

Guía de operaciones del dispositivo virtual Cisco IQ v1.2.0

Introducción

Cisco IQTM le ofrece mejoras y funciones diseñadas para mejorar la visibilidad de los recursos, ofrecer una perspectiva más inteligente de sus entornos y simplificar la gestión de casos. Además, las funciones de inteligencia artificial, como Cisco IQ AI Assistant, optimizan los resultados operativos y la experiencia del usuario de Cisco IQ al proporcionar una comprensión contextual que le permite tomar decisiones proactivas e informadas y agilizar los procesos para lograr el compromiso y el éxito del cliente.

Cisco IQ On-Prem Air-Gapped es uno de los modos de implementación de Cisco IQ, diseñado para clientes de sectores altamente regulados con estrictos requisitos de cumplimiento, propiedad de datos y seguridad. En este modo, Cisco IQ se proporciona como una máquina virtual (VM) independiente denominada dispositivo virtual (VA) de Cisco IQ. El VA se ejecuta completamente en las instalaciones del cliente y funciona de forma totalmente aislada de las redes externas. Para mantener este aislamiento, las actualizaciones de software y los paquetes de mantenimiento se obtienen de Cisco IQ SaaS y se transfieren al VA mediante un proceso aprobado y manual.

Cisco IQ On-Prem Air-Gapped amplía las capacidades clave de Cisco IQ SaaS a entornos con espacios aislados, lo que permite a los equipos críticos funcionar con una velocidad e inteligencia de diagnóstico comparables a las empresas conectadas en la nube.

Para acceder al dispositivo virtual de Cisco IQ, abra un explorador compatible y navegue hasta <https://<fqdn-of-the-appliance>>. Inicie sesión con el nombre de usuario y la contraseña de administrador establecidos durante el proceso de instalación.

 Nota: El VA de Cisco IQ se limita actualmente a los clientes inscritos en el programa de disponibilidad controlada. El acceso a las descargas del software del sistema de VA y los paquetes operativos adicionales (módulos, reglas y derechos) desde el portal Cisco IQ está disponible exclusivamente para determinados clientes. Póngase en contacto con su representante de cuentas para obtener más información.

Administración de conexiones (recopilación de datos)

Cisco IQ VA es una solución in situ para la recopilación de datos de red con el fin de proporcionar

una visibilidad detallada de su infraestructura. Recopila datos mediante Catalyst Center y Direct Connection. Simplifica la forma de gestionar la autenticación de red y la detección de dispositivos. La configuración de la recolección de datos consiste en:

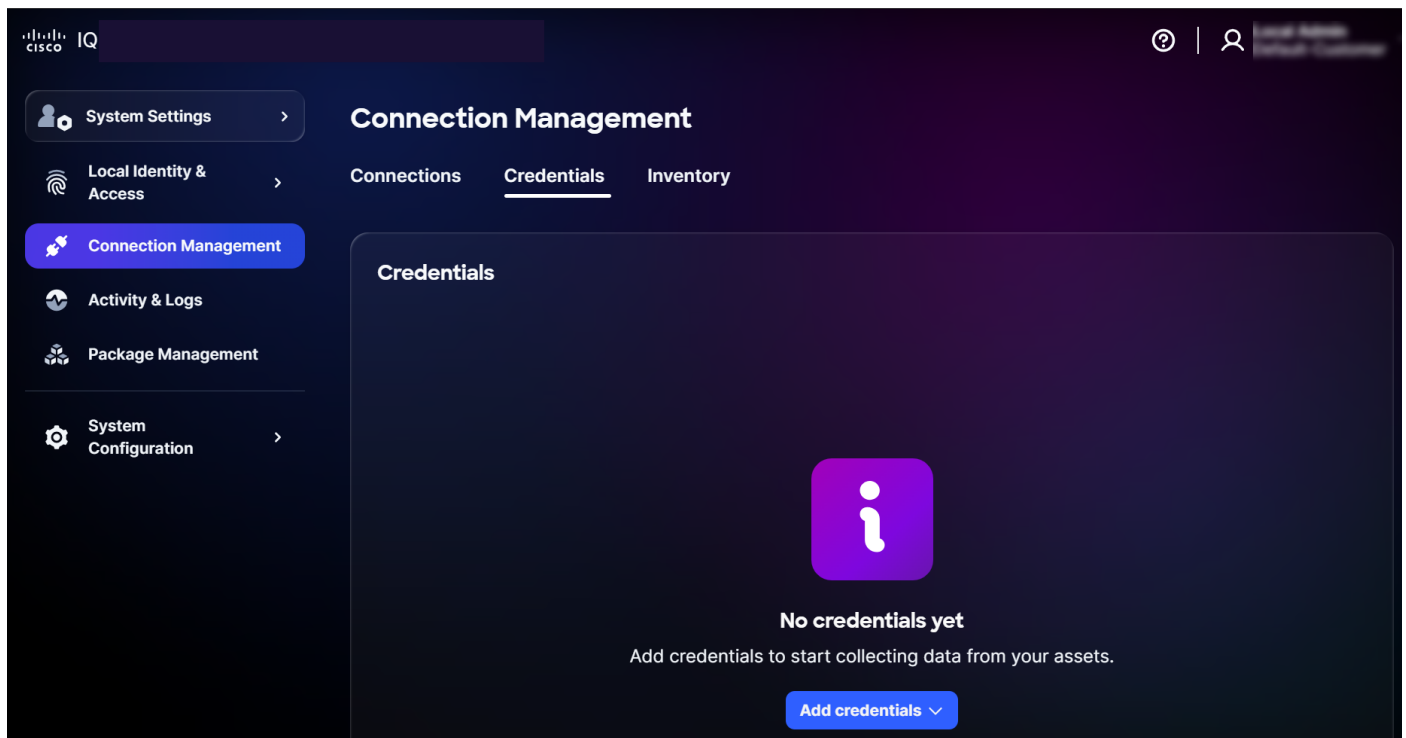
- Creación de conjuntos de credenciales: Establezca los protocolos de autenticación (por ejemplo, protocolo simple de administración de red (SNMP) v1/v2c/v3) para comunicarse con los dispositivos de red. La centralización de credenciales por zona o ubicación de seguridad (por ejemplo, "SanJose-SNMPv3") permite actualizar contraseñas en una ubicación, con los cambios que se propagan automáticamente a todos los dispositivos asociados.
- Asignación de credenciales al inventario: Asigne sus conjuntos de credenciales a los recursos de inventario para automatizar el proceso de autenticación. Al crear reglas que vinculan rangos de IP específicos a conjuntos de credenciales definidos, el sistema aplica automáticamente la autenticación correcta durante la recopilación de datos. Esto elimina los errores de entrada manual y garantiza que la configuración siga siendo precisa a medida que crece la red.

 Nota: Se requieren SNMPv2c/SNMPv3 y SSH para la detección de dispositivos y se deben proporcionar credenciales HTTP/HTTPS antes de configurar Catalyst Center.

Adición de credenciales

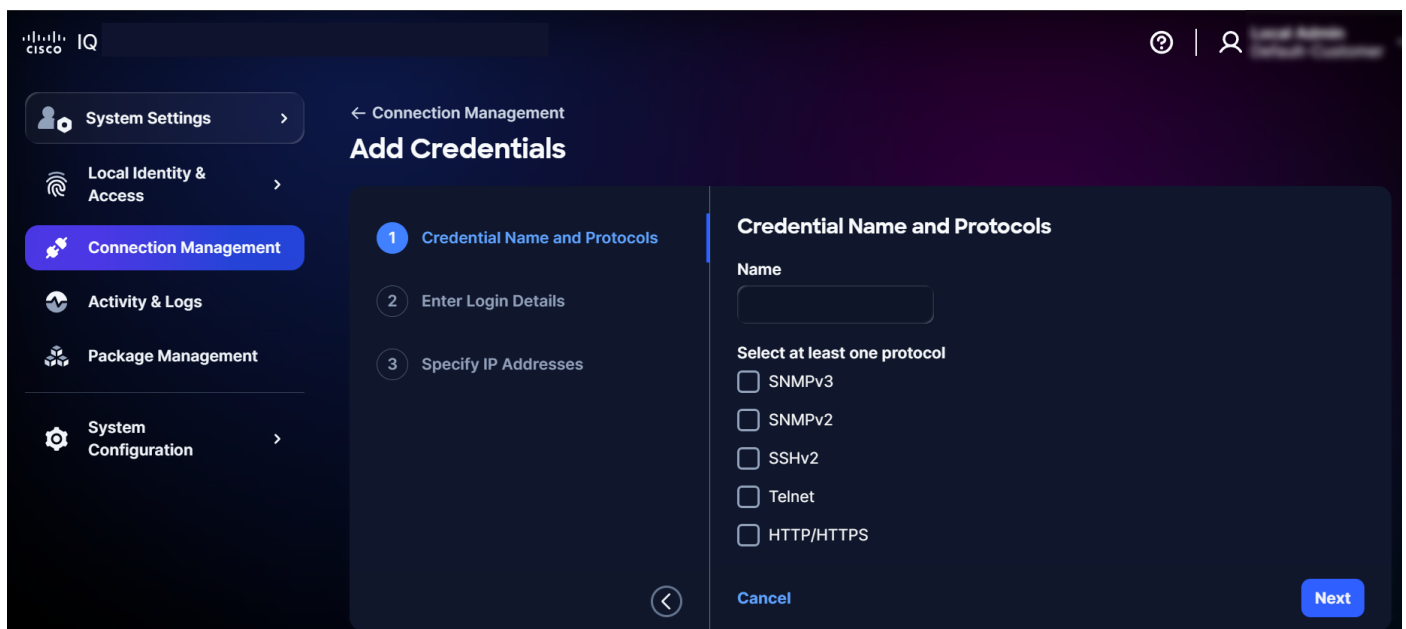
En primer lugar, debe agregar credenciales para realizar la recopilación de datos. Para agregar credenciales:

1. En Configuración del sistema, elija Administración de conexiones. Se muestra la página Connection Management.
2. Haga clic en la pestaña Credenciales.



Ficha Credenciales

3. Haga clic en Agregar credenciales.



Agregar credenciales

4. Introduzca un nombre.

5. Marque todas las casillas de verificación de protocolo aplicables.

6. Haga clic en Next (Siguiente).

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

Agregar detalles de credenciales



Nota: Para la imagen anterior, se ilustra la vista en la que se seleccionaron todos los protocolos en el paso anterior. La interfaz solo muestra los protocolos seleccionados.

7. Introduzca los detalles de inicio de sesión para cada protocolo seleccionado.

8. Haga clic en Next (Siguiente).

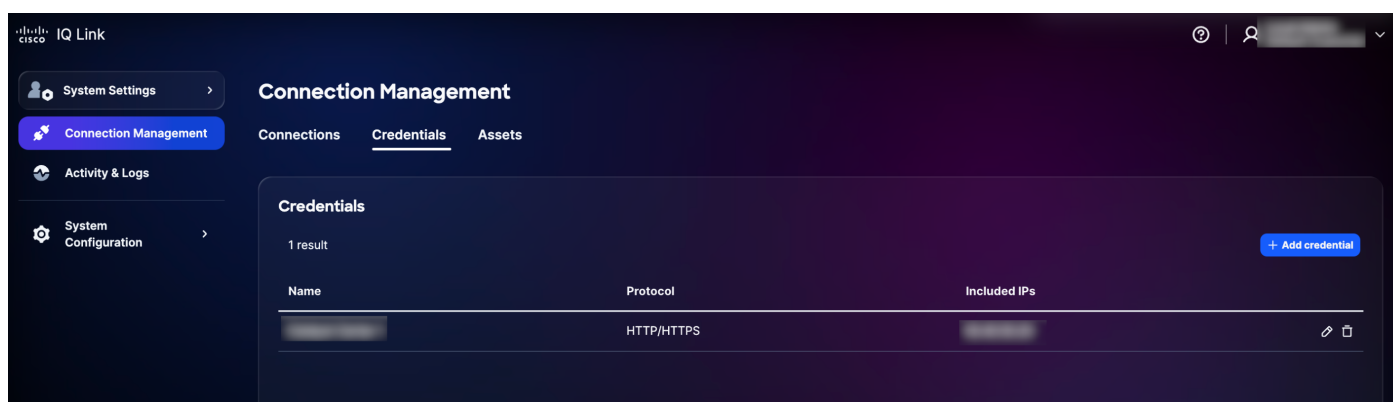
The screenshot shows the 'Add Credentials' wizard in the Cisco IQ Link interface. The left sidebar contains navigation links: System Settings, Connection Management (highlighted), Activity & Logs, System Configuration, and System Configuration. The main panel is titled 'Add Credentials' and has three steps: 1. Credential Name and Protocols, 2. Enter Login Details, and 3. Specify IP Addresses (current step). The 'Specify IP Addresses' step includes a text area for 'Included IPs' with a hint 'e.g. *-*-*, 192.168.1.0/24, 172.16.*.*'. At the bottom, there are 'Cancel', 'Back', 'Save and add another credential', and 'Save' buttons.

Especificar direcciones IP

9. Ingrese las IPs incluidas.

 Nota: Este campo define las direcciones IP o los intervalos IP en los que se pueden utilizar las credenciales para establecer una conexión. Admite una combinación de direcciones IP y máscaras IP (mediante la notación de caracteres comodín). Para obtener más información sobre los formatos compatibles, consulte [Selección de credenciales y lógica de coincidencia](#).

10. Click Save. Se muestra una confirmación y se le redirige a la pestaña Credenciales.



Credenciales agregadas

Puede editar las credenciales haciendo clic en el icono Edit y eliminarlas haciendo clic en el icono Delete.

Selección de credenciales y lógica de coincidencia

El motor de telemetría emplea una lógica de coincidencia basada en prioridades para determinar qué credenciales se deben aplicar durante la detección y la recopilación. La comprensión de esta jerarquía garantiza que se utilicen las credenciales correctas para los dispositivos deseados.

- Clasificación de prioridad: Cuando se aplican varios conjuntos de credenciales a un dispositivo, Cisco IQ los evalúa en función de la coincidencia específica con el dispositivo; el sistema aplica la prioridad siguiente, con mayor prioridad a las coincidencias más específicas:
 - Coincidencia de IP exacta: Prioridad más alta
 - Coincidencia de comodín final: la prioridad depende del número de estrellas finales;

menos estrellas indican una coincidencia más específica y, por lo tanto, una prioridad más alta

- Reglas de formato de comodines: Los comodines (*) sólo se admiten como caracteres finales en una dirección IP; deben aplicarse de derecha a izquierda.
 - Formatos admitidos:
 - 1.2.3.* (máxima prioridad)
 - 1.2.*
 - 1.*.*
 - *.*.* (prioridad más baja)
 - Formatos no admitidos:
 - Caracteres comodín iniciales (por ejemplo, *.1.2.3)
 - Caracteres comodín entre octetos (por ejemplo, 10.10.*.20)
 - Uso de guiones u otros delimitadores no estándar

Ejemplo de selección de credenciales:

En la tabla siguiente se muestra cómo el motor de telemetría selecciona el conjunto de credenciales más adecuado cuando un dispositivo coincide con varios patrones definidos.

Tabla 1: Ejemplo de Selección de Credenciales

IP del dispositivo	Conjuntos de credenciales disponibles	Conjunto de credenciales seleccionado
10.10.1.5	10.10.1.5, 10.10.1, 10.10..*	10.10.1.5 (Coincidencia exacta)
10.10.2.15	10.10.2, 10.10..*	10.10.2.* (Más específica)
10.10.5.50	10:10 ..., ...	10.10.2010. (Más específica)



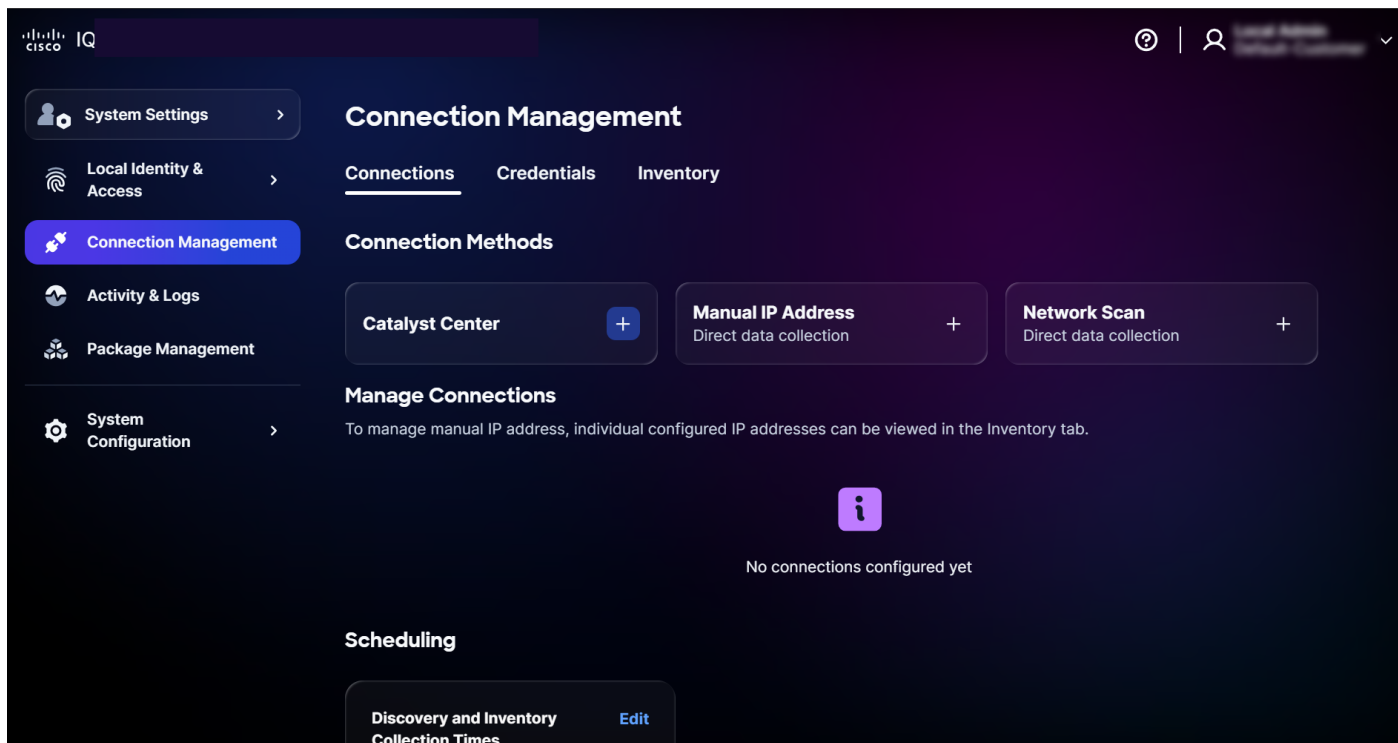
Nota: Si un dispositivo entra en varias categorías superpuestas, el sistema siempre selecciona el conjunto de credenciales con la especificidad más alta (es decir, el menor número de comodines finales).

Recopilación de datos mediante Catalyst Center

Puede conectar hasta 20 Catalyst Centers (no de clúster) para cada instancia de Cisco IQ VA.

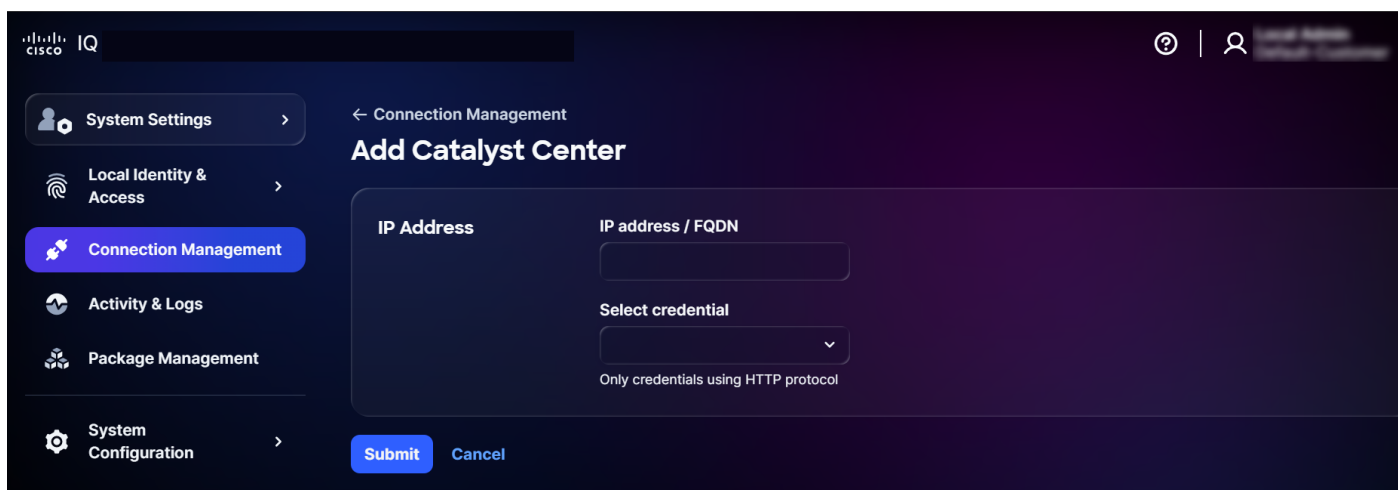
Para la recopilación de datos mediante Catalyst Center:

1. En Configuración del sistema, elija Administración de conexiones. Se muestra la página Connection Management.



Administración de conexiones

2. Haga clic en la opción Catalyst Center.



Agregar Catalyst Center

3. Introduzca la dirección IP o FQDN.
4. Elija una credencial HTTP/HTTPS configurada en la lista desplegable Select credential.
5. Haga clic en Submit (Enviar). Aparecerá una confirmación (puede tardar hasta 75 minutos). Puede ver el Catalyst Center recién agregado en Conexiones configuradas.

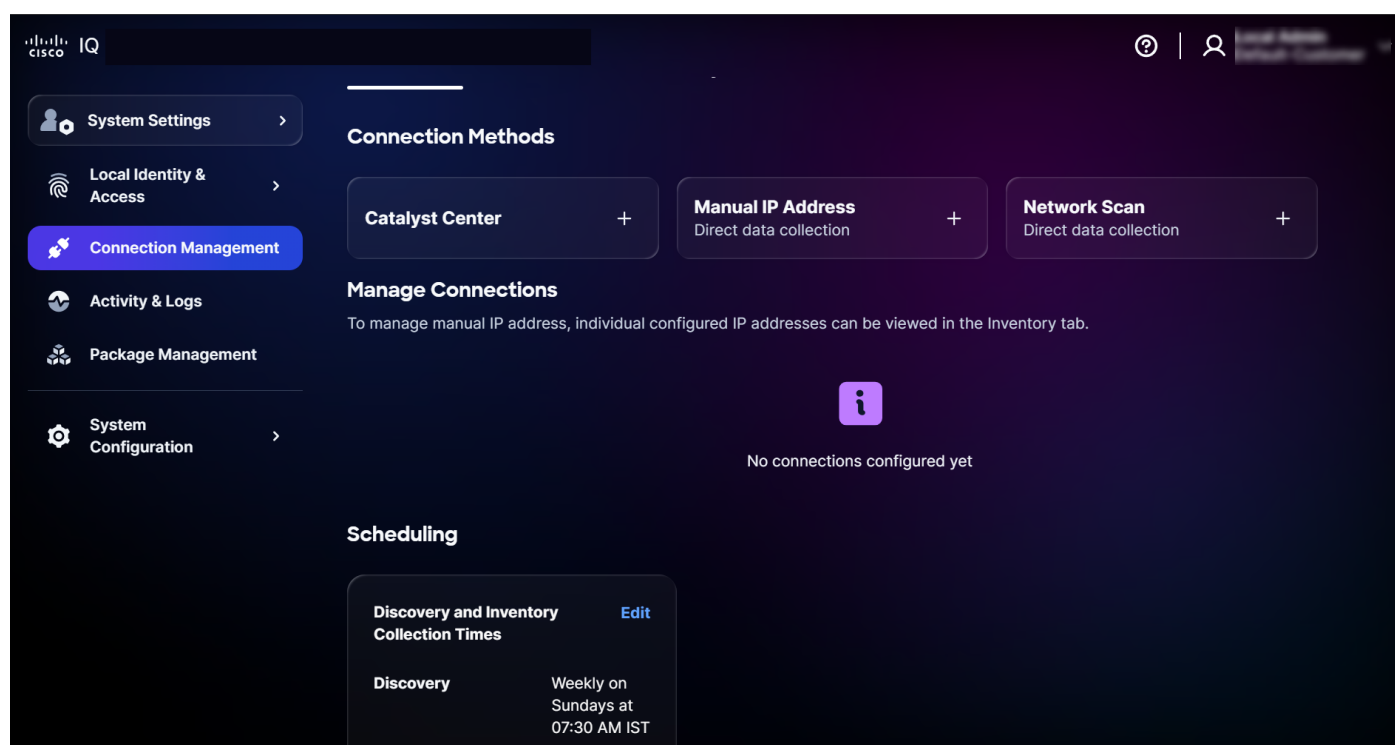
6. Programe una recopilación. Consulte [Programación](#) para obtener más detalles.

 Nota: Cisco IQ VA está preconfigurado con una configuración de programación automatizada y el sistema inicia una programación de recopilación automatizada predeterminada. Se recomienda encarecidamente que edite la programación para ajustarla a los requisitos y ventanas de mantenimiento de su organización.

Recopilación manual de datos

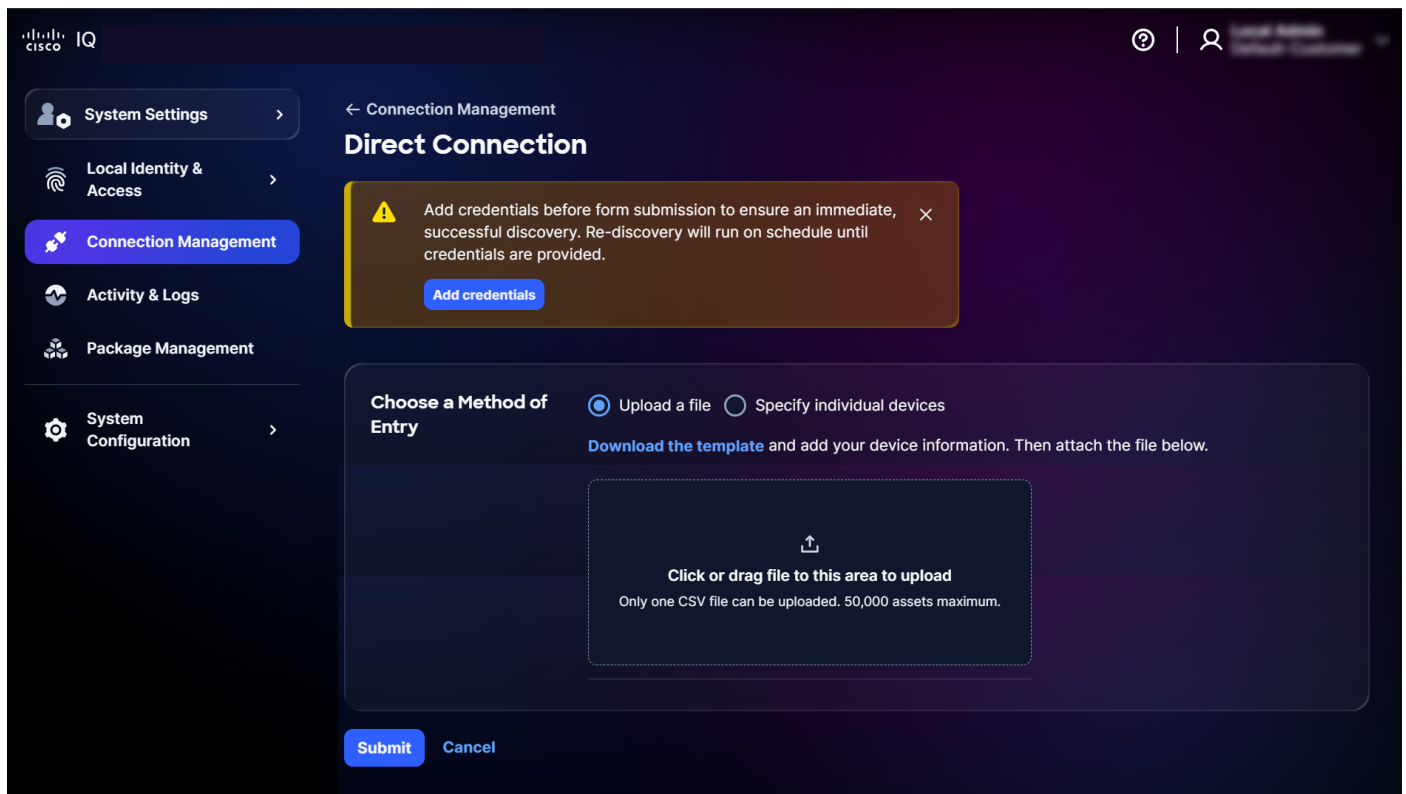
Para agregar dispositivos para la conexión directa de datos:

1. En Configuración del sistema, elija Administración de conexiones. Se muestra la página Connection Management.



Administración de conexiones

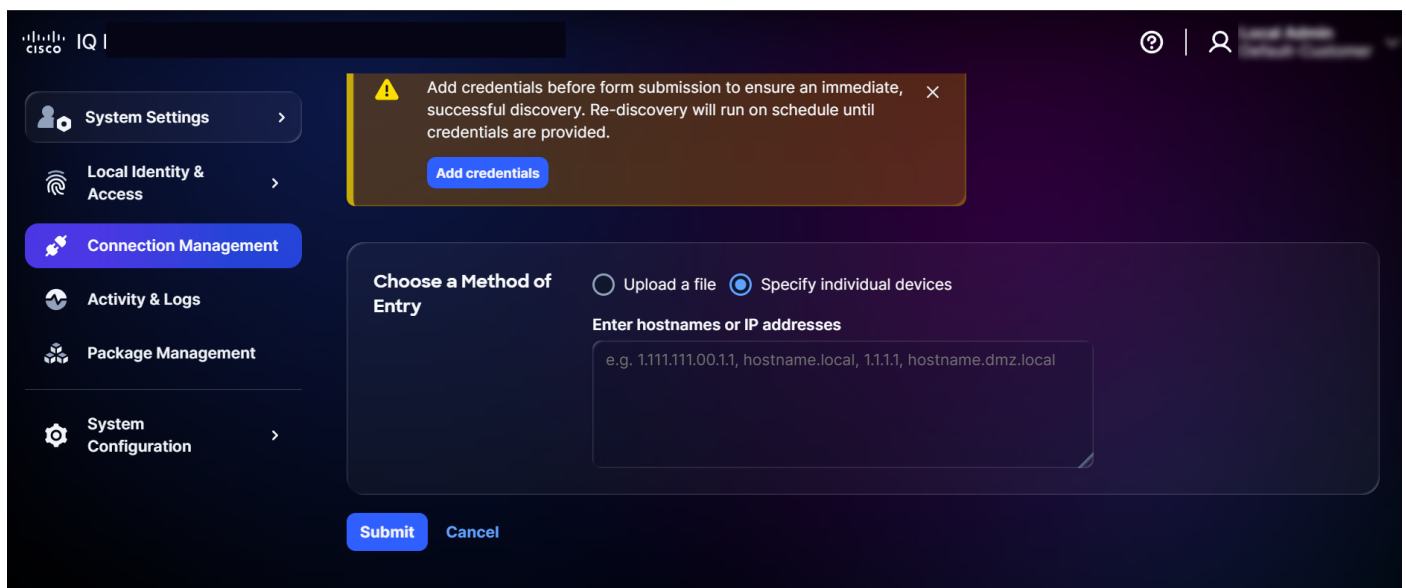
2. Haga clic en Manual IP Address. La página Conexión directa se muestra con dos (2) opciones para recopilar datos.



Cargar archivo

3. Haga clic en la opción preferida en Elegir un método de entrada y proporcione la información de su dispositivo mediante uno de los siguientes métodos:

- Cargar un archivo: Haga clic o arrastre y suelte el archivo



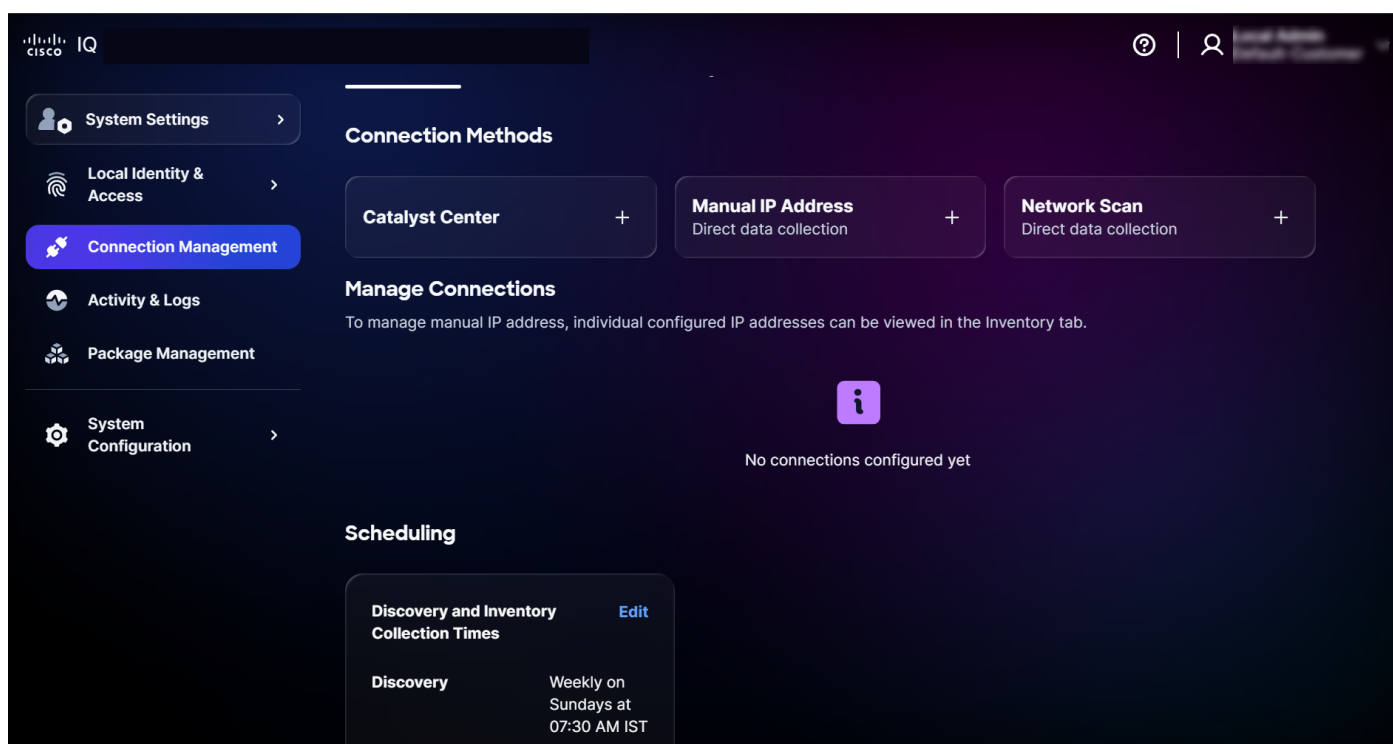
Especificar dispositivos individuales

- Especificar dispositivos individuales: Introduzca un único nombre de host, direcciones IP o una lista de nombres de host o direcciones IP separados por comas
4. Haga clic en Submit (Enviar). Se le redirigirá a la pestaña Activos tras el envío correcto.
 5. Programe una recopilación. Consulte [Programación](#) para obtener más detalles.

 Nota: Cisco IQ VA está preconfigurado con una configuración de programación automatizada y el sistema inicia una programación de recopilación automatizada predeterminada. Se recomienda encarecidamente que edite la programación para ajustarla a los requisitos y ventanas de mantenimiento de su organización.

Análisis de red

1. En Configuración del sistema, elija Administración de conexiones. Se muestra la página Connection Management.



Análisis de red

2. Haga clic en Network Scan. Se muestra la página Connect Assets by Network Scan con tres (3) opciones.

- Especificar intervalo IP: Defina un intervalo de direcciones IP para los dispositivos de destino dentro de ese intervalo para las tareas de detección o administración de redes
- Especificar protocolo de detección (CDP/LLDP): Elija el protocolo de detección de red que desea utilizar
- Carga de archivos: Cargar un archivo, como archivos de configuración o datos

3. Introduzca Nombre.

4. Introduzca Inicio IP y Fin IP.

5. En Análisis programado, seleccione Frecuencia y hora.

6. Haga clic en Conectar recursos.

Planificación

La programación le permite definir cuándo Cisco IQ VA realiza la recopilación de datos automatizada. Para programar la recopilación:

1. En la sección Programación de la página Administración de conexiones, haga clic en Editar para la programación que desea modificar. Se muestra la página Editar programación.

The screenshot shows the Cisco IQ 'Edit Schedule' page. The left sidebar has a navigation menu with 'Connection Management' selected. The main content area is titled 'Edit Schedule' and contains two sections: 'Schedule Discovery' and 'Schedule Inventory Collection'. Each section has a 'Frequency' dropdown, a 'Time' input field, and a 'Day' dropdown. The 'Schedule Discovery' section has 'Weekly' for frequency, '07:30' for time, and 'Sunday' for day. The 'Schedule Inventory Collection' section has 'Daily' for frequency, '05:30' for time, and a clock icon labeled 'IST' for day. At the bottom of the main area are 'Submit' and 'Cancel' buttons.

Editar programación

2. En la sección Programación de Detección, elija su Frecuencia y Día preferidos en las listas desplegables e ingrese la Hora de inicio deseada.
3. En la sección Recopilación de Inventario de Programación, elija su Frecuencia preferida en las listas desplegables e ingrese la Hora de inicio que desee.
4. Haga clic en Submit (Enviar).

 Nota: Espere de 5 a 10 minutos para que los cambios realizados en las programaciones de detección o recopilación se sincronicen y reflejen con precisión en el dispositivo virtual.

Instalación de paquetes (módulos, reglas y derechos)

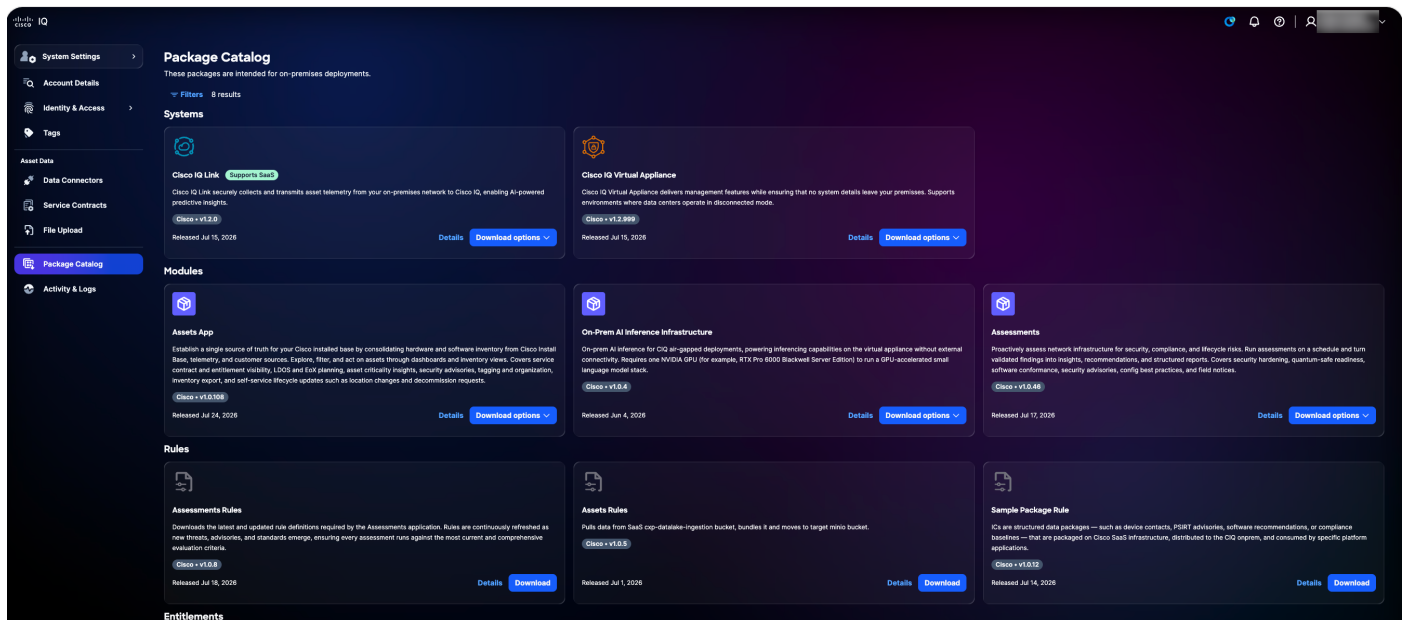
Puede gestionar el ciclo de vida del software (es decir, la instalación y la configuración) de los módulos operativos, las reglas, los derechos y las funciones especializadas alimentadas por IA del dispositivo virtual. Puede instalarlos descargando las versiones más recientes de Cisco IQ (SaaS) en el Catálogo de paquetes. El Catálogo de paquetes muestra las instancias de software disponibles. Le permite supervisar y gestionar las actualizaciones sin problemas, lo que garantiza un seguimiento y una gestión eficaces de las instancias del sistema.

Adición de módulos

Un módulo es un paquete de software independiente que proporciona la funcionalidad principal del dispositivo virtual. Se trata de un servicio independiente con su propio ciclo de vida, que permite la instalación, el mantenimiento y el cambio de tamaño. El consumo de recursos (incluida la CPU, la unidad de procesamiento de gráficos (GPU) y la RAM) se asigna dinámicamente en

función del tamaño de implementación (pequeño, mediano o grande) seleccionado durante la instalación inicial.

1. Inicie sesión en [Cisco IQ](#).
2. Vaya a System Settings > Package Catalog .

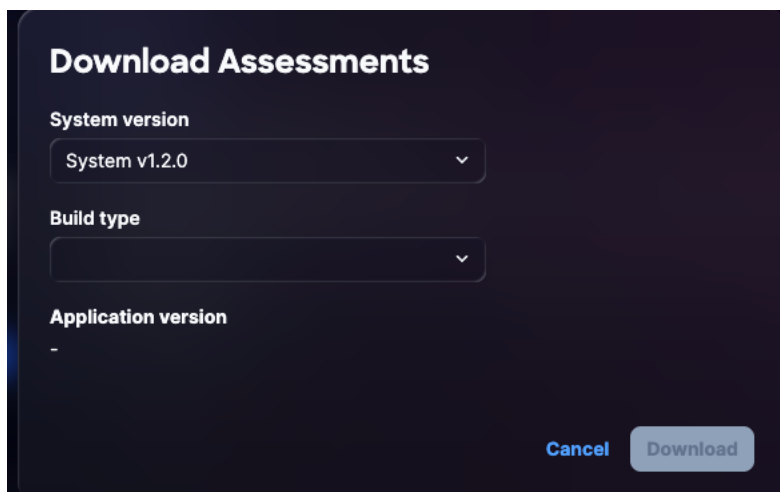


Catálogo de paquetes

3. Desde la tarjeta de módulo deseada, haga clic en Opciones de descarga > Paquetes de instalación. Se abre la ventana Download.



Nota: El módulo Assessment se utiliza para las imágenes de ejemplo.



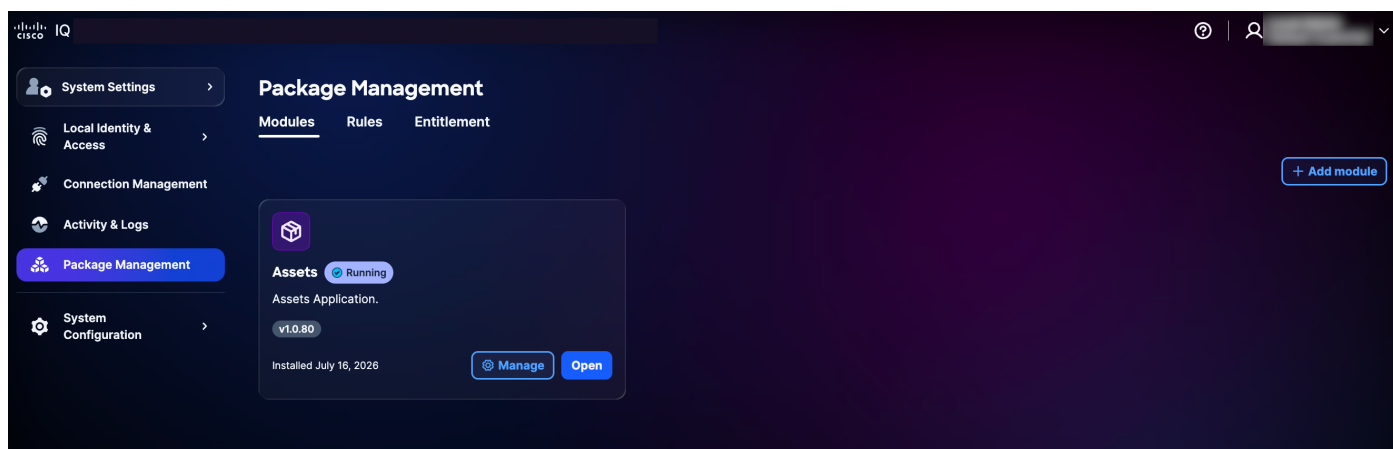
Descargar

4. Elija una versión del sistema en la lista desplegable.
5. Elija un tipo de generación en la lista desplegable.
6. Haga clic en Descargar para guardar el archivo localmente.



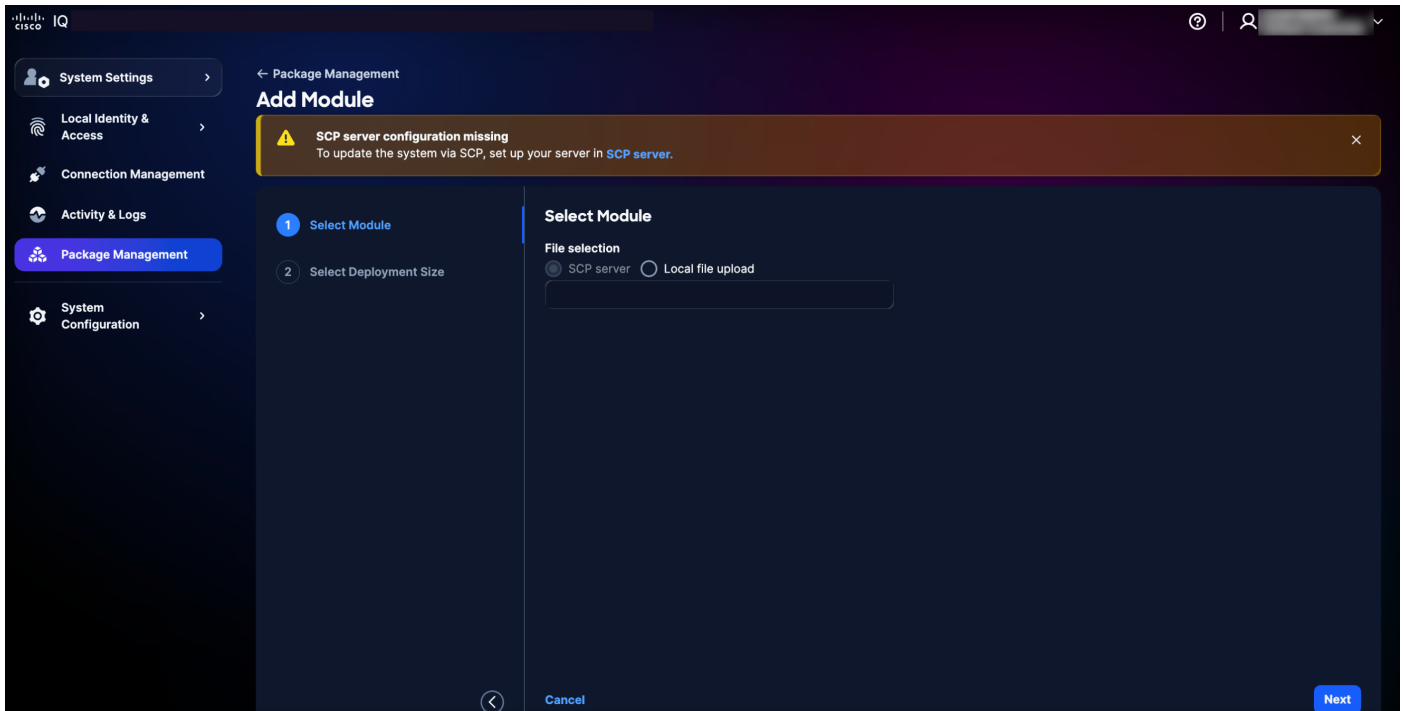
Nota: Los archivos de instalación son grandes (10-25 GB); asegúrese de que dispone de suficiente espacio en disco antes de realizar la descarga.

