

思科IQ虚拟设备操作指南v1.2.0

简介

Cisco IQ™为您提供各种增强功能和特性，旨在提高资产可视性、跨环境提供更智能的见解，并简化案例管理。此外，Cisco IQ AI Assistant等AI功能通过提供情景理解来优化运营成果和Cisco IQ用户体验，使您能够做出主动的、明智的决策，并简化客户参与和成功的流程。

Cisco IQ On-Prem Air-Gapled是Cisco IQ的部署模式之一，专为具有严格的合规性、数据主权和安全要求的监管行业中的客户设计。在此模式下，思科IQ作为独立的虚拟机(VM)提供，称为思科IQ虚拟设备(VA)。VA完全在客户驻地运行，与外部网络完全隔离。为了保持这种隔离，可从Cisco IQ SaaS获取软件更新和维护包，并通过经过批准的手动流程将其传输到VA。

Cisco IQ On-Prem Air-Gapled将Cisco IQ SaaS的关键功能扩展到气隙环境，使任务关键型团队能够以与云连接企业相当的速度和诊断智能进行运营。

要访问Cisco IQ VA，请打开支持的浏览器并导航至<https://<fqdn-of-the-appliance>>。使用安装过程中设置的admin用户名和密码登录。

 **注意：** Cisco IQ VA目前仅限注册参加受控可用性计划的客户。从Cisco IQ门户下载访问VA系统软件和其他操作包（模块、规则和授权）的权限专供选定客户使用。请联系您的客户代表了解更多信息。

连接管理（数据收集）

Cisco IQ VA是一种内部部署的网络数据收集解决方案，可深入了解您的基础设施。它通过Catalyst Center和Direct Connection收集数据。它简化了网络身份验证和设备发现的管理方式。配置数据收集包括：

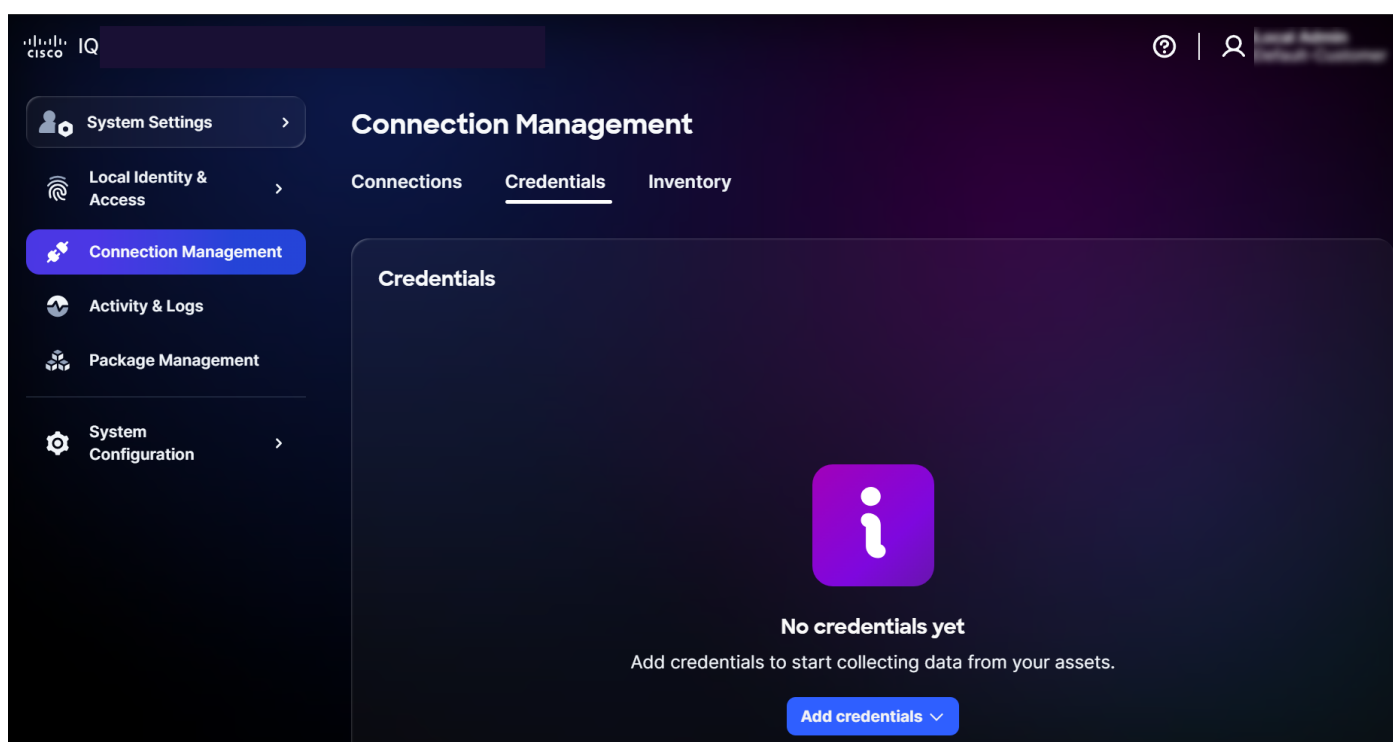
- **创建凭证集:**建立身份验证协议(例如，简单网络管理协议(SNMP)v1/v2c/v3)以与网络设备通信。通过按安全区域或位置集中凭证（例如，“SanJose-SNMPv3”），您可以在一个位置更新密码，使更改自动传播到所有相关设备。
- **将凭证映射到资产:**将凭证集与库存资产进行映射，以自动执行身份验证过程。通过创建将特定IP范围链接到已定义的凭证集的规则，系统在数据收集期间自动应用正确的身份验证。这消除了手动输入错误，并确保您的配置在网络扩展时保持准确。

