

Cisco IQ: Erste Schritte

Einleitung

Cisco IQ™ bietet Kunden Verbesserungen und Funktionen, die darauf ausgelegt sind, die Transparenz ihrer Ressourcen zu verbessern, intelligentere Einblicke in ihre Umgebungen 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 es Benutzern ermöglichen, proaktive, fundierte Entscheidungen zu treffen, und Prozesse optimieren, die das Kundenengagement und den Erfolg fördern.

Dieses Dokument enthält Informationen zu den ersten Schritten mit Cisco IQ und den zugehörigen Anwendungen. Weitere Informationen finden Sie in den [Cisco IQ Versionshinweisen](#) oder den Dokumenten [mit häufig gestellten Fragen zu Cisco IQ](#).

Integration

Voraussetzungen


Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie Cisco IQ verwenden.

Unterstützte Browser

Cisco IQ wird von den neuesten stabilen Versionen der folgenden Browser unterstützt:

- Google Chrome
- Microsoft Edge
- Apple Safari
- Mozilla Firefox

 Anmerkung: Die Unterstützung ist auf aktuelle Browserversionen beschränkt, und ältere

 Versionen bieten möglicherweise nicht den vollen Funktionsumfang oder werden bei der Veröffentlichung neuer Updates möglicherweise nicht mehr unterstützt.

Cisco Konto

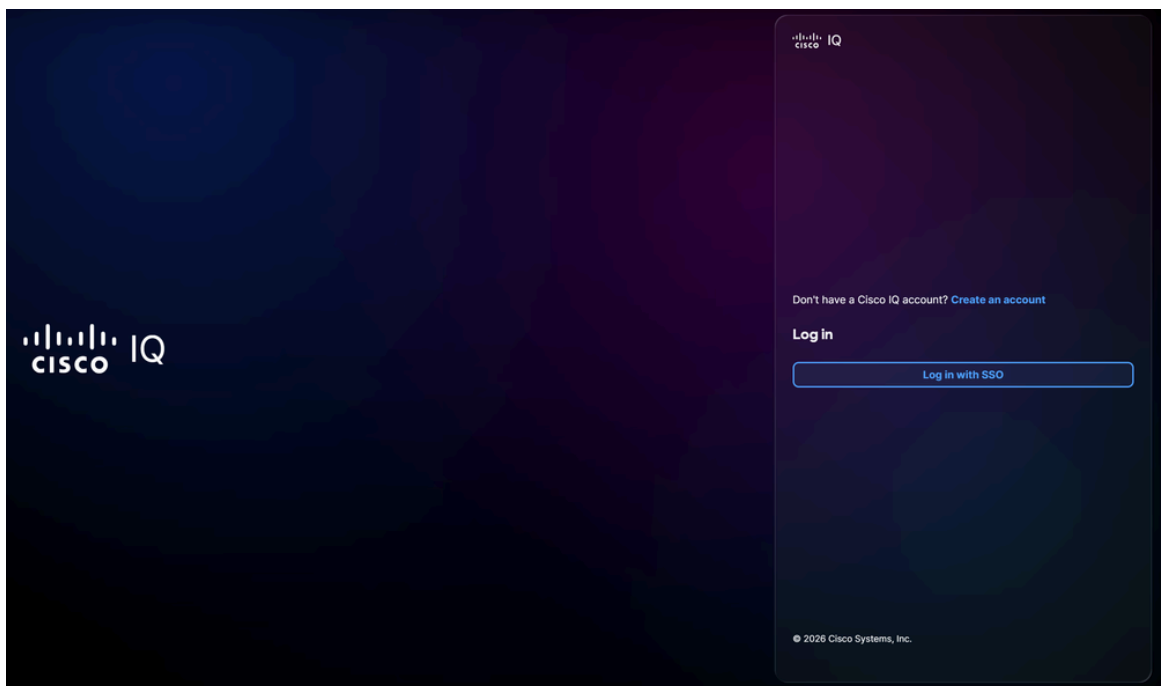
Um auf Cisco IQ zugreifen zu können, benötigen Sie ein Cisco.com Konto. Weitere Informationen zu Cisco Konten finden Sie in der [Anmelde- und Kontohilfe](#).

Kontoerstellung

Erstellen eines neuen Cisco IQ-Kontos

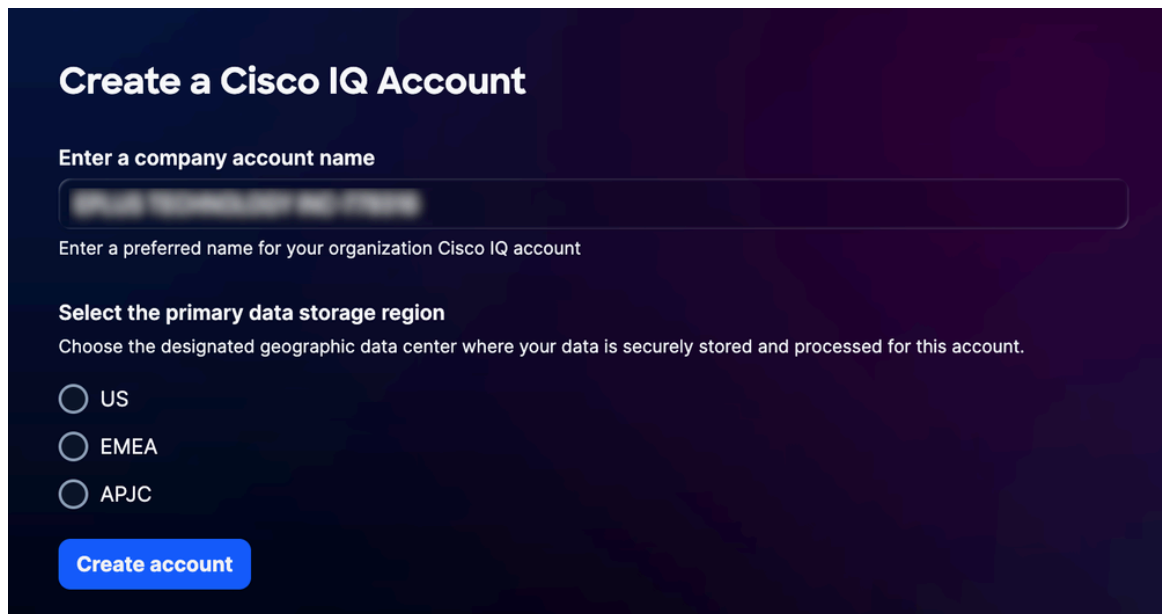
So erstellen Sie ein neues Cisco IQ-Konto:

1. Navigieren Sie zu [Cisco IQ](#). Die Seite Cisco Log in (Cisco-Anmeldung) wird angezeigt.



Cisco IQ-Anmeldung

2. Klicken Sie auf Konto erstellen.
3. Geben Sie Ihre Cisco Connection Online (CCO) ID in das Feld "E-Mail" ein.
4. Klicken Sie auf Next (Weiter).
5. Geben Sie Ihr Kennwort ein.
6. Klicken Sie auf Überprüfen. Die Seite Cisco IQ-Konto erstellen wird angezeigt.



Create a Cisco IQ Account

Enter a company account name

Enter a preferred name for your organization Cisco IQ account

Select the primary data storage region

Choose the designated geographic data center where your data is securely stored and processed for this account.

US

EMEA

APJC

Create account

Cisco IQ-Konto erstellen


7. Geben Sie im Feld "Geben Sie einen Firmenkontonamen ein" den eindeutigen Namen ein, den Sie für das Cisco IQ-Konto Ihrer Organisation verwenden möchten.
8. Wählen Sie den primären Datenspeicherbereich aus.
9. Klicken Sie auf Konto erstellen. Sie werden zum Cisco IQ Launchpad weitergeleitet.


Migration von CX Cloud-Kunden auf Cisco IQ


 Anmerkung: Nur Kontoadministratoren können vorhandene CX Cloud-Konten zu Cisco IQ migrieren.


Wenn Sie bereits über ein CX Cloud-Konto verfügen, können Sie vorhandene CX Cloud-Daten zu Cisco IQ migrieren. Die folgenden Daten werden automatisch vom vorhandenen CX Cloud-Konto migriert:

- Benutzer und Benutzergruppen (ohne Benutzer und Gruppen von Partnern)
- Verträge
- Hinzufügen von Cloud-Datenquellen für Intersight, WebEx, Software-Defined Wide Area Network (SD-WAN) und Meraki

 Anmerkung: Um einen reibungslosen Übergang zu gewährleisten und genauere Einblicke in die personalisierten, vorausschauenden und proaktiven KI-gestützten Informationen von Cisco IQ zu erhalten, sollten Sie Ihre CX Cloud-Kontodaten vor der Migration validieren und

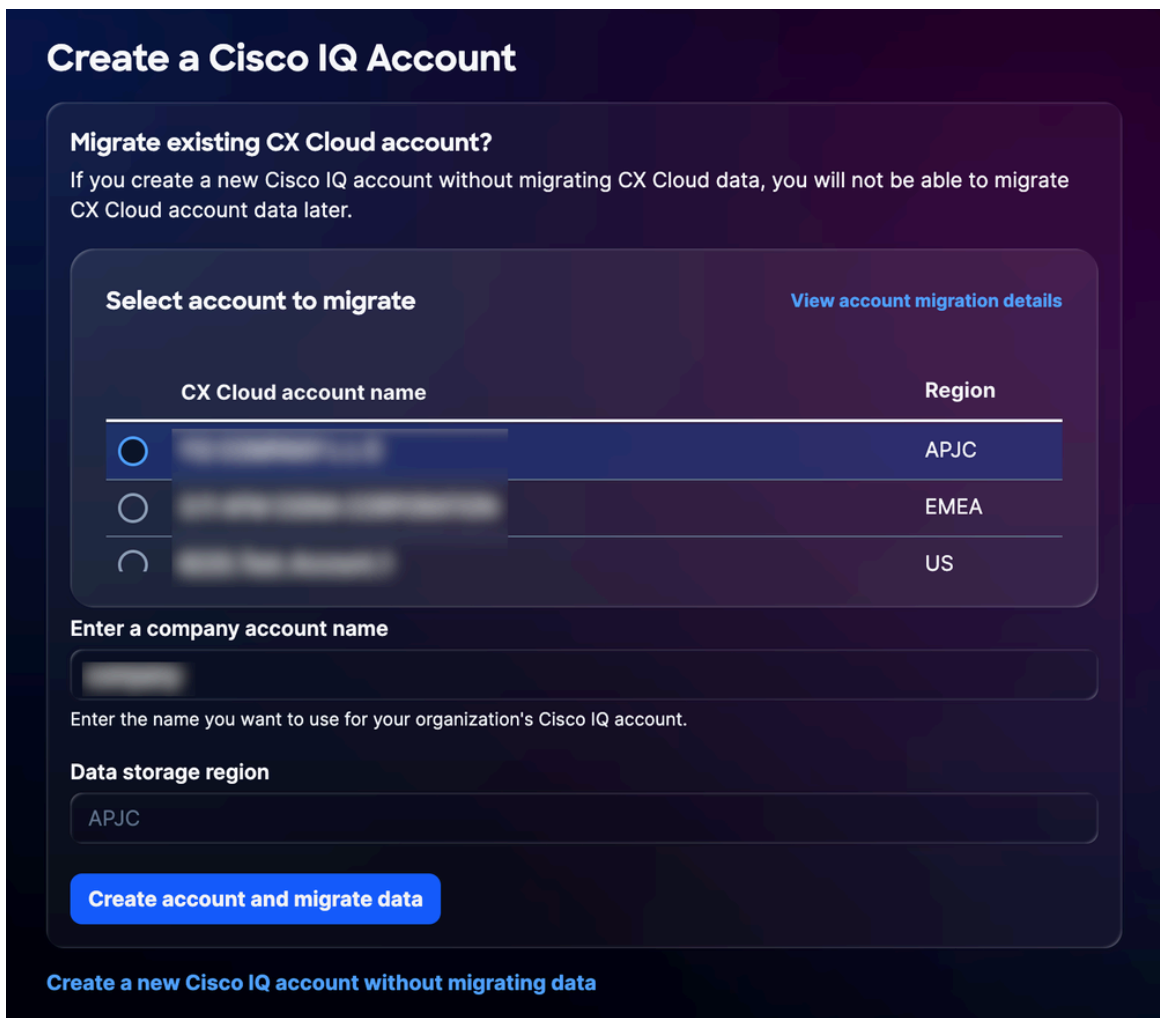
 organisieren.

 **Warnung:** Wenn Sie ein neues Cisco IQ-Konto erstellen, ohne CX Cloud-Daten zu migrieren, können Sie CX Cloud-Kontodaten nicht zu einem späteren Zeitpunkt migrieren.

 **Anmerkung:** Es kann jeweils nur ein CX Cloud-Konto migriert werden. Wenn Sie weitere Konten migrieren müssen, wiederholen Sie die in diesem Abschnitt beschriebenen Schritte.

So migrieren Sie ein vorhandenes CX Cloud-Konto:

1. Navigieren Sie zu [Cisco IQ](#). Die Seite Cisco Log in (Cisco-Anmeldung) wird angezeigt.
2. Klicken Sie auf Konto erstellen.
3. Geben Sie Ihre Cisco Connection Online (CCO) ID in das Feld "E-Mail" ein.
4. Klicken Sie auf Next (Weiter).
5. Geben Sie Ihr Kennwort ein.
6. Klicken Sie auf Überprüfen. Die Seite Cisco IQ-Konto erstellen wird angezeigt.



Create a Cisco IQ Account

Migrate existing CX Cloud account?
If you create a new Cisco IQ account without migrating CX Cloud data, you will not be able to migrate CX Cloud account data later.

[View account migration details](#)

CX Cloud account name	Region
<input checked="" type="radio"/> [Redacted]	APJC
<input type="radio"/> [Redacted]	EMEA
<input type="radio"/> [Redacted]	US

Enter a company account name


Enter the name you want to use for your organization's Cisco IQ account.

Data storage region

[Create account and migrate data](#)

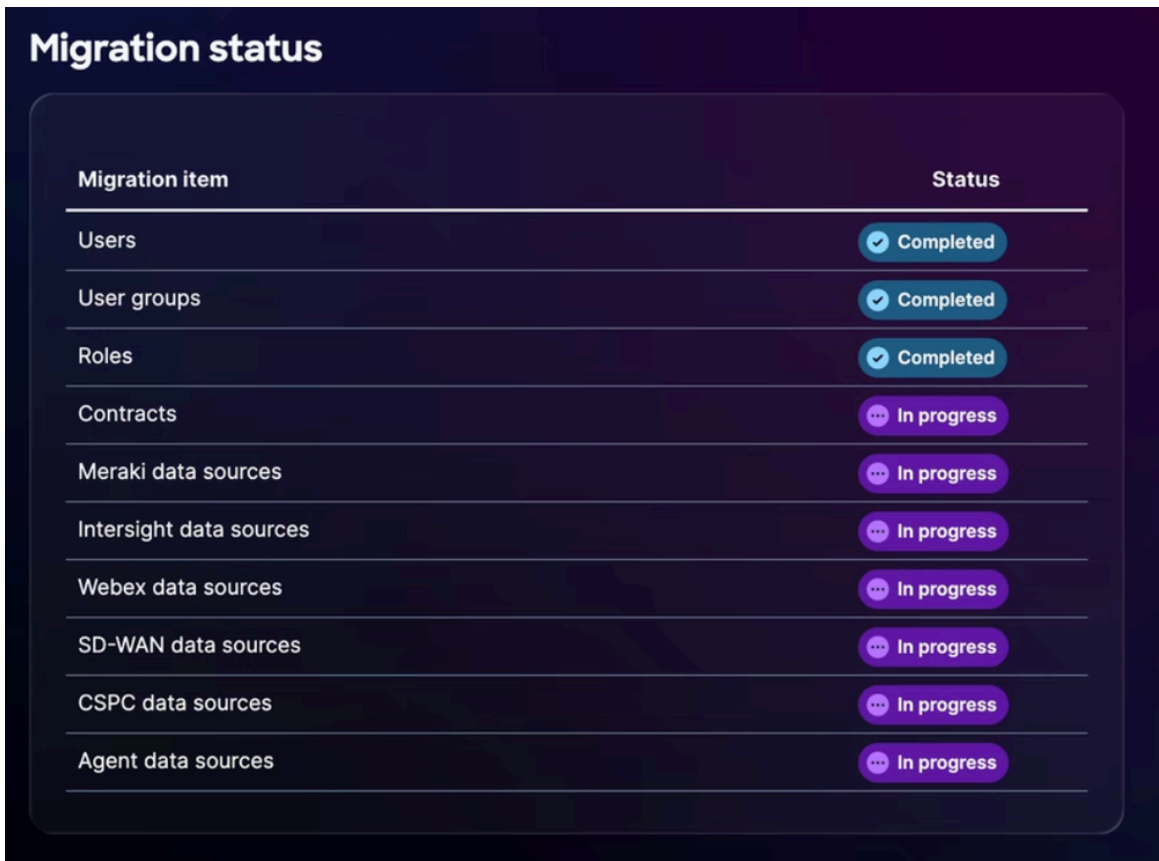
[Create a new Cisco IQ account without migrating data](#)

- Wählen Sie das CX Cloud-Konto aus, von dem Sie Daten migrieren möchten.
- Geben Sie den eindeutigen Namen ein, den Sie für das Cisco IQ-Konto Ihres Unternehmens verwenden möchten.

 Anmerkung: Der Bereich für die Datenspeicherung des ursprünglichen Kontos wird automatisch ausgefüllt und in das Cisco IQ-Unternehmenskonto migriert. Um den Datenspeicherbereich zu ändern, müssen Sie ein neues Cisco IQ-Unternehmenskonto erstellen.

- Klicken Sie auf Konto erstellen und Daten migrieren. Die Seite Migrationsstatus wird angezeigt.

Auf der Seite Migrationsstatus wird der Abschlussstatus der Daten angezeigt, die zu Cisco IQ migriert werden. Folgende Status sind verfügbar:



Migration item	Status
Users	Completed
User groups	Completed
Roles	Completed
Contracts	In progress
Meraki data sources	In progress
Intersight data sources	In progress
Webex data sources	In progress
SD-WAN data sources	In progress
CSPC data sources	In progress
Agent data sources	In progress


Migrationsstatus

- In progress: Daten werden gerade migriert
- Completed: Migration abgeschlossen
- Migration nicht möglich: Die Datenmigration ist unvollständig, und Cisco IQ kann die Daten nicht migrieren.

Wenn die Daten nicht migriert werden können, müssen Sie die Daten manuell auf das neue Cisco IQ-Unternehmenskonto migrieren. Weitere Informationen zum Hinzufügen zusätzlicher Daten zum Cisco IQ finden Sie unter [Systemeinstellungen](#).

10. Klicken Sie nach Abschluss der Migration auf Weiter. Sie werden zum Cisco IQ Launchpad weitergeleitet.

Anmelden bei vorhandenen Konten

 Anmerkung: Kunden mit einem bestehenden Cisco IQ-Konto, die noch nicht zu einem Unternehmenskonto hinzugefügt wurden, müssen sich an den Account-Administrator des Unternehmens wenden, um Zugriff auf das Konto zu beantragen.

So melden Sie sich bei einem vorhandenen Konto an:

1. Navigieren Sie zu [Cisco IQ](#). Die Seite Cisco Log in (Cisco-Anmeldung) wird angezeigt.
2. Klicken Sie auf Mit SSO anmelden.
3. Geben Sie Ihre CCO-ID in das Feld "E-Mail" ein.
4. Klicken Sie auf Next (Weiter).
5. Geben Sie Ihr Kennwort ein.
6. Klicken Sie auf Überprüfen.

Wenn Sie über ein Konto verfügen, werden Sie zum Cisco IQ Launchpad weitergeleitet.

Wenn Sie über mehr als ein Konto verfügen, werden Sie zur Seite Willkommen bei Cisco IQ weitergeleitet.

Welcome to Cisco IQ!

Select an account below

Q Search

Account name

Region

US


US

US

US

Kontonamen auswählen

Erste Schritte

 Anmerkung: Bevor Sie beginnen, stellen Sie sicher, dass Sie den Cisco IQ vollständig integriert haben. Weitere Informationen finden Sie unter [Onboarding](#).

Support-Stufen

Die Cisco IQ Support-Stufen definieren den Zugriff und die Funktionen, die Ihnen innerhalb von Cisco IQ zur Verfügung stehen, und wurden entwickelt, um den Support und die Professional Services-Erfahrung zu verbessern. Diese Stufen sind an Ihren gültigen Cisco Supportvertrag gebunden und bestimmen, welche Funktionen und Tools Sie nutzen können, von künstlichen Intelligenzen über die Fehlerbehebung bis hin zum Ressourcen- und Vertragsmanagement. Wenn Sie Ihre Servicestufe kennen, können Sie die Funktionen von Cisco IQ optimal nutzen und gleichzeitig Ihre vertraglichen Rechte einhalten. In der folgenden Tabelle sind die für jede Ebene verfügbaren Cisco IQ-Funktionen aufgeführt.

 Anmerkung: Die Funktionen sind auf allen Support-Ebenen kumulativ. höhere Ebenen

 umfassen alle Funktionen der niedrigeren Ebenen.

	Basisstufe	Standardstufe	Signaturebene
	Sie müssen wissen,	Priorisierung der Ausfallsicherheit	Optimierung von
Vollständige Übersichtlichkeit	<p>Mit den folgenden Funktionen können Sie alle Ressourcen und Unterkomponenten von Cisco dynamisch und sicher nachverfolgen.</p> <ul style="list-style-type: none"> • Ressourcen-bestand • End-of-Life-Berichte (EOL) • Serviceabdeckungsberichte • Letztes Datum für Support (LDOS) Dashboard 	<p>Verwenden Sie die folgenden Funktionen, um die Netzwerkleistung zu analysieren und zu bestimmen, wo Sie Ressourcen zuweisen müssen. So können Sie fundierte Entscheidungen über Infrastrukturinvestitionen treffen.</p> <ul style="list-style-type: none"> • EOL-Erkenntnisse¹ • Erkenntnisse zur Serviceabdeckung¹ • LDOS-Erkenntnisse¹ • Informationen zu kostenkritischen Ressourcen¹ • Bestandskennzeichnung 	
Proaktive Ausfallsicherheit	<p>Mit den folgenden Funktionen erhalten Sie Einblick in wichtige Benachrichtigungen, mit denen Sie potenzielle Risiken in Ihrer Umgebung identifizieren und beheben können.</p> <ul style="list-style-type: none"> • Berichte zu Sicherheitsberatern • Berichte zu Problemhinweisen 	<p>Cisco IQ verwandelt Daten in Erkenntnisse, indem es Ressourcenrisiken korreliert, sodass Sie die wichtigsten Sicherheitsrisiken identifizieren und priorisieren können.</p> <ul style="list-style-type: none"> • Einblicke in Sicherheitsberatung¹ • Erkenntnisse zur Sicherheitssicherung¹ • Einblicke in Problemhinweise¹ • Konfigurationsinformationen¹ 	<p>Die folgenden Funktionen umsetzbare Empfehlungen zur Verbesserung des Sicherheitsstatus und zur Optimierung von Ihrer Umgebung.</p> <ul style="list-style-type: none"> • Konfiguration • Empfehlungen zur Sicherheits-

Schnelle Problembeseitigung	<p>Verwalten Sie Ihre Support-Tickets, und verfolgen Sie den Lösungsstatus an einem Standort, um Probleme mithilfe der folgenden Funktionen schneller zu lösen.</p> <ul style="list-style-type: none"> • Ticket-Management • Self-Service-Fehlerbehebung¹ 	<p>Mit der folgenden Funktion können Sie Falltrends und Effizienzmetriken verfolgen, um eine kontinuierliche Verbesserung der betrieblichen Abläufe zu erzielen. Cisco IQ bietet einen kontextsensitiven Lösungsassistenten, mit dem Sie aktive Probleme beheben und die zugrunde liegenden Ursachen untersuchen können.</p> <ul style="list-style-type: none"> • Case-Einblicke¹ 	
-----------------------------	--	---	--

¹ Unterstützt Geräte- und Telemetrierbindungen über Cisco IQ Link, Intersight, Meraki, SD-WAN Manager und WebEx Control Hub.

Grundlegende Funktionen

Die grundlegende Support-Stufe bietet grundlegende Kontrolle durch zuverlässigen und reaktiven Support, einschließlich Zugang zu technischen Produktsupport-Experten, Self-Service-Fehlerbehebung und zentralisiertes Ticket-Management. Um eine vollständige Transparenz zu gewährleisten, vereint Cisco IQ Ressourcen-Telemetrie, Vertragsinformationen und den Support-Verlauf und bietet so einen umfassenden Überblick über die Lebenszyklen Ihrer Ressourcen, Sicherheitsempfehlungen und Problemhinweise. Darüber hinaus können Sie Ihr technisches Fachwissen vertiefen, indem Sie auf grundlegende Lernressourcen zugreifen, die über das [Cisco U](#) zur Verfügung stehen.

In der folgenden Tabelle sind die verfügbaren Funktionen für die Support-Stufe Basic aufgeführt.

Funktionen	Beschreibung
Ressourcen-bestand	Die Bestandsaufnahme bietet eine aktuelle Liste und umfassende Visualisierungen für Hardwareprodukte, Modell- und Seriennummern, Betriebssystemversion, am Standort installierte Geräte und Details zur Serviceabdeckung. Darüber hinaus bietet es eine Möglichkeit zur Filterung nach dem "letzten Signal". Zu diesem Zeitpunkt wusste Cisco, dass die Ressource aktiv war, basierend auf Fällen im Technical Assistance Center (TAC), Vertragsverlängerungen, Telemetrie usw.
EOL-Bericht	Die EOL-Berichte bieten eine aktuelle Liste und umfassende Visualisierungen für Hardware und Software, die sich den EOL-

	<p>Meilensteinen vom Vertriebsende bis hin zu LDOS nähert, diese erreicht oder bereits überschritten hat. Dies ermöglicht die Planung von Lebenszyklus- und Technologieaktualisierungen.</p>
Bericht zur Serviceabdeckung	<p>Berichte zur Serviceabdeckung bieten eine aktuelle Liste und umfassende Visualisierungen für abgedeckte und nicht abgedeckte Ressourcen.</p>
LDOS-Dashboard	<p>Das LDOS Dashboard bietet eine zentrale Übersicht über die LDOS Meilensteine und ermöglicht so eine verbesserte Ressourcenplanung und Budgetplanung, bevor die Hardware oder Software das Ende ihrer Lebensdauer erreicht, wodurch das betriebliche Risiko verringert werden kann.</p>
Sicherheitsempfehlungen	<p>Sicherheitsankündigungen stellen eine automatisierte Lösung dar, die Risiken erkennt, Schwachstellen basierend auf Schweregrad und Wichtigkeit priorisiert und Einblicke auf Führungsebene liefert, um die Eindämmung kritischer Bedrohungen zu beschleunigen und so die Widerstandsfähigkeit des Unternehmens gegen neue Bedrohungen zu verbessern.</p>
Problemhinweise	<p>Problemhinweise stellen eine automatisierte Lösung dar, die nicht sicherheitsrelevante Produktprobleme erkennt, Probleme nach Schweregrad und Wichtigkeit der Auswirkungen priorisiert und Einblicke auf Führungsebene liefert, um die Lösung kritischer betrieblicher Probleme zu beschleunigen und so die Widerstandsfähigkeit des Unternehmens zu erhöhen und eine optimale Leistung aufrechtzuerhalten.</p>
Ticket-Management	<p>Ticket-Management bietet eine aktuelle Liste der Cisco TAC-Tickets, einschließlich Ticketanzahl, Status, Schweregrad und Retouren genehmigungen (Return Material Authorizations, RMAs), die mit Tickets verknüpft sind. Darüber hinaus bietet es die Möglichkeit, TAC-Tickets (über eine Weiterleitung an den Support Case Manager (SCM) zu erstellen und Ticketinformationen schnell zu aktualisieren, um die Bearbeitung zu vereinfachen.</p>
Self-Service-Fehlerbehebung ¹	<p>Self-Service-Fehlerbehebung ermöglicht die sofortige Behebung von Problemen mit dem Cisco IQ AI Assistant. Dieses interaktive Tool bietet kontextsensitive Fehlerbehebung in Echtzeit und Empfehlungen von Experten direkt aus der verifizierten Wissensdatenbank von Cisco. So können Sie Probleme lösen, ohne ein Support-Ticket erstellen zu</p>

	müssen.
--	---------

¹ Unterstützt Geräte- und Telemetrieverbindungen über Cisco IQ Link, Intersight, Meraki, SD-WAN Manager und WebEx Control Hub.

Standardfunktionen

Die Standard-Support-Stufe verbessert Ihre Betriebseffizienz durch eine zentrale Klassifizierung von Problemen auf Lösungsebene und einen dedizierten Fallinhaber, der sich mit den erforderlichen technischen Experten abstimmt. Sie können Risiken proaktiv mindern, indem Sie KI-gestützte Informationen nutzen, die Bestandsdaten mit geschäftskritischer Bedeutung korrelieren und so einen klaren Überblick über Ihre Bestandsaufnahme-, Sicherheits- und Konfigurationsbewertungen bieten. Darüber hinaus können Sie das Know-how Ihres Teams über personalisierte Lernpfade, die in [Cisco Unified Communications](#) zur Verfügung stehen, auf Ihre spezifischen geschäftlichen Anforderungen abstimmen.

In der folgenden Tabelle sind die verfügbaren Funktionen für die Standard-Support-Stufe aufgeführt.

Funktionen	Beschreibung
EOL-Erkenntnisse ¹	EOL Insights bietet intelligente Abfragen, Zusammenfassungen, Visualisierungen und Berichte zu EOL-Meilensteinen, um eine personalisierte Priorisierung des Lebenszyklus und der Planung von Technologieaktualisierungen zu ermöglichen.
Erkenntnisse zur Serviceabdeckung ¹	Service Coverage Insights bietet eine Visualisierung und Analyse von Details zur Serviceabdeckung und von Meilensteinen für die Verlängerung, sodass Sie Abdeckungs-Updates und die Verlängerungsplanung personalisiert priorisieren können.
Bestandskennzeichnung	Asset Tagging bietet eine Möglichkeit, den Bestand anhand der geschäftlichen Anforderungen zu organisieren, indem Asset Tags verwendet werden. Dies ermöglicht die flexible Organisation von Hardware- und Software-Ressourcen nach Abteilung, Standort oder Projekt als Schlüssel-Wert-Paare.
LDOS-Erkenntnisse ¹	LDOS Insights bietet eine Visualisierung und Analyse von Ressourcen, die über die LDOS Meilensteine hinausgehen oder sich ihnen nähern, und ermöglicht so eine personalisierte

	Priorisierung des Lebenszyklus und der Planung von Technologieaktualisierungen.
Informationen zu kostenkritischen Ressourcen ¹	Erkenntnisse zur Bedeutung von Ressourcen ermöglichen die Evaluierung und Identifizierung von Ressourcenrollen und ihrer relativen Bedeutung in Ihrem Netzwerk, um Maßnahmen zur Risikominimierung zu priorisieren und die betriebliche Ausfallsicherheit zu verbessern.
Einblicke in Sicherheitsberatung ¹	Security Advisory Insights ermöglichen die intelligente Abfrage, Zusammenfassung, Visualisierung und Berichterstellung für Ressourcen, die von Security Advisories betroffen sind, und ermöglichen so eine personalisierte Priorisierung von Risiken und der Reaktion auf Sicherheitsvorfälle.
Erkenntnisse zur Sicherheitssicherung ¹	Erkenntnisse zur Sicherheitssicherung bieten eine automatisierte Lösung, die Gerätekonfigurationen bewertet, Sicherheitslücken basierend auf dem Schweregrad und der Wichtigkeit der Auswirkungen identifiziert und Einblicke auf Führungsebene liefert, um die Implementierung wichtiger Sicherheitsmaßnahmen zu beschleunigen. Sie erhöht die Ausfallsicherheit und reduziert die Angriffsfläche gegen neue Bedrohungen. Gleichzeitig ermöglicht sie die personalisierte Priorisierung eines verbesserten Sicherheitsstatus durch intelligente Abfrage, Zusammenfassung, Visualisierung und Berichterstellung zu gefährdeten Ressourcen.
Einblicke in Problemhinweise ¹	Problemhinweise ermöglichen die intelligente Abfrage, Zusammenfassung, Visualisierung und Berichterstellung für Ressourcen, die von Problemhinweisen betroffen sind. So können Risiken und die Reaktion auf bekannte Probleme personalisiert priorisiert werden.
Konfigurationsinformationen ¹	Configuration Insights bietet eine automatisierte Lösung, die Gerätekonfigurationen anhand der von Cisco empfohlenen Best Practices auf Basis praxisbewährter Fachkenntnisse bewertet. Intelligente Abfrage, Zusammenfassung, Visualisierung und Berichterstellung für betroffene Ressourcen ermöglichen eine personalisierte Priorisierung und beschleunigen die Behebung kritischer Konfigurationslücken, verbessern die Ausfallsicherheit der Infrastruktur und reduzieren betriebliche Risiken im gesamten Netzwerk.

Case-Einblicke ¹	Case Insights bieten intelligente Funktionen zum Abfragen, Zusammenfassen, Visualisieren und Berichten von Cisco TAC-Tickets. Dies ermöglicht eine personalisierte Überwachung der Betriebseffizienz.
-----------------------------	---

¹ Unterstützt Geräte- und Telemetrieverbindungen über Cisco IQ Link, Intersight, Meraki, SD-WAN Manager und WebEx Control Hub.

Signaturfunktionen

Die Signature-Supportstufe baut auf der Standard-Supportstufe auf, um Ihre betriebliche Leistung durch definierte Service Level Agreements für die Wiederherstellung und den Zugang zu einem dedizierten Team von Experten, die mit Ihrer einzigartigen Umgebung vertraut sind, zu verbessern. Diese Stufe konzentriert sich auf die Vermeidung von Unterbrechungen, bevor diese sich auf Ihre Betriebsabläufe auswirken, indem proaktive Sicherheitsmaßnahmen, eine systematische Beseitigung der Ursachen und eine kontinuierliche, von Experten gesteuerte Analyse Ihrer Ressourcen bereitgestellt werden. Darüber hinaus können Sie die erweiterten [Cisco U.-Zertifizierungsschulungen](#) und virtuelle Übungseinheiten nutzen, um umfassende technische Kenntnisse aufzubauen.


In der folgenden Tabelle sind die verfügbaren Funktionen für die Signatur-Support-Stufe aufgeführt.

Funktionen	Beschreibung
Konfigurationsempfehlung ¹	Die Konfigurationsempfehlungen enthalten umsetzbare Empfehlungen, um auf potenzielle Fehlkonfigurationen und Inkonsistenzen zu reagieren.
Empfehlungen zur Sicherheitssicherung ¹	Empfehlungen zur Sicherheitsaushärtung stellen eine automatisierte Lösung mit allgemeinen Empfehlungen für jeden fehlgeschlagenen Härtungstest dar, die die zugrunde liegenden Sicherheitsprobleme klar und prägnant ansprechen.

¹ Unterstützt Geräte- und Telemetrieverbindungen über Cisco IQ Link, Intersight, Meraki, SD-WAN Manager und WebEx Control Hub.

Erste Schritte für Administratoren


Wenn Sie sich zum ersten Mal bei Ihrem neu erstellten oder migrierten Cisco IQ-Konto anmelden, wird auf der Willkommenseite eine Einführung angezeigt. Der "Get Started"-Prozess hängt davon ab, ob das Konto mit oder ohne migrierte Daten erstellt wurde.

 Anmerkung: Das Get Started Journey-Erlebnis hängt von den rollenbasierten Zugriffsberechtigungen ab.

Neues Konto über Erstellung

Der "Get Started"-Prozess für neu erstellte Kunden führt Sie durch die ersten Schritte zur Integration, die Sie zur Konfiguration Ihrer Cisco IQ-Umgebung und zur Erkundung des Cisco IQ durchführen müssen.


Vernetzung von Cisco Cloud-Produkten

 Anmerkung: Sie müssen mindestens ein (1) Cloud-Produkt anschließen, damit dieser Schritt abgeschlossen werden kann.

Die Verbindung Ihrer Cisco Cloud-Produktdaten mit Cisco IQ ist der schnellste Weg, um die leistungsstarken und personalisierten Funktionen zu nutzen. Sie erhalten innerhalb von Minuten nach der Einrichtung Ihrer Datenverbindungen maßgeschneiderte Einblicke.

Informationen zur Verbindung Ihrer Cisco Cloud-Produkte finden Sie unter [Data Connectors](#).


Verknüpfung von Serviceverträgen

 Anmerkung: Sie müssen mindestens einen (1) Servicevertrag verknüpfen, damit dieser Schritt abgeschlossen werden kann.

Durch die Verknüpfung von Verträgen werden Daten aus Verträgen mit unterschiedlichen Teammitgliedern zusammengeführt. Außerdem werden Ressourcen einbezogen, die nicht über Telemetrie mit Ihrem Bestand verbunden sind. So wird ein zentraler Überblick über die Supportabdeckung ermöglicht, und es werden Überraschungen bei Verlängerungen vermieden.

Informationen zum Verknüpfen Ihrer Serviceverträge finden Sie unter [Serviceverträge](#).


Anschließen von Geräten am Standort

 Anmerkung: Sie müssen mindestens einen (1) Cisco IQ-Link registrieren, damit dieser Schritt abgeschlossen werden kann.

Um die Kommunikation mit Ihren lokalen Geräten herzustellen, müssen Sie Cisco IQ Link konfigurieren. Cisco IQ Link bietet die gesamte Leistung von Cisco IQ für Ihre Geräte vor Ort, die noch nicht über eine Cisco Cloud-Plattform verwaltet werden. Cisco IQ Link kann als virtuelles System in Ihrem Rechenzentrum installiert und mit Ihrem Cisco IQ-Konto verknüpft werden.

Weitere Informationen zum Anschließen der Geräte am Standort finden Sie unter [Data Connectors](#).

Verwalten des Benutzerzugriffs

 Anmerkung: Sie müssen mindestens zwei (2) Benutzer hinzufügen, damit dieser Schritt abgeschlossen werden kann.

Die Funktionen zur einfachen Zugriffskontrolle von Cisco IQ sind für kleine Teams und große Unternehmen konzipiert. Sie können Benutzer hinzufügen und Gruppen und Einzelpersonen Administrator- oder Nur-Anzeige-Rollen zuweisen.

Informationen zum Hinzufügen von Benutzern und zum Zuweisen von Berechtigungen finden Sie unter [Benutzer](#).

Cisco IQ

Informieren Sie sich über die Funktionen und Anwendungen von Cisco IQ, die Ihnen zur Verfügung stehen:

- Launchpad: Zugriff auf Anwendungen, Erkennung neuer Funktionen und Erstellung von Dashboards
- Anwendung für Ressourcen: Weitere Informationen finden Sie unter [Anwendungen](#) für [Ressourcen](#)
- Bewertungsanwendung: Weitere Informationen finden Sie unter [Anträge](#) auf Leistungsbeurteilungen.
- Support-Anwendung: Weitere Informationen finden Sie unter [Support Application](#)
- Cisco IQ AI Assistant: Weitere Informationen finden Sie unter [AI Assistant](#)
- Systemeinstellungen: Verwalten Sie Ihre Kontoeinstellungen, gewähren Sie Benutzern

Zugriff, konfigurieren Sie Datenverbindungen, und zeigen Sie Aktivitäten und Protokolle für Ihr Konto an. Weitere Informationen finden Sie unter [Systemeinstellungen](#).

Neuer Kunde über Migration

Wenn Ihr neues Cisco IQ-Konto im Rahmen einer Migration erstellt wurde, sind die Informationen Ihres vorherigen Kontos bereits verfügbar. Daher beschränkt sich der Einstieg für neu migrierte Kunden auf die Überprüfung der Migration (siehe unten).