7. Vaya a VA.
8. Vaya a Inicio > Configuración del sistema > Administración de paquetes. Se muestra la página Administración de paquetes con las fichas siguientes:
 - Módulos
 - Reglas
 - Derechos



Módulos

9. Haga clic en Agregar módulo.

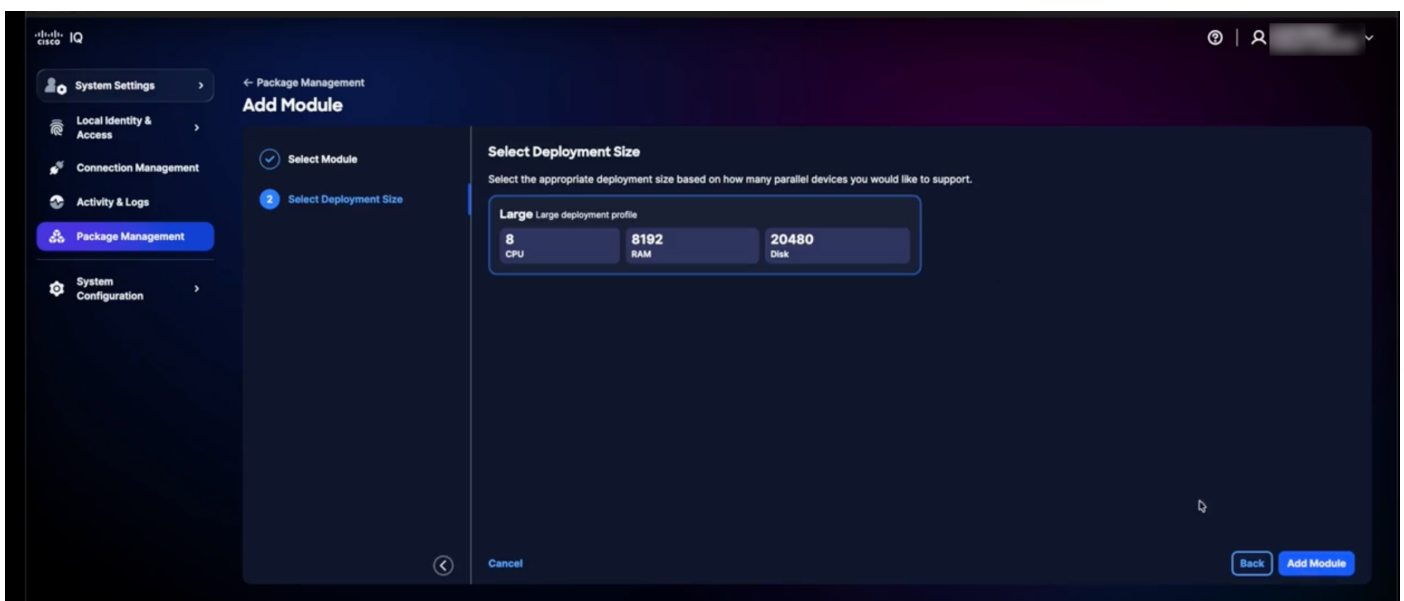


Agregar módulo

10. Elija la opción de selección de archivos que prefiera:

- Servidor SCP: Introduzca el nombre de archivo exacto del paquete de instalación (recomendado para archivos grandes)
- Carga de archivo local: Arrastre y suelte el archivo de instalación descargado (no se recomienda para archivos de 30 GB o más debido al tiempo de carga)

11. Haga clic en Next (Siguiente).

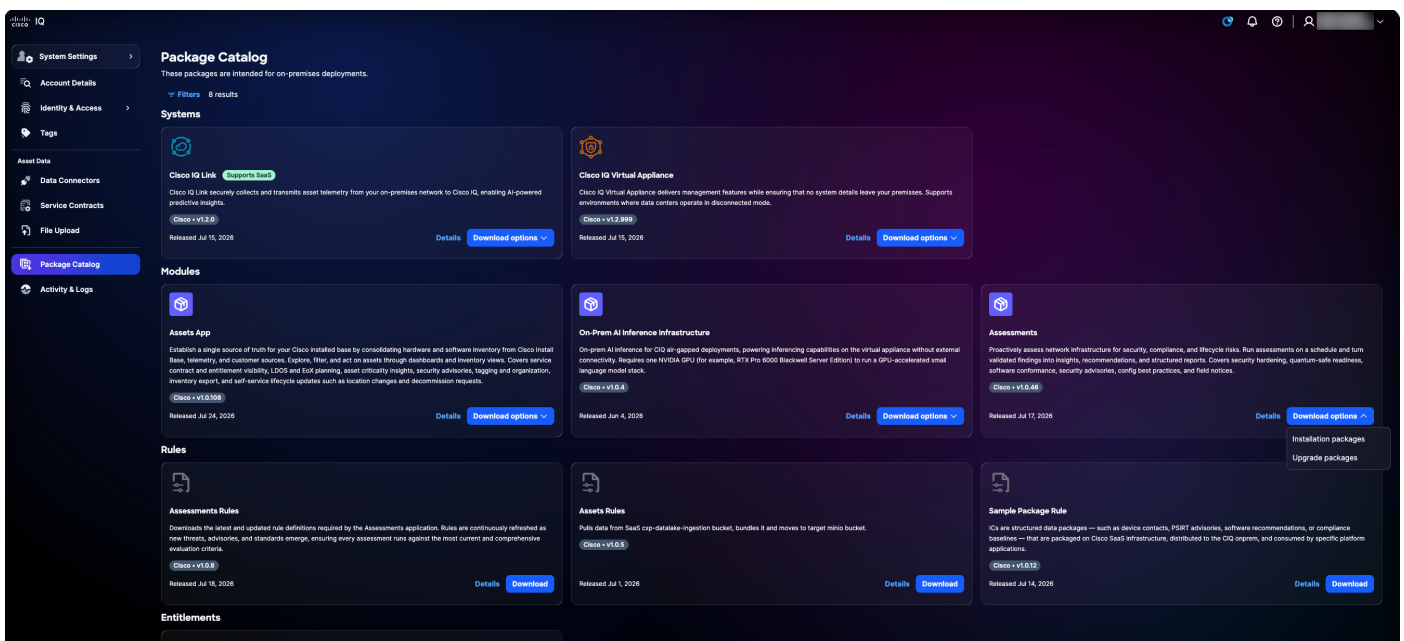


Tamaño de implementación

12. Elija el Tamaño de implementación (por ejemplo, Pequeño, Mediano o Grande). Estos tamaños están predefinidos y determinan los requisitos de recursos.
13. Haga clic en Agregar módulo. El módulo recién instalado se muestra en la pestaña Módulos en Administración de paquetes. Una vez finalizado, el estado del módulo cambia a "En ejecución" y el botón Abrir queda disponible.

Actualización de un módulo

Los últimos módulos se actualizan continuamente en Package Catalog (en Cisco IQ). Para actualizar a la última versión:



Conexión de recursos mediante análisis de red

1. Desde la tarjeta de módulo deseada, haga clic en Opciones de descarga > Paquetes de actualización. Se abre la ventana Download.



Nota: El módulo de evaluación se utiliza como ejemplo para las imágenes.

Upgrade Assessments

System version

System v1.2.0



Current app version



Build type



Application version

-

Cancel

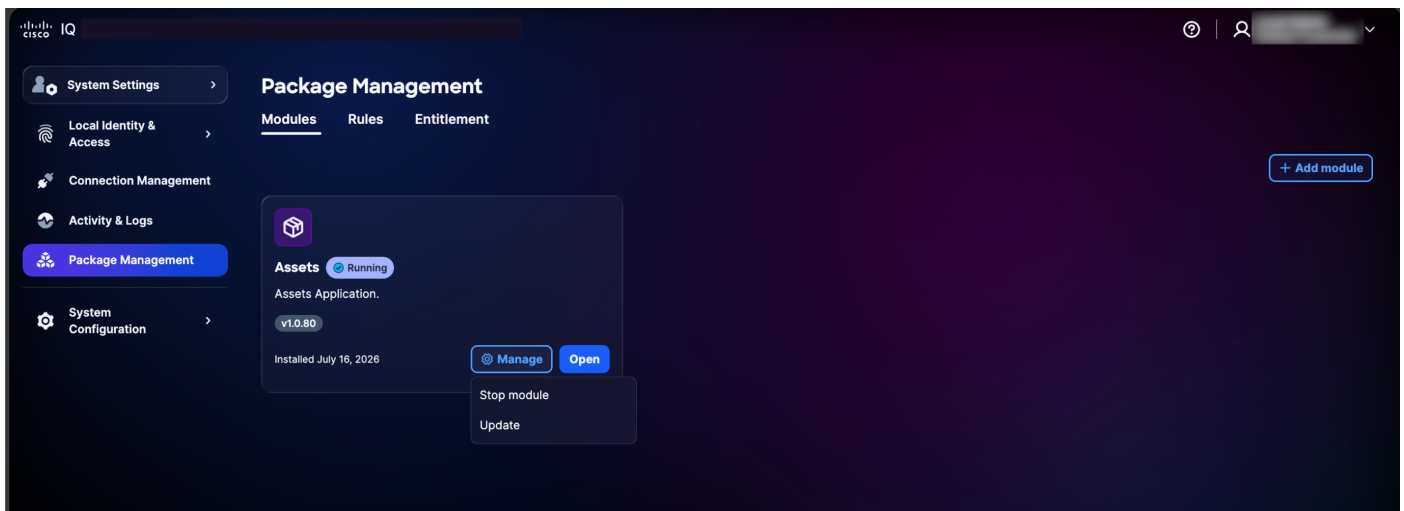
Download

Descargar

2. Elija una versión del sistema en la lista desplegable.
3. Elija una versión de la aplicación actual en la lista desplegable.
4. Elija un tipo de generación en la lista desplegable.
5. Haga clic en Descargar para guardar el archivo localmente.
6. Vaya a VA y complete la instalación del archivo descargado.

Administración de módulos

Después de agregar un módulo, puede modificarlo desde la página Administración de paquetes haciendo clic en Administrar. Las opciones de modificación disponibles incluyen cambiar el tamaño y actualizar a una versión superior. Para administrar un módulo:



Tipo de actualización

1. En la página Administración de paquetes, haga clic en Administrar > Actualizar para el módulo deseado.
2. Elija el tipo de actualización:
 - Cambiar sólo el tamaño de implementación
 - Actualizar versión
3. Si selecciona Cambiar tamaño de implementación, haga clic en Siguiente y elija el nuevo tamaño de implementación en la página siguiente.

O

Si se selecciona Update Version, se muestra la opción File selection. Elija SCP Server e ingrese el nombre de archivo exacto del paquete de instalación o elija Local file upload y arrastre y suelte el archivo de instalación descargado.

4. Haga clic en Next (Siguiente). Se muestra la página Seleccionar programación de actualización.
5. Elija una de las siguientes opciones de botones de opción para actualizar la programación:
 - Actualizar ahora
 - Actualizar más tarde



Nota: Algunos módulos admiten actualizaciones sin tiempo de inactividad. Si se requiere tiempo de inactividad, un banner muestra los detalles.

6. Si selecciona Update later, ingrese la Date y la Time.

7. Haga clic en Next (Siguiente). Se muestra Update Summary.

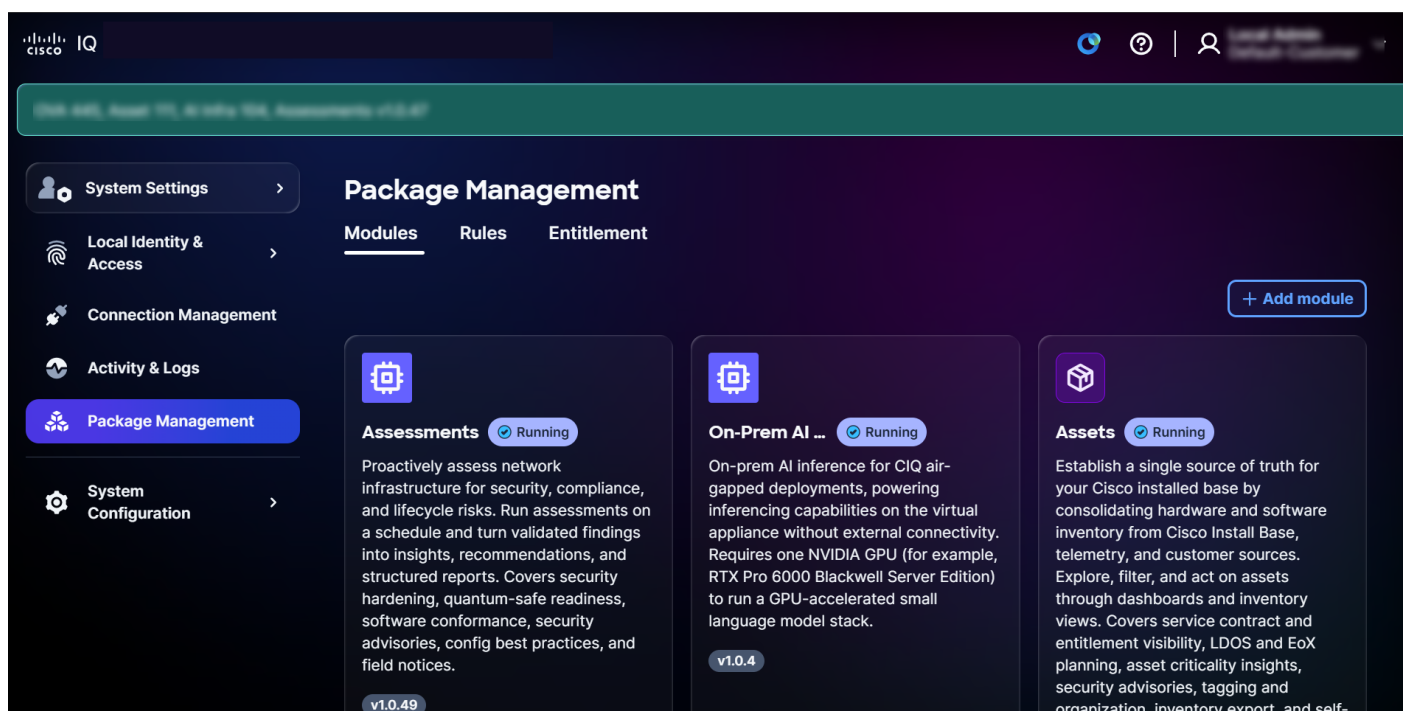


Nota: Puede acceder a Release Notes desde el Resumen de actualización.

8. Haga clic en Update Module y navegue hasta la pestaña Module. El módulo muestra un estado de "actualización programada".

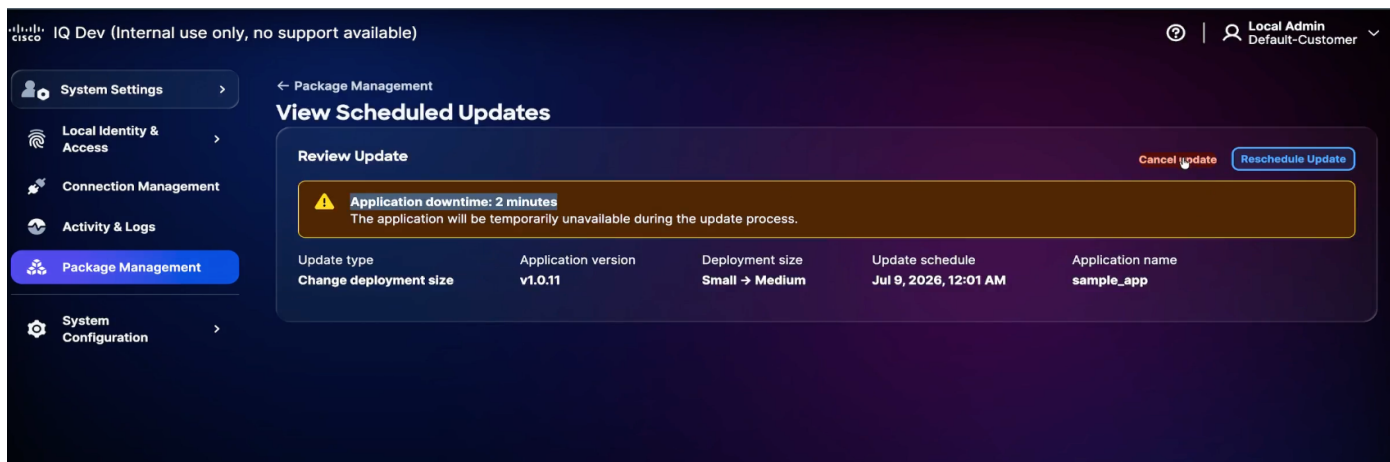
Edición de planificaciones

También puede ver, editar o cancelar las actualizaciones programadas. Para editar o cancelar una actualización programada:



Editar programación

1. En la página Administración de paquetes, haga clic en Administrar > Ver actualización programada del módulo deseado. Se muestra la ventana View Scheduled Updates.



Programar actualizaciones

- Haga clic en Cancelar actualización o Reprogramar actualización según sea necesario.
- Siga las instrucciones que aparecen en pantalla para completar las operaciones.



Nota: Si se produce un error en una operación de módulo (por ejemplo, la instalación, la actualización o el cambio de tamaño), elija una de las siguientes opciones:

Reintentar: La interfaz de usuario muestra un botón Reintentar, que le permite volver a intentar la operación. Registros: Si persiste un error, haga clic en Logs (Registros) para ver información de diagnóstico detallada. Éste es el método principal para identificar la causa de los errores de tiempo de ejecución o de instalación.

Instalación de reglas

Una regla es un componente especializado o "complemento" que amplía o modifica la funcionalidad de un módulo existente. Las reglas no están diseñadas para ejecutarse como programas independientes; se "conectan" a un módulo para proporcionar reglas, lógica o funciones específicas. Las reglas están vinculadas a módulos específicos. Cuando se instala una regla, se vincula al módulo que admite. Las reglas permiten que el sistema se actualice o se personalice sin que sea necesario actualizar completamente el módulo principal. Si se necesita un nuevo conjunto de reglas o funciones, simplemente puede agregar una nueva regla al módulo existente.

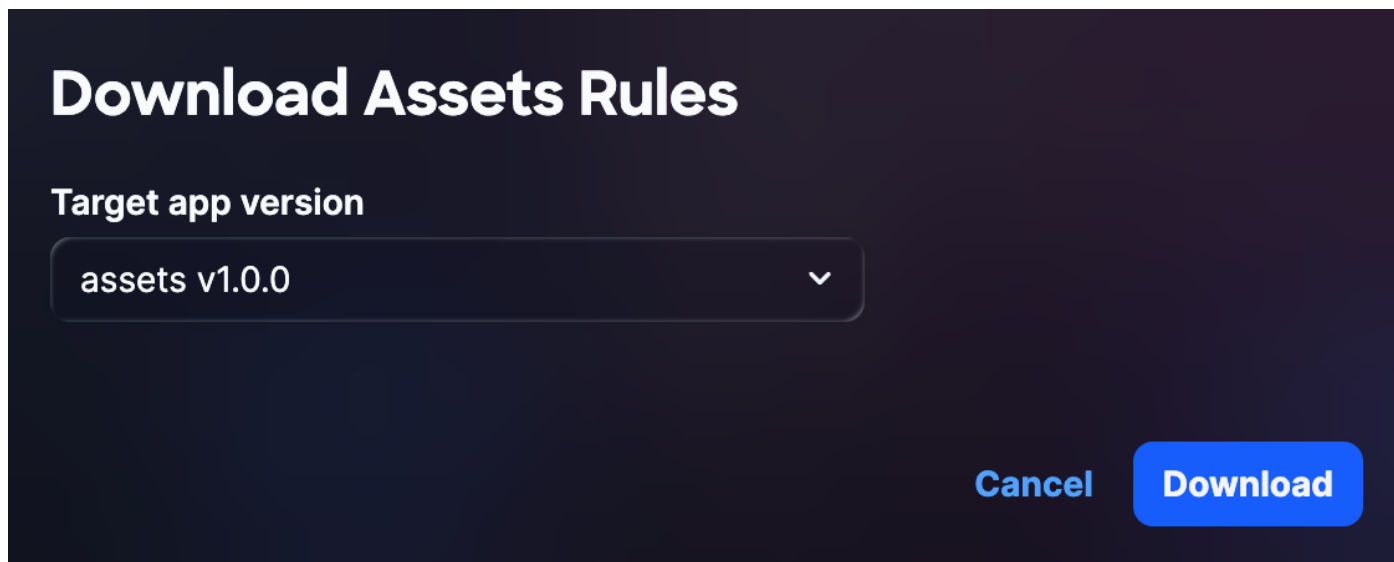
Para descargar una regla:

- Inicie sesión en [Cisco IQ](#).

2. Vaya a Configuración del sistema > Catálogo de paquetes.
3. En la tarjeta de reglas deseada, haga clic en Descargar.



Nota: La siguiente imagen de ejemplo corresponde a una regla Assets.



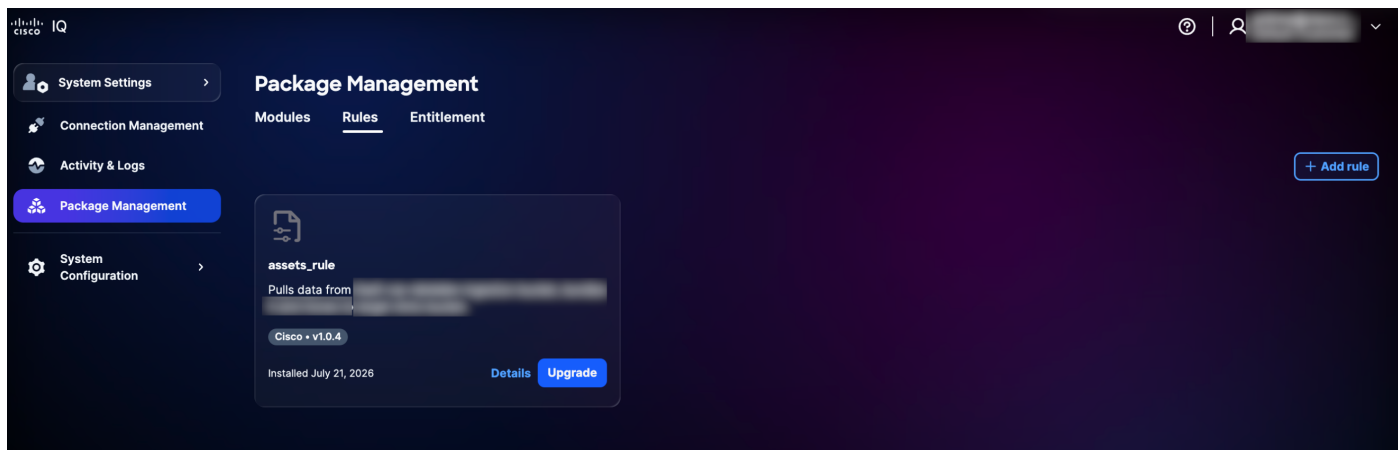
Descargar

4. Elija una versión de aplicación objetivo en la lista desplegable.
5. Haga clic en Descargar para guardar el archivo localmente.



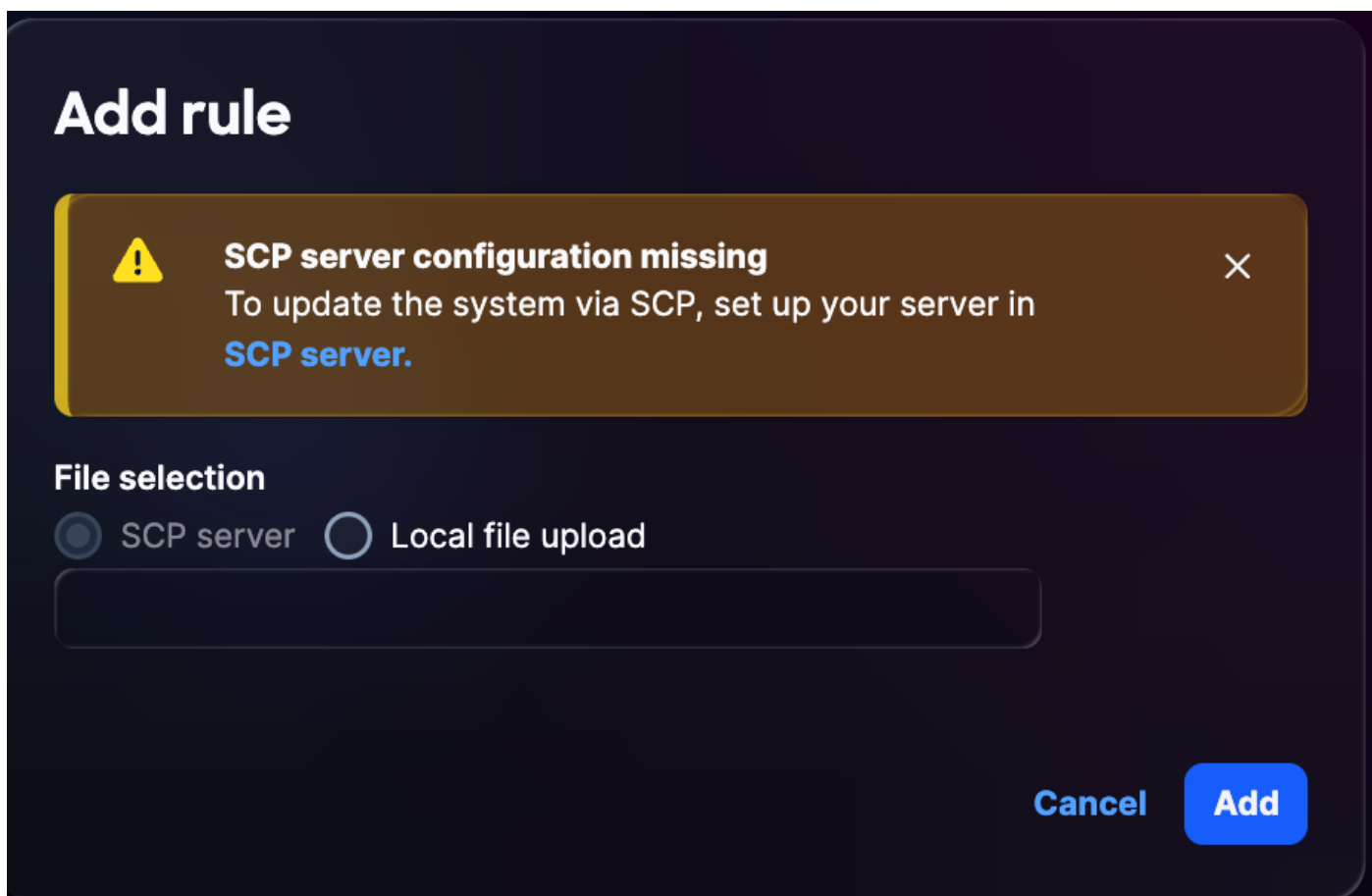
Nota: Los archivos de instalación son grandes (10-25 GB); asegúrese de que dispone de suficiente espacio en disco antes de realizar la descarga.

6. Vaya a VA.
7. Vaya a Inicio > Configuración del sistema > Administración de paquetes. Se muestra la página Administración de paquetes con las fichas siguientes.
 - Módulos
 - Reglas
 - Derechos
8. Haga clic en la pestaña Reglas.



Gestión de paquetes

9. Haga clic en Agregar regla.



Agregar regla

10. Elija la opción de selección de archivos que prefiera:

- Servidor de protocolo de copia segura (SCP): Introduzca el nombre de archivo exacto del

paquete de instalación. Este método se recomienda para archivos grandes.

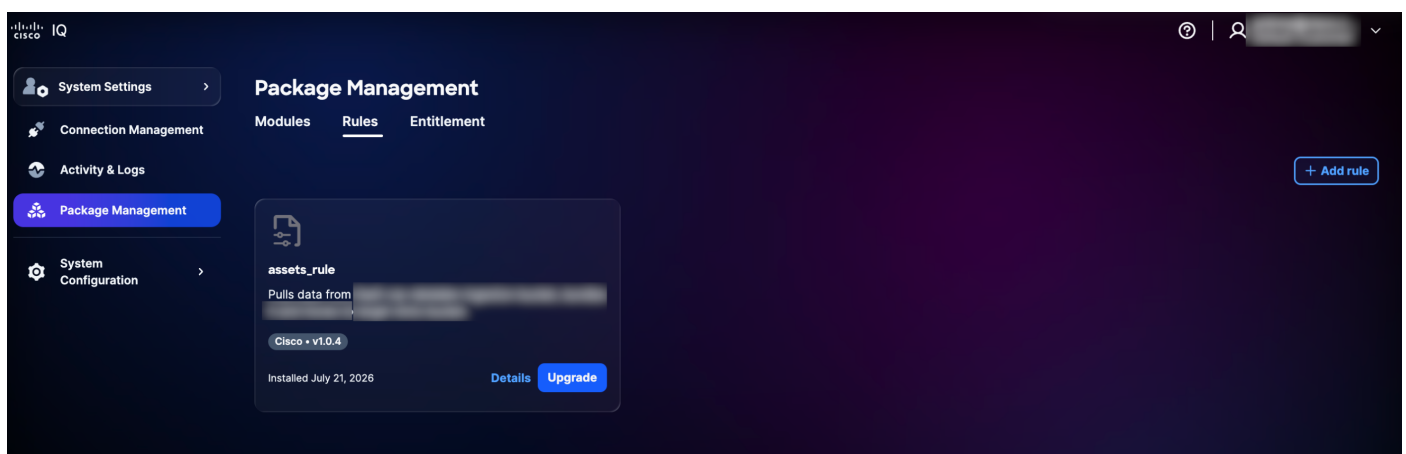
- Carga de archivo local: Arrastre y suelte el archivo de instalación descargado.

11. Haga clic en Add (Agregar). La regla agregada se muestra en Administración de paquetes.

Actualización de reglas

Para actualizar reglas:

1. Vaya a System Settings > Package Management in VA.



Actualizar

2. En la regla deseada, haga clic en Upgrade. Se abre la ventana Regla de actualización.

Upgrade Rule

File selection

☒ SCP server ☐ Local file upload

Cancel

Add

Regla de actualización

3. Elija la opción de selección de archivos que prefiera:

- Servidor de protocolo de copia segura (SCP): Introduzca el nombre de archivo exacto del paquete de instalación. Este método se recomienda para archivos grandes.
- Carga de archivo local: Arrastre y suelte el archivo de instalación descargado.

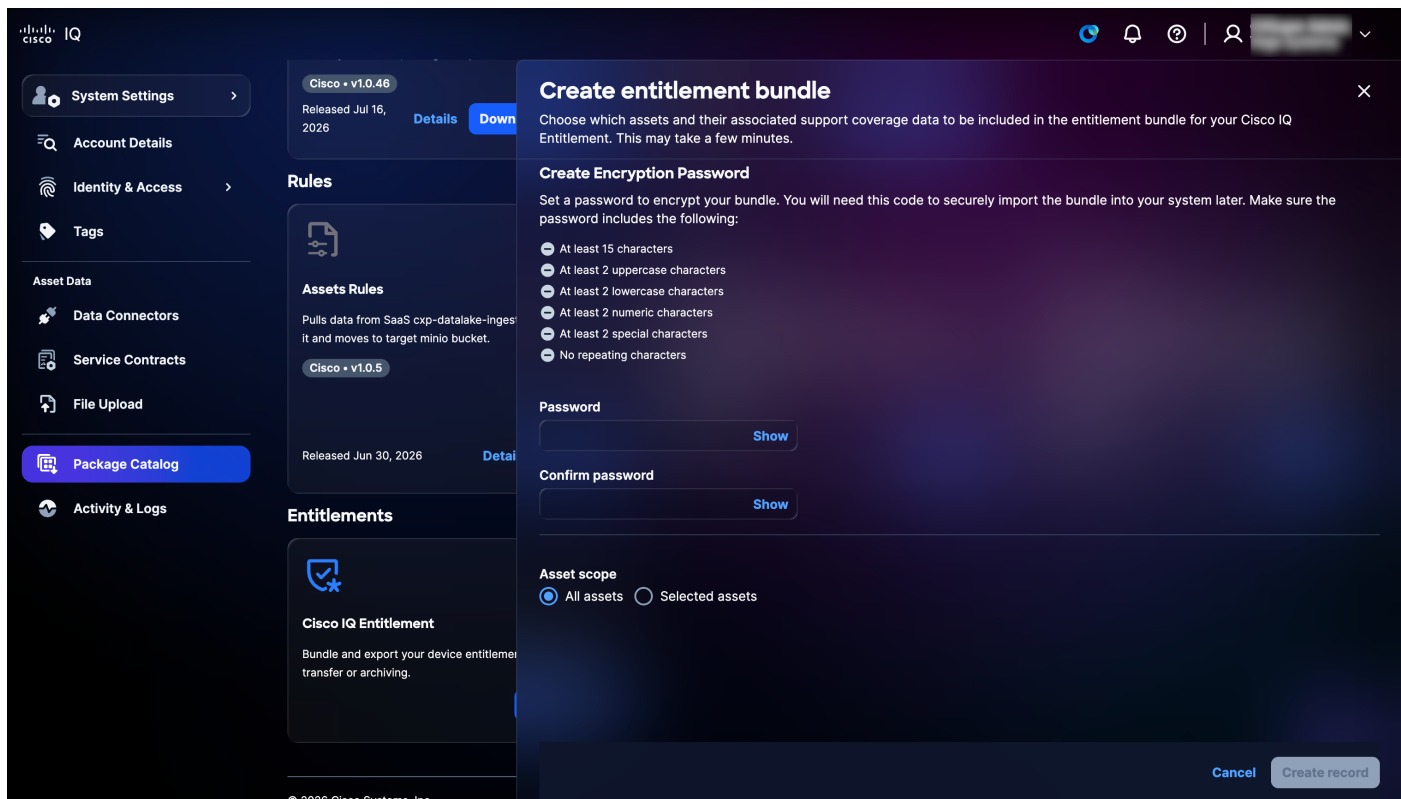
4. Haga clic en Add (Agregar).

 Nota: Estas reglas se aplican en la recopilación de telemetría de dispositivos programada recurrente. Para una aplicación inmediata, puede iniciar manualmente la recopilación de telemetría del dispositivo.

Instalación de derechos

Un derecho proporciona la validación del derecho de su organización a utilizar funciones, módulos o servicios de software específicos. Para instalar un derecho:

1. Inicie sesión en [Cisco IQ](#).
2. Vaya a System Settings > Package Catalog.
3. En la tarjeta de derechos, haga clic en Create record. Se abrirá la ventana Create right bundle.



Crear paquete de derechos

4. Ingrese una contraseña. Consulte las reglas de creación de contraseñas que se muestran en pantalla.
5. Vuelva a introducir la misma contraseña en Confirmar contraseña.
6. Seleccione el botón de opción **Ámbito de activo** preferido.
 - Todos los recursos: Incluye todos los activos vinculados a usted
 - Activos seleccionados: Permite seleccionar dispositivos específicos alineados con su entorno; si se selecciona esta opción, active las casillas de verificación de todos los activos aplicables
7. Haga clic en **Create record** para guardar el archivo localmente.

 **Nota:** Después de crear el paquete de derechos, no se desplace fuera de la pantalla actual. Si se desplaza a otra página, el paquete se invalida y debe volver a crearlo para activar la opción de descarga.

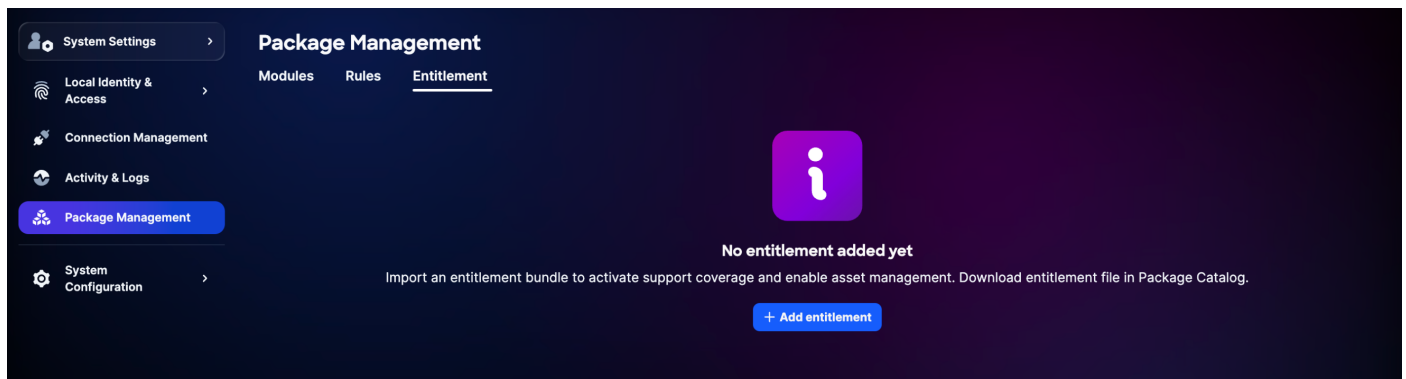
 **Nota:** Los archivos de instalación son grandes (10-25 GB); asegúrese de que dispone de suficiente espacio en disco antes de realizar la descarga.

8. Inicie sesión en VA.

9. Vaya a Inicio > Configuración del sistema > Administración de paquetes. La página Administración de paquetes contiene las fichas siguientes:

- Módulos
- Reglas
- Derechos

10. Haga clic en la pestaña Derechos.



Ficha Derechos

11. Haga clic en Add Entitlement.

Add Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

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

Agregar derecho

12. Elija la opción de selección de archivos que prefiera.

- Servidor de protocolo de copia segura (SCP): Introduzca el nombre de archivo exacto del paquete de instalación; este método se recomienda para archivos grandes
- Carga de archivo local: Arrastrar y soltar el archivo de instalación descargado

13. Ingrese una contraseña.

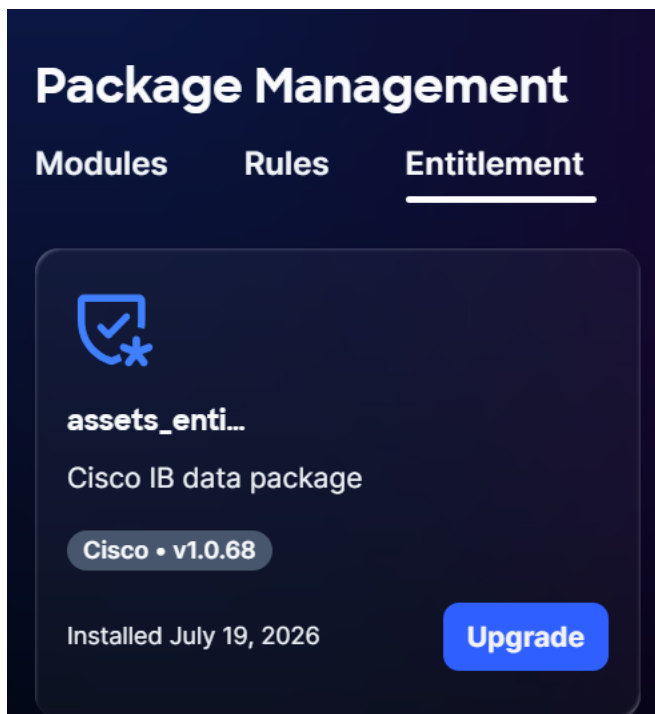
14. Haga clic en Add (Agregar). El derecho recién instalado se muestra en la pestaña Entitlement en Administración de paquetes.

15. Para habilitar los derechos, espere de 5 a 10 minutos después de agregarlos y, a continuación, inicie la recopilación de telemetría del dispositivo.

 Nota: Al añadir un contrato de servicio en el proceso de autorización, se añaden todos los dispositivos vinculados a dicho contrato al inventario de activos de dispositivos in situ. Dispone de opciones para filtrar los dispositivos por número de serie, utilizar varios ID de cuenta o seleccionar dispositivos específicos para administrar los derechos.

Actualización de derechos

Para actualizar un derecho:



Actualización de derechos

1. En el derecho deseado, haga clic en Upgrade.

Upgrade Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

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

Derecho de actualización

2. Elija la opción de selección de archivos que prefiera:

- Servidor de protocolo de copia segura (SCP): Introduzca el nombre de archivo exacto del paquete de instalación; este método se recomienda para archivos grandes
- Carga de archivo local: Arrastrar y soltar el archivo de instalación descargado

3. Ingrese una contraseña.

4. Haga clic en Add (Agregar).

Funciones alimentadas por IA

El módulo On-Prem AI Inference Infrastructure habilita capacidades in situ alimentadas por IA en AV. Ejecuta un modelo de lenguaje pequeño (SLM) localmente, lo que permite al sistema responder a avisos alimentados por IA. Una vez instalado, puede interactuar con él directamente en la interfaz del dispositivo virtual.

Se admiten los siguientes tipos de consulta:

- Recursos: Identificar los recursos en riesgo debido al estado de fin de vida útil, la moneda del software o la no conformidad, las vulnerabilidades de seguridad y las brechas de cobertura de contratos
- Inventario: Solicitar un análisis basado en IA sobre los activos de su inventario

El paquete de instalación de la infraestructura de inferencia de inteligencia artificial in situ está disponible en el catálogo de paquetes de Cisco IQ y se distribuye de la misma manera que otros módulos, como Assets.

 Nota: Solo se puede ejecutar una (1) infraestructura de inferencia de IA en las instalaciones por GPU a la vez. La instalación tarda aproximadamente 40-45 minutos en completarse. Los archivos de instalación son grandes (aproximadamente 30 GB); asegúrese de que dispone de suficiente espacio en disco antes de realizar la descarga.

Prerrequisitos de On-Prem AI Inference Infrastructure

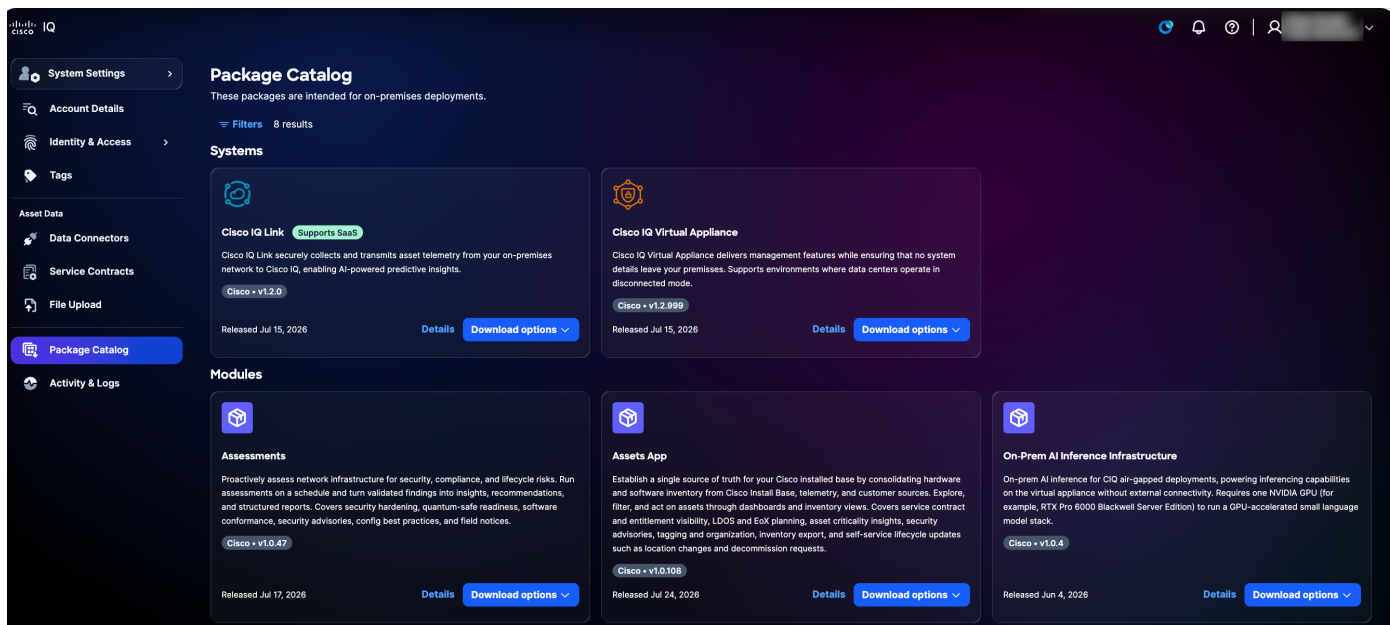
Antes de instalar On-Prem AI Inference Infrastructure, deben cumplirse las siguientes condiciones:

- El AV debe incluir una VM con acceso a GPU; el SLM requiere una GPU y no se puede ejecutar sin una
- La GPU VM debe tener 80 GB o más de GPU VRAM disponibles

Instalación de la infraestructura de inferencia de IA in situ

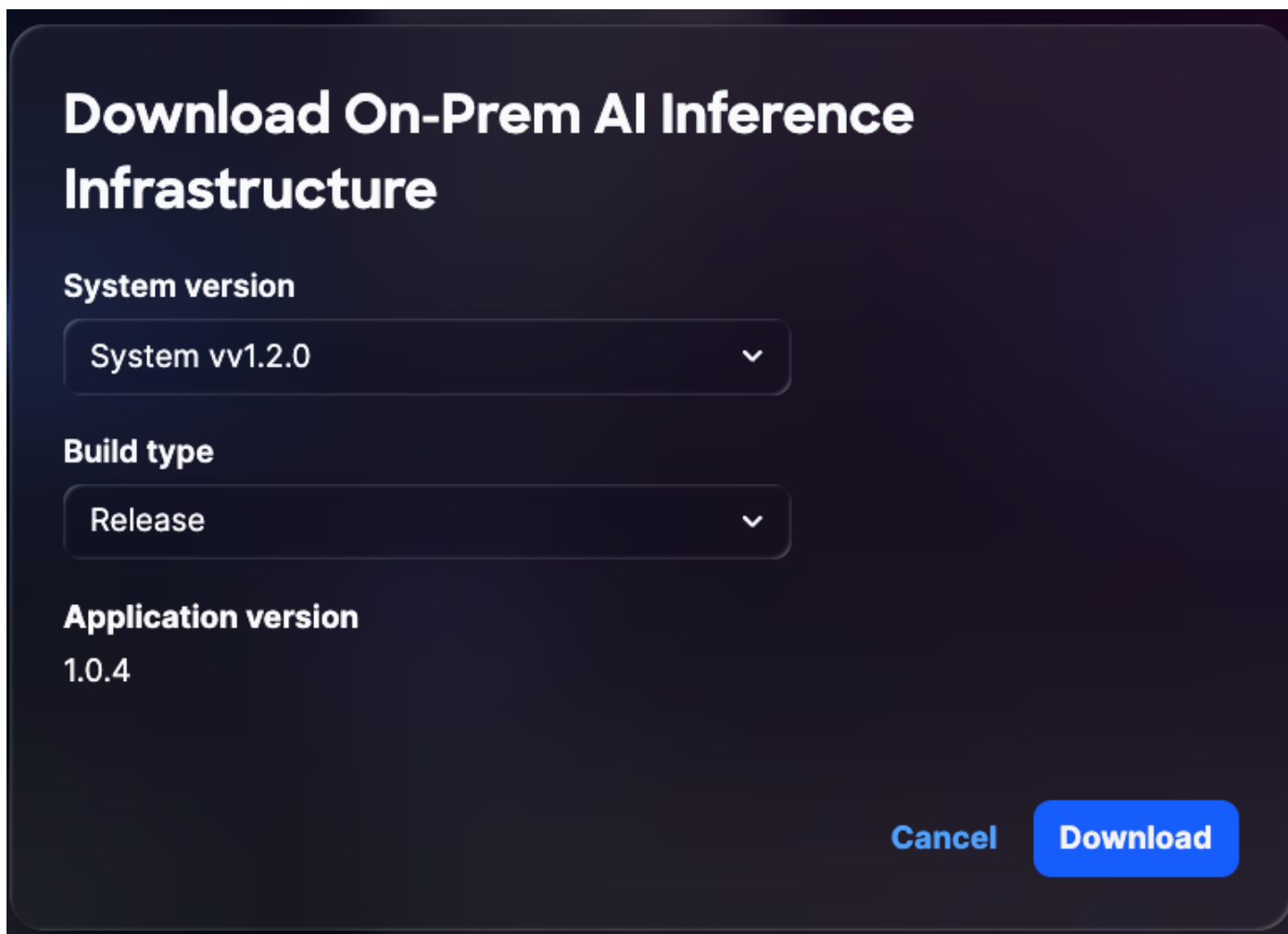
Para instalar On-Prem AI Inference Infrastructure en el VA, descargue el módulo On-Prem AI Inference Infrastructure desde Cisco IQ SaaS:

1. Inicie sesión en [Cisco IQ](#).
2. Vaya a System Settings > Package Catalog.



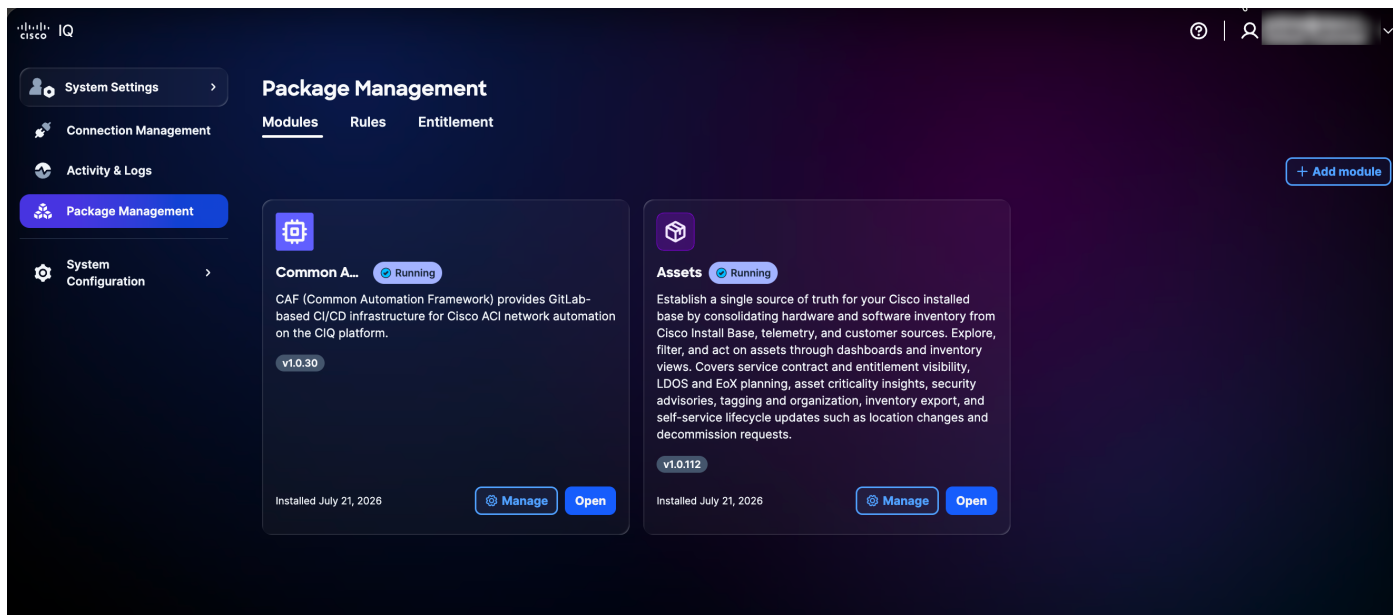
Instalar paquete

3. En la tarjeta On-Prem AI Inference Infrastructure, haga clic en Download options > Installation packages. Se abre la ventana Descargar aplicación.



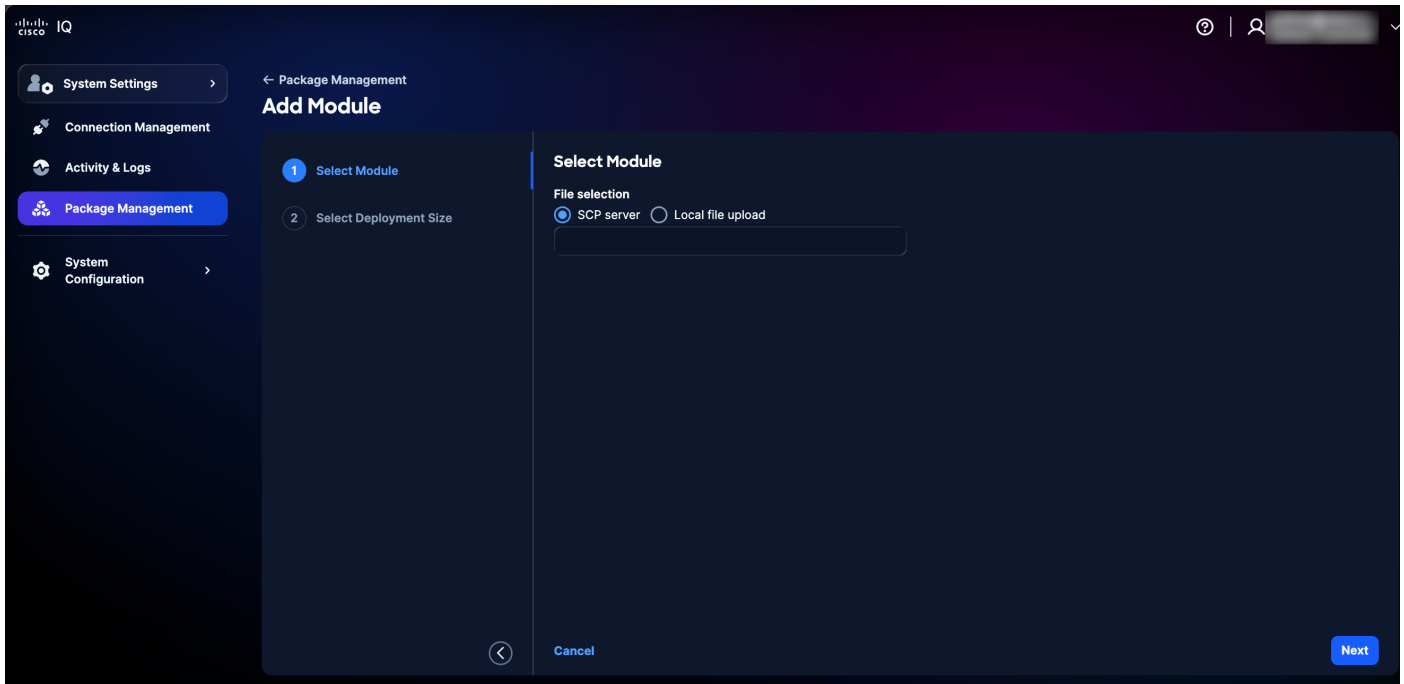
Descargar infraestructura de inferencia de IA

4. Elija una versión del sistema en la lista desplegable.
5. Elija un tipo de generación en la lista desplegable.
6. Haga clic en Descarga.
7. Vaya a VA.