 注意：设备发现需要SNMPv2c/SNMPv3和SSH，并且在配置Catalyst Center之前必须提供HTTP/HTTPS凭证。

添加凭证

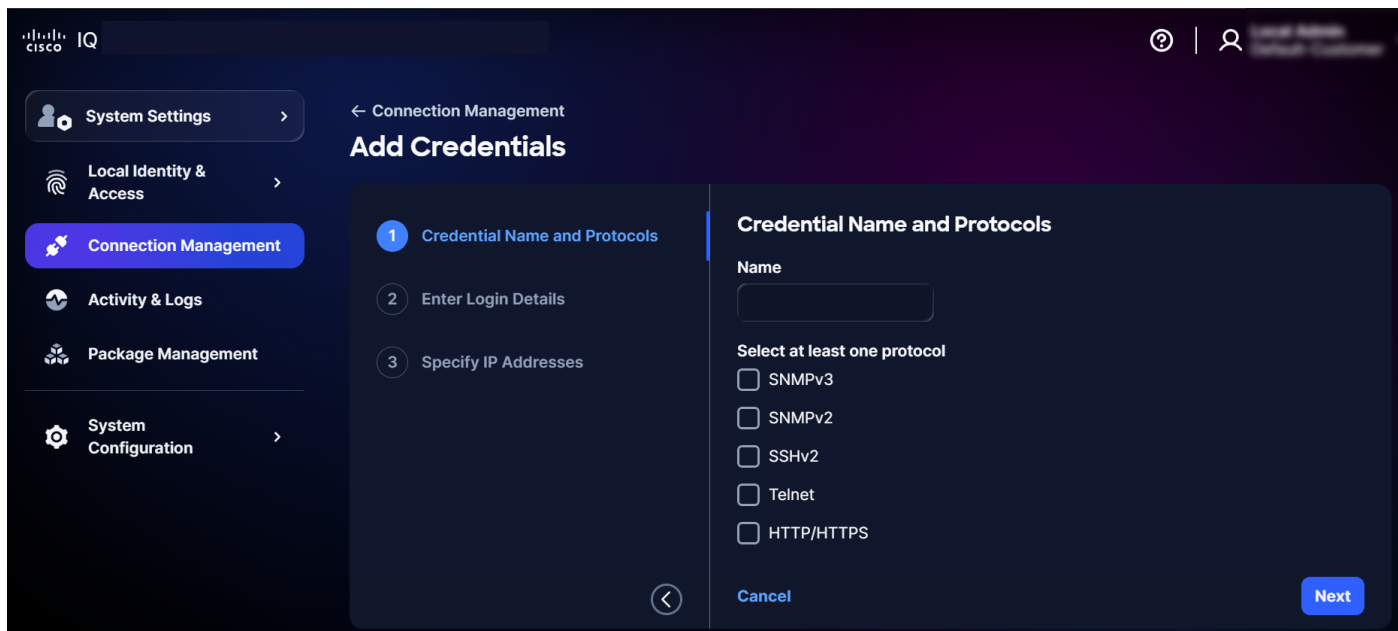
必须先添加凭据才能执行数据收集。要添加凭证，请执行以下操作：

1. 从系统设置中选择连接管理。系统随即会显示Connection Management页面。
2. 单击Credentials选项卡。



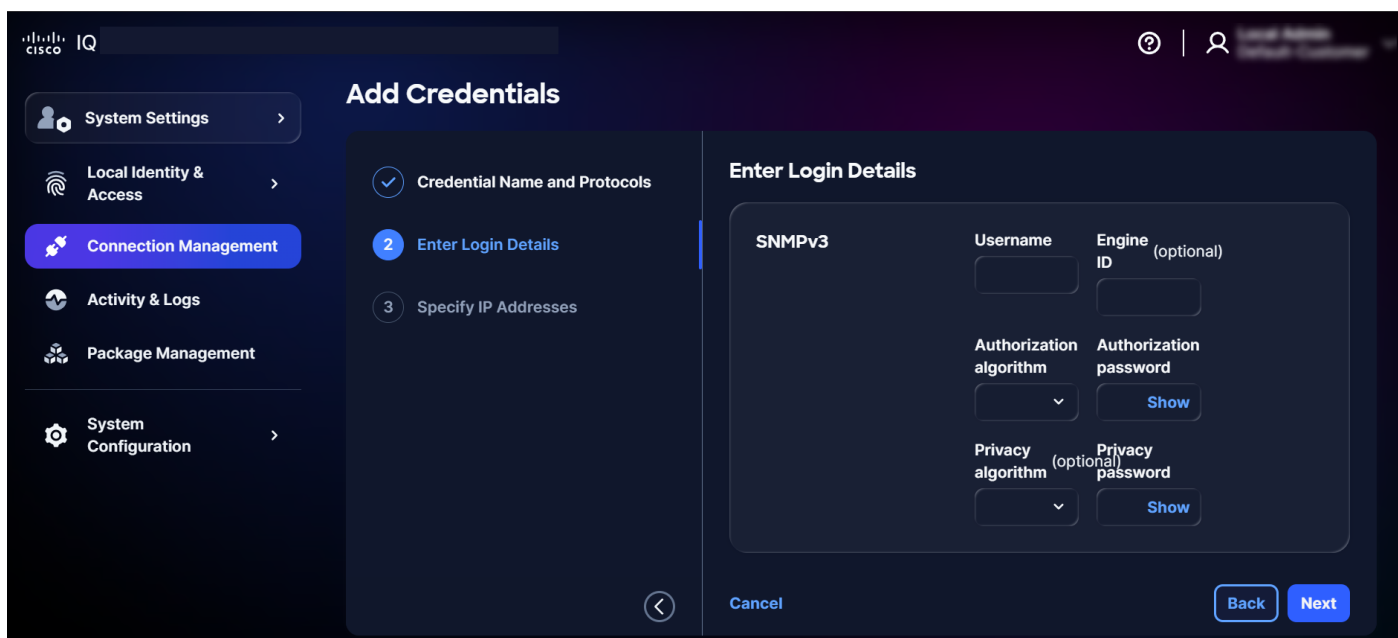
Credentials选项卡

3. 点击添加凭证。



添加凭证

4. 输入Name。
5. 选中所有适用的协议复选框。
6. 单击 Next。

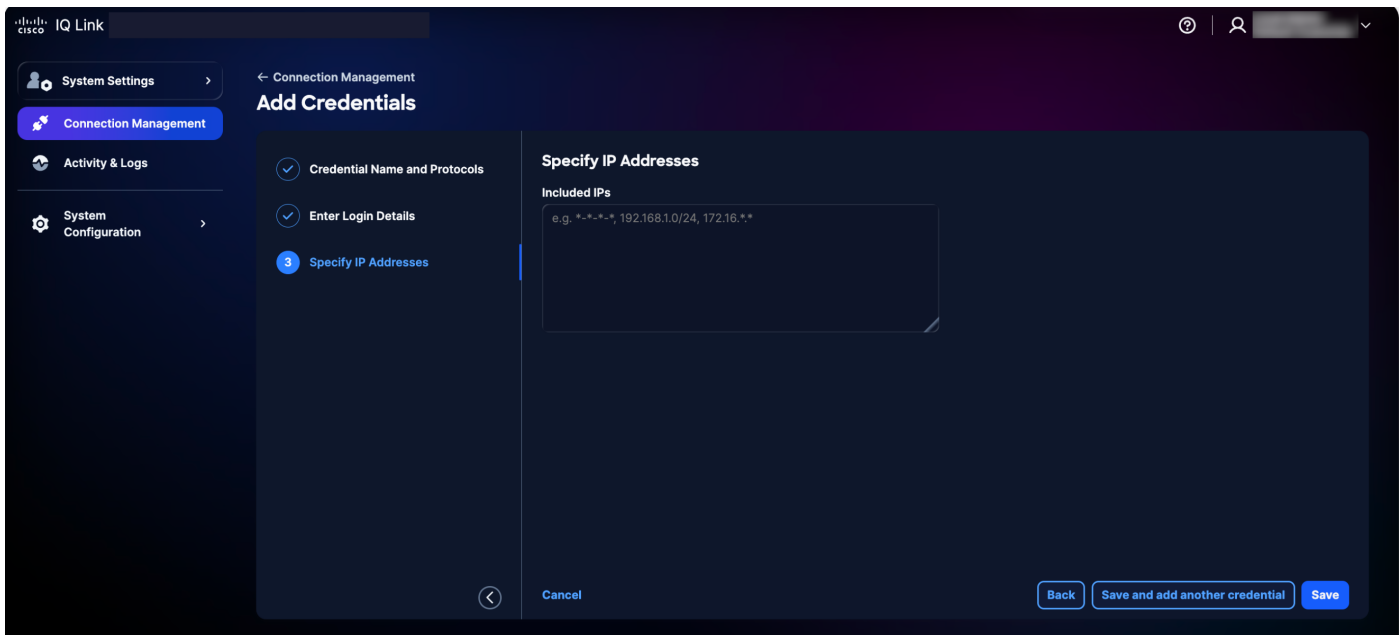