Überprüfen der Migration

So überprüfen Sie die Migration:

- Überprüfen Sie Ihre erfolgreich migrierten Verträge unter Home > System Settings > Service Contracts.
- Überprüfen Sie, ob alle erforderlichen Datenverbindungen ordnungsgemäß konfiguriert sind unter Home > System Settings > Data Connectors
- Überprüfen Sie die erfolgreich migrierten Benutzerdaten, und gewähren Sie migrierten Benutzern Zugriff, indem Sie ihre Konten unter Home > System Settings > Identity & Access > Users aktivieren.
- Überprüfen Sie, ob Ihre Ressourcen unter Startseite > Ressourcen > Bestand erfolgreich migriert wurden.

Erste Schritte für allgemeine Benutzer

Wenn Sie sich zum ersten Mal bei Ihrem Cisco IQ-Konto anmelden, wird auf der Willkommenseite die Kampagne "Erste Schritte" angezeigt. Dieser Weg führt Sie durch die Cisco IQ-Funktionen und die gängigen Workflows.

 Anmerkung: Das Get Started Journey-Erlebnis hängt von den RBAC-Berechtigungen ab.

Cisco IQ

Informieren Sie sich über die Funktionen und Anwendungen von Cisco IQ, die Ihnen zur Verfügung stehen:

- Launchpad: Zugriff auf Anwendungen, Erkennung neuer Funktionen und Erstellung von Dashboards
- Anwendung für Ressourcen: Weitere Informationen finden Sie unter [Anwendungen für Ressourcen](#)
- Bewertungsanwendung: Weitere Informationen finden Sie unter [Anträge](#) auf Leistungsbeurteilungen.
- Support-Anwendung: Weitere Informationen finden Sie unter [Support Application](#)
- Cisco IQ AI Assistant: Weitere Informationen finden Sie unter [AI Assistant](#)

Erstellen Ihres ersten KI-Berichts

Die KI-gestützte Analysefunktion von Cisco IQ generiert anpassbare, zielgerichtete Berichte, die auf ausgewählten Ressourcen basieren und an Ihre spezifischen geschäftlichen Anforderungen angepasst werden können.

Weitere Informationen zur Erstellung Ihres ersten KI-Berichts finden Sie im [Anlagenantrag](#).

Stellen einer Frage an den Cisco IQ AI Assistant

Der letzte Schritt besteht darin, den Cisco IQ AI Assistant von jedem Standort aus zu starten und Fragen zu Ihren Ressourcen, Tickets oder Bewertungen zu stellen.

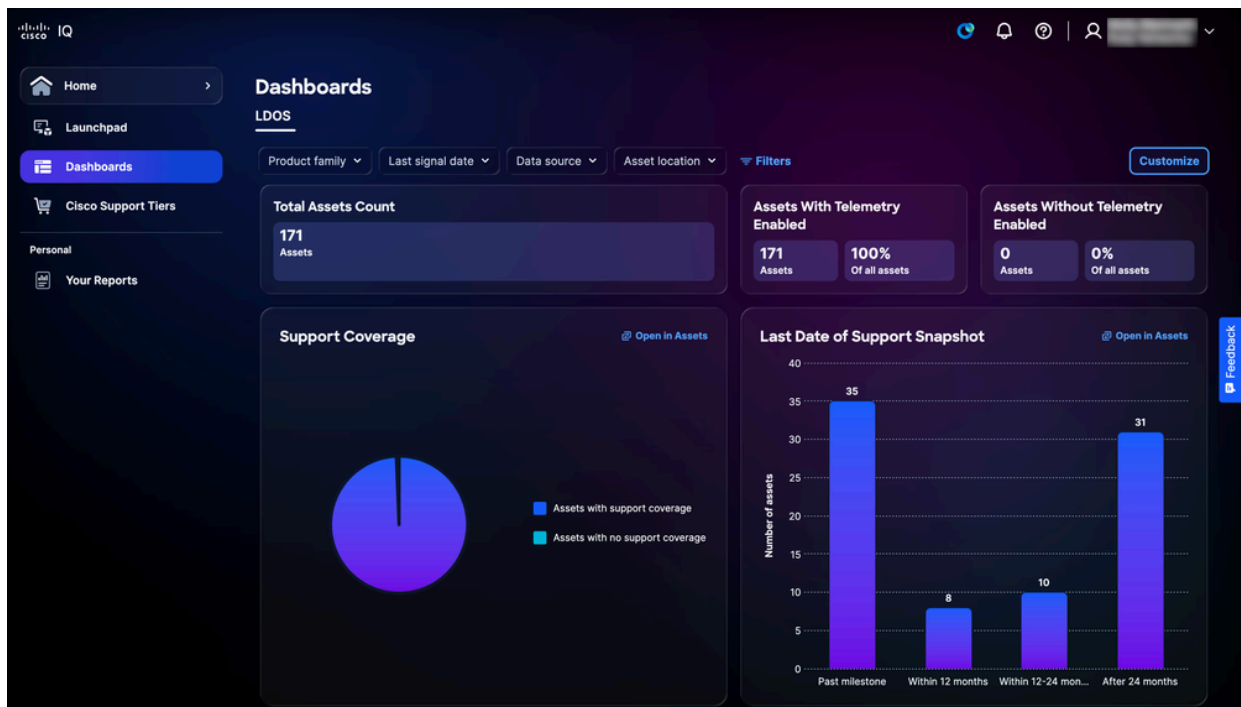
Weitere Informationen zur Verwendung des Cisco IQ AI Assistant finden Sie unter [AI Assistant](#).

Dashboards

Die Registerkarte Dashboards bietet eine Ansicht der folgenden verfügbaren Dashboards in Cisco IQ.

LDOS-Dashboard


Das LDOS Dashboard bietet umfassende und detaillierte Einblicke in LDOS-Metriken und ermöglicht so die Transparenz für Kunden, das proaktive Risikomanagement für Benutzer und eine effizientere und fundiertere Entscheidungsfindung.




LDOS-Dashboard

Filtern von Ansichten für LDOS Dashboard

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

 Anmerkung: Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet.

 Anmerkung: Je nach den Rollen und Berechtigungen des Benutzers stehen verschiedene Filter zur Verfügung.

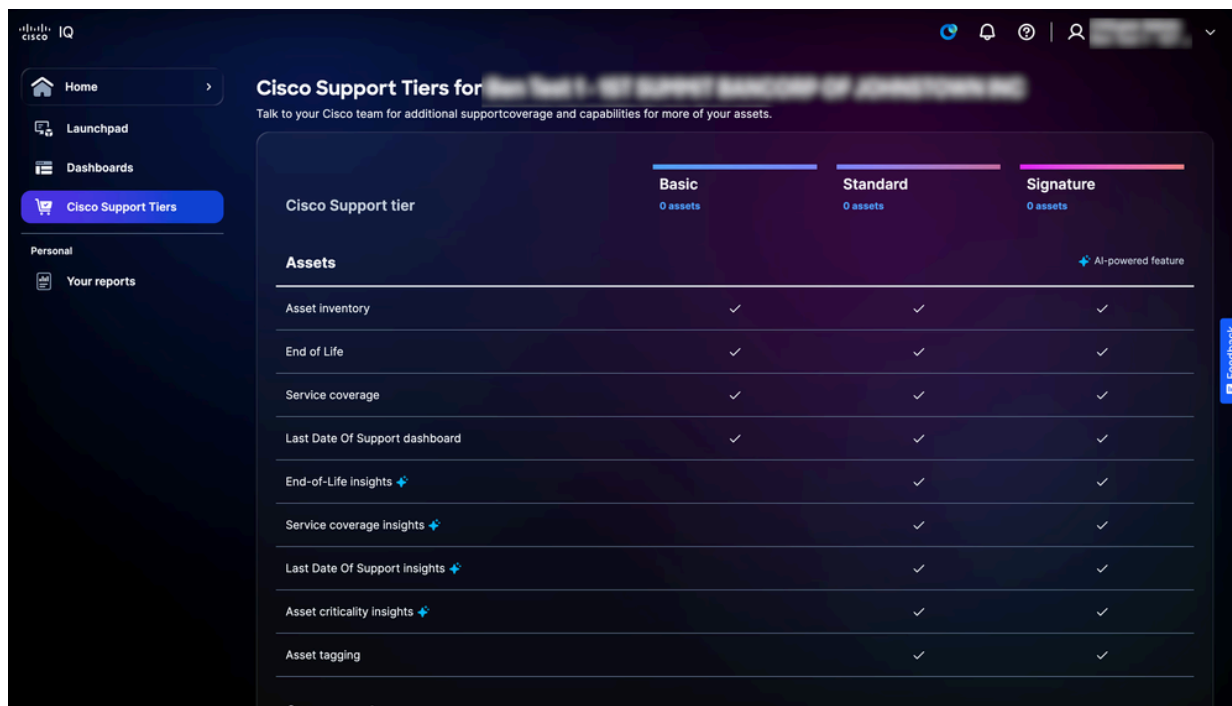
Anzeigen von Details für das LDOS Dashboard

Wenn Sie auf In Anlagen öffnen klicken, wird die Seite zur Seite Bestand umgeleitet. Weitere Informationen finden Sie unter [Bestand](#).

Cisco Support-Stufen

Die Seite für die Cisco Support-Stufen bietet einen Überblick über die Funktionen der erworbenen Support-Stufe und die Anzahl der Ressourcen im Zusammenhang mit verknüpften Support-

Verträgen. So können Sie die enthaltenen Support-Funktionen leicht verstehen und entsprechende Maßnahmen zu deren Verwaltung und Überprüfung ergreifen. Detailliertere Informationen zu den Funktionen der Support-Stufe finden Sie unter [Support-Stufen](#).



Cisco Support-Stufen

Ihre Berichte

Mit der Funktion "Berichte" können Sie KI-generierte Einblicke aus dem gesamten Cisco IQ zentralisieren und verwalten, indem Sie sie in einer personalisierten Liste Ihrer Berichte speichern. So können Sie schnell und sicher auf Ihre eigenen Daten zugreifen.

The screenshot shows the Cisco IQ Reports interface. On the left is a navigation sidebar with options like Home, Launchpad, Dashboards, Cisco Support Tiers, and Personal. The main area is titled 'Reports' and contains a 'Saved Reports' section. This section has a search bar, a 'Created' dropdown, a 'Select created from' dropdown, and a '4 results' indicator. Below this is a table with the following data:

Report Name	Description	Created	Created from	
> Past-LDOS Assets Ove...	Summary of 52 assets past Last Date of Support,...	Apr 20, 2026, 4:...	Assets (AI Assistant)	...
> Security Advisory Expo...	Overview of security advisories sorted by affecte...	Apr 20, 2026, 3:...	Assessments	...
> Security Advisory Expo...	Overview of security advisories sorted by affecte...	Apr 20, 2026, 3:...	Assessments	...
> Asset Inventory Risk O...	Critical coverage gaps, lifecycle deadlines, and te...	Apr 20, 2026, 3:...	Assets	...

At the bottom right of the table area, it says 'Rows per page 30 1-4 of 4'. A 'Feedback' button is visible on the right edge of the interface.

Ihre Berichte

Systemeinstellungen

Um zum Menü Systemeinstellungen zu navigieren, wählen Sie Home > System Settings (Startseite > Systemeinstellungen). Die Seite "Kontodetails" wird angezeigt.

 Anmerkung: Die Systemeinstellungen stehen nur Kontoadministratoren zur Verfügung.

Kontodetails


Die Funktion "System Settings" (Systemeinstellungen) vereinfacht Verwaltung, Zugriffskontrolle und Datenzuweisung und stellt umfassende Transparenz und Zugriffsmöglichkeiten für Kontoadministratoren sicher. Wenn Sie die Seite Kontodetails anzeigen, werden im Abschnitt Details folgende Informationen angezeigt:

- Kontoname
- Kontotyp
- Datenspeicherbereich
- Benutzer
- Datum erstellen

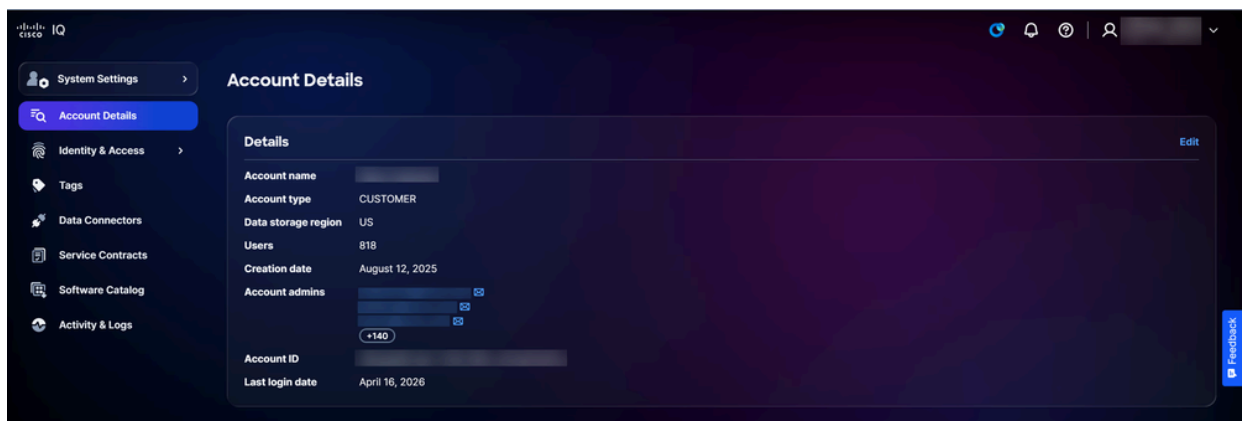
- Kontoadministratoren
- Konto-ID
- Letztes Anmeldedatum

Kontoname bearbeiten

Nur der Kontoname kann auf der Seite Kontendetails geändert werden.

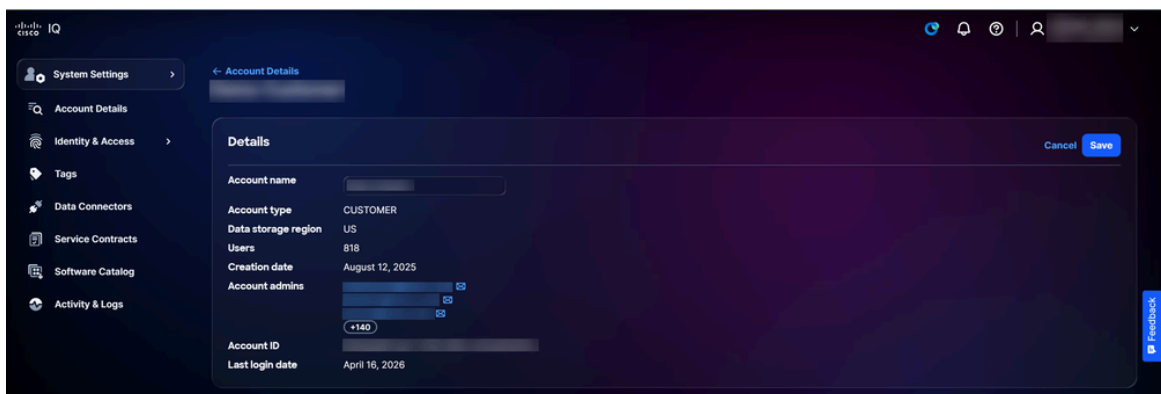
 Anmerkung: Zum Ändern von Feldern, z. B. des Datenspeicherbereichs, muss ein neues Unternehmenskonto erstellt werden.

So bearbeiten Sie einen Kontonamen:



Kontodetails

1. Klicken Sie auf Bearbeiten.



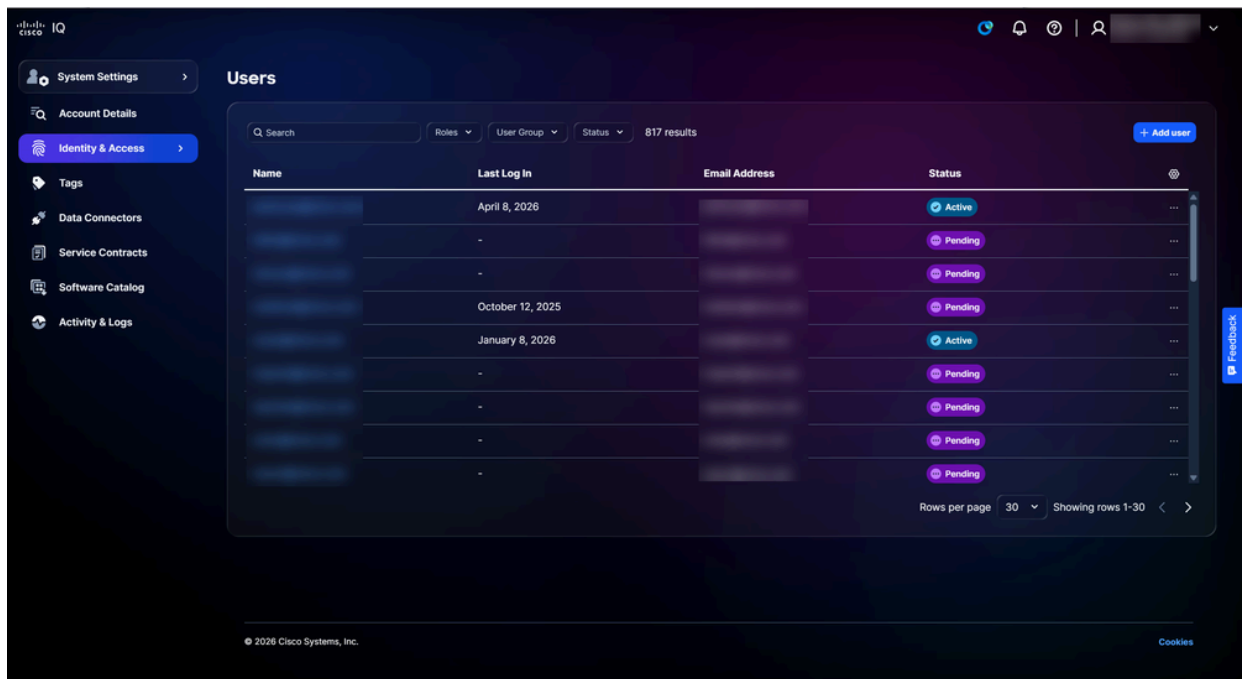
Kontoname bearbeiten

2. Korrigieren Sie den Kontonamen.

3. Klicken Sie auf Speichern.

Benutzer

Benutzerkonten werden auf der Seite Benutzer erstellt, geändert und gelöscht. Um zur Seite "Benutzer" zu navigieren, wählen Sie Systemeinstellungen > Identität und Zugriff > Benutzer aus. Die Seite Benutzer wird angezeigt.




Benutzer

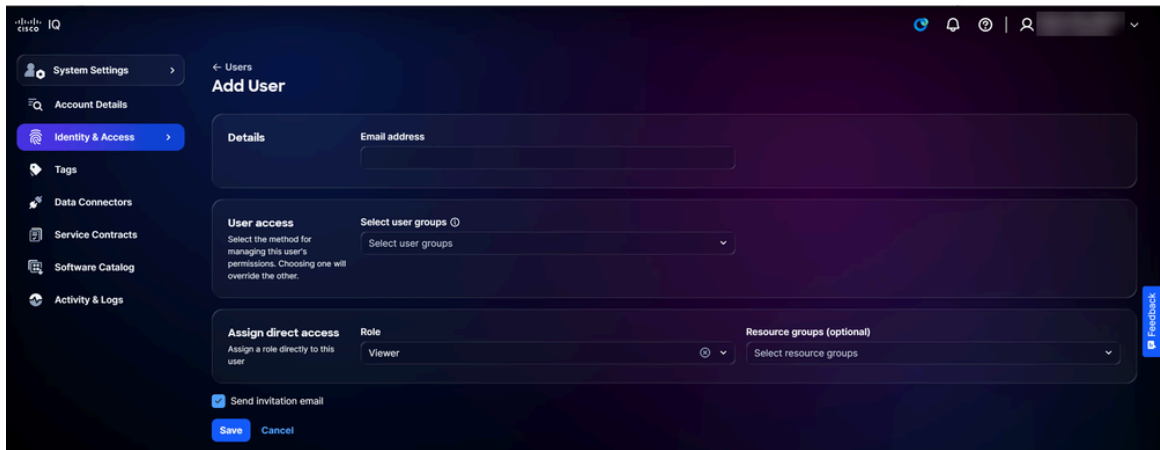
Sie können die Liste mithilfe der Felder am oberen Seitenrand eingrenzen, indem Sie nach Suchen und Filtern suchen.

Hinzufügen neuer Benutzer

So fügen Sie einen neuen Benutzer hinzu

 Anmerkung: Nur Kontoadministratoren oder andere autorisierte Benutzer können neue Benutzer hinzufügen.

1. Klicken Sie auf der Seite Benutzer auf Benutzer hinzufügen. Die Seite Benutzer hinzufügen wird angezeigt.




Benutzer hinzufügen

2. Geben Sie eine E-Mail-Adresse ein.
3. Wählen Sie optional die Benutzergruppe(n) aus der Dropdown-Liste Benutzergruppen auswählen aus.
4. Wählen Sie die Rolle aus der Dropdown-Liste aus.

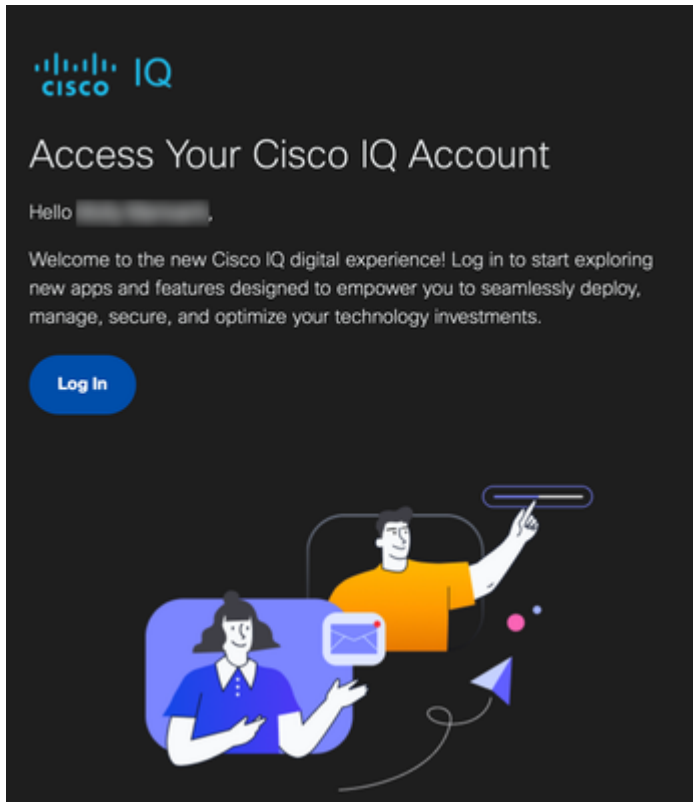
 Anmerkung: Benutzer müssen mindestens einer Benutzergruppe mit einer Rolle angehören oder mindestens einer Rolle zugewiesen sein.

5. Wählen Sie optional die Ressourcengruppen aus der Dropdown-Liste aus.

 Anmerkung: Die Dropdown-Liste Ressourcengruppen wird nur für ausgewählte Rollen angezeigt.

6. Vergewissern Sie sich, dass das Kontrollkästchen Einladungs-E-Mail senden aktiviert ist.
7. Klicken Sie auf Speichern. Auf der Seite "Benutzer" wird eine Bestätigung angezeigt.

Benutzer erhalten eine E-Mail, nachdem sie von einem Kontoadministrator eingeladen wurden.

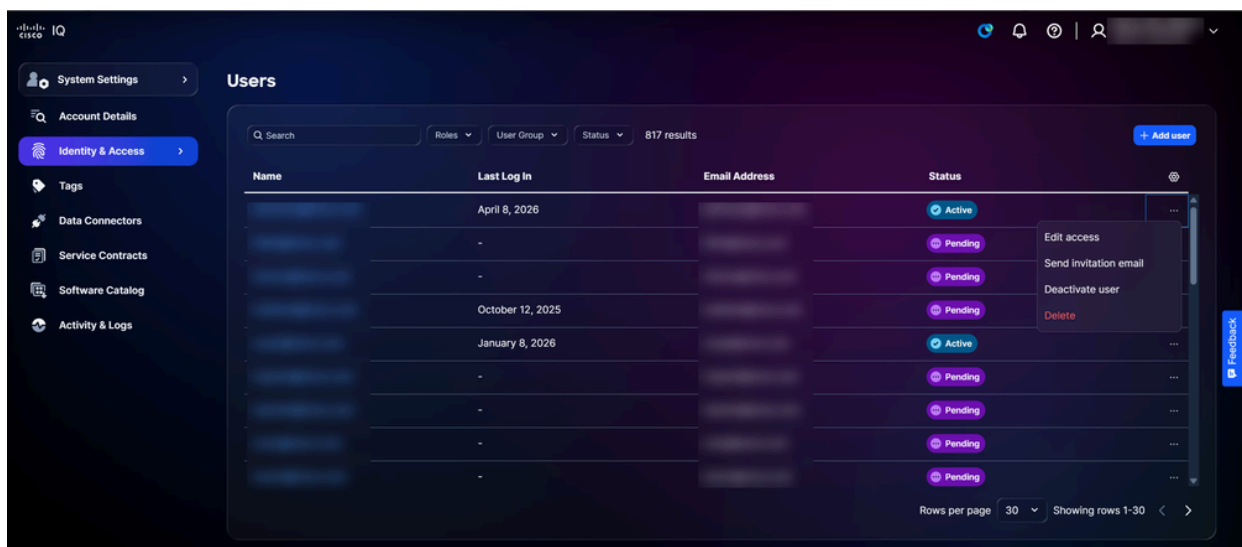


E-Mail-Einladung

Eingeladene Benutzer können auf Anmelden in der E-Mail klicken, um sich bei ihrem Konto anzumelden. Nach der Anmeldung erhält der Benutzer den Status "Aktiv".

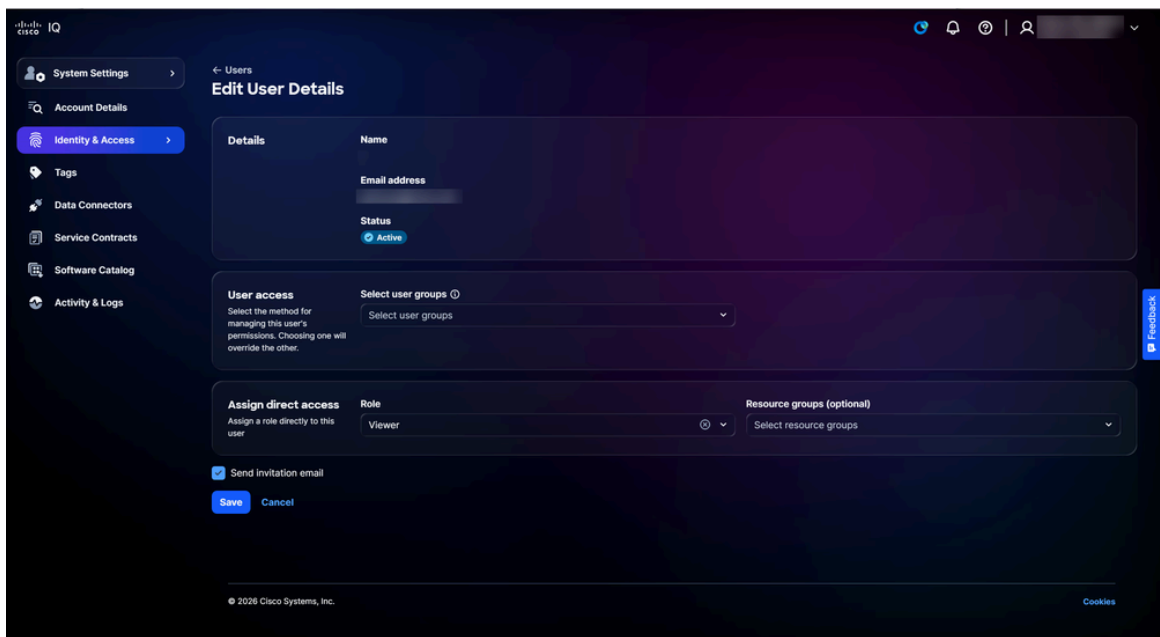
Bearbeiten des Benutzerzugriffs

So bearbeiten Sie die Benutzergruppen, Rollen oder Ressourcengruppen eines Benutzerkontos:



Zugriff bearbeiten

1. Wählen Sie bei einem gewünschten Benutzer auf der Seite Benutzer das Symbol Weitere Optionen > Zugriff bearbeiten aus. Die Seite Benutzerdetails bearbeiten wird angezeigt.



Benutzerdetails bearbeiten

2. Bearbeiten der gewünschten Benutzergruppen, Rollen und Ressourcengruppen.

 Anmerkung: Ressourcengruppen werden nur für ausgewählte Rollen angezeigt.

3. Klicken Sie auf Speichern.

Einladungs-E-Mails versenden

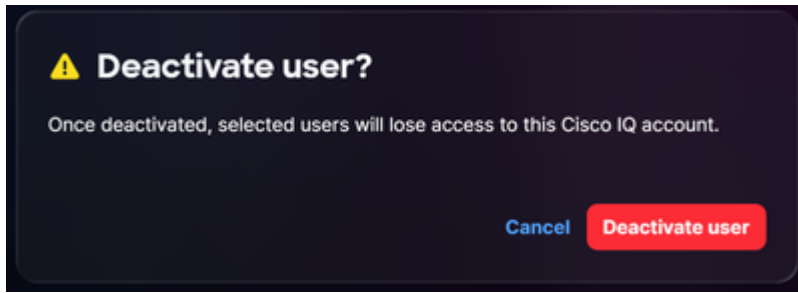
So senden Sie eine Einladungs-E-Mail an ein bestehendes Benutzerkonto:

1. Navigieren Sie zur Seite Benutzer.
2. Wählen Sie bei einem gewünschten Benutzer das Symbol Weitere Optionen > Einladungs-E-Mail senden aus. Es wird eine Bestätigung angezeigt.

Deaktivieren von Benutzern

So deaktivieren Sie ein Benutzerkonto:

1. Wählen Sie bei einem gewünschten Benutzer auf der Seite Benutzer das Symbol Weitere Optionen > Benutzer deaktivieren aus. Das Fenster Benutzer deaktivieren wird geöffnet.



Benutzerbestätigung deaktivieren

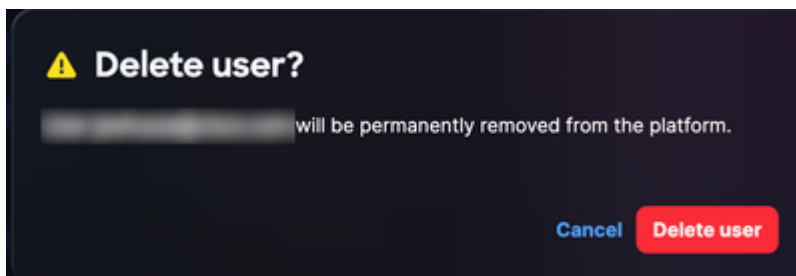
2. Klicken Sie zur Bestätigung auf Benutzer deaktivieren. Es wird eine Bestätigung angezeigt.

Benutzer löschen

 **Warnung:** Benutzer können nicht gelöscht werden.

So löschen Sie einen Benutzer

1. Wählen Sie bei einem gewünschten Benutzer auf der Seite Benutzer das Symbol Weitere Optionen > Löschen aus. Das Fenster Benutzer löschen wird geöffnet.



Löschen des Benutzers bestätigen

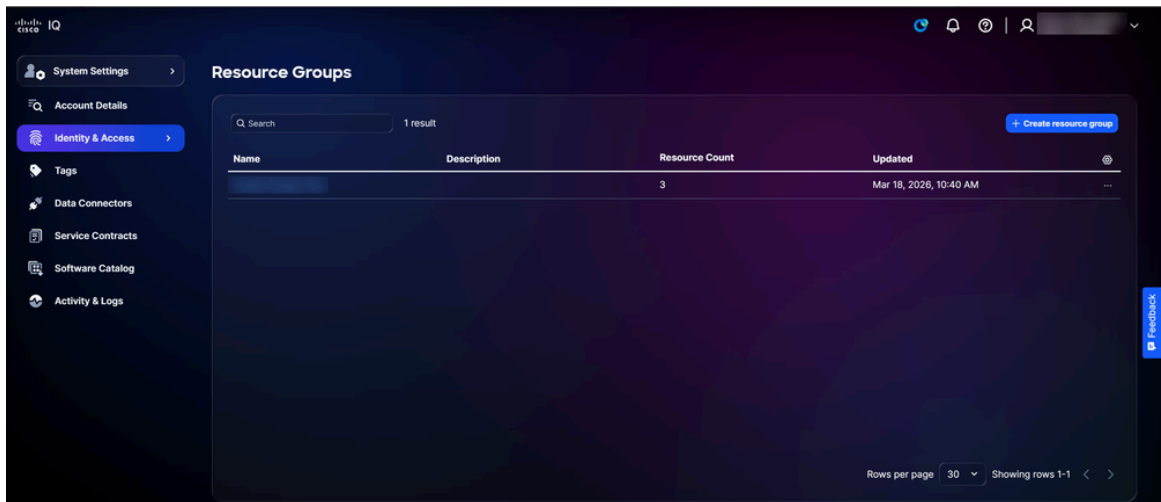
2. Klicken Sie auf Benutzer löschen. Der Benutzer wird gelöscht.

Ressourcengruppen

Ressourcengruppen sind dynamische Auflistungen, die Ressourcen basierend auf ihrem Typ und ihren Attributen angeben. Durch das Konfigurieren von Ressourcengruppen können Sie den Datenzugriff einer Rolle auf die Ressourcen beschränken, die die Bedingungen der Gruppe erfüllen. Ressourcen können mehreren Ressourcengruppen angehören. Als Kontoadministrator können Sie Ressourcengruppen erstellen, bearbeiten und löschen.

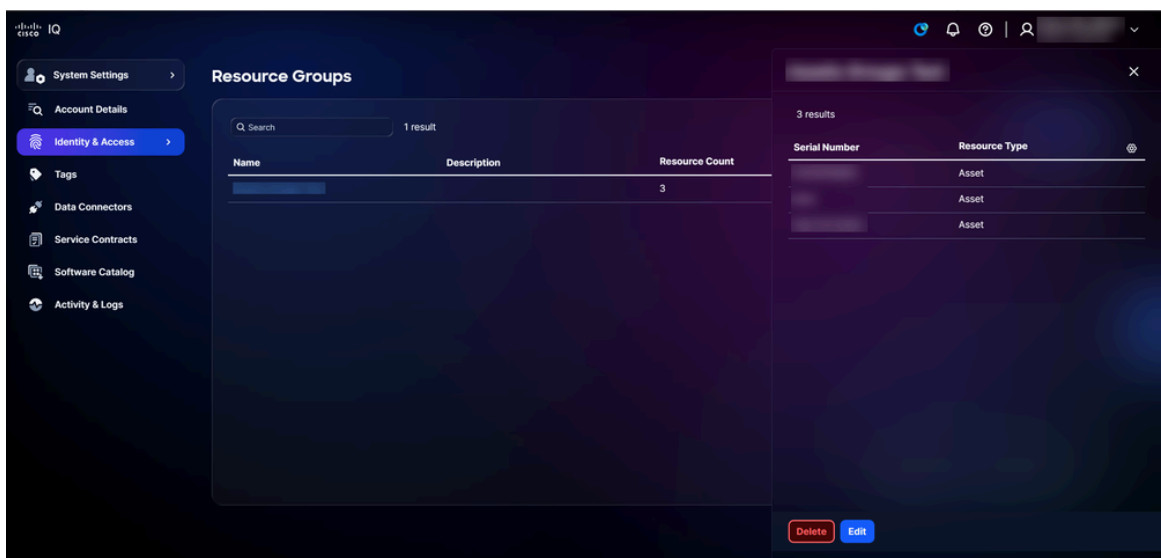
So zeigen Sie Ressourcengruppen an

1. Wählen Sie Systemeinstellungen > Identität und Zugriff > Ressourcengruppen aus. Die Seite "Ressourcengruppen" wird angezeigt.



Ressourcengruppen

2. Verwenden Sie die Felder Suchen und Filtern, um die Liste einzugrenzen.
3. Klicken Sie auf den Namen einer Ressourcengruppe, um deren Details anzuzeigen.

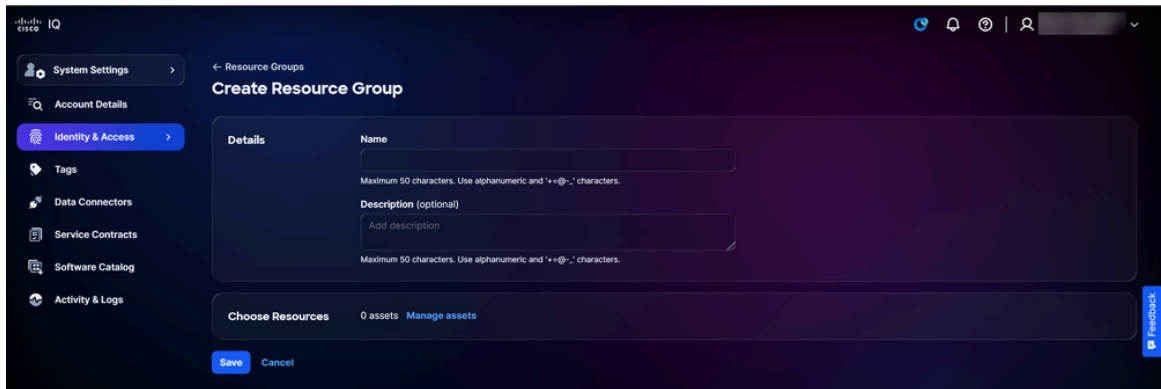


Ressourcengruppen-Details

Ressourcengruppen erstellen

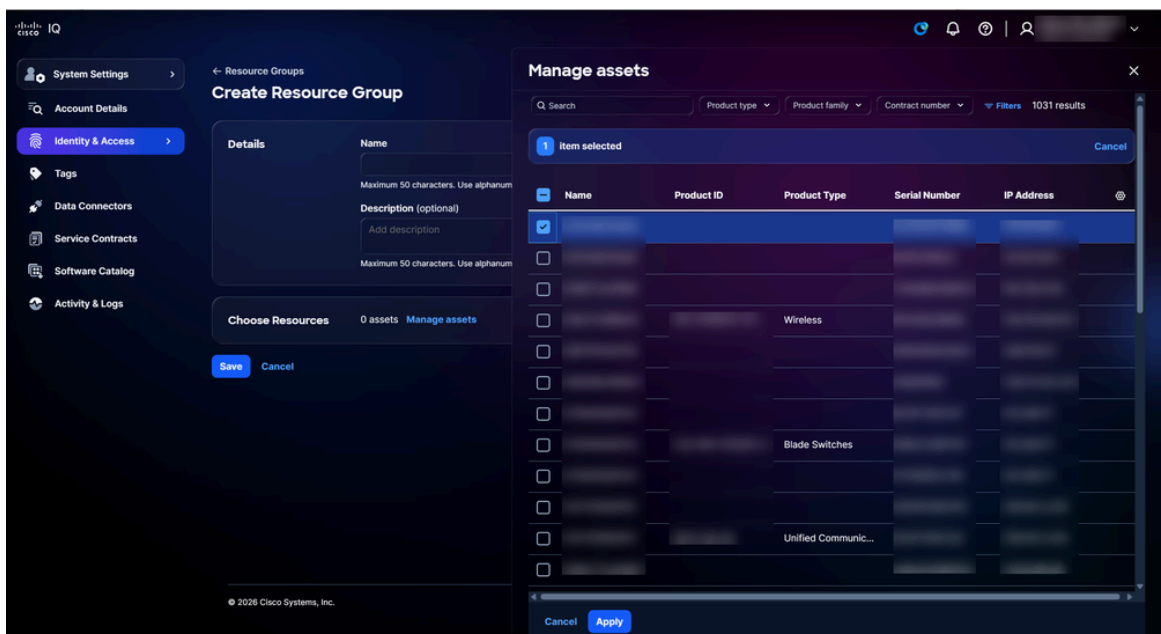
So erstellen Sie eine neue Ressourcengruppe

1. Klicken Sie auf der Seite Ressourcengruppen auf Ressourcengruppe erstellen. Die Seite "Ressourcengruppe erstellen" wird angezeigt.