Gestión de paquetes

8. Vaya a Inicio > Configuración del sistema > Administración de paquetes. Se muestra la página Administración de paquetes con las fichas siguientes:
 - Módulos
 - Reglas
 - Derechos
9. En la pestaña Módulos, haga clic en Agregar módulos.



Seleccionar módulo

10. Elija la opción de selección de archivos que prefiera:

- Servidor SCP: Introduzca el nombre exacto del paquete de instalación (recomendado para archivos grandes).
- Carga de archivo local: Arrastre y suelte el archivo de instalación descargado (no se recomienda para archivos de 30 GB o más debido al tiempo de carga). Nota: El método de carga del archivo local tiene un umbral de 20 minutos. Si el proceso de carga excede esta duración, la instalación falla. El uso de un servidor SCP es el método preferido para garantizar una instalación correcta y estable.

11. Haga clic en Next (Siguiente). El sistema comienza a cargar el archivo.

12. Elija un tamaño de implementación (por ejemplo, pequeño, mediano o grande).

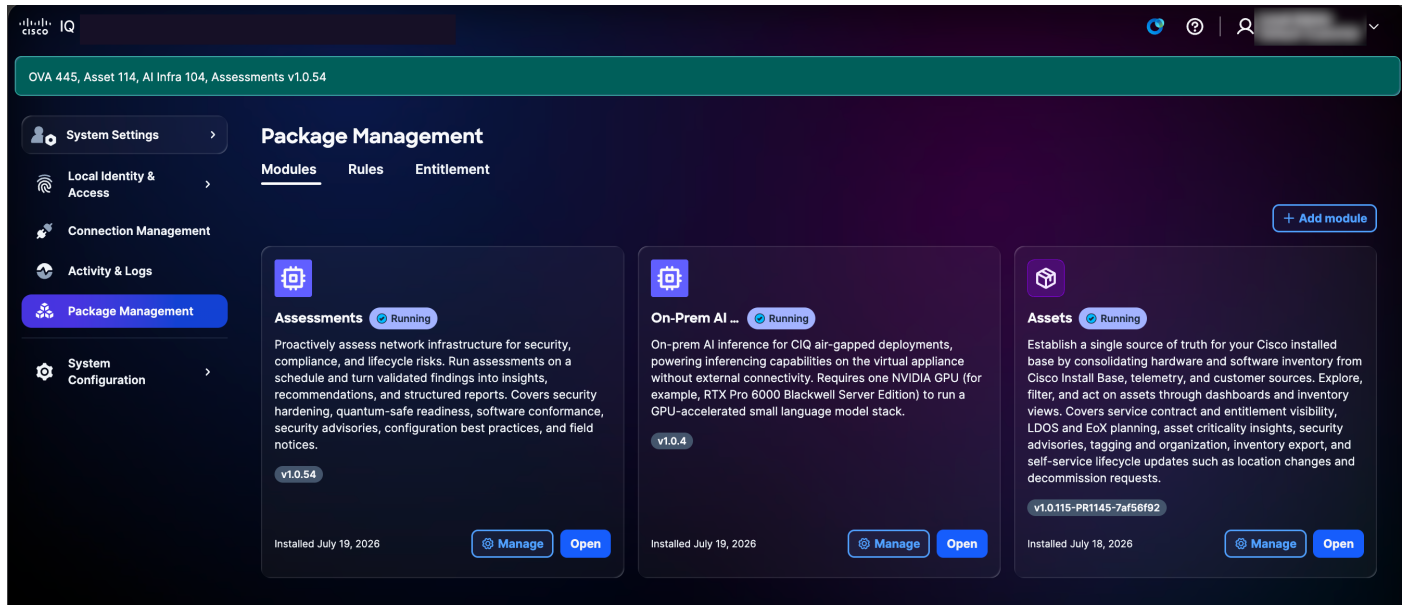
13. Haga clic en Agregar módulo. La instalación comienza y tarda aproximadamente 40-45 minutos en completarse.

Una vez completada la instalación, On-Prem AI Inference Infrastructure se muestra en la pestaña Módulo de Administración de paquetes.

 Nota: Solo se puede ejecutar un módulo de infraestructura de inferencia de IA en las instalaciones por GPU. El módulo utiliza aproximadamente el 90% de la GPU VRAM. No se admite el intento de instalar una instancia adicional en la misma GPU.

Administración del módulo de infraestructura de inferencia de IA in situ

Una vez instalado, el módulo On-Prem AI Inference Infrastructure se puede administrar desde la pestaña Applications en Package Management.



Edición de la infraestructura de inferencia AI

Para administrar el módulo, haga clic en Manage junto al módulo On-Prem AI Inference Infrastructure. Consulte [Administración de módulos](#) para obtener más detalles.

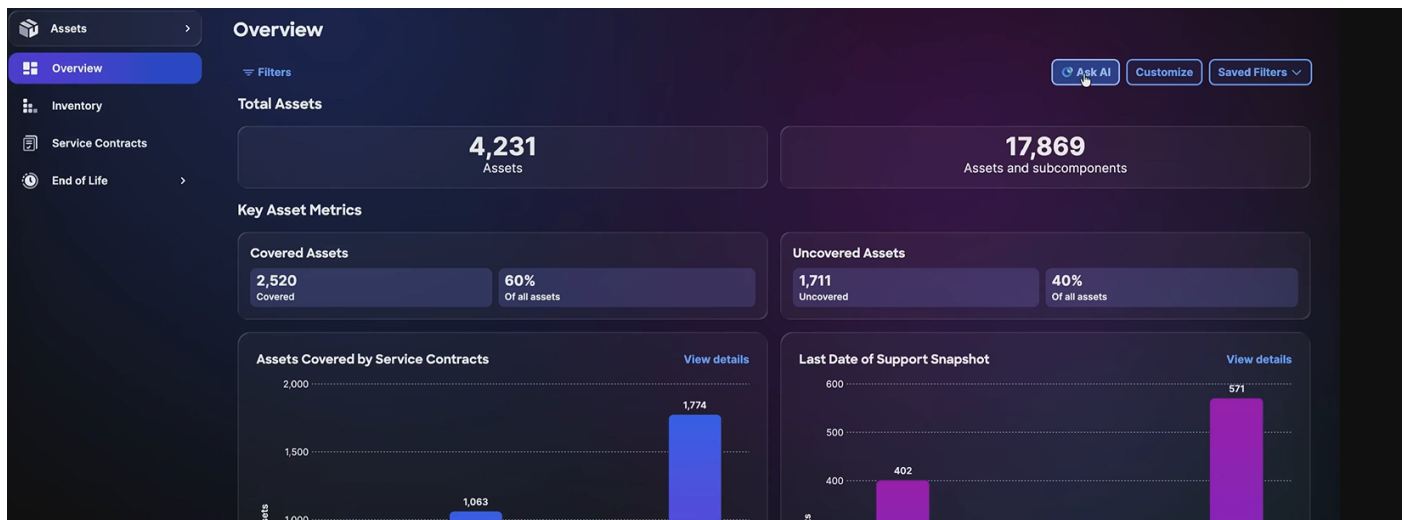
Uso de funciones alimentadas por IA

Una vez que el módulo On-Prem AI Inference Infrastructure se haya instalado correctamente, el botón Ask AI estará disponible en la interfaz VA.

Pregunte sobre la IA en Assets

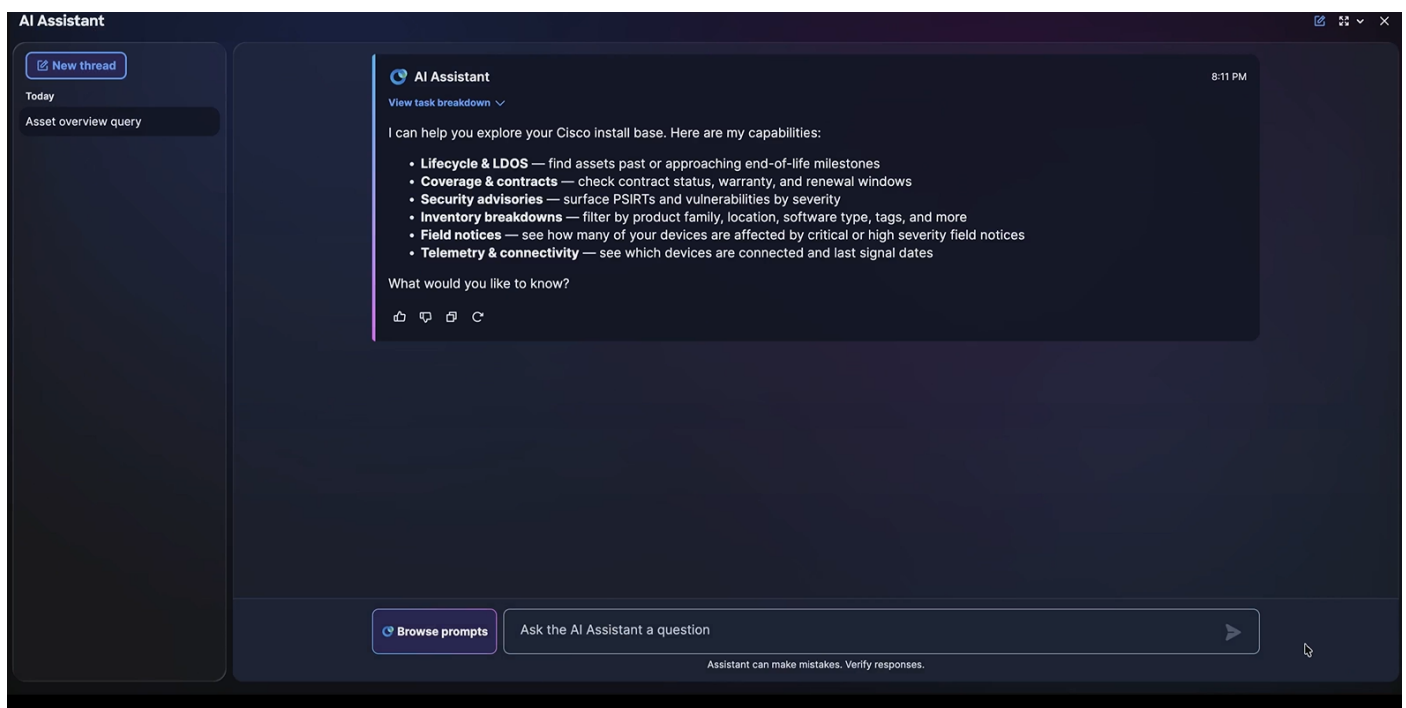
Para utilizar Preguntar AI en Activos:

1. Elija el menú Inicio > Activos. Se muestra la página Assets.



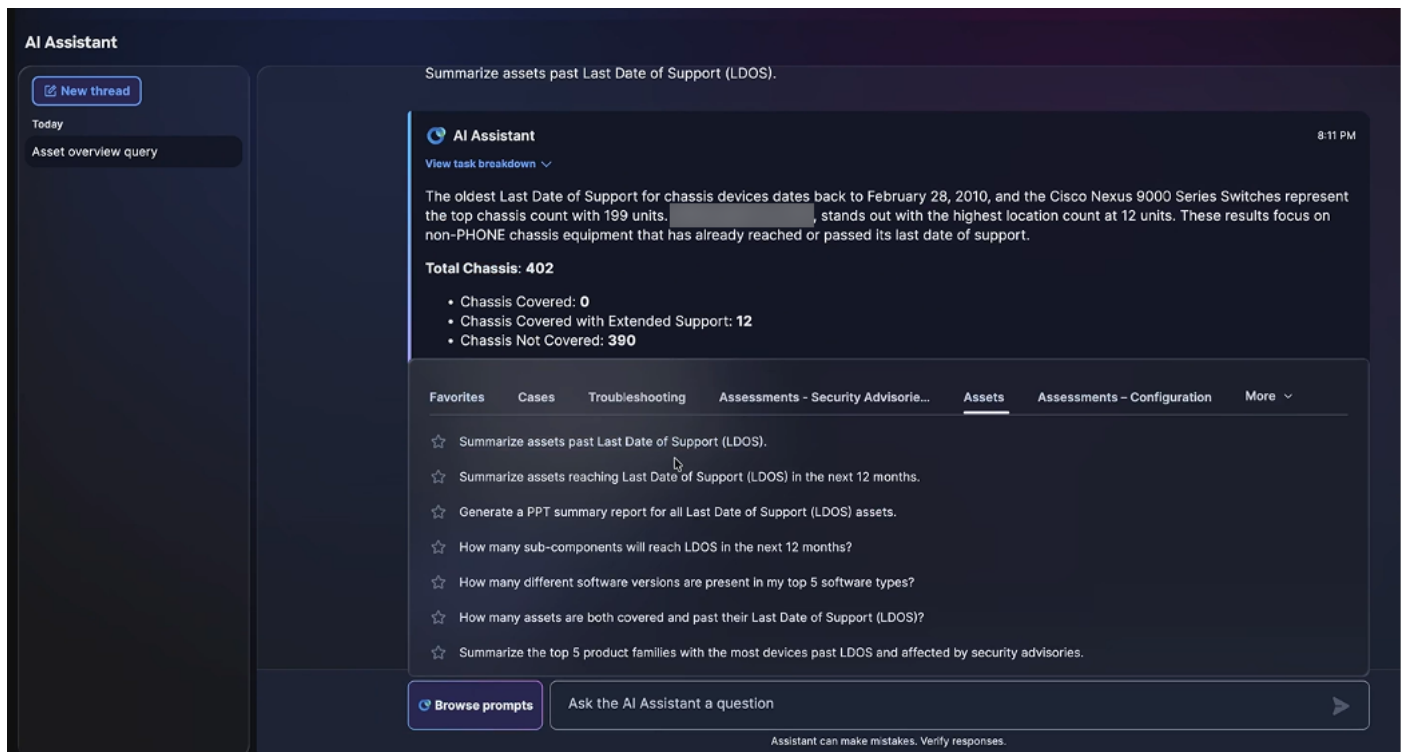
Página Activos

2. Haga clic en Preguntar AI. Se lanza la infraestructura de inferencia de IA in situ.



Examinar avisos

3. Haga clic en Examinar avisos para ver los avisos disponibles o escriba una pregunta personalizada en el campo Preguntar al asistente de AI.



Conjunto de mensajes

4. Haga clic en el mensaje deseado o pulse Intro. El SLM in situ genera una respuesta.

Análisis de IA en el inventario

El módulo On-Prem AI Inference Infrastructure proporciona análisis automatizados impulsados por IA en la sección Inventory. Los resultados del análisis se muestran automáticamente una vez que se rellenan los datos de inventario.

Para ver el análisis de IA en Inventory:

1. Seleccione el menú Inicio > Inventario. Se muestra la página Inventory.

Assets

Overview

Inventory

Service Contracts

End of Life

Assets

Q Search

1 Equipment type

Filters (1)

4231 results

Reset filters

Export

Saved Filters

Insights

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

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

Full Analysis

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

Inventario

-
2. Vea el análisis generado por IA. Los resultados se muestran en la vista de inventario una vez que los datos están disponibles.

 Nota: Haga clic en Análisis completo para obtener visualizaciones como gráficos, paneles y gráficos que proporcionan información adicional.

Características comunes de los módulos

En esta sección se detallan las funciones principales compartidas entre todos los módulos. Estas funciones ofrecen una experiencia de usuario coherente, optimizan el rendimiento del sistema y agilizan los flujos de trabajo administrativos

Análisis de datos

El panel Insights ofrece un análisis basado en IA de los datos de esa página, proporcionando información procesable para mejorar la seguridad y el estado de su entorno de red.

 Nota: La función Análisis (Analysis) sólo está disponible en las páginas seleccionadas.

Assets

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

Insights

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

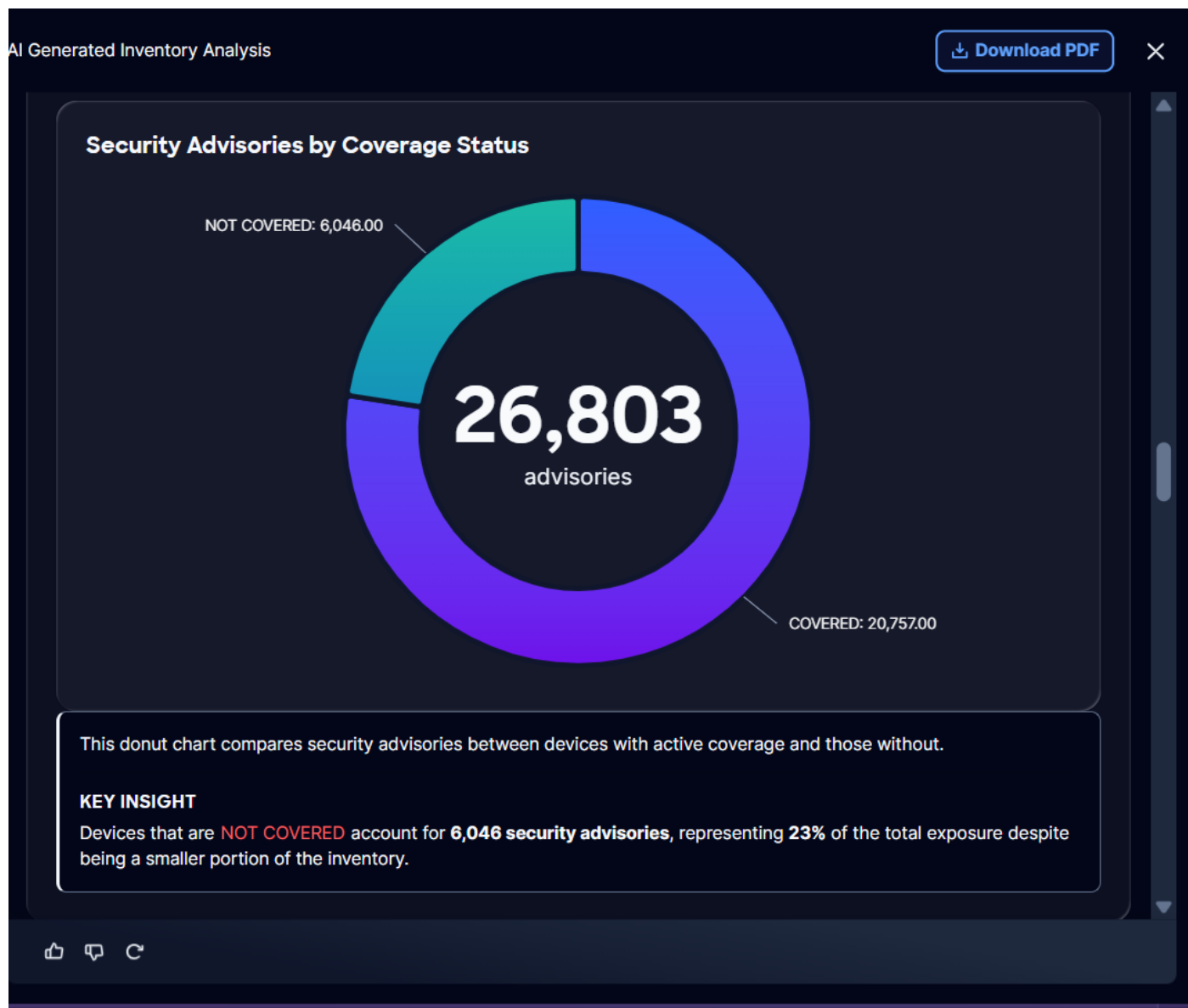
Full Analysis

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

Panel de información

Las siguientes opciones están disponibles en el panel Perspectivas:

- Haga clic en el icono Expand para expandir el panel y mostrar información adicional
- Haga clic en el icono Pulgares arriba o Pulgares abajo para proporcionar comentarios sobre la información generada por IA
- Haga clic en Análisis completo para mostrar información adicional, análisis más profundos y visualizaciones como gráficos, paneles y gráficos



Análisis completo

Las siguientes opciones están disponibles en un análisis completo:

- Haga clic en Descargar PDF para guardar una copia sin conexión del análisis para sus registros o para la colaboración

Exportación de información

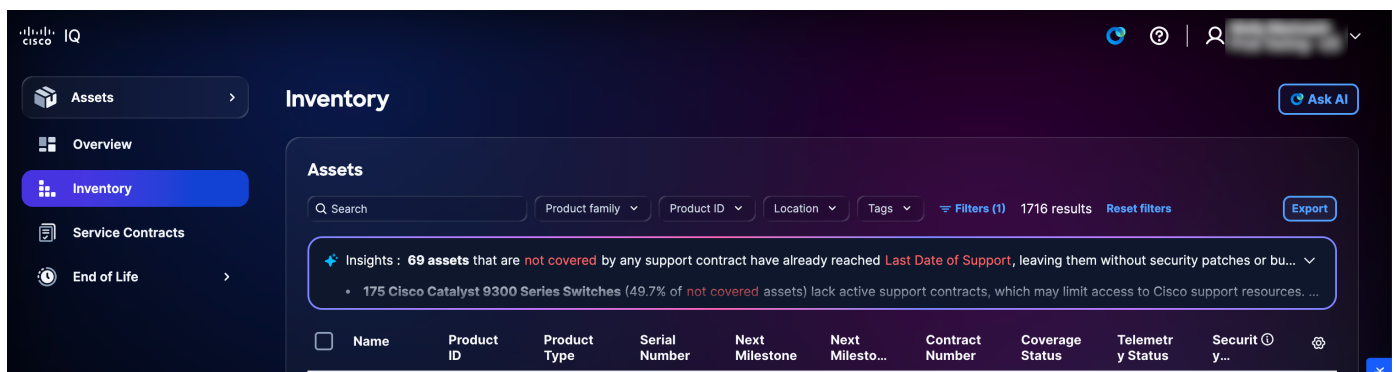
La función de exportación permite exportar vistas personalizadas para la información de Activos y Seguridad en formato .xls o .csv.



Nota: La función de exportación sólo está disponible para las páginas seleccionadas.

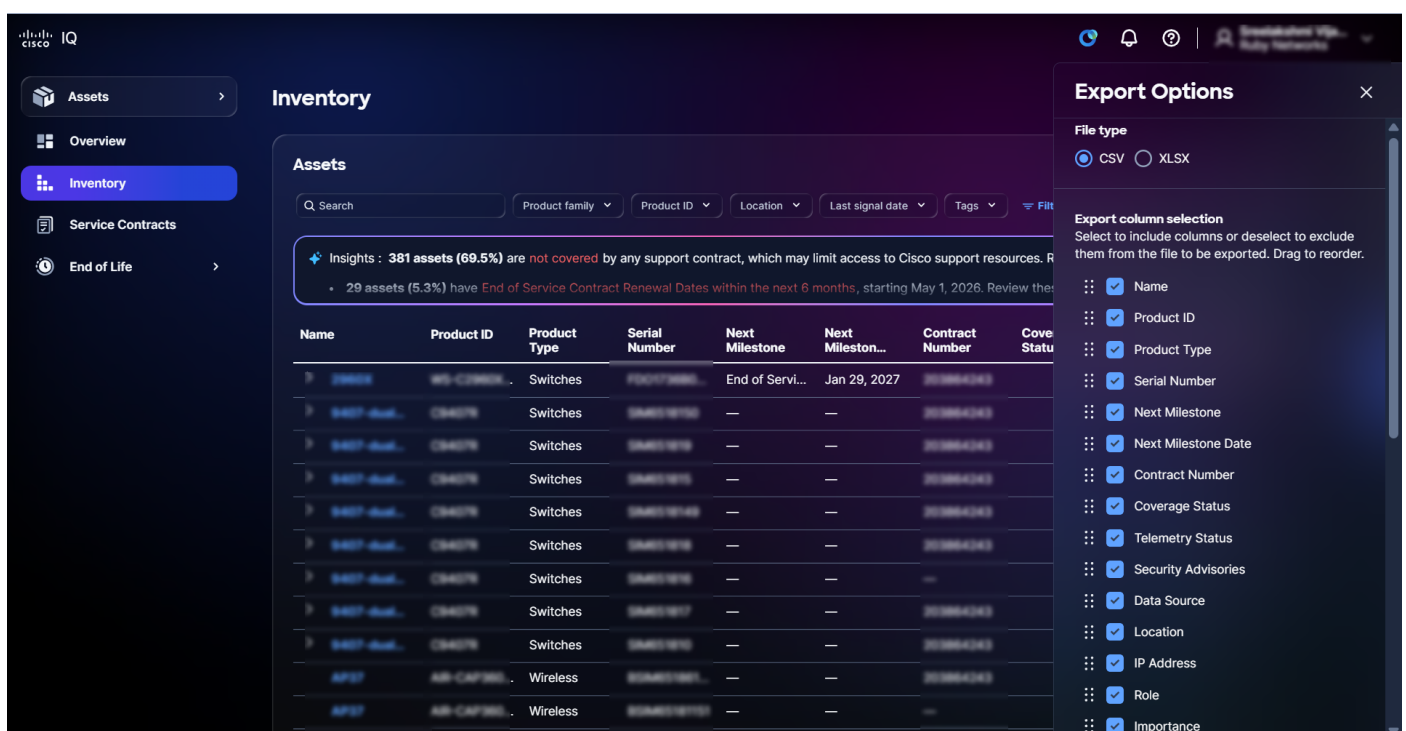
Para exportar información desde una página:

1. Desplácese hasta la página.



Exportación de Inventario en el Módulo Activos

2. Haga clic en Exportar. Se muestra Opciones de exportación.



Opciones de exportación

3. Seleccione un tipo de archivo.

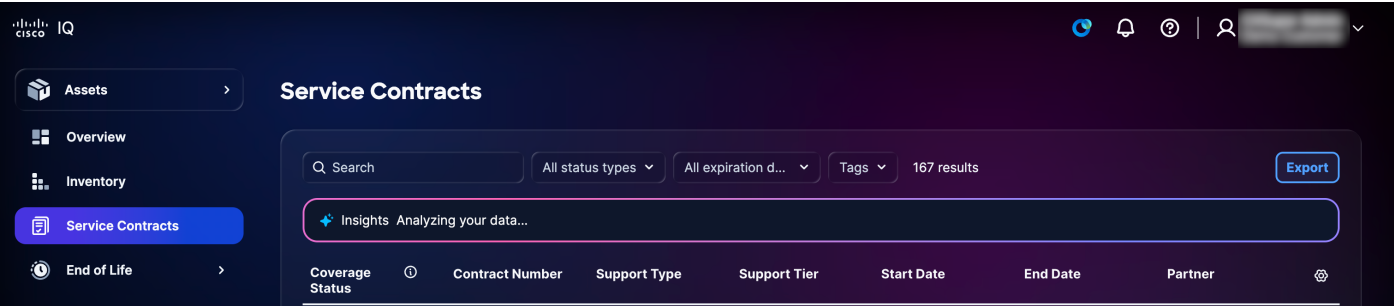
4. Marque las casillas de verificación de las columnas deseadas.

5. Haga clic en Exportar. El archivo se descarga en la carpeta de descarga local del

explorador.

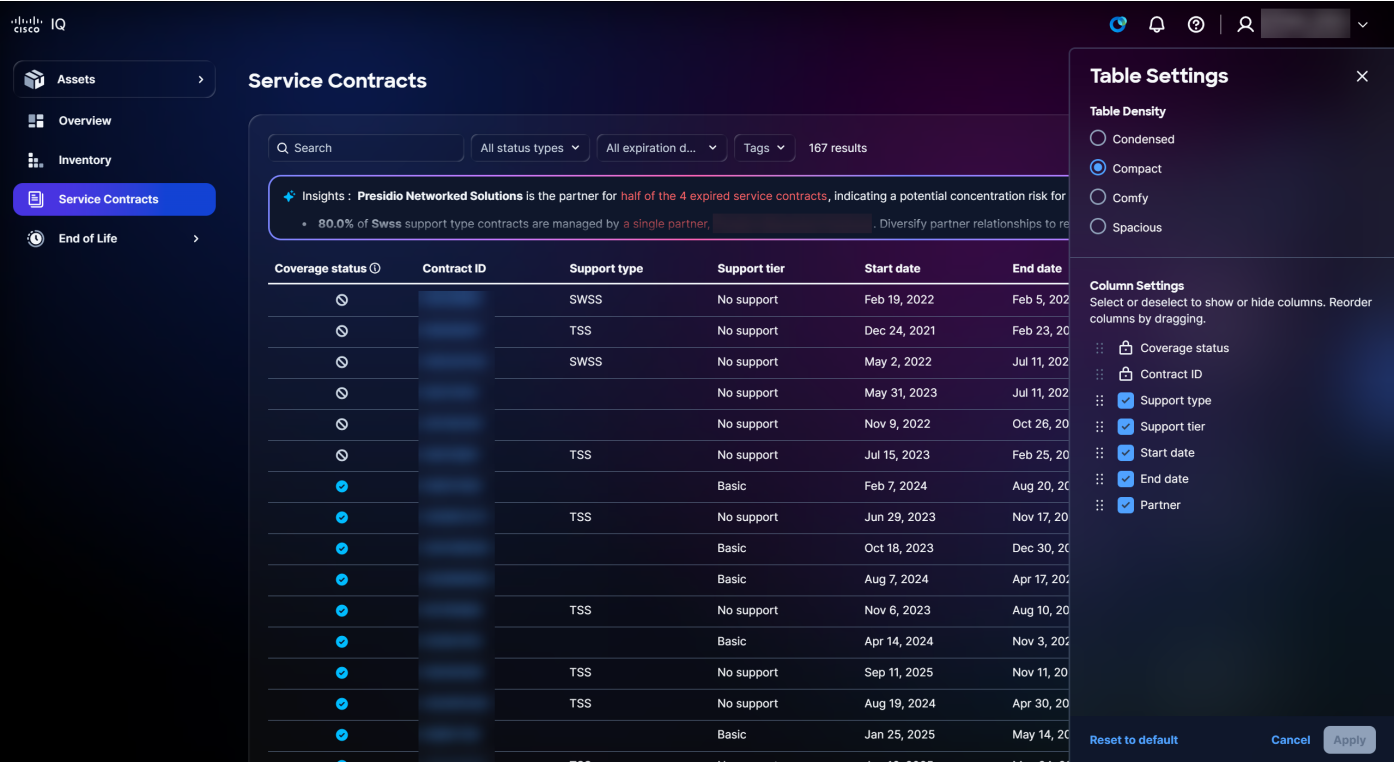
Configuración de tabla

Puede configurar la tabla para crear vistas personalizadas y refinadas para las diferentes funciones del módulo.



Configuración de tabla

Para cambiar las columnas que se muestran en las páginas seleccionadas, haga clic en el icono Configuración de tabla. Se muestra la configuración de la tabla.



Opciones de configuración de tabla

Cambio de la vista Tabla

Para cambiar la vista de tabla:

1. Seleccione una de las siguientes opciones de densidad de tabla:

- Condensado: Minimiza los elementos visuales y el espaciado para mostrar más información
- Compacto: Reduce los espacios en blanco y ajusta el espaciado entre los elementos de la interfaz de usuario
- Cómodo: Utiliza más espacios en blanco y más espacio entre los elementos
- Amplio: Enfatiza los espacios en blanco abundantes y los elementos UI más grandes

2. Haga clic en Apply (Aplicar).

Adición y eliminación de columnas

Para agregar o quitar columnas:

1. Active o desactive las casillas de verificación Configuración de columnas.

2. Haga clic en Apply (Aplicar).



Nota: La columna Nombre no se puede quitar de la vista de tabla.

Cambio del orden de columnas

Para cambiar el orden de las columnas:

1. Arrastre y suelte el nombre de la columna para organizar los elementos en el orden deseado.

2. Haga clic en Apply (Aplicar).

Personalización de paneles

La función Panel personalizado permite personalizar paneles estándar a través de una serie de opciones de personalización intuitivas:

- Reorganizar los widgets o paneles del panel mediante la funcionalidad de arrastrar y colocar
- Elimine los componentes que no sean relevantes para el flujo de trabajo
- La disposición personalizada del panel se almacena de forma segura en su perfil de usuario y se aplica automáticamente a todas las sesiones y dispositivos
- Restaure el diseño original del panel con una sencilla opción de reinicio

Para personalizar un tablero:

1. Desplácese hasta el panel.



Personalizar

2. Haga clic en Personalizar.



Editar panel

3. Cambie el panel como desee:

- Reorganizar: Arrastre y suelte los widgets en el diseño deseado
- Extraer: Haga clic en el icono Eliminar para eliminar un widget
- Reiniciar: Haga clic en Restablecer valores predeterminados para restablecer el panel a su diseño original

4. Click Save. Se muestra un mensaje Dashboard Saved.

El diseño del panel se aplica automáticamente a todas las sesiones y dispositivos.

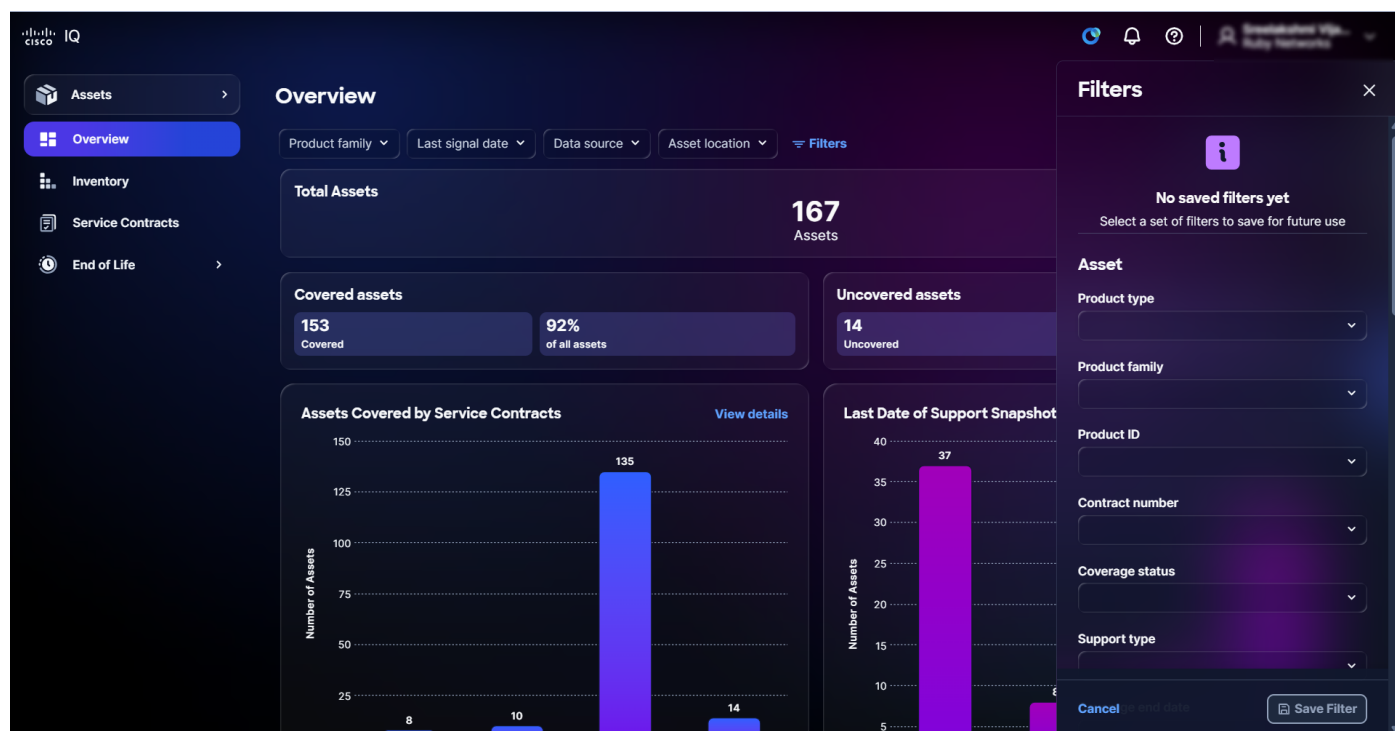
Personalización de filtros

Puede guardar configuraciones de filtro personalizadas para cualquier vista de panel, lo que le permitirá volver fácilmente a la configuración preferida según sea necesario. Todas las preferencias de filtrado se almacenan de forma segura por usuario y cuenta, lo que garantiza una experiencia personalizada y uniforme cada vez que acceda a Cisco IQ.

Creación de un filtro

Para crear un filtro personalizado:

1. Desplácese hasta el panel.
2. Haga clic en Filtros.



Filtros

3. Elija los filtros que desee en las listas desplegables.
4. Haga clic en Guardar filtro. Se abrirá la ventana Filtro guardado de nombre.

Name saved Filter

Filter name *

Custom Filter |

Cancel

Save Filter

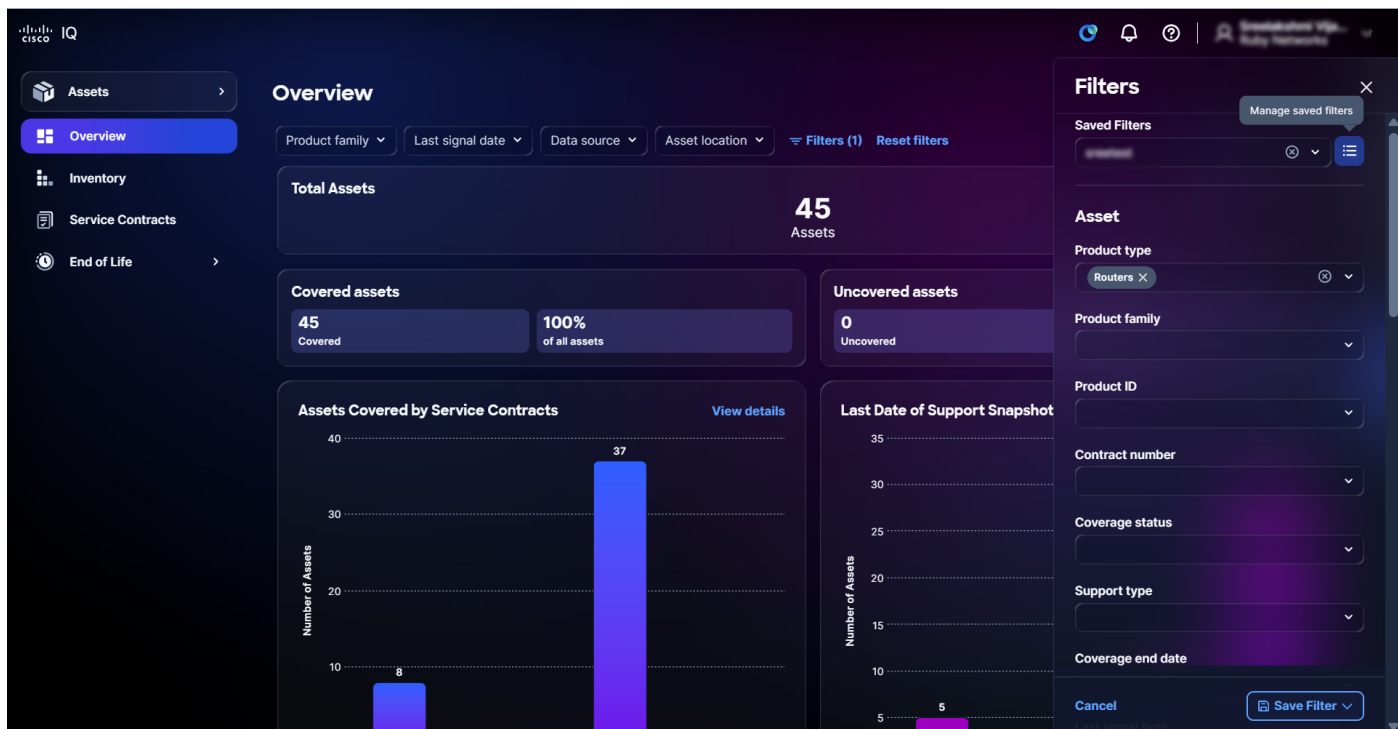
Nombre del filtro

5. Introduzca un nombre de filtro.
6. Haga clic en Guardar filtro para confirmar.

Edición de un nombre de filtro

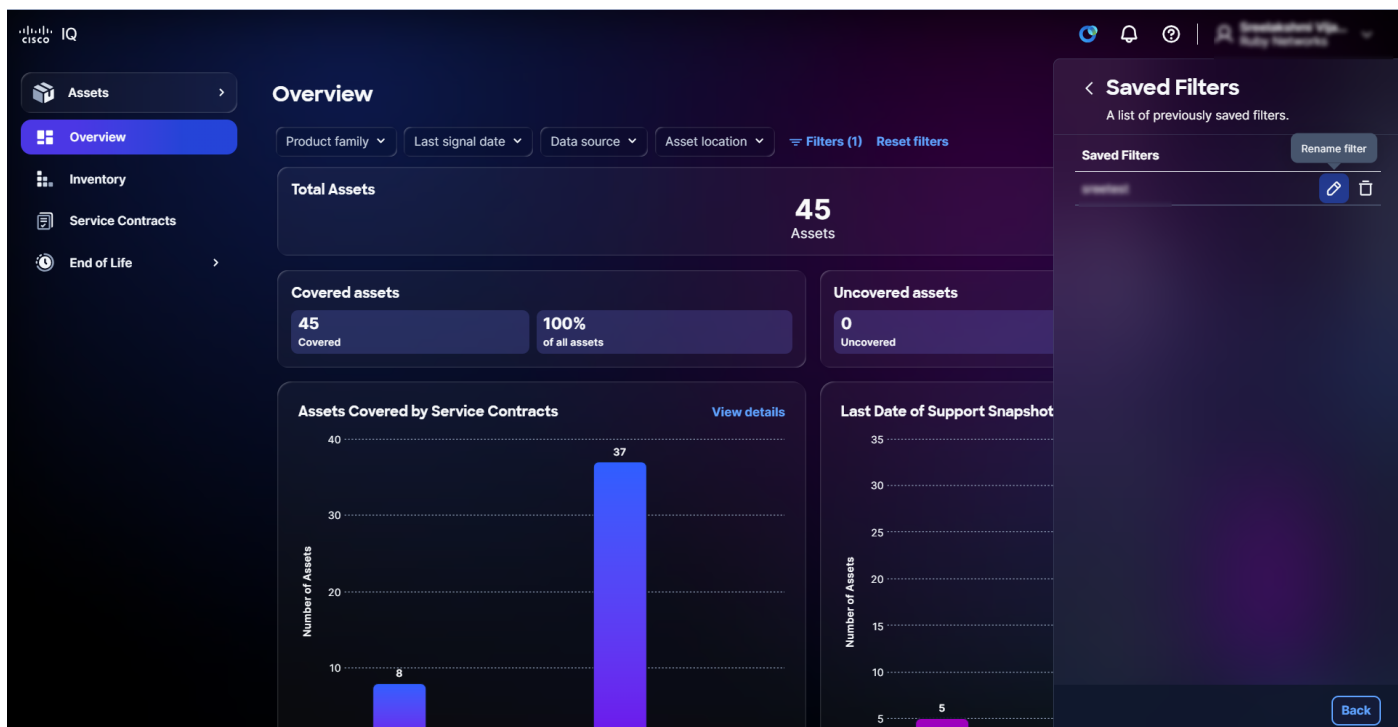
Para editar un filtro personalizado:

1. Haga clic en Filtros.



Administrar filtros guardados

2. Haga clic en el icono Administrar filtros guardados.
3. Desplácese hasta el filtro.



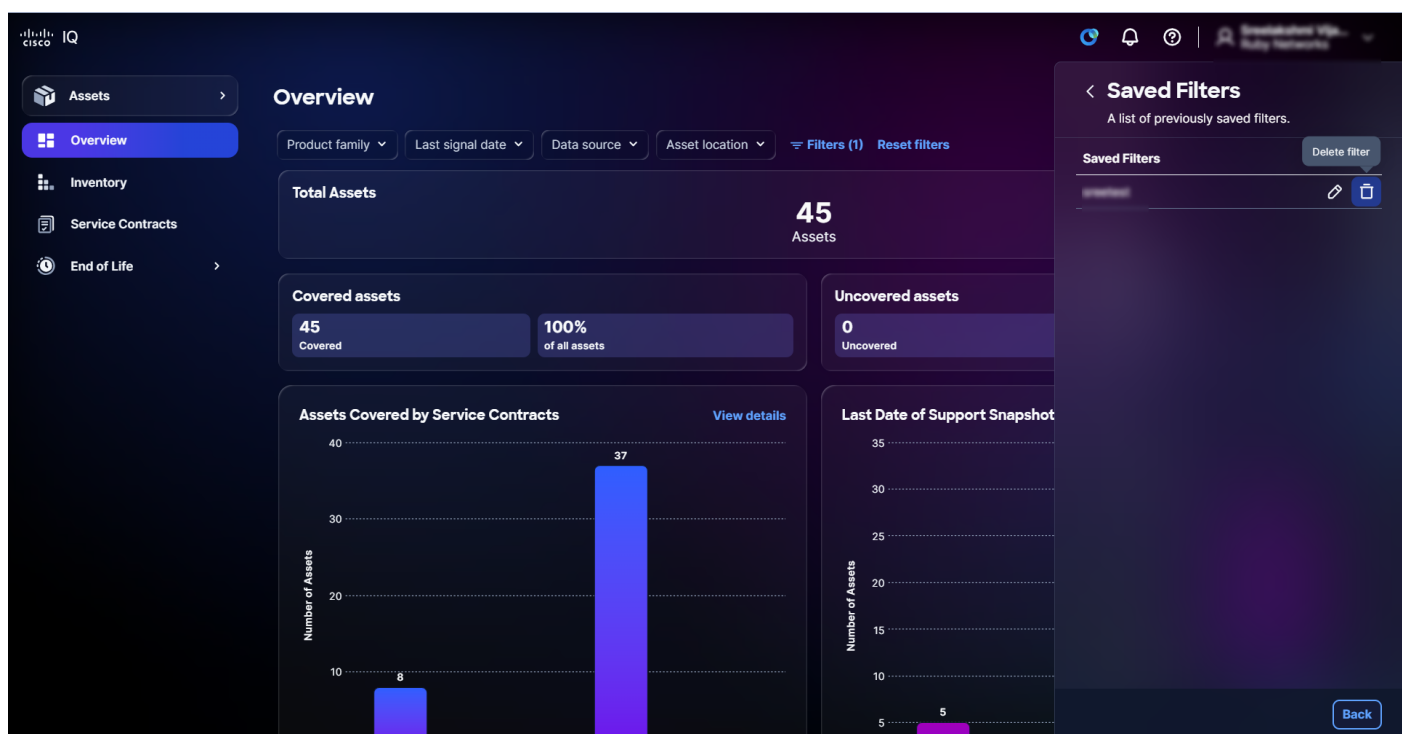
Editar filtro

4. Haga clic en el icono Edit. Se abre la ventana Filtro guardado de nombre.
5. Edite el nombre del filtro.
6. Haga clic en Guardar filtro para confirmar.

Eliminación de un filtro

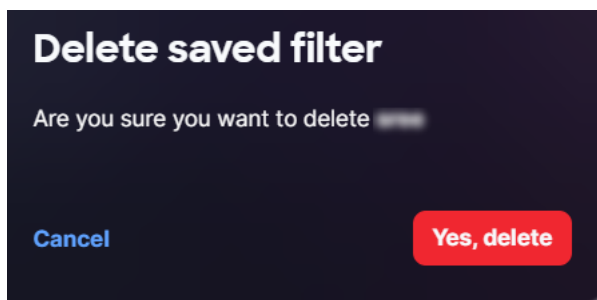
Para eliminar un filtro personalizado:

1. Haga clic en Filtros.
2. Haga clic en el icono Filtros guardados gestionados
3. Desplácese hasta el filtro.



Eliminar filtro guardado

4. Haga clic en el icono Delete (Eliminar). Se abrirá la ventana Eliminar filtro guardado.



Eliminar confirmación filtro guardado

5. Haga clic en Yes, delete para confirmar.

Módulo de recursos

El módulo Assets ofrece funciones de gestión y visibilidad completas para los recursos de Cisco y sirve de base para Cisco IQ, ya que proporciona una lista centralizada de todos los dispositivos de una organización. Al recopilar información de varias fuentes, actúa como una única fuente fidedigna para el inventario de dispositivos. Es esencial mantener una lista de recursos completa y precisa, ya que otros módulos de Cisco IQ, como el módulo Evaluaciones, se basan en estos datos para evaluar el estado y la seguridad de sus dispositivos.

Conceptos básicos

El módulo Activos se basa en los siguientes conceptos básicos:

- **Activo:** Cualquier dispositivo físico, hardware o software que se registre y administre como parte de la prestación de servicios de Cisco con un seguimiento detallado de su identidad, función, cobertura de servicio y ciclo de vida
- **Recursos generados por contratos:** Activos que se ingieren en el inventario directamente a partir de datos de contratos de servicio vinculados, en lugar de hacerlo mediante telemetría. Cisco IQ ingiere los siguientes tipos de equipos a partir de los datos del contrato: Chasis, módulos, fuentes de alimentación y ventiladores. Estos recursos están visibles en el inventario aunque no haya ninguna conexión de telemetría
- **Fecha final de soporte técnico (LDOS):** Seguimiento de los hitos del fin de vida útil y fin de asistencia para los productos de Cisco
- **Cobertura del servicio:** Contratos de asistencia activos, garantías y niveles de derechos asociados a un componente de hardware o software específico
- **Etiqueta de activo:** Una etiqueta definida por el usuario asignada a un recurso para la

organización, el filtrado y los flujos de trabajo operativos

- Señal del dispositivo: Se refiere a la última vez que Cisco observó un dispositivo (por su número de serie) en función de la telemetría del dispositivo, los casos de soporte y las renovaciones de contratos; Los datos de telemetría de activos se ingieren y se enriquecen a través de un flujo de datos multicapa

Acceso al módulo Assets

Para acceder a las funciones de gestión de activos de Cisco IQ, seleccione el menú Inicio > Activos o haga clic en Activos de la sección Aplicación de la pestaña Página de inicio > Launchpad. Se muestra la página Descripción general.

Descripción general de activos

La página Descripción general muestra un panel que permite evaluar rápidamente el estado y el estado de los dispositivos.