添加凭证详细信息



注意：上图显示了上一步中选择所有协议的视图。您的接口仅显示您选择的协议。

- 7. 输入每个所选协议的登录详细信息。
- 8. 单击 Next。

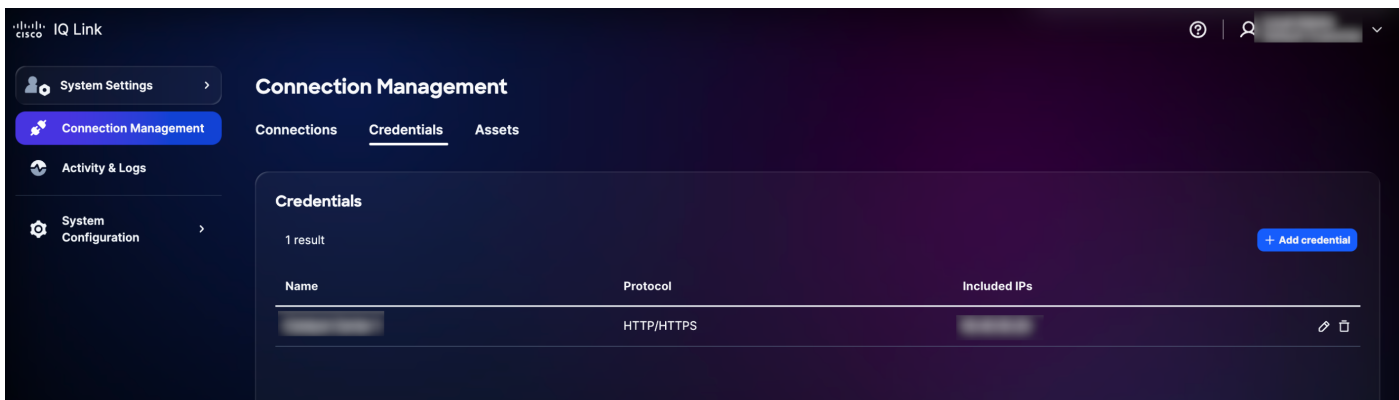


指定IP地址

- 9. 输入Included IPs。

 注意：此字段定义可用于建立连接的凭证的IP地址或IP范围。它支持IP和IP掩码的组合（使用通配符记法）。有关支持的格式的详细信息，请参阅[凭证选择和匹配逻辑](#)。

- 10. Click Save.系统将显示一个确认消息，您将被重定向到凭证选项卡。



已添加凭据

您可以通过单击Edit图标编辑凭证，并通过单击Delete图标删除凭证。

凭据选择和匹配逻辑

遥测引擎使用基于优先级的匹配逻辑来确定在发现和收集期间应用哪些凭证。了解此层次结构可确保为目标设备使用正确的凭证。

- 优先级排名：当多个凭证集应用于一台设备时，思科IQ会根据它们与设备的具体匹配程度来评估它们；系统应用以下优先级，且更具体的匹配优先：
 - 精确的IP匹配:最高优先级
 - 尾随通配符匹配:优先级取决于尾随星号的数量；星号越少，表示匹配项越具体，优先级越高
- 通配符格式规则:通配符(*)仅作为IP地址中的尾部字符受支持；必须从右到左应用它们。
 - 支持的格式：
 - 1.2.3.* (最高优先级)
 - 1.2.*.*
 - 1.*
 - *.*.* (最低优先级)
 - 不支持的格式：
 - 前导通配符 (例如*.1.2.3)
 - 八位组之间的通配符 (例如，10.10.*.20)
 - 使用破折号或其他非标准分隔符