Ressourcengruppe erstellen

2. Geben Sie einen Namen für die Ressourcengruppe ein.
3. Geben Sie optional eine Beschreibung ein.
4. Klicken Sie auf Ressourcen verwalten. Das Fenster Ressourcen verwalten wird geöffnet.

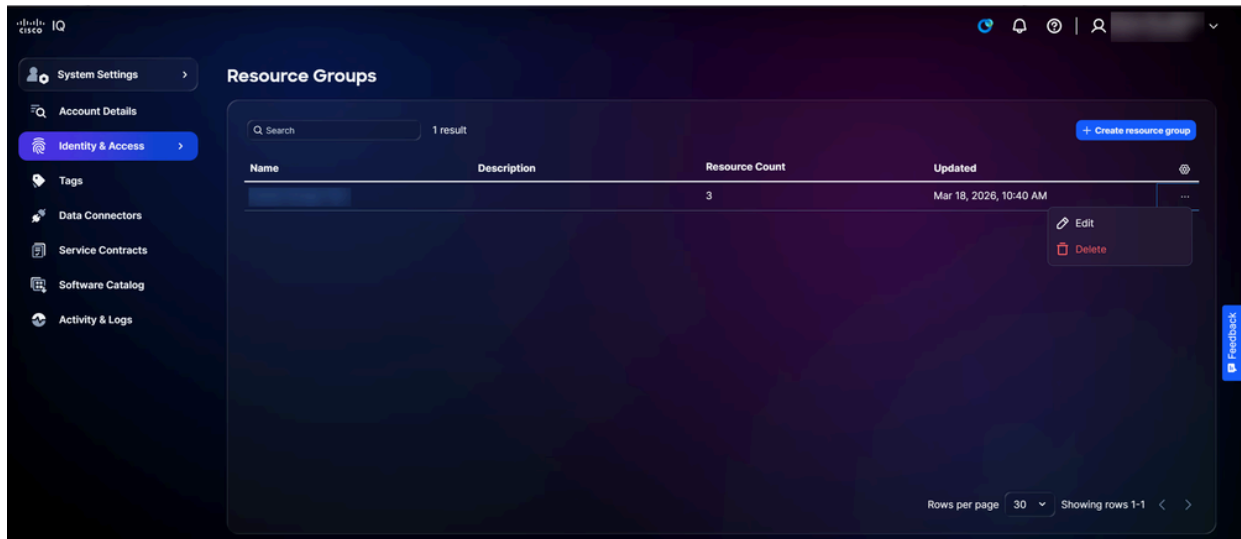


Ressourcen verwalten

5. Aktivieren Sie das Kontrollkästchen für die gewünschten Ressourcen.
6. Klicken Sie auf Apply (Anwenden).
7. Klicken Sie auf Speichern.

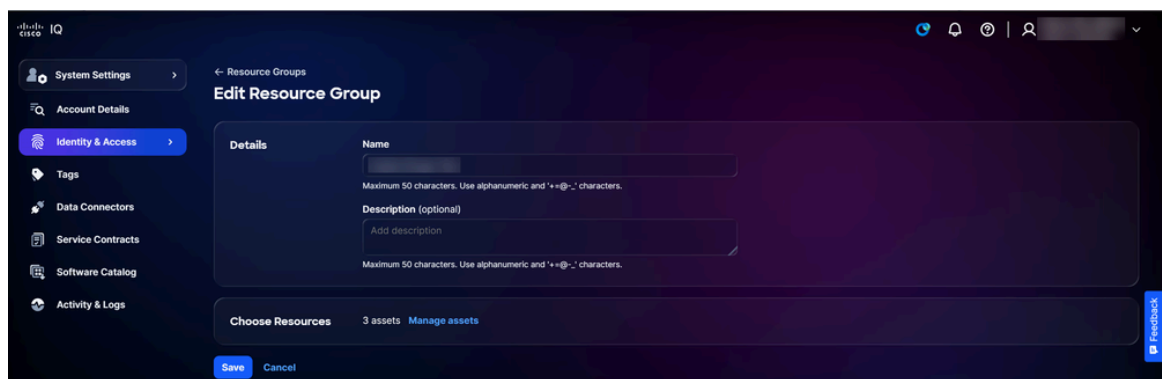
Bearbeiten von Ressourcengruppen

So bearbeiten Sie eine Ressourcengruppe:



Bearbeiten

1. Wählen Sie aus einem Datensatz auf der Seite Ressourcengruppen das Symbol Weitere Optionen > Bearbeiten aus. Die Seite Ressourcengruppe bearbeiten wird angezeigt.



Ressourcengruppe bearbeiten

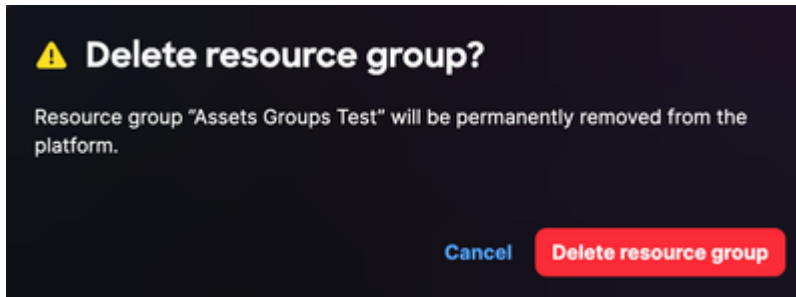
2. Bearbeiten Sie die Ressourcengruppenattribute nach Bedarf.
3. Klicken Sie auf Speichern.

Ressourcengruppen löschen

 **Warnung:** Das Löschen von Ressourcengruppen kann nicht rückgängig gemacht werden.

So löschen Sie eine Ressourcengruppe:

1. Wählen Sie aus einem Datensatz auf der Seite Ressourcengruppen das Symbol Weitere Optionen > Löschen aus. Das Fenster Ressourcengruppe löschen wird geöffnet.




Ressourcengruppe löschen

2. Klicken Sie auf Ressourcengruppe löschen. Die Ressourcengruppe wird gelöscht.

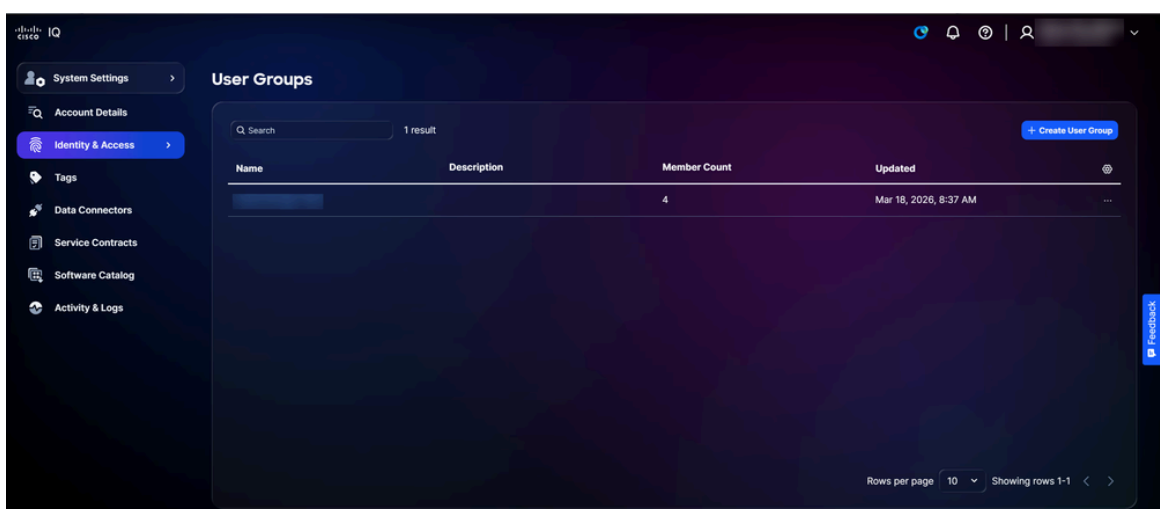
Benutzergruppen

Benutzergruppen ermöglichen Ihnen eine effektive Kontrolle der Benutzer im gesamten Konto, indem Sie Benutzergruppen erstellen, bearbeiten und löschen.

 Anmerkung: Die Benutzergruppe All account users ist standardmäßig auf allen Konten in Cisco IQ vorhanden und kann nicht gelöscht oder bearbeitet werden. Es schließt immer alle Benutzer eines bestimmten Typs ein. Sein Zweck ist es, Rollen auf alle Benutzer des Kontos anzuwenden.

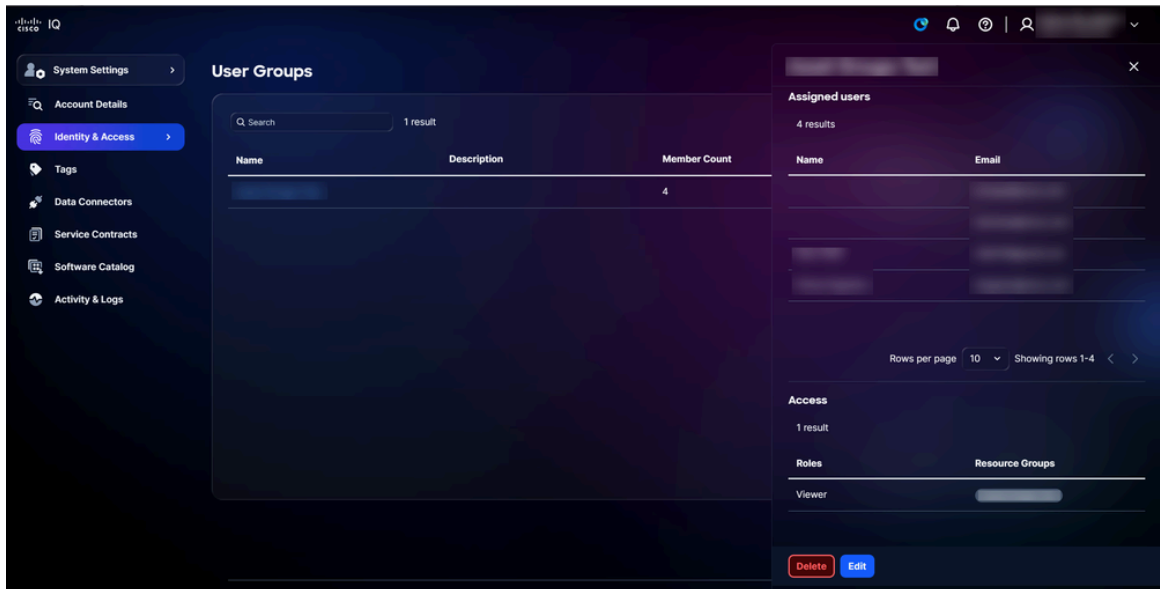
Benutzergruppen anzeigen:

1. Wählen Sie Systemeinstellungen > Identität und Zugriff > Benutzergruppen aus. Die Seite Benutzergruppen wird angezeigt.



Benutzergruppen

2. Verwenden Sie die Felder Suchen und Filtern, um die Liste einzugrenzen.
3. Klicken Sie auf den Namen einer Benutzergruppe, um deren Details anzuzeigen.

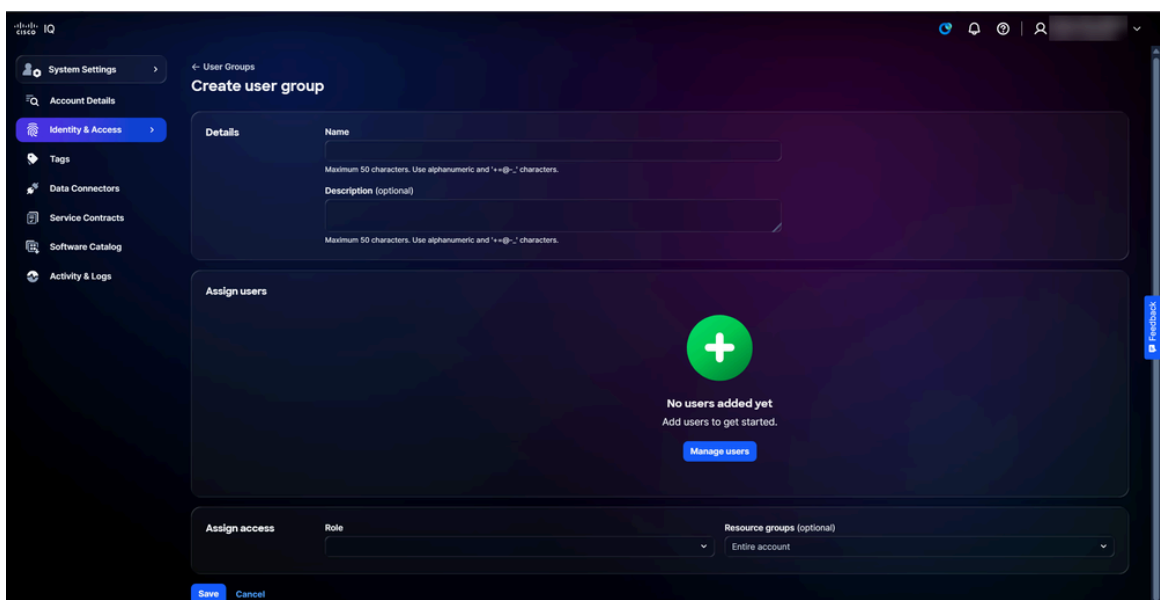


Benutzergruppendetails

Erstellen von Benutzergruppen

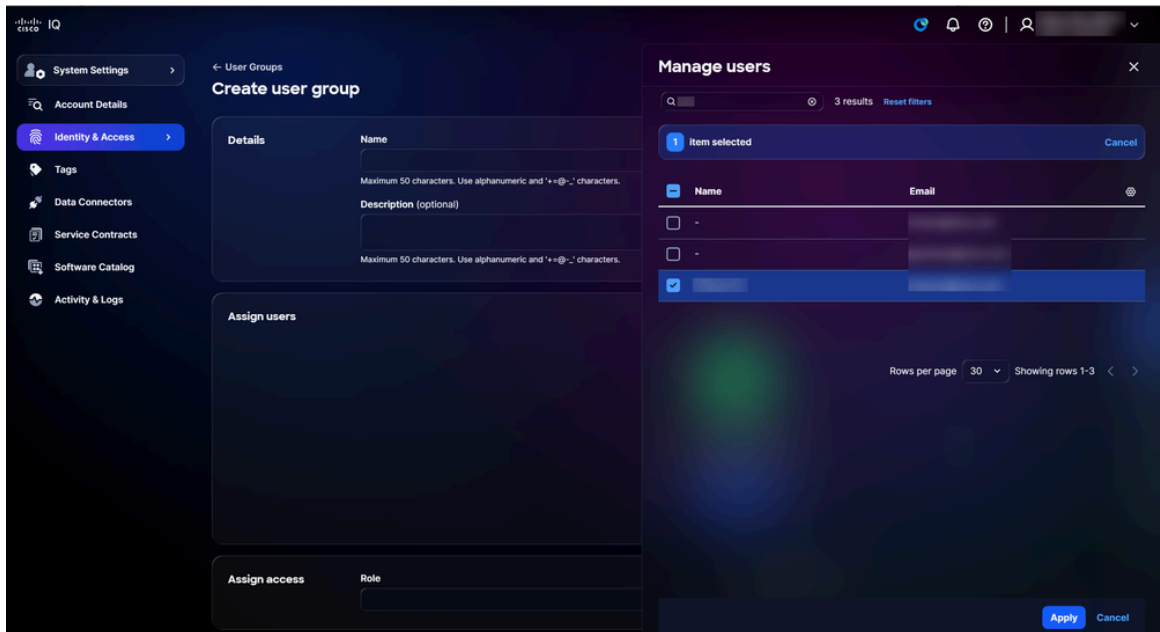
So erstellen Sie eine neue Benutzergruppe

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




Benutzergruppe erstellen

2. Geben Sie einen Namen für die Benutzergruppe ein.
3. Geben Sie optional eine Beschreibung ein.
4. Klicken Sie auf Benutzer verwalten. Das Fenster Benutzer verwalten wird geöffnet.



Benutzer verwalten

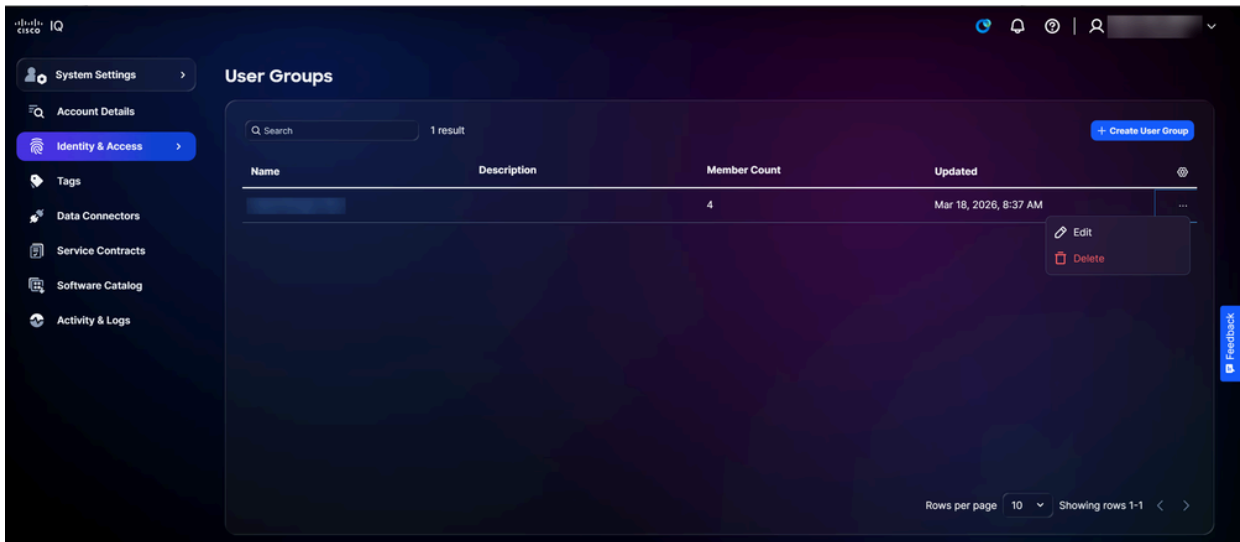
5. Aktivieren Sie die Kontrollkästchen der gewünschten Benutzer.
6. Klicken Sie auf Apply (Anwenden).
7. Wählen Sie eine Rolle aus der Dropdown-Liste aus.
8. Wählen Sie optional eine Ressourcengruppe aus der Dropdown-Liste aus.

 Anmerkung: Durch das Hinzufügen von Ressourcengruppen werden die Ressourcen eingeschränkt, auf die die Benutzergruppe Zugriff hat. Wenn eine Rolle zugewiesen wurde, aber keine Ressourcengruppen ausgewählt wurden, wird die Rolle auf alle Ressourcen angewendet, die für die Rolle im Konto relevant sind.

9. Klicken Sie auf Speichern. Die neue Benutzergruppe wird in der Tabelle Benutzergruppen angezeigt.

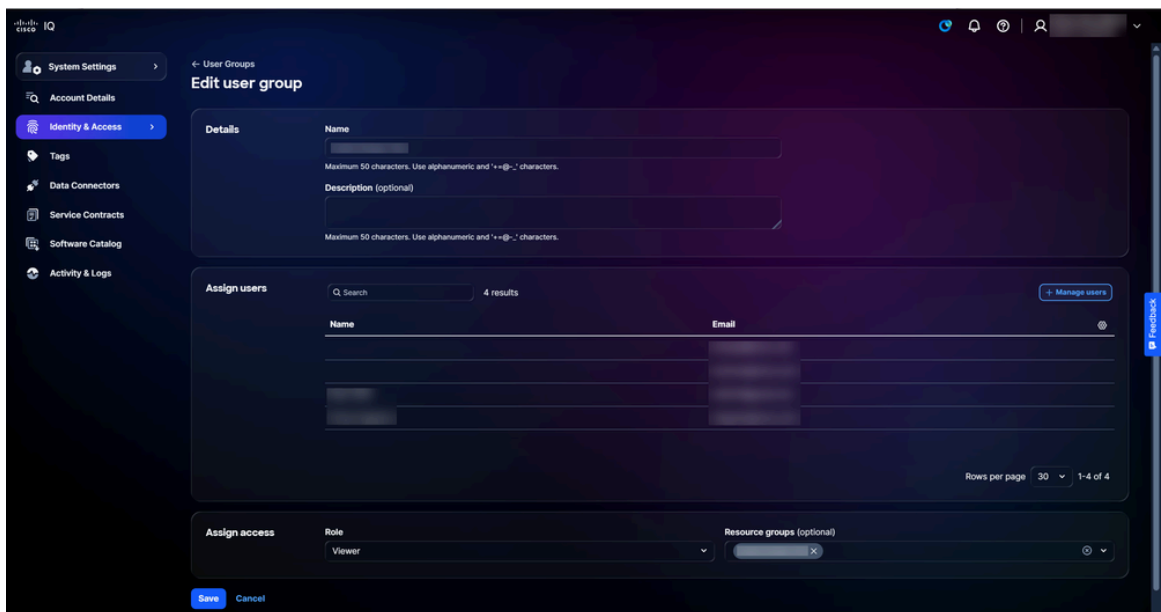
Benutzergruppen bearbeiten

So bearbeiten Sie eine Benutzergruppe:



Bearbeiten

1. Wählen Sie aus einem Datensatz auf der Seite Benutzergruppen das Symbol Weitere Optionen > Bearbeiten aus. Die Seite Benutzergruppe bearbeiten wird angezeigt.



Benutzergruppe bearbeiten

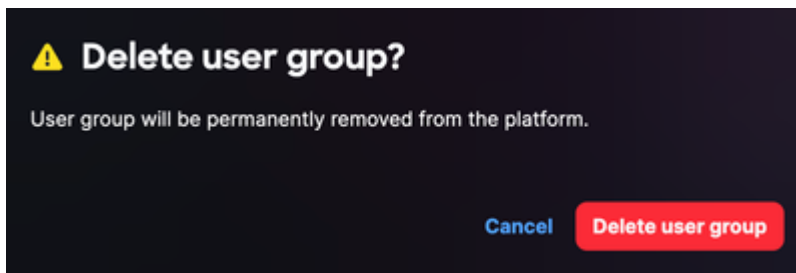
2. Bearbeiten Sie die Benutzergruppenattribute nach Bedarf.
3. Klicken Sie auf Speichern.

Benutzergruppen löschen

 **Warnung:** Das Löschen von Benutzergruppen kann nicht rückgängig gemacht werden.

So löschen Sie eine Benutzergruppe:

1. Wählen Sie aus einem Datensatz auf der Seite Benutzergruppen das Symbol Weitere Optionen > Löschen aus. Das Fenster Benutzergruppe löschen wird geöffnet.



Benutzergruppe löschen

2. Klicken Sie auf Benutzergruppen löschen. Die Benutzergruppe wird gelöscht.

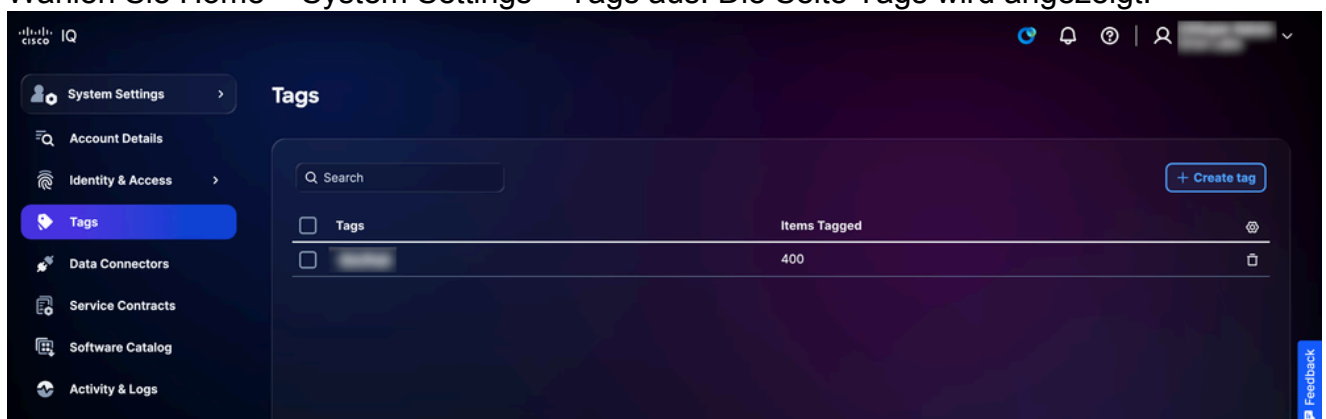
Tags

Asset-Tags sind benutzerdefinierte Labels, die Sie Inventarressourcen im Cisco IQ zuweisen. Ein Tag ist ein von Ihnen definiertes Schlüssel-Wert-Paar, z. B. Environment:Prod oder Label:Campus. Kontoadministratoren können Tags erstellen und löschen und Benutzer einer Ressourcengruppe zuweisen, sodass sie einem Gerät Asset-Tags zuweisen können. Weitere Informationen zum Zuordnen von Benutzern zu einer Ressourcengruppe finden Sie unter [Ressourcengruppen](#).

Erstellen von Asset-Tags

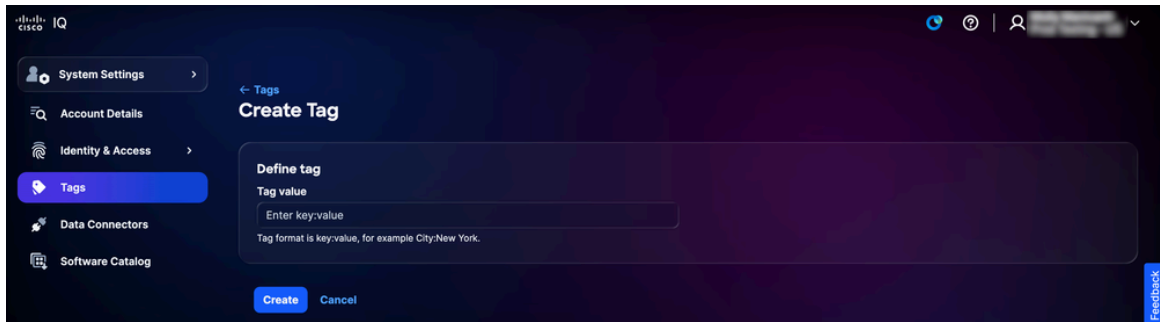
So erstellen Sie ein Tag:

1. Wählen Sie Home > System Settings > Tags aus. Die Seite Tags wird angezeigt.




Tags

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



Tag erstellen

3. Geben Sie den Tag-Wert in das Feld Enter key:value ein.

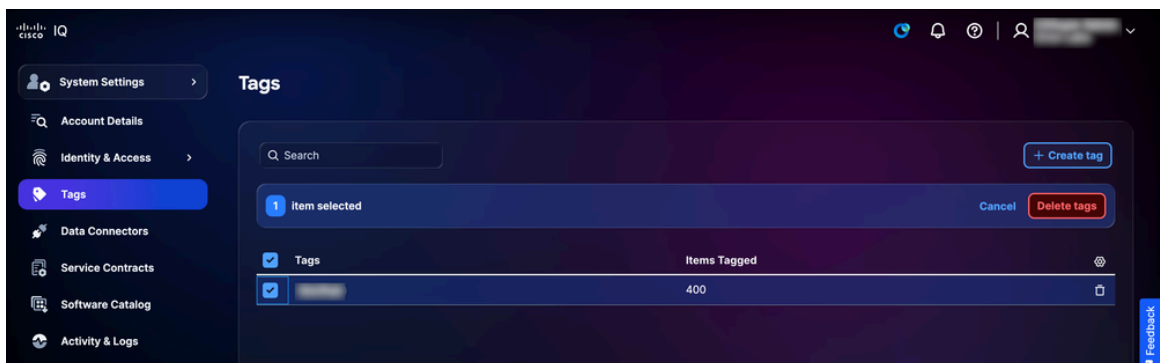
 Anmerkung: Tagnamen haben das Format key:value (z. B. City:NYC).

4. Klicken Sie auf Erstellen. Das neue Tag wird in der Tag-Liste auf der Seite Tags angezeigt.

Bestandskennungen löschen

So löschen Sie ein Tag:

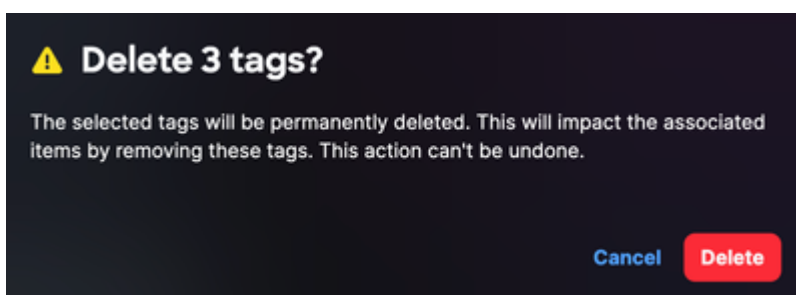
1. Wählen Sie Home > System Settings > Tags aus. Die Seite Tags wird angezeigt.



Tags

2. Aktivieren Sie das bzw. die Kontrollkästchen der zu löschenden Tags.

3. Klicken Sie auf Tags löschen. Es wird eine Bestätigung angezeigt.



Stichwort löschen

4. Klicken Sie zur Bestätigung auf Löschen.

Data Connectors

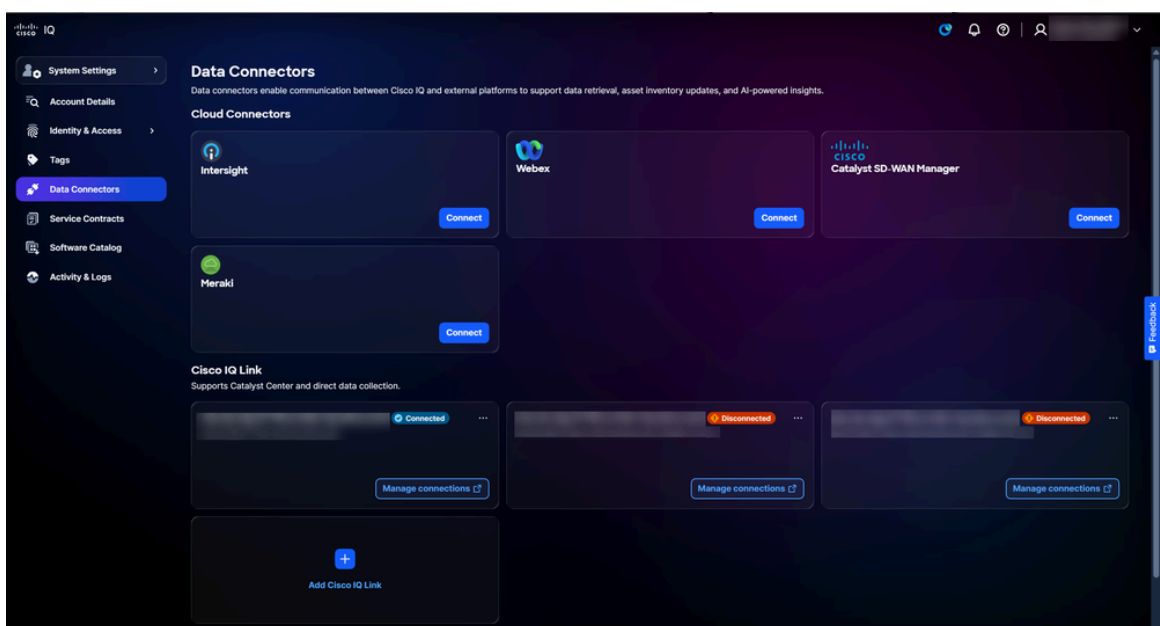
Cisco IQ nutzt Data Connectors als Teil eines mehrschichtigen Datenerhebungsansatzes, um umfassende Netzwerkinformationen bereitzustellen. Data Connectors sammeln Telemetriedaten zu Ressourcen in Ihrem Netzwerk, sodass Cisco IQ relevante Informationen und Fachwissen bereitstellen kann.

Hinzufügen von Cloud Connectors

Die Verbindung Ihrer Cisco Cloud-Produktdaten mit Cisco IQ ist der schnellste Weg, um die leistungsstarken und personalisierten Funktionen zu nutzen. Sie erhalten innerhalb von Minuten nach der Einrichtung Ihrer Datenverbindungen zu den folgenden Produkt-Controllern maßgeschneiderte Einblicke: Intersight®, Meraki Dashboard, SD-WAN Manager, WebEx® Control Hub

So vernetzen Sie Ihre Cisco Cloud-Produkte:

1. Wählen Sie Systemeinstellungen > Datenverbindungen aus. Die Seite Data Connectors wird angezeigt.

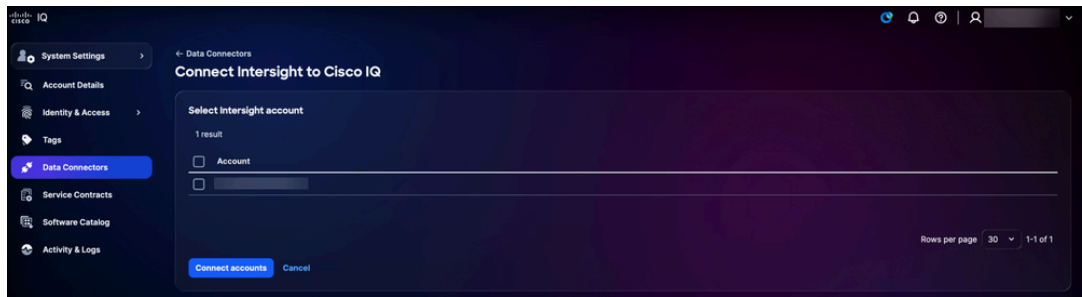


Cloud Connectors

2. Klicken Sie auf Verbinden, um den gewünschten Cloud Connector zu erhalten.

3. Führen Sie für den ausgewählten Cloud Connector die folgenden Schritte aus:

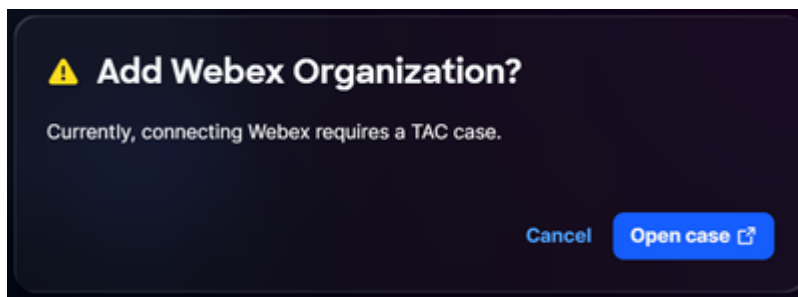
- Intersight



Intersight verbinden

1. Aktivieren Sie das bzw. die Kontrollkästchen der gewünschten Konten.
2. Klicken Sie auf Konten verbinden. Sie werden zur Seite Data Connectors weitergeleitet und eine Bestätigung wird angezeigt.

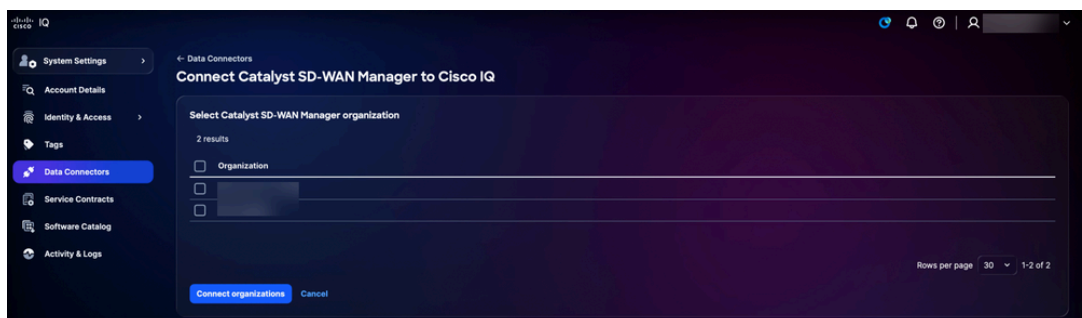
- Webex



WebEx verbinden

1. Klicken Sie im Fenster Add WebEx Organization (WebEx Organisation hinzufügen) auf Open case. Sie werden an SCM weitergeleitet.
2. Erstellen eines Support-Tickets in SCM

- Catalyst SD-WAN-Manager

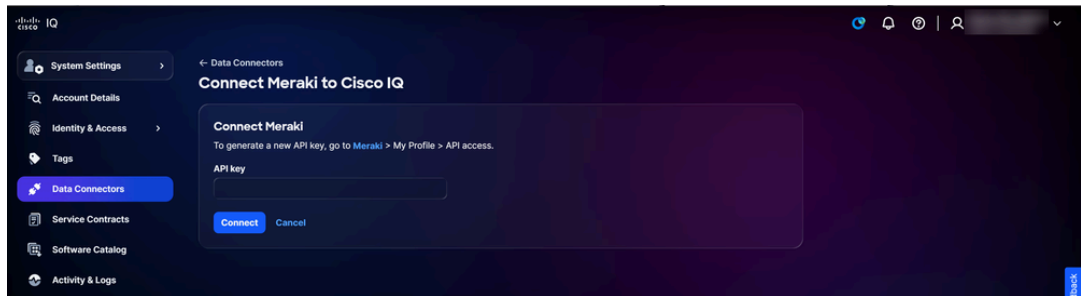


Verbinden des Catalyst SD-WAN Managers

1. Aktivieren Sie die Kontrollkästchen der gewünschten Organisation(en).

2. Klicken Sie auf Organisationen verbinden. Sie werden zur Seite Data Connectors weitergeleitet und eine Bestätigung wird angezeigt.

- Meraki




Meraki verbinden

1. Befolgen Sie die Anweisungen auf dem Bildschirm.
2. Geben Sie den API-Schlüssel ein.
3. Klicken Sie auf Verbinden. Sie werden zur Seite Data Connectors weitergeleitet und eine Bestätigung wird angezeigt.