100% 400 Assets 100% 400 Assets 100% 400 Assets



Assets



Overview



Inventory



Service Contracts



End of Life



Overview

Filters

Ask AI

Customize

Saved Filters

Total Assets

199

Assets

928

Assets and subcomponents

Key Asset Metrics

Covered Assets

186

Covered

93%

Of all assets

Uncovered Assets

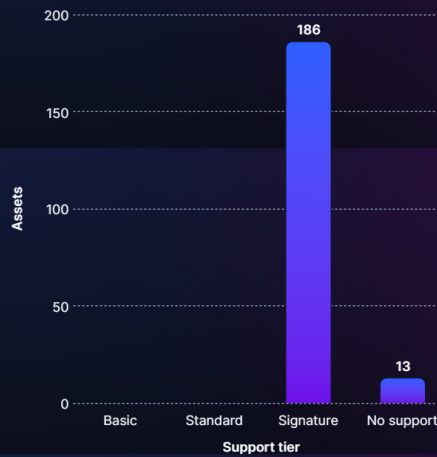
13

Uncovered

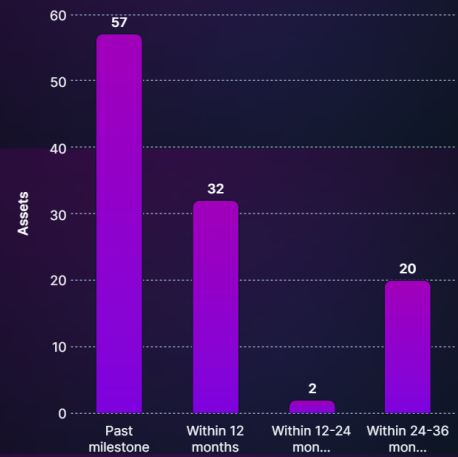
7%

Of all assets

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



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



Assets With Telemetry Enabled

186

With telemetry

93%

Of all assets

Assets Without Telemetry Enabled

13

Without telemetry

7%

Of all assets

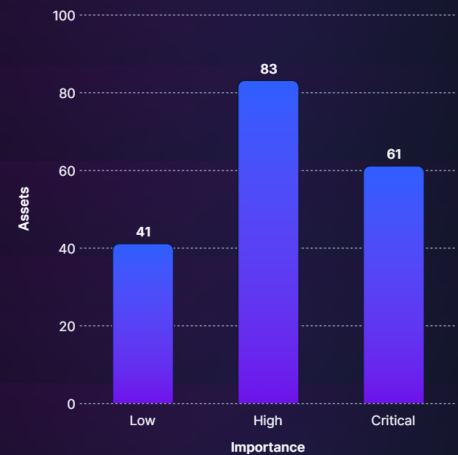
Assets With Critical or High Security Advisories [View details](#)



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

Assets by Importance [View details](#)

Importance can be evaluated for 185 assets.

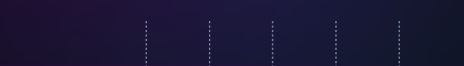


Asset Breakdown

Top 5 Product Families [View details](#)



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



Descripción general de activos

El panel muestra la siguiente información:

- **Activos totales:** El número total de recursos de la cuenta de Cisco IQ
- **Métricas de activos clave:** Métricas clave adicionales como el estado de la telemetría, los avisos de seguridad críticos y la información de LDOS
- **Activos cubiertos:** Número total y porcentaje de activos cubiertos por contratos de servicio
- **Activos no cubiertos:** Número total y porcentaje de activos no cubiertos por contratos de servicio
- **Activos cubiertos por contratos de servicio:** Un desglose del número de activos (hardware o software) que cubren los contratos de servicio, clasificados por nivel de derechos
- **Última fecha de instantánea de soporte técnico:** Desglose del número de activos que han superado la LDOS o han alcanzado la LDOS
- **Recursos con Telemetría Activada:** Número total y porcentaje de recursos con la telemetría habilitada
- **Activos sin Telemetría Activada:** Número total y porcentaje de recursos sin la telemetría habilitada
- **Activos con Asesores de Seguridad Críticos o de Alta Seguridad:** Porcentaje del total de recursos con la telemetría habilitada y que tienen recomendaciones de seguridad críticas o altas
- **Activos por importancia:** Desglose de la prioridad asignada a un dispositivo en relación con otros dispositivos de la red.
- **Desglose de activos:** Una visualización detallada de la información de activos, como familias de productos, ubicaciones de instalación, versiones de software y roles de activos

Filtrado de vistas de recursos

Puede filtrar la vista de panel seleccionando un filtro de las listas desplegables o haciendo clic en Filtros y eligiendo una opción de la lista de filtros disponibles.



Nota: Algunos filtros pueden estar ocultos en función de la configuración del zoom de la



pantalla. Hay distintos filtros disponibles en función de las funciones y los permisos del usuario.

Consulta de Detalles de Activos

Al hacer clic en Ver detalles, la página se redirige a la página Inventario. Consulte [Inventario](#) para obtener más información.

Perspectivas sobre la importancia de activos

Cisco IQ incluye Asset Criticality Insights, una nueva capacidad del módulo Assets que predice la función funcional y la importancia empresarial de los dispositivos de red. Al analizar las configuraciones de los dispositivos y las funciones habilitadas, Asset Criticality Insights le ayuda a identificar qué recursos tienen el mayor impacto en su red, por lo que puede priorizarlos para la remediación de la seguridad, las actualizaciones de software, la planificación del fin de vida útil (EOL) y las decisiones sobre la cobertura.



Nota: Asset Criticality Insights está disponible exclusivamente para recursos con niveles Standard o Signature que tienen conexiones de telemetría activas. Asegúrese de que sus recursos cumplen los requisitos de configuración para incluir estas perspectivas en el panel.

Asset Criticality Insights está disponible en la aplicación Assets en las siguientes áreas:

- Descripción general de activos: Filtrar y ver desgloses de resumen por atributos de Asset Criticality Insights
- Inventario de activos: Mostrar, buscar, filtrar y ordenar dispositivos por función e importancia
- Detalles de activos: Ver la función y la importancia de los dispositivos individuales, con consejos informativos que explican cada valor

Clasificaciones de importancia y función dominantes

Cisco IQ predice automáticamente la función y la importancia de cada recurso en función de los datos de telemetría. Los administradores de cuentas pueden corregir manualmente estas clasificaciones cuando la predicción automatizada no refleja con precisión la función o la importancia del activo en la red.



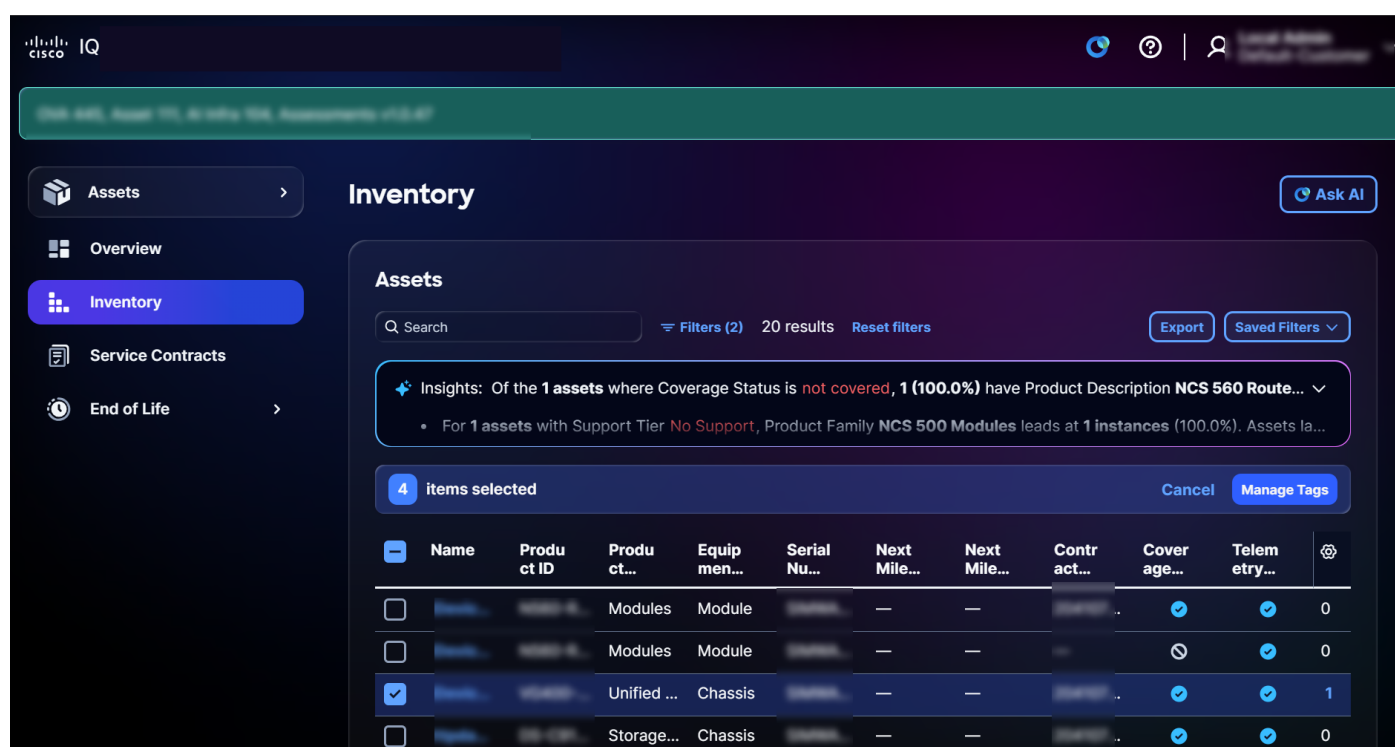
Nota: Los controles de sustitución solo están disponibles para los administradores de

 cuentas. Los valores Role e Importance son de sólo lectura para el resto de funciones de usuario.

Sustitución de Clasificaciones de la Tabla de Inventario

Para sustituir el rol o la importancia de uno o varios activos:

1. Navegue hasta Activos > Inventario.
2. Haga clic en la casilla de verificación de la fila de activos deseada. Para actualizar varios activos simultáneamente, active varias casillas de verificación.



The screenshot shows the Cisco IQ Inventory page. The left sidebar has a menu with 'Assets', 'Overview', 'Inventory' (selected), 'Service Contracts', and 'End of Life'. The main area is titled 'Inventory' and shows a table of assets. The table has columns: Name, Product ID, Product, Equipment, Serial Number, Next Mile, Next Mile, Contract, Coverage, Telemetry, and Importance. The table shows 4 items selected, and the Importance column has values 0, 0, 1, and 0.

	Name	Product ID	Product	Equipment	Serial Number	Next Mile	Next Mile	Contract	Coverage	Telemetry	Importance
☐			Modules	Module		—	—		✓	✓	0
☐			Modules	Module		—	—		⊘	✓	0
☒			Unified ...	Chassis		—	—		✓	✓	1
☐			Storage...	Chassis		—	—		✓	✓	0

Función e importancia

3. En la columna Rol o Importancia, elija el valor correcto en la lista desplegable de la fila de activos.
4. Haga clic en Apply para confirmar la invalidación.

Los activos con valores reemplazados manualmente muestran un indicador visual en la columna Función o Importancia.

 Nota: Para eliminar una sustitución configurada anteriormente y volver a la predicción



automatizada, seleccione la opción guión (—) en la lista desplegable Rol o Importancia.

Sustitución de Clasificaciones de Detalles de Activos

Para sustituir Rol o Importancia desde la vista de detalles de activos:

1. Navegue hasta Activos > Inventario y haga clic en un activo.
2. En el panel de detalles del activo, localice los campos Rol e Importancia.
3. Haga clic en la lista desplegable del campo que desea actualizar y seleccione el valor correcto.
4. Haga clic en Apply para confirmar.

La vista de detalle de un activo también muestra una explicación de los atributos de telemetría que informaron a la predicción automatizada original, para ayudar a determinar si una sustitución es adecuada.

Visualización de la Pista de Auditoría de Sustitución

Todas las sustituciones de funciones e importancia se registran en una pista de auditoría de nivel de cuenta. Para acceder a la pista de auditoría:

1. Seleccione Inicio > Configuración del sistema > Actividad y registros.
2. Elija Filters > Action Type > override para mostrar sólo eventos de sustitución.

La pista de auditoría muestra el nombre del activo, los valores anterior y nuevo, el usuario que realizó el cambio y la fecha y hora del cambio. La pista de auditoría se puede exportar mediante la opción Export.



Nota: La pista de auditoría se puede filtrar por intervalo de fechas, usuario y nombre de activo.

Inventario

La página Inventory proporciona una lista de todos los recursos de Cisco dentro de la cuenta de Cisco IQ.

Inventario

Búsqueda y Filtrado de Vistas de Inventario de Activos

Puede filtrar la vista de lista seleccionando un filtro de las listas desplegables o haciendo clic en Filtros y eligiendo una opción de la lista de filtros disponibles. También puede buscar activos introduciendo el nombre del activo en el campo Buscar.

 Nota:

- Algunos filtros pueden estar ocultos en función de la configuración del zoom de la pantalla.
- Hay distintos filtros disponibles en función de las funciones y los permisos del usuario.

Análisis de inventario

El panel Insights de la página Inventory muestra un análisis basado en la IA que proporciona un resumen de los recursos con un enfoque en la cobertura de soporte, conectividad e hitos. Haga clic en Análisis completo para obtener visualizaciones como gráficos, paneles y gráficos que proporcionan información adicional. Consulte [Análisis de Datos](#) en Funciones de Módulo Comunes para obtener más detalles.

Exportación de inventario

Haga clic en Exportar para guardar una lista de inventario filtrada en formato .xls o .csv. Consulte [Exportación de Información](#) en Funciones Comunes del Módulo para obtener más detalles.

Consulta de Detalles de Activos

Haga clic en un activo para ver sus detalles. Se muestra la vista detallada de un activo con las siguientes pestañas:

- Detalles: Muestra detalles de recursos como el producto, los datos de señal, la identidad, la ubicación, la garantía y la información de cobertura

Assets

Overview

Inventory

Service Contracts

End of Life

Inventory

10.197.238.131

Cisco Catalyst Center Appliance (Gen 2) - 44 Core

Details

Product Alerts

Hardware

Software

Product

Product ID

Product type

Product family

Last Date of Support

Identity

Serial number

IP address

Hostname

Software version

Role

Importance

Tags

Sold by

Location

Install-at

Signals

Last signal

Last signal type

Telemetry

Telemetry status

Last data collection

Data connector

Warranty

Warranty type

Warranty end date

Coverage

Coverage status

Contract number

Support tier

Coverage end date

Ask AI

Detalles de activos

- Alertas de productos: Muestra alertas de productos relacionados, como avisos de seguridad

y avisos de campo

- Hardware Proporciona una vista detallada de la fecha de finalización de la vida útil del hardware (por ejemplo, las fechas de fin de venta, último envío y última fecha de soporte).
- Software: Proporciona una vista detallada de la línea de tiempo para la EOL de software

Etiquetas de activos

Las etiquetas de activos son etiquetas personalizadas que se asignan a los activos de inventario en Cisco IQ. Una etiqueta es un par clave-valor (por ejemplo, Entorno:Producto o Etiqueta:Campus) que se define. Puede asignar etiquetas a activos individuales o a muchos activos a la vez, y puede filtrar su inventario por etiqueta para encontrar rápidamente los activos que le interesan.

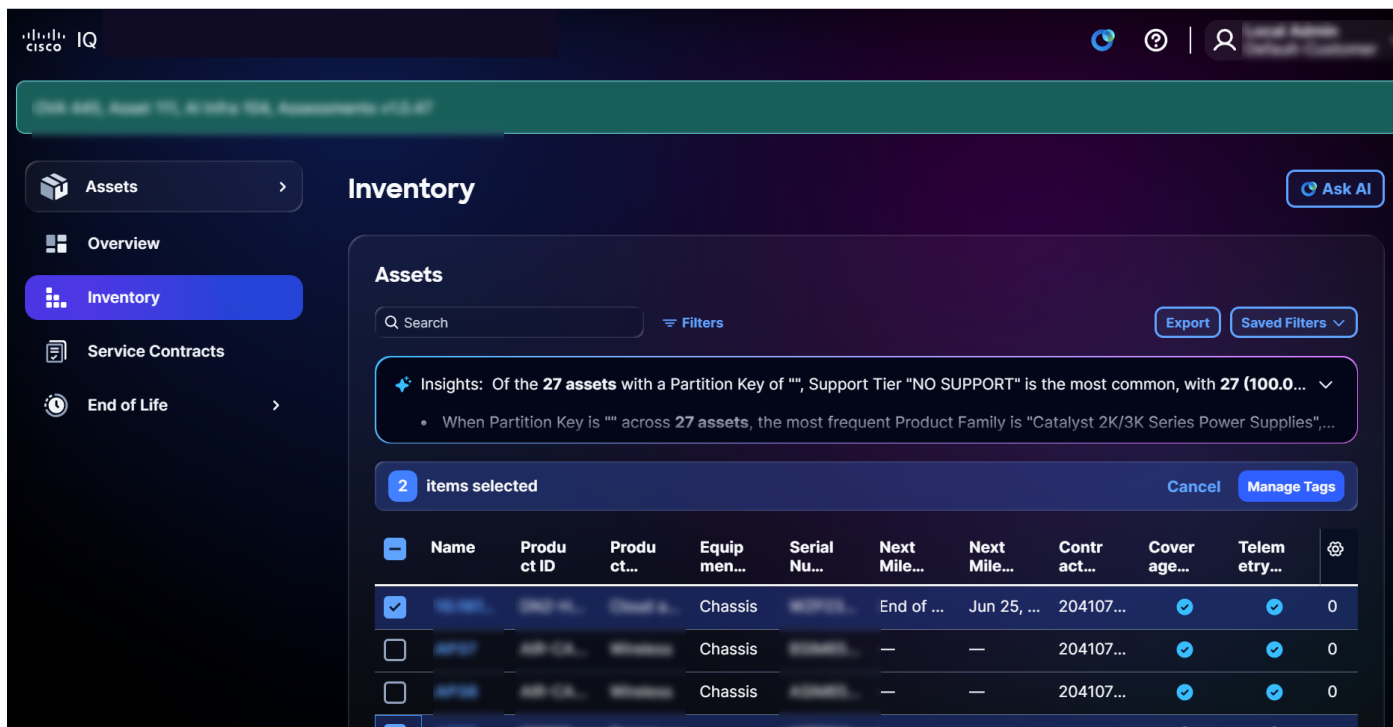
 Nota: Después de que un administrador de cuentas haya creado una etiqueta, los usuarios pueden asignar una etiqueta a un activo.

Asignación de etiquetas

La asignación de etiquetas a activos seleccionados en la vista Inventario permite la organización y categorización de activos para mejorar el filtrado, la generación de informes y la gestión.

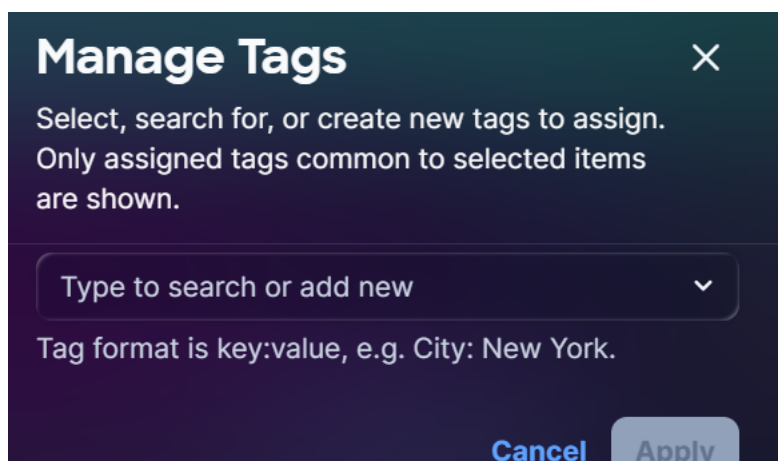
Para asignar una etiqueta a un activo:

1. Navegue hasta Activos > Inventario.



Etiquetado de recursos

2. Active las casillas de verificación de los activos deseados.
3. Haga clic en Administrar etiquetas. Se abre la ventana Administrar etiquetas.



Asignación de etiquetas

4. En el campo de texto, introduzca o seleccione el nombre de la etiqueta de las opciones existentes y pulse Intro.



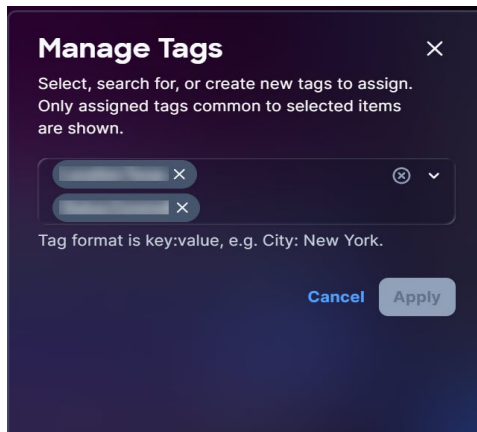
Nota: Las etiquetas tienen el formato clave:valor (por ejemplo, Ciudad:Nueva York).

5. Haga clic en Apply (Aplicar).

Eliminación de etiquetas de activos

Para eliminar una etiqueta de uno o varios activos:

1. Navegue hasta Activos > Inventario.
2. Active la casilla de verificación situada junto a uno o varios activos.
3. Haga clic en Administrar etiquetas. Se abrirá la ventana Administrar etiquetas.



Eliminación de etiquetas

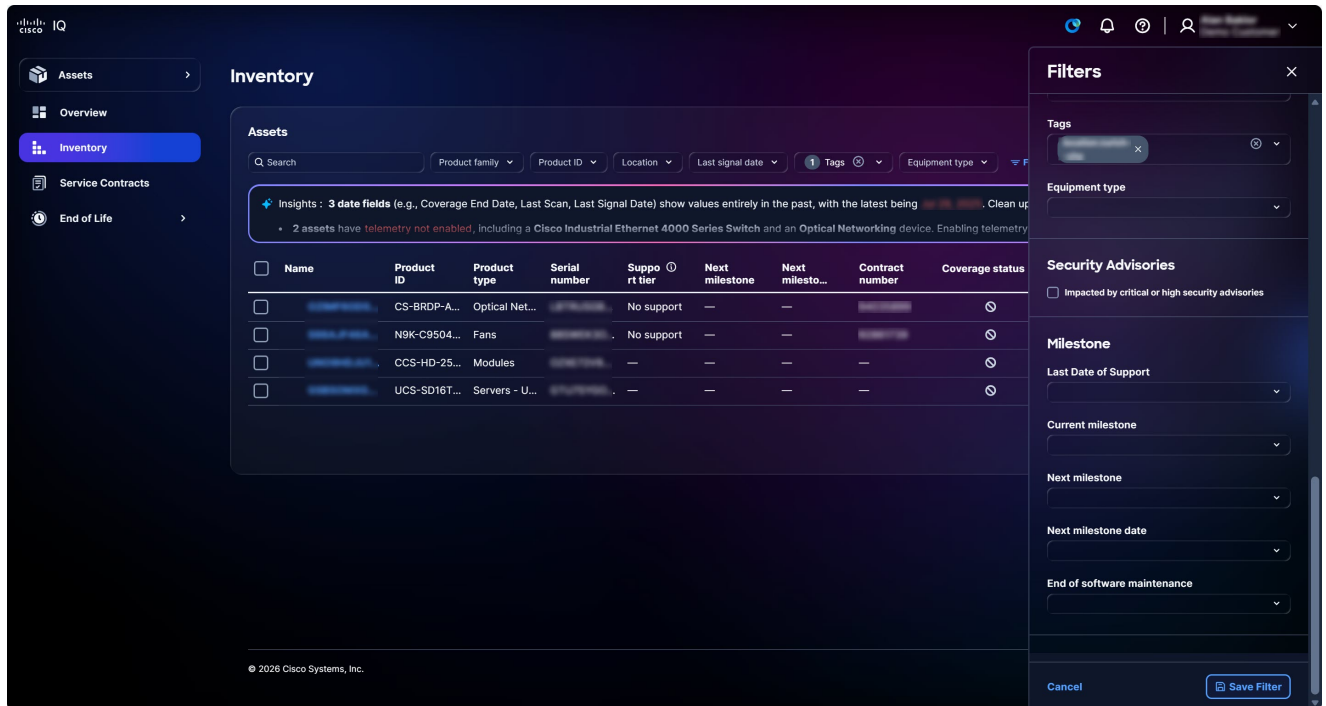
4. Haga clic en la X de cualquier etiqueta para quitarla de la selección.
5. Haga clic en Apply (Aplicar).

Uso de etiquetas de activos como filtros

Después de crear una etiqueta, puede utilizarla como filtro.

Para utilizar una etiqueta como filtro:

1. Navegue hasta la página Inventory.
2. Haga clic en Filtros. Se abre la ventana Filters.

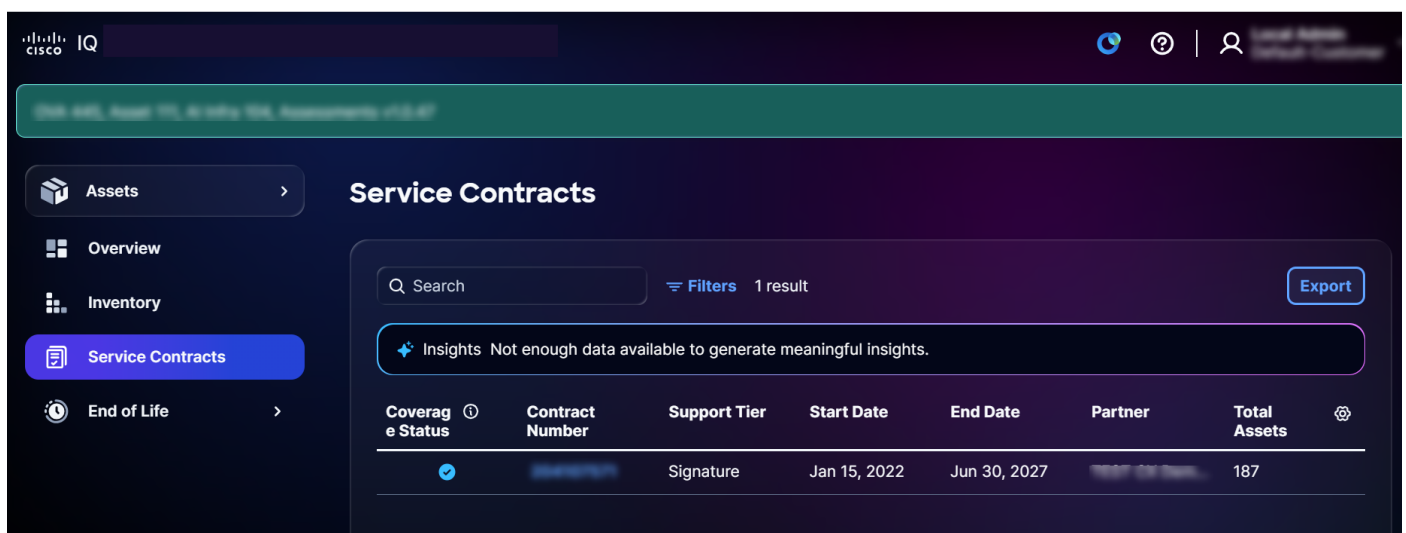


Utilizar etiqueta como filtro

3. En la lista desplegable Etiquetas, active las casillas de verificación de las etiquetas deseadas. Después de seleccionar la etiqueta, la vista de la página Inventario se actualiza a la vista filtrada.

Contratos de servicio

La página Contratos de servicio simplifica la supervisión de los contratos de soporte proporcionando resúmenes e información detallada sobre los contratos, apoyando una planificación eficaz de las renovaciones y estrategias de cobertura.



Contratos de servicio

Búsqueda y Filtrado de Vistas para Contratos de Servicio

Puede filtrar la vista de lista seleccionando un filtro de las listas desplegables. También puede buscar contratos de servicio introduciendo el número de contrato en el campo Buscar.

Exportación de contratos de servicio

Haga clic en Exportar para guardar una lista filtrada de contratos en formato .xls o .csv. Consulte [Exportación de Información](#) en Funciones Comunes del Módulo para obtener más detalles.

Resumen de EA de servicios

La página Resumen del acuerdo empresarial de servicios proporciona una vista consolidada del crecimiento de la base instalada en toda la cartera de activos. Los datos se obtienen directamente de los registros de la base instalada de Cisco, lo que le proporciona a usted y a sus equipos de cuentas una visión uniforme de los cambios de la cartera a lo largo del tiempo.

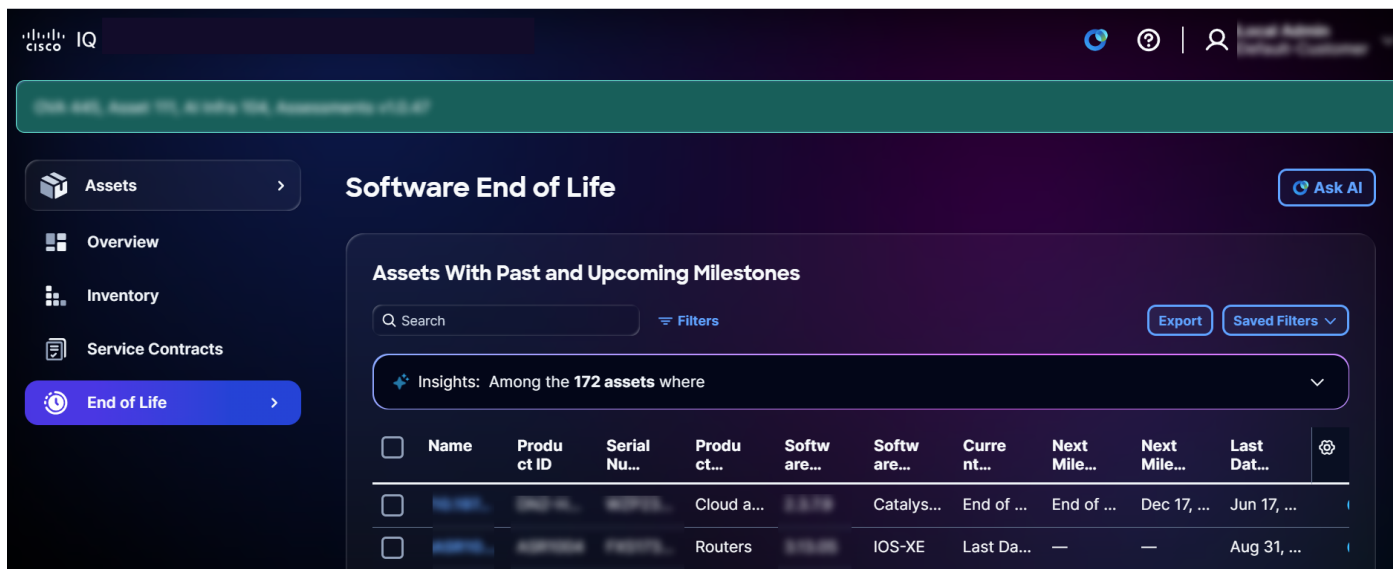
La página Resumen de EA de servicios muestra la siguiente información:

- Activos agregados: Nuevos activos añadidos a la base instalada durante el período de referencia
- Cambio neto: El cambio global en el tamaño de la base instalada para el período de informe

 Nota: El acceso a la página Resumen de EA de servicios puede estar sujeto a los requisitos de permisos y funciones. Póngase en contacto con el administrador de su cuenta si esta página no está visible en su sistema de navegación.

Fin de vida útil

Las páginas Fin de vida útil del hardware y Fin de vida útil del software proporcionan información detallada sobre la EOL, lo que proporciona a los usuarios el soporte necesario para gestionar proactivamente los ciclos de actualización de productos y la cobertura de soporte. Al hacer clic en un activo en las páginas Fin del ciclo de vida, se le redirigirá al activo correspondiente de la página Inventario.



Fin de vida útil del software

Análisis del fin del ciclo de vida

El panel Insights de la página End of Life muestra una descripción general de los recursos basada en IA con un Día final de soporte definido. Haga clic en Análisis completo para obtener visualizaciones como gráficos, paneles y gráficos que proporcionan información adicional. Consulte [Análisis de Datos](#) en Funciones de Módulo Comunes para obtener más detalles.

Exportación del fin de vida útil

Haga clic en Exportar para guardar una lista filtrada de activos en fase EOL en formato .xls o .csv. Consulte [Exportación de Información](#) en Funciones Comunes del Módulo para obtener más detalles.

Módulo de evaluaciones

El módulo Evaluaciones proporciona un marco de evaluación que le permite investigar y mitigar de forma proactiva los riesgos relacionados con la seguridad, la estabilidad, la capacidad, el cumplimiento y el envejecimiento, lo que mantiene las redes seguras, estables y fiables.

Conceptos básicos

El módulo Evaluaciones se basa en los siguientes conceptos básicos:

- **Evaluación:** Una evaluación sistemática de las entidades de infraestructura con respecto a criterios predefinidos para medir el rendimiento, el cumplimiento, la seguridad o la capacidad operativa; Las evaluaciones se activan a demanda, según una programación o por un evento
- **Ejecución de la evaluación:** Una instancia o una sola ejecución de una evaluación; Cada ejecución crea un nuevo registro de ejecución que realiza un seguimiento del alcance, el mecanismo de desencadenador, la marca de tiempo y los datos resultantes generados por la evaluación
- **Descubrimiento:** Una observación validada y procesable que identifica una brecha, riesgo, problema o estado notable. Los resultados representan los datos a nivel del suelo durante una evaluación
- **Perspectiva:** Conclusión analítica de nivel superior derivada de patrones o tendencias a través de múltiples hallazgos. Las perspectivas interpretan lo que significan las conclusiones en un contexto empresarial u operativo más amplio
- **Recomendación:** Una prescripción específica y procesable vinculada a hallazgos o percepciones; Las recomendaciones proporcionan una orientación clara sobre las medidas necesarias para abordar los problemas detectados o aprovechar las oportunidades
- **Informe:** Documento estructurado que agrega conclusiones, perspectivas y recomendaciones para un público objetivo; Los informes son el principal producto para comunicar los resultados de las evaluaciones a los clientes, ejecutivos y equipos técnicos

Acceso al módulo Evaluaciones

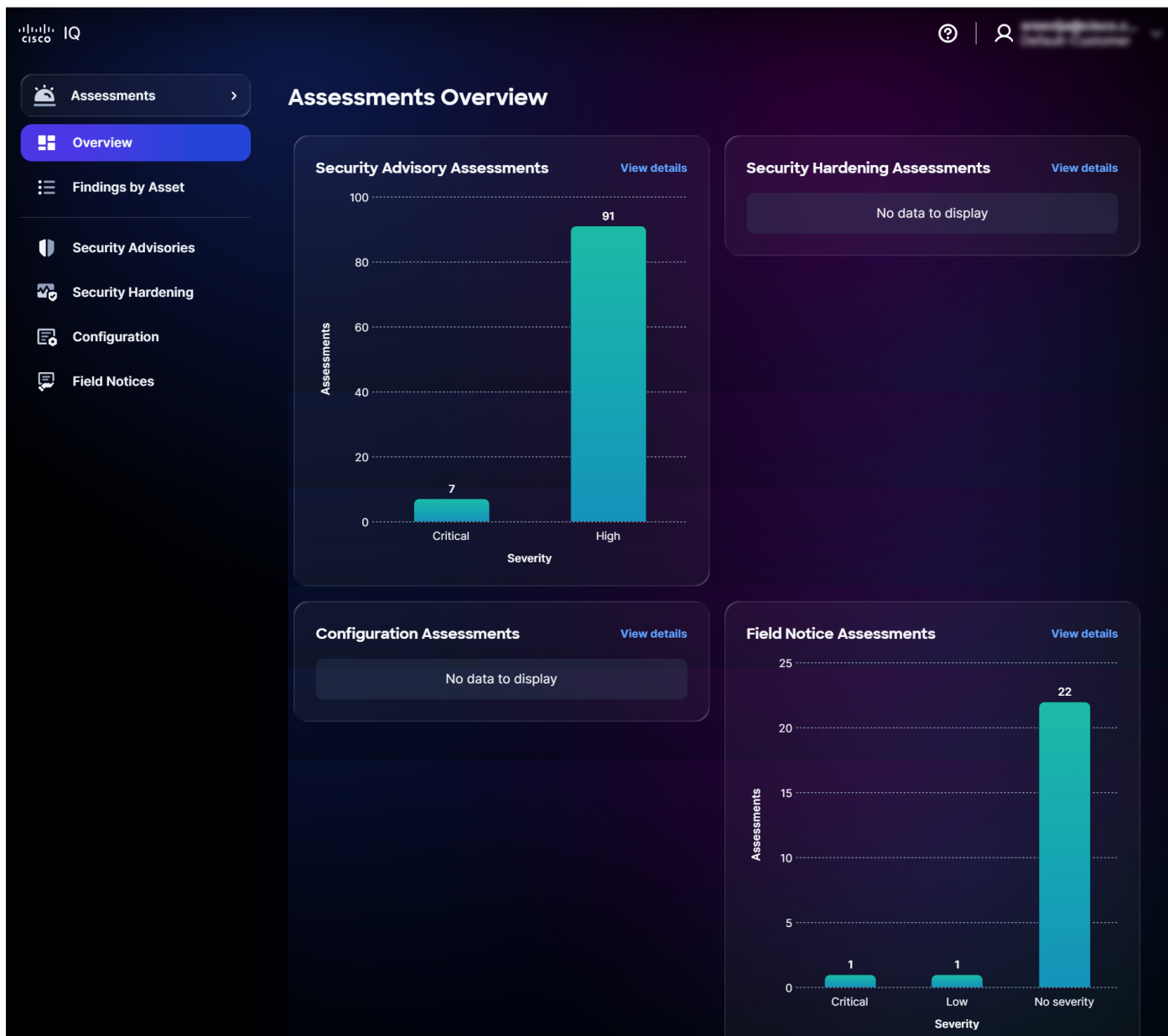
Para acceder a las funciones de seguridad y evaluación del dispositivo virtual, seleccione el menú Inicio > Evaluaciones o haga clic en Evaluaciones en la sección Aplicación de la pestaña Página de inicio > Launchpad. Se muestra la página Visión General de las Evaluaciones.



Nota: El módulo de evaluación también se puede iniciar desde System Configuration > Package Management.

Descripción general de evaluaciones

La página Descripción General de Evaluaciones muestra el siguiente panel:



Descripción general de evaluaciones

El panel muestra la siguiente información:

- **Evaluaciones de asesoría de seguridad:** Muestra las evaluaciones de los avisos de seguridad, categorizados por gravedad Crítica y Alta
- **Evaluaciones de refuerzo de la seguridad:** Muestra los activos que no cumplen las reglas de seguridad, clasificados por gravedad alta, media, baja e informativa
- **Evaluaciones de configuración:** Muestra los recursos que no cumplen las reglas de conformidad de la configuración, clasificados por gravedad crítica, alta, media, baja e informativa
- **Evaluaciones de avisos de campo:** Muestra las evaluaciones de los avisos de campo,

clasificados por gravedad crítica, alta y no aplicable



Nota: Solo puede ver los recursos a los que tiene derecho de acceso.

Conclusiones por activo

La página Conclusiones por Activo proporciona una lista de los activos que se han evaluado utilizando al menos una de las siguientes evaluaciones: Avisos de seguridad, refuerzo de la seguridad, avisos de configuración y avisos de campo.

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

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

Conclusiones Por Activos

Búsqueda y Filtrado de Vistas para Búsquedas por Activo

Puede filtrar la vista de lista seleccionando un filtro de las listas desplegables o haciendo clic en Filtros y eligiendo una opción de la lista de filtros disponibles. También puede buscar resultados por activo en el campo Buscar.



Nota:

- Algunos filtros pueden estar ocultos en función de la configuración del zoom de la pantalla.
- Hay distintos filtros disponibles en función de las funciones y los permisos del usuario.

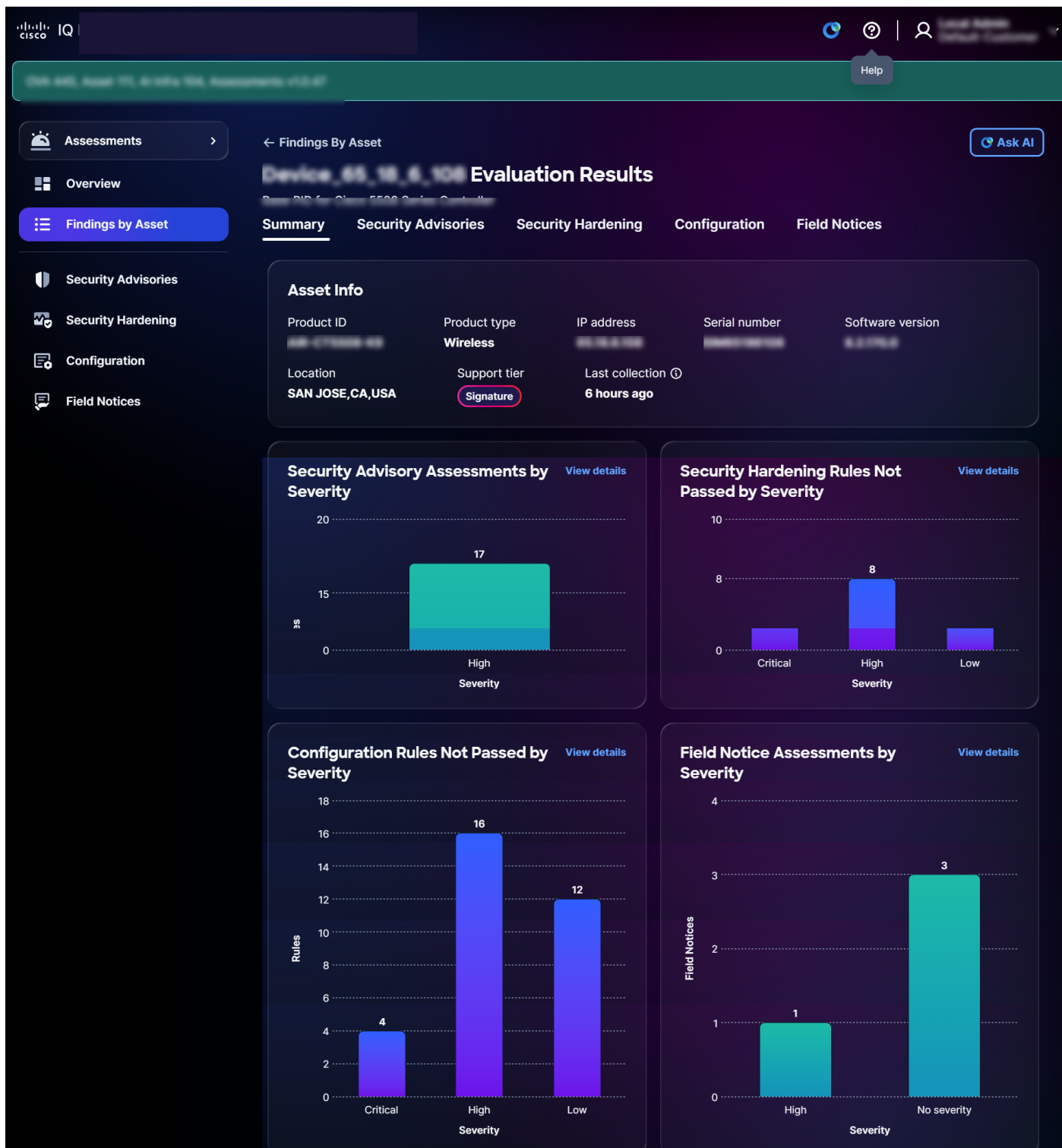
Exportación de Conclusiones por Activo

Para exportar las conclusiones por vista de lista de activos, haga clic en Exportar. Consulte [Exportación de información](#) para obtener más información.

Consulta de Conclusiones por Detalles de Activos

Para consultar las conclusiones por detalles de activos, haga clic en un activo. Las siguientes pestañas muestran los detalles del activo seleccionado:

- **Resumen** Proporciona información detallada sobre los recursos, incluido el número de avisos de seguridad, refuerzo de la seguridad, configuración y avisos prácticos
- **Avisos de seguridad:** Proporciona una lista de evaluaciones de asesoría de seguridad relacionadas.
- **Consolidación de la seguridad:** Proporciona una lista de activos que no cumplen las reglas de refuerzo de la seguridad
- **Configuración:** Proporciona una lista de los recursos que no cumplen las reglas de prácticas recomendadas de configuración
- **Avisos de problemas:** Proporciona una lista de evaluaciones de avisos de campo relacionadas



Conclusiones por detalles de activos

Al hacer clic en Ver detalles en un mosaico, la página se redirige a la página correspondiente dentro del módulo.

Al hacer clic en Ver detalles completos del activo, se muestra la página de vista detallada del activo.

Avisos de seguridad

Las evaluaciones de asesoría de seguridad identifican las vulnerabilidades y les asignan prioridades en función de su riesgo, gravedad y criticidad, con lo que se mejoran las capacidades de gestión de riesgos de la organización. Los consejos de seguridad ofrecen una perspectiva granular de las vulnerabilidades, ayudan a acelerar la mitigación de las amenazas críticas y garantizan la alineación con los objetivos empresariales y de cumplimiento. Esto refuerza la condición en materia de seguridad, optimiza la asignación de recursos y fomenta la resistencia frente a las amenazas en constante evolución en toda la empresa. Los avisos de seguridad se actualizan automáticamente en Cisco IQ en cuanto se publican.

La página Asesores de seguridad proporciona una lista de todos los asesores de seguridad con vulnerabilidades detectadas en la organización. Al hacer clic en un aviso de la lista de evaluaciones de asesoría de seguridad, se accede a la vista de detalle correspondiente.

Assessments
Overview
Findings by Asset
Security Advisories
Security Hardening
Configuration
Field Notices

Security Advisories

About the Assessments

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

Security Advisory Assessments

Filters 98 results
Export
Saved Filters

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

Avisos de seguridad

Búsqueda y filtrado de vistas para avisos de seguridad

Puede filtrar la vista de lista seleccionando un filtro de la lista desplegable. También puede buscar evaluaciones de asesoría de seguridad introduciendo el nombre de la evaluación en el campo Buscar.



Nota: Algunos filtros pueden estar ocultos en función de la configuración de zoom de la pantalla. Algunos filtros pueden estar ocultos en función de la configuración de zoom de la pantalla. Hay distintos filtros disponibles en función de las funciones y los permisos del usuario. Los valores de gravedad que faltan se muestran como "-" con un mensaje descriptivo.

Exportación de avisos de seguridad

Para exportar evaluaciones de Security Advisory, haga clic en Export. Consulte [Exportación de información](#) para obtener más información.

Consulta de Detalles de Evaluación de Asesoramiento de Seguridad

Haga clic en una evaluación para ver más detalles sobre ella. La página de detalles proporciona información como la puntuación del sistema de puntuación de vulnerabilidades habituales (CVSS), vulnerabilidades y exposiciones habituales (CVE), gravedad y un enlace al aviso de seguridad de Cisco al que se hace referencia.

Puede ver los siguientes tipos de resultados en la tabla Resultado de la evaluación:

- **Afectado:** Indica que el activo o componente tiene una vulnerabilidad confirmada que puede ser explotada por un atacante y que requiere remediación
- **Potencialmente afectados:** Indica que el activo o componente muestra signos que pueden dar lugar a una vulnerabilidad, pero no se ha confirmado definitivamente; puede ser necesario realizar más investigaciones

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

Asset Results

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

Detalles de avisos de seguridad

Búsqueda y filtrado de vistas para los resultados de la evaluación de activos

Puede filtrar la vista de lista seleccionando un filtro de las listas desplegadas o haciendo clic en Filtros y eligiendo una opción de la lista de filtros disponibles. También puede buscar activos introduciendo el nombre del activo en el campo Buscar.



Nota: Algunos filtros pueden estar ocultos en función de la configuración del zoom de la pantalla. Existen distintos filtros disponibles en función de las funciones y los permisos del usuario.

Consulta de Resultados de Evaluación de Activos

Para ver los detalles de un resultado de evaluación, haga clic en un activo de la tabla Resultado de la evaluación. Se muestra la página de detalles del resultado de la evaluación del activo.

Security Advisories > Cisco Secure Boot Hardware Tampering Vulnerability

Device_65_10_4_108 Result [Ask AI](#)

Assessment: Cisco Secure Boot Hardware Tampering Vulnerability

Result Details Potentially affected

Evidence

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

Additional Verification Needed

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

About the Assessment

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

[Show more](#)

Severity	CVE	CVSS score
High	65_10_4_108	6.7
First published	Last updated	
May 13, 2019	Nov 20, 2019	

References

[Security Advisory](#)

About the Asset [View evaluated asset](#)

Product ID	Product type	IP Address
65_10_4_108	Switches	10.10.10.10
Serial Number	Software version	Location
1010101010	10.10.10	SAN JOSE, CA, USA
Support tier		
Signature		

Detalles del resultado

Exportación de Resultados de Activos para Avisos de Seguridad

Para exportar resultados de activos, haga clic en Exportar. Consulte [Exportación de información](#) para obtener más información.

Refuerzo de seguridad

La protección de la seguridad proporciona una visibilidad automatizada y casi en tiempo real de la condición en materia de seguridad de su infraestructura de red mediante la evaluación continua de routers, switches y firewalls frente a los índices de referencia estándares del sector. Identifica lagunas en la configuración y proporciona una guía de remediación procesable, lo que permite a los administradores de cuentas reducir de forma eficaz la superficie de ataque y mantener una alineación coherente con las rigurosas prácticas

recomendadas de seguridad de Cisco. Al centralizar la supervisión del cumplimiento y simplificar el proceso de consolidación, el módulo transforma la gestión de la seguridad de una tarea reactiva en una estrategia proactiva basada en datos, lo que garantiza una red empresarial resistente y segura.

 **Nota:** Las evaluaciones de refuerzo de la seguridad están disponibles exclusivamente para los recursos con niveles de asistencia estándar.

Visualización de evaluaciones de refuerzo de seguridad

La página Evaluación de Consolidación de la Seguridad muestra la siguiente información:

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Security Hardening Assessment

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

About the Assessment

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

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

Summary

Rule evaluations

179

Assets included

146

Rule evaluations

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

Q Search

Filters

179 results

Export

Saved Filters

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

Refuerzo de seguridad

- **Acerca de la evaluación:** Proporciona detalles adicionales al resumir el propósito de la evaluación
- **Resultado de la ejecución:** Proporciona un resumen de los resultados de la evaluación de activos, incluido el número total de evaluaciones de reglas y activos incluidos
- **Evaluaciones de reglas:** Proporciona información detallada sobre la regla, incluidos Gravedad, Activos evaluados, No aprobado, Aprobado, No concluyente, No aplicable y Tipo de software

- Gravedad: Proporciona el nivel de importancia o impacto de la evaluación de reglas
- Recursos evaluados: Proporciona el número total de activos evaluados según los criterios de la regla
- No pasó: Proporciona los recursos que no cumplieron los criterios de la regla durante la evaluación
- Aprobado: Proporciona los recursos que cumplen los criterios de la regla durante la evaluación.
- No concluyente: Proporciona los recursos para los que la evaluación no pudo determinar el error
- No aplicable: Indica los activos o escenarios en los que la regla no se aplica o no es relevante
- Tipo de software: Proporciona el tipo de software de los recursos

Búsqueda y filtrado de vistas para reglas

Puede filtrar la vista de lista seleccionando un filtro de las listas desplegables o haciendo clic en Filtros y eligiendo una opción de la lista de filtros disponibles. También puede buscar una regla introduciendo el nombre de la regla en el campo Buscar.