凭证选择示例:

下表说明当设备匹配多个定义的模式时，遥测引擎如何选择最合适的凭证集。

表 1：凭证选择示例

设备IP	可用的凭据集	选定的凭证集
10.10.1.5	10.10.1.5、10.10.1、10.10..*	10.10.1.5 (完全匹配)
10.10.2.15	10.10.2、10.10.*	10.10.2.* (更详细)
10.10.5.50	10.10...	10.10.. (更详细)

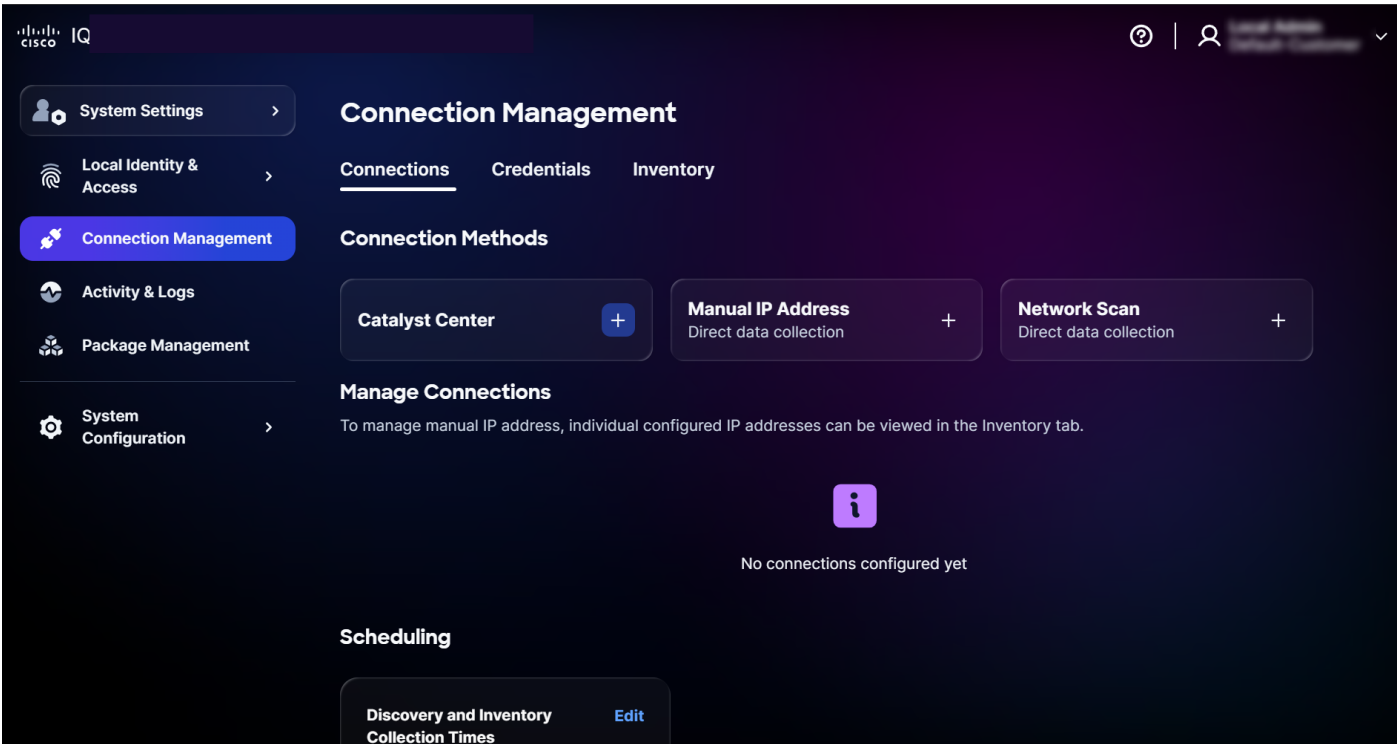
 注意：如果设备属于多个重叠类别，系统始终会选择具有最高特异性的凭证集（换言之，最少的尾部通配符）。