Hinzufügen von Cisco IQ Link-Instanzen

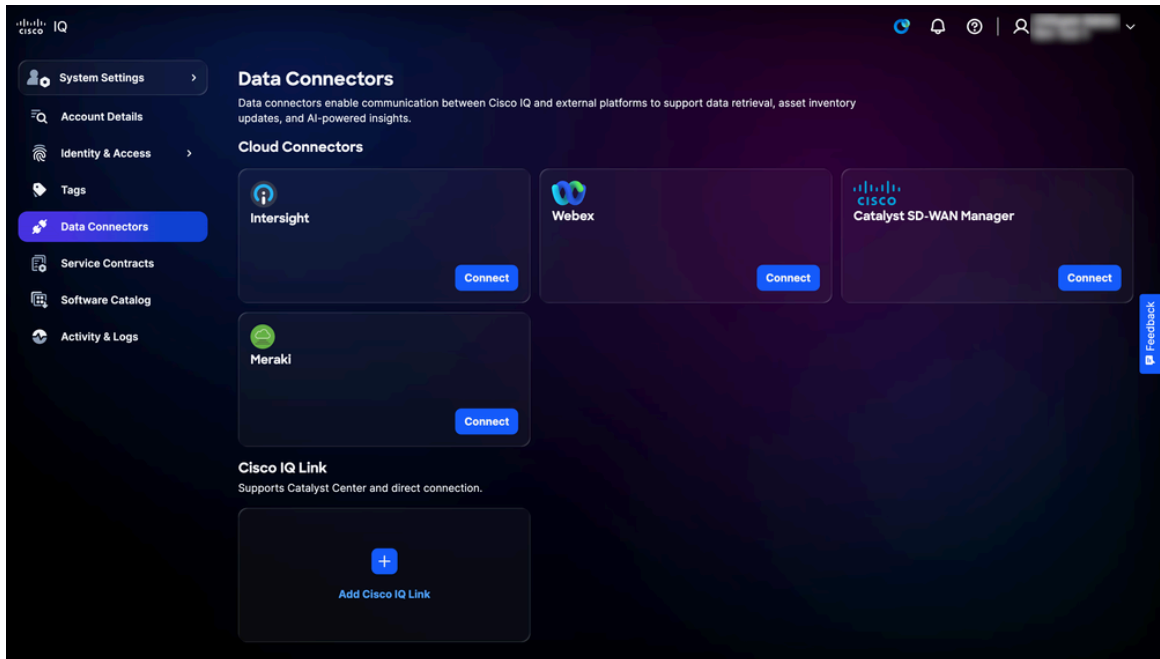
Cisco IQ Link ist eine standortbasierte Komponente von Cisco IQ. Sie bietet umfassendere und intelligentere Informationen, z. B. zum Hardware- und Software-Lebenszyklus und zur Bestandsaufnahme. Frühere Collectors werden in einem einzigen Connector konsolidiert, den Sie auf einem virtuellen System installieren, um detaillierte Telemetriedaten von Ihren Geräten zu erfassen.

Cisco IQ Link wird in Ihrem lokalen Netzwerk bereitgestellt, um die Geräteerkennung und Telemetriesammlung zu automatisieren. Cisco IQ Link unterstützt die direkte Verbindung und Integration mit Catalyst Center. Wenn Ihr Konto im Rahmen einer Migration erstellt wurde, können Sie Ihren CX Agent oder CSPC nutzen, um Telemetriedaten zu verbinden.

 Anmerkung: Für Cloud-Managed Controller ist Cisco IQ Link nicht erforderlich, da der Zugriff auf die erforderlichen Daten direkt über die Cisco Cloud möglich ist.

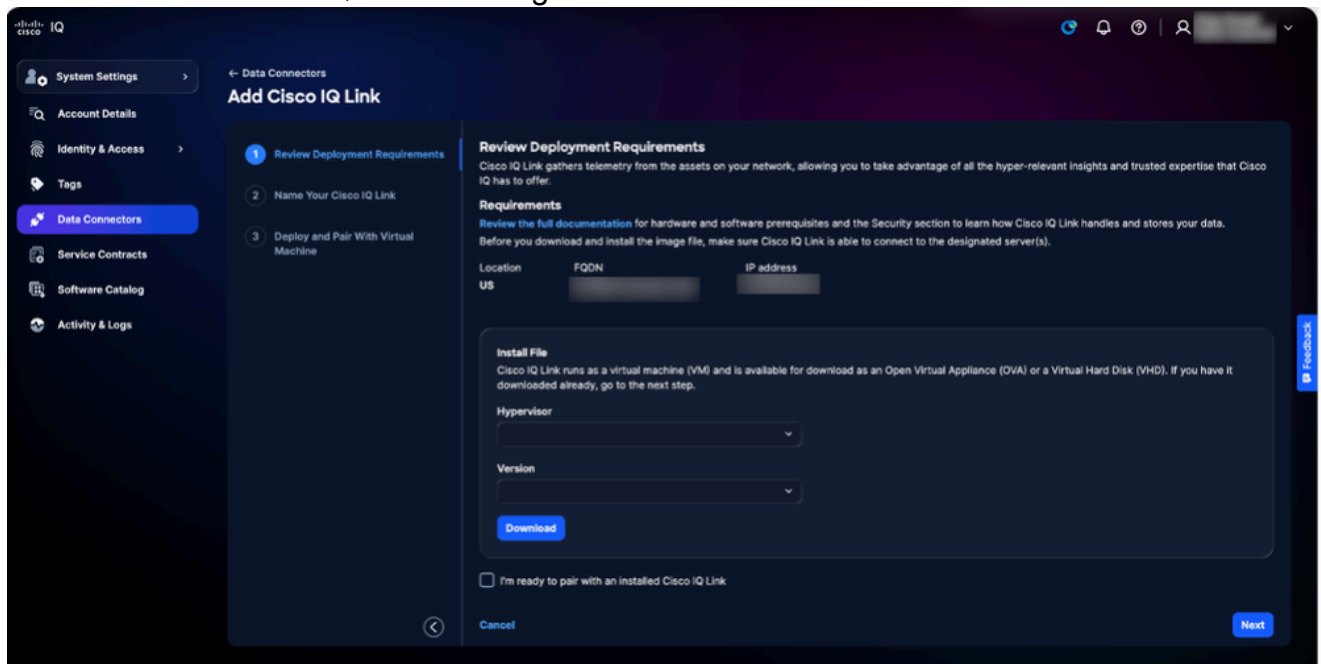
So fügen Sie Cisco IQ Link-Instanzen zu Cisco IQ hinzu:

1. Navigieren Sie zur Seite Data Connectors.



Cisco IQ-Link hinzufügen

2. Klicken Sie auf Cisco IQ-Link hinzufügen.



OVA oder VHD herunterladen

3. Laden Sie die Open Virtual Appliance (OVA) oder Virtual Hard Disk (VHD) herunter:

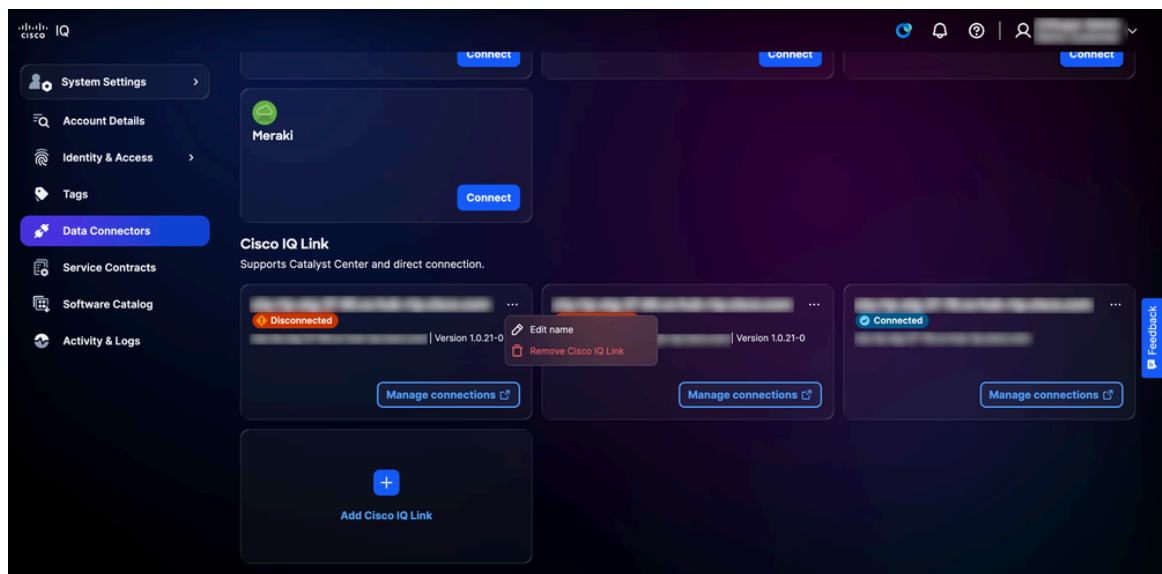
1. Wählen Sie den Hypervisor aus der Dropdown-Liste aus.
 2. Wählen Sie die Version aus der Dropdown-Liste aus.
 3. Klicken Sie auf Download (Herunterladen).
4. Klicken Sie auf Vollständige Dokumentation, um den [Cisco IQ Link Getting Started Guide aufzurufen](#). Dieses Dokument enthält umfassende, schrittweise Anleitungen zur Installation

von Cisco IQ Link mithilfe der im vorherigen Schritt heruntergeladenen Datei. Er deckt den gesamten Bereitstellungs-Workflow ab, einschließlich aller notwendigen Übergänge zwischen der Cisco IQ- und Cisco IQ Link-Schnittstelle, um die Kopplung und Konfiguration abzuschließen.

Bearbeiten der Namen von Cisco IQ-Verbindungsinstanzen

So bearbeiten Sie einen Instanznamen für einen Cisco IQ Link:

1. Navigieren Sie auf der Seite Data Connectors zur gewünschten Instanz von Cisco IQ Link.



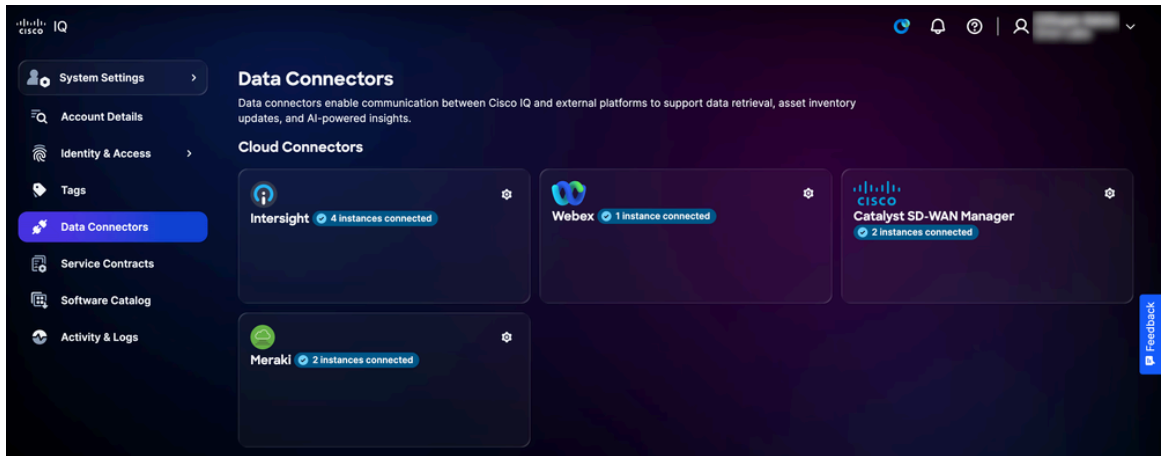
Name bearbeiten

2. Wählen Sie das Symbol Weitere Optionen > Name bearbeiten aus.
3. Bearbeiten Sie den Namen wie gewünscht.
4. Klicken Sie auf Aktualisieren.

Cloud Connectors für verbundene Kunden

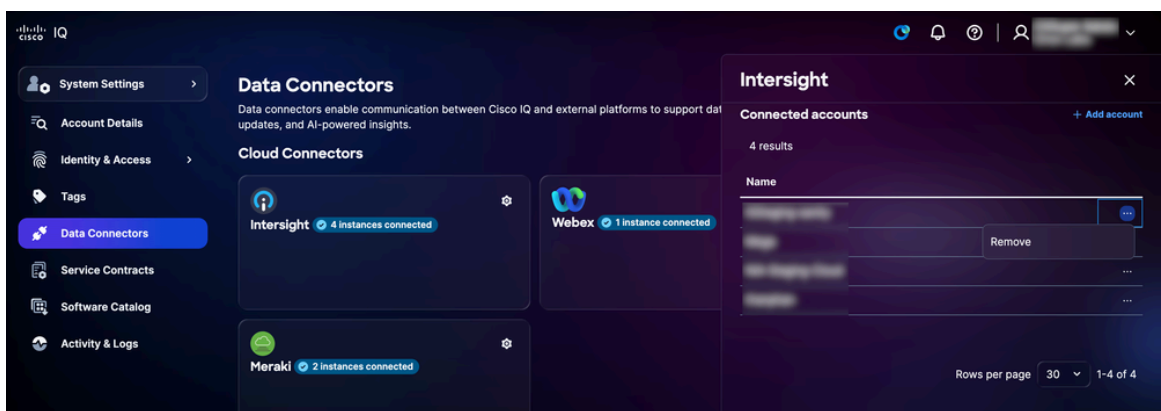
So entfernen Sie ein verbundenes Konto aus Ihren Cloud Connectors:

1. Navigieren Sie auf der Seite Data Connectors (Datenkonnektoren) zum gewünschten Cloud Connector.



Cloud Connectors - Einstellungen

2. Klicken Sie auf das Symbol Einstellungen. Das Fenster Verbundene Konten wird geöffnet.



Cloud Connector Connected Account entfernen

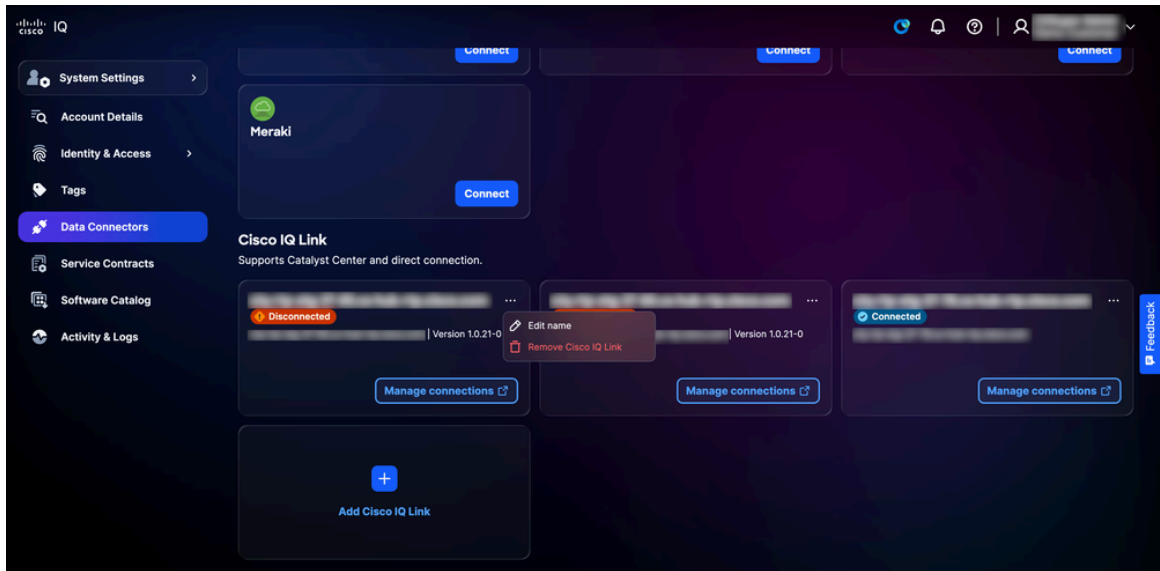
3. Wählen Sie im gewünschten Konto das Symbol Weitere Optionen > Entfernen aus. Es wird eine Bestätigung angezeigt.

4. Klicken Sie zur Bestätigung auf Entfernen.

Entfernen von Cisco IQ Link-Instanzen

So entfernen Sie eine Cisco IQ Link-Instanz von Ihren Daten-Connectors:


1. Navigieren Sie auf der Seite Data Connectors zur gewünschten Instanz von Cisco IQ Link.



Cisco IQ-Link entfernen

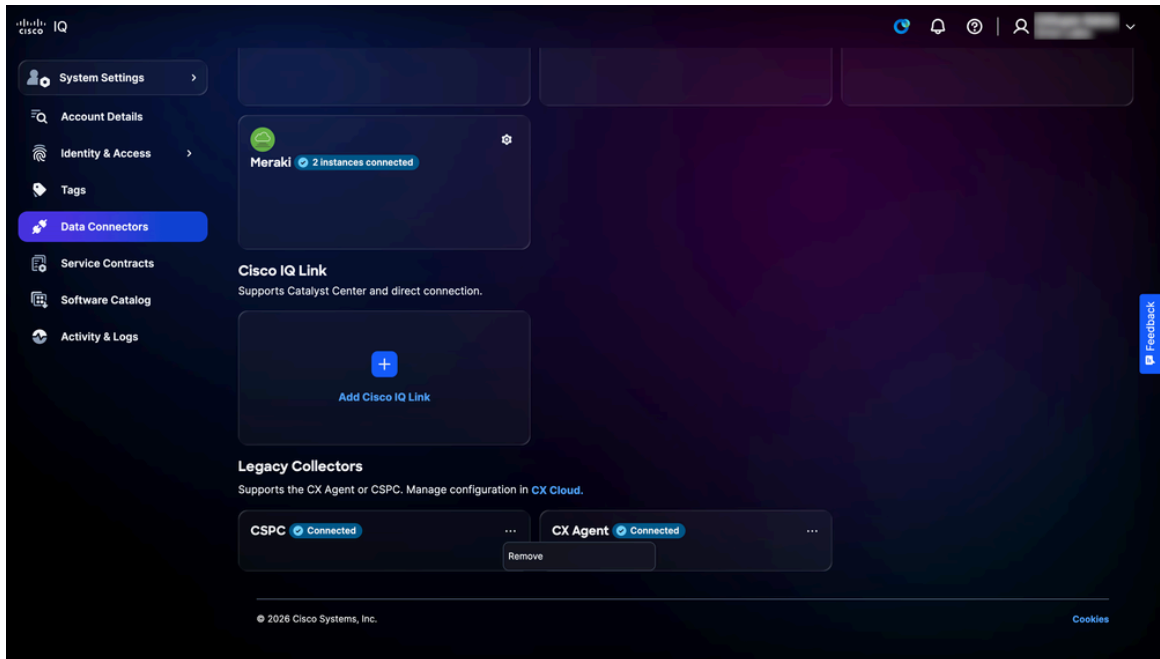
2. Wählen Sie das Symbol More Options (Weitere Optionen) > Remove Cisco IQ Link (Cisco IQ-Link entfernen). Es wird eine Bestätigung angezeigt.
3. Klicken Sie auf Open case, um ein Support-Ticket zu öffnen und Cisco IQ Link zu entfernen.

Entfernen älterer Collectors

 Anmerkung: Ältere Collectors werden nur bei Kunden angezeigt, die von der CX Cloud migriert wurden.

So entfernen Sie einen angeschlossenen Legacy-Anschluss:

1. Navigieren Sie auf der Seite Data Connectors (Datenverbindungen) zum gewünschten Sammler für ältere Systeme.




Verknüpfung des älteren Collectors aufheben

2. Wählen Sie das Symbol Weitere Optionen > Entfernen aus. Es wird eine Bestätigung angezeigt.
3. Klicken Sie auf Öffnen, um ein Support-Ticket zu öffnen und den Legacy Collector zu entfernen.

Serviceverträge

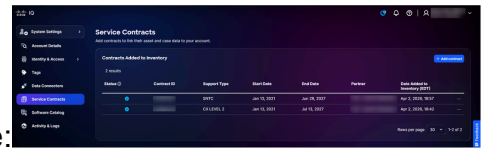
Durch die Verknüpfung von Verträgen werden Daten aus Verträgen mit unterschiedlichen Teammitgliedern zusammengeführt. Geräte, die nicht über Telemetrie mit Ihrem Bestand verbunden sind, werden einbezogen, wodurch die Transparenz der Supportabdeckung zentralisiert wird und Überraschungen bei Verlängerungen vermieden werden. Die Verknüpfung von Verträgen erfordert die Vertragsnummer, die zum Öffnen von Support-Tickets verwendet wird.

 Anmerkung: Wenn Sie Support zu Vertragsnummern benötigen, wenden Sie sich an Ihren Partner oder Cisco Vertreter.

Zu den wichtigsten Vorteilen von Serviceverträgen gehören:

- Erstellung einer zentralen Übersicht über die Supportabdeckung Ihres Unternehmens
- Anpassbare Dashboards, mit denen Sie Ihre Vertragsverlängerungen Monate im Voraus durchführen können
- Erweiterung der Bestandstransparenz um Ressourcen, die nicht an Telemetriedaten oder Teile luftdurchlässiger Umgebungen angeschlossen sind

Verknüpfen von Verträgen



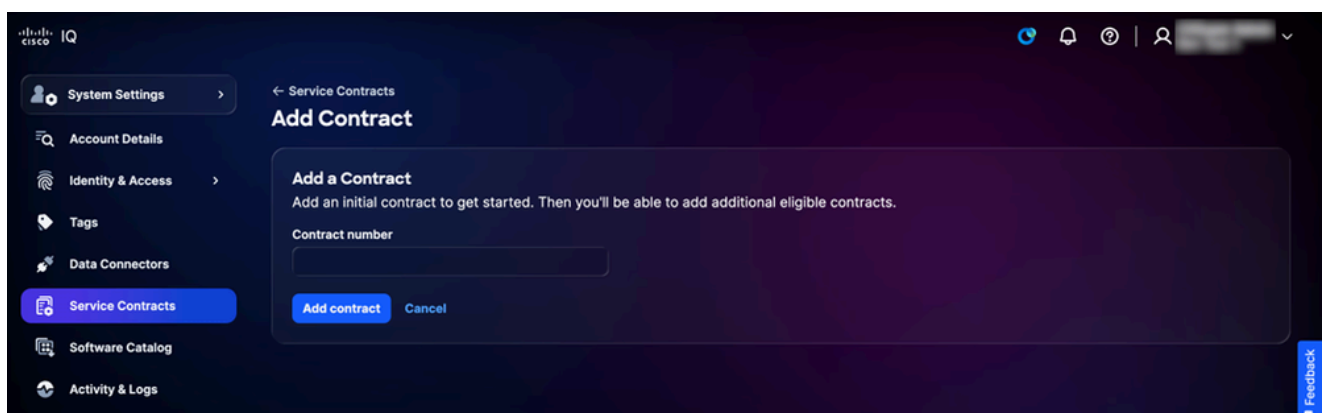
So verknüpfen Sie einen Vertrag über die Seite Service-Verträge:

Vertrag hinzufügen

1. Klicken Sie auf Vertrag hinzufügen. Die Seite "Vertrag hinzufügen" wird angezeigt.



Anmerkung: Weitere Verträge können hinzugefügt werden, nachdem dem Konto ein Erstvertrag hinzugefügt wurde.



Vertragsnummer eingeben

2. Geben Sie die Vertragsnummer ein.
3. Klicken Sie auf Vertrag hinzufügen. Der Vertrag wird dem Konto hinzugefügt.

Softwarekatalog

Im Softwarekatalog 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.

Um auf den Softwarekatalog zuzugreifen, navigieren Sie zu Startseite > Systemeinstellungen > Softwarekatalog. Die Seite Softwarekatalog wird angezeigt. Auf dieser Seite werden die verfügbaren Softwareinstanzen als Link Collector Availability Cards angezeigt. Jede Link Collector-Verfügbarkeitskarte zeigt den Namen, die Beschreibung, den Herausgeber und die Version einer Softwareinstanz an.

Anzeigen von Details für Softwareinstanzen

Um Versionshinweise für eine Softwareinstanz anzuzeigen, klicken Sie auf Details. Ein Fenster mit den letzten Versionshinweisen der Instanz wird geöffnet. Wählen Sie in der Dropdown-Liste eine Versionshinweise aus, um die vorherigen Versionshinweise anzuzeigen.

Installieren von Paketen für neue Softwareinstanzen

So laden Sie ein Installationsprogramm zum Erstellen einer neuen Instanz herunter:

1. Wählen Sie auf einer gewünschten Link Collector-Verfügbarkeitskarte Download-Optionen > Pakete installieren aus. Das Fenster zum Installieren des Pakets wird geöffnet.
2. Wählen Sie eine der folgenden Hypervisor-Optionen aus der Dropdown-Liste aus:
 - ESXi: für VMware ESXi
 - Hyper-V: für Microsoft Hyper-V
 - KVM: für Linux Kernel-basiertes virtuelles System (KVM)
3. Wählen Sie eine Version aus der Dropdown-Liste aus.
4. 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.

5. Bereitstellen der Datei in Ihrem Rechenzentrum Weitere Informationen finden Sie im [Cisco IQ Link Getting Started Guide](#).

Aktivität und Protokolle

Der Service Activity & Logs zentralisiert die Nachverfolgung aller Benutzeraktionen und Systemereignisse in Cisco IQ für Compliance, Fehlerbehebung und Überwachung. Es erfasst unveränderliche Prüfdatensätze für Authentifizierungsereignisse, Autorisierungsentscheidungen, Ressourcenzugriff, Konfigurationsänderungen und Verwaltungsaktionen mit detailliertem Kontext, einschließlich Benutzeridentität, Zeitstempel, Quell-IP-Adressen und betroffenen Ressourcen. Activity & Logs erzwingt Aufbewahrungsrichtlinien und ermöglicht die flexible Abfrage und Filterung von Überwachungsereignissen mit Unterstützung von Zeitbereichssuchen, benutzerbasierten Filtern und ressourcenspezifischer Aktivitätsüberwachung.

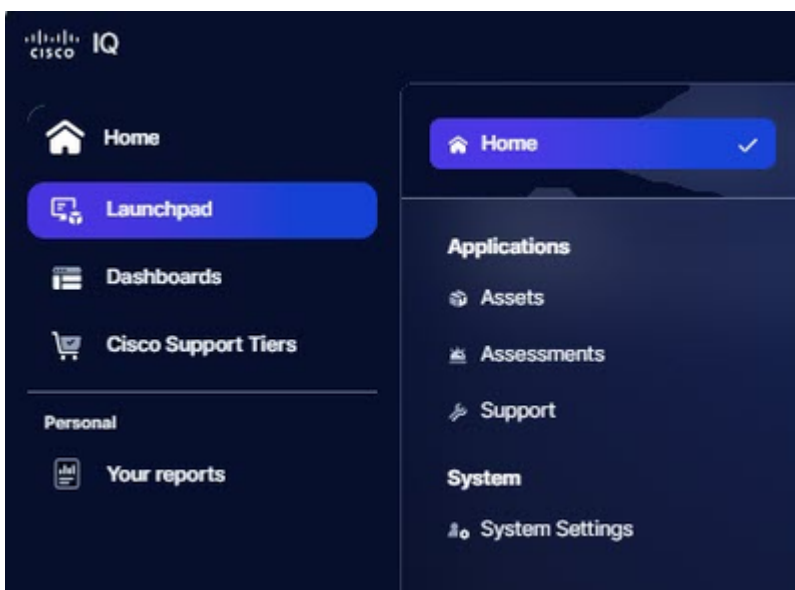
The screenshot shows the 'Activity & Logs' section of the Cisco IQ interface. It features a search bar, a 'Logged' dropdown, and a 'Filters' button. The table displays 10 rows of activity logs, all with the action 'read'. The page also includes an 'Export' button and a 'Feedback' button on the right side.

Date and Time	Application	Action	Email	Event
Apr 16, 2026, 12:27:56.12 PM EDT		read		
Apr 16, 2026, 12:27:54.93 PM EDT		read		
Apr 16, 2026, 12:16:30.09 PM EDT		read		
Apr 16, 2026, 12:16:15.68 PM EDT		read		
Apr 16, 2026, 12:16:15.83 PM EDT		read		
Apr 16, 2026, 12:16:15.82 PM EDT		read		
Apr 16, 2026, 12:16:15.81 PM EDT		read		
Apr 16, 2026, 12:16:15.78 PM EDT		read		
Apr 16, 2026, 12:13:12.84 PM EDT		read		

Aktivität und Protokolle

Anwendungen für Ressourcen

Die Anwendung Assets bietet umfassende Transparenz- und Managementfunktionen für Cisco Ressourcen und dient als Grundlage für Cisco IQ. Sie stellt eine zentrale Liste aller Geräte in einer Organisation bereit. Durch das Sammeln von Informationen aus mehreren Quellen wird der Gerätebestand als einheitliche Datenquelle genutzt. Die Pflege einer vollständigen und präzisen Liste der Ressourcen ist von entscheidender Bedeutung, da andere Anwendungen innerhalb von Cisco IQ - wie z. B. die Anwendung Assessments - diese Daten zur Beurteilung des Zustands und der Sicherheit Ihrer Geräte heranziehen.



Home-Menü

Kernkonzepte

Die Ressourcenanwendung 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
- 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. Erfassung und Bereicherung von Telemetriedaten über eine mehrschichtige Daten-Pipeline

Zugriff auf die Anwendung "Ressourcen"

Um auf die Bestandsverwaltungsfunktionen von Cisco IQ zuzugreifen, wählen Sie Home menu > Assets. 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.

- Assets
- Overview**
- Inventory
- Service Contracts
- End of Life

Overview

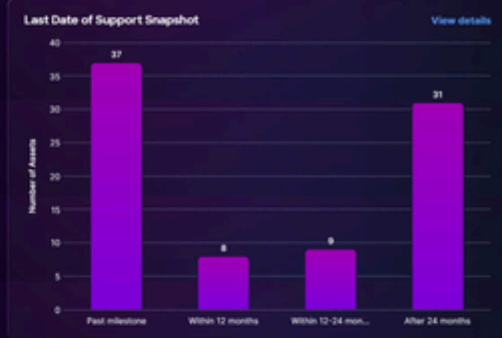
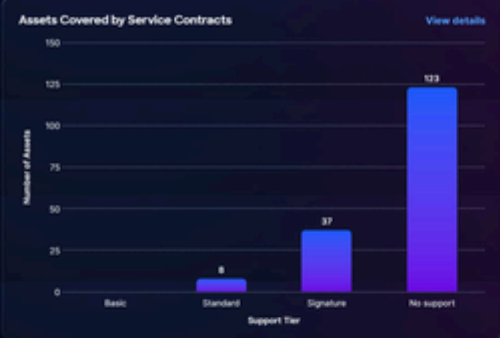
Product family Last signal date Data source Asset location Filters

🗨️ Ask AI Customize

Total Assets 168 Assets

Covered assets
58 Covered 97% of all assets

Uncovered assets
2 Uncovered 3% of all assets



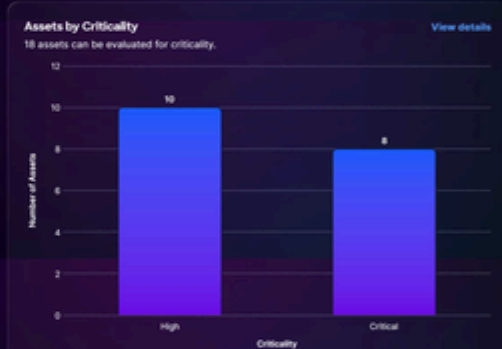
Key Asset Metrics

Assets with telemetry
168 with telemetry 100% of all assets

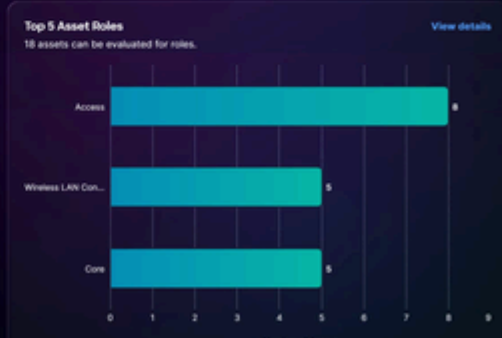
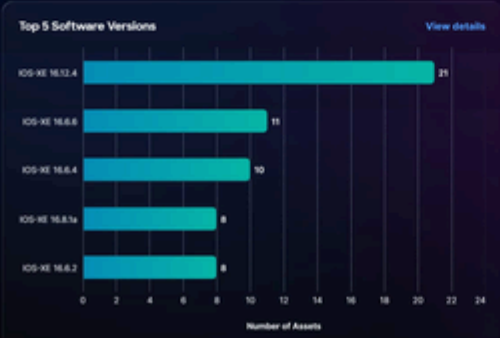
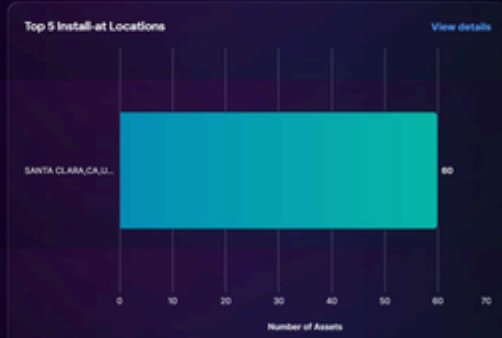
Assets without telemetry
0 without telemetry 0% of all assets

Assets With Critical or High Security Advisories View details

85%
Of the 168 assets with telemetry enabled, 142 have critical or High Security Advisories



Asset Breakdown



Das Dashboard zeigt die folgenden Informationen an:


- **Aktiva insgesamt:** Die Gesamtzahl der Ressourcen des Cisco IQ-Kontos
- **Abgedeckte Aktiva:** Gesamtzahl und Prozentsatz der durch Serviceverträge abgedeckten Ressourcen
- **Nicht gedeckte Aktiva:** 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
- **Wichtige Ressourcenmetriken:** Zusätzliche wichtige Kennzahlen wie Telemetriestatus, wichtige Sicherheitsempfehlungen und LDOS-Informationen
 - **Ressourcen mit Telemetrie:** Gesamtzahl und Prozentsatz der Ressourcen mit aktivierter Telemetrie
 - **Ressourcen ohne Telemetrie:** Gesamtzahl und Prozentsatz der Ressourcen ohne aktivierte Telemetrie
 - **Ressourcen mit kritischen oder hohen Sicherheitsempfehlungen:** Prozentualer Anteil der gesamten Ressourcen mit aktivierter Telemetrie und kritischen oder hohen Sicherheitsempfehlungen
 - **Ressourcen nach Kritikalität:** 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.


 Anmerkung: 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 umfasst Asset Criticality Insights, eine neue Funktion in der Ressourcen-App, 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, wenn es um Sicherheitskorrekturen, Software-Upgrades, EOL-Planung und Abdeckungsentscheidungen geht.

 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

Bestand

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

Assets Next subcomponents

Search Product family Product ID Location Last signal date Tags Equipment type Filters 1692 results Export

Insights : 75 assets that are **not covered** by any support contract have already reached **Last Date of Support**, leaving them without access to security patches or bug fixes. Prioritize ...


- 170 Cisco Catalyst 9300 Series Switches (30.9% of uncovered assets) are **not covered** by any support contract, which may limit access to Cisco support resources. Align renewal pla...


Name	Product ID	Product Type	Serial Number	Next Milestone	Next Milestone...	Contract Number	Coverage Status	Telemetry Status	Security Adviso...
		Cloud and Sy...		End of Servic...	Jun 25, 2028		🟡	🟢	0
		Switches		End of Servic...	Jan 29, 2027		🟡	🟢	4
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24

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.

 Anmerkung: 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 Anwendungsfeatures.

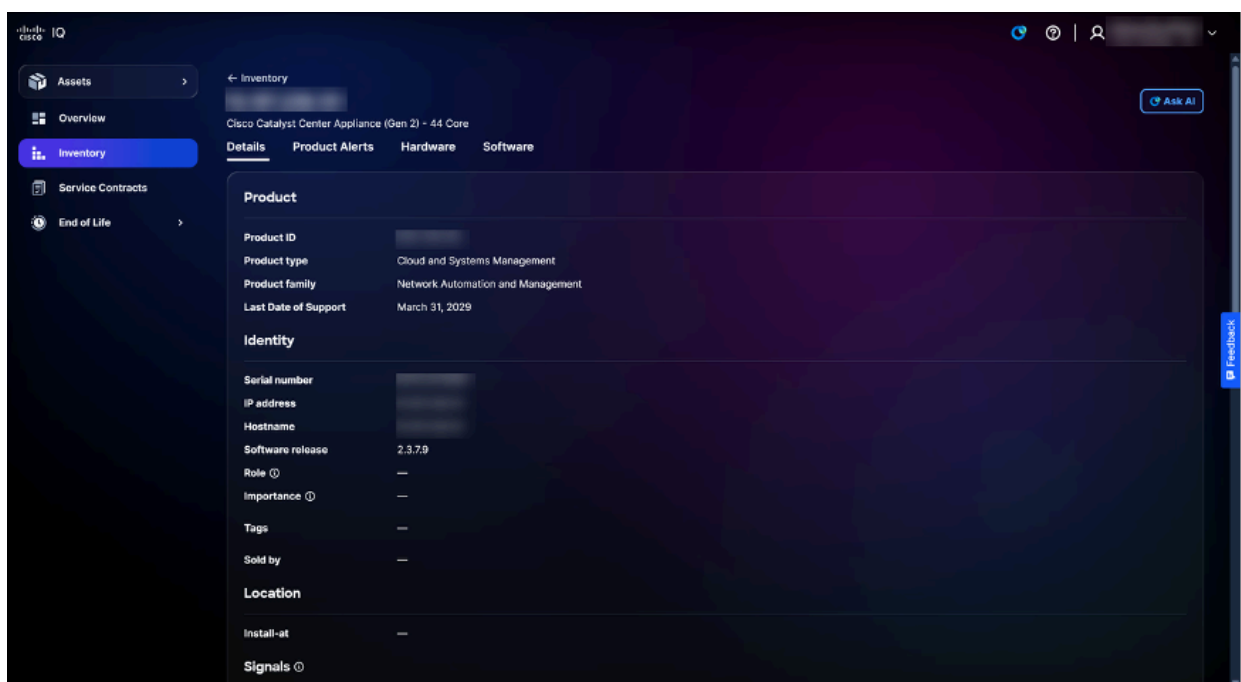
Exportieren des Bestands

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

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.




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 `key:value` Paar, das Sie definieren, z. `Environment:Prod B.` 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.

Erstellen und Löschen von Asset-Tags

Weitere Informationen zum Erstellen und Löschen von Systemtags finden Sie unter [Tags](#) in den Systemeinstellungen.

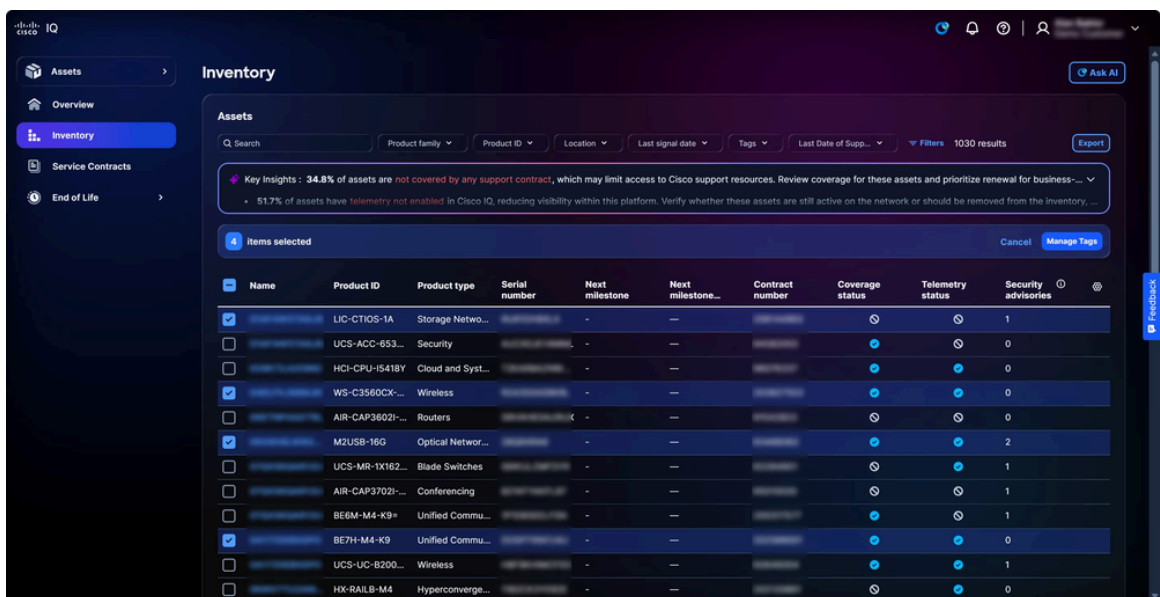
 Anmerkung: Nur Kontoadministratoren können Tags erstellen und löschen.

