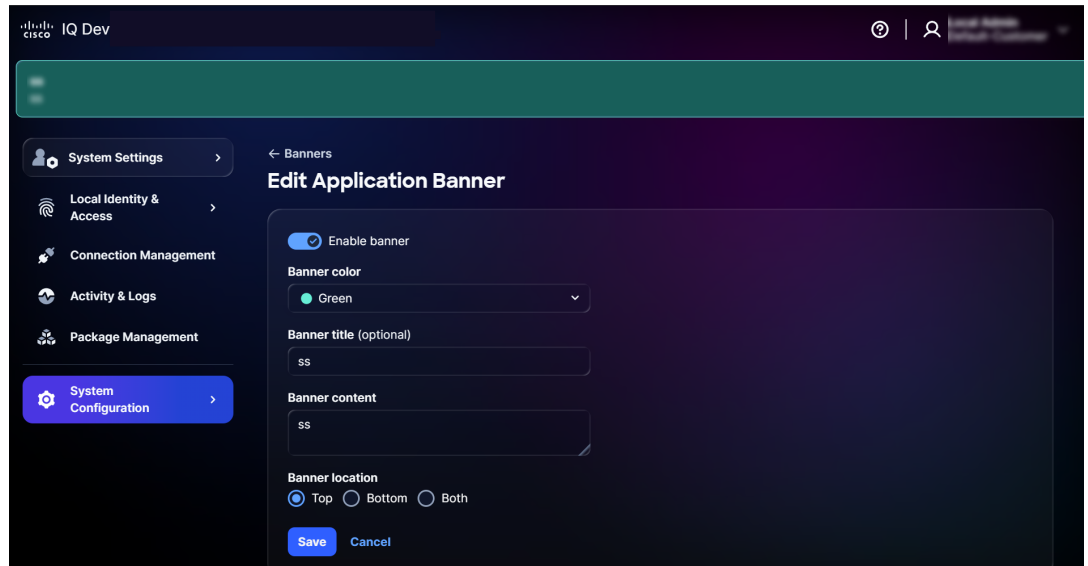
So bearbeiten Sie ein Banner:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Banner aus. Die Seite Banner wird angezeigt.



Banner bearbeiten

2. Klicken Sie auf Bearbeiten. Die Seite Bewerbungsbanner bearbeiten wird angezeigt.



Anwendungsbanner bearbeiten

3. Bearbeiten Sie die gewünschten Details.
4. Klicken Sie auf den Umschalter, um den Banner zu aktivieren oder zu deaktivieren.
5. Klicken Sie auf Speichern.

Fehlerbehebung

Sie können Diagnose- und Protokolldateien vom Cisco IQ-System sammeln und sicher auf einen SCP-Server übertragen. Diese Dateien können für das Support-Team freigegeben werden, wenn Probleme gemeldet werden, um wertvollen Kontext zu schaffen und die Fehlerbehebung zu unterstützen.

So sammeln Sie Diagnose- und Protokolldateien:

1. Melden Sie sich bei Cisco IQ an.

```

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

```

Hauptmenü

2. Geben Sie im Cisco IQ-Hauptmenü "3" ein, und drücken Sie die Eingabetaste, um Systemdiagnose auszuwählen.

```

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: ]

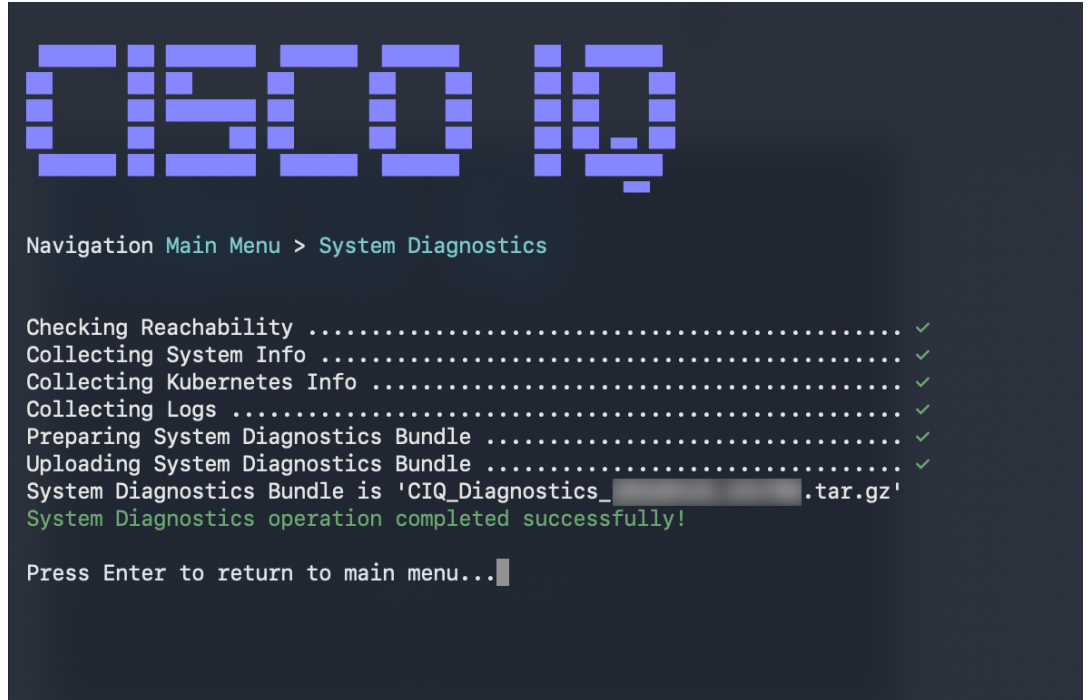
Continue with System Diagnostics? ([c]ontinue/[B]ack):