Nota: algunos filtros pueden estar ocultos en función de la configuración del zoom de la pantalla. Hay distintos filtros disponibles en función de las funciones y los permisos del usuario.

Consulta de Detalles de Evaluación de Reglas

Para ver detalles adicionales sobre una evaluación de regla, haga clic en una regla. Se muestra la página de detalles de evaluación de la regla con la siguiente información:

The screenshot shows the Cisco IQ interface for a Security Hardening Assessment. The main title is 'Minimum Password Length Policy', evaluated on Jul 20, 2026, at 5:39 AM. The interface includes a sidebar with navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening (selected), Configuration, and Field Notices. The main content area is divided into three sections: 'About the Rule', 'Results Summary', and 'Asset Results'.

About the Rule: Check 'Min. Password length' in show switch config, and warn if it is lower than 8. Proper security configuration protects the wireless infrastructure from unauthorized access, data interception, and compliance violations. Severity: High (High icon). Software type: AireOS. Assets evaluated: 31.

Results Summary: 31 assets. 0 Passed (Passed icon), 31 Didn't pass (Didn't pass icon), 0 Inconclusive (Inconclusive icon), 0 Not applicable (Not applicable icon).

Asset Results: 31 results. Search bar, Filters, Export, and Saved Filters (dropdown) are available. The table below shows the results for the first five assets.

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

Vista de reglas

- **Acerca de la regla:** Proporciona detalles acerca de la regla como Gravedad, Tipo de software, Versión y Activos evaluados e incluye vínculos descriptivos etiquetados a la documentación de origen relevante
- **Resumen de resultados:** Proporciona un resumen de los resultados de los activos relacionados con la regla, como Aprobado, No aprobado, No concluyente y No aplicable
- **Resultados de activos:** Proporciona una lista de recursos con detalles como el activo, el resultado, la ID del producto, el número de serie, la dirección IP y el nivel de asistencia.

 **Nota:** Cisco IQ proporciona una orientación clara cuando una conclusión de la evaluación es "no concluyente", explicando la causa (por ejemplo, falta telemetría o SO no compatible) y recomendando pasos como la verificación de la recopilación de datos, la actualización de credenciales o la actualización de datos. También se proporcionan enlaces con etiquetas a la documentación relevante para ayudar a resolver problemas.

Búsqueda y Filtrado de Vistas para Reglas de Activos

Puede filtrar la vista de lista seleccionando un filtro de las listas desplegables o haciendo clic en Filtros y eligiendo una opción de la lista de filtros disponibles. También puede buscar resultados de evaluaciones de activos introduciendo el nombre del activo en el campo Buscar.



Nota: algunos filtros pueden estar ocultos en función de la configuración del zoom de la pantalla. Hay distintos filtros disponibles en función de las funciones y los permisos del usuario.

Exportación de resultados de activos

Para exportar los resultados de evaluación de las reglas, haga clic en Exportar. Consulte [Exportación de información](#) para obtener más información.

Búsqueda y Filtrado de Vistas para Resultados de Activos

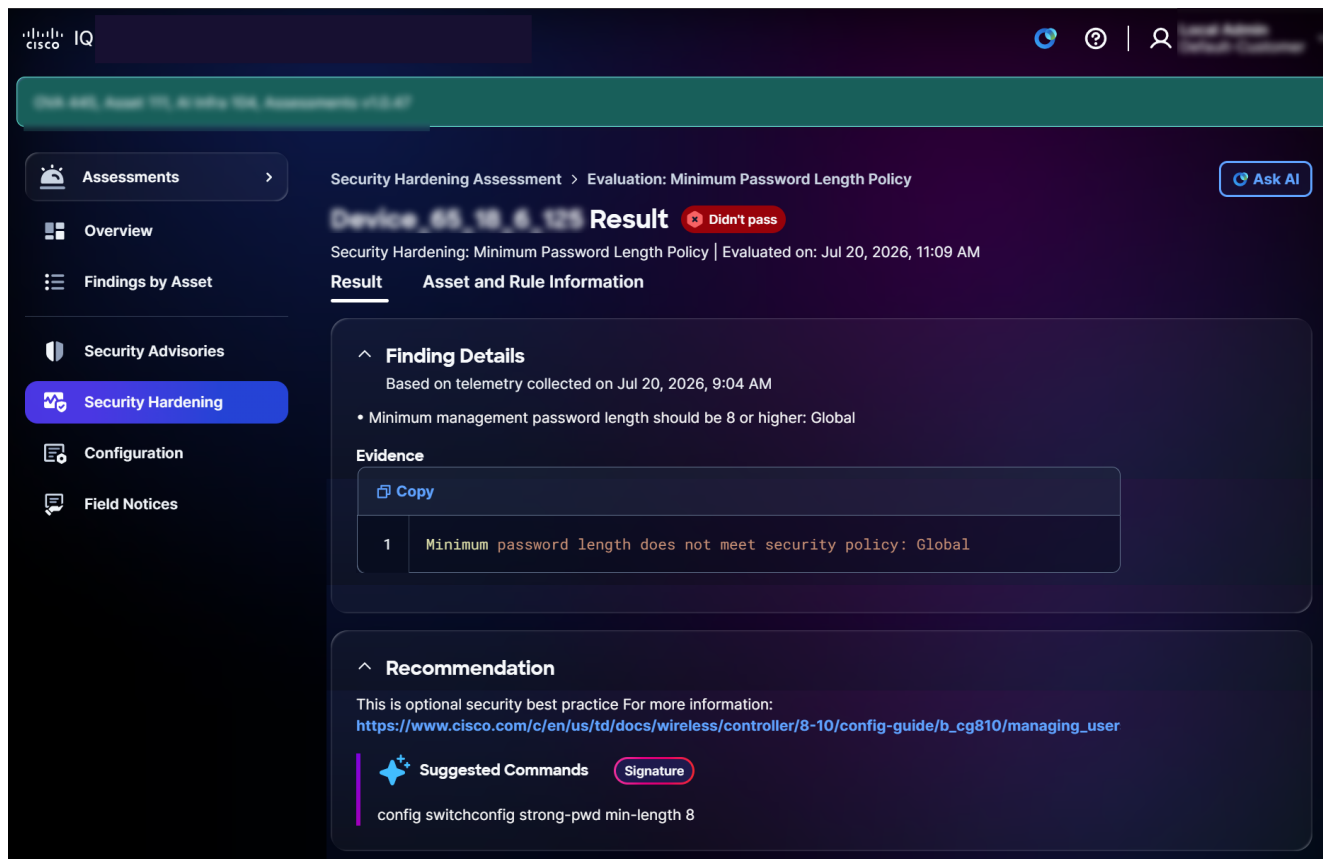
Puede filtrar la vista de lista seleccionando un filtro de las listas desplegables o haciendo clic en Filtros y eligiendo una opción de la lista de filtros disponibles. También puede buscar resultados de activos introduciendo el nombre del activo en el campo Buscar.



Nota: Algunos filtros pueden estar ocultos en función de la configuración del zoom de la pantalla. Hay distintos filtros disponibles en función de las funciones y los permisos del usuario.

Consulta de Resultados de Activos para Consolidación de Seguridad

Haga clic en un activo de Resultados de Activos para ver sus detalles. La página de detalles de resultados del activo muestra información según su nivel o nivel de derechos.



Nivel estándar de refuerzo de seguridad

- Nivel estándar
- Búsqueda de detalles: Proporciona información sobre las desviaciones de la configuración identificadas durante la evaluación, junto con registros de pruebas
- Recomendaciones: Proporciona orientación para abordar las conclusiones y garantizar la coherencia de la configuración

Consulta de Información de Activos y Reglas para la Consolidación de la Seguridad

Para ver los detalles de un activo y sus reglas, haga clic en la pestaña Información de activo y regla. Se muestra la página Información de activo y regla.

Acerca del activo: Proporciona los detalles del recurso, como la ID del producto, el tipo de producto, la dirección IP, el número de serie, la versión del software, la ubicación y el nivel de asistencia.

- Acerca de la regla: Proporciona detalles de la regla (incluidos Gravedad y Tipo de software) y la importancia de esa verificación de endurecimiento en particular

Configuración

Las evaluaciones de configuración evalúan sus recursos frente a las prácticas recomendadas basadas en la experiencia demostrada de Cisco para detectar desviaciones

de la configuración que puedan afectar a la disponibilidad, la seguridad o el rendimiento de su infraestructura. Cada regla de prácticas recomendadas se evalúa en todos los activos cubiertos y se asigna prioridad a las conclusiones en función de su gravedad para garantizar la coherencia de la configuración, una mayor resistencia y una reducción del riesgo operativo.

 Nota: Las evaluaciones de configuración están disponibles exclusivamente para los recursos con niveles de soporte estándar.

Visualización de evaluaciones de configuración

La página Evaluación de Configuración muestra la siguiente información:

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Configuration Assessment

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

About the Assessment

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

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

Summary

Rule evaluations

729

Assets included

146

Rule Evaluations

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

Search

Filters

729 results

Export

Saved Filters

Rule	Severity	Assets	Did Not...	Passed	Inconclus...	Not...	Category
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless
Console Memory Reservation	Medium	6	0	0	6	0	Platform
SSH Server Logging	Medium	10	9	0	0	1	Logging

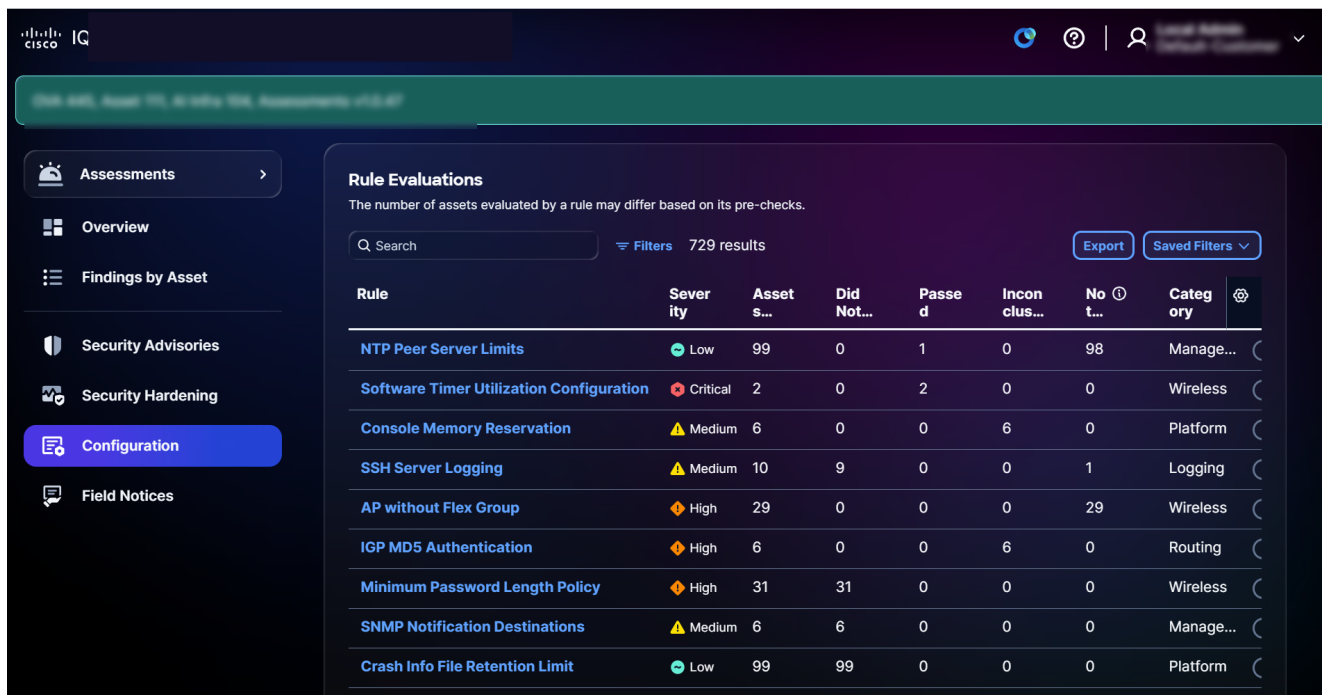
Evaluación de configuración

- Acerca de la evaluación: Proporciona detalles adicionales al resumir el propósito de la evaluación
- Resumen Proporciona un resumen de la ejecución de la configuración, como Reglas evaluadas y Activos evaluados
- Datos: Proporciona información sobre las lagunas de configuración identificadas

generadas a través del análisis de patrones y una correlación de los hallazgos; se muestran como tarjetas clave agrupadas de forma inteligente para resaltar las áreas más críticas que requieren atención

- **Evaluaciones de reglas:** Proporciona información detallada sobre la regla, incluidos Gravedad, Activos evaluados, No aprobado, Aprobado, No concluyente, No aplicable, Categoría y Tipo de software
- **Gravedad:** Proporciona el nivel de importancia o impacto de la evaluación de reglas
- **Recursos evaluados:** Proporciona el número total de activos evaluados según los criterios de la regla
- **No pasó:** Proporciona el número total de activos que no cumplieron los criterios de la regla durante la evaluación
- **No concluyente:** Proporciona el número total de activos para los que no se pudo ejecutar la evaluación
- **Aprobado:** Proporciona los recursos que cumplen los criterios de la regla durante la evaluación.
- **No aplicable:** Indica los activos o escenarios en los que la regla no se aplica o no es relevante
- **Categoría:** Proporciona el área de dominio a la que pertenece la regla
- **Tipo de software:** Indica el tipo de activos de software a los que se aplica la regla

Búsqueda y filtrado de vistas para reglas



The screenshot shows the Cisco IQ interface for Rule Evaluations. The left sidebar contains navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (highlighted), and Field Notices. The main content area displays a table of rule evaluations with the following columns: Rule, Severity, Asset Count, Did Not Pass, Passed, Inconclusive, Not Applicable, and Category. The table lists 10 rules, including NTP Peer Server Limits, Software Timer Utilization Configuration, Console Memory Reservation, SSH Server Logging, AP without Flex Group, IGP MD5 Authentication, Minimum Password Length Policy, SNMP Notification Destinations, and Crash Info File Retention Limit. Each rule entry includes a severity indicator (Low, Medium, High, Critical) and a count for each evaluation status.

Rule	Severity	Asset Count	Did Not Pass	Passed	Inconclusive	Not Applicable	Category
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless
Console Memory Reservation	Medium	6	0	0	6	0	Platform
SSH Server Logging	Medium	10	9	0	0	1	Logging
AP without Flex Group	High	29	0	0	0	29	Wireless
IGP MD5 Authentication	High	6	0	0	6	0	Routing
Minimum Password Length Policy	High	31	31	0	0	0	Wireless
SNMP Notification Destinations	Medium	6	6	0	0	0	Manage...
Crash Info File Retention Limit	Low	99	99	0	0	0	Platform

Evaluaciones de reglas

Puede filtrar la vista de lista seleccionando un filtro de las listas desplegadas o haciendo clic en Filtros y eligiendo una opción de la lista de filtros disponibles. También puede buscar una regla introduciendo el nombre de la regla en el campo Buscar.



Nota: Algunos filtros pueden estar ocultos en función de la configuración del zoom de la pantalla. Hay distintos filtros disponibles en función de las funciones y los permisos del usuario.

Consulta de Detalles de Evaluación de Reglas

Para ver detalles adicionales sobre una evaluación de regla, haga clic en cualquier regla. Se muestra la página de detalles de evaluación de la regla con la siguiente información:

The screenshot shows the Cisco IQ interface for a Configuration Assessment titled "NTP Peer Server Limits". The page is evaluated on Jul 20, 2026, at 5:40 AM. It includes a sidebar with navigation options like Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration, and Field Notices. The main content area shows details about the rule, including its severity (Low), category (Management), software type (IOS-XE), and the number of assets evaluated (99). A Results Summary section displays counts for Passed (1), Didn't pass (0), Inconclusive (0), and Not applicable (98). Below this is an Asset Results table with columns for Asset, Result, Product ID, Serial Number, IP Address, and Support Tier. The table shows several rows where the result is "Not applicable" and the support tier is "Signature".

Asset	Result	Product ID	Serial Number	IP Address	Support Tier
...	Not applicable	...	...	...	Signature
...	Not applicable	...	...	...	Signature
...	Not applicable	...	...	...	Signature
...	Not applicable	...	...	...	Signature

Evaluación

- Acerca de la regla: Proporciona detalles sobre una regla como Gravedad, Categoría, Tipo de software y Activos evaluados e incluye enlaces descriptivos con etiquetas a la documentación de origen relevante
- Resumen de resultados: Proporciona resultados generales de los recursos mostrando el número de recursos en los estados Aprobado, No pasó, No concluyente y No aplicable.

- Resultados de activos: Proporciona una lista de los activos afectados por la regla seleccionada con el estado de resultados



Nota: Cisco IQ proporciona una orientación clara cuando una conclusión de la evaluación es "no concluyente", explicando la causa (por ejemplo, falta telemetría o SO no compatible) y recomendando pasos como la verificación de la recopilación de datos, la actualización de credenciales o la actualización de datos. También se proporcionan enlaces con etiquetas a la documentación relevante para ayudar a resolver problemas. El módulo de evaluación admite la selección de varias categorías de reglas, lo que permite el procesamiento y la evaluación simultáneos en varias categorías de reglas.

Exportación de resultados de activos

Para exportar los resultados de los activos de las reglas, haga clic en Exportar. Consulte [Exportación de información](#) para obtener más información.

Búsqueda y Filtrado de Vistas para Resultados de Activos

Puede filtrar la vista de lista seleccionando un filtro de las listas desplegadas o haciendo clic en Filtros y eligiendo una opción de la lista de filtros disponibles. También puede buscar resultados de activos introduciendo el nombre del activo en el campo Buscar.

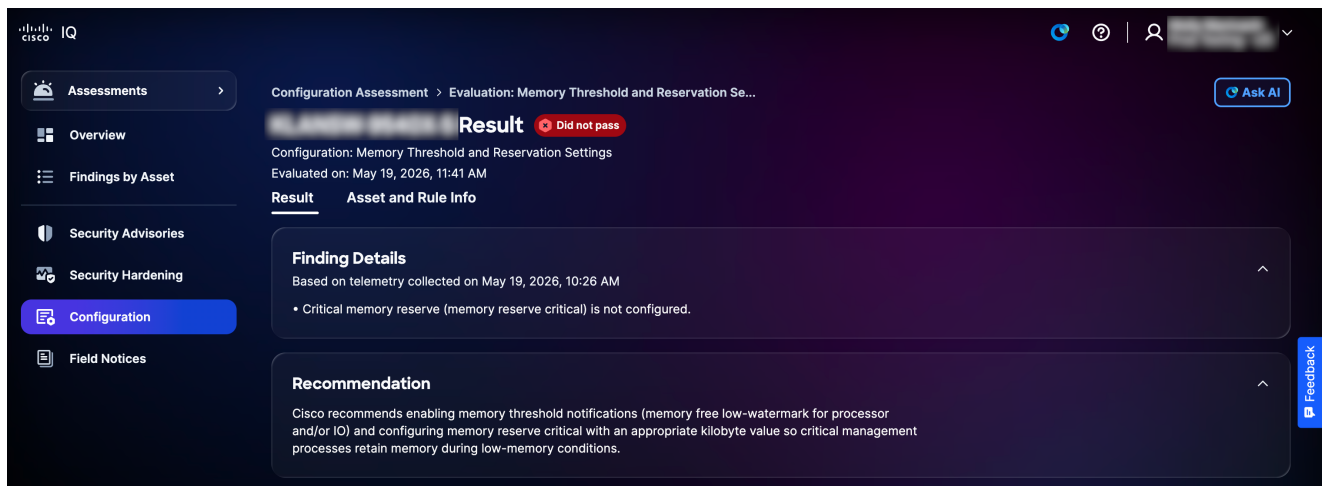


Nota: Algunos filtros pueden estar ocultos en función de la configuración del zoom de la pantalla. Hay distintos filtros disponibles en función de las funciones y los permisos del usuario.

Consulta de Resultados de Activos para Evaluaciones de Configuración

Para consultar los detalles de los resultados de los activos, pulse un activo en los resultados de activos.

La página de detalles de resultados del activo muestra información según su nivel o nivel de derechos.

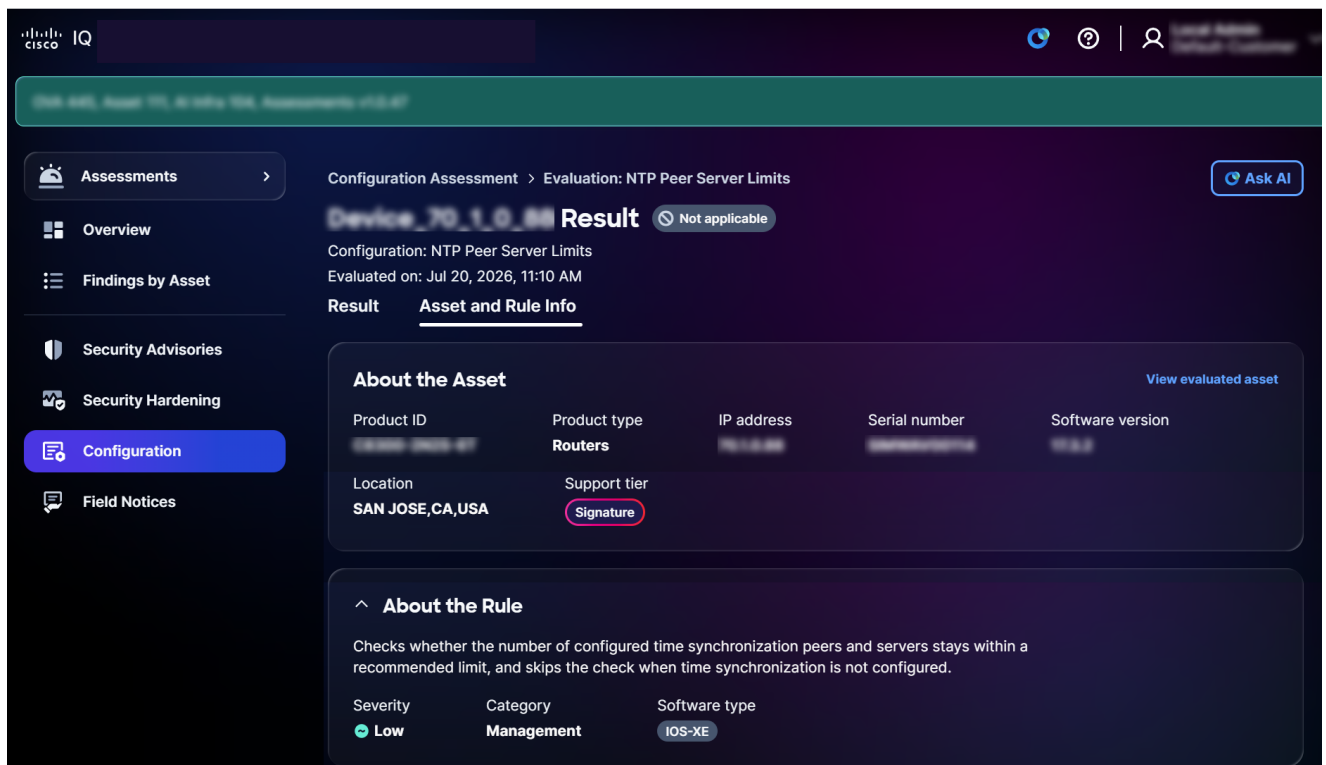


Nivel estándar de configuración

- Nivel estándar
- Búsqueda de detalles: Proporciona información sobre las desviaciones de la configuración identificadas durante la evaluación, junto con registros de pruebas
- Recomendaciones: Proporciona orientación para abordar las conclusiones y garantizar la coherencia de la configuración

Consulta de Información de Activos y Reglas para Evaluaciones de Configuración

Para ver los detalles de información de activos y reglas, haga clic en la pestaña Información de activo y regla.



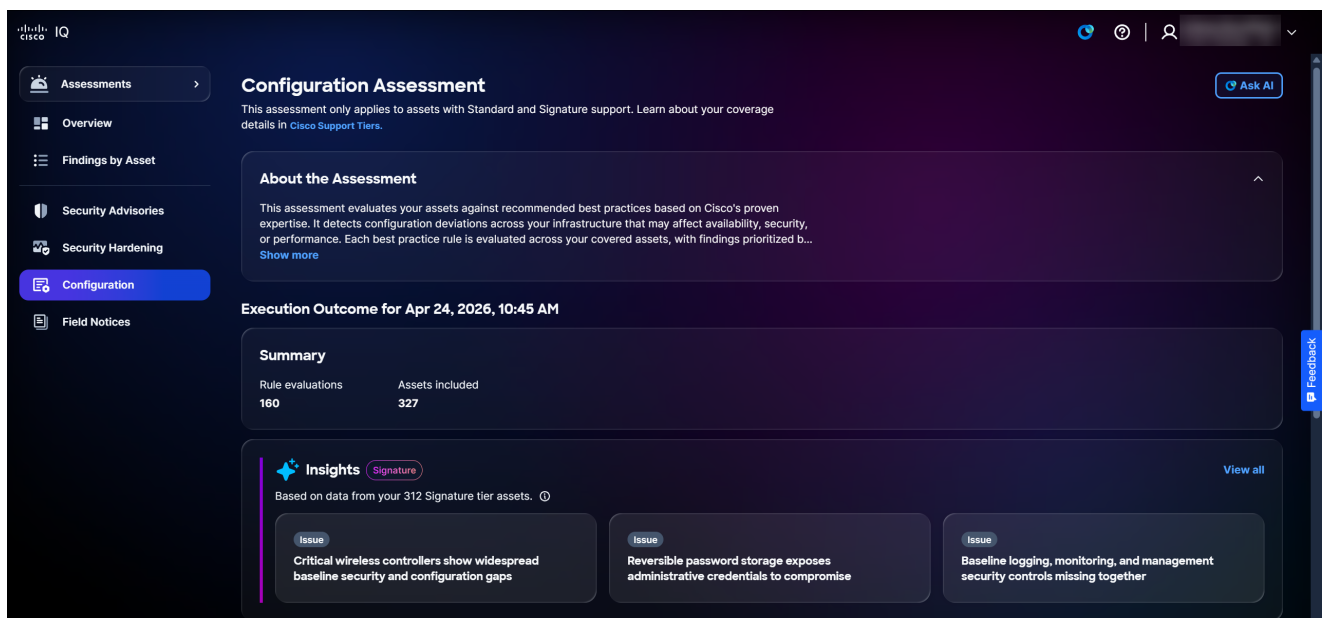
Información de regla y activo

La página Información de Activo y Regla se muestra con la siguiente información:

- Acerca del activo: Proporciona los detalles de un recurso, como la ID de producto, el tipo de producto, la dirección IP, el número de serie, la versión de software, la ubicación y el nivel de asistencia.
- Acerca de la regla: Proporciona detalles de una regla como Gravedad, Categoría y Tipo de software

Visualización de perspectivas

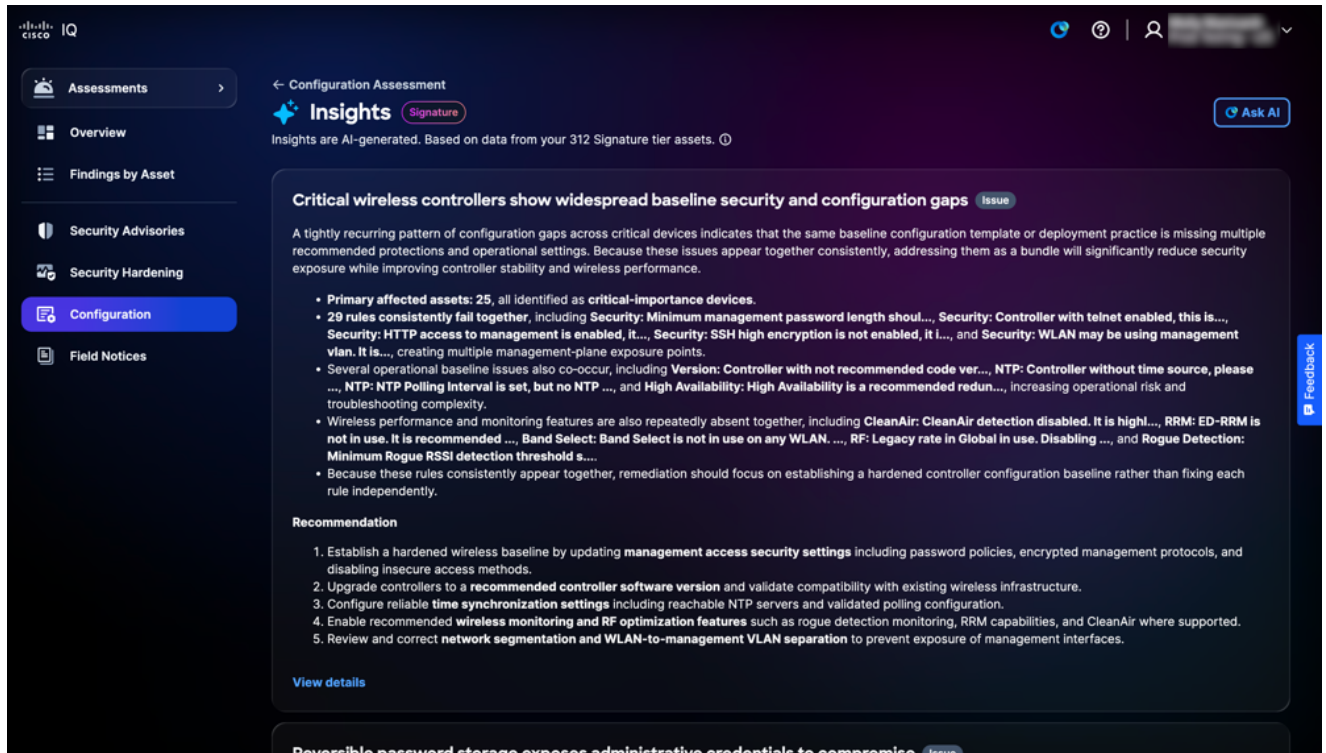
Las perspectivas son generadas por IA y sirven como panel inteligente que sintetiza los datos de evaluación en tarjetas clave con prioridad, lo que pone de relieve las disparidades de configuración críticas entre varias conclusiones. Le permite abordar los riesgos más importantes de la infraestructura de forma eficaz centrándose en estas áreas urgentes. También destaca los puntos fuertes identificando las áreas en las que su infraestructura está funcionando bien, según las prácticas recomendadas.



Perspectivas

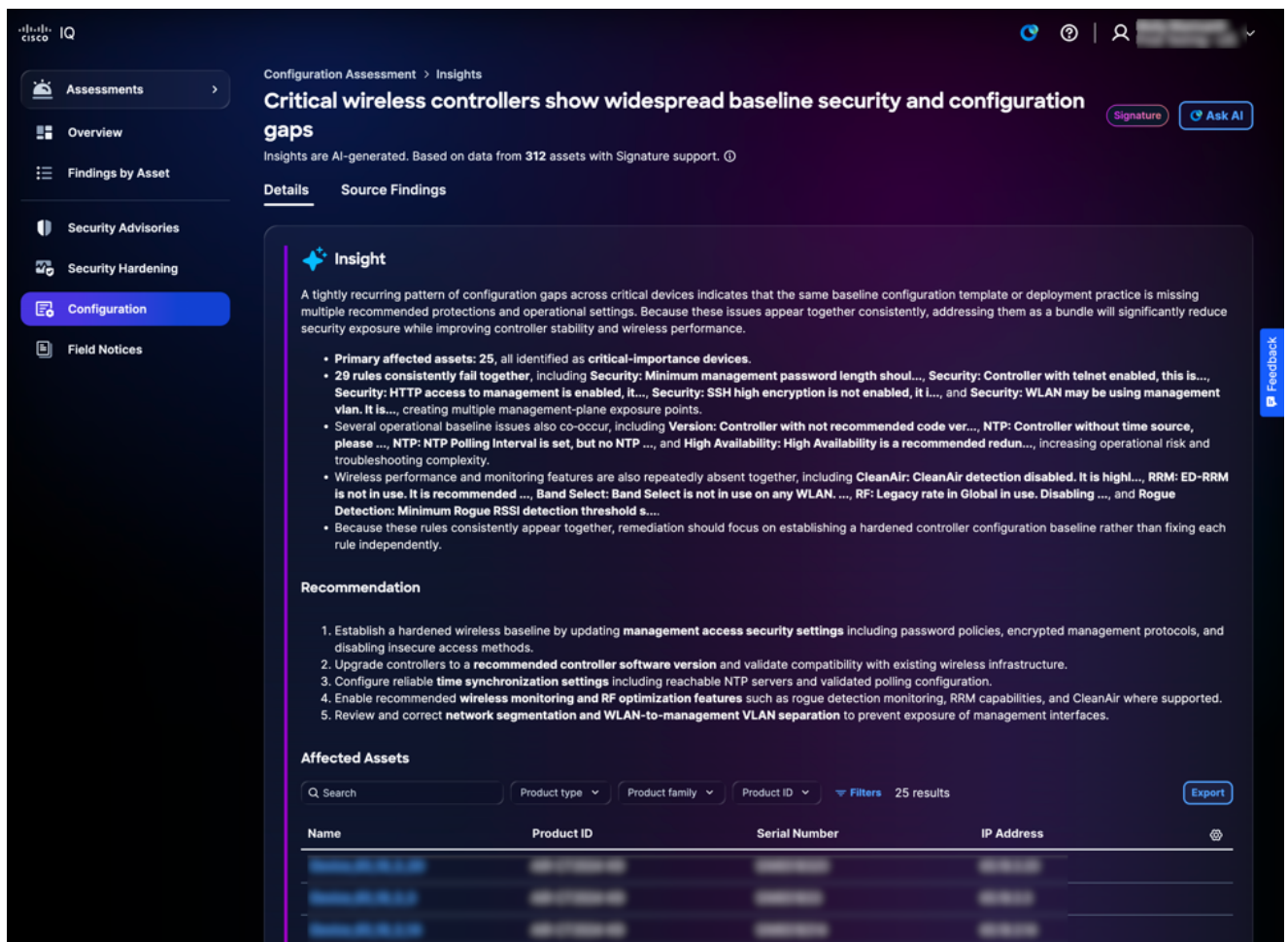
Para ver detalles de Insights:

1. En el panel Perspectivas, haga clic en Ver todo. La página Insights muestra todas las insights.



Página Perspectivas

- Haga clic en Ver detalles o en cualquier tarjeta. Se muestra la página de detalles de Insights con la siguiente información:



Detalles de Insights

- **Perspectiva:** Proporciona un resumen que resalta los patrones recurrentes de desviaciones de configuración identificadas a través de un análisis exhaustivo de varias conclusiones, así como las áreas de excelencia de su infraestructura en las que las configuraciones se alinean con las prácticas recomendadas
- **Recomendación:** Proporciona pasos procesables para remediar las brechas de configuración identificadas
- **Recursos afectados:** Proporciona una lista de dispositivos específicos en los que se ha identificado la desviación de la configuración según se define en la sección Insight.

3. Haga clic en Source Findings. La página Conclusiones de Origen muestra las conclusiones individuales detalladas que respaldan sus conclusiones.

The screenshot displays the Cisco IQ Configuration Assessment Insights page. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (highlighted), and Field Notices. The main content area shows the 'Configuration Assessment > Insights' section. A title reads 'Critical wireless controllers show widespread baseline security and configuration gaps'. Below the title, it states 'Insights are AI-generated. Based on data from 312 assets with Signature support.' The 'Source Findings' tab is active, showing a table with 725 results. The table has columns for Asset, Rule, Severity, Serial Number, and Result. The first few rows show rules related to 'High Availability: High Availability' with a severity of 'Low' and a result of 'Did not pass'.

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

Conclusiones de origen

Puede filtrar la vista de tabla seleccionando un filtro de las listas desplegables Gravedad y Resultado.

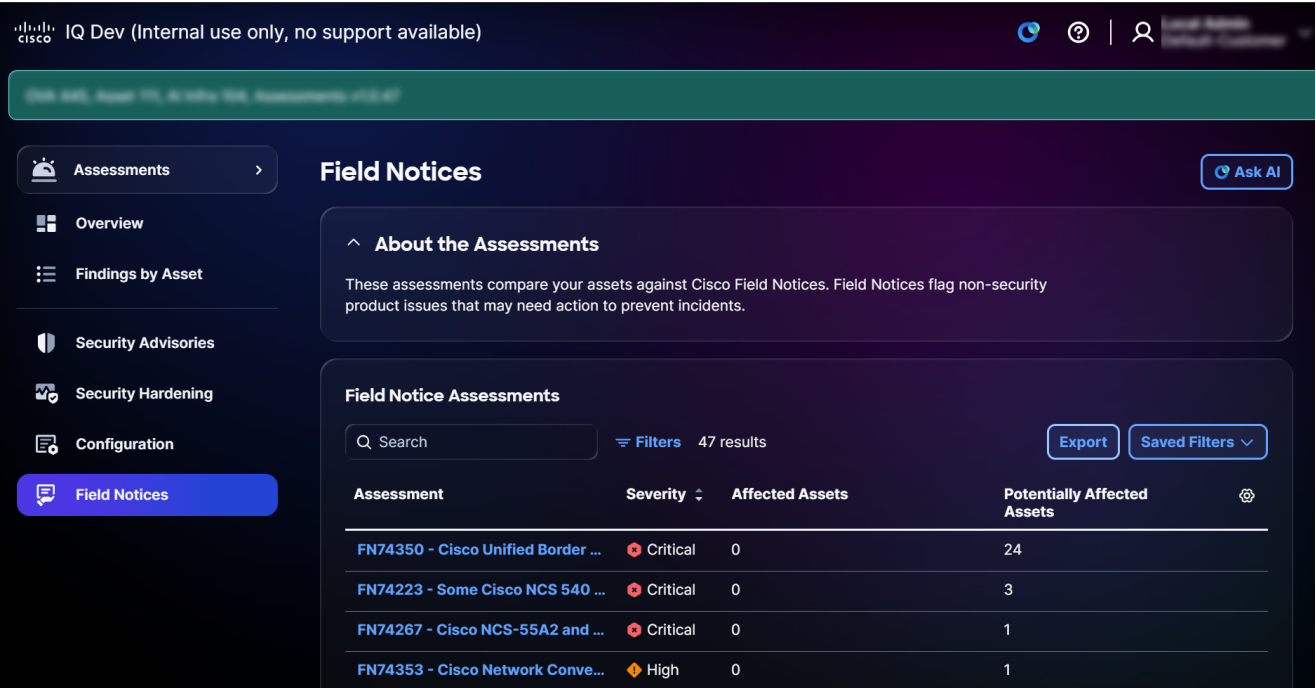


Nota: Las recomendaciones y los recursos afectados son opcionales en función del resultado de cada análisis.

Field Notices

Los avisos de campo identifican problemas importantes de productos no relacionados con la seguridad y los organizan en función de la gravedad y el impacto, lo que mejora la capacidad de la organización para gestionar los riesgos de los productos. Los avisos prácticos ofrecen información práctica sobre los defectos de los productos, aceleran la

mitigación mediante actualizaciones recomendadas o soluciones alternativas, y garantizan la alineación con los objetivos empresariales y operativos. Esto refuerza la fiabilidad de los productos, optimiza la asignación de recursos y fomenta la resistencia frente a los retos cambiantes de los productos en toda la empresa.



Field Notices

Búsqueda y filtrado de vistas para avisos de campo

Puede filtrar la vista de lista seleccionando un filtro de las listas desplegadas. También puede buscar evaluaciones de avisos de campo introduciendo el nombre de la evaluación en el campo Buscar.

Visualización de evaluaciones para avisos de campo

Para ver detalles adicionales sobre un aviso de campo, haga clic en una evaluación. Se muestran los siguientes detalles de la evaluación:

- Acerca de las evaluaciones: Proporciona detalles adicionales al resumir el propósito de la evaluación
- Evaluaciones de avisos de campo: Muestra una lista de los activos afectados por el aviso de campo seleccionado, incluidos los activos con vulnerabilidades detectadas

The screenshot displays the Cisco IQ interface for a Field Notice. The left sidebar contains navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration, and Field Notices (highlighted). The main content area shows the details of Field Notice FN74223. The title is 'FN74223 - Some Cisco NCS 540 Series Medium Density Routers May Become Unresponsive After Upgrade to Cisco IOS XR Software Release 7.11.1 or Later - Workaround Provided'. The severity is 'Critical', and it was last updated on 'Dec 11, 2024'. The 'About the assessment' section provides context: 'Some medium density Cisco Network Convergence System (NCS) 540 Series Routers may not boot when subjected to a field programmable device (FPD) upgrade during installation of Cisco IOS XR Software Release 7.11.1 or later.' The 'Asset Results' section shows a table with 3 results, all marked as 'Potentially affected'.

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

Visualización de evaluaciones para avisos de campo

Búsqueda y Filtrado de Vistas de Resultados de Activos para Avisos de Campo

Puede filtrar la vista de lista seleccionando un filtro de las listas desplegables o haciendo clic en Filtros y eligiendo una opción de la lista de filtros disponibles. También puede buscar resultados de activos introduciendo el nombre del activo en el campo Buscar.



Nota: Algunos filtros pueden estar ocultos en función de la configuración del zoom de la pantalla. Hay distintos filtros disponibles en función de las funciones y los permisos del usuario.

Exportación de Resultados de Activos para Avisos de Campo

Para exportar los resultados de los activos de evaluación de los avisos de campo, haga clic en Exportar. Consulte [Exportación de información](#) para obtener más información.

Consulta de Resultados de Evaluación de Activos para Avisos de Campo

Para ver los detalles de los resultados de la evaluación de un activo, haga clic en un activo en Resultados de la evaluación de activos. Se muestra la página de detalles del resultado de la evaluación del activo.

Puede ver los siguientes tipos de resultados:

- **Afectado:** Indica los activos que cumplen todos los criterios comprobados automáticamente para un aviso práctico y que no requieren ninguna verificación manual adicional para confirmar que se han visto afectados
- **Potencialmente afectados:** Indica los activos que cumplen todos los criterios verificados automáticamente para un aviso práctico, pero que requieren una verificación manual adicional para confirmar si se han visto realmente afectados

Las siguientes indicaciones están disponibles en la pestaña Evaluaciones - Consolidación de la seguridad:

- ¿Cuáles son las prácticas recomendadas de consolidación de la seguridad de Cisco para los dispositivos de red?
- ¿Cómo reafirmo mis dispositivos Cisco IOS XE?
- Enumere los pasos clave de refuerzo de la seguridad para routers y switches.
- ¿Cuáles son los parámetros de refuerzo de línea base recomendados para los dispositivos de Cisco?
- ¿Cuántos recursos infringen las prácticas recomendadas de refuerzo de la seguridad?

Autenticación local

Los administradores de cuentas deben utilizar las siguientes credenciales para iniciar sesión correctamente en el VA:

- Nombre de usuario predeterminado: admin
- Contraseña predeterminada: contraseña que se establece durante el proceso de instalación del dispositivo virtual; consulte la Guía de inicio para obtener más información
- Contexto de cuenta predeterminado: Cliente predeterminado

Al iniciar sesión, el usuario predeterminado, "admin", y el nombre de cuenta, "Default-Customer" (Cliente predeterminado) se muestran en la página de inicio.

Configuración de la seguridad del administrador local

Puede cambiar su contraseña y configurar preguntas de seguridad mediante el menú Perfil del usuario en la página de inicio.

Configuración de bloqueo

Se pueden configurar los siguientes ajustes de bloqueo de cuentas durante la implementación:

- Estado de bloqueo: habilita o deshabilita la función de bloqueo de cuentas.
- Número máximo de intentos de inicio de sesión: establece el número máximo de intentos fallidos consecutivos permitidos antes de que se bloquee una cuenta (valor predeterminado: 3; Rango: 0-10).
- Ventana Tiempo de Acumulación: Define el período de tiempo para realizar un seguimiento de los intentos fallidos (Valor por Defecto: 15 minutos; Rango: 0-60 minutos).
- Duración: establece la duración durante la que una cuenta permanece bloqueada después de alcanzar el número máximo de intentos (valor predeterminado: 30 minutos; Rango: 0-60 minutos).



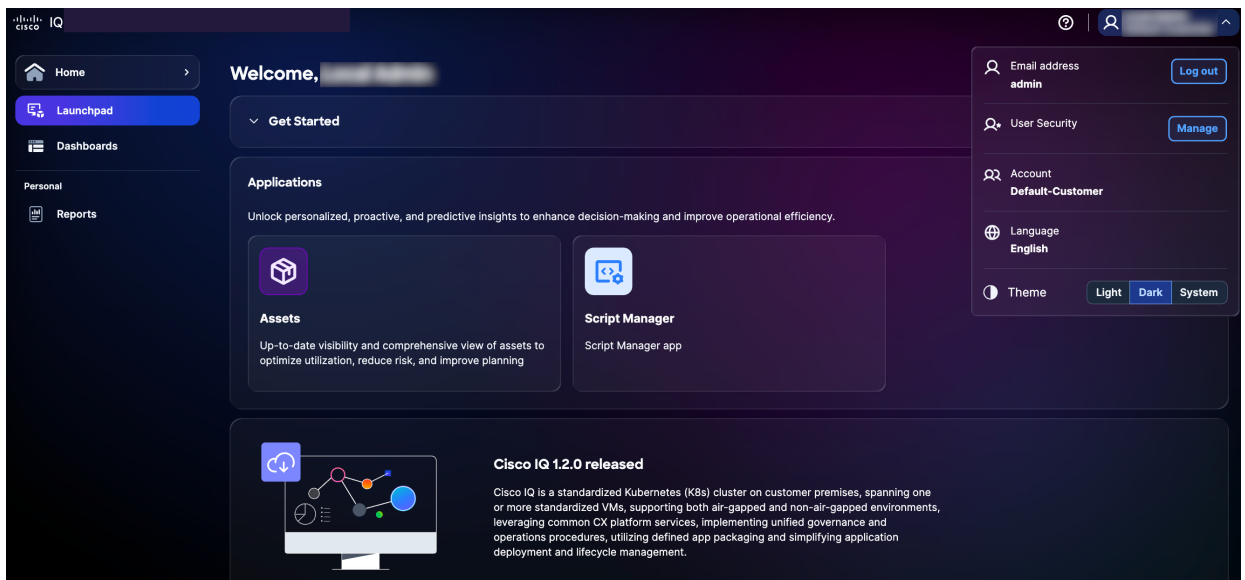
Nota: Tiene tres (3) intentos para introducir la contraseña correcta en un período de 15 minutos. Si los tres (3) intentos no tienen éxito, su cuenta se bloquea temporalmente durante 30 minutos para proteger su seguridad. No puede intentar iniciar sesión durante el período de bloqueo. El sistema muestra el mensaje: "Cuenta bloqueada debido a demasiados intentos fallidos. Inténtelo de nuevo más tarde", incluida la hora a la que caduca el bloqueo. La cuenta se desbloquea automáticamente transcurridos 30 minutos, momento en el que puede intentar iniciar sesión o restablecer la contraseña.

Configuración de preguntas y respuestas de seguridad

Las preguntas de seguridad ayudan a verificar su identidad si olvida su contraseña. Los administradores de cuentas deben configurar respuestas a cinco (5) preguntas de seguridad para habilitar la función de restablecimiento de contraseña. Esta es una configuración única.

Para configurar preguntas de seguridad:

1. En la página de inicio, haga clic en el icono Perfil de usuario. Se abre el menú desplegable.



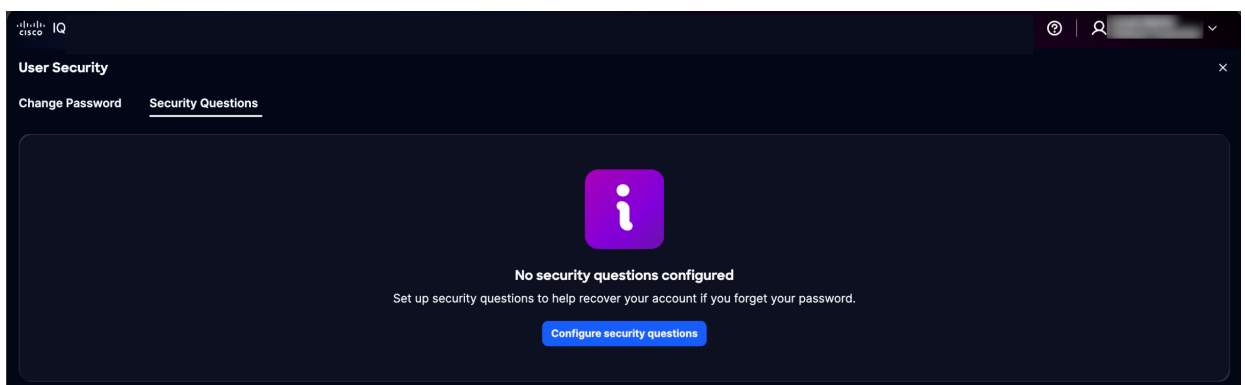
Usar seguridad

2. Haga clic en Administrar en Seguridad del usuario. Se muestra la página User Security.



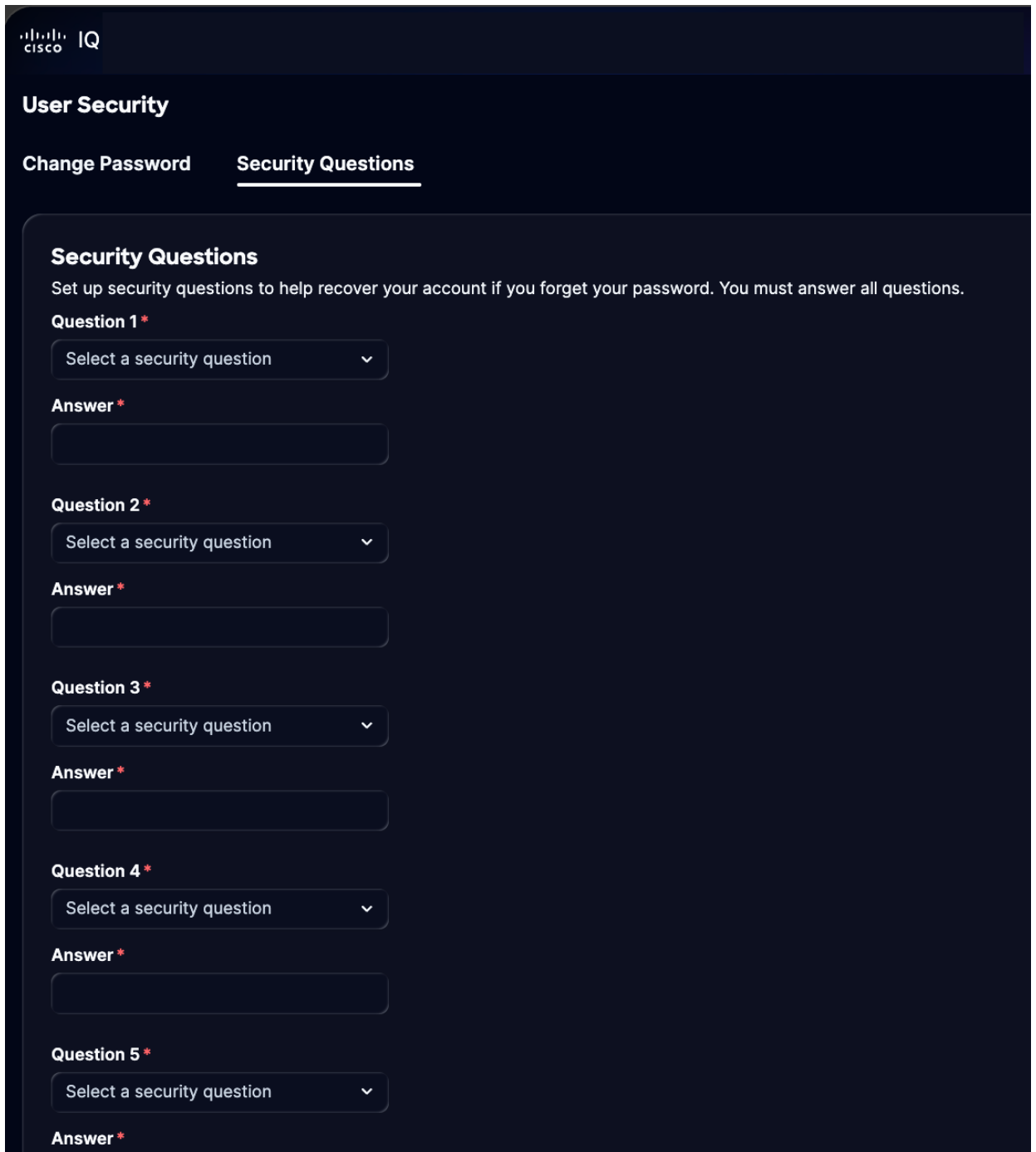
Preguntas de seguridad

3. Haga clic en Preguntas de seguridad para abrir la ficha.



Ficha Preguntas de seguridad

4. Haga clic en Configurar preguntas de seguridad.



The screenshot shows the Cisco IQ User Security interface. At the top, there's a header with the Cisco logo and 'IQ'. Below it, the 'User Security' section is active, with two tabs: 'Change Password' and 'Security Questions'. The 'Security Questions' tab is selected and underlined. The main content area is titled 'Security Questions' and includes a sub-header 'Set up security questions to help recover your account if you forget your password. You must answer all questions.' Below this, there are five identical question sets. Each set consists of a dropdown menu labeled 'Select a security question' and a text input field labeled 'Answer *'. The questions are labeled 'Question 1 *', 'Question 2 *', 'Question 3 *', 'Question 4 *', and 'Question 5 *'.