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:

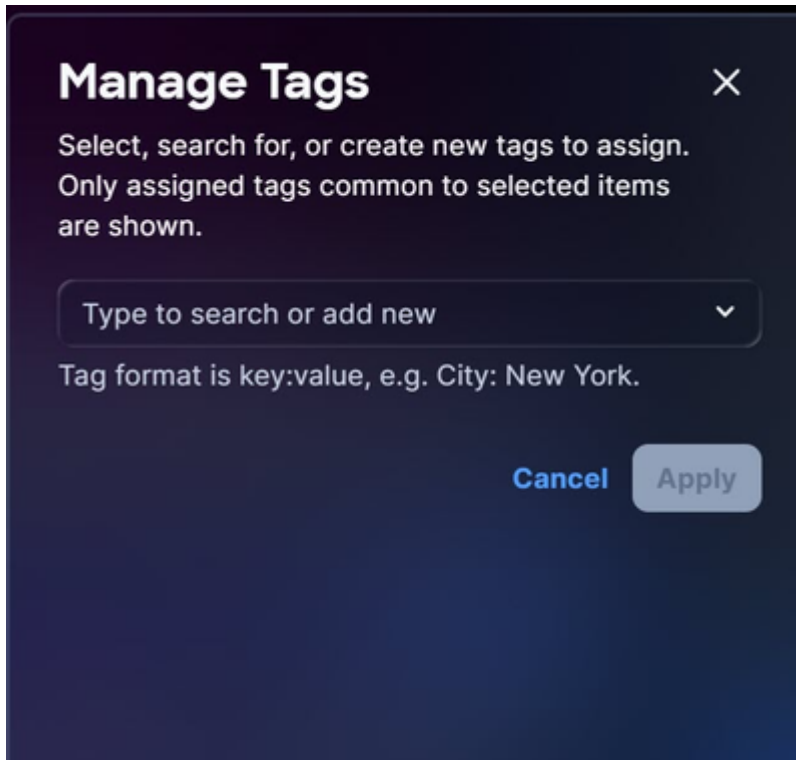
1. Navigieren Sie zu Anlagen > Lager.



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.

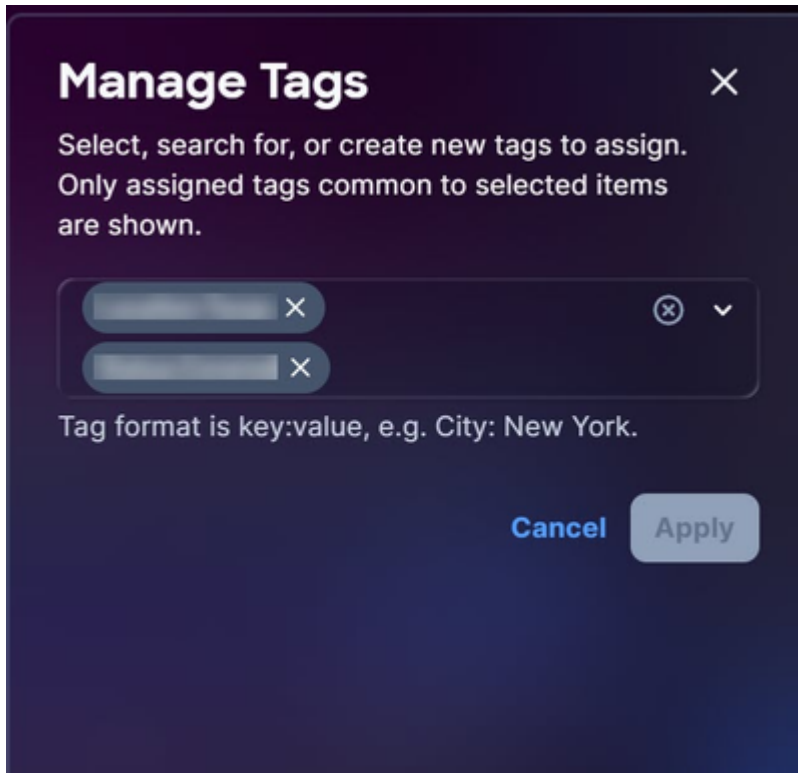
 Anmerkung: Tags haben ein `key:value` Format (z. B. `City:NYC`).

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

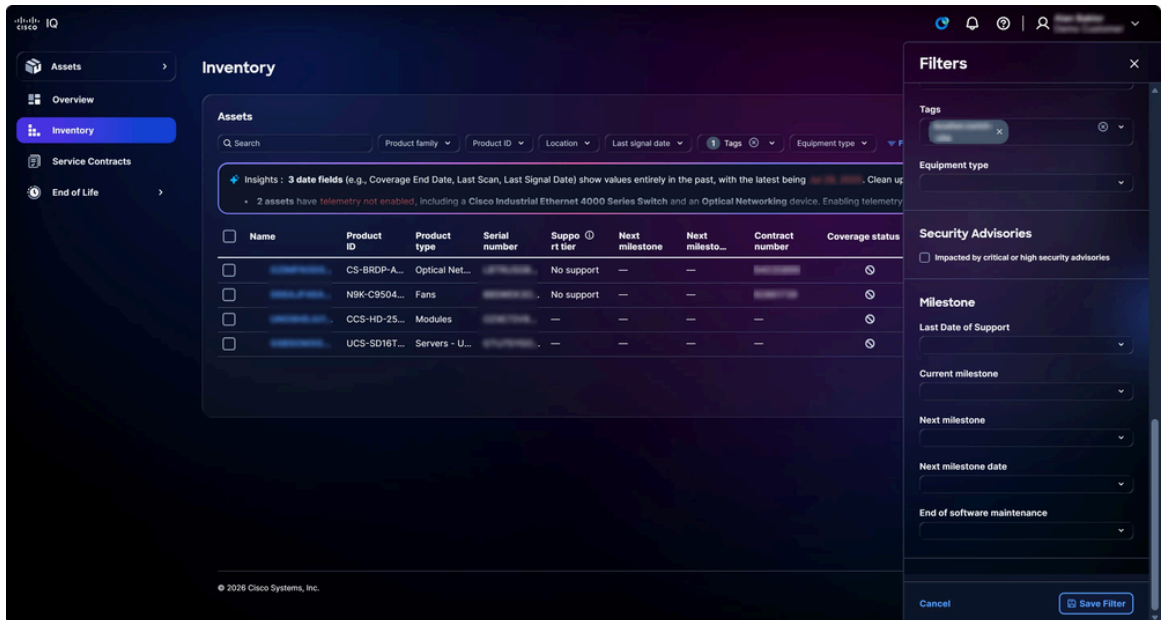
4. Klicken Sie auf das X für ein beliebiges Tag, um es aus der Auswahl zu entfernen.
5. Klicken Sie auf Apply (Anwenden).

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

3. 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.

The screenshot shows the Cisco IQ Service Contracts page. On the left, there is a navigation menu with 'Assets', 'Overview', 'Inventory', 'Service Contracts', and 'End of Life'. The main area displays a table of service contracts with columns: Coverage Status, Contract Number, Support Type, Support Tier, Start Date, End Date, and Partner. Above the table, there are filters for 'All status types', 'All expiration d...', and 'Tags', along with a search bar and an 'Export' button. Below the table, there are insights: '2 of 4 expired service contracts are linked to 1 expired support contract, representing 50.0% of all expired coverage. Review these contracts to determine if the associated assets r...' and '15 service contracts (9.0%) have start dates within the next 6 months, with the earliest deadline on Apr 16, 2026. Initiate onboarding or renewal processes now to avoid coverage gaps.' The table contains 15 rows of contract data.

Serviceverträge

Ansichten für Serviceverträge suchen und filtern

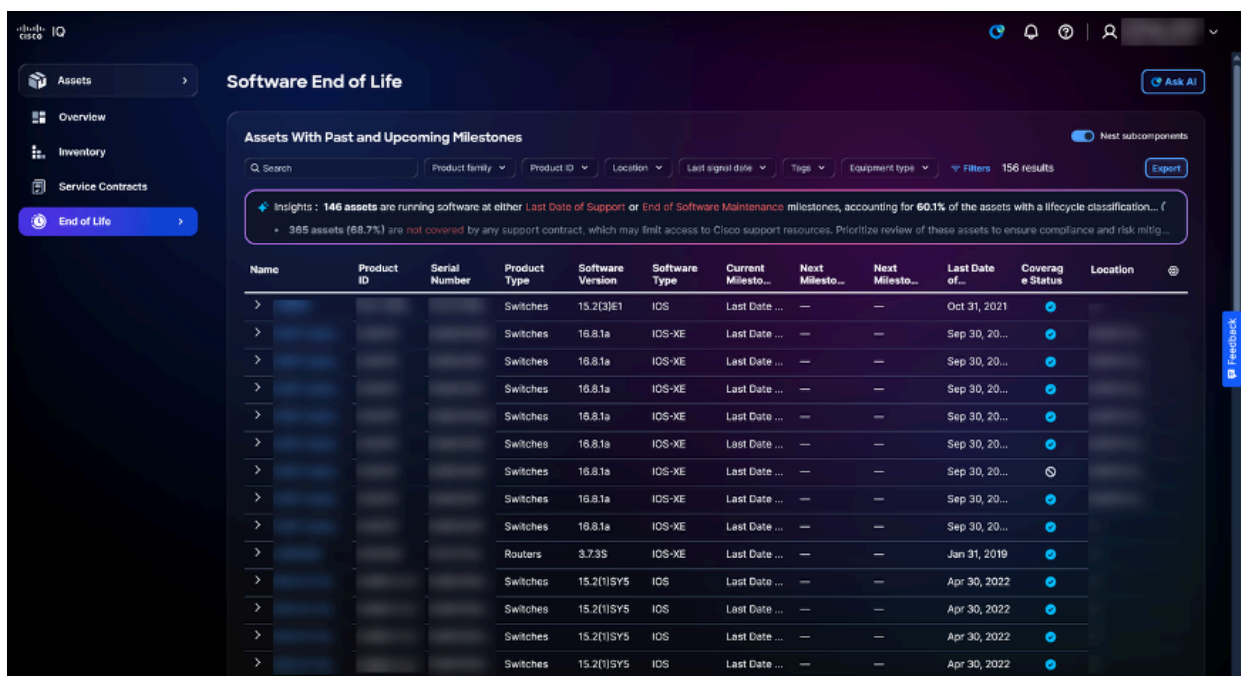
Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen. Sie können auch nach Serviceverträgen suchen, indem Sie die Vertragsnummer in das Feld Suchen eingeben.

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](#) in allgemeinen Anwendungsfunktionen.

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.



The screenshot displays the 'Software End of Life' dashboard in Cisco IQ. The main heading is 'Assets With Past and Upcoming Milestones'. Below this, there is a search bar and several filter dropdowns: Product family, Product ID, Location, Last signal date, Tags, and Equipment type. A filter summary indicates '156 results'. An 'Export' button is visible. An insight box states: '146 assets are running software at either Last Date of Support or End of Software Maintenance milestones, accounting for 60.1% of the assets with a lifecycle classification...'. Below this, a secondary insight notes: '365 assets (68.7%) are not covered by any support contract, which may limit access to Cisco support resources. Prioritize review of these assets to ensure compliance and risk mitigation...'. The main table lists assets with columns: Name, Product ID, Serial Number, Product Type, Software Version, Software Type, Current Milestone, Next Milestone, Next Milestone, Last Date of..., Coverage Status, and Location. The table contains 12 rows of data, including switches and routers with various software versions and end dates.

Name	Product ID	Serial Number	Product Type	Software Version	Software Type	Current Milestone	Next Milestone	Next Milestone	Last Date of...	Coverage Status	Location
>			Switches	15.2(3)E1	IOS	Last Date ...	—	—	Oct 31, 2021	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Routers	3.73S	IOS-XE	Last Date ...	—	—	Jan 31, 2019	🟢	
>			Switches	15.2(1)SY5	IOS	Last Date ...	—	—	Apr 30, 2022	🟢	
>			Switches	15.2(1)SY5	IOS	Last Date ...	—	—	Apr 30, 2022	🟢	
>			Switches	15.2(1)SY5	IOS	Last Date ...	—	—	Apr 30, 2022	🟢	
>			Switches	15.2(1)SY5	IOS	Last Date ...	—	—	Apr 30, 2022	🟢	

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 Anwendungsfeatures.

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](#) in allgemeinen Anwendungsfunktionen.

Anwendung für Leistungsbeurteilungen

Die Anwendung Assessments bietet ein Bewertungs-Framework, mit dem Benutzer Risiken in Bezug auf Sicherheit, Stabilität, Kapazität, Compliance und Alterung proaktiv untersuchen und mindern können, um die Sicherheit, Stabilität und Zuverlässigkeit von Netzwerken zu gewährleisten.

Kernkonzepte

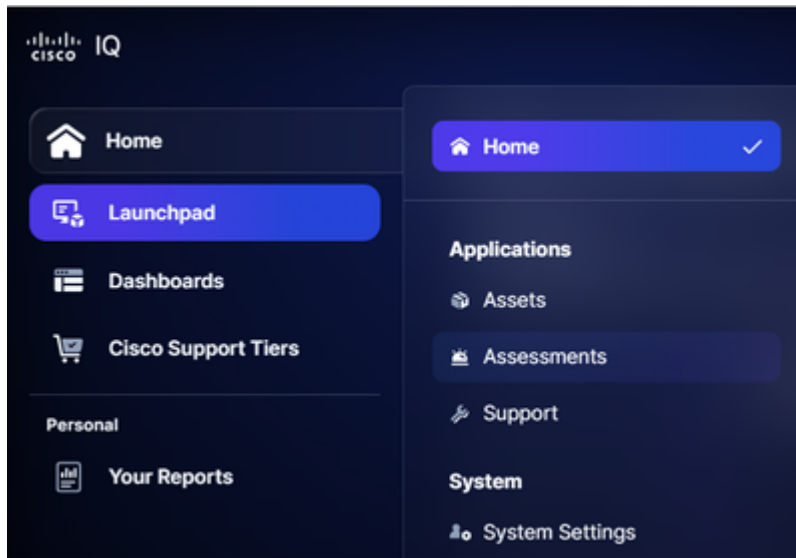
Die Anwendung Leistungsbeurteilungen basiert auf den folgenden Kernkonzepten:

- 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 die Bewertungsanwendung



Assessments

Um auf die Sicherheits- und Bewertungsfunktionen von Cisco IQ zuzugreifen, wählen Sie Home menu > Assessments. Die Seite "Übersicht Leistungsbeurteilungen" wird angezeigt.

Leistungsbeurteilungen - Überblick

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



Leistungsbeurteilungen - Überblick

Das Dashboard zeigt die folgenden Informationen an:

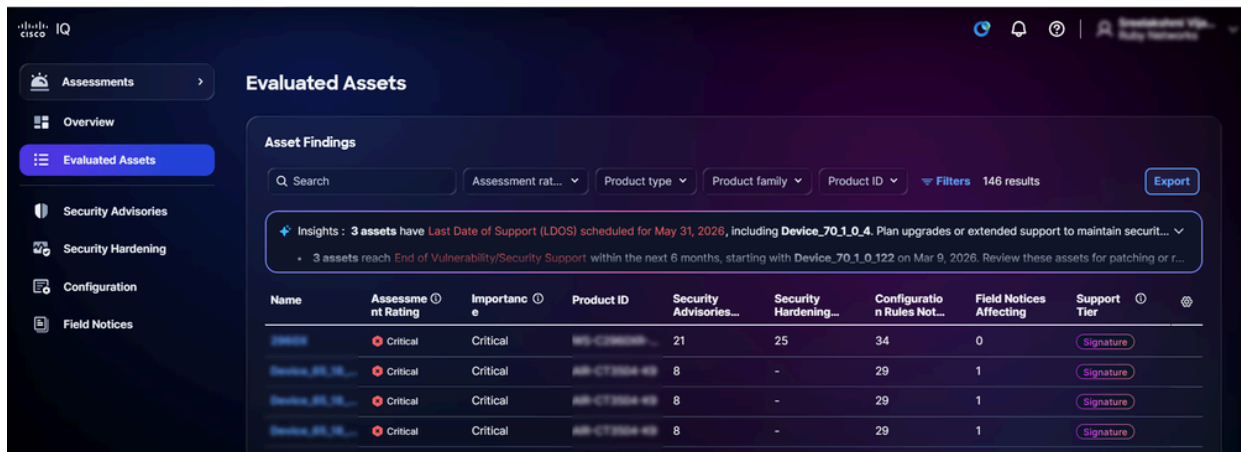
- Sicherheitsratgeber-Analysen: Zeigt Bewertungen von Sicherheitsempfehlungen an, die nach kritischem und hohem Schweregrad kategorisiert sind.
- Regeln für die Sicherheitsabsicherung bei Ressourcen, die nicht bestanden wurden: Zeigt Ressourcen an, die die Sicherheitshärtungsregeln nicht erfüllen, kategorisiert nach Schweregrad Hoch, Mittel, Niedrig und Informativ
- Konfigurationsregeln für nicht bestandene Ressourcen: 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 Schweregrad Kritisch, Hoch, Mittel und Kein kategorisiert sind.

 Anmerkung: Kunden 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, einschließlich Sicherheitsempfehlungen, Sicherheitssicherung, Konfiguration und Problemhinweisen.




The screenshot shows the 'Evaluated Assets' interface in Cisco IQ. It features a sidebar with navigation options like 'Assessments', 'Overview', 'Evaluated Assets', 'Security Advisories', 'Security Hardening', 'Configuration', and 'Field Notices'. The main content area displays 'Asset Findings' with a search bar and several dropdown filters. Below the filters, there are two insight boxes: one stating '3 assets have Last Date of Support (LDOS) scheduled for May 31, 2026' and another stating '3 assets reach End of Vulnerability/Security Support within the next 6 months'. A table below lists asset findings with the following columns: Name, Assessment Rating, Importance, Product ID, Security Advisories, Security Hardening, Configuration Rules Not, Field Notices Affecting, and Support Tier. The table contains three rows of data, all with a 'Critical' assessment rating.


Name	Assessment Rating	Importance	Product ID	Security Advisories	Security Hardening	Configuration Rules Not	Field Notices Affecting	Support Tier
Device_70_1_0_4	Critical	Critical	80-C20000...	21	25	34	0	Signature
Device_70_1_0_4	Critical	Critical	80-C70004-02	8	-	29	1	Signature
Device_70_1_0_4	Critical	Critical	80-C70004-02	8	-	29	1	Signature

Ergebnisse nach Ressource

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.

 Anmerkung: Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung.

Exportieren der Ergebnisse nach Ressource

Klicken Sie zum Exportieren einer Listenansicht "Suche nach Ressource" auf Exportieren. Weitere Informationen zum Exportieren finden Sie unter [Exportieren von Informationen](#).

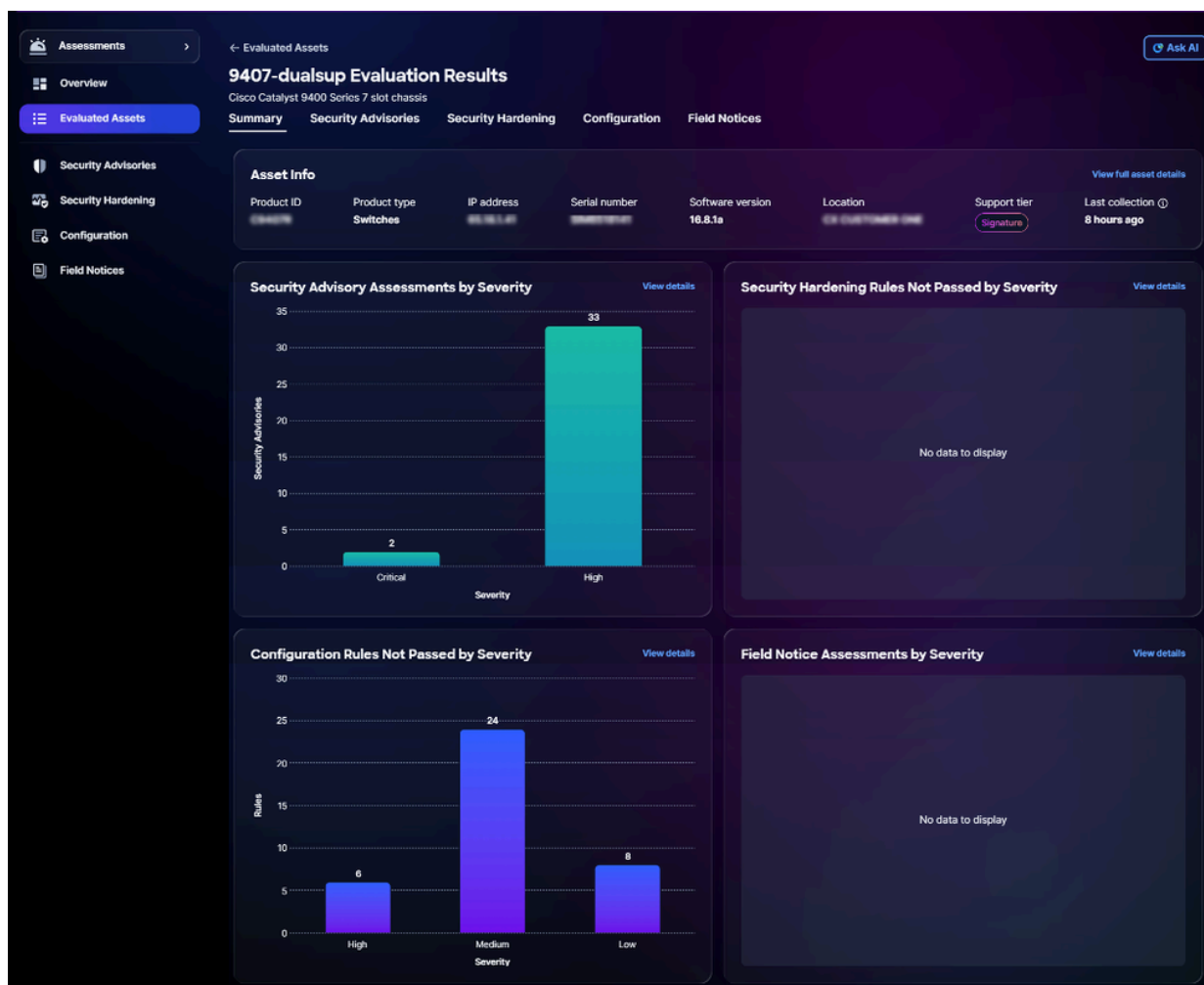
Ergebnisse nach Ressourcendetails anzeigen

Um die Ergebnisse nach Ressourcendetails anzuzeigen, klicken Sie auf eine Ressource. 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: Bietet eine Liste von Ressourcen, die nicht mit den Best Practice-Regeln der Konfiguration übereinstimmen
- Problemhinweise: Bietet eine Liste zugehöriger Analysen für Problemhinweise



Ergebnisse nach Ressourcendetails

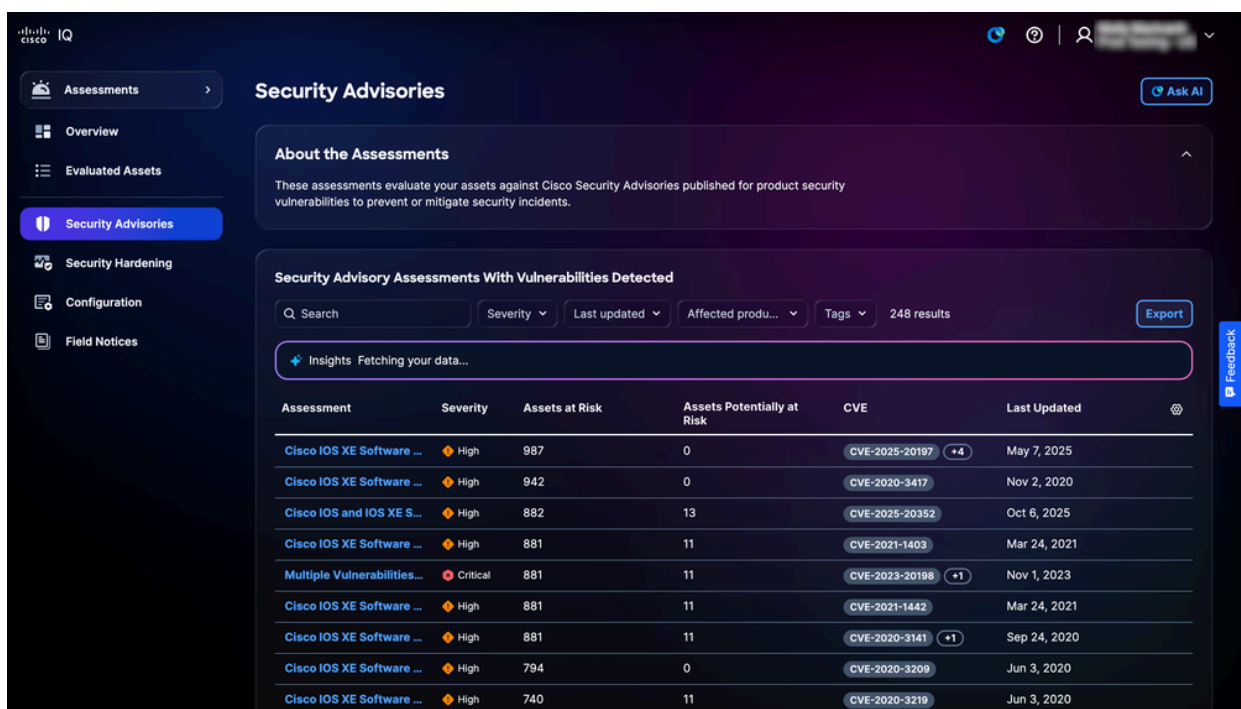
Wenn Sie auf Details anzeigen auf einer Kachel klicken, wird die Seite zur entsprechenden Seite in der Anwendung umgeleitet.

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.




Assessment	Severity	Assets at Risk	Assets Potentially at Risk	CVE	Last Updated
Cisco IOS XE Software ...	High	987	0	CVE-2025-20197 +4	May 7, 2025
Cisco IOS XE Software ...	High	942	0	CVE-2020-3417	Nov 2, 2020
Cisco IOS and IOS XE S...	High	882	13	CVE-2025-20352	Oct 6, 2025
Cisco IOS XE Software ...	High	881	11	CVE-2021-1403	Mar 24, 2021
Multiple Vulnerabilities...	Critical	881	11	CVE-2023-20198 +1	Nov 1, 2023
Cisco IOS XE Software ...	High	881	11	CVE-2021-1442	Mar 24, 2021
Cisco IOS XE Software ...	High	881	11	CVE-2020-3141 +1	Sep 24, 2020
Cisco IOS XE Software ...	High	794	0	CVE-2020-3209	Jun 3, 2020
Cisco IOS XE Software ...	High	740	11	CVE-2020-3219	Jun 3, 2020

Sicherheitsempfehlungen


Filteransichten nach Sicherheitsempfehlungen durchsuchen

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

 Anmerkung: Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet.

 Anmerkung: Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur

 Verfügung.

 Anmerkung: Fehlende Schweregrade werden mit einem beschreibenden Tooltip als "-" angezeigt.

Exportieren von Sicherheitsempfehlungen

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

Anzeigen der Bewertungsdetails für Sicherheitsberatung

Um weitere Details zu einer Leistungsbeurteilung anzuzeigen, klicken Sie auf einen Hinweis. Diese 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

About the Assessment

A vulnerability in Cisco access point (AP) software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of certain parameters within 802.11 frames. An attacker could exploit this vulnerability by sendin...
[Show more](#)

Severity	CVE	CVSS score	Version	First published
High	CVE-2023-20199	7.4	1.0	Mar 22, 2023

Last updated: Mar 22, 2023
 Source documents: [Security Advisory](#)

Asset Results

Q Search Result Product type Product family Product ID Software type Asset type Filters 28 results

Asset	Result	Product ID	IP address	Serial number	Support Tier
IP-27-C2850-487...	Potentially Affected	C2850-487	10.10.10.10	JK23000000	—
C2850A	Potentially Affected	C2850A-487-48	10.10.10.10	JK23000001	Signature
C2850-487-E	Potentially Affected	C2850-487	10.10.10.10	JK23000004	Signature
F340L7L20-C2850-4...	Potentially Affected	W3-C2850-487-E	10.10.10.10	POCT28500004	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 Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet.

Anmerkung: 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 Asset Assessment Results (Ergebnisse der Ressourcenbewertung) auf eine Ressource. Die Seite "Leistungsbeurteilungsergebnisse" wird angezeigt.


Ergebnisdetails

Exportieren von Ressourcenergebnissen für Sicherheitsempfehlungen

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

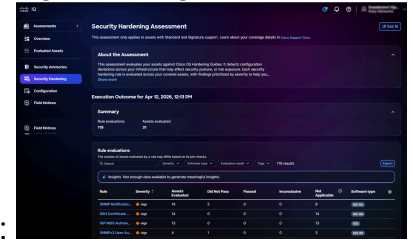
Sichern

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 aussagekräftige Anleitungen für die Problembehebung, sodass Administratoren die Angriffsfläche effektiv verringern und eine konsistente Ausrichtung an den strikten Best Practices von Cisco beibehalten können. Durch die Zentralisierung der Compliance-Überwachung und die Vereinfachung des Härtingsprozesses verwandelt die Anwendung das Sicherheitsmanagement von einer reaktiven Aufgabe in eine proaktive, datengesteuerte Strategie, die ein ausfallsicheres und sicheres Unternehmensnetzwerk gewährleistet.

 Anmerkung: Bewertungen zur Sicherheitshärtung sind ausschließlich für Ressourcen mit Standard- oder Signatur-Supportstufen verfügbar.

Sicherheitsbewertungen anzeigen

Klicken Sie auf eine Analyse, um weitere Details zur Sicherheitssicherung anzuzeigen. Auf der




Seite Sicherheitsbewertung werden folgende Informationen angezeigt:


Sichern

- Informationen zur Leistungsbeurteilung: Zusätzliche Details durch Zusammenfassung des Zwecks der Leistungsbeurteilung
- Zusammenfassung der Ausführung: 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

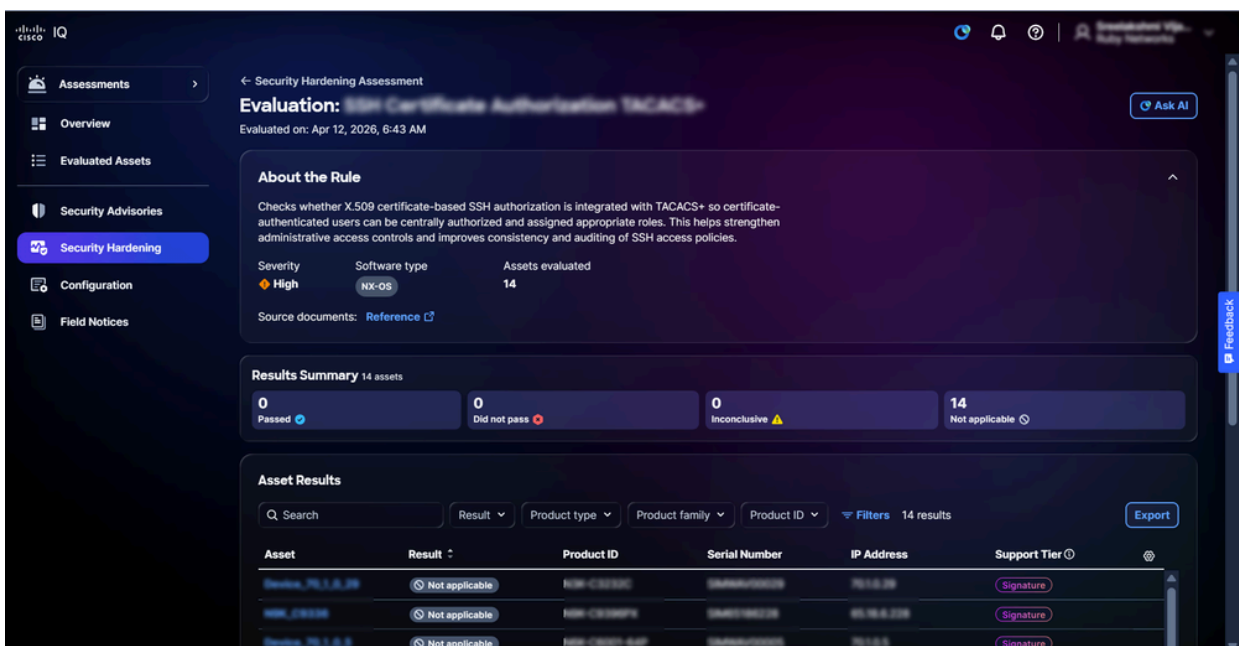
Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen oder auf Filter klicken und eine Option aus der Liste der verfügbaren Filter auswählen. Sie können auch nach einer Regel suchen, indem Sie den Namen der Regel in das Feld Suchen eingeben.

 Anmerkung: Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet.

 Anmerkung: 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 displays the Cisco IQ interface for a Security Hardening Assessment. The main content area shows the 'Evaluation' details for a rule titled 'Certificate Authorization TACACS+'. The rule is evaluated on April 12, 2026, at 6:43 AM. The severity is 'High', the software type is 'NX-OS', and 14 assets were evaluated. The 'About the Rule' section explains that it checks for X.509 certificate-based SSH authorization integration with TACACS+. Below this, a 'Results Summary' for 14 assets shows 0 Passed, 0 Did not pass, 0 Inconclusive, and 14 Not applicable. The 'Asset Results' section includes a search bar and filters, followed by a table of results.


Asset	Result	Product ID	Serial Number	IP Address	Support Tier
Device_76.1.1.2_20	Not applicable	IOS-C2950E	2000000000	76.1.1.20	Signature
76.1.1.20	Not applicable	IOS-C2950E	2000000000	76.1.1.20	Signature
Device_76.1.1.2	Not applicable	IOS-C2950E-E	2000000000	76.1.1.2	Signature


Regelansicht

- Über die Regel: Enthält Details zu der Regel wie Schweregrad, Softwaretyp, Version und bewertete Ressourcen.
- Zusammenfassung der Ergebnisse: Bietet eine Zusammenfassung der Anlagenergebnisse im Zusammenhang mit der Regel wie Bestanden, Nicht bestanden, Nicht schlüssig und Nicht zutreffend
- Ergebnisse der Ressourcen: Bietet eine Liste der Ressourcen mit Details wie Ressource, Ergebnis, Produkt-ID, Seriennummer, IP-Adresse und Support-Stufe

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.

 Anmerkung: Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet.


 Anmerkung: 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 zum Exportieren 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.

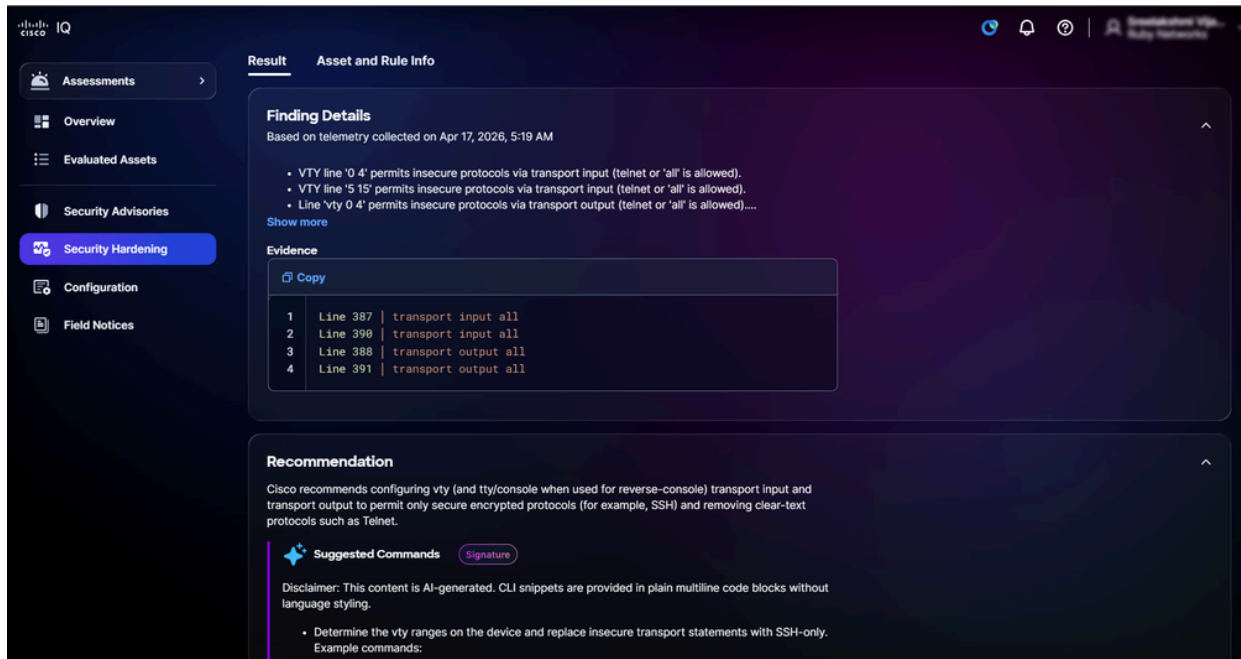
 Anmerkung: Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung.

Anzeigen von Ressourcenergebnissen für die Sicherheitssicherung

Um die Details eines Anlagenergebnisses anzuzeigen, klicken Sie in den Anlagenergebnissen auf eine Anlage. Auf der Detailseite für das Anlageergebnis werden Informationen entsprechend Ihrer Berechtigungsstufe oder -stufe angezeigt.

- 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



Signaturebene für die Sicherheitssicherung

• Signaturebene

- Details suchen: Stellt Informationen zu den bei der Bewertung identifizierten Konfigurationsabweichungen zusammen mit Evidenzprotokollen bereit
- Empfehlung: Aussagekräftige Anleitungen auf Geräteebene mit Codeausschnitten zur Gewährleistung der Konfigurationskonsistenz

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.


The screenshot shows a security assessment result for a device. The interface includes a sidebar with navigation options like 'Assessments', 'Overview', 'Evaluated Assets', 'Security Advisories', 'Security Hardening', 'Configuration', and 'Field Notices'. The main content area displays the assessment details, including the device name 'Device_65_16_3_22', the result 'Result' with a 'Did not pass' status, and the evaluation date 'Apr 22, 2026, 7:56 PM'. Below this, there are two sections: 'About the Asset' and 'About the Rule'. The 'About the Asset' section lists details such as Product ID, Product type (Wireless), IP address, Serial number, Software version (NA), Location, and Support tier (Signature). The 'About the Rule' section provides a description of the rule, its severity (High), and software type (AireOS).

Ressourcen- und Regelinformationen

- 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 verbesserte Ausfallsicherheit und ein geringeres betriebliches Risiko zu gewährleisten.

 Anmerkung: Konfigurationsbewertungen sind ausschließlich für Ressourcen mit Standard- oder Signatur-Supportstufen verfügbar.