```

Systemdiagnose

3. Geben Sie die SCP-/SFTP-Serveradresse ein.
4. Geben Sie den SCP-/SFTP-Server-Port ein.
5. Geben Sie den SCP-/SFTP-Serverpfad ein.
6. Wählen Sie ein Protokoll aus.

7. Geben Sie den Benutzernamen ein.
8. Geben Sie das Kennwort ein.
9. Geben Sie "C" ein, und drücken Sie die Eingabetaste, um mit der Systemdiagnose fortzufahren.

A screenshot of a terminal window with a dark background. At the top, the Cisco IQ logo is displayed in a stylized, blocky font. Below the logo, the text 'Navigation Main Menu > System Diagnostics' is shown in a light blue color. The main part of the terminal displays a list of diagnostic steps, each followed by a green checkmark: 'Checking Reachability', 'Collecting System Info', 'Collecting Kubernetes Info', 'Collecting Logs', 'Preparing System Diagnostics Bundle', and 'Uploading System Diagnostics Bundle'. Below this list, a message states 'System Diagnostics Bundle is 'CIQ_Diagnostics_...' .tar.gz' where the ellipsis is represented by a greyed-out box. The final line of the diagnostic process is 'System Diagnostics operation completed successfully!' in green. At the bottom, a prompt 'Press Enter to return to main menu...' is visible with a cursor.

Systemdiagnosevorgang abgeschlossen

Das System startet den Diagnoseprozess und führt die folgenden Aktionen aus:

- Überprüfen der Erreichbarkeit
- Erfassen von Systeminformationen
- Sammeln von Kubernetes-Informationen
- Protokolle werden gesammelt
- Vorbereiten des Systemdiagnosepakets
- Hochladen des Systemdiagnosepakets

Nach Abschluss des Vorgangs wird eine Bestätigungsmeldung mit dem generierten Paketnamen angezeigt.

Support-Modul

Sie können VA- und modulspezifische Support-Tickets über Cisco IQ SaaS erstellen. Das Support-Modul ist in Cisco IQ SaaS verfügbar und bietet eine

konsolidierte Ansicht Ihrer Support-Tickets. Mit dieser Anwendung können Sie die Anfrageliste filtern, sortieren und anpassen. So erhalten Sie einen transparenten Überblick über alle offenen und abgeschlossenen Fälle, auf die Sie zugreifen können. Weitere Informationen zum Support-Modul in Cisco IQ SaaS finden Sie im [Cisco IQ SaaS-Handbuch "Erste Schritte"](#).



Anmerkung: Cisco IQ VA-Kunden haben Zugriff auf die meisten Funktionen des Cisco IQ SaaS Support-Moduls, darunter das Öffnen von Tickets des Technical Assistance Center (TAC) für Cisco IQ VA und die zugehörigen Module sowie das Erstellen und Verwalten von ProduktTickets.

Erstellen eines Support-Tickets

Sie können VA- und modulspezifische Tickets in Cisco IQ SaaS erstellen. So erstellen Sie ein Ticket:

1. Melden Sie sich bei [Cisco IQ \(SaaS\) an](#).
2. Klicken Sie auf das Symbol Hilfe > Problem melden. Das Fenster Problem melden wird geöffnet.

The screenshot shows a dark-themed web form titled "Report an Issue". Below the title is a subtitle: "Experiencing an issue with Cisco IQ? Let us know what's going on and we'll open a support case for you." The form contains several sections: "Issue type" with four radio button options: "Portal login issues", "Error message", "Data discrepancy", and "Other"; "Issue description" with a large text area and a placeholder "Describe what happened."; "Preferred contact method" with three radio button options: "Telephone", "Email", and "Virtual space via Webex"; and "Include recipients (optional)" with a dropdown menu labeled "Select or add email addresses". Below the dropdown is a hint: "Select or enter email addresses to include." At the bottom right are two buttons: "Cancel" and "Submit".

Problem melden

3. Geben Sie die erforderlichen Details an.
4. Klicken Sie auf Senden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.