使用Catalyst Center进行数据收集

每个Cisco IQ VA实例最多可连接20个Catalyst Center（非集群）。

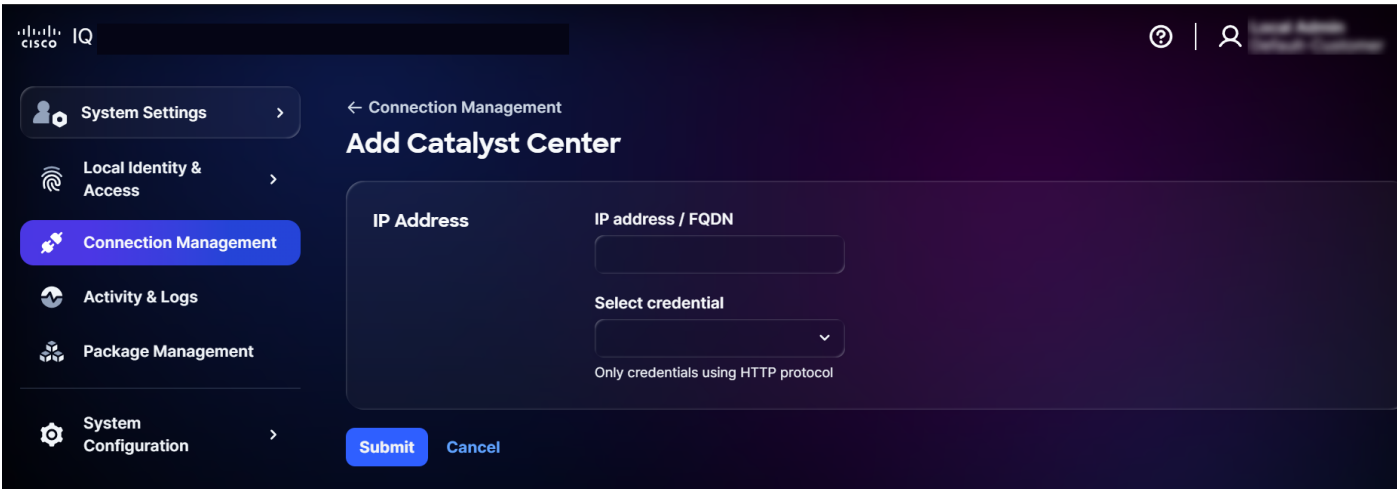
对于使用Catalyst Center的数据收集：

- 1. 从系统设置中选择连接管理。系统随即会显示Connection Management页面。



连接管理

- 2. 单击Catalyst Center选项。



添加Catalyst Center

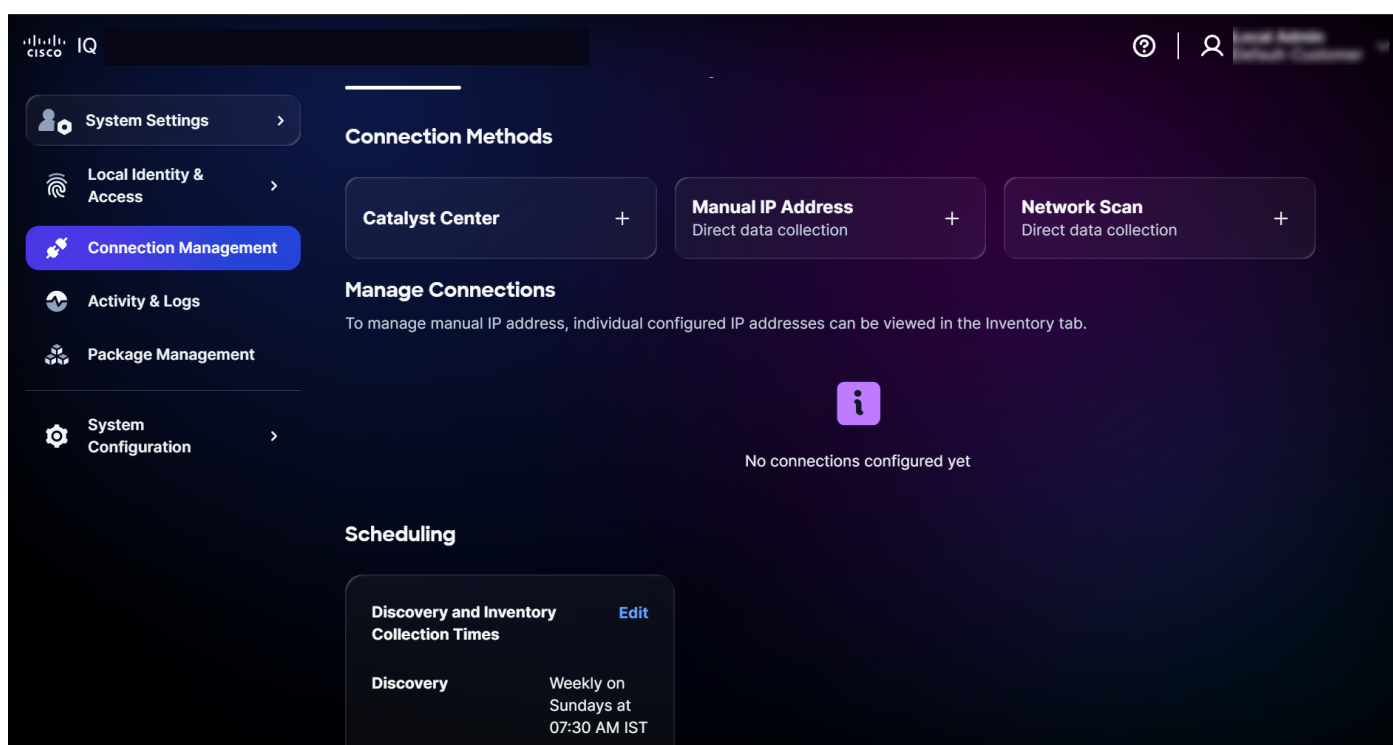
3. 输入IP地址或FQDN。
4. 从Select credential下拉列表中选择已配置的HTTP/HTTPS凭证。
5. 单击 submit。系统随即会显示确认（最多可能需要75分钟）。您可以在Configured Connections下查看新添加的Catalyst Center。
6. 计划收集。有关详细信息，请参阅[计划](#)。