Anzeigen der Konfigurationsbewertung

Klicken Sie auf eine Leistungsbeurteilung, um weitere Details zur Konfiguration anzuzeigen. Auf der Seite Konfigurationsbewertung werden folgende Informationen angezeigt:

The screenshot displays the Cisco IQ Configuration Assessment dashboard. It features a sidebar with navigation options: Assessments, Overview, Evaluated Assets, Security Advisories, Security Hardening, Configuration (highlighted), and Field Notices. The main content area is titled 'Configuration Assessment' and includes a sub-header 'About the Assessment' explaining that it evaluates assets against best practices. Below this is the 'Execution Outcome for Apr 19, 2026, 11:43 AM' section, which includes a 'Summary' showing 412 rule evaluations and 136 assets included. The 'Insights' section provides key findings, such as 'Product Family 'Cisco Catalyst 9500 Series Switches' has the strongest configuration compliance compared to other product families' and 'Critical wireless controllers lack coordinated security, RF, and baseline hardening'. The 'Rule Evaluations' section includes a table with columns for Rule, Severity, Assets Evaluated, Did Not Pass, Passed, Inconclusive, Not Appli..., Category, and Software Type. The table lists three rules with 'Critical' severity: 'Webauth: HTTPS interception for Web...', 'RRM: RF tag points to non-existing RF ...', and 'Version: Controller with not recommen...'. The first rule shows 8 assets evaluated, 2 did not pass, and 6 passed. The second rule shows 8 assets evaluated, 1 did not pass, and 7 passed. The third rule shows 8 assets evaluated, 7 did not pass, and 1 passed.

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: Geben Sie den Domänenbereich an, zu dem die Regel gehört.
- Softwaretyp: Geben Sie den Typ der Software-Ressourcen an, für die die Regel gilt.


Suchen und Filtern von Ansichten nach Regeln

Rule	Severity	Assets Evaluated	Did Not Pass	Passed	Inconclusive	Not Appli...	Category	Software Type
Webauth: HTTPS interception for Web...	Critical	8	2	6	0	0	Wireless	AireOS
RRM: RF tag points to non-existing RF ...	Critical	8	1	7	0	0	Wireless	IOS-XE
Version: Controller with not recommen...	Critical	8	7	1	0	0	Wireless	AireOS
uPC Domain Compatibility Parameters	Critical	14	0	0	14	0	Availability	IOS-XE

Regelauswertungen

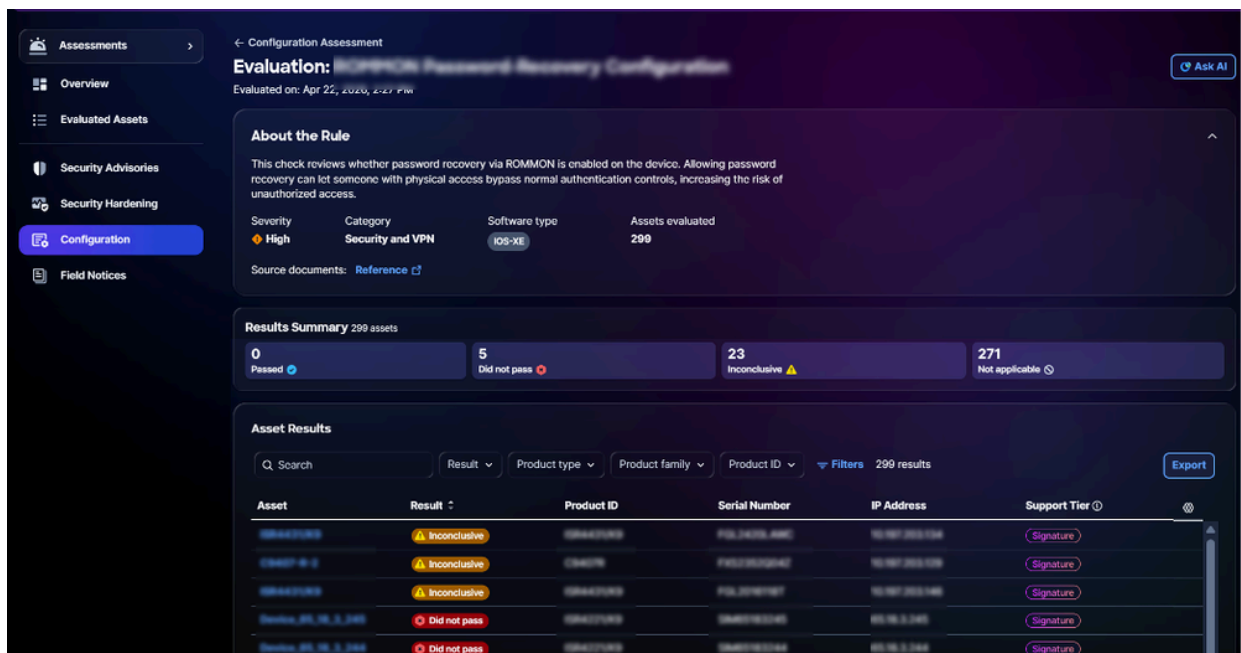
Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen oder auf Filter klicken und eine Option aus der Liste der verfügbaren Filter auswählen. Sie können auch nach einer Regel suchen, indem Sie den Namen der Regel in das Feld Suchen eingeben.

 Anmerkung: Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet.

 Anmerkung: 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:



Evaluierung


- Über die Regel: Enthält Details zu einer Regel wie Schweregrad, Kategorie, Softwaretyp und bewertete Ressourcen sowie 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


Exportieren der Ressourcenergebnisse

Zum Exportieren der Ressourcenergebnisse für Regeln klicken Sie auf Exportieren. Weitere Informationen zum Exportieren 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.

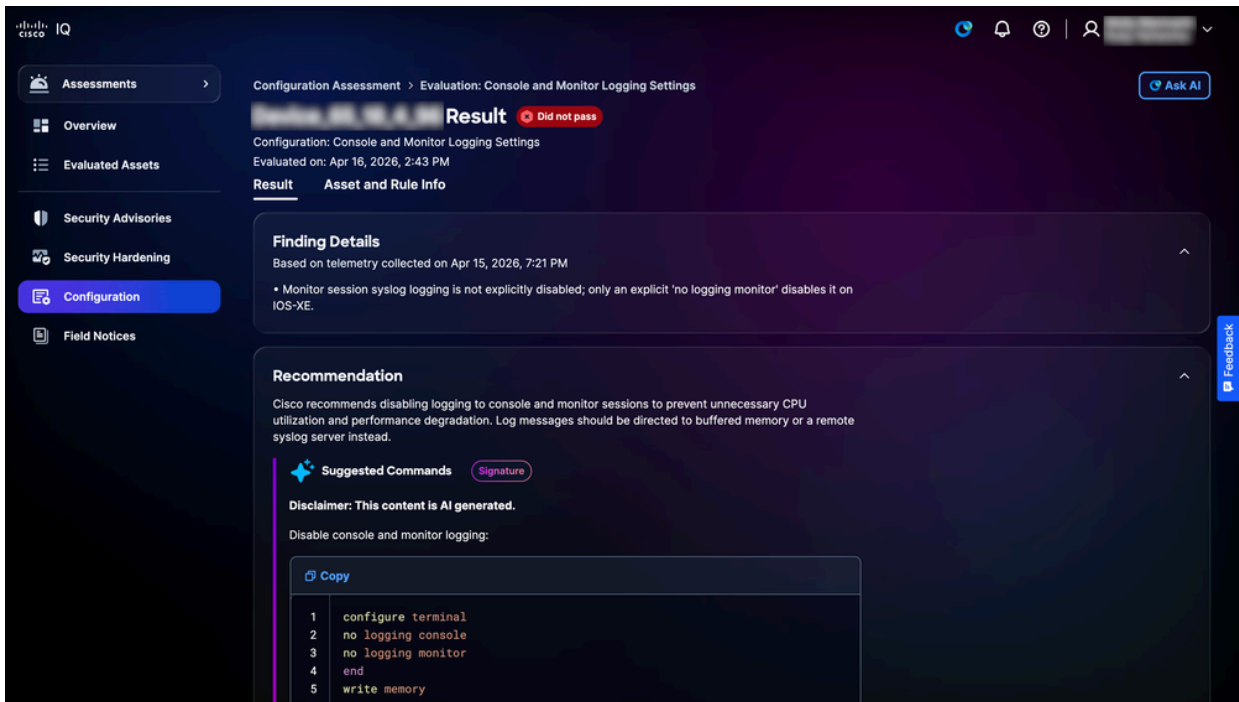
 Anmerkung: Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung.

Anzeigen von Ressourcenergebnissen für Konfigurationsanalysen

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

Auf der Detailseite für das Anlageergebnis werden Informationen entsprechend Ihrer Berechtigungsstufe oder -stufe angezeigt.

- 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



The screenshot displays the Cisco IQ Configuration Assessment interface. The main content area shows a finding titled "Configuration: Console and Monitor Logging Settings" with a "Result" of "Did not pass". The finding details state: "Based on telemetry collected on Apr 15, 2026, 7:21 PM" and "Monitor session syslog logging is not explicitly disabled; only an explicit 'no logging monitor' disables it on IOS-XE." Below this, a recommendation section provides context: "Cisco recommends disabling logging to console and monitor sessions to prevent unnecessary CPU utilization and performance degradation. Log messages should be directed to buffered memory or a remote syslog server instead." A "Suggested Commands" section includes a "Signature" button and a disclaimer: "Disclaimer: This content is AI generated." Below the disclaimer, the command "Disable console and monitor logging:" is followed by a code block containing the following commands:

```
1 configure terminal
2 no logging console
3 no logging monitor
4 end
5 write memory
```

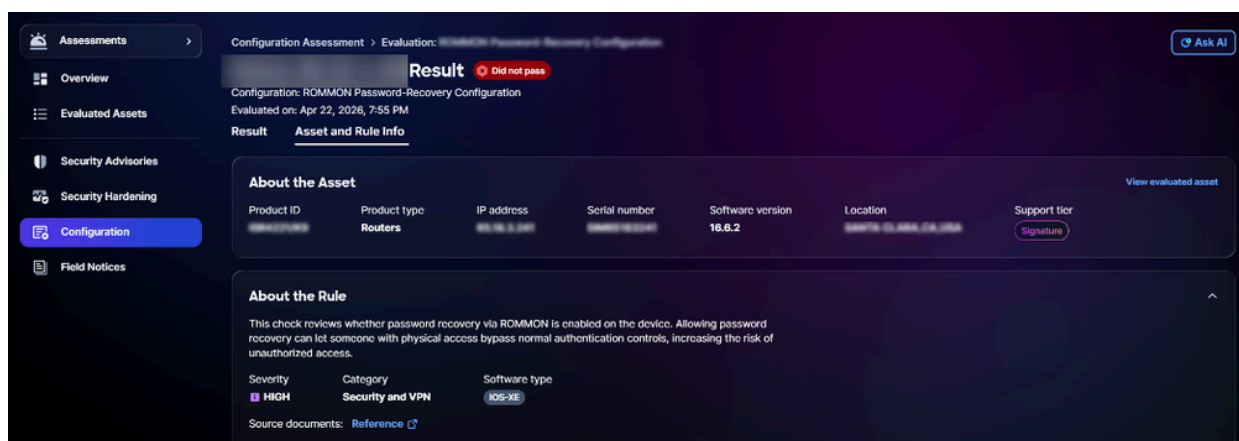
Signatureebene der Konfiguration

- Signaturebene

- Details suchen: Stellt Informationen zu den bei der Bewertung identifizierten Konfigurationsabweichungen zusammen mit Evidenzprotokollen bereit
- Empfehlung: Aussagekräftige Anleitungen auf Geräteebene mit Codeausschnitten, die die Ergebnisse aufgreifen und eine konsistente Konfiguration sicherstellen.

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.



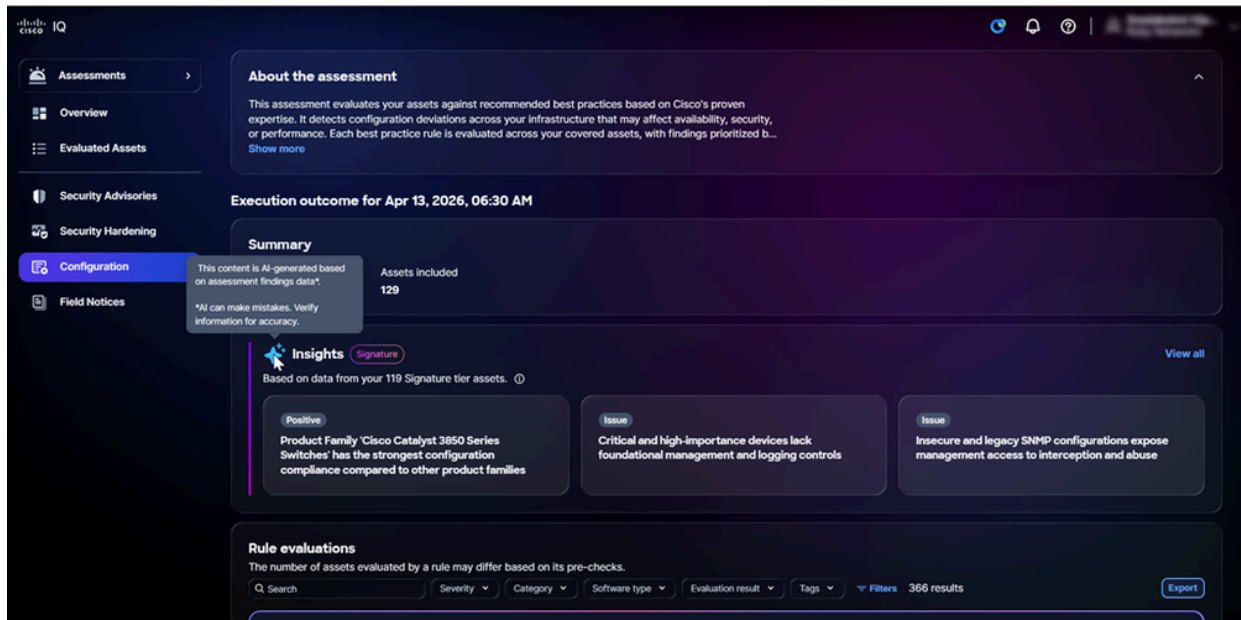
Ressourcen- und Regelinformationen

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

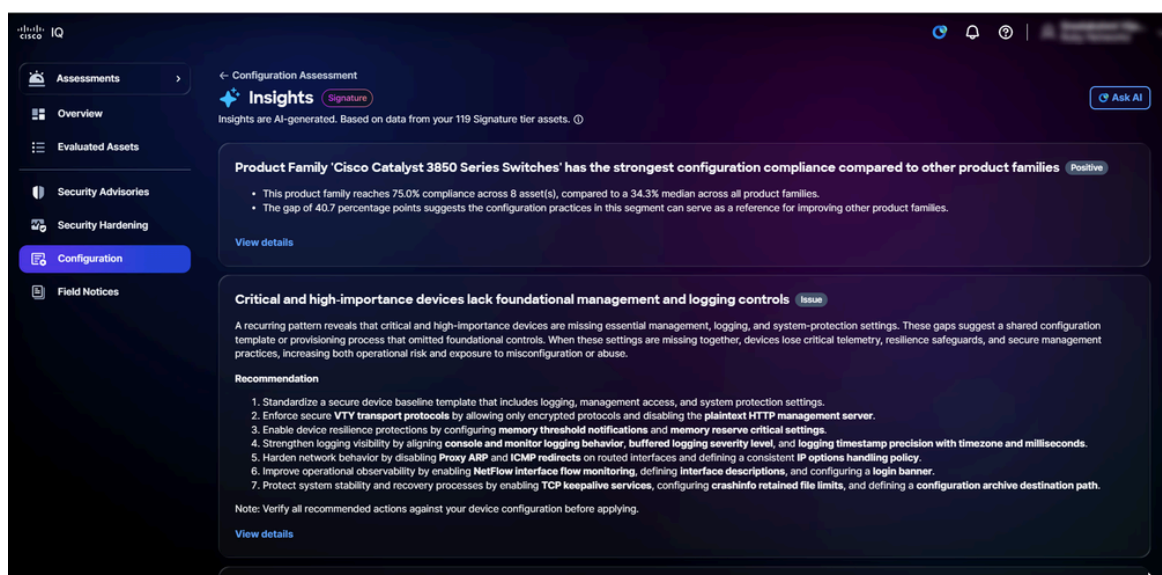
Die Erkenntnisse werden durch KI generiert und dienen als intelligentes Dashboard, das Bewertungsdaten in priorisierte Schlüsselkarten integriert und so wichtige Konfigurationsunterschiede zwischen verschiedenen Ergebnissen aufzeigt. Mit der Lösung können Sie die größten Infrastrukturrisiken effizient 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

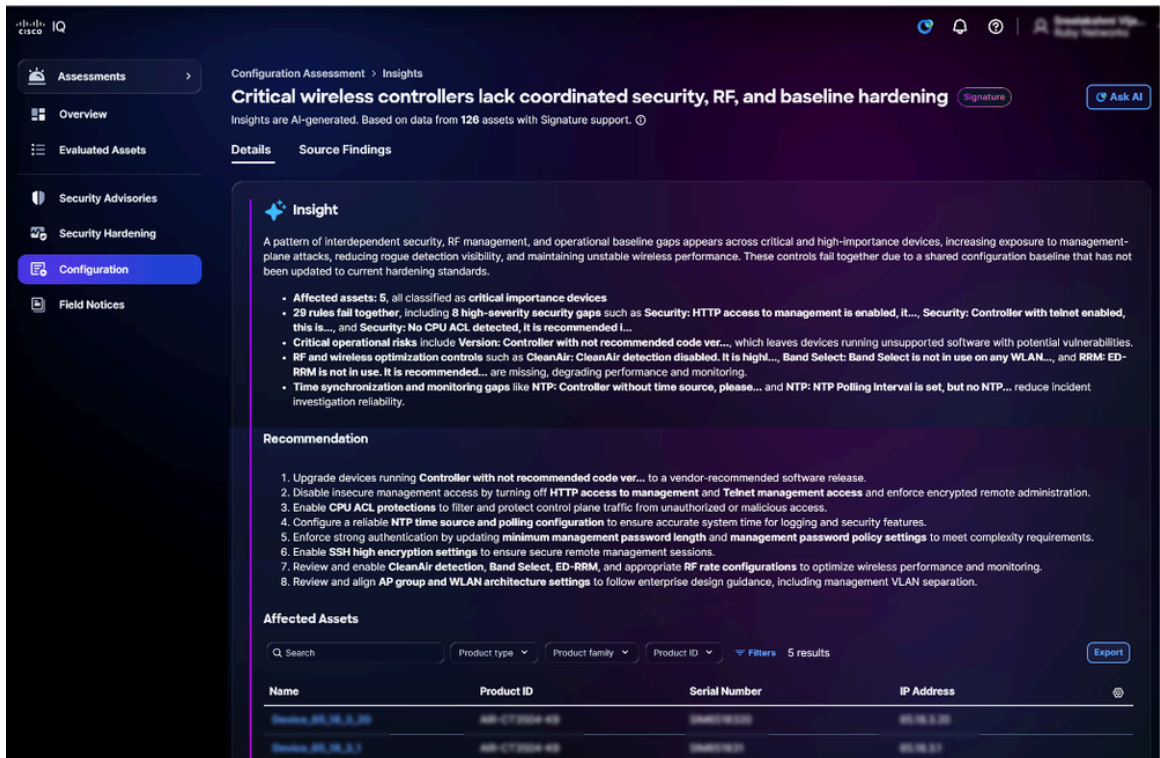
So zeigen Sie Details zu Einblicken an:

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



Einblicke

2. Klicken Sie auf Details anzeigen. Die Detailseite "Einblicke" wird mit den folgenden Informationen angezeigt: Sie können auch auf eine beliebige Karte klicken, um die Detailseite zu öffnen.



Einblicke - Details

- Erkenntnis: Bieten Sie eine Zusammenfassung, in der die Muster von Konfigurationsabweichungen hervorgehoben werden, die durch eine umfassende Analyse anhand zahlreicher Ergebnisse ermittelt wurden, sowie die 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 mit den Quellenergebnissen werden die detaillierten individuellen Ergebnisse angezeigt, die Ihre Erkenntnisse unterstützen.

Configuration Assessment > Insights

Critical wireless controllers lack cohesive security, RF, and management hardening

Insights are AI-generated. Based on data from 109 assets with Signature support. ⓘ


Details Source Findings

Q Search Severity Result 145 results Export

Asset	Rule	Severity	Serial Number	Result
...	Webauth: Virtual Gateway IP...	Low	...	Did not pass
...	Webauth: Virtual Gateway IP...	Low	...	Did not pass
...	Webauth: Virtual Gateway IP...	Low	...	Did not pass
...	Webauth: Virtual Gateway IP...	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
...	Webauth: Virtual Gateway IP...	Low	...	Did not pass

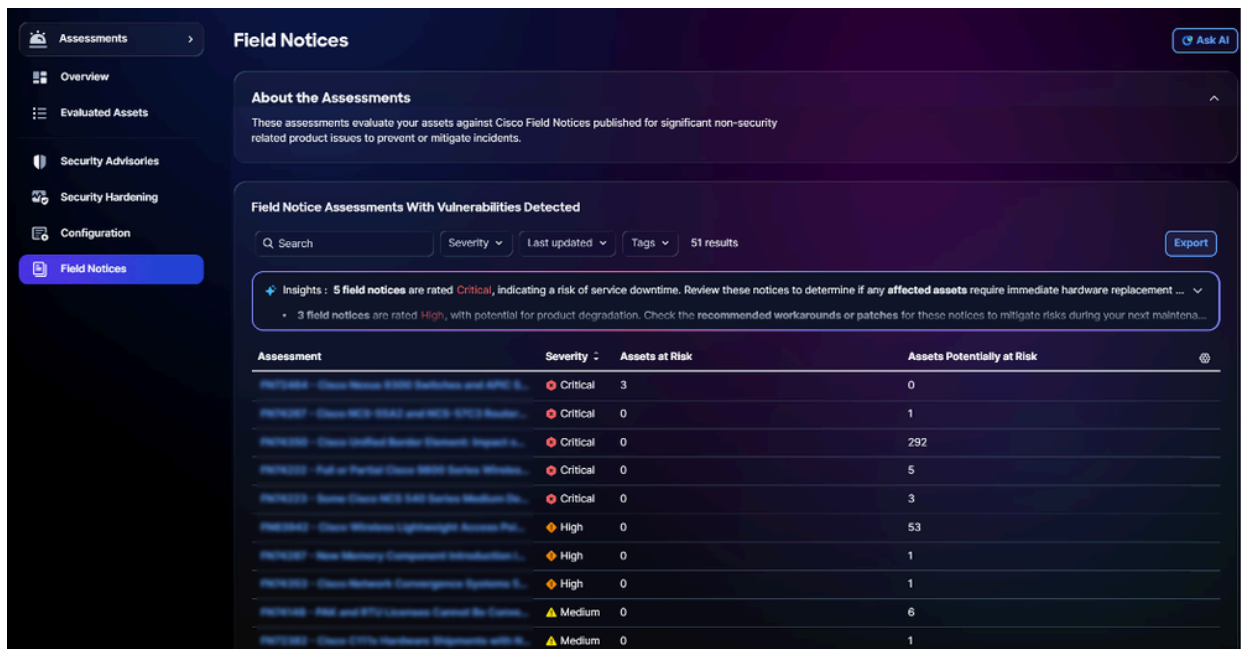
Ergebnisse

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 Wichtigkeit 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.



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 Details zur Anlagenbewertung werden angezeigt:


- Informationen zur Leistungsbeurteilung: Zusätzliche Details durch Zusammenfassung des Zwecks der Leistungsbeurteilung
- Aussagekräftige Analysen mit erkannten Schwachstellen: Zeigt eine Liste der Ressourcen an, die von der ausgewählten Problemmeldung betroffen sind, einschließlich Ressourcen mit erkannten Schwachstellen.

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.

 Anmerkung: Je nach Ihren Rollen und Berechtigungen stehen verschiedene Filter zur Verfügung.

Exportieren der Ergebnisse der Leistungsbeurteilungsressourcen für Problemhinweise

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

Anzeigen der Ergebnisse der Leistungsbeurteilungsressourcen für Problemhinweise

Klicken Sie in den Anlagenbewertungsergebnissen auf eine Ressource, um die Details des Anlagenresultates einer Bewertung anzuzeigen. Die Detailseite der bewerteten Ressource 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.

Support-Anwendung

Die Support-Anwendung bietet eine konsolidierte Ansicht der Support-Tickets für Kunden. 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.

Um in Cisco IQ auf die Support-Anwendung zuzugreifen, wählen Sie Home > Support. Die Seite Support Overview (Support-Übersicht) wird angezeigt.

Support-Überblick



Support-Überblick

Die Seite Support Overview (Support-Übersicht) ist ein interaktives Dashboard mit Diagrammen mit den folgenden Informationen:

- Offene Tickets nach Schweregrad: Alle offenen Tickets der letzten 90 Tage nach Schweregrad S1 bis S4
- Offene Tickets nach Ticketstatus: Alle offenen Tickets der letzten 90 Tage sortiert nach Ticketstatus
- RMAs nach Status: Alle RMAs der letzten 90 Tage nach ihrem Status kategorisiert
- Geschlossene Fälle nach Schweregrad: Die Gesamtzahl der abgeschlossenen Fälle aus den letzten 90 Tagen, kategorisiert nach Schweregrad

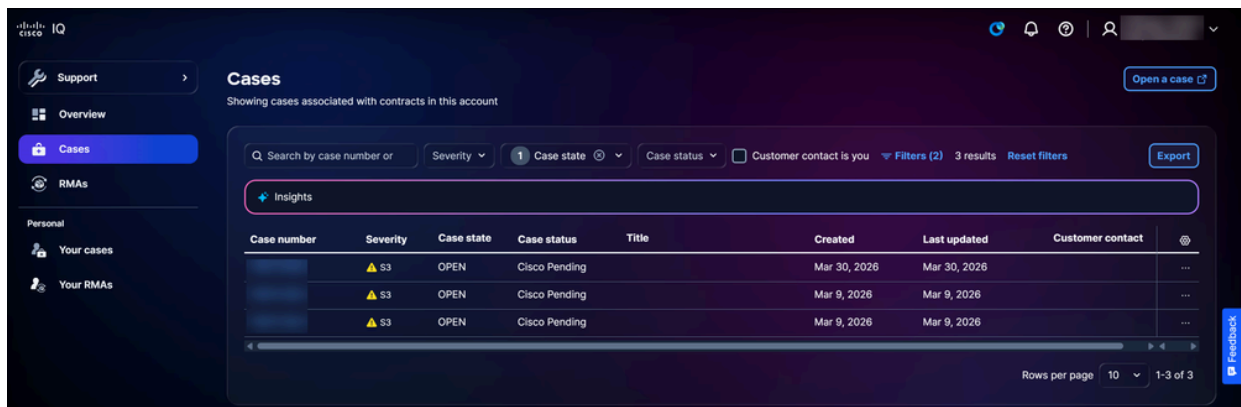
Anzeigen von Details zu Tickets

Durch Klicken auf Details anzeigen wird die Seite auf die Seite Fälle des Kontos umgeleitet. Durch Klicken auf eine Leiste aus einem Diagramm auf der Seite Übersicht wird die Seite auf die Seite Fälle des Kontos umgeleitet, auf der relevante Filter angewendet werden. Wenn Sie beispielsweise im Diagramm Offene Tickets nach Schweregrad auf die S1-Schweregrad-Leiste klicken, wird die Ticket-Seite des Kontos aufgerufen, deren Ticket-Status auf "Offen" und Schweregrad auf "S1" gesetzt ist. Weitere Informationen finden Sie unter [Tickets](#).

Cases

Account-Tickets

Navigieren Sie zur Seite Tickets, indem Sie im linken Bereich auf Tickets (Tickets) klicken.



Case number	Severity	Case state	Case status	Title	Created	Last updated	Customer contact
	▲ S3	OPEN	Cisco Pending		Mar 30, 2026	Mar 30, 2026	...
	▲ S3	OPEN	Cisco Pending		Mar 9, 2026	Mar 9, 2026	...
	▲ S3	OPEN	Cisco Pending		Mar 9, 2026	Mar 9, 2026	...

Cases

Auf der Seite Cases (Fälle) wird eine konsolidierte Liste aller Fälle angezeigt, die mit den Verträgen in Ihrem Cisco IQ-Konto verknüpft sind. Sie können die in der Liste angezeigten Spalten konfigurieren, indem Sie auf das Symbol Einstellungen klicken, die Kontrollkästchen der gewünschten Spalten aktivieren und auf Anwenden klicken. Die Spalten Ticketnummer, Schweregrad, Ticketstatus, Ticketstatus, Titel und Erstellt werden immer angezeigt und können nicht deaktiviert werden.

Verfügbare Aktionen

Die folgenden Aktionen können auf der Seite Cases (Fälle) ausgeführt werden:

- Ticket erstellen: Klicken Sie auf Ticket öffnen, um [SCM](#) zu starten und ein Ticket zu erstellen.
- Daten exportieren: Klicken Sie auf Exportieren, um alle Daten herunterzuladen, die derzeit im Dashboard als CSV-Datei angezeigt werden.
- Details zum Ticket anzeigen: Klicken Sie auf eine Ticketnummer oder eine Tabellenzeile, um die Detailansicht eines Tickets anzuzeigen (weitere Informationen finden Sie unter [Ticketdetails](#)).
- Schließen eines Tickets: Wählen Sie das Symbol "Weitere Optionen" > "Ticket schließen", um das Fenster Ticket schließen zu öffnen, in dem Sie einen Grund für den Abschluss angeben und das Ticket schließen können.
- Ticket erneut öffnen: Wählen Sie das Symbol Weitere Optionen > Ticket erneut öffnen, um das Fenster Ticket erneut öffnen zu öffnen. Hier können Sie einen Grund für das erneute Öffnen angeben.




Anmerkung: Geschlossene Rechtssachen können innerhalb von 14 Tagen nach ihrer Schließung wieder geöffnet werden.

Filtern von Ansichten nach Tickets

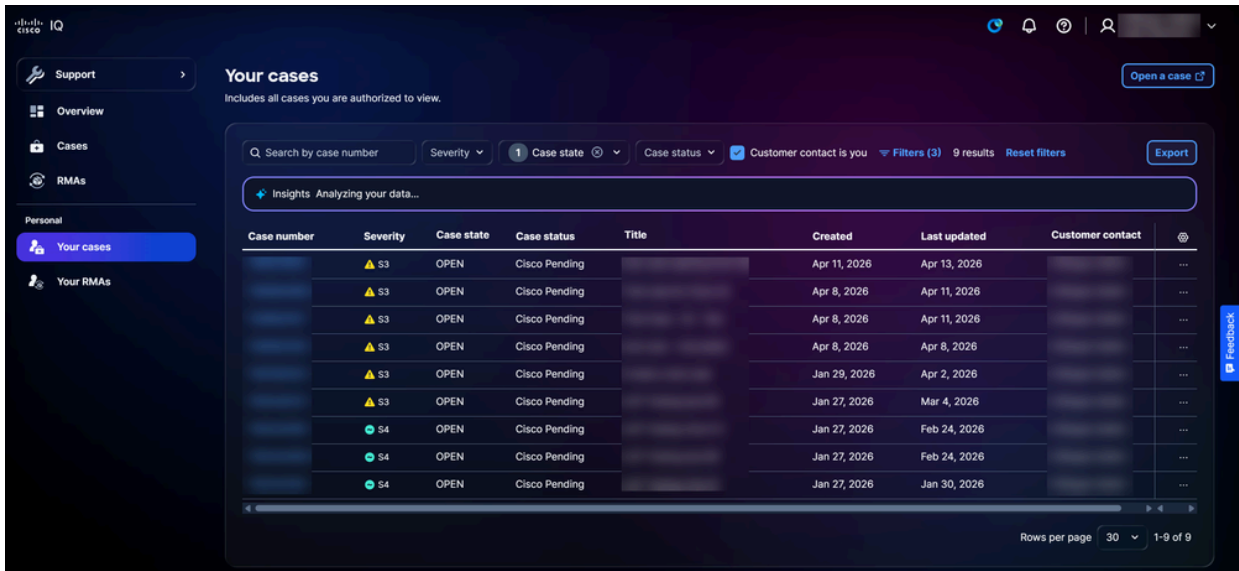
Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen oder das Kontrollkästchen Kundenkontakt ist für Sie aktiviert. Klicken Sie optional auf Filter, und wählen Sie aus der Liste der verfügbaren Filteroptionen aus. Filter und Auswahlen bleiben während der Sitzungen und Anmeldungen erhalten, um das Dashboard zu personalisieren. Folgende Standardfilter werden angewendet:

- Ticketstatus: Geöffnet
- Erstellt: Erstellt innerhalb von 90 Tagen

 Anmerkung: Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet.

Ihre Fälle

Navigieren Sie zur Seite Ihre Fälle, indem Sie im linken Bereich auf Ihre Fälle klicken.



Case number	Severity	Case state	Case status	Title	Created	Last updated	Customer contact	
	▲ S3	OPEN	Cisco Pending		Apr 11, 2026	Apr 13, 2026		...
	▲ S3	OPEN	Cisco Pending		Apr 8, 2026	Apr 11, 2026		...
	▲ S3	OPEN	Cisco Pending		Apr 8, 2026	Apr 11, 2026		...
	▲ S3	OPEN	Cisco Pending		Apr 8, 2026	Apr 8, 2026		...
	▲ S3	OPEN	Cisco Pending		Jan 29, 2026	Apr 2, 2026		...
	▲ S3	OPEN	Cisco Pending		Jan 27, 2026	Mar 4, 2026		...
	● S4	OPEN	Cisco Pending		Jan 27, 2026	Feb 24, 2026		...
	● S4	OPEN	Cisco Pending		Jan 27, 2026	Feb 24, 2026		...
	● S4	OPEN	Cisco Pending		Jan 27, 2026	Jan 30, 2026		...

Ihre Fälle

Auf der Seite Ihre Tickets wird eine konsolidierte Liste der Tickets angezeigt, die Sie anzeigen und verwalten dürfen. Sie können die in der Liste angezeigten Spalten konfigurieren, indem Sie auf das Symbol Einstellungen klicken, die Kontrollkästchen der gewünschten Spalten aktivieren und auf Anwenden klicken. Die Spalten Ticketnummer, Schweregrad, Ticketstatus, Ticketstatus, Titel und Erstellt werden immer angezeigt und können nicht deaktiviert werden.

Verfügbare Aktionen

Die folgenden Aktionen können auf der Seite "Ihre Tickets" ausgeführt werden:

- Ticket erstellen: Ticket erstellen: Klicken Sie auf Ticket öffnen, um SCM zu öffnen und ein Ticket zu erstellen.
- Daten exportieren: Klicken Sie auf Exportieren, um alle Daten herunterzuladen, die derzeit im Dashboard als CSV-Datei angezeigt werden.
- Details zum Ticket anzeigen: Klicken Sie auf eine Ticketnummer oder eine Tabellenzeile, um die Detailansicht eines Tickets anzuzeigen (weitere Informationen finden Sie unter [Ticketdetails](#)).

- Schließen eines Tickets: Wählen Sie das Symbol "Weitere Optionen" > "Ticket schließen", um das Fenster Ticket schließen zu öffnen, in dem Sie einen Grund für den Abschluss angeben und das Ticket schließen können.
- Ticket erneut öffnen: Wählen Sie das Symbol Weitere Optionen > Ticket erneut öffnen, um das Fenster Ticket erneut öffnen zu öffnen. Hier können Sie einen Grund für das erneute Öffnen angeben.



Anmerkung: Geschlossene Rechtssachen können innerhalb von 14 Tagen nach ihrer Schließung wieder geöffnet werden.

Filtern von Ansichten für Ihre Tickets

Sie können die Listenansicht filtern, indem Sie einen Filter aus den Dropdown-Listen auswählen oder das Kontrollkästchen Kundenkontakt ist für Sie aktiviert. Klicken Sie optional auf Filter, und wählen Sie aus der Liste der verfügbaren Filteroptionen aus. Filter und Auswahlen bleiben während der Sitzungen und Anmeldungen erhalten, um das Dashboard zu personalisieren. Folgende Standardfilter werden angewendet:

- Ticketstatus: Geöffnet
- Kundenkontakt ist Ihr Kontrollkästchen
- Erstellt: Erstellt innerhalb von 90 Tagen




Anmerkung: Einige Filter werden je nach Vergrößerungseinstellung des Bildschirms möglicherweise ausgeblendet.

Ticket-Detailansichten

Um die Details eines Tickets anzuzeigen, klicken Sie in der Liste auf ein Ticket.

Ticket-Detailansicht

Die Ticket-Detailansicht wird angezeigt. Sie bietet eine zentralisierte Ansicht eines Support-Tickets, in der Sie Ticket-Informationen und betroffene Ressourcen überprüfen, den Fortschritt des TAC verfolgen und auf verfügbare Ticket-Aktionen zugreifen können. Zu den verfügbaren Aktionen gehören das erneute Öffnen eines abgeschlossenen Tickets durch Klicken auf Ticket erneut öffnen, das Schließen eines offenen Tickets durch Klicken auf Ticket schließen und das Starten des KI-Assistenten mit dem Kontext des Tickets durch Klicken auf KI fragen. Die verfügbaren Registerkarten werden in den folgenden Abschnitten beschrieben.

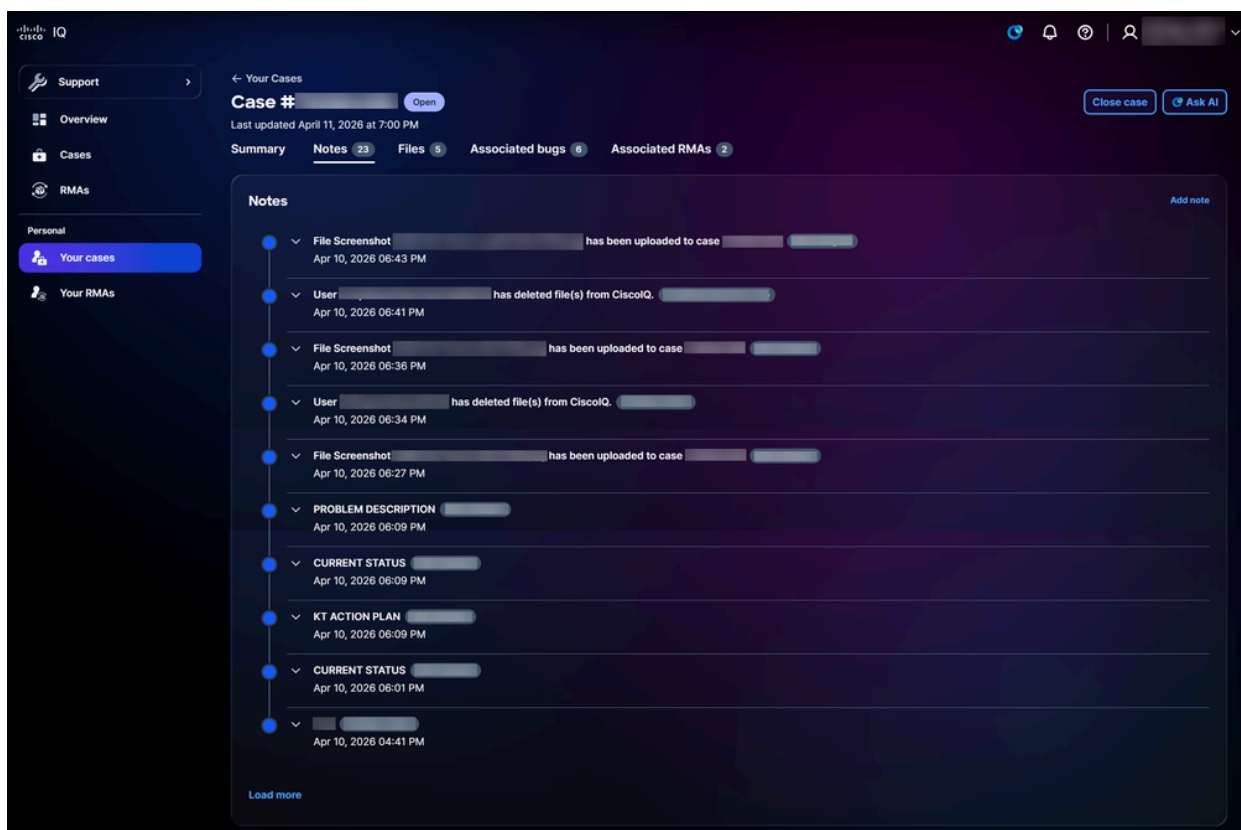
 Anmerkung: KI-generierte Felder werden ggf. mit einem Sternsymbol gekennzeichnet.