Configurar preguntas de seguridad

5. Elija cinco (5) preguntas de seguridad cualesquiera de las listas desplegables.
6. Introduzca la respuesta para cada pregunta.
7. Click Save.



Nota: Las respuestas no distinguen entre mayúsculas y minúsculas; por

 ejemplo, "SMITH" y "smith" se consideran iguales. Se omiten los espacios adicionales, lo que significa que "Smith" y "Smith" reciben el mismo trato. Recuerde cómo ha introducido la respuesta (por ejemplo, nombres completos frente a apodos). Utilice respuestas directas que recordará años más tarde. Elija preguntas con respuestas que no cambiarán con el tiempo.

 Nota: Si es necesario, puede actualizar las respuestas más adelante. Al actualizar las respuestas, se sustituyen todas las respuestas anteriores, por lo que debe volver a proporcionar las respuestas a las cinco (5) preguntas y no solo a las que desea cambiar.

Administración de contraseñas

Los administradores de cuentas y los usuarios locales pueden administrar la contraseña de Cisco IQ.

Para garantizar la seguridad de su cuenta, se aplican las siguientes políticas de contraseñas:

- Restricción de reutilización: Su nueva contraseña no puede coincidir con ninguna de las cinco (5) contraseñas anteriores. Esta política se aplica a los flujos Suscripción, Contraseña olvidada y Cambiar contraseña.
- Variación de caracteres: al cambiar la contraseña mientras está autenticado, la contraseña nueva debe tener al menos ocho (8) caracteres diferentes de la contraseña actual.
- Intervalo mínimo de cambio: de forma predeterminada, debe esperar 24 horas antes de volver a cambiar la contraseña. Si se configura un intervalo diferente, no podrá actualizar la contraseña hasta que haya transcurrido ese tiempo.
- Vencimiento de contraseña: Las contraseñas caducan cada 60 días. La primera vez que inicie sesión después de la fecha de vencimiento, se le pedirá que establezca una nueva contraseña antes de poder acceder al sistema (si está configurado en 0, la caducidad de la contraseña está desactivada).

Prerequisites

Para administrar contraseñas, se deben cumplir las siguientes condiciones:

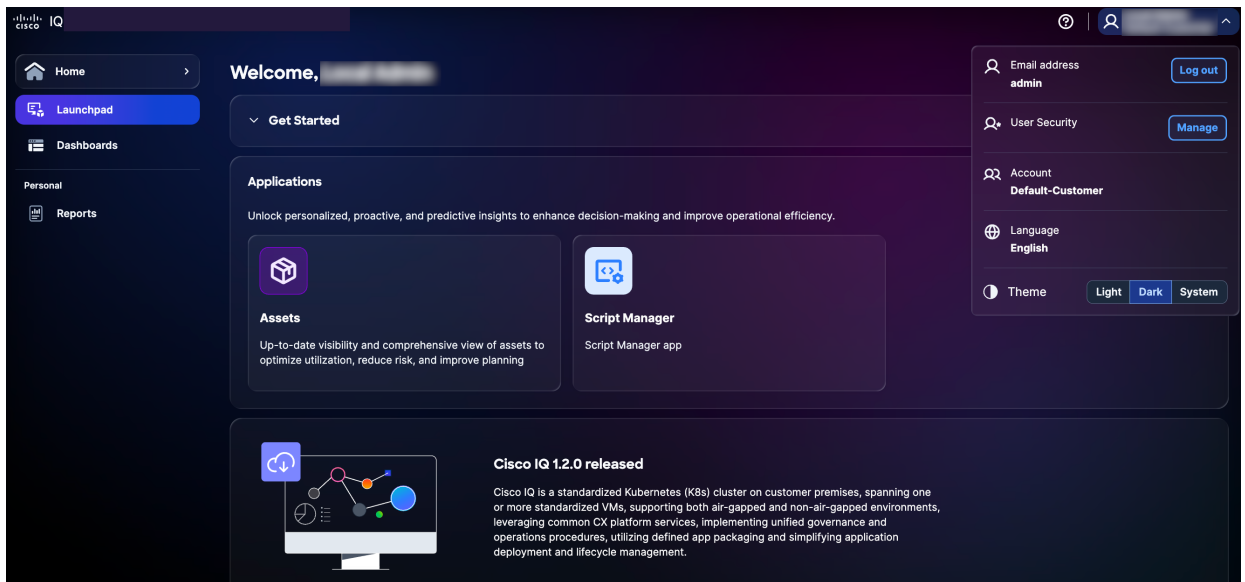
- Es un usuario o administrador de cuenta local
- Está utilizando una cuenta local (no un inicio de sesión único (SSO) ni autenticación externa)
- Ha iniciado sesión en Cisco IQ

- Conoce la contraseña actual

Cambio de contraseñas

Para cambiar la contraseña:

1. En la página de inicio, haga clic en el icono Perfil de usuario. Se abre el menú desplegable.



Gestionar seguridad del usuario

2. Haga clic en Administrar en Seguridad del usuario. Se muestra la página User Security.



Cambiar contraseña

3. Introduzca la contraseña actual.
4. Introduzca la nueva contraseña.

5. Vuelva a introducir la nueva contraseña para confirmarla.

6. Click Save.

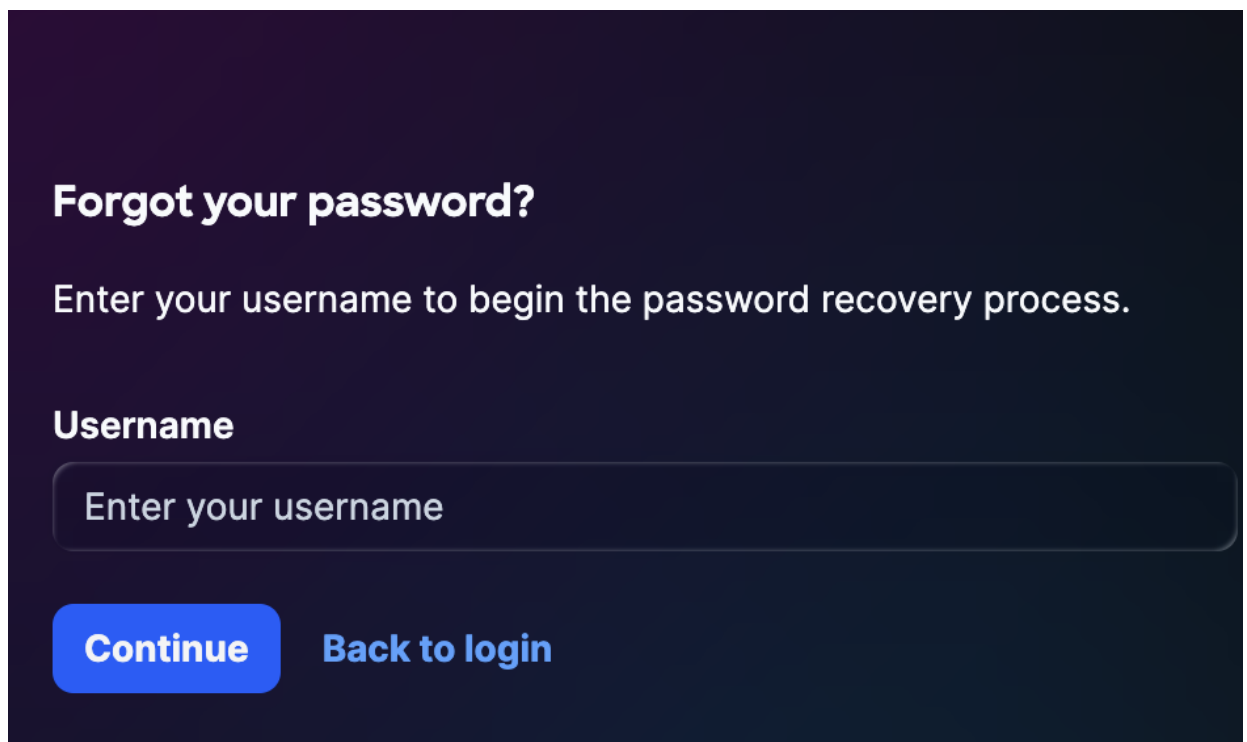
La contraseña se actualiza en el sistema Cisco IQ, incluida la máquina virtual Cisco IQ.

Restablecimiento de una Contraseña Olvidada

Puede restablecer una contraseña mediante el proceso de verificación de preguntas de seguridad.

Para restablecer una contraseña olvidada:

1. Navegue hasta la página de inicio de sesión de Cisco IQ VA.
2. Haga clic en Olvidó su contraseña.



Forgot your password?

Enter your username to begin the password recovery process.

Username

Enter your username

Continue **Back to login**

Contraseña olvidada

3. Introduzca el nombre de usuario.
4. Haga clic en Continue (Continuar). La página Verificar identidad muestra tres (3) preguntas de seguridad aleatorias de las cinco (5) preguntas configuradas anteriormente.

Verify Identity

Answer the following security questions to verify your identity.

What city were you born in?

Enter your answer

Show

What is your mother's maiden name?

Enter your answer

Show

What was the name of your elementary school?

Enter your answer

Show

Verify and continue

Back to login

Verificar identidad

5. Introduzca las respuestas para las tres (3) preguntas mostradas.
6. Haga clic en Verificar y continuar. Si la respuesta enviada coincide con las respuestas guardadas anteriormente, se le solicitará que introduzca una nueva contraseña.

Set New Password

Choose a strong password that contains the following:

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

New password

Show

Confirm password

Show

Reset password

Back to login

Restablecer contraseña

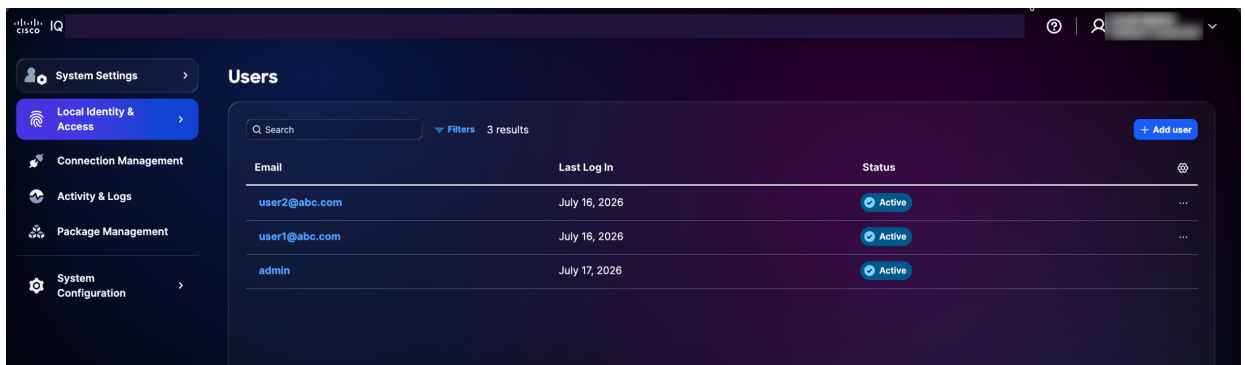
 Nota: Tiene tres (3) intentos para introducir la contraseña correcta en un período de 15 minutos. Si los tres (3) intentos no tienen éxito, su cuenta se bloquea temporalmente durante 30 minutos para proteger su seguridad. No puede intentar iniciar sesión durante el período de bloqueo. El sistema muestra el mensaje: "Cuenta bloqueada debido a demasiados intentos fallidos. Inténtelo de nuevo más tarde", incluida la hora a la que caduca el bloqueo. La cuenta se desbloquea automáticamente transcurridos 30 minutos, momento en el que puede intentar iniciar sesión o restablecer la contraseña.

- Introduzca la nueva contraseña.
- Vuelva a introducir la contraseña para confirmarla.
- Haga clic en Submit (Enviar).

Adición de usuarios locales

Los administradores de cuentas pueden agregar usuarios a la cuenta de Cisco IQ. Para agregar un nuevo usuario:

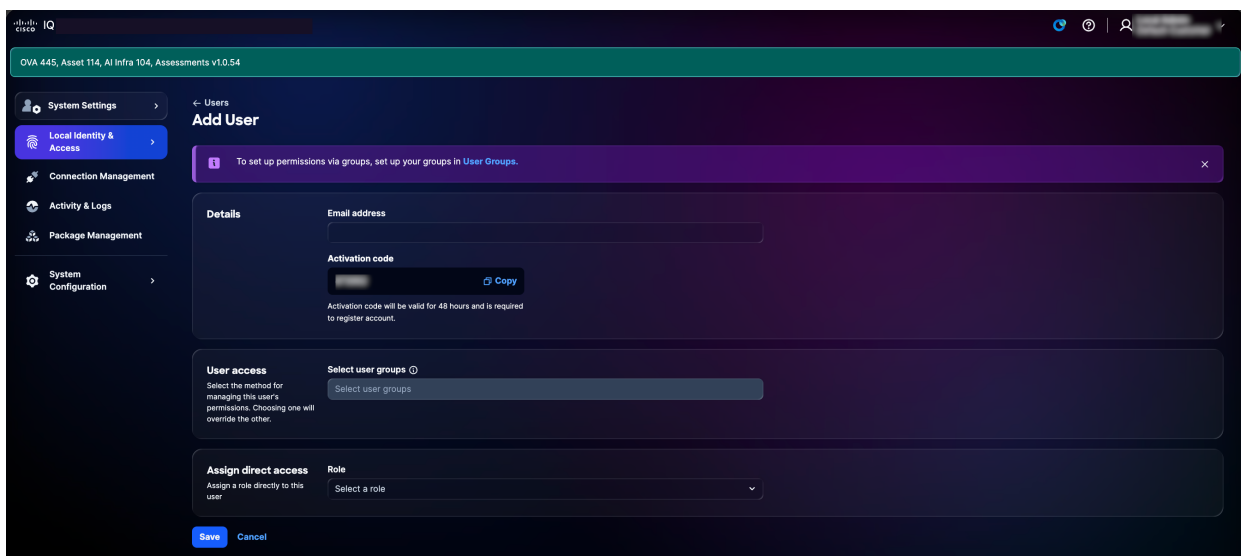
1. Vaya a System Settings > Local Identity & Access > Users. Se muestra la página Users. Enumera todos los usuarios locales existentes junto con su estado.



Página Usuarios

 Nota: No comparta el código de activación a través de canales inseguros. Si el código se pierde o se ve comprometido, utilice el icono Menú para volver a generar un nuevo código de activación, que invalida el anterior. Los códigos de activación son válidos durante 48 horas. Si su código caduca, póngase en contacto con el administrador de su cuenta para solicitar uno nuevo.

- Haga clic en Agregar usuarios. Se muestra la página Add User.



Agregar usuario

3. Introduzca la dirección de correo electrónico.
4. Introduzca el código de activación.

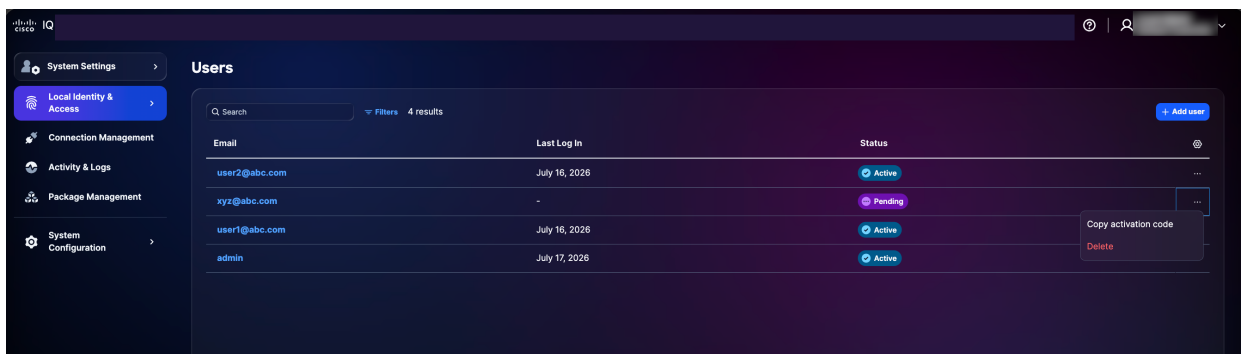
 Nota: El código de activación se muestra de forma predeterminada. Comparta el código de activación mostrado con el usuario, ya que es necesario para el registro.

5. En Acceso de usuario, elija el grupo de usuarios de la lista desplegable Seleccionar grupos de usuarios.



Nota: Los usuarios heredan el acceso del grupo seleccionado.

6. En Asignar acceso directo, seleccione un rol de la lista desplegable Rol. Hay dos (2) funciones disponibles:
 - Visor: Ver y acceder a aplicaciones
 - Administrador de cuentas: Acceder a los módulos y gestionar la configuración del sistema, excepto la gestión del sistema y el proveedor de identidad (IDP)
7. Click Save. Se crea el nuevo usuario y se muestra en la lista de usuarios con el estado Pendiente. Pendiente indica que el usuario aún no ha completado la autoactivación.
8. Localice el usuario recién creado en la lista y confirme que la columna Estado muestra Pendiente.
9. Haga clic en el icono Más opciones situado junto al usuario recién creado.



Copiar código de activación

10. Seleccione Copiar código de activación en la lista desplegable. El código de activación se copia en el portapapeles.
11. Comparta este código con el usuario de forma segura (por ejemplo, mediante un canal interno seguro). El código de activación es para un solo uso y es necesario para completar el registro.



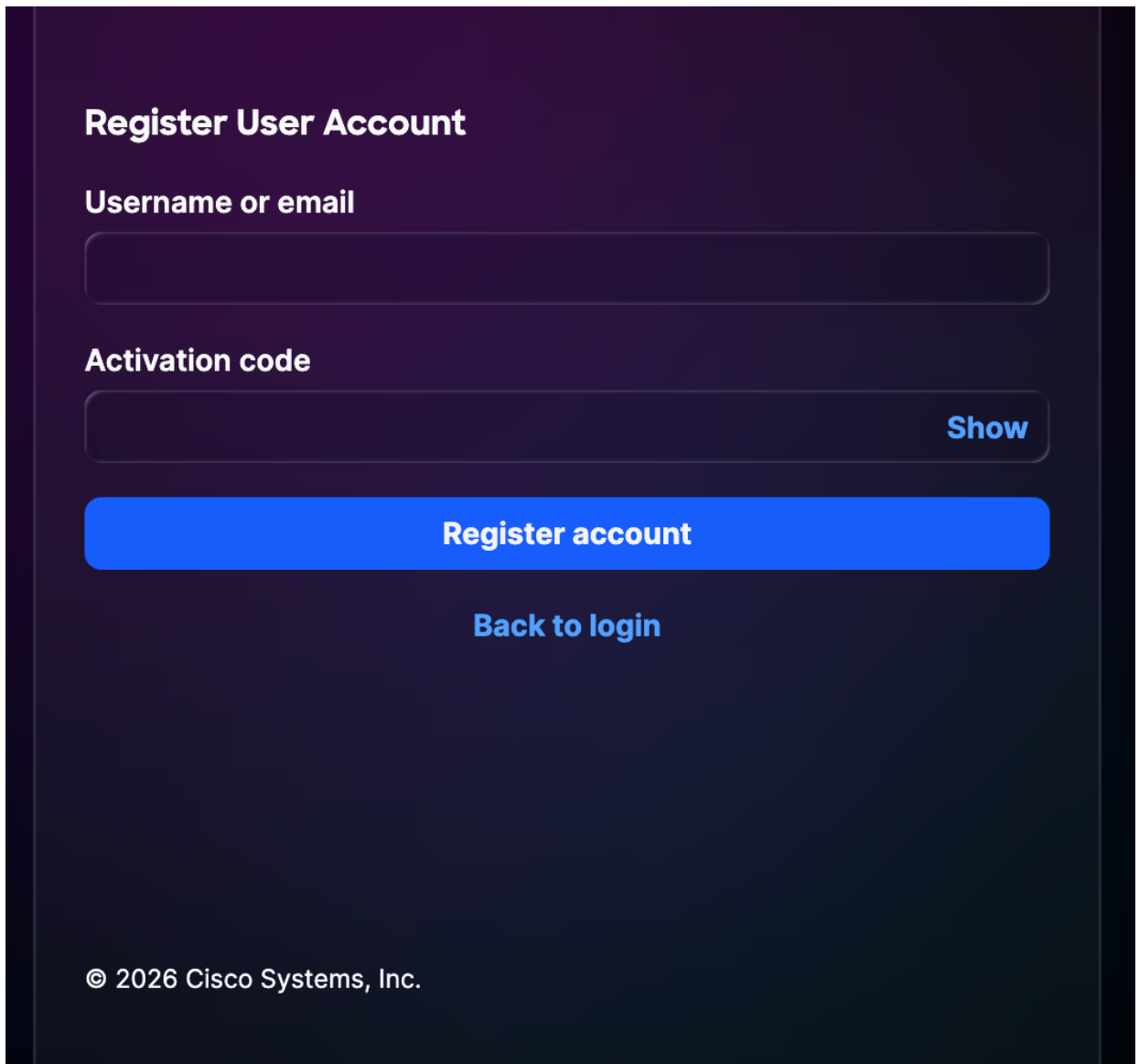
Nota: No comparta el código de activación a través de canales inseguros. Si el código se pierde o se ve comprometido, utilice el icono Menú para volver a generar un nuevo código de activación, que invalida el anterior. Los códigos de activación son válidos durante 48 horas. Si su código caduca, póngase en contacto con el administrador de su cuenta para solicitar uno nuevo.

12. Para cerrar la sesión, haga clic en el icono User Profile en la esquina superior derecha y seleccione Logout. Volverá a la página de inicio de sesión de Cisco IQ.

Registro de nuevas cuentas de usuario

Para registrar la nueva cuenta de usuario:

1. En la página de inicio de sesión, haga clic en el enlace Registrar una nueva cuenta de usuario.



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

Register User Account

Username or email

Activation code

Show

Register account

Back to login

© 2026 Cisco Systems, Inc.

Nueva cuenta de usuario

2. Introduzca el nombre de usuario o la dirección de correo electrónico que se utilizó cuando se creó el usuario (por ejemplo, user1@abc.com)
3. Introduzca el código de activación compartido por el administrador de la cuenta.
4. Haga clic en Registrar cuenta. Se muestra la ventana Set New Password.

Set New Password

Choose a strong password that contains the following:

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

New password

Show

Confirm password

Show

[Reset password](#)

[Back to login](#)

Contraseña de cuenta de usuario nueva

5. Introduzca una nueva contraseña.
6. Vuelva a introducir la contraseña en Confirmar contraseña.
7. En el primer inicio de sesión correcto, se le pide al usuario que configure cinco (5) preguntas de seguridad. (Consulte [Configuración de preguntas de seguridad](#)).

Administración de grupos de usuarios locales

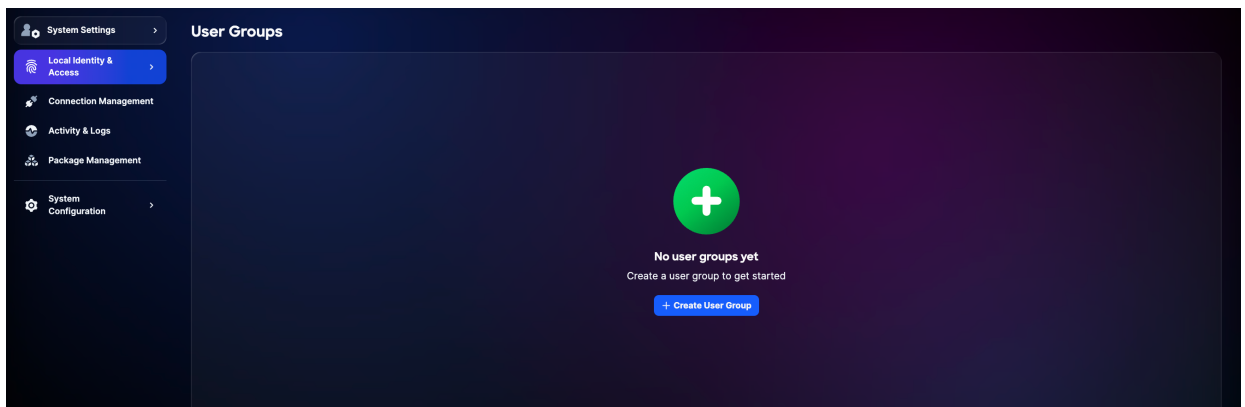
Los grupos de usuarios permiten al administrador de cuentas administrar funciones para varios usuarios locales a la vez. En lugar de asignar una función a cada usuario de forma individual, puede crear un grupo, adjuntar una función y un conjunto de usuarios a la misma, y actualizar la función o la pertenencia en un único lugar. Toda la gestión de grupos de usuarios se realiza desde la página Identidad local y acceso.

 Nota: Sólo un administrador de cuentas puede crear, editar o eliminar grupos de usuarios. Los grupos están formados por usuarios locales existentes; los usuarios deben crearse antes de poder agregarlos a un grupo. Consulte [Adición de Usuarios Locales](#) para obtener más información.

Creación de un grupo de usuarios

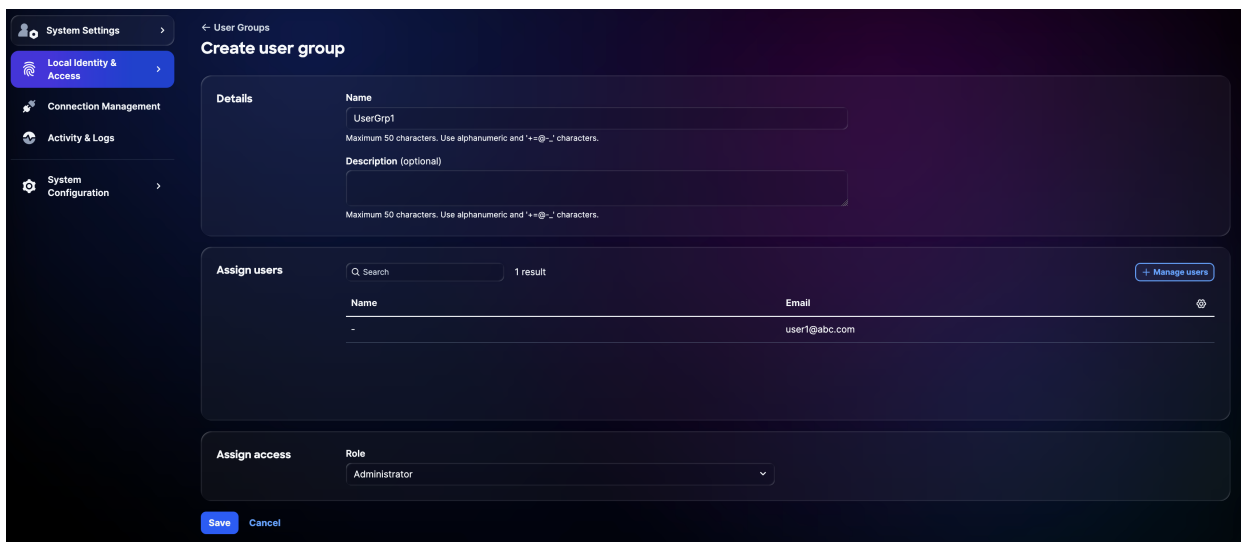
Para crear un grupo de usuarios:

1. En System Settings, elija Local Identity & Access > User Groups. Se muestra la página Grupos de usuarios.



Grupos de usuarios

2. Haga clic en Create User Group. Se muestra la página Crear grupo de usuarios.



Crear grupo de usuarios

3. Complete las siguientes secciones:

- Detalles
- Nombre: Introduzca un nombre único para el grupo (por ejemplo,

Operadores de sólo lectura)

- Descripción (opcional): Breve descripción del grupo (máximo 50 caracteres; alfanumérico y + = @ - _ (se permiten caracteres)
- Asignar usuarios: Busque y seleccione uno o varios usuarios locales existentes para agregarlos al grupo. Nota: Para agregar usuarios que aún no aparezcan en la lista, haga clic en Administrar usuarios.
- Asignar acceso
- Función: Seleccione el rol del sistema que desea asignar a todos los miembros de este grupo. Están disponibles los siguientes roles:
- Visor: Ver y acceder a módulos (solo lectura)
- Administrador: Acceder a módulos y gestionar la configuración del sistema

4. Click Save.

El nuevo grupo de usuarios se muestra en la lista Grupos de usuarios junto con su función asignada y número de miembros.

Edición de un grupo de usuarios

Para editar un grupo de usuarios:

1. En la lista Grupos de usuarios, localice el grupo que desea modificar.
2. Elija el icono Más opciones > Editar del grupo deseado. Se muestra la página Editar grupo de usuarios.

The screenshot shows the 'Edit user group' page within a system settings application. The left sidebar contains navigation links: System Settings, Local Identity & Access (highlighted), Connection Management, Activity & Logs, and System Configuration. The main content area is titled 'Edit user group' and includes a back arrow and 'User Groups' label. It features three sections: 'Details' with input fields for 'Name' (containing 'UserGrip1') and 'Description (optional)'; 'Assign users' with a search bar, a table showing one user ('user1@abc.com'), and a '+ Manage users' button; and 'Assign access' with a 'Role' dropdown menu set to 'Administrator'. At the bottom are 'Save' and 'Cancel' buttons.

Editar grupo de usuarios

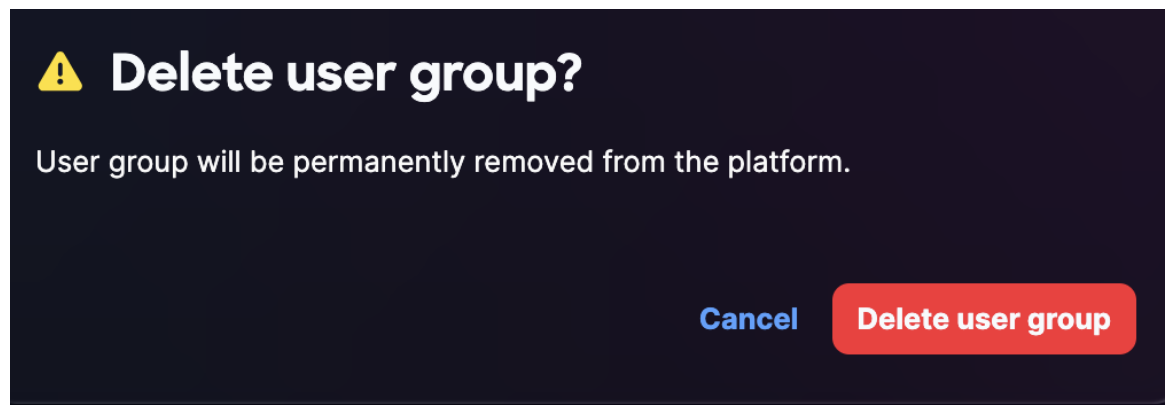
3. Realice los cambios que desee.
4. Click Save.

El grupo actualizado se muestra en la lista Grupos de usuarios. La nueva función surte efecto para todos los miembros del grupo.

Eliminación de un grupo de usuarios

Para eliminar un grupo de usuarios:

1. En la lista Grupos de usuarios, localice el grupo que desea eliminar.
2. Haga clic en el icono Más opciones junto al grupo y seleccione Eliminar.



Eliminar grupo de usuarios

3. Confirme la eliminación cuando se le solicite.

El grupo se elimina de la lista Grupos de usuarios.



Nota: Al eliminar un grupo de usuarios, se quita la asignación de función basada en grupo de todos los miembros. Las cuentas de usuario individuales no se eliminan.

Configuración del proveedor de identidad

Una vez que hayan iniciado sesión en VA, los administradores de cuentas pueden configurar diversos ajustes. Los administradores de cuentas pueden iniciar sesión mediante la administración local o la configuración de IDP.

Configuración SAML de IDP Okta para SSO

Prerrequisitos para Configurar IDP SAML

- Acceso de administrador local a Cisco IQ
- Acceso al portal IDP

Configuración SAML de IDP para SSO

Para configurar el Lenguaje de marcado de aserción de seguridad (SAML) IDP para SSO:

1. Desplácese hasta el portal IDP.

Tabla 2: Atributos de Cisco IQ

Campo	Valor
Nombre de aplicación	<Application Name>
Entorno	aplicación empresarial ESP
Grupos de propietarios de aplicaciones	Propietario de la configuración de IDP
Correo del equipo	Correo para el equipo
Destinatarios	No empleados
Categoría de incorporación	Seleccione "Nueva incorporación"

Tabla 3: Parámetros de configuración de SAML

Parámetro	Configuración	Ejemplo:
Audiencia (ID de entidad)	Nombre de dominio completo (FQDN)	mymanagementhost.mydomain.com
URL de inicio de sesión único	Terminal de servicio al cliente (ACS) de afirmación de SAML	https://mymanagementhost.mydomain.com/saml/acs
Formato de ID de nombre	Dirección de correo	NA
Nombre de usuario de aplicación	Nombre de usuario	NA

5. Configure las sentencias de atributo.



Nota: Los cambios en el atributo IDP dependen del proveedor y la configuración específicos. Cisco IDP y sus atributos se comparten a continuación como ejemplo.

- Primera entrada
 - Nombre: Nombre de usuario
 - Valor: user.login
- Segunda entrada
 - Nombre: Correo electrónico principal
 - Valor: usuario.correo electrónico
- Sentencias de Atributo de Grupo

- Nombre: grupos
- Filtro: REGEX
- Valor: .*

6. Configure los parámetros de Single Logout (SLO) en la aplicación.

Tabla 4: Parámetros de configuración de SLO

Campo	Valor
Certificado de firma	Para Okta, este certificado solo es necesario si elige habilitar SLO. Descargue el certificado de firma mediante Download SP Certificate en Identity Providers. Guarde el archivo como sp-public-key.crt. Consulte Configuración de cierre de sesión único para obtener más detalles.
Metadatos SP	Los metadatos del proveedor de servicios (SP) solo son necesarios para los IDP de ADFS (y no para Okta).
¿Desea activar el cierre de sesión único?	Sí o No
URL de cierre de sesión único	https://mymanagementhost.mydomain.com/saml/logout
Emisor SP (ID de entidad/público o URL ACS)	https://mymanagementhost.mydomain.com

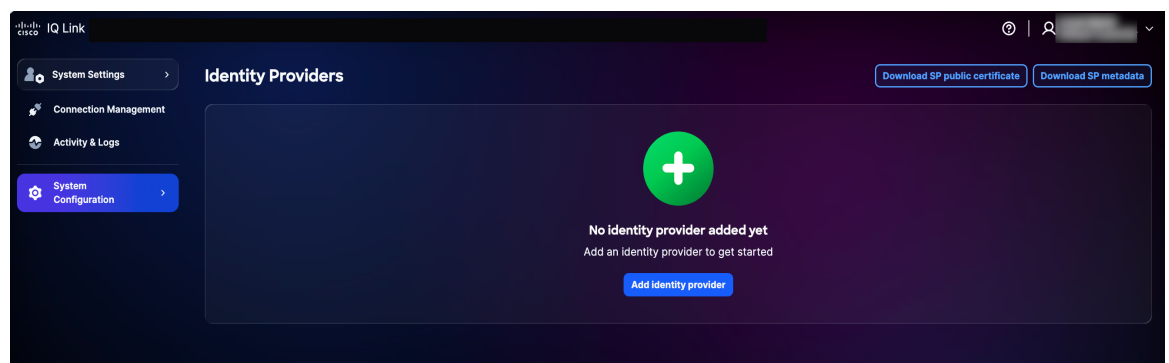
8. Haga clic en el icono Download para descargar el archivo "IDP Metadata XML".

9. Aprovisione o cree la aplicación según lo requiera el proveedor.

Adición de Okta IDP

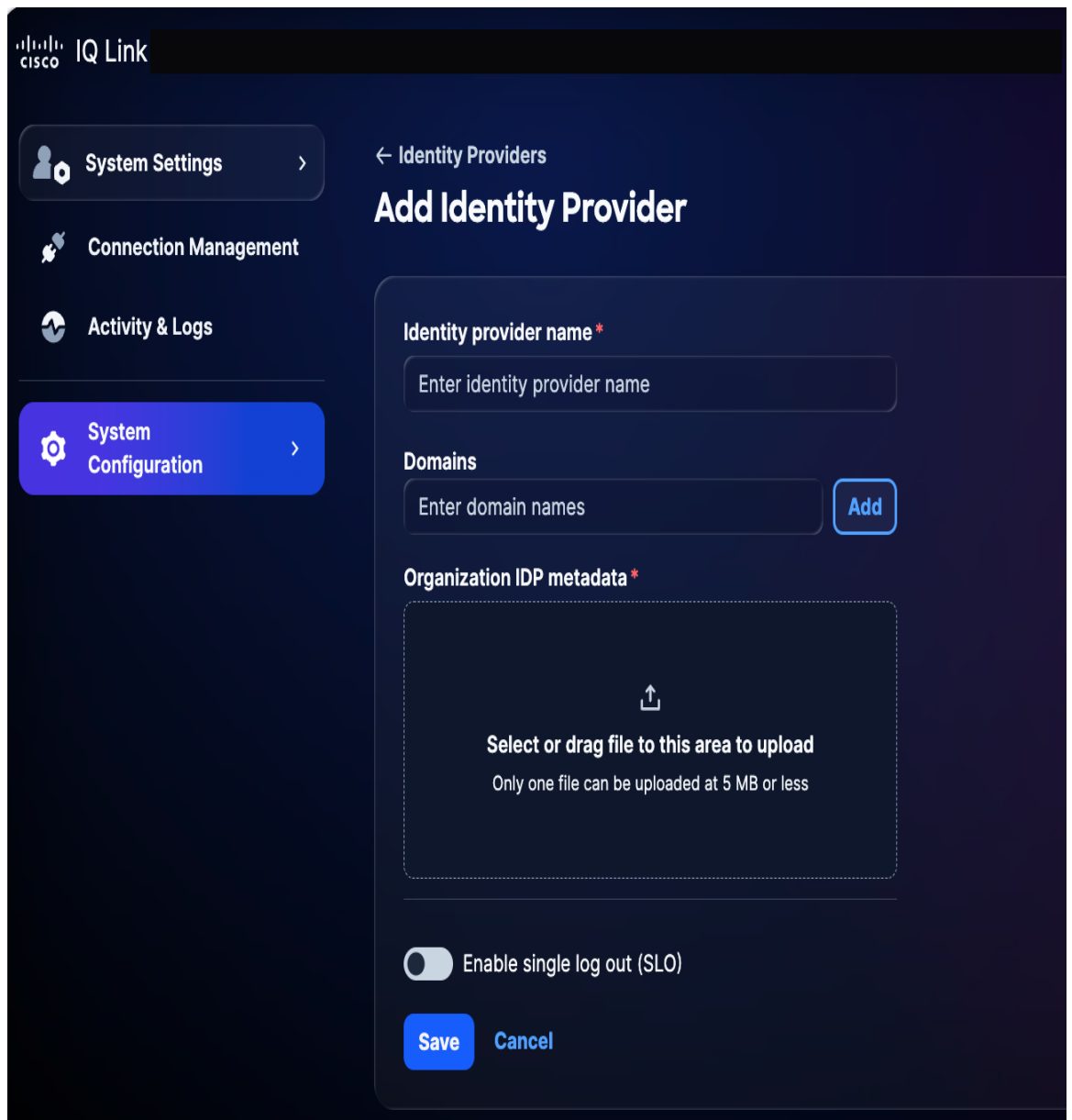
Para agregar un IDP en Cisco IQ:

1. En System Settings, elija System Configuration > Identity Providers. Se muestra la página Identity Providers.



 Nota: Solo se puede agregar un (1) IDP en un momento dado.

2. Haga clic en Agregar proveedor de identidad. Se muestra la página Add Identity Provider.



Agregar proveedor de identidad

3. Introduzca el nombre del proveedor de identidad.
4. Haga clic en Agregar para agregar un nombre de dominio configurado de Cisco IQ al campo Dominio(s).
5. Arrastre y suelte o cargue el archivo de metadatos SAML obtenido de la aplicación IDP en el campo de metadatos Organization IDP. Este archivo contiene los detalles del certificado y los detalles de la entidad SP.

6. (Opcionalmente) active el botón de alternancia Enable single logout. También puede activar el SLO más adelante.

7. Click Save.

Configuración de asignación de roles

1. En el IDP agregado, elija el icono Más opciones > Asignar roles. Se muestra la página Asignar roles de usuario.

×

Map identity provider roles to system roles to assign permissions.

Map User Roles

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

+ Add identity provider role

Save

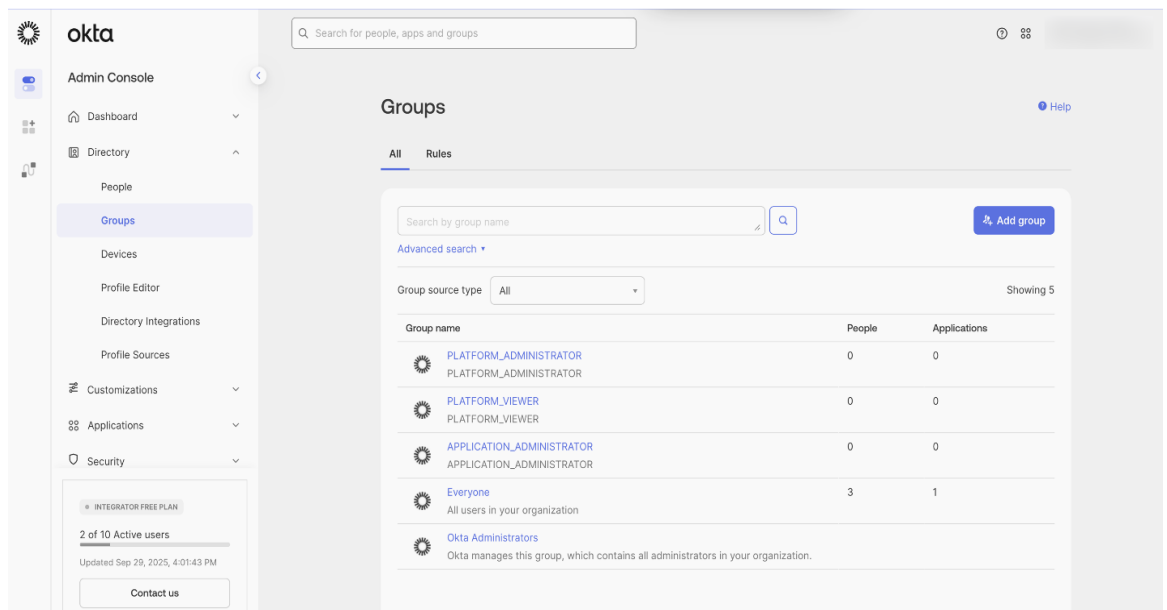
Asignar funciones de usuario

- Introduzca un rol IDP para el rol de sistema seleccionado. Se admiten los siguientes roles del sistema:

- Administrador general de cuentas: El administrador de cuentas general tiene permisos completos para realizar todas las acciones del producto
- Visor de cuentas general: El Visor de cuentas general tiene acceso de solo lectura



Nota: El rol IDP es un campo de texto abierto. Debe coincidir exactamente con el nombre de grupo o rol configurado en el IDP de su organización. A continuación se comparte un ejemplo de grupos Okta.



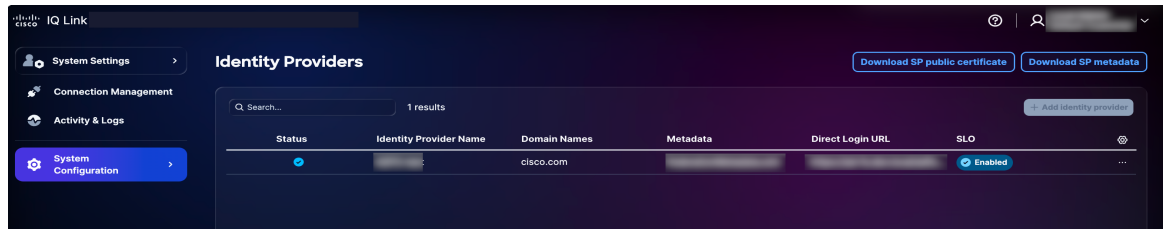
Referencia de asignación de roles

3. Asigne funciones adicionales según sea necesario haciendo clic en Agregar función de proveedor de identidad.
4. Click Save. Una vez configurada, la página de inicio de sesión muestra una opción para iniciar sesión con SSO (mediante IDP).

Configuración de cierre de sesión único

Si elige habilitar SLO, debe cargar metadatos que incluyan la URL de SLO. Puede configurarlo editando la configuración del proveedor de identidad y activando la opción Enable Single Log Out. Para completar la configuración de SLO:

1. En la página de inicio de Identity Providers, haga clic en Download SP public certificate.



Certificado público SP

2. Guarde el archivo descargado como sp-public-key.crt.
3. Desplácese hasta el portal IDP.
4. Cargue el archivo de certificado de firma generado en [IDP SAML Configuration for SSO](#).
5. Introduzca la URL de SLO (por ejemplo, https://ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com/saml/logout).
6. Introduzca el emisor SP (por ejemplo, ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com).
7. Haga clic en Submit (Enviar).
8. Vuelva a descargar el archivo de metadatos IDP.
9. En la página Proveedores de identidad, elija el icono Más opciones del IDP agregado > Editar.
10. Active el botón de alternancia Enable single log out (SLO).
11. Cargue el archivo de metadatos recién descargado.
12. Utilice la siguiente lista de comprobación para verificar la funcionalidad de SSO y SLO:

Lista de verificación:

- El inicio de sesión del administrador local se ha realizado correctamente
- Se configura y se aprovisiona el portal IDP
- IDP se agrega a Cisco IQ con el estado "Correcto"
- Las asignaciones de funciones se configuran y se prueban
- Se descargan los metadatos SP y se extrae el certificado
- Si SLO está habilitado, la configuración de SLO se completa con el certificado de firma real
- El flujo de SSO y SLO de extremo a extremo se ha probado correctamente

Solución de problemas de IDP

Las siguientes tablas enumeran problemas comunes y posibles soluciones para ayudar a identificar y resolver rápidamente problemas relacionados con el estado IDP, errores de certificado, fallas de inicio de sesión SSO y configuración SLO:

Tabla 5: Resolución de problemas

Problema	Solución
El estado de IDP aparece como "Incompleto"	Verificar las configuraciones de asignación de roles
Errores de certificado	Comprobar el formato y la validez del certificado
Fallos de inicio de sesión SSO	Validar asignación de atributos y asignaciones de grupos
SLO no funciona como se esperaba	Asegúrese de que el certificado se haya cargado correctamente y de que las URL de SLO estén configuradas

Configuración ADFS IDP SAML para SSO

En esta sección se proporciona orientación para configurar los Servicios de federación de Microsoft Active Directory (AD) como el IDP de SAML para Cisco IQ, que admite la autenticación basada en contraseña y la infraestructura de clave pública (PKI) o la autenticación basada en certificados.

Prerrequisitos para Configurar ADFS IDP SAML for SSO

- Se recomienda ADFS 6.0+
- Windows Server 2016 + (recomendado para 2019)
- Integración de AD configurada con cuentas de usuario
- Certificados SSL/TLS en servidor ADFS
- Acceso de administrador a Cisco IQ
- Acceso administrativo al servidor ADFS (Windows Server)
- Acceso a PowerShell en servidor ADFS
- Conectividad de red entre ADFS y Cisco IQ
- Autoridad de certificación empresarial (CA) (instalada o accesible)
- Privilegios de administrador de dominio o administrador de empresa (sólo se requiere para PKI)

- Detalles de la configuración del servidor ADFS (como se indica en la tabla siguiente)

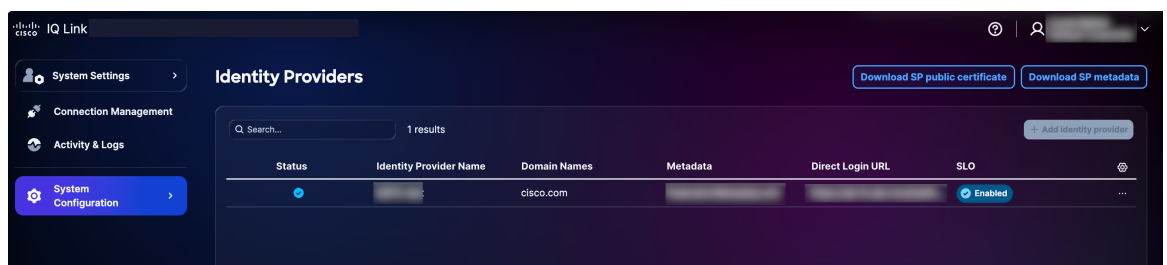
Tabla 6: Descripción General del Flujo de Autenticación

Ítem	Descripción	Ejemplo:
FQDN de Cisco IQ	Nombre de host de implementación de usuario	<Your-CIQ-FQDN> Por ejemplo, dev35-23.cx-xxx-xxx.cisco.com
URL del servidor ADFS	Dirección del servidor ADFS del usuario	https://<Your-ADFS-HOSTNAME> Por ejemplo, https://adfs.dev.local
Dominio de la empresa	Dominio de correo electrónico	<Your-Domain>
Grupos AD	Grupo de Active Directory Nombres de dominio (DN)	CN=Función: desarrolladores de CXIQ OU=Grupos, DC=dev, DC=local
Nombre de CA (PKI)	Nombre de CA de empresa	<Your-CA-Name>
Puerto de autenticación de certificado (PKI)	Puerto TLS alternativo ADFS	49443
Huella digital de certificado SSL	certificado SSL del servidor ADFS	<Your-SSL-CERT-THUMBPRINT>

Configuración de ADFS SAML Base

Para configurar ADFS:

1. En System Settings, elija System Configuration > Identity Providers. Se muestra la página Identity Providers.



Opciones de descarga

2. Haga clic en Download SP public certificate y Download SP metadata para descargar estos archivos.
3. Copie y guarde los archivos service-provider-metadata.xml y service-

provider-certificate.crt en el servidor ADFS (por ejemplo, C:\.