 **注意：** Cisco IQ VA预配置了自动计划设置，系统启动默认自动收集计划。强烈建议您编辑计划以符合组织的要求和维护窗口。

手动数据收集

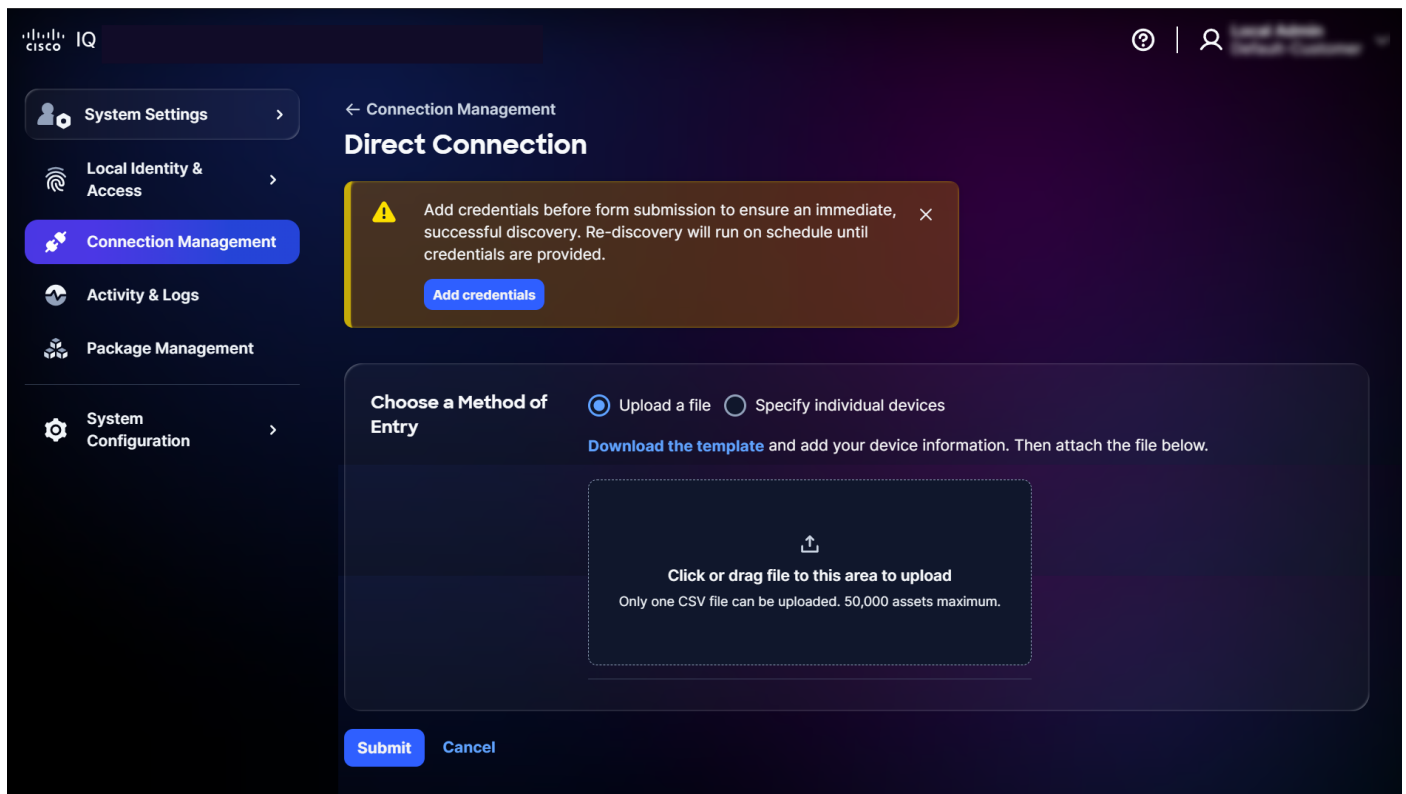
要添加直接数据连接的设备，请执行以下操作：

1. 从系统设置中选择连接管理。系统随即会显示Connection Management页面。