Sternsymbol

Zusammenfassung

Auf der Registerkarte Übersicht werden wichtige Informationen zu Supportfällen angezeigt, die Ihnen einen schnellen Überblick über den aktuellen Status, den Kontext und den Fortschritt eines einzelnen Support-Falls ermöglichen. Sie können Ticket-Details und betroffene Ressourcen einsehen, den Lebenszyklus Ihres Tickets über Details zum Fortschritt des TAC-Vorgangs überwachen, Kontaktinformationen ändern und E-Mail-Adressen angeben, um Benachrichtigungen zu Ticket-Aktualisierungen zu erhalten. Nur ausgewählte Felder können bearbeitet werden.

Hinweise



Hinweise

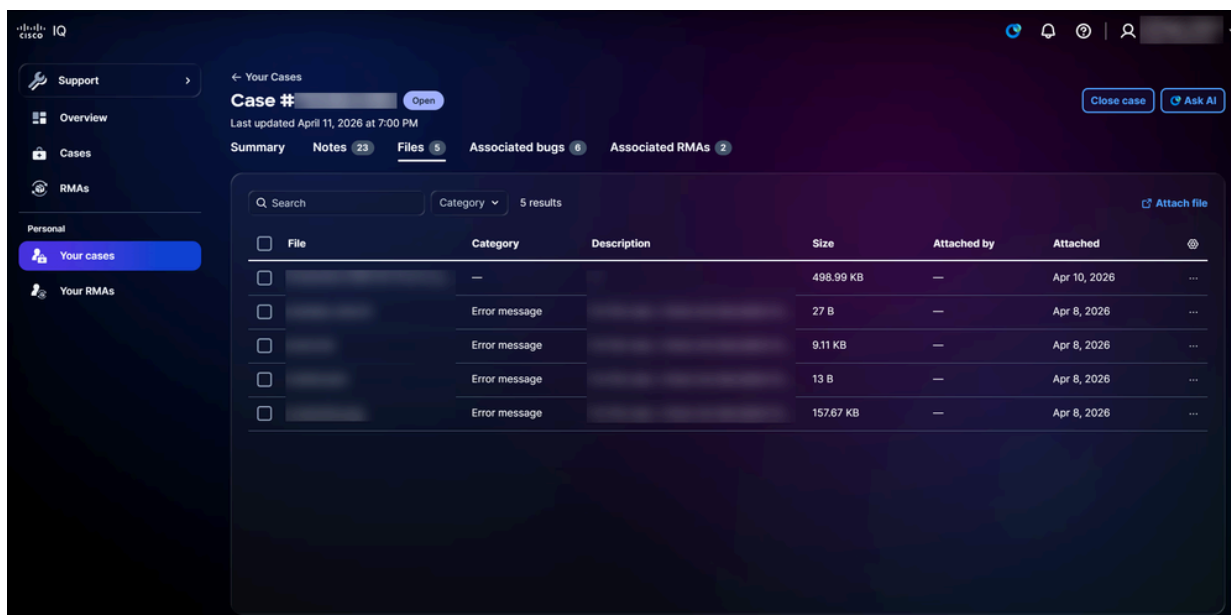
Durch Klicken auf die Registerkarte Notizen wird die Seite Notizen geöffnet. Sie können alle Notizen zu einem Ticket anzeigen, unabhängig davon, ob ein Kunde oder ein Cisco Techniker sie eingereicht hat.

So fügen Sie eine neue Notiz hinzu:

 **Warnung:** Notizen können nicht gelöscht werden.

1. Klicken Sie auf Hinweis hinzufügen. Das Fenster Notiz hinzufügen wird geöffnet.
2. Geben Sie einen Titel ein.
3. Geben Sie die Details ein.
4. Klicken Sie auf Hinzufügen.

Dateien



Dateien

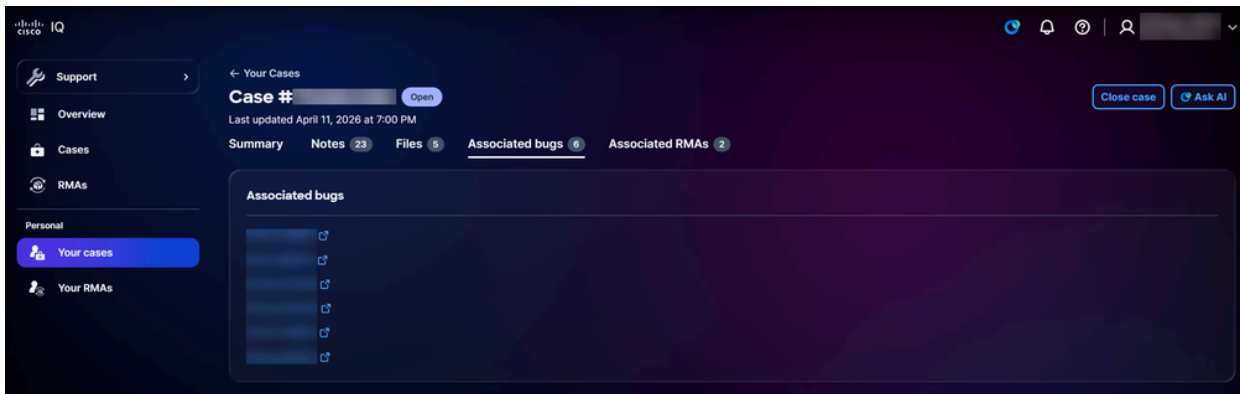
Durch Klicken auf die Registerkarte Dateien wird die Seite Dateien geöffnet. Sie können den Namen, die Größe und das Datum der Dateien eines Tickets anzeigen lassen sowie Dateien hinzufügen oder löschen. Filtern Sie Dateien, indem Sie eine Option aus der Dropdown-Liste Kategorie auswählen. Klicken Sie optional auf Filter, und wählen Sie eine der verfügbaren Filteroptionen aus. Sie können die in der Liste angezeigten Spalten auch konfigurieren, indem Sie auf das Symbol Einstellungen klicken, die Kontrollkästchen der gewünschten Spalten aktivieren und auf Anwenden klicken.

Klicken Sie zum Hinzufügen einer Datei auf Datei anhängen. Sie werden zu SCM weitergeleitet, wo Sie eine Datei für das Ticket hochladen können.

Um eine Datei zu löschen, aktivieren Sie das bzw. die Kontrollkästchen der gewünschten Datei(en), und klicken Sie auf Löschen. Das Fenster Datei(en) löschen wird geöffnet. Klicken Sie auf Datei(en) löschen.

 Anmerkung: Dateidownloads werden nicht unterstützt.

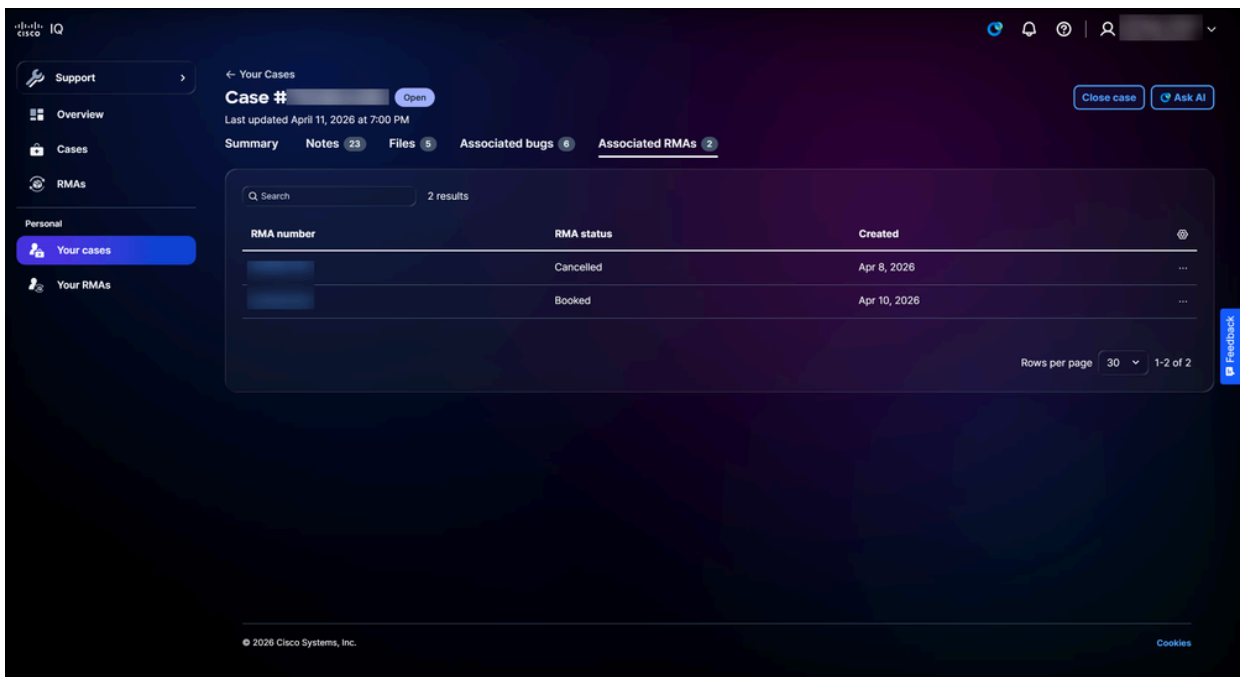
Zugehörige Fehler



Zugehörige Fehler

Durch Klicken auf die Registerkarte Zugehörige Bugs wird die Seite Zugehörige Bugs geöffnet. Sie können auf eine Bug-ID klicken, um detaillierte Informationen zu Fehlern im [Bug Search Tool](#) von Cisco.com zu durchsuchen.

Zugehörige RMAs



Zugehörige RMAs

Durch Klicken auf die Registerkarte "Zugeordnete RMAs" wird die Seite "Zugeordnete RMAs" geöffnet. Sie können die in der Liste angezeigten Spalten konfigurieren, indem Sie auf das Symbol Einstellungen klicken, die Kontrollkästchen der gewünschten Spalten aktivieren und auf Anwenden klicken. Auf der Seite für zugeordnete RMAs können Sie die folgenden Aktionen durchführen:

- Schließen eines Tickets: Klicken Sie auf Close case, um das Fenster Close case zu öffnen, in dem Sie einen Grund für den Abschluss angeben und das Ticket schließen können.
- RMA-Details anzeigen: Klicken Sie auf eine RMA-Nummer oder Tabellenzeile, um die Detailansicht einer RMA zu öffnen (weitere Informationen finden Sie in [RMA-Detailansichten](#)).
- Kontakt Cisco Logistics: Klicken Sie in einer Zeile auf das Symbol More Options (Weitere Optionen) > Contact Cisco logistics (Cisco Logistik kontaktieren), um das Cisco Logistics Team zu kontaktieren.

RMA

Konto-RMAs

The screenshot shows the Cisco IQ interface for managing Return Merchandise Authorizations (RMAs). The main content area displays a table titled "RMAs" with the subtitle "Showing RMAs associated with cases in this account." The table has four columns: "RMA number", "RMA status", "Associated case number", and "Created". There are 71 results shown. The table includes an "Export" button in the top right corner. The "Created" column shows dates ranging from Sep 8, 2025 to Apr 10, 2026. The "RMA status" column shows various statuses such as "Booked", "Cancelled", and "Closed".

RMA number	RMA status	Associated case number	Created
	Booked		Apr 10, 2026
	Cancelled		Apr 8, 2026
	Cancelled		Apr 8, 2026
	Closed		Jan 28, 2026
	Closed		Dec 11, 2025
	Closed		Oct 22, 2025
	Closed		Oct 7, 2025
	Closed		Oct 1, 2025
	Closed		Sep 15, 2025
	Closed		Sep 8, 2025

Liste der RMAs

Navigieren Sie zur Seite RMAs, indem Sie im linken Bereich auf RMAs klicken. Auf der Seite für RMAs wird eine konsolidierte Liste aller RMAs angezeigt, die den Tickets in Ihrem Cisco IQ-Konto zugeordnet sind. Sie können die in der Liste angezeigten Spalten konfigurieren, indem Sie auf das Symbol Einstellungen klicken, die Kontrollkästchen der gewünschten Spalten aktivieren und auf Anwenden klicken.

Verfügbare Aktionen

Auf der Seite "RMAs" können Sie die folgenden Aktionen durchführen:

- Daten exportieren: Klicken Sie auf Exportieren, um alle Daten herunterzuladen, die derzeit

als CSV-Datei angezeigt werden.

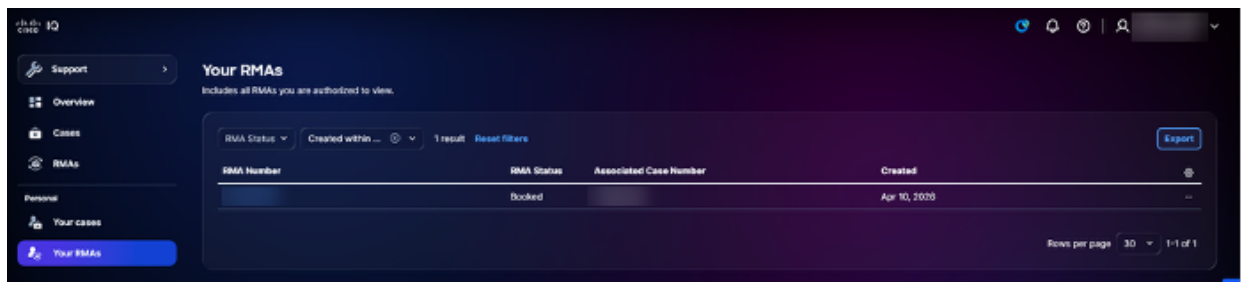
- RMA-Details anzeigen: Klicken Sie auf eine RMA-Nummer oder Tabellenzeile, um die Detailansicht einer RMA zu öffnen (weitere Informationen finden Sie in [RMA-Detailansichten](#)).
- Kontakt Cisco Logistics: Klicken Sie in einer Zeile auf das Symbol More Options (Weitere Optionen) > Contact Cisco logistics (Cisco Logistik kontaktieren), um das Cisco Logistics Team zu kontaktieren.

Ansichten für Konto-RMAs filtern

Sie können die Listenansicht filtern, indem Sie in den Dropdown-Listen Filter auswählen.

Ihre RMA

Navigieren Sie zur Seite Ihre RMAs, indem Sie im linken Bereich auf Ihre RMAs klicken.



Ihre RMA

Auf der Seite Ihre RMAs wird eine konsolidierte Liste der RMAs angezeigt, für die Sie die erforderlichen Berechtigungen besitzen. Sie können die in der Liste angezeigten Spalten konfigurieren, indem Sie auf das Symbol Einstellungen klicken, die Kontrollkästchen der gewünschten Spalten aktivieren und auf Anwenden klicken.

Verfügbare Aktionen

Auf der Seite Ihre RMAs können Sie die folgenden Aktionen durchführen:

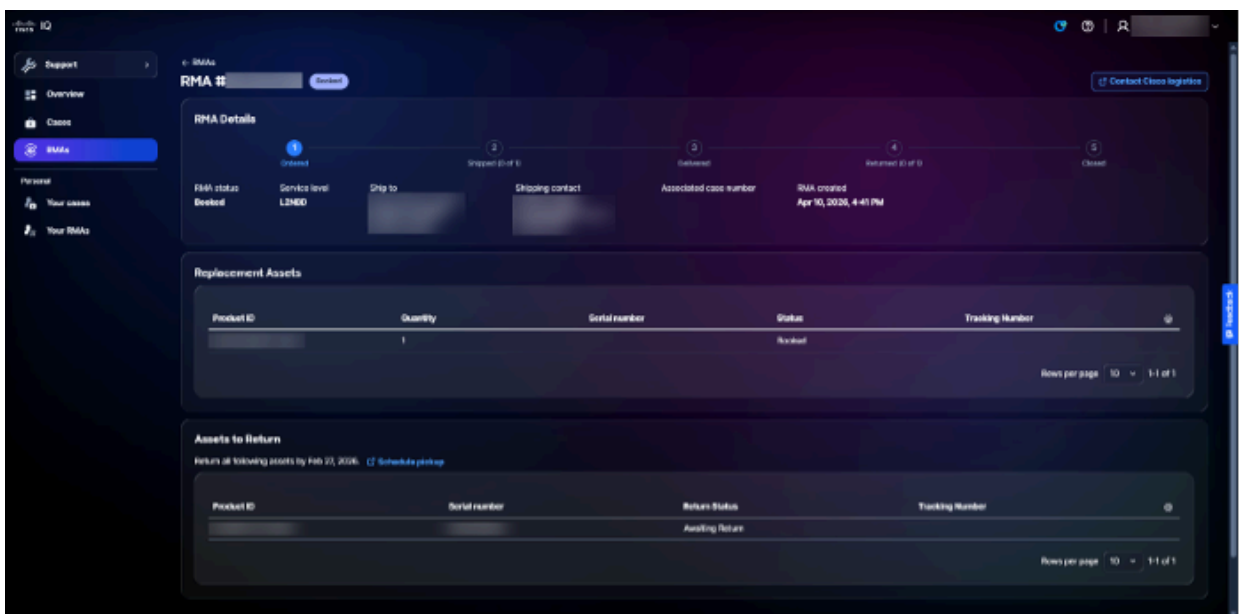
- Daten exportieren: Klicken Sie auf Exportieren, um alle Daten herunterzuladen, die derzeit als CSV-Datei angezeigt werden.
- RMA-Details anzeigen: Klicken Sie auf eine RMA-Nummer oder Tabellenzeile, um die Detailansicht einer RMA zu öffnen (weitere Informationen finden Sie in [RMA-Detailansichten](#)).

- Kontakt Cisco Logistics: Klicken Sie in einer Zeile auf das Symbol More Options (Weitere Optionen) > Contact Cisco logistics (Cisco Logistik kontaktieren), um das Cisco Logistics Team zu kontaktieren.

Filtern von Ansichten für RMAs

Sie können die Listenansicht filtern, indem Sie eine Option aus der Dropdown-Liste Erstellt auswählen.

RMA-Detailansichten




RMA-Detailansicht

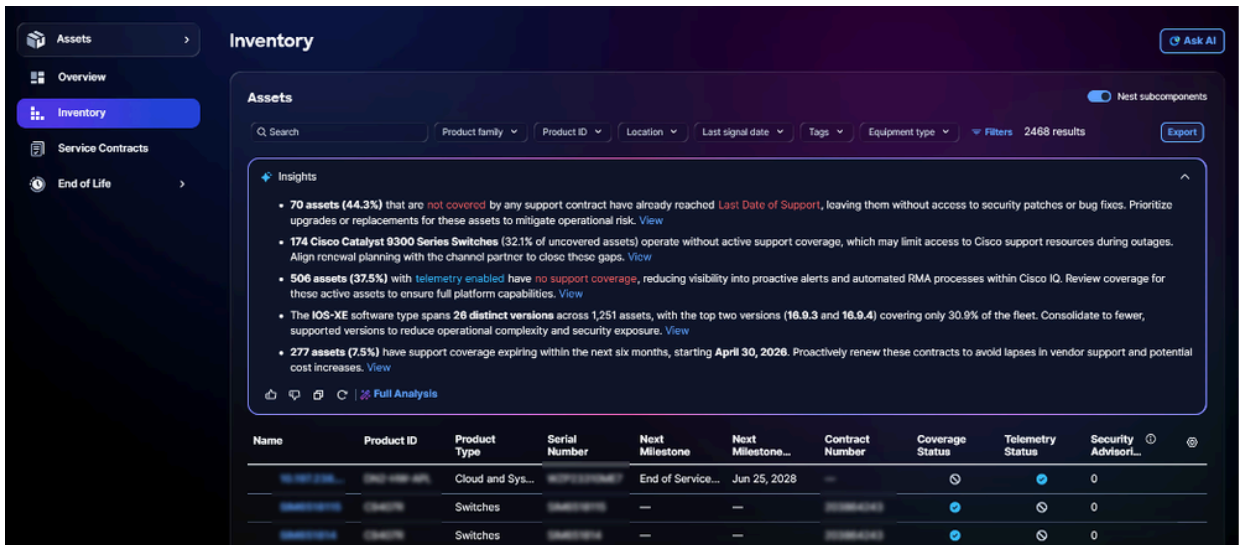
Die RMA-Detailansicht bietet eine zentralisierte Ansicht einer RMA, in der Sie die RMA-Informationen prüfen, den Fortschritt verfolgen und auf die verfügbaren RMA-Aktionen zugreifen können. Zu den verfügbaren Aktionen gehören die Kontaktaufnahme mit dem Cisco Logistik-Team, der Zugriff auf Nachverfolgungsnummern und die Planung der Abholung von Ressourcen.

Allgemeine Anwendungsfunktionen

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.



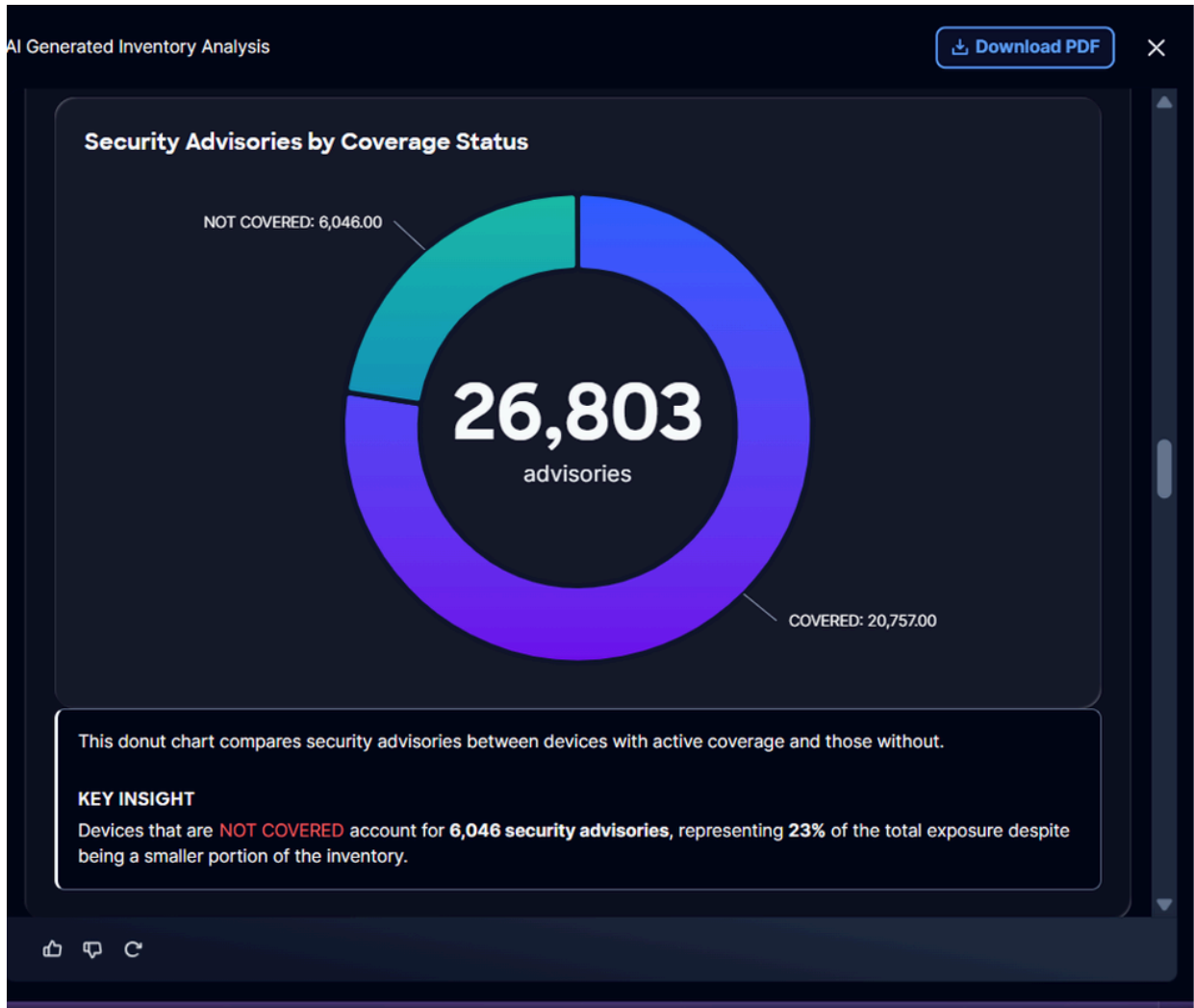
The screenshot displays the 'Inventory' section of a software interface. The main content area is titled 'Assets' and includes a search bar and various filters. Below the filters, there is an 'Insights' panel with several bullet points providing analysis on asset coverage, support contracts, and telemetry. At the bottom, there is a table with columns for 'Name', 'Product ID', 'Product Type', 'Serial Number', 'Next Milestone', 'Next Milestone...', 'Contract Number', 'Coverage Status', 'Telemetry Status', and 'Security Advisor...'. The table contains three rows of data.

Name	Product ID	Product Type	Serial Number	Next Milestone	Next Milestone...	Contract Number	Coverage Status	Telemetry Status	Security Advisor...
...	...	Cloud and Sys...	...	End of Service...	Jun 25, 2028	0
...	...	Switches	...	—	—	0
...	...	Switches	...	—	—	0

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.

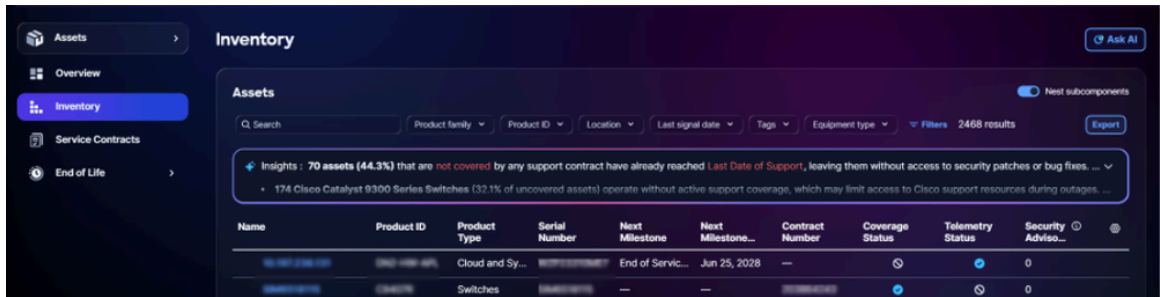
Exportieren von Informationen

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.

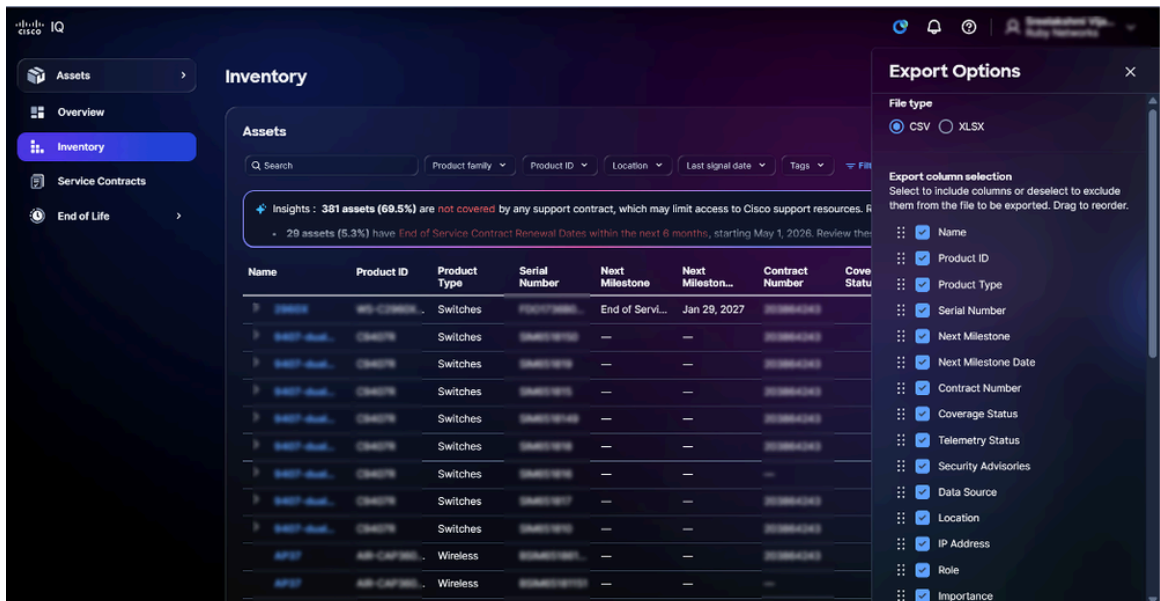
So exportieren Sie Informationen von einer Seite:

1. Navigieren Sie zur Seite.



Exportieren von Beständen in der Anwendung "Anlagen"

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



Exportoptionen

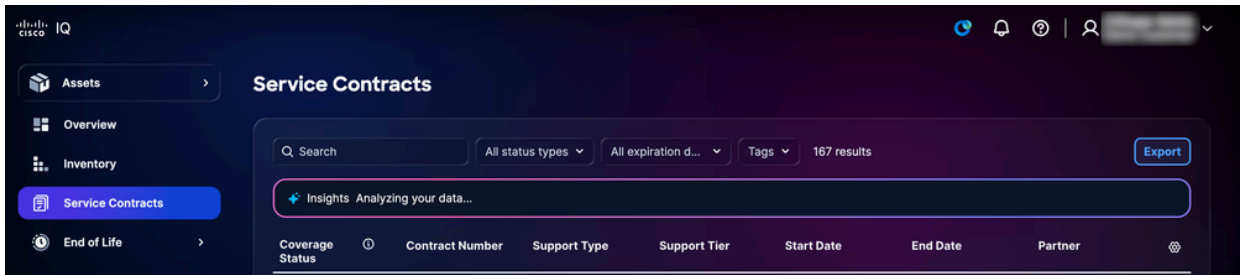
3. Wählen Sie einen Dateityp aus.

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.

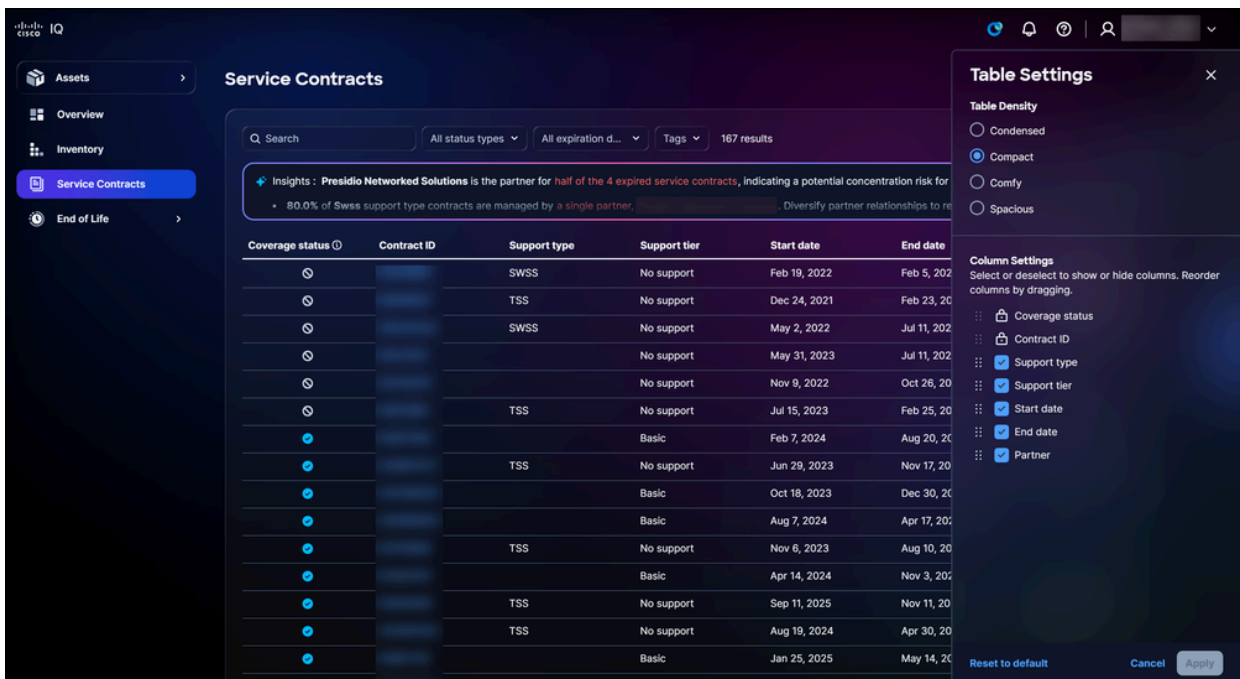
Tabelleneinstellungen

Sie können Tabelleneinstellungen konfigurieren, um benutzerdefinierte und verfeinerte Ansichten für verschiedene Anwendungsfeatures 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.

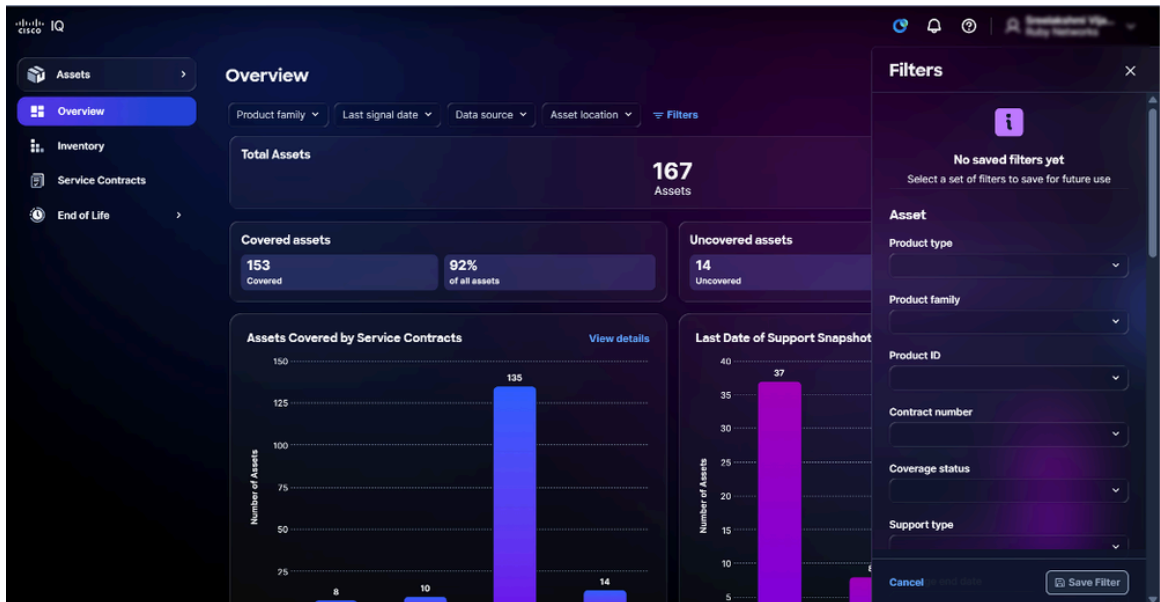
Anpassen von Filtern

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

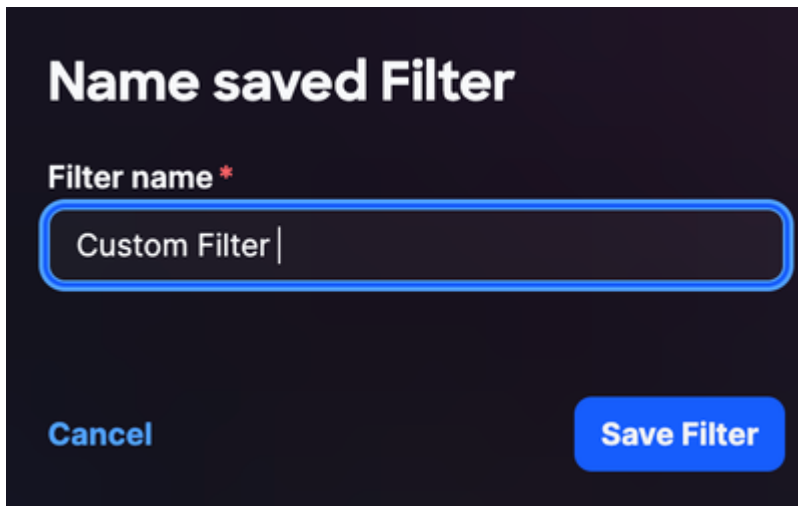
So erstellen Sie einen benutzerdefinierten Filter:

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 Name saved Filter wird geöffnet.