4. Inicie sesión en el servidor ADFS.
5. En el menú Administración de ADFS, haga clic en Confianza de terceros.
6. En el menú Confianzas de usuario de confianza, haga clic en Agregar confianzas de usuario de confianza. Se abrirá el nuevo asistente.
7. Haga clic en el botón de opción Reclamaciones.
8. Haga clic en Start para continuar con la configuración.
9. Haga clic en Importar datos sobre el usuario de confianza desde un archivo para obtener detalles del archivo que se guarda como parte del paso 3.
10. Haga clic en Examinar para seleccionar el archivo de metadatos del proveedor de servicios y completar la carga del archivo.
11. Haga clic en Next (Siguiente).
12. Introduzca un nombre para mostrar (por ejemplo, "Cisco IQ"), agregue notas relevantes y haga clic en Next (Siguiente).
13. En la página Choose Access Control Policy, haga clic en Permit everyone (o la política requerida por la configuración de seguridad de su organización).
14. Haga clic en Next en las pantallas restantes.
15. Haga clic en Cerrar para completar la configuración de Confianza de usuario de confianza.



Nota: No seleccione "Permitir a todos con MFA" a menos que el servidor ADFS tenga un adaptador Multi-Factor Authentication (MFA) registrado (por ejemplo, Azure MFA, Contraseña de un solo uso basada en tiempo (TOTP) configurada).

Si esta directiva está habilitada sin un proveedor MFA configurado, ADFS autentica al usuario pero, en última instancia, deniega la solicitud con el estado urn:oasis:names:tc:SAML:2.0:status:RequestDenied. Dado que la respuesta SAML no contiene aserción, el plugin falla e informa de un error de "correo electrónico faltante".

Problema: "Permitir a todos con MFA" está seleccionado.

Solución alternativa: En PowerShell, compruebe la directiva actual ejecutando el comando siguiente.


```
Get-AdfsRelyingPartyTrust -Name  
“
```

```
”).AccessControlPolicyName
```

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

```
”
```

```
-AccessControlPolicyName “Permit everyone”
```

You can also create the trust through PowerShell:

```
-Add-AdfsRelyingPartyTrust `  
=Name “
```

```
” `
```

```
-Identifier “
```

```
” `
```

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

```
”) `
```

```
-AccessControlPolicyName “Permit everyone” `  
-IssuanceAuthorizationRules '=> issue(Type =  
“http://schemas.microsoft.com/authorization/claims/permit”, Value =  
“true”);
```

Configuración de reglas de reclamación de ADFS

Para configurar las reglas de reclamación de ADFS, lleve a cabo los pasos que se indican en las secciones siguientes.

Reclamaciones necesarias

Consulte la tabla siguiente para obtener información sobre las reclamaciones

necesarias.

Tabla 7: Reclamaciones necesarias

Afirmación	Propósito	Fuente
Correo electrónico	Identificador de usuario	Correo AD
Mostrar nombre:	Nombre completo del usuario	Nombre para mostrar de AD
UPN	PKI/autenticación de certificados	ADFS asigna el certificado de cliente a un usuario de AD mediante UPN
ID de nombre	asunto SAML	Transformado a partir del correo electrónico
Grupos	Acceso basado en roles	Pertenencia a grupos AD (memberOf)

Aplicación de reglas de reclamación

1. Defina el nombre de su fideicomiso de usuario de confianza (por ejemplo, "Cisco IQ - Producción").

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

2. Defina reglas de reclamación para enviar información de usuario y pertenencia a grupos a Cisco IQ.

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

3. Aplique las reglas de reclamación ejecutando el siguiente comando:

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

Write-Host "Reglas de reclamación configuradas correctamente" -
ColorDePrimerPlano Verde

Advertencia: Cada cuenta de usuario de AD debe tener el atributo de correo rellenado. Si falta este atributo, la afirmación SAML no contiene una notificación de correo electrónico, lo que provoca un rechazo de autenticación.

Para actualizar la dirección de correo electrónico de un usuario, ejecute el siguiente comando de PowerShell:

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

Verificación de grupos de usuarios

1. Establezca el nombre de usuario para comprobar la pertenencia al grupo del usuario mediante la ejecución del siguiente comando:

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

2. Ejecute los siguientes comandos para buscar la cuenta del usuario:

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

3. Muestre los grupos a los que pertenece el usuario mediante el siguiente

comando:

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

Ejemplo de salida:

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

Configuración de ADFS para Confiar en el Certificado de Firma SP

1. En el servidor ADFS, importe el certificado SP en el almacén TrustedPeople:

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

2. Elija una de las opciones siguientes:



Nota: El certificado SP lo emite una CA interna que ADFS no puede validar mediante la cadena de confianza estándar.

- Deshabilitar la validación de cadena globalmente para este usuario de confianza

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

```
" `
```

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

- Si el certificado SP lo emite una CA (no autofirmada), importe el certificado de CA emisor en el almacén de certificados raíz

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

3. Aplique los cambios reiniciando el servicio ADFS.

Restart-Service adfssrv

Configuración de la Autenticación PKI/de Certificados

En esta sección se describe cómo agregar autenticación basada en certificados (es decir, tarjeta inteligente o certificado de software) junto con contraseñas. Esta sección se puede omitir si la autenticación de solo contraseña es suficiente.

Instalación del rol CA de AD CS

Para instalar el rol de CA de Servicios de certificados de AD (CS):

1. Verifique si ya existe una CA empresarial en su dominio ejecutando el siguiente comando:

```
certutil -config -ping
```

Si el comando devuelve una respuesta válida, puede omitir el resto de esta sección. Su entorno ya está configurado. Si el comando indica que no se ha encontrado ninguna CA, vaya al paso 2.

2. Instale el rol de CA ejecutando el siguiente comando:

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

3. Configure el rol de CA ejecutando el siguiente comando:

```
install-AdcsCertificationAuthority `
-CAType EnterpriseRootCA `
-CACommonName "
    " `
-KeyLength 2048 `
-HashAlgorithmName SHA256 `
-CryptoProviderName "RSA#Microsoft Software Key Storage Provider" `
-ValidityPeriod Years `
-ValidityPeriodUnits 10 `
-Force
```

4. Verifique la instalación ejecutando el siguiente comando:

```
certutil -ca
```

5. Confirme que el servicio está activo y accesible ejecutando el siguiente comando:

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

Configuración de una Plantilla de Certificado

Para configurar una plantilla de certificado con el Uso mejorado de claves de autenticación de cliente (EKU):

1. Abra `certsrv.msc` y expanda el nodo CA.
2. Haga clic con el botón derecho en Plantillas de certificado > Administrar.
3. Duplicar la plantilla de usuario.



Nota: La plantilla de usuario integrada es funcional o válida sólo si el certificado emitido desde ella incluye EKU de autenticación de cliente.

4. Configure los parámetros de las siguientes fichas:
 - General: Introduzca "Autenticación de usuario CIQ" en el campo Nombre con un período de validez de un (1) año
 - Gestión de solicitudes: Seleccione Signature and encryption en la lista desplegable Purpose y marque la casilla de verificación Allow private key to be export
 - Nombre del sujeto: Seleccione Build from Active Directory Information e incluya un correo electrónico en los campos Subject y SAN

Advertencia: Los campos Subject y SAN deben contener el nombre principal de usuario (UPN) de un usuario o un correo electrónico que coincida con una cuenta de AD. ADFS asigna el certificado a un usuario de AD mediante estos campos.

- Extensiones: Asegúrese de que las políticas de aplicación incluyen "Autenticación de cliente (1.3.6.1.5.5.7.3.2)"
- Seguridad: Agregue usuarios de dominio y conceda permisos de lectura e inscripción

5. Publique la plantilla mediante el siguiente comando:

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

Inscripción de un Certificado de Usuario

1. Inicie sesión como usuario de destino.
2. Inscriba el certificado ejecutando el siguiente comando:

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

3. Verifique la instalación del certificado ejecutando el siguiente comando:

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

Exportación de un certificado de usuario desde Windows e instalación en el cliente (Mac)

Para exportar un certificado de usuario de Windows a Mac:

1. Exporte el certificado de Windows como un archivo PFX ejecutando los siguientes comandos:

```
$cert = Get-ChildItem Cert:| Where-Object { $_.Subject -like "*  
  
*" }  
$password = ConvertTo-SecureString -String "  
  
" -Force -AsPlainText  
Export-PfxCertificate -Cert $cert -FilePath "C:-cert.pfx" -Password $password
```

2. Transfiera el archivo user-cert.pfx a su dispositivo Mac.
3. Importe el certificado en el llavero de Mac ejecutando el siguiente comando:

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



Nota: Después de importar el certificado, el explorador debe cerrarse y abrirse de nuevo para que se reconozca.

4. Confíe en CA en Mac ejecutando:

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

Habilitación de los Extremos de Autenticación de Certificado ADFS

Para habilitar los extremos de autenticación de certificados ADFS:

1. Habilite los extremos de certificado ADFS requeridos ejecutando los siguientes comandos:

```
EEnable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificate  
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificatetransport  
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificate  
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificatetransport
```

2. Verifique que todos los terminales estén habilitados ejecutando el siguiente comando:

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

Habilitación de la Autenticación de Certificados como Principal

Para habilitar la autenticación de certificados como principal:

1. Configure los proveedores de autenticación principales para el acceso a la intranet y a la extranet mediante el siguiente comando:

```
Set-AdfsGlobalAuthenticationPolicy `\  
-PrimaryIntranetAuthenticationProvider @(“CertificateAuthentication”, “WindowsAuthentic
```



```
-PrimaryExtranetAuthenticationProvider @"CertificateAuthentication", "FormsAuthentication"
```

2. Verifique que ambas listas incluyan CertificateAuthentication y FormsAuthentication mediante los siguientes comandos:

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

3. Verifique la configuración actual del puerto del cliente TLS mediante el siguiente comando:

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

4. Si TlsClientPort no es 49443, actualice el puerto y reinicie el servicio ADFS con los siguientes comandos:

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

Correcciones SChannel/TLS (CRÍTICO para PKI)

Los pasos de las siguientes secciones resuelven los errores CERT_E_UNTRUSTEDROOT (0x800B0109) que impiden que funcione la autenticación de certificados.

Enlace de certificados SSL en el puerto 49443

Para enlazar certificados SSL en el puerto 49443:

1. Elimine cualquier enlace de certificado SSL existente en el puerto 49443 mediante el siguiente comando:

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

:49443

2. Cree un nuevo enlace con la negociación de certificado de cliente habilitada mediante el siguiente comando:

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

```
          :49443 `
certhash=
```

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

3. Verifique que la negociación de certificado de cliente esté habilitada mediante el siguiente comando:

```
http show sslcert
hostnameport=
```

```
          :49443
```

Limpieza del almacén de certificados (CRÍTICO)

Para limpiar el almacén de certificados:

Advertencia: Windows SChannel rechaza todos los certificados de cliente si hay certificados no autofirmados en el almacén raíz de confianza. Esta es la causa principal de las fallas de PKI.

1. Identifique los certificados no autofirmados en el almacén raíz de confianza ejecutando el siguiente comando:

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

2. Mueva estos certificados al almacén de CA intermedio ejecutando el siguiente comando:

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

3. Verifique que no queden certificados no autofirmados en el almacén raíz de confianza ejecutando el siguiente comando:

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

Correcciones de registro de SChannel (CRÍTICO)

Para configurar los valores del Registro de SChannel para garantizar una autenticación de certificado adecuada:

1. Defina la variable de ruta de acceso del Registro mediante el siguiente comando:

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

2. Aplique la configuración del Registro definida en la tabla siguiente mediante los siguientes comandos:

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

Tabla 8: Configuración del Registro de SChannel

Configuración	Valor	Propósito
ClientAuthTrustMode	2	Habilita la confianza exclusiva de la CA para corregir la ruta de validación predeterminada.
SendTrustedIssuerList	0	Impide que el servidor envíe la lista completa de emisores de confianza durante el intercambio de señales TLS.

Verificación del almacén de certificados de la CA

Para comprobar el almacén de certificados de la CA:



Nota: El certificado de CA que emite los certificados de usuario debe estar en el almacén de certificados del sistema para garantizar que se reconoce correctamente.

1. Defina la huella digital de su certificado de CA mediante el siguiente comando:

```
$caThumbprint = “
```

```
”
```

2. Verifique que el certificado de la CA ya esté presente en LocalMachinestore* mediante el siguiente comando:

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

Si no se encuentra el certificado, impórtelo en el almacén LocalMachine:

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

Reinicio del servidor ADFS (OBLIGATORIO)

Reinicie el servidor ADFS con el siguiente comando:

```
Restart-Computer -Force
```



Nota: El cambio de registro ClientAuthTrustMode sólo tiene efecto después de reiniciar el servidor.

Exportación de metadatos ADFS

Puede descargar los metadatos de ADFS mediante PowerShell o el explorador web.

PowerShell

Para exportar metadatos de ADFS mediante PowerShell:

1. Abra PowerShell en el servidor ADFS.
2. Ejecute los siguientes comandos para descargar el archivo de metadatos.

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

Después de ejecutar los comandos, el archivo de metadatos se guarda en C:-metadata.xml.

Explorador web

Para exportar metadatos de ADFS mediante un explorador web:

1. Vaya a <https://<your-adfs-server>/FederationMetadata/2007-06/FederationMetadata.xml>, sustituyendo "<your-adfs-server>" por el nombre de host del servidor ADFS.
2. Guarde el archivo XML de metadatos en el equipo cuando se le solicite.

Configuración en Cisco IQ

Para configurar en Cisco IQ:

1. Transfiera adfs-metadata.xml a su estación de trabajo.
2. En Cisco IQ, vaya a System Settings > System Configuration > Identity Providers.
3. Cargue el archivo de metadatos ADFS para extraer automáticamente el certificado IDP, la ID de entidad y la URL SSO.
4. Guarde la configuración.



Nota: Si ADFS realiza una renovación automática del certificado de firma de tokens, debe volver a exportar el archivo de metadatos y cargarlo en Cisco IQ para garantizar una autenticación continua.

Adición de IDP de ADFS

1. En la página Proveedores de identidad, haga clic en Agregar proveedor de identidad.

2. Introduzca el nombre del proveedor de identidad.
3. Introduzca el dominio o dominios (por ejemplo, company.com).
4. (Opcionalmente) active el botón de alternancia Enable single logout, si es necesario.
5. Arrastre y suelte o cargue el archivo de metadatos SAML obtenido de la aplicación IDP en el campo Upload IDP Metadata.
6. Click Save.



Nota: El estado se muestra como "Incompleto" hasta que se complete la asignación de roles; debe ocurrir lo siguiente.

Configuración de mapeo de roles

Antes de continuar con la configuración de la asignación de funciones, asegúrese de que puede encontrar grupos de AD para utilizarlos en la asignación. Para buscar grupos desde AD, ejecute el siguiente comando de PowerShell:

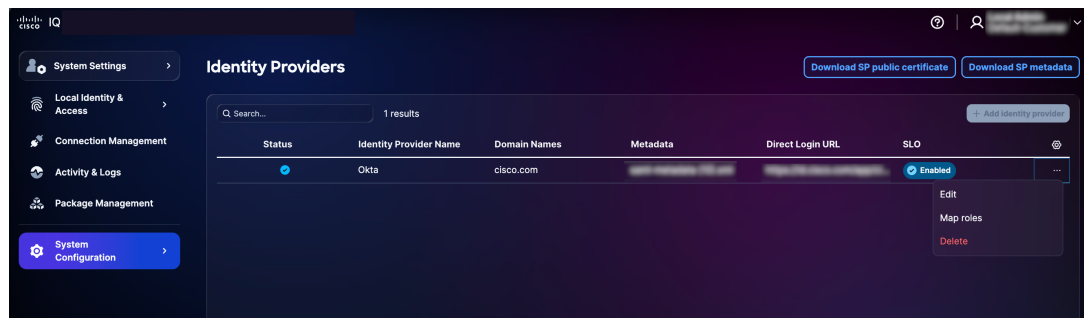
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = "(&(objectClass=group)(cn=Role - CXIQ*))"
$searcher.PropertiesToLoad.Add("distinguishedName") | Out-Null
$searcher.PropertiesToLoad.Add("cn") | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties["distinguishedname"]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

El sistema consulta a AD directamente a través del protocolo ligero de acceso a directorios (LDAP), sin necesidad de módulos adicionales. La información de grupo se devuelve en formato completo de nombre distinguido, por ejemplo:

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

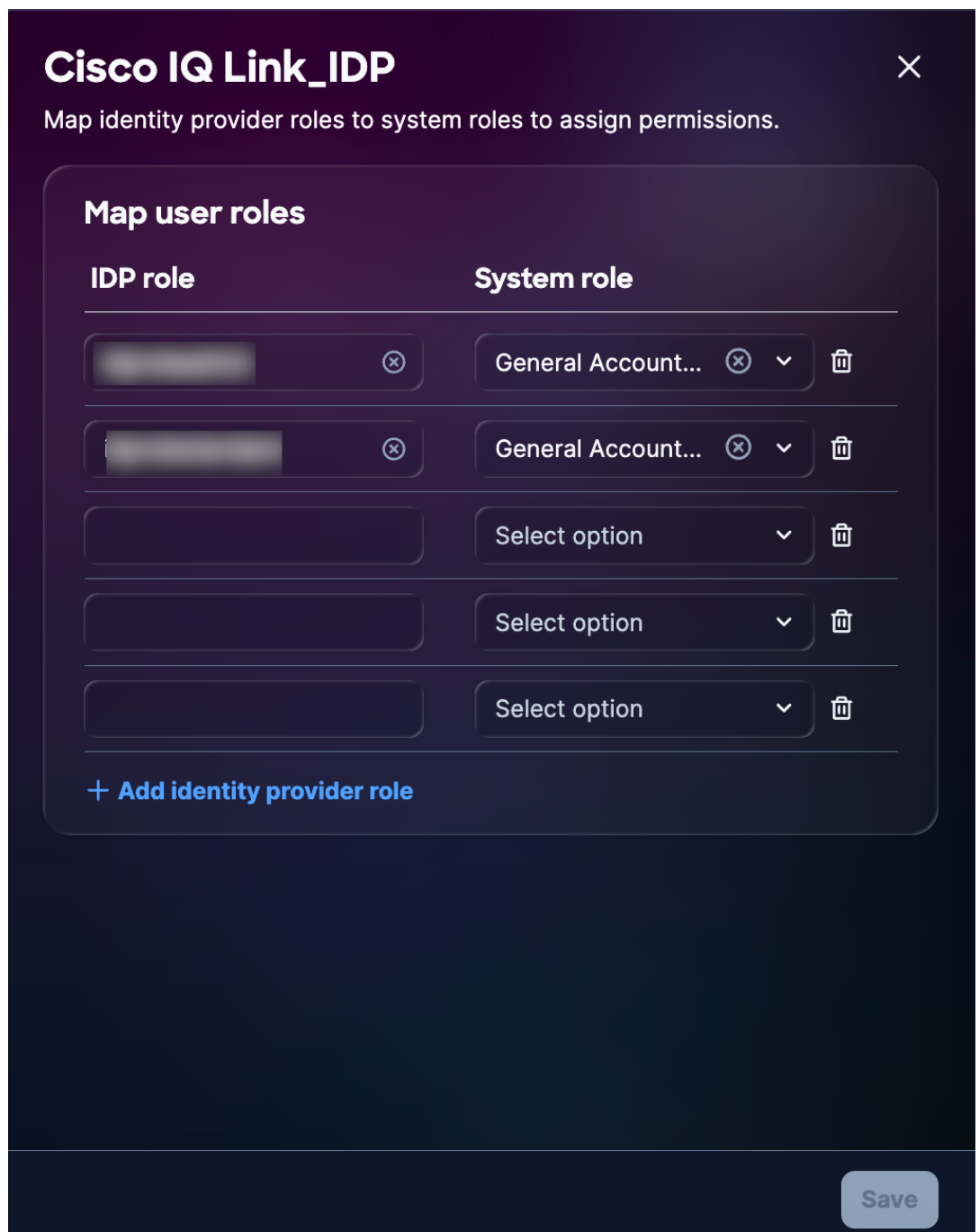
Si los grupos requeridos no aparecen en la lista, un administrador de cuentas debe crearlos en AD para que pueda completar la asignación de funciones de ADFS.

Para configurar la asignación de roles:



Asignación de funciones

1. En el IDP agregado, elija el icono Más opciones > Asignar roles. Se muestra la página Asignar roles de usuario.



Asignación de funciones

2. Introduzca un rol IDP para el rol del sistema seleccionado. Se admiten los siguientes roles del sistema:

- Administrador general de cuentas: El administrador de cuentas general tiene permisos completos para realizar todas las acciones del producto. El rol IDP (nombre analizado) es CXIQ Admins.
- Visor de cuentas general: El Visor de cuentas general tiene acceso de sólo lectura. El rol IDP (nombre analizado) es CXIQ Developers y CXIQ Viewers.



Nota: Utilice nombres analizados (por ejemplo, CXIQ Developers) y no DNs completos.

3. Click Save. El estado se actualiza a Correcto.

Prueba de certificado de cliente SChannel

Para comprobar que SChannel está correctamente configurado para aceptar certificados de cliente, abra una nueva ventana de PowerShell y ejecute el siguiente comando:

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

```
:49443/adfs/1s/"
```

El resultado esperado es una respuesta HTTP (por ejemplo, una redirección o la página ADFS). Si se produce un error de intercambio de señales TLS, la conexión ha fallado.

Prueba de explorador de extremo a extremo para flujo PKI

Antes de comenzar la prueba del navegador de extremo a extremo para el flujo PKI, asegúrese de que el certificado de usuario esté instalado en MacOS Keychain (consulte [Importación del certificado de usuario en la máquina cliente \(MacOS\)](#)). Para probar:

1. Navegue hasta la URL de inicio de sesión de SAML de la aplicación. ADFS presenta opciones de certificado y contraseña.
2. Elija Autenticación de certificado. El explorador solicita el certificado.
3. Cargue el certificado. ADFS autentica al usuario, redirige la solicitud con una respuesta SAML y establece una nueva sesión.

Prueba de explorador de extremo a extremo para flujo de contraseña

Antes de comenzar con la prueba del navegador de extremo a extremo para el flujo de contraseñas:

1. Navegue hasta la URL de inicio de sesión de SAML de la aplicación. ADFS presenta opciones de certificado y contraseña.
2. Seleccione Password/Forms Authentication .
3. Ingrese Username.
4. Ingrese la contraseña.
5. Verifique que el inicio de sesión se haya realizado correctamente.



Nota: Ambos flujos deben funcionar simultáneamente.

Solución de problemas de ADFS

La siguiente lista describe los problemas comunes y las posibles soluciones para ayudar a identificar y resolver rápidamente los problemas relacionados con el estado de ADFS, los errores de certificado, los errores de inicio de sesión de SSO y la configuración de SLO.

Tabla 9: Problemas de ADFS

Problema	Síntomas / Descripción	Causas / Comprobaciones / Soluciones temporales y soluciones
Grupos no extraídos	No hay roles después de iniciar sesión	◦ Falta la regla de reclamación: Vuelva a ejecutar las instrucciones de Configuración de reglas de reclamación de ADFS
Error de descifrado	"Error al descifrar la	Comprobar la

Problema	Síntomas / Descripción	Causas / Comprobaciones / Soluciones temporales y soluciones
	aserción" en los registros	configuración del certificado ADFS ◦ URL ACS no válida: Controle lo siguiente: https://your-fqdn/saml/acs
Bucle de inicio	Atascado en el bucle de autenticación o inicio de sesión	◦ Discordancia de cookies: Compruebe las cookies del navegador para el dominio correcto

Comandos de diagnóstico para solucionar problemas

Para garantizar una integración correcta entre su entorno ADFS y Cisco IQ, utilice los siguientes comandos de diagnóstico. Estos comandos ayudan a comprobar la accesibilidad de los metadatos, las configuraciones de certificados y la configuración de extremos.

- Verificar accesibilidad de metadatos de ADFS: Confirma que los metadatos de federación de ADFS son accesibles al público; este es un paso crítico para establecer la confianza inicial

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

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

- Validar el certificado de cifrado: Garantiza que el certificado de cifrado correcto esté asociado a la confianza de usuario de confianza de Cisco IQ

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

- Revisar configuración de terminal SAML: Verifica que los terminales SAML para la confianza de Cisco IQ estén correctamente configurados y que las solicitudes de autenticación y las aserciones se enruten a las URL esperadas

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

Configuración SAML de Microsoft Entra ID para SSO

Esta sección proporciona una guía para configurar Microsoft Entra ID (Entra ID) como SAML IDP para Cisco IQ, soportando tanto la autenticación basada en contraseña como la PKI o la autenticación basada en certificados (CBA).

Prerrequisitos para Configurar Entra ID SAML for SSO

- Inquilino con ID de acceso (por ejemplo, "ciqtestdev.onmicrosoft.com")
- Acceso a Cisco IQ con la función de administrador global o administrador de aplicaciones
- Conectividad entre Entra ID (nube) y Cisco IQ
- CA empresarial instalada o accesible (sólo se requiere para PKI)
- Punto de distribución de la lista de revocación de certificados (CRL) accesible desde Internet (sólo se requiere para PKI)

Tabla 10: Configuración del servidor de ID de entrada

Ítem	Descripción	Ejemplo:
ID de arrendatario	Identificador de arrendatario de ID de entrada	37352d8f-0ebe-4762-8161-8775ffe897cb
FQDN de Cisco IQ	Nombre de host de implementación	<YOUR-CIQ-FQDN>
ID de entidad IDP	URL del emisor de ID de entrada	https://sts.windows.net/<TENANT-ID>/
URL SSO IDP	terminal de inicio de sesión SAML	https://login.microsoftonline.com/<TENANT-ID>/saml2
Dominio de la empresa	Dominio de correo electrónico	<YOUR-DOMAIN>

Ítem	Descripción	Ejemplo:
	para usuarios	

Configuración de la Aplicación SAML Entra ID

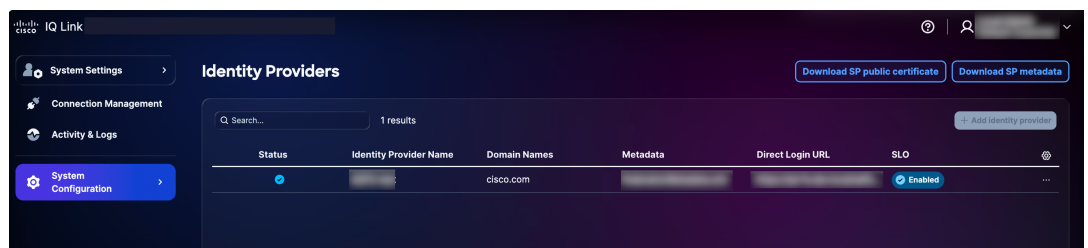
Crear una aplicación empresarial

1. Inicie sesión en el [centro de administración de Microsoft Entra](#).
2. Navegue hasta Identidad > Aplicaciones > Aplicaciones de empresa.
3. Haga clic en Nueva aplicación > Crear su propia aplicación.
4. Introduzca el nombre (por ejemplo, "Cisco IQ").
5. Elija Integrar cualquier otra aplicación que no encuentre en la galería (que no sea la galería).
6. Haga clic en Crear.

Configuración de SAML Single Sign-On

Para configurar el inicio de sesión único SAML, debe cargar el archivo de metadatos SP. Puede obtenerla realizando los siguientes pasos desde el AV:

1. En System Settings, elija System Configuration > Identity Providers. Se muestra la página Identity Providers.



Opciones de descarga

2. Haga clic en Descargar metadatos SP para descargar. Este archivo de metadatos SP descargado se carga para completar la configuración de inicio de sesión único de SAML.
3. Haga clic en el botón Cargar archivo de metadatos para cargar el archivo de metadatos SP. Los datos del archivo de metadatos SP se rellenarán automáticamente en la pantalla Single Sign-on basada en SAML después de una carga correcta.

También puede optar por introducir manualmente estos detalles para configurar los parámetros de inicio de sesión único. Para configurar

manualmente el inicio de sesión único de SAML:

4. En la aplicación Enterprise, navegue hasta Single Sign-on y elija SAML.
5. En la sección Configuración SAML Básica, haga clic en Editar e ingrese lo siguiente:
 - Identificador (Id. de entidad): <YOUR-CIQ-FQDN>
 - URL de respuesta (URL de ACS): https://<YOUR-CIQ-FQDN>/saml/acs
 - URL de inicio de sesión: https://<YOUR-CIQ-FQDN>/saml/login
 - URL de cierre de sesión: https://<YOUR-CIQ-FQDN>/saml/logout
6. Click Save.



Nota: El ID de entidad debe coincidir exactamente con lo que Cisco IQ utiliza como su ID de entidad SP. Este suele ser el FQDN de la implementación.

7. Para configurar atributos y notificaciones SAML, haga clic en Editar en la sección Atributos y notificaciones.
8. Configure las siguientes notificaciones:

Tabla 11: Reclamaciones SAML necesarias

Afirmación	Atributo de origen	Espacio de nombres
Identificador de usuario único (NameID)	user.userprincipalname (predeterminado)	
correo electrónico	user.mail	http://schemas.xmlsoap.org/ws/2005/05/identity
nombre dado	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity
apellidar	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity
nombre grupos	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity
	user.assignedroles	(EMPTY: borra el espacio de nombres)



Nota: Para la reclamación de grupos:

- Utilice user.assignedroles como el origen, no user.groups
- El campo Namespace debe estar vacío. Esto garantiza que el nombre de atributo en la afirmación SAML sea simplemente grupos en lugar de un identificador uniforme de recursos (URI) completo
- No agregue una notificación de grupo duplicada con user.groups, ya que esto provoca conflictos

Configuración de funciones de aplicaciones

Los roles de aplicación se configuran en el registro de aplicación (no en la aplicación de empresa); para configurar las funciones de aplicación:

1. Vaya a Identidad > Aplicaciones > Registros de aplicaciones.
2. Busque y seleccione su aplicación.
3. Vaya a Funciones de aplicación > Crear función de aplicación.
4. Para cada función necesaria, configure lo siguiente:
 - Nombre para mostrar: Por ejemplo, Cisco IQ Admins
 - Tipos de miembros permitidos: Usuarios/grupos
 - Valor: Por ejemplo, Cisco IQ Admins
 - Descripción: Por ejemplo, Cisco IQ Administrators
5. Haga clic en Apply (Aplicar).



Nota: Cree funciones que coincidan con los requisitos de asignación de funciones de Cisco IQ (por ejemplo, Administradores CXIQ, Desarrolladores CXIQ o Visores CXIQ).

Los roles de aplicación se utilizan en lugar de las notificaciones de grupo por los siguientes motivos:

- Los arrendatarios solo en la nube no pueden enviar nombres para mostrar de grupo sin una licencia P1 o P2
- sAMAccountName solo funciona para grupos sincronizados desde AD en las instalaciones
- El origen de ID de grupo envía identificadores únicos universales (UUID) difíciles de asignar
- Los roles de aplicación envían valores de cadena exactos que

coinciden con las expectativas de rol de Cisco IQ

Asignación de usuarios a funciones de aplicaciones

Para asignar usuarios a funciones de aplicación:

1. Vuelva a Aplicación empresarial > Usuarios y grupos.
2. Haga clic en Agregar usuario/grupo.
3. Elija el usuario o usuarios y asigne el rol de aplicación correspondiente.
4. Haga clic en Asignar. Los valores de rol se muestran como cadenas legibles en el atributo de grupos de aserción SAML.

Descarga de metadatos y certificados de IDP

Para descargar metadatos y certificados de IDP:

1. En la aplicación Enterprise, elija Single Sign-On > SAML Signing Certificate.
2. Descargar XML de metadatos de federación (guardar como entra-id-metadata.xml).

O bien

Descargue el certificado (Base64) para la entrada manual del certificado.

3. Tome nota de los siguientes valores de la sección Configuración:
 - URL de inicio de sesión (URL SSO IDP)
 - Azure AD Identifier (ID de entidad IDP)
 - URL de desconexión (URL de IDP SLO)



Nota: Dado que el ID de entrada rota los certificados de firma periódicamente, debe volver a descargar los metadatos y cargarlos en el dispositivo virtual cada vez que cambie el certificado activo para garantizar un servicio SSO ininterrumpido.

Adición de IDP de ID de entrada



Nota: Las rutas APISIX para SAML se crean automáticamente

 cuando se agrega un IDP en Cisco IQ, lo que elimina la necesidad de una configuración de ruta manual.

Para agregar el ID de entrada IDP:

1. Inicie sesión en VA como administrador de cuenta.
2. Vaya a System Settings > System Configuration > Identity Providers.
3. Haga clic en Agregar proveedor de identidad.
4. Introduzca el nombre del IDP (por ejemplo, "ID de entrada").
5. Ingrese el Dominio(s) (por ejemplo, "ciqtestdev.onmicrosoft.com" o el dominio de su compañía).
6. (Opcionalmente) active el botón de alternancia Enable single logout, si es necesario.
7. Arrastre y suelte o cargue el archivo entra-id-metadata.xml obtenido de Entra ID en el campo Upload IDP Metadata.
8. Click Save.

 Nota: El estado sigue siendo "Incompleto" hasta que finalice la asignación de roles; ésta es la conducta esperada.

Configuración de mapeo de roles

Para configurar la asignación de funciones:

1. En el IDP agregado, elija el icono Más opciones> Asignar roles. Se muestra la página Asignar roles de usuario.
2. Introduzca un rol IDP para cada rol del sistema. Se admiten los siguientes roles del sistema:

Tabla 12: Funciones del sistema

Función del sistema	Función IDP (App Role Value)	Descripción
administrador_cuenta_general	Administradores de CXIQ	Permisos completos para todas las acciones

Función del sistema	Función IDP (App Role Value)	Descripción
general_account_viewer	Desarrolladores de CXIQ	Acceso de sólo lectura
general_account_viewer	Visores CXIQ	Acceso de sólo lectura



Nota: Utilice las cadenas App Role Value exactamente como se configuraron en Entra ID (consulte [Configuración de Funciones de Aplicación](#) para obtener más detalles)

4. Click Save. El estado se actualiza a Correcto.

Verificación del Flujo SAML (Autenticación de Contraseña)

Para verificar el flujo SAML:

1. Abra un navegador en modo Incógnito o Privado.
2. Vaya a <https://<YOUR-CIQ-FQDN>/saml/login>.
3. Compruebe que se le redirige a la página de inicio de sesión de Microsoft.
4. Realice la autenticación con sus credenciales (y MFA si se ha configurado).
5. Después de la autenticación, compruebe que se le redirige de nuevo a </saml/acs> y que se muestra la aplicación Cisco IQ.
6. Verifique la extracción del grupo ejecutando el siguiente comando:

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

Resultado esperado

Autenticación compatible con SAML 2.0 correcta para el usuario:
user@domain.com con nombre completo: N/D y 1 grupos

Grupo extraído: Administradores CXIQ (original: CXIQ (administradores))

Total de grupos extraídos: 1

Configuración de la autenticación basada en certificados

En esta sección se describe cómo agregar CBA junto con las contraseñas. Esta sección se puede omitir si la autenticación de solo contraseña es suficiente.

Prerrequisitos de CBA

- Windows Server con AD CS con CA empresarial configurada (por ejemplo, "DEV-ADCS-CA")
- Acceso de administrador de PowerShell en el servidor de la CA
- El certificado UPN debe coincidir con el ID de entrada `userPrincipalName`
- El punto de distribución CRL debe estar accesible desde Internet

Creación de una plantilla de certificado en AD CS

1. Abra `certtmpl.msc` en el servidor de la CA.
2. Duplique la plantilla User y asígnele el nombre "EntraUserCert".
3. Configuración de la plantilla:
 - General: Nombre para mostrar EntraUserCert, validez 1-2 años
 - Gestión de solicitudes: Objetivo = Firma y cifrado
 - Nombre del sujeto: Seleccione Aprovisionar en la solicitud
 - Extensiones: Las políticas de aplicación deben incluir autenticación de cliente (1.3.6.1.5.5.7.3.2)
 - Seguridad: Conceder permisos de lectura e inscripción a usuarios autenticados
4. Publique la plantilla mediante el siguiente comando:

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

Solicitud y emisión de un certificado de usuario

1. Cree un archivo de configuración de certificados (INF) (por ejemplo, `C:-cert.inf`) mediante el siguiente script de PowerShell:

@"

```

[Version]
Signature = ``$Windows NT`$"
[NewRequest]
Subject = "CN=

"

KeyLength = 2048
KeySpec = 1
KeyUsage = 0xa0
MachineKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
RequestType = PKCS10
[RequestAttributes]
CertificateTemplate = EntraUserCert
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.2
OID = 1.3.6.1.4.1.311.20.2.2
[Extensions]
2.5.29.17 = "{text}"
_continue_ = "upn=

&"
_continue_ = "email=

"
"@ | Out-File -FilePath C:-cert.inf -Encoding ASCII

```

2. Sustituya <USER-UPN> por su ID de usuario UPN (por ejemplo, user@ciqtestdev.onmicrosoft.com).

3. Para generar el certificado, ejecute los siguientes comandos:

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

4. Para enviar la solicitud a la CA, ejecute el siguiente comando:

```
certreq -submit -config "
```

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

5. Para instalar el certificado en la CA, ejecute el siguiente comando:

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

Exportación de certificados

Para exportar el certificado de usuario como un archivo PFX (para el cliente), ejecute la siguiente secuencia de comandos:

```
$cert = Get-ChildItem Cert:| Where-Object { $_.Subject -like "*"
*"} }
$password = ConvertTo-SecureString -String "
" -Force -AsPlainText
Export-PfxCertificate -Cert $cert -FilePath C:-cert.pfx -Password $password
```

Para exportar el certificado raíz de la CA (para el ID de entrada), ejecute el siguiente script:

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

Importación del certificado de usuario en el equipo cliente (MacOS)

Para importar el certificado de usuario (PFX), ejecute el siguiente comando:

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

”

Para importar el certificado raíz de la CA, ejecute el siguiente comando:

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

Para establecer el certificado de la CA en Confiar siempre en el Acceso mediante Cadena de Llave:

1. Abra Acceso mediante llavero.
2. Busque el certificado de la CA y haga clic en Obtener información.
3. En Confianza, establezca en "Confiar siempre".



Nota: Después de la importación, salga del explorador y vuelva a abrirlo para que se reconozca el certificado.

Carga del certificado raíz de la CA en la ID de entrada

1. Inicie sesión en el [centro de administración de Microsoft Entra](#).
2. Vaya a Protección > Seguridad > Autoridades de certificados.
3. Haga clic en Upload y seleccione el archivo ca-root.cer.
4. Marcarlo como certificado de CA raíz.
5. Introduzca la URL del punto de distribución de CRL (debe ser accesible públicamente).

Habilitación de CBA en Métodos de Autenticación de Entra ID

1. Navegue hasta Protección > Métodos de autenticación > Políticas.
2. Haga clic en Autenticación basada en certificados para configurar.
3. Habilite CBA y agregue los usuarios o grupos de destino.
4. En Configurar, establezca el nivel de protección en Autenticación de

factor único.

Configuración de Username Binding

En la configuración de CBA, vaya a la pestaña Enlace de nombre de usuario y establezca el siguiente enlace:

- Campo de certificado: NombrePrincipal
- Atributo de usuario: userPrincipalName

De este modo, se asigna el UPN en el nombre alternativo de asunto (SAN) del certificado al usuario de ID de entrada.

Verificación del flujo de CBA

1. Abra un navegador en modo Incógnito o Privado.
2. Vaya a <https://<YOUR-CIQ-FQDN>/saml/login>.
3. En la página de inicio de sesión de Microsoft, introduzca el correo electrónico del usuario y haga clic en Next.
4. Elija Utilizar un certificado o una tarjeta inteligente (o puede que se solicite automáticamente).
5. Elija el certificado de usuario aplicable cuando el explorador solicite la selección de certificados.
6. Verifique que Entra ID valida el certificado, redirige con una respuesta SAML y crea una sesión.



Nota: Asegúrese de seleccionar el certificado de cliente correcto. La selección de un certificado incorrecto (por ejemplo, un certificado de usuario diferente o un certificado caducado) provoca un error de autenticación.

Resolución de problemas de ID entrante

La siguiente lista describe los problemas comunes y las posibles soluciones para ayudar a identificar y resolver rápidamente los problemas relacionados con la configuración SAML de Entra ID.

Tabla 13: Resolución de problemas

Problema	Causa	Corregir
Respuesta SAML no	La afirmación	Verifique la configuración de

Problema	Causa	Corregir
válida; falta correo electrónico	SAML no tiene ningún atributo NameID o email	notificaciones de ID de entrada (consulte Configuración del inicio de sesión único de SAML para obtener más detalles). Compruebe que el usuario ha rellenado el atributo de correo.
Total de grupos extraídos: 0	Los grupos afirman que no están configurados o que el origen es incorrecto	Utilice user.assignedroles como origen. Asegúrese de que el usuario esté asignado a un rol de aplicación (consulte Asignación de usuarios a roles de aplicación para obtener más detalles).
Reclamaciones de grupos duplicados	Tanto user.groups como user.assignedroles están activos	Quite la notificación user.groups. Mantener sólo user.assignedroles.
Grupos que se muestran como UUID	El atributo de origen es "Group ID"	Utilice el enfoque Funciones de aplicación (consulte Configuración de funciones de aplicación para obtener más detalles).
El nombre del atributo muestra un URI largo	El campo Espacio de nombres no está vacío	Borre el campo Espacio de nombres en la configuración de notificación de grupos.
Firma SAML no válida	Certificado IdP girado o no coincide	Vuelva a descargar los metadatos de la ID de entrada y vuelva a cargarlos en Cisco IQ. Publique la CRL en una URL de acceso público o utilice el enfoque de CA autofirmada (consulte Solución alternativa de CRL para problemas de disponibilidad para obtener más detalles).
ADSTS500191	CRL no accesible desde Internet	Verifique que el certificado de usuario se importe en MacOS Keychain Access (consulte Importación del certificado de usuario en la máquina cliente (MacOS) para obtener más detalles), CBA esté habilitado en Entra ID con la configuración
Certificado no solicitado	El certificado no está en la cadena de claves, la CA no es de confianza en el cliente o el CBA no está habilitado	

Problema	Causa	Corregir
		necesaria (consulte Habilitación de CBA en Métodos de Autenticación de Entra ID para obtener más detalles) y Chrome se reinicie para aplicar los cambios.
Afirmación SAML caducada	Diferencia de reloj entre sistemas	Aumente clock_skew_seconds en la configuración del plugin (el valor predeterminado es 300; utilizar 30000 para el laboratorio).
Estado "Incompleto" en el dispositivo virtual	Asignación de roles aún no configurada	Completar la asignación de funciones (consulte Configuración de la asignación de funciones para obtener más detalles).

Solución alternativa de CRL para problemas de disponibilidad

Si el punto de distribución de CRL de su CA no está accesible desde Internet (lo habitual en las configuraciones de laboratorio), utilice una CA autofirmada sin requisitos de CRL:

```
powershell
# Create self-signed CA
$rootCA = New-SelfSignedCertificate `
-Subject "CN=CIQ-Test-CA" `
-CertStoreLocation "Cert:" `
-KeyUsage CertSign, CRLSign `
-KeyLength 2048 `
-NotAfter (Get-Date).AddYears(5) `
-TextExtension @"2.5.29.19={text}ca=TRUE"@
# Create user cert signed by the CA
$userCert = New-SelfSignedCertificate `
-Subject "CN=
" `
-CertStoreLocation "Cert:" `
-Signer $rootCA `
-KeyUsage DigitalSignature `
-KeyLength 2048 `
-NotAfter (Get-Date).AddYears(2) `
-TextExtension @"2.5.29.37={text}1.3.6.1.5.5.7.3.2",
"2.5.29.17={text}upn=
```


&email=

”

)

Cargue sólo el certificado de CA raíz en la ID de entrada. Dado que se firma automáticamente sin el protocolo de detección de Cisco (CDP), el ID de entrada no intenta la validación de CRL.

Lista de comprobación de configuración completa

En esta sección se describe una lista de comprobación de configuración completa para configurar el AV con la aplicación SAML Microsoft Entra ID y CBA opcional.

Configuración de aplicación SAML de ID de entrada

- Crear una aplicación empresarial (que no sea una galería) en Id. de entrada
- Configurar una configuración básica de SAML introduciendo manualmente los metadatos SP
- Configurar atributos y reclamaciones (incluidos correo electrónico, nombre y grupos con user.assignedroles)
- Crear funciones de aplicaciones en el registro de aplicaciones
- Asignar usuarios a funciones de aplicación
- Descargar XML de metadatos de federación

Configuración de Cisco IQ

- Añadir un IDP en Cisco IQ cargando los metadatos de la ID de entrada
- Configuración de la asignación de funciones para asignar valores de funciones de aplicaciones a funciones del sistema Cisco IQ
- Verificar que el inicio de sesión basado en contraseña funcione de

extremo a extremo

- Comprobar que los grupos se extraen correctamente en los registros

Autenticación basada en certificados (opcional)

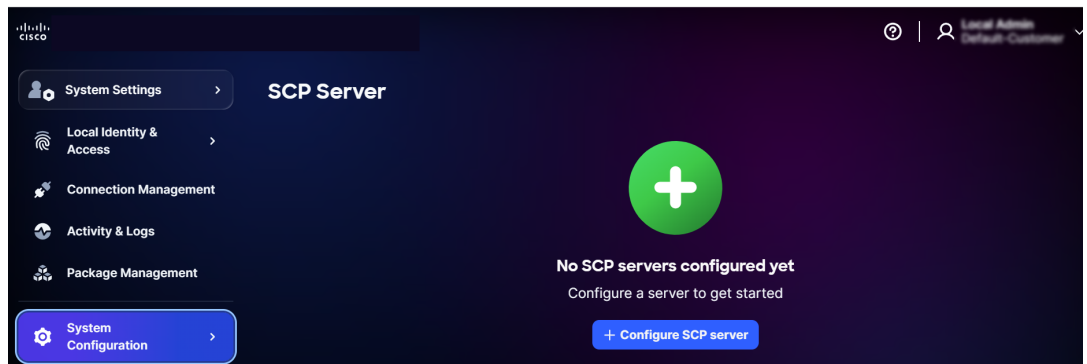
- Crear plantilla de certificado en AD CS con EKU de autenticación de cliente
- Emita un certificado de usuario con un UPN que coincida con el usuario de ID de entrada
- Exportar un certificado de usuario como archivo PFX e instalarlo en el equipo cliente
- Confiar en el certificado de la CA en el equipo cliente
- Cargue el certificado raíz de la CA a la ID de entrada en Protección > Autoridades de certificados
- Habilite el CBA en los métodos de autenticación
- Configurar enlace de nombre de usuario (PrincipalName y userPrincipalName)
- Verificar que el inicio de sesión de CBA funciona de extremo a extremo

Adición de un servidor SCP

Un servidor SCP es un requisito previo para importar archivos de actualización que son esenciales para agregar, actualizar o reparar la instalación de Cisco IQ.

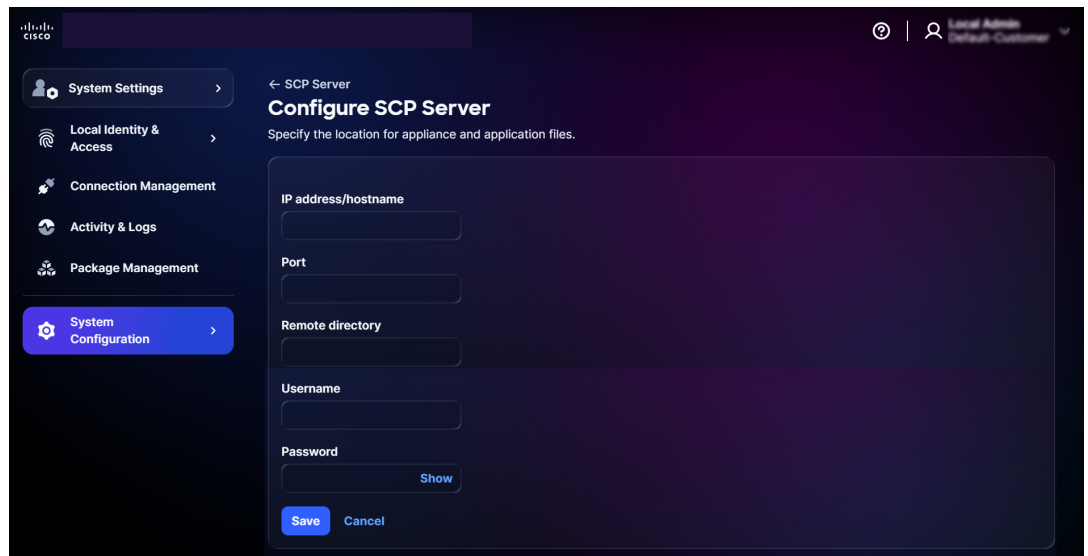
Para agregar un servidor SCP:

1. En System Settings, elija System Configuration > SCP Server. Se muestra la página SCP Server.



Página de inicio del servidor SCP

2. Haga clic en Configure SCP server. Se muestra la página Configure SCP Server.



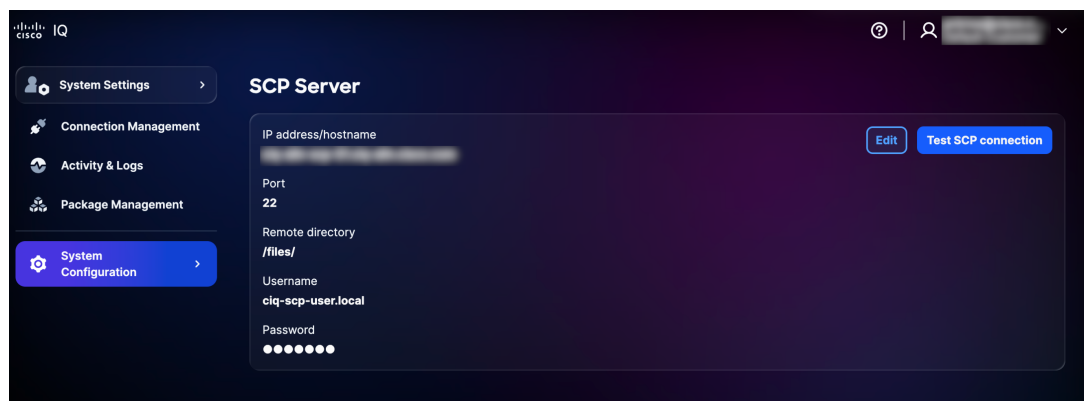
Configuración del servidor SCP

3. Introduzca una dirección IP/nombre de host.
4. Introduzca un puerto.
5. Introduzca un directorio remoto.
6. Introduzca un nombre de usuario.
7. Ingrese una contraseña.
8. Click Save. Aparecerá una confirmación.