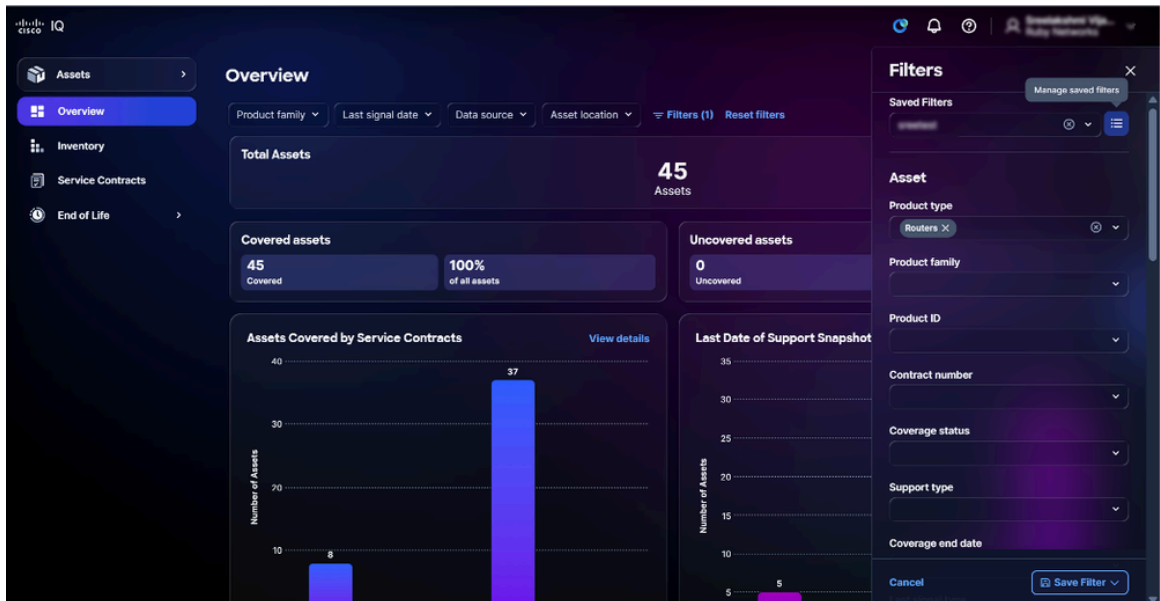
Filtername

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

Bearbeiten eines Filternamens

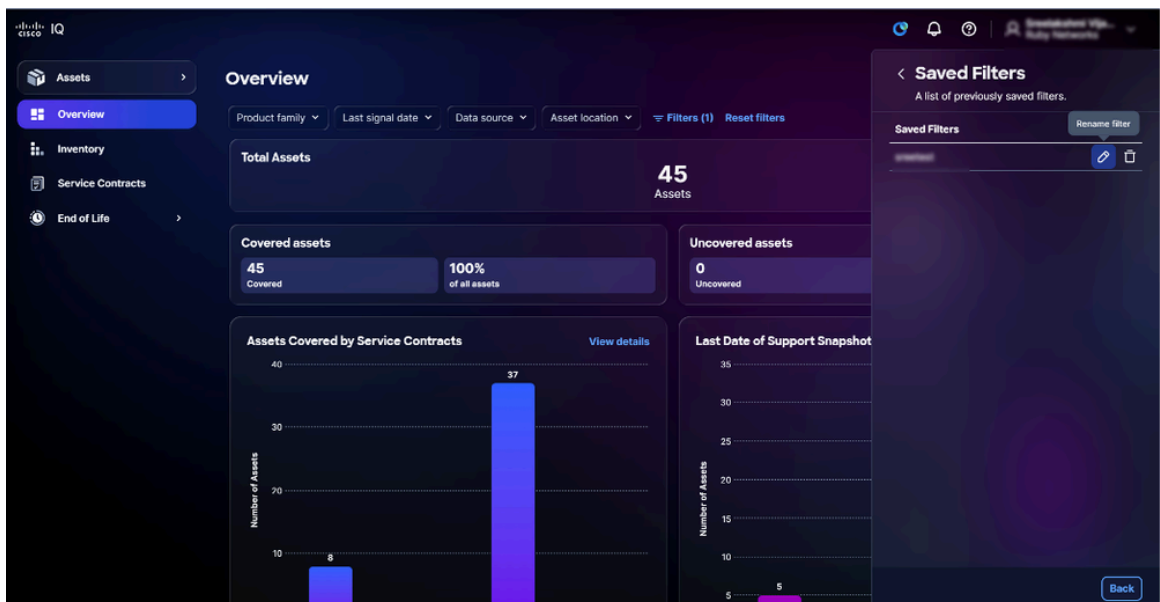
So bearbeiten Sie einen benutzerdefinierten Filter:

1. Klicken Sie auf Filter.



Gespeicherte Filter verwalten

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



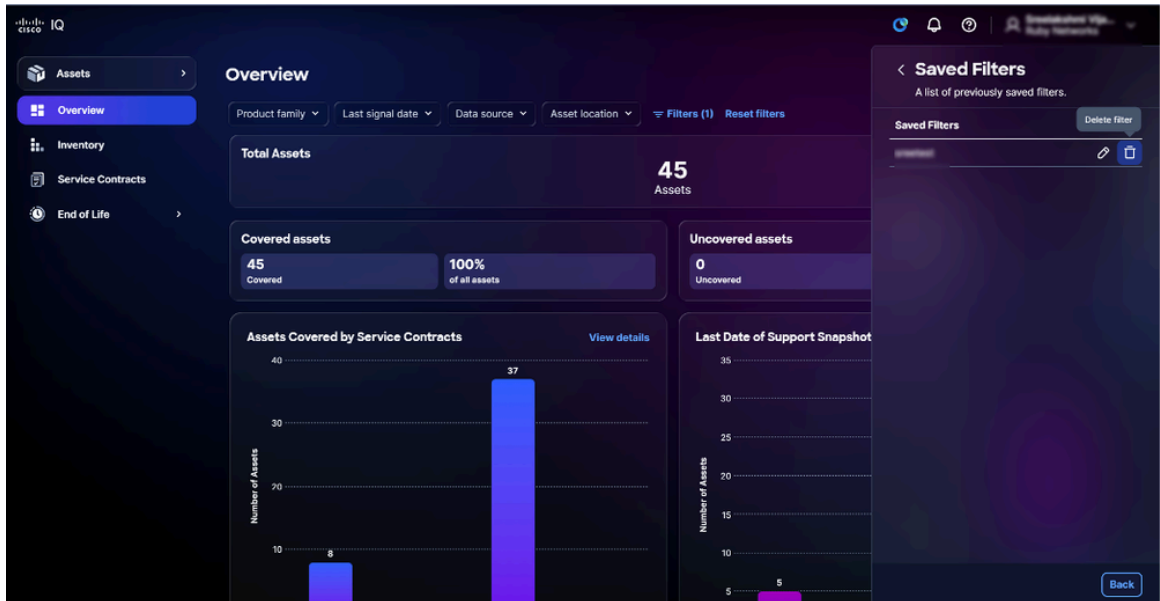
Filter bearbeiten

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.
5. Klicken Sie zur Bestätigung auf Ja, löschen.

AI-Assistent


Überblick

Der Cisco IQ AI Assistant wurde entwickelt, um das Verständnis und die Nutzung von Cisco IQ zu verbessern, indem Rohdaten in verwertbare Informationen, Empfehlungen und Aktionen umgewandelt werden. Die Lösung lässt sich in vorhandene Tools integrieren, die individuelle Datenquellen nutzen und Informationen aus mehreren Datenströmen synthetisieren, um Vorschläge in Echtzeit zu liefern. Der Cisco IQ AI Assistant bietet kontextbezogene Informationen, die es den Benutzern ermöglichen, proaktive, fundierte Entscheidungen zu treffen und Prozesse

zu optimieren, die das Kundenengagement und den Erfolg fördern. Auf diese Weise wird das Betriebsergebnis optimiert und die Benutzererfahrung mit Cisco IQ verbessert.

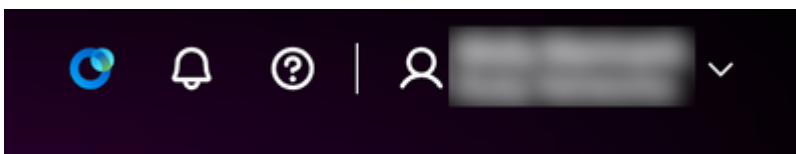
Zu den Funktionen des Cisco IQ AI Assistant gehören:

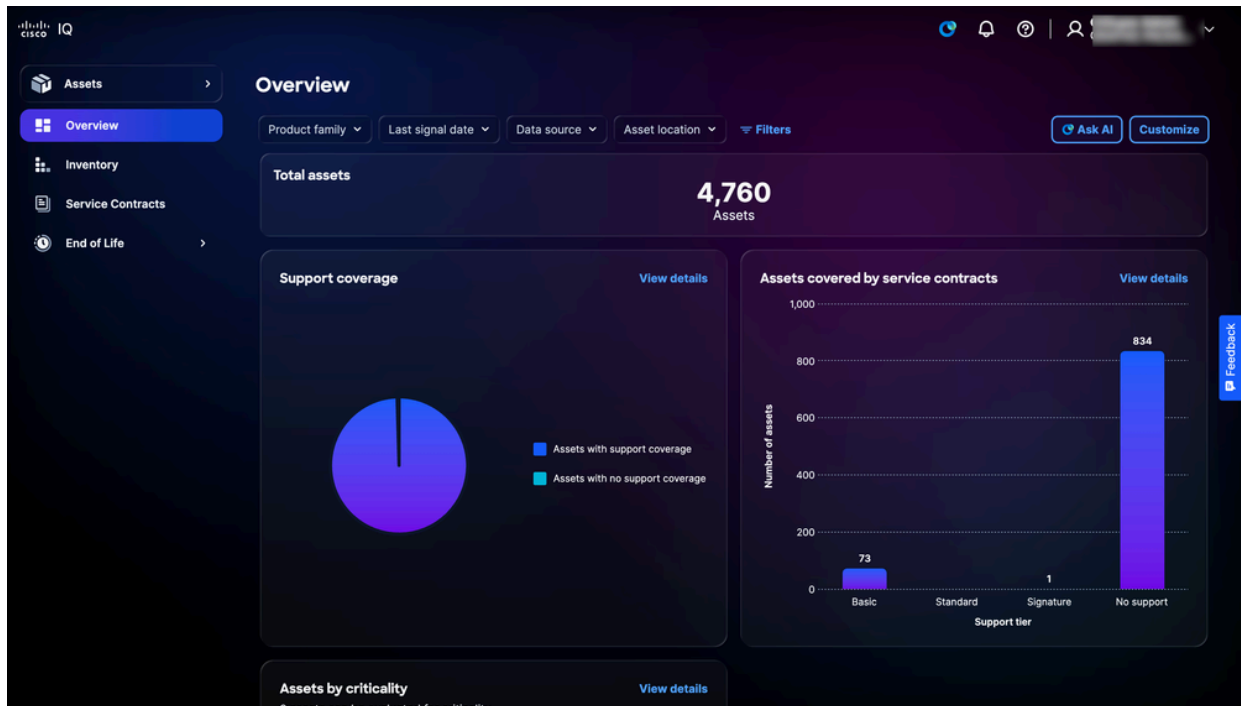
- Robuste Bearbeitung von Kantengehäusen: Transparente Erläuterungen und klare Umleitung sorgen für reibungslosen Support und eine höhere Benutzerzufriedenheit
- Streaming-Funktionen: Anzeigen der generierten Antworten
- Erweiterte Kontextdaten: Dynamischer Kontext ermöglicht nahtlose Interaktionen über Anwendungen, Seiten und Sitzungen hinweg
- Support zur Ticketverwaltung: Erstellen, Anzeigen und Verwalten von Tickets, die in der Ticket-Listenansicht angezeigt werden
- Bestandsverwaltung: Nachverfolgen, Verwalten und Erstellen von Berichten für die Ressourcen eines Unternehmens
- Ressourcenkritik: Priorisierung von Ressourcen für Maßnahmen zur Risikominimierung basierend auf ihrer Rolle und Bedeutung im Netzwerk
- Risikobewertung und Risikomanagement: Bewertung und Management potenzieller Risiken im Zusammenhang mit den Vermögenswerten einer Organisation
- Sicherheitssicherung: Vergleich der auf Kundengeräten ausgeführten Konfigurationen für unterstützte Geräte mit den entsprechenden Härtingsrichtlinien von Cisco und der Cybersecurity and Infrastructure Security Agency (CISA)
- Konfiguration: Auswerten der auf den Geräten des Kunden ausgeführten Konfigurationen anhand empfohlener Best Practices, Identifizieren von Konfigurationsabweichungen und Bereitstellen umsetzbarer Empfehlungen

 Anmerkung: Der Cisco IQ AI Assistant kann von jedem beliebigen Standort innerhalb von Cisco IQ gestartet werden. Sie ist für alle Benutzer verfügbar, die angebotenen Funktionen unterscheiden sich jedoch je nach Support-Stufe (Basic, Standard oder Signature).

Zugriff auf den Cisco IQ AI Assistant


So verwenden Sie den Cisco IQ AI Assistant:

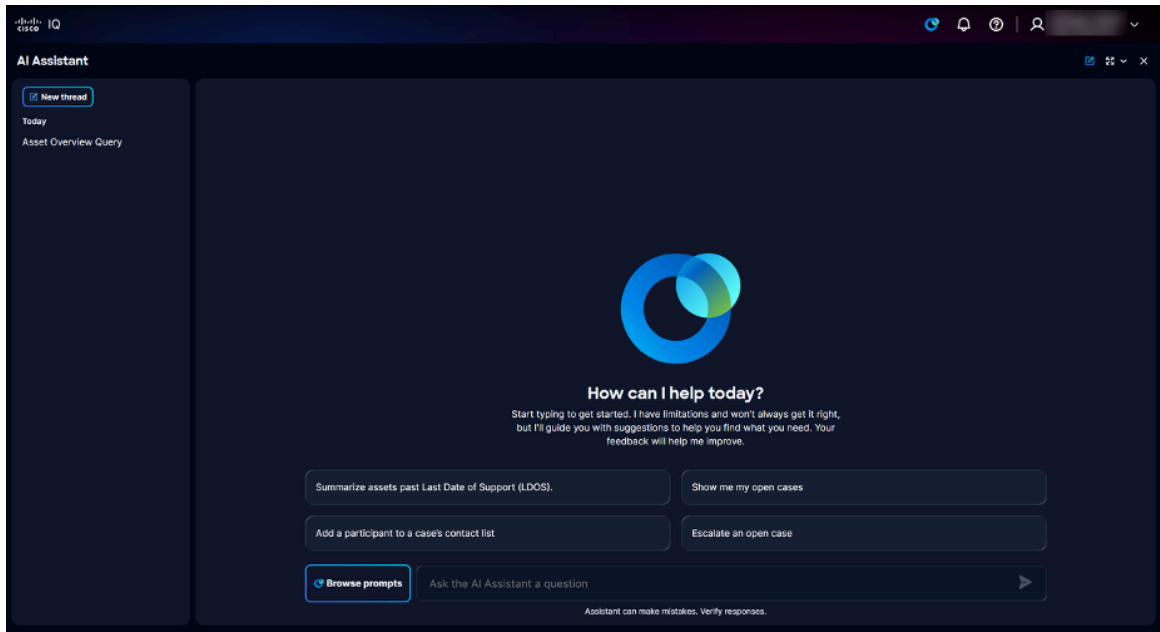





AI fragen

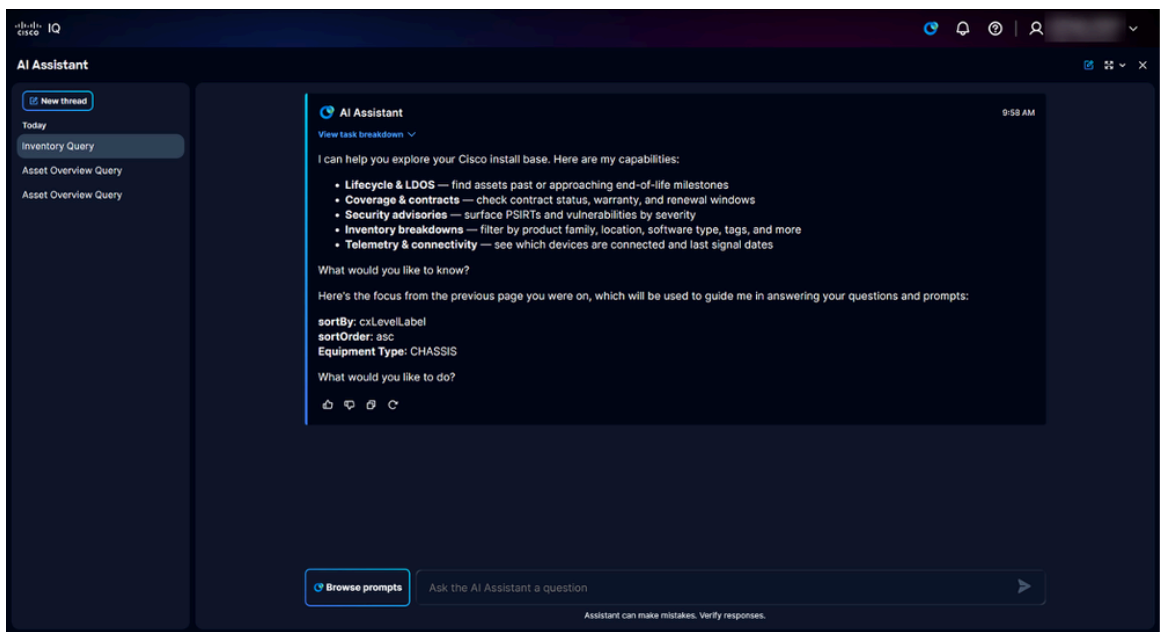
1. Starten Sie den Cisco IQ AI Assistant, indem Sie auf das Symbol AI Assistant klicken oder auf Ask AI (AI fragen) klicken.

 **Anmerkung:** Sie können den Cisco IQ AI Assistant innerhalb von Cisco IQ von einem beliebigen Ort aufrufen, indem Sie auf diese beiden Optionen klicken. Dabei werden die Daten und der Kontext der Seite genutzt, von der aus die Benutzer die Anwendung starten. So können aussagekräftige Informationen und Empfehlungen gegeben werden. Die Lösung kennt Ihre aktuelle Aufgabe und bietet personalisierte Anleitungen, Fehlerbehebungsschritte und eine höhere Effizienz.




Landing Page

 Anmerkung: Sie können eine neue Eingabeaufforderung eingeben oder die Bibliothek mit vordefinierten Eingabeaufforderungen durchsuchen.



Landing Page mit Anwendungskontext

 Anmerkung: Standardmäßig ist die Ansicht des Cisco IQ AI Assistant auf Vollbildmodus eingestellt. Wenn Sie eine neue Ansicht auswählen, behält der Cisco IQ AI Assistant die zuvor ausgewählte Ansicht bei.

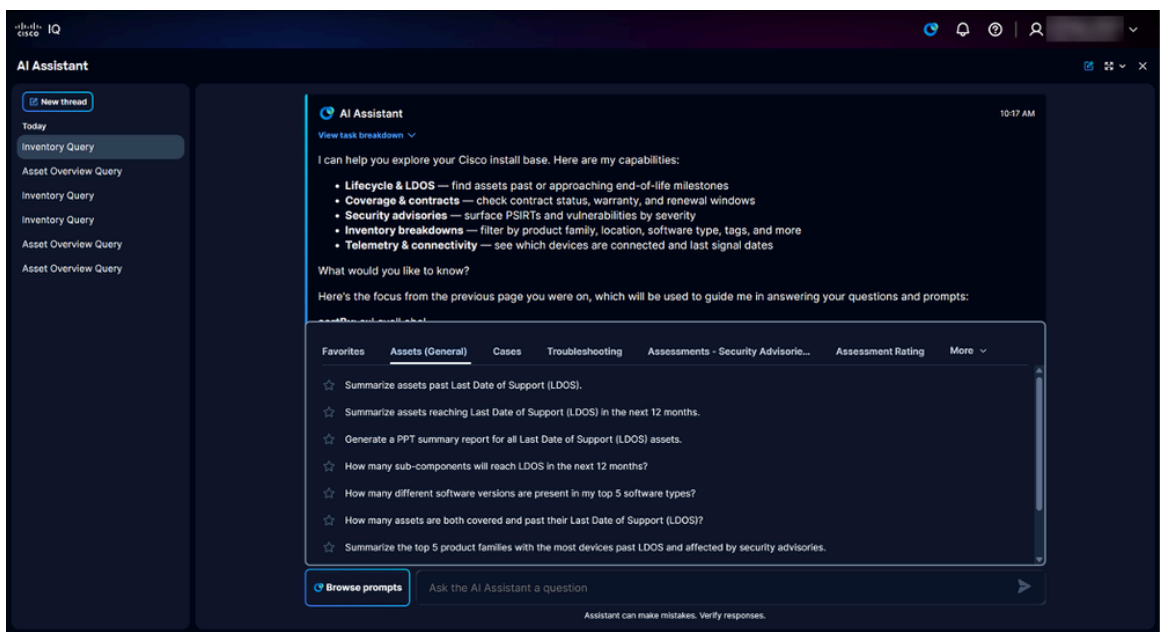
Der Cisco IQ AI Assistant zeigt die folgenden verfügbaren Optionen an:

- Vorherige Threads: Stellt 30 Tage Abfrageverlauf bereit

- Aufforderungen durchsuchen: Öffnet die Eingabeaufforderungsbibliothek. siehe [Anhang A: Der Cisco IQ AI Assistant zeigt](#) eine Liste aller in der Sprachbibliothek verfügbaren Fragen an.
- Stellen Sie dem KI-Assistenten ein Fragenfeld: Textfeld, um dem KI-Assistenten eine Frage zu stellen; verwenden Sie vollständige, beschreibende Sätze, um bessere Antworten zu erhalten.

2. Wählen Sie eine Eingabeaufforderung mit einer der folgenden Methoden aus:

- Suchen Sie nach Eingabeaufforderungen, indem Sie ein (1) oder mehrere Schlüsselwörter in das Feld Ask the AI Assistant a question eingeben und auf die Eingabeaufforderung klicken.
- Geben Sie im Feld Ask the AI Assistant a question (Fragen an den AI Assistant) eine formlose Frage mit detaillierten und vollständigen Sätzen ein.



Bibliothek mit Eingabeaufforderungen

- Klicken Sie auf Aufforderungen durchsuchen, um die Aufforderungsbibliothek zu öffnen, und wählen Sie eine der folgenden Aufforderungskategorien aus:
 - Aktiva (allgemein): Fragen zum Lebenszyklus von Ressourcen, einschließlich LDOS und allgemeine Fragen zum Bestand
 - Cases: Aufforderung zur Unterstützung von Ticket-Verwaltungsaktionen wie Anzeigen, Aktualisieren, Eskalieren und Schließen von Tickets, um eine effiziente Nachverfolgung und Kontaktaufnahme mit dem Cisco Support-Techniker zu ermöglichen
 - Fehlerbehebung: Aufforderung zur Unterstützung bei Syslog-Fehlermeldungen oder Konfigurationsfragen

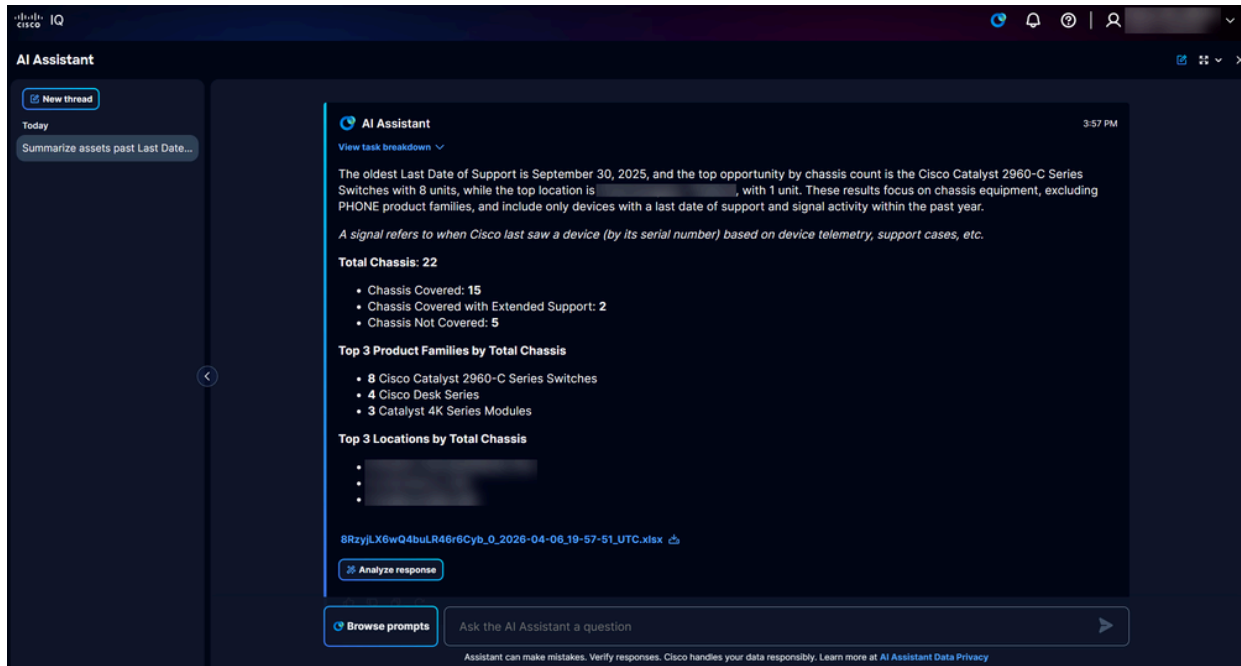
- Bewertungen - Sicherheitsempfehlungen: Eingabeaufforderungen zur Bewertung des allgemeinen Netzwerksicherheitsstatus, zur Identifizierung kritischer Schwachstellen und zur Auflistung spezifischer Ressourcen, die von schwerwiegenden Sicherheitsbedrohungen oder Konfigurationsschwächen betroffen sind
- Ressourcenkritik: Aufforderungen zur Priorisierung von Ressourcen für Aktivitäten zur Risikominimierung basierend auf ihrer Rolle und Bedeutung im Netzwerk
- Leistungsbeurteilungen - Konfiguration: Aufforderungen zur Zusammenfassung der Konfigurationsbewertungsergebnisse, Ermittlung von Konfigurationsabweichungen im Vergleich zu empfohlenen Best Practices und Erstellung umsetzbarer Empfehlungen
- Bewertungen - Sicherheit: Aufforderungen zur Identifizierung der empfohlenen Basiskonfigurationen für die Sicherheit, Best Practices für die Gerätesicherung und schrittweiser Verfahren zur Sicherung der Cisco Netzwerkinfrastruktur

3. Klicken Sie auf eine Aufforderung. Eine Antwort wird generiert.

Erweiterte Kontextdaten für den AI Assistant

Der Cisco IQ AI Assistant stellt sicher, dass der Kontext dynamisch ist und ermöglicht nahtlose Interaktionen zwischen Anwendungen, Seiten und Sitzungen. Dadurch wird sichergestellt, dass bei jeder Antwort kontextbezogene Daten verwendet werden, um die für Ihre Frage am relevantesten passenden Antworten bereitzustellen.

LDOS-Zusammenfassung und -Priorisierung



LDOS-Bericht

Die LDOS-Funktion für Zusammenfassung und Priorisierung ermöglicht die schnelle Identifizierung und Behebung von Risiken im Zusammenhang mit Netzwerkressourcen. Mit dieser Funktion werden Ressourcen nach ihren erwarteten Netzwerkrollen und ihrem Sicherheitsschwachstellenstatus klassifiziert, sodass Schwachstellen behoben und die Servicequalität insgesamt verbessert werden kann.

Wichtigste Vorteile

Wichtigste Vorteile der LDOS Summarization and Prioritization-Funktion:

- Priorisierte Risikoansicht
- Analyse der betrieblichen Auswirkungen
- Aussagekräftige Erkenntnisse

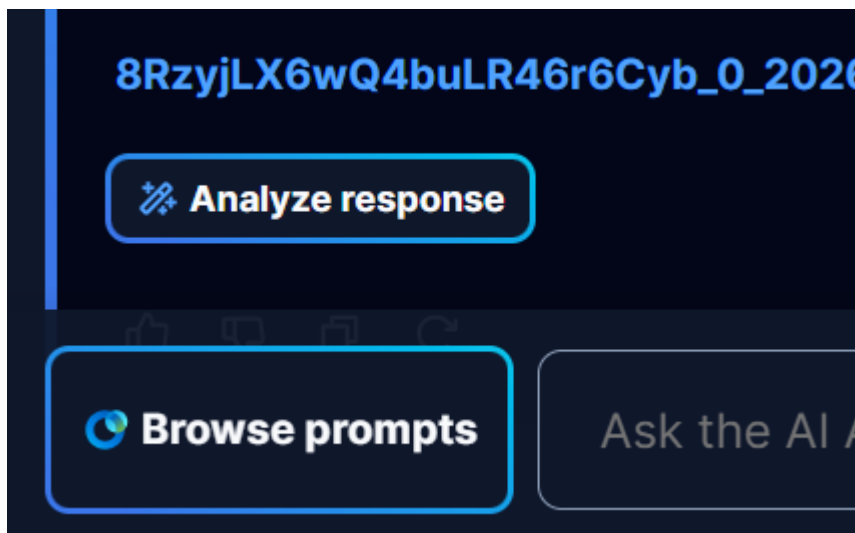
Als Teil dieser Funktion können Sie eine begrenzte Anzahl vordefinierter Fragen (gekennzeichnet durch "**") in der Benutzeroberfläche oder beim Anzeigen von LDOS-Erkenntnissen anzeigen.

Berichte

Erstellung von LDOS-Berichten

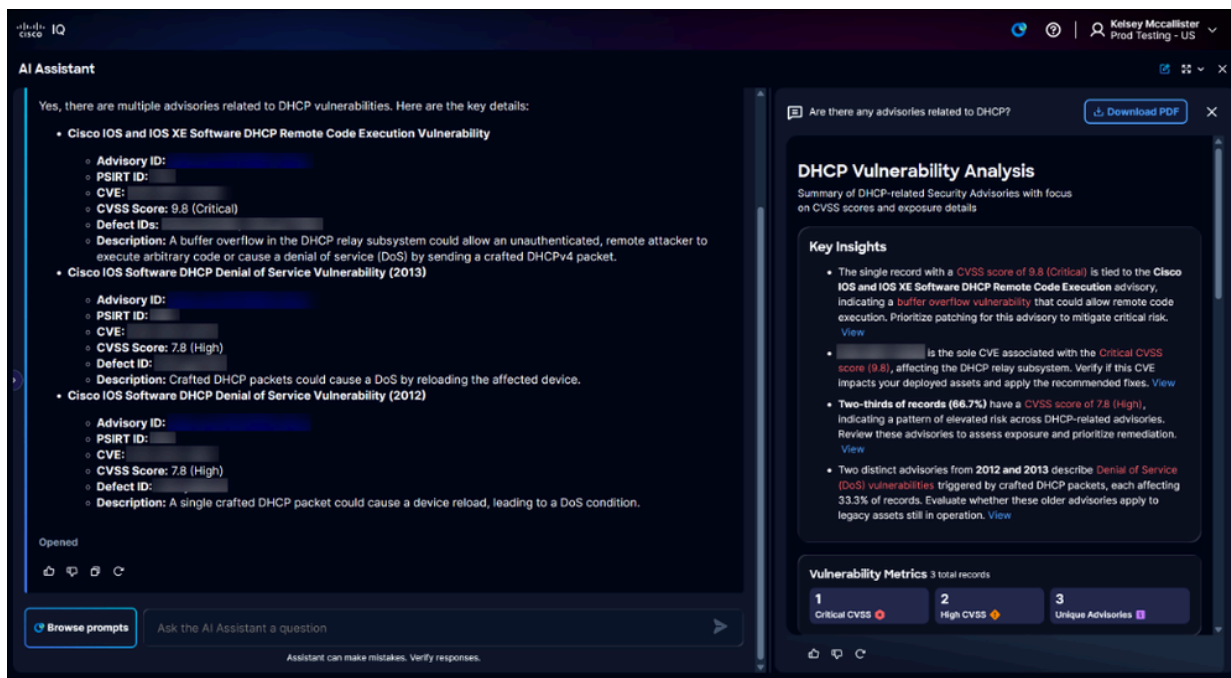
KI-generierte, kuratierte LDOS-Berichte bieten Zusammenfassungen der Ressourcen, die sich ihrem LDOS nähern oder dieses bereits überwunden haben. In den Berichten werden zudem Aktualisierungsoptionen hervorgehoben sowie Sicherheitsempfehlungen und Schwachstellen identifiziert, die Ihnen ein schnelles Verständnis der Risiken in Ihrem Netzwerk vermitteln.

Antwort analysieren



Antwort analysieren

Wenn Sie auf Antwort analysieren klicken, erhalten Sie eine KI-gestützte Zusammenfassung, die Daten zusammenfasst und verschiedene Visualisierungen wie Diagramme, Dashboards und Diagramme erzeugt, um aufschlussreiche Informationen bereitzustellen.



AI-Zusammenfassung

Die KI-gesteuerte Zusammenfassung enthält eine Schaltfläche PDF herunterladen, um den Bericht als PDF herunterzuladen.

Datenquellen für LDOS-Zusammenfassung und Berichterstellung

Die LDOS Summarization and Prioritization-Funktion nutzt die folgenden wichtigen Datenquellen:

- Basisressourcen und -verträge installieren
- Telemetrie-Ressourcen und -Verträge
- CX-Signaldaten
- EOL-Meilensteine für Hardware- und Software-Ressourcen

Fehlerbehebung mit dem Cisco IQ AI Assistant

Mit Cisco IQ können Sie Geräteprobleme unabhängig mit dem Cisco IQ AI Assistant beheben. Der intuitive, interaktive Assistent basiert auf zertifizierten Fehlerbehebungstools von Cisco und einer bewährten Wissensdatenbank und bietet kontextbezogene Echtzeit-Empfehlungen.

Es wurde für die tägliche Fehlerbehebung entwickelt und unterstützt Netzwerktechniker bei der Untersuchung von Cisco Produktproblemen, der Untersuchung von Symptomen und der Identifizierung der nächsten aussagekräftigen Schritte. Sie interpretiert technische Details wie Fehlermeldungen, Syslogs, Softwarefehler, Versionshinweise und konfigurationsbezogene Fragen. Indem Sie Herausforderungen sofort angehen, können Sie eine optimale Leistung erzielen und Zeit sparen, indem Sie Probleme lösen, ohne ein Support-Ticket öffnen zu müssen.

Best Practices

Wenn Sie den Cisco IQ AI Assistant zur Fehlerbehebung verwenden, befolgen Sie die folgenden Best Practices:

- möglichst genaue Angaben; die Plattform, die Produktfamilie und die Softwareversion in die erste Nachricht aufnehmen,

 Anmerkung: Wenn Sie den Cisco IQ AI Assistant von einer Ressource aus starten, liegen diese Informationen bereits vor.

- Fügen Sie den genauen Fehler-, Alarm- oder Syslog-Text ein, anstatt ihn zu paraphrasieren.

- Beschreiben Sie die Änderungen, die vor Beginn des Problems vorgenommen wurden, z. B. ein Upgrade, ein Konfigurations-Update oder eine Topologieänderung.
- Klare Weitergabe der Auswirkungen, z. B. ob sich das Problem auf ein (1) Gerät, einen (1) Standort oder mehrere Benutzer auswirkt


Cases

Die Funktion zur Verwaltung von Servicetickets ermöglicht es Benutzern, ihre Support-Tickets über Self-Service zu verwalten, wodurch sichergestellt wird, dass Geschäftsanwendungen und -services umgehend wiederhergestellt werden. Mit dieser Funktion können Sie Tickets effizient verwalten und das Support-Erlebnis optimieren. Weitere Informationen zur Vorgangsverwaltung finden Sie unter [Support-Anwendung](#).

Cases Management ermöglicht es Benutzern, Supportanfragen schnell und zentral anzuzeigen und zu verfolgen. So können Sie den Status von Tickets überprüfen, Updates überprüfen, den Fortschritt verfolgen und sich über die nächsten Schritte informieren. So können Sie Probleme einfacher beheben und schneller Support erhalten.

Anhang A: Cisco IQ AI Assistant-Eingabeaufforderungen

In diesem Anhang finden Sie eine detaillierte Übersicht über die verfügbaren Eingabeaufforderungen im Cisco IQ AI Assistant, die nach Fragenthemen in Listen sortiert sind.

 Anmerkung: Sie können verfügbare Eingabeaufforderungen durchsuchen, indem Sie relevante Vorschläge auswählen, da die Eingabeaufforderungsbibliothek die Optionen basierend auf Ihrer Eingabe einengt, oder Sie können Ihre eigene benutzerdefinierte Eingabeaufforderung senden. Der Cisco IQ AI Assistant verwendet Spracheingaben, enthält jedoch keine Eingabeformulare wie Dropdown-Menüs und sorgt so für eine nahtlose Benutzererfahrung.

Auf der Registerkarte "Assets" (Ressourcen) (Allgemein) sind die folgenden Aufforderungen verfügbar:

- Fassen Sie die Ressourcen nach dem Last Date of Support (LDOS) zusammen.
- Geben Sie einen Überblick über alle Ressourcen, die in den nächsten 12 Monaten das letzte Support-Datum erreicht haben.
- Erstellen Sie einen PPT-Übersichtsbericht für alle LDOS-Ressourcen (Last Date of Support).
- Wie viele Unterkomponenten werden in den nächsten 12 Monaten LDOS erreichen?
- Wie viele verschiedene Softwareversionen sind in meinen fünf häufigsten Softwaretypen

enthalten?

- Wie viele Ressourcen sind abgedeckt und haben das letzte Support-Datum überschritten?
- Geben Sie einen Überblick über die fünf Produktfamilien mit den meisten Geräten nach LDOS, die von Sicherheitsempfehlungen betroffen sind.
- Zusammenfassen von Karten und Modulen, die LDOS überschritten haben und von Sicherheitsempfehlungen betroffen sind
- Wie viele Unterkomponenten erreichen End-of-Life-Meilensteine vor dem übergeordneten Chassis?

Die folgenden Eingabeaufforderungen sind auf der Registerkarte Cases (Fälle) verfügbar:

- Meine offenen Tickets anzeigen
- Einen Fall zusammenfassen
- Status einer RMA anzeigen
- Status eines Fehlers anzeigen
- Update zu einem Ticket
- Neueste Aktualisierung und alle ausstehenden Aktionselemente für ein Ticket angeben
- Schließen eines offenen Tickets
- Hinzufügen eines Teilnehmers zur Kontaktliste eines Tickets
- Erstellen einer WebEx Space-Kommunikation zu einem Ticket
- Verbinden Sie mich mit dem Techniker, der das Ticket bearbeitet
- Erhöhen des Schweregrads eines offenen Tickets
- Eskalieren eines offenen Tickets
- Neuen Techniker für einen Fall anfordern
- Erneutes Einreihen eines offenen Tickets in eine Warteschlange
- Hinzufügen einer Notiz zu einem Ticket

Die folgenden Aufforderungen sind auf der Registerkarte Fehlerbehebung verfügbar:

- Wie kann ich Syslog-Fehler [Fehler] beheben und die Ursache ermitteln?
- Wie kann ich Konfigurationsprobleme beheben und die Ursache für [ABCD] ermitteln?
- Wie konfiguriere ich [XYZ] für die Produkt-ID [ABCD]?

Auf der Registerkarte "Assessments - Security Advisories" (Bewertungen - Sicherheitsempfehlungen) sind folgende Eingabeaufforderungen verfügbar:

- Gibt es Ratschläge in Bezug auf DHCP?
- Gibt es eine Sicherheitsempfehlung, um nach WebUI-Privilegien-Eskalationsschwachstellen im Zusammenhang mit dem Salz-Taifun zu suchen?
- Können Sie vor der Aktivierung von HTTP nach bekannten Sicherheitsempfehlungen oder

Schwachstellen im Zusammenhang mit der Aktivierung von HTTP suchen?

- Wie viele Sicherheitsankündigungen sind in meinem Netzwerk anfällig?
- Wie viele Geräte sind durch Sicherheitsempfehlungen gefährdet?

Auf der Registerkarte "Asset Criticality" (Anlagenkritik) sind die folgenden Aufforderungen verfügbar:

- Welche meiner wichtigsten Ressourcen sind nach Rolle und Bedeutung geordnet?
- Wie viele Core-Geräte sind von Sicherheitsempfehlungen betroffen?
- Zusammenfassung wichtiger und wichtiger Geräte, deren Abdeckung in den nächsten 12 Monaten abläuft
- Priorisieren Sie die LDOS-Ressourcen für eine Aktualisierung nach Rolle und Bedeutung.
- Priorisieren Sie nicht abgedeckte oder demnächst nicht abgedeckte Ressourcen für eine Verlängerung basierend auf Rolle und Bedeutung.
- Priorisieren Sie ablaufende Verträge für die Verlängerung basierend auf der Rolle und Bedeutung der abgedeckten Ressourcen.
- Priorisierung von PSIRT-Schwachstellen basierend auf Schweregrad, Rolle und Bedeutung der betroffenen Ressourcen

Auf der Registerkarte "Bewertungen - Konfiguration" sind folgende Eingabeaufforderungen verfügbar:

- Könnten Sie eine Zusammenfassung meiner aktuellen Konfigurationsbewertung zur Verfügung stellen?
- Wie viele Best Practice-Konfigurationsregeln wurden evaluiert, und wie viele führten dazu, dass mindestens eine Ressource nicht bestanden wurde?
- Was sind die häufigsten Konfigurationsabweichungen im Netzwerk?
- Welche Cisco Produktfamilien unterscheiden sich am meisten von den Best Practices für die Konfiguration?
- Wie viele Ressourcen wurden bewertet, und welcher Prozentsatz wurde nicht bestanden?
- Welche Kategorien unterscheiden am meisten von den Best Practices für die Konfiguration?
- Welche Konfigurationsabweichungen stellen das höchste Risiko für mein Netzwerk dar, und welche Korrekturmaßnahmen werden empfohlen?
- Für welche Ressourcen sind die größten Konfigurationsabweichungen mit kritischem und hohem Schweregrad vorhanden? Welche Korrekturmaßnahmen werden empfohlen?
- Aufschlüsselung der kritischen und schwerwiegenden Konfigurationsabweichungen nach Anlagenkritik
- Aufschlüsselung der Abweichungen von Best Practice-Konfigurationsregeln nach Schweregrad, Kategorie und Softwaretyp

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?

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.