Edición de un servidor SCP existente

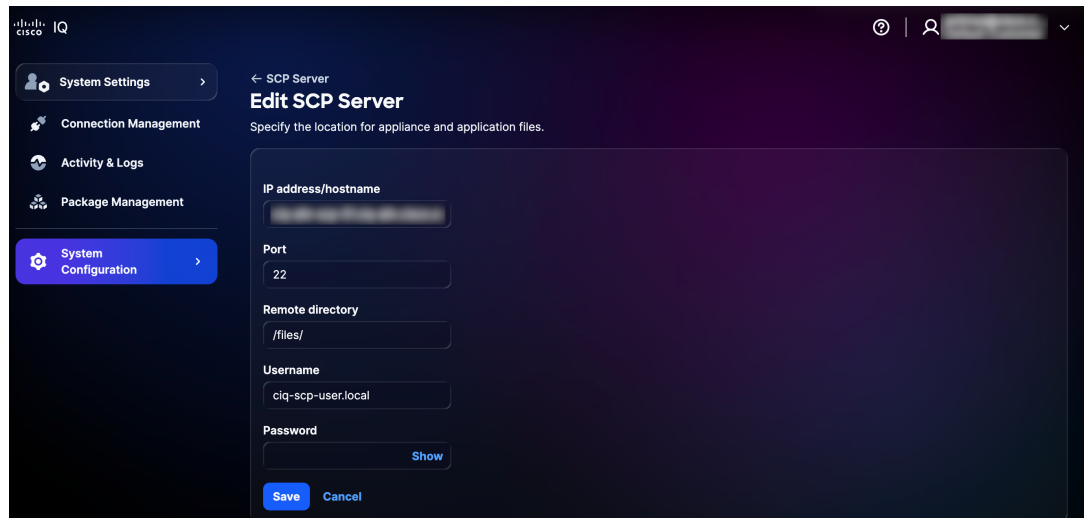
Para editar un servidor SCP existente:

1. Vaya a la página SCP Server.



Servidor SCP agregado

2. Haga clic en Editar del servidor SCP existente que desee.



Edición del servidor SCP

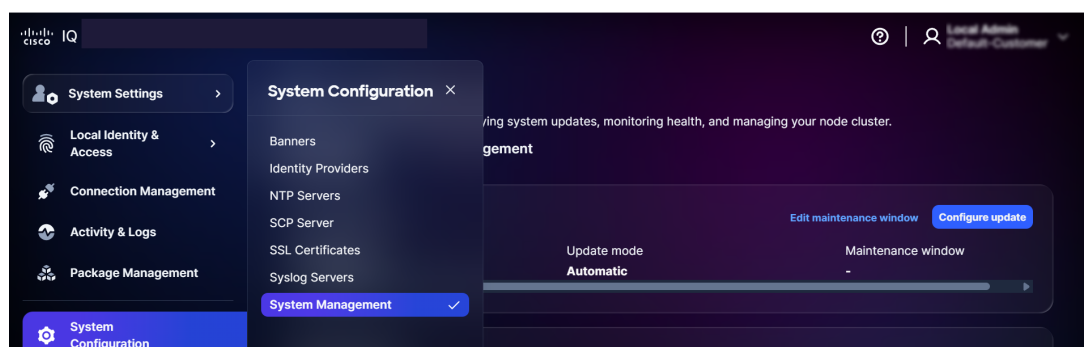
3. Modifique los detalles según sea necesario.
4. Click Save.

Administración del sistema

Puede actualizar a la última versión de Cisco IQ VA a través de la interfaz de usuario. También puede verificar desde la página Cisco IQ Data Connectors.

Reprogramación de actualización del sistema

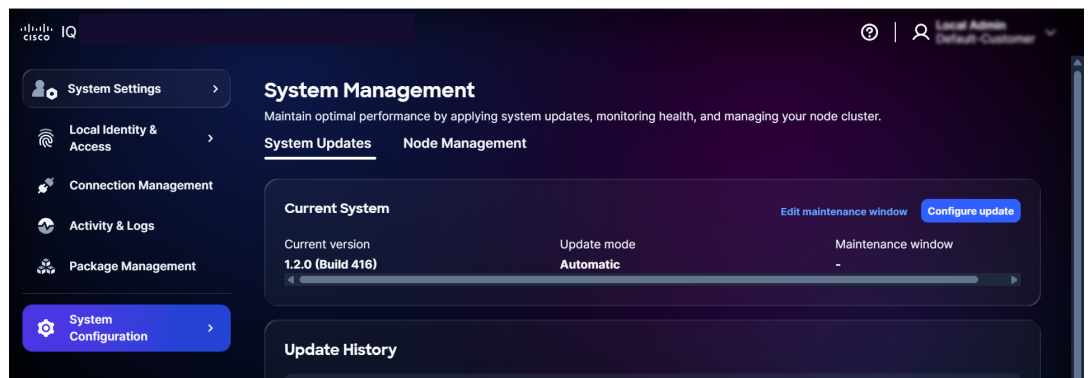
Para reprogramar la actualización del sistema:



Administración del sistema

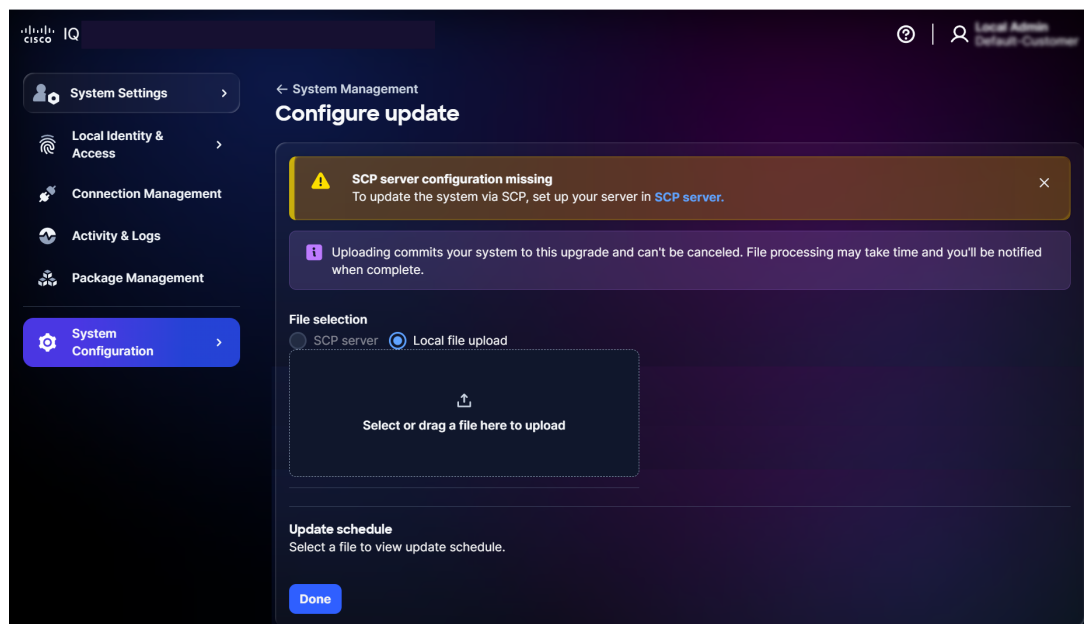
1. En System Settings, elija System Configuration > System Management. Se muestra la página Administración del sistema. Esta página muestra la versión del sistema que se está ejecutando

actualmente; si no se ha configurado ninguna actualización, la sección Historial de actualizaciones está vacía.



Actualización del sistema

2. Haga clic en Configurar actualización. Se muestra la página Configurar actualización.



Configurar actualización

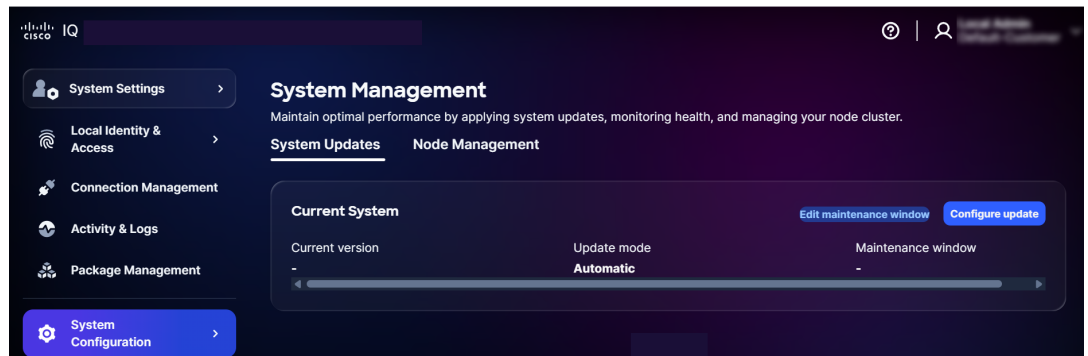
3. Elija la programación de actualización para programar otra hora.
4. Espere a que se complete la carga del archivo; la duración depende del tamaño del paquete y de la velocidad de la red.

Confirme la actualización correcta comprobando el icono de marca de verificación que aparece en la columna Estado de actualización.

Edición de programaciones de actualización del sistema

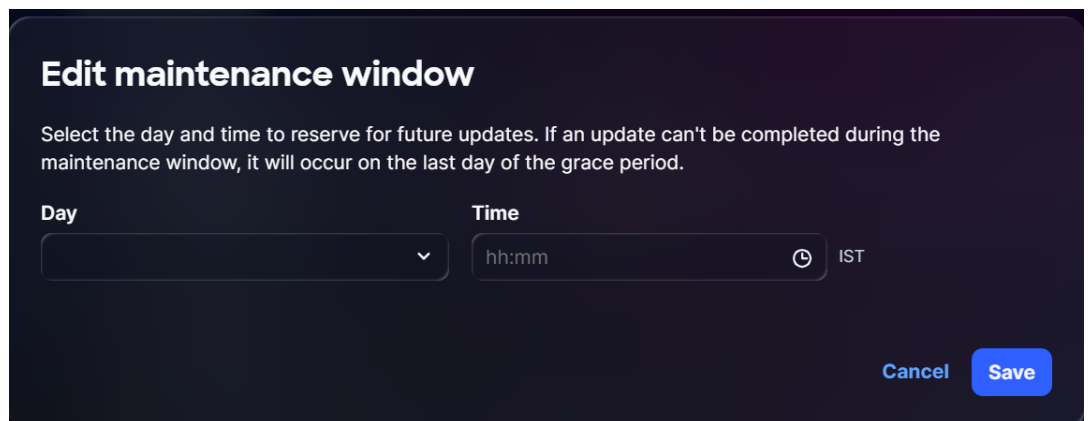
Puede crear una programación personalizada para las actualizaciones del sistema. Si se configura una programación personalizada, las

actualizaciones se realizan en fechas definidas por el usuario siempre que permanezcan dentro del período de gracia máximo. Para crear una programación de actualización del sistema:



Editar mantenimiento

1. En la sección Sistema actual de la página Administración del sistema, haga clic en Editar ventana de mantenimiento.



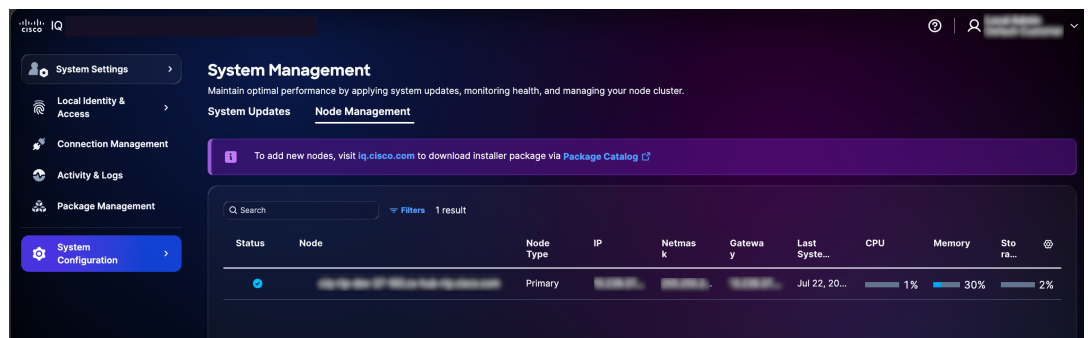
Editar ventana de mantenimiento

2. Elija una opción de las listas desplegables Día y Hora.
3. Haga clic en Guardar. La ventana de mantenimiento se ha programado correctamente. La actualización se desencadena según la programación mostrada.

 **Nota:** Si no se configura ninguna programación de actualización, el sistema establece de forma predeterminada períodos de gracia de dos (2) semanas para las actualizaciones sin reinicio y de cuatro (4) semanas para las actualizaciones que requieren reinicio. Después de estos períodos de gracia, las actualizaciones se deben realizar manualmente. En caso de que se produzca un fallo en la actualización, el sistema realiza hasta dos (2) reintentos automáticos. Se ha programado un tercer intento, pero es necesario iniciarlo manualmente.

Gestión de nodos

1. Vaya a System Configuration > System Management > Node Management para ver y administrar los nodos del clúster.



Gestión de nodos

2. La lista de nodos muestra el estado, el nombre de host, el tipo de nodo, la dirección IP, la máscara de red, la puerta de enlace y la hora de la última sincronización de cada nodo.

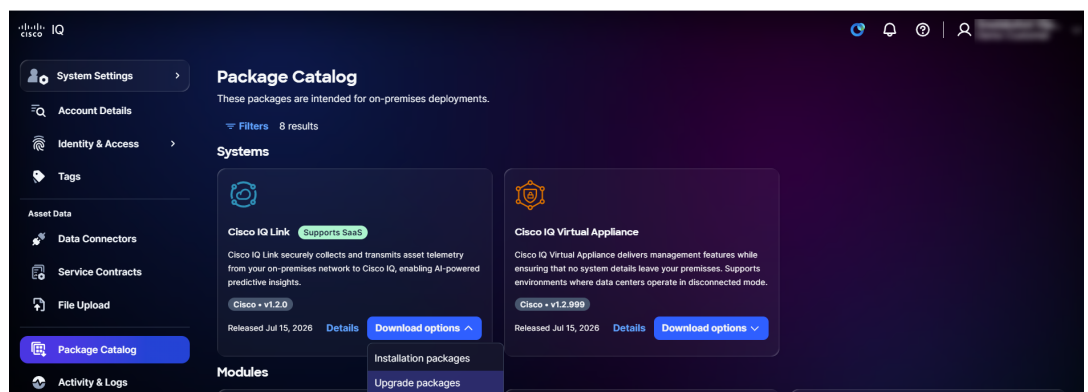


Nota: Una marca de verificación azul en la columna Estado indica que el nodo está activo.

Actualización manual del sistema

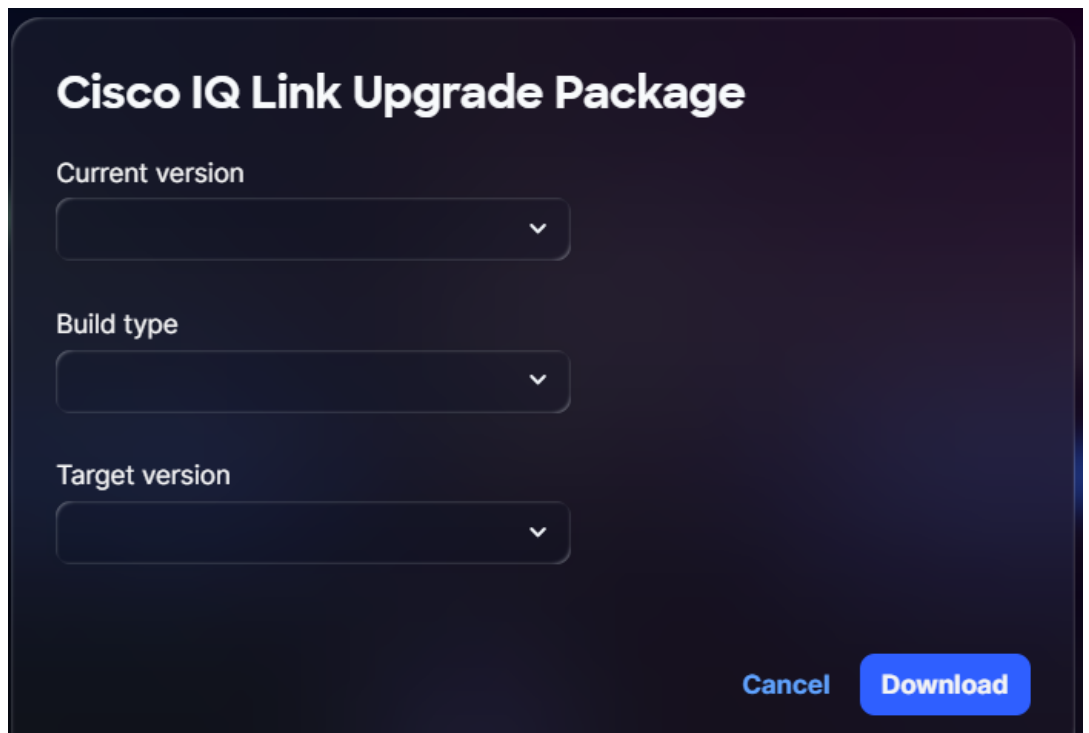
En situaciones en las que la distribución automática de Cisco IQ SaaS no está disponible o se ha retrasado, puede realizar manualmente una actualización del sistema descargando el paquete de actualización directamente desde Cisco IQ SaaS. Para actualizar manualmente el sistema:

1. Inicie sesión en [Cisco IQ SaaS](#).
2. Vaya a Inicio > Configuración del sistema > Catálogo de paquetes.



Catálogo de software

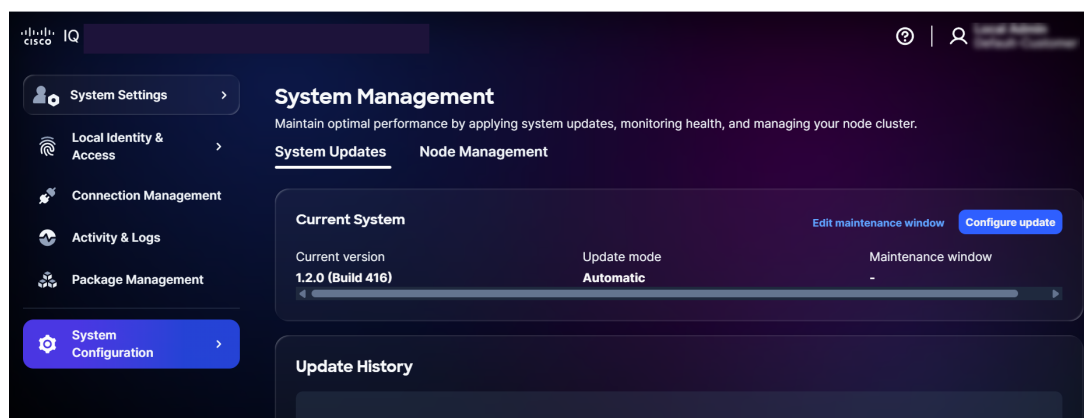
3. En la tarjeta de Cisco IQ Virtual Appliance, haga clic en Opciones de descarga > Paquetes de actualización.



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

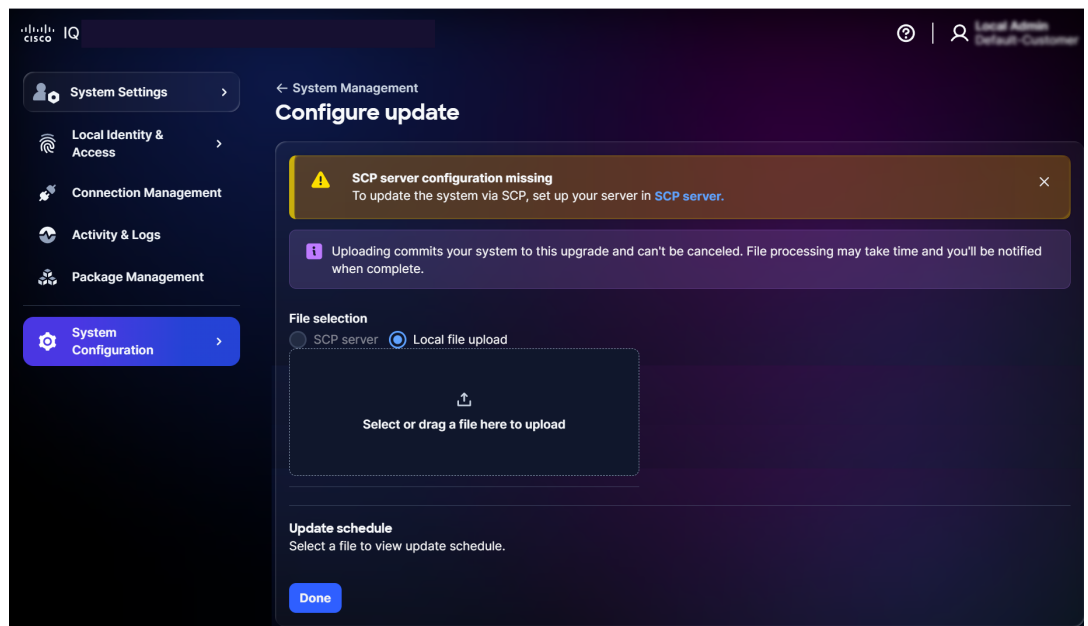
Paquete de actualización

4. Elija la versión actual en la lista desplegable.
5. Elija el tipo de generación en la lista desplegable.
6. Elija la versión de destino en la lista desplegable.
7. Haga clic en Descarga. Se descarga el paquete de actualización.
8. Vaya a Cisco IQ VA.
9. En System Settings, elija System Configuration > System Management.



Configurar actualización

10. Haga clic en Configurar actualización.



Carga de archivos locales

11. Haga clic en el botón de opción Carga de archivo local.

12. Seleccione o arrastre el archivo de paquete de actualización descargado al campo de carga.

13. Espere a que se complete la carga del archivo; la duración depende del tamaño del paquete y de la velocidad de la red.

Configuración de certificados SSL

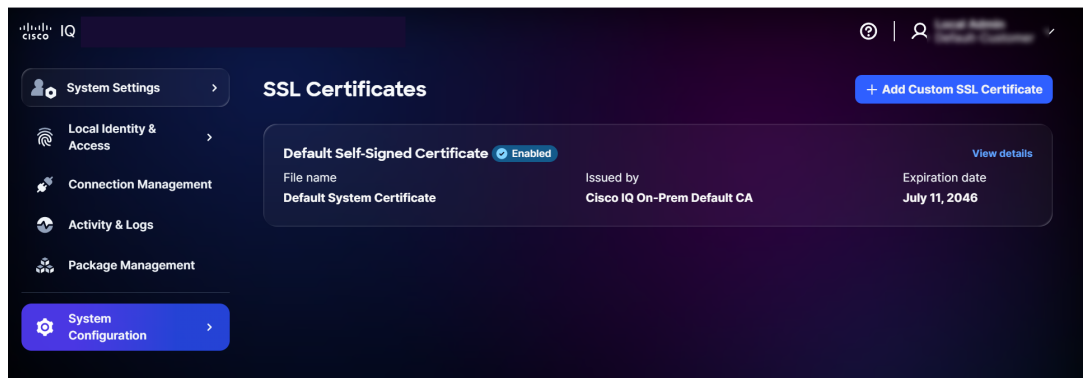
Un certificado autofirmado predeterminado está preinstalado y habilitado en Cisco IQ, pero puede cargar opcionalmente certificados SSL personalizados. Cuando se habilita un certificado SSL personalizado, se utiliza para conexiones HTTPS; si el certificado está deshabilitado o eliminado, el sistema vuelve automáticamente al certificado predeterminado. El certificado SSL predeterminado no se puede editar ni eliminar.

 Nota: El certificado debe tener al menos 90 días de validez restantes. Se considera que un certificado está "a punto de caducar" cuando le quedan menos de 90 días para su caducidad. Después de agregar, editar o eliminar un certificado SSL, debe cargar el nuevo certificado SSL como se describe en [Completar la Configuración de SLO](#) para Okta IDP o ADFS IDP.

Agregar certificado SSL personalizado

Para agregar un certificado SSL personalizado:

1. En System Settings, elija System Configuration > SSL Certificates. Se muestra la página SSL Certificates, que enumera todos los certificados SSL del sistema.

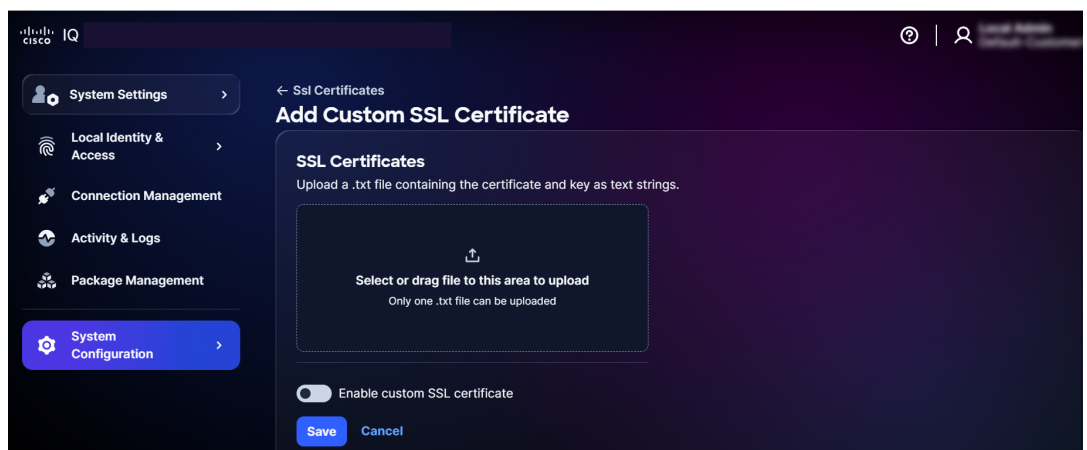


Agregando certificado SSL

2. Haga clic en Agregar certificado SSL personalizado.



Nota: Cargue un archivo .txt que incluya el certificado y la clave codificados en Privacy-Enhanced Mail como cadenas de texto. Sólo se puede cargar un archivo .txt cada vez. El archivo debe contener el certificado y la clave privada.



Cargar certificado SSL

3. Arrastre y suelte o cargue el certificado SSL personalizado en la sección Certificado SSL.
4. Active el botón de alternancia Habilitar certificado SSL personalizado.

Enable Certificate?

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

Cancel

Enable certificate

Habilitar certificado



Nota: Mantenga la tecla de apagado si desea cargar el certificado sin activarlo inmediatamente.

5. Haga clic en Habilitar certificado.

6. Click Save.

El certificado SSL personalizado está activado y activo. El certificado predeterminado del sistema se desactiva automáticamente.

Editar certificado SSL personalizado

Puede editar el certificado SSL personalizado para cargar un nuevo certificado o para deshabilitar el certificado habilitado actualmente. Para editar:

1. Vaya al certificado SSL personalizado que desee.

2. Elija el icono Más opciones > Editar. Se muestra la página Editar Certificado SSL.

3. Edite los detalles del certificado según sea necesario.

4. Click Save.

Eliminando certificado SSL personalizado

Advertencia: Un certificado SSL personalizado se puede eliminar en cualquier momento, pero es una acción irreversible; puede cargar un nuevo certificado personalizado en cualquier momento después de la eliminación.

Para eliminar:

1. Desplácese hasta el certificado SSL personal deseado.

2. Elija el icono Más opciones > Eliminar.
3. Haga clic en Eliminar certificado. El certificado personalizado se elimina y el certificado predeterminado se reactiva automáticamente.

Configuración del servidor Syslog

Los usuarios con la función de administrador de cuentas pueden configurar servidores syslog externos para exportar registros del sistema. Se pueden configurar hasta dos (2) servidores syslog.

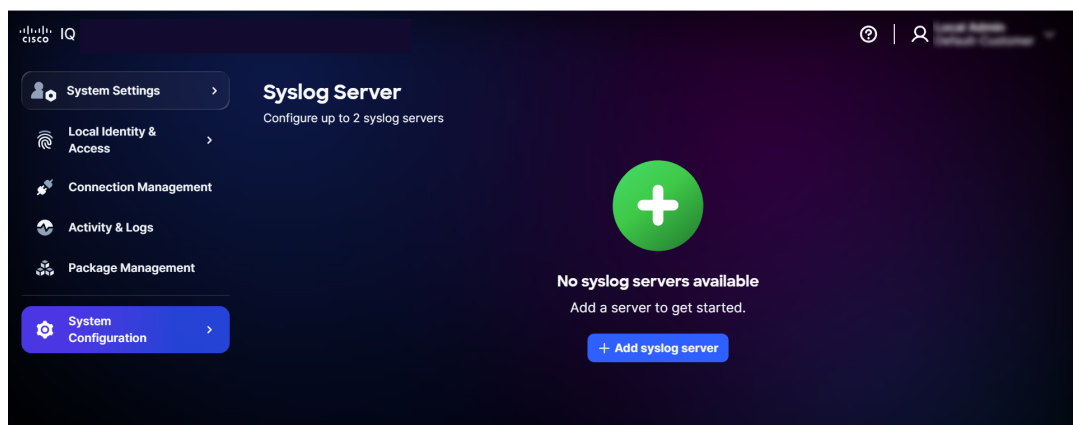


Nota: El servidor Syslog debe especificarse como una dirección IP y no como un nombre de dominio completo (FQDN).

Agregando servidor Syslog

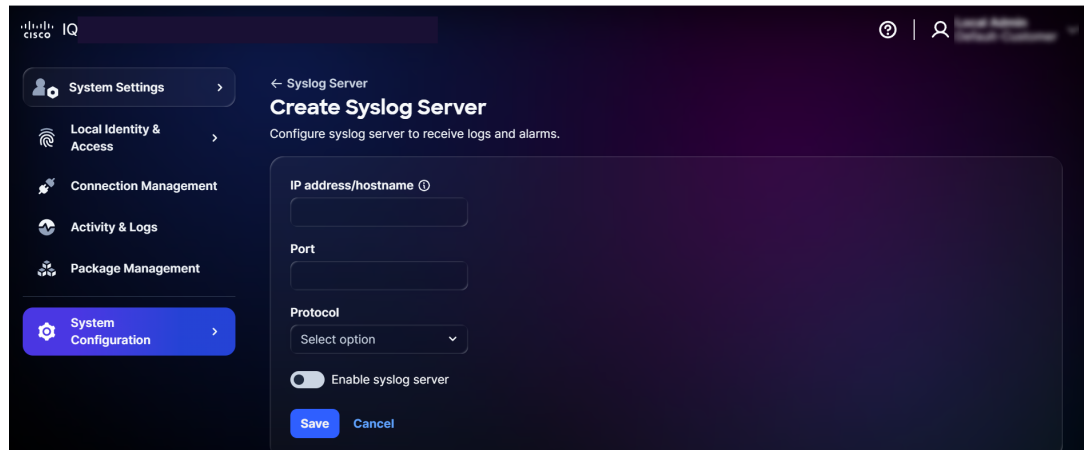
Para agregar un servidor syslog:

1. En System Settings, elija System Configuration > Syslog Server. Se muestra la página Syslog Server.



Agregar servidor Syslog

2. Haga clic en Add syslog server. Se muestra la página Create Syslog Server.



Crear servidor Syslog

3. Introduzca la dirección IP/nombre de host.
4. Ingrese Port.
5. Seleccione el protocolo aplicable en la lista desplegable Protocol (por ejemplo, UDP, TCP).
6. Active el botón de alternancia Enable syslog server.
7. Click Save. Aparecerá una confirmación y el servidor syslog recién agregado aparecerá en la página de inicio del servidor Syslog.

Edición del servidor Syslog configurado

Para editar un servidor syslog configurado:

1. Desplácese hasta el servidor syslog deseado.
2. Elija el icono Más opciones > Editar. Se muestra la página Edit Syslog Server.
3. Edite los detalles o desactive la opción Enable syslog server, según sea necesario.
4. Click Save.

Eliminación del servidor Syslog configurado

Para eliminar un servidor syslog configurado:

1. Desplácese hasta el servidor syslog deseado.
2. Elija el icono Más opciones > Eliminar. Aparecerá una confirmación.
3. Haga clic en Delete syslog server.

Actividad y registros

Activity & Logs proporciona un registro detallado de las acciones y cambios de los usuarios en Cisco IQ, lo que permite a los administradores de cuentas realizar un seguimiento de las actividades de los usuarios y mantener la transparencia.

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

Actividad y registros

Para ver la actividad y los registros, seleccione Activity & Logs en el menú System Settings.

Actividad y registros:

- Registra todas las operaciones de la API en el nivel de gateway
- Admite filtros, paginación y funciones de búsqueda para ayudarle a encontrar y administrar información con facilidad

Están disponibles las siguientes opciones de filtro:

- Fecha de la última sesión: Filtra los registros a un rango de tiempo específico
- Nivel de registro: Filtra los registros por gravedad (por ejemplo, error, advertencia e información)
- Tipo de actividad: Filtra los registros por tipo de actividad del sistema
- Código de error: Filtra por un código de error específico

Banners

Los administradores de cuentas pueden configurar banners para todo el

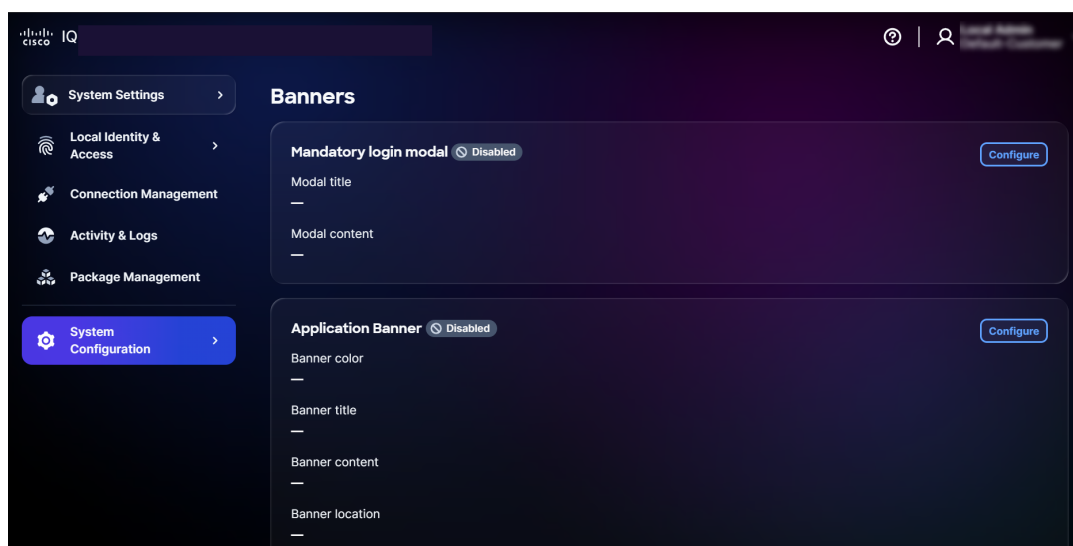
sistema con el fin de cumplir los estándares de seguridad y cumplimiento.

- Modal de inicio de sesión obligatorio: Debe confirmar el banner obligatorio antes de pasar a la pantalla de inicio de sesión.
- Banner de aplicación: Se trata de banners personalizados que se muestran en toda la aplicación después de una autenticación correcta.

Configuración de Banners Modales de Login Obligatorios

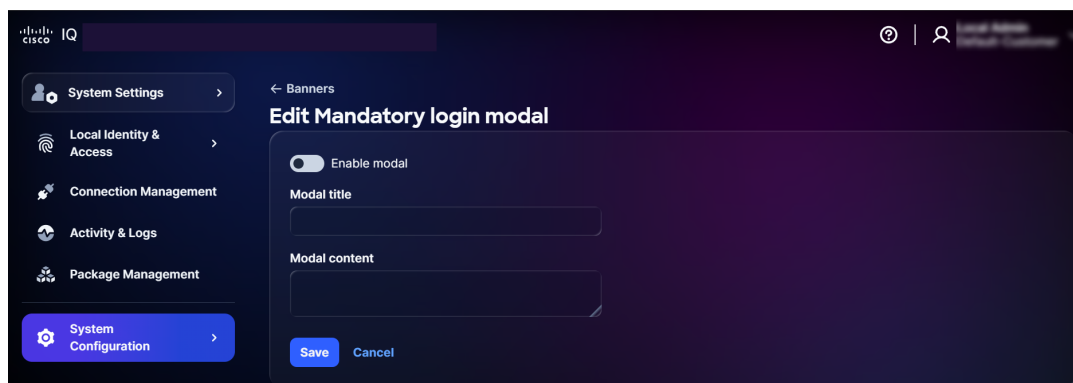
Para configurar un banner obligatorio:

1. En System Settings, elija System Configuration > Banners. Se muestra la página Banners.



Configurar banner obligatorio

2. Haga clic en Configure en el modal de login obligatorio. Se muestra la página Editar modal de inicio de sesión obligatorio.



Editar Banner modal de inicio de sesión obligatorio

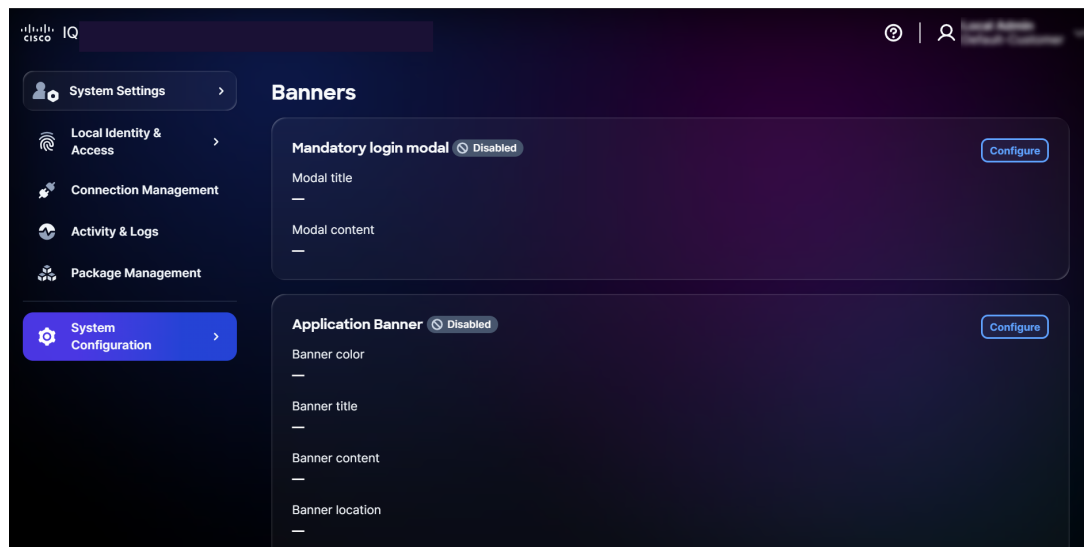
3. Haga clic en el botón para activar o desactivar el banner.

4. Introduzca el título Modal.
5. Ingrese el contenido Modal.
6. Click Save. Se guarda el modo de inicio de sesión obligatorio.

Configuración de banners de aplicaciones

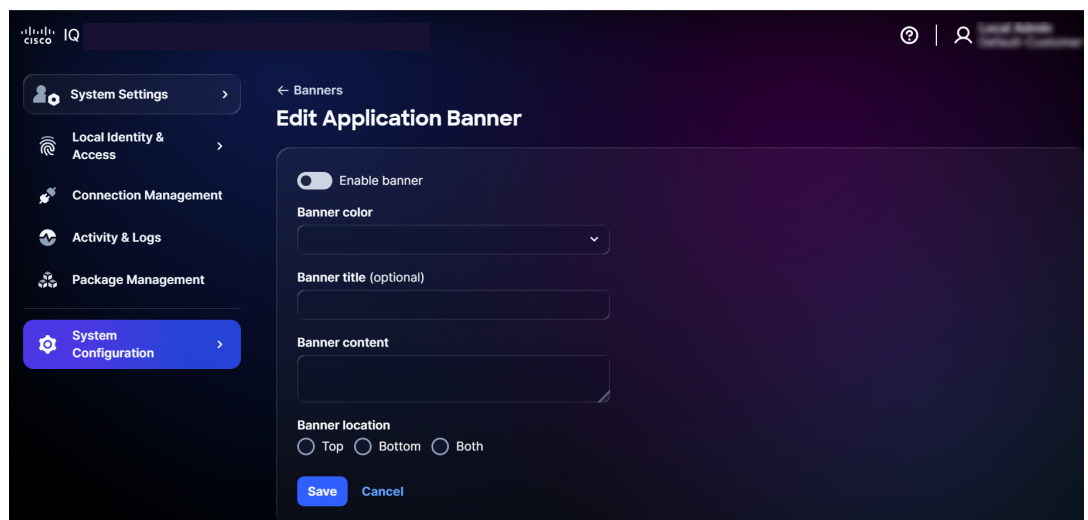
Para configurar un banner de aplicación:

1. En System Settings, elija System Configuration > Banners. Se muestra la página Banners.



Banner de configuración

2. Haga clic en Configurar en el banner de aplicación. Se muestra la página Editar anuncio de aplicación.



Banner de Editar aplicación

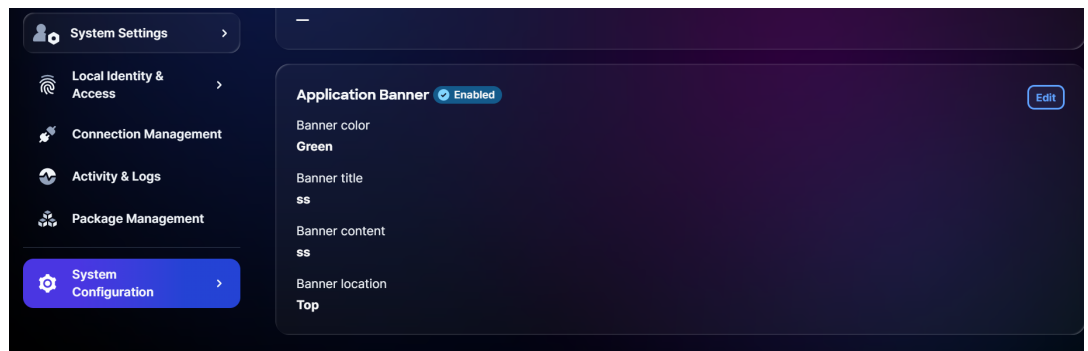
3. Haga clic en el botón para activar o desactivar el banner.

4. Elija un color de banner.
5. Introduzca el título del banner.
6. Introduzca el contenido del banner.
7. Elija una ubicación de banner.
8. Click Save. El banner se muestra en toda la aplicación.

Edición de banners

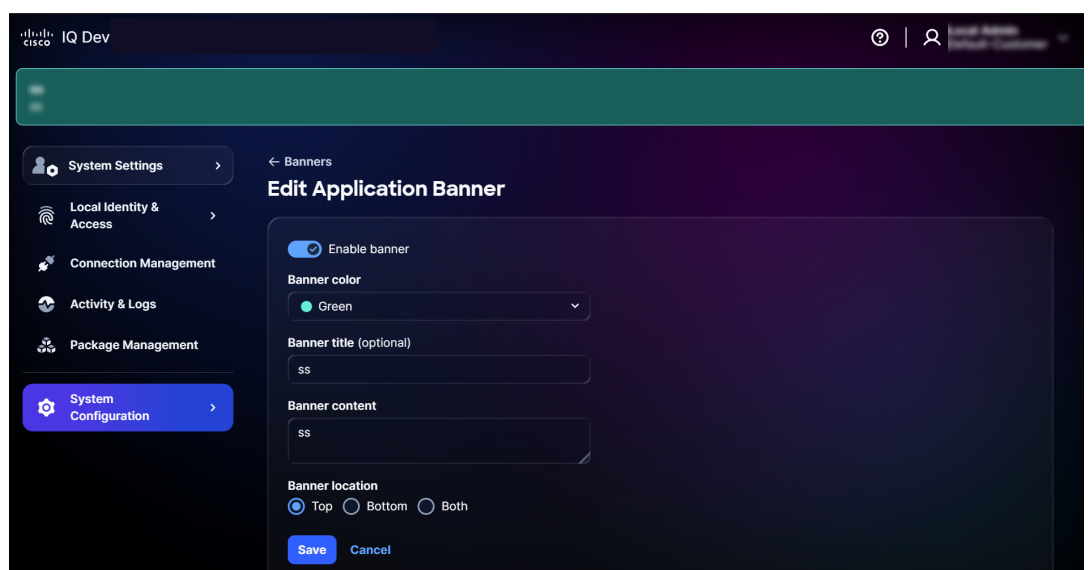
Para editar un banner:

1. En System Settings, elija System Configuration > Banners. Se muestra la página Banners.



Editar banners

2. Haga clic en Editar. Se muestra la página Editar anuncio de aplicación.



Banner de Editar aplicación

3. Edite los detalles que desee.

4. Haga clic en el botón para activar o desactivar el banner.
5. Click Save.

Resolución de problemas

Puede recopilar archivos de diagnóstico y de registro del sistema Cisco IQ y transferirlos de forma segura a un servidor SCP. Estos archivos se pueden compartir con el equipo de soporte técnico al informar sobre problemas para proporcionar un contexto valioso y ayudar con la resolución de problemas.

Para recopilar archivos de diagnóstico y de registro:

1. Inicie sesión en Cisco IQ.



Menú principal

2. En el menú principal de Cisco IQ, introduzca "3" y pulse Intro para seleccionar Diagnóstico del sistema.

```

  CSO 10

Navigation Main Menu > System Diagnostics

Please provide the following server connection details:

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

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

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

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

```

Diagnóstico del sistema

3. Introduzca la dirección del servidor SCP/SFTP.
4. Introduzca el puerto del servidor SCP/SFTP.
5. Introduzca la ruta del servidor SCP/SFTP.
6. Seleccione un protocolo.
7. Introduzca el nombre de usuario.
8. Ingrese la contraseña.
9. Ingrese "C" y presione Enter para continuar con el diagnóstico del sistema.



```
Navigation Main Menu > System Diagnostics

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

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

Operación de diagnóstico del sistema finalizada

El sistema inicia el proceso de diagnóstico y realiza las siguientes acciones:

- Comprobación de disponibilidad
- Recopilación de información del sistema
- Recopilación de información de Kubernetes
- Recopilación de registros
- Preparación del paquete de diagnósticos del sistema
- Cargando paquete de diagnósticos del sistema

Una vez completada, se muestra un mensaje de confirmación que indica el nombre del paquete generado.

Módulo de soporte

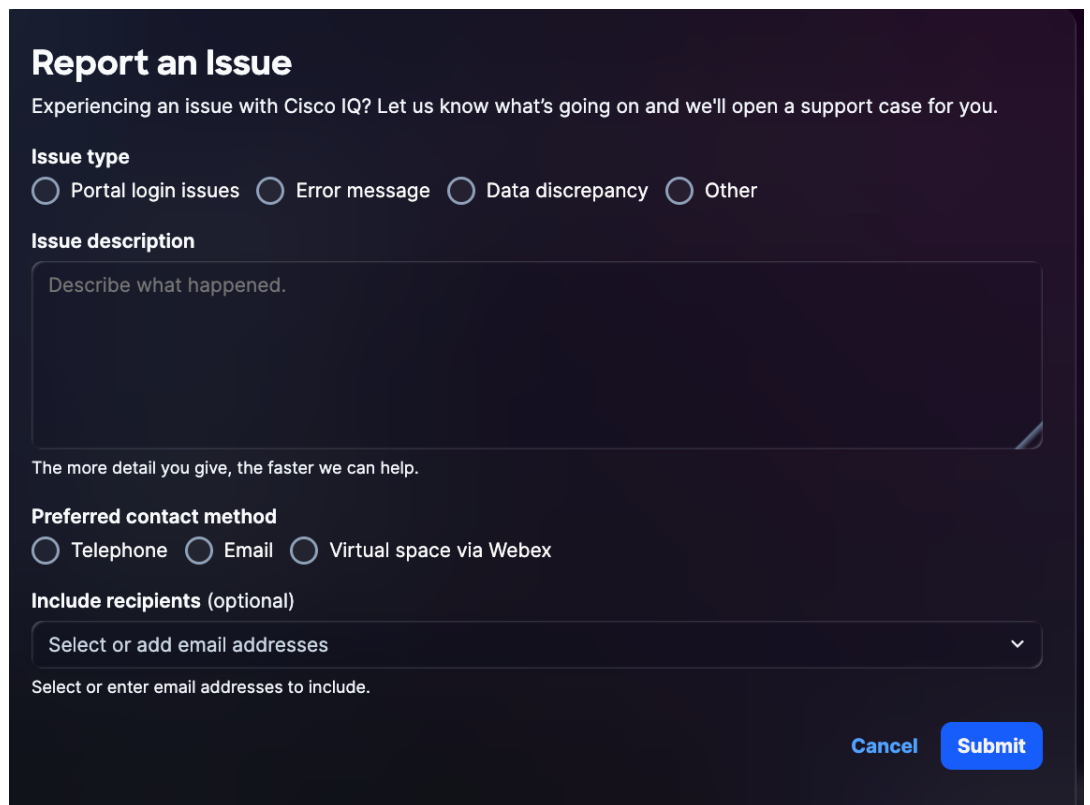
Puede crear casos de asistencia específicos de módulos y de dispositivos virtuales desde Cisco IQ SaaS. El módulo Support está disponible en Cisco IQ SaaS y ofrece una vista consolidada de sus casos de soporte. Permite filtrar, ordenar y personalizar la vista de lista de casos, lo que proporciona visibilidad tanto de los casos abiertos como de los cerrados a los que tiene derecho de acceso. Para obtener información más detallada sobre el módulo Support en Cisco IQ SaaS, consulte la [Guía de inicio de Cisco IQ SaaS](#).

 Nota: Los clientes de VA de Cisco IQ pueden acceder a la mayoría de las funciones del módulo de soporte SaaS de Cisco IQ, incluidos los casos de apertura del Technical Assistance Center (TAC) relacionados con el VA de Cisco IQ y sus módulos, así como la creación y gestión de casos de productos.

Creación de un caso de soporte

Puede crear casos específicos de módulo y VA en Cisco IQ SaaS. Para crear un caso:

1. Inicie sesión en [Cisco IQ \(SaaS\)](#).
2. Haga clic en el icono Ayuda > Informar sobre un problema. Se abre la ventana Informar sobre un problema.



Report an Issue

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

Issue type

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

Issue description

Describe what happened.

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

Preferred contact method

☐ Telephone ☐ Email ☐ Virtual space via Webex

Include recipients (optional)

Select or add email addresses

Select or enter email addresses to include.

Cancel Submit

Informar sobre un problema

3. Proporcione los detalles necesarios.
4. Haga clic en Submit (Enviar).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).