连接管理

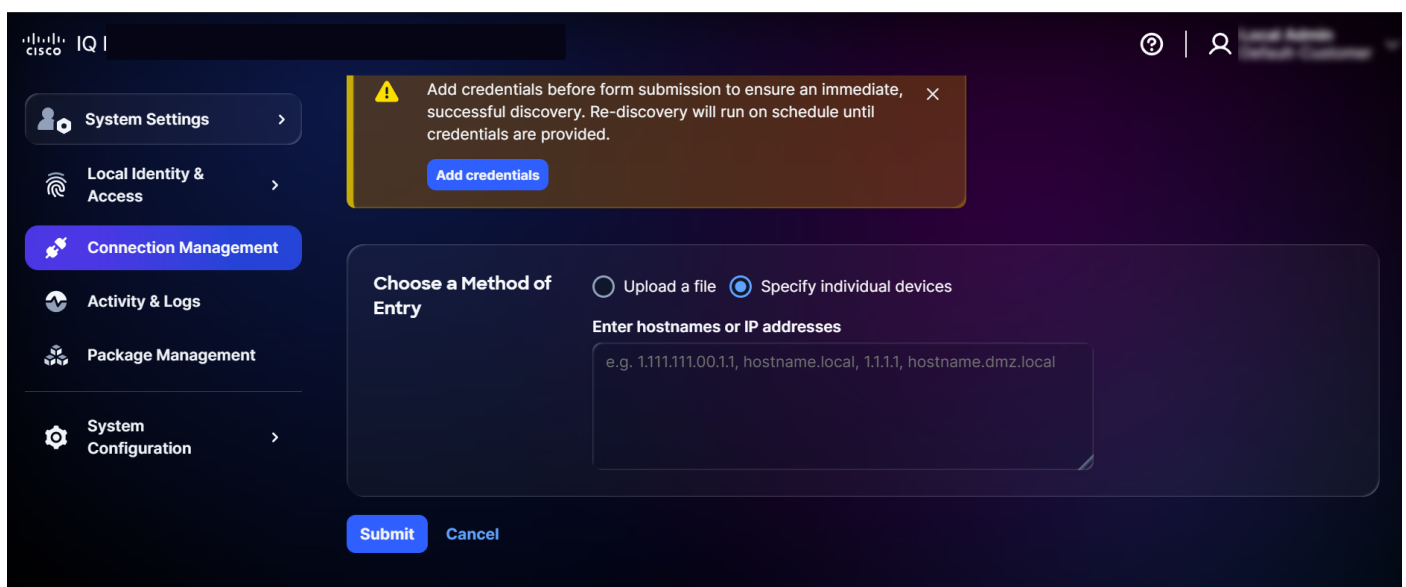
2. 单击手动IP地址。系统随即会显示Direct Connection页面，其中包含两(2)个用于收集数据的选项。



上载文件

3. 单击Choose a Method of Entry中的首选选项，并使用以下方法之一提供设备信息：

- 上载文件:单击或拖放文件



指定单个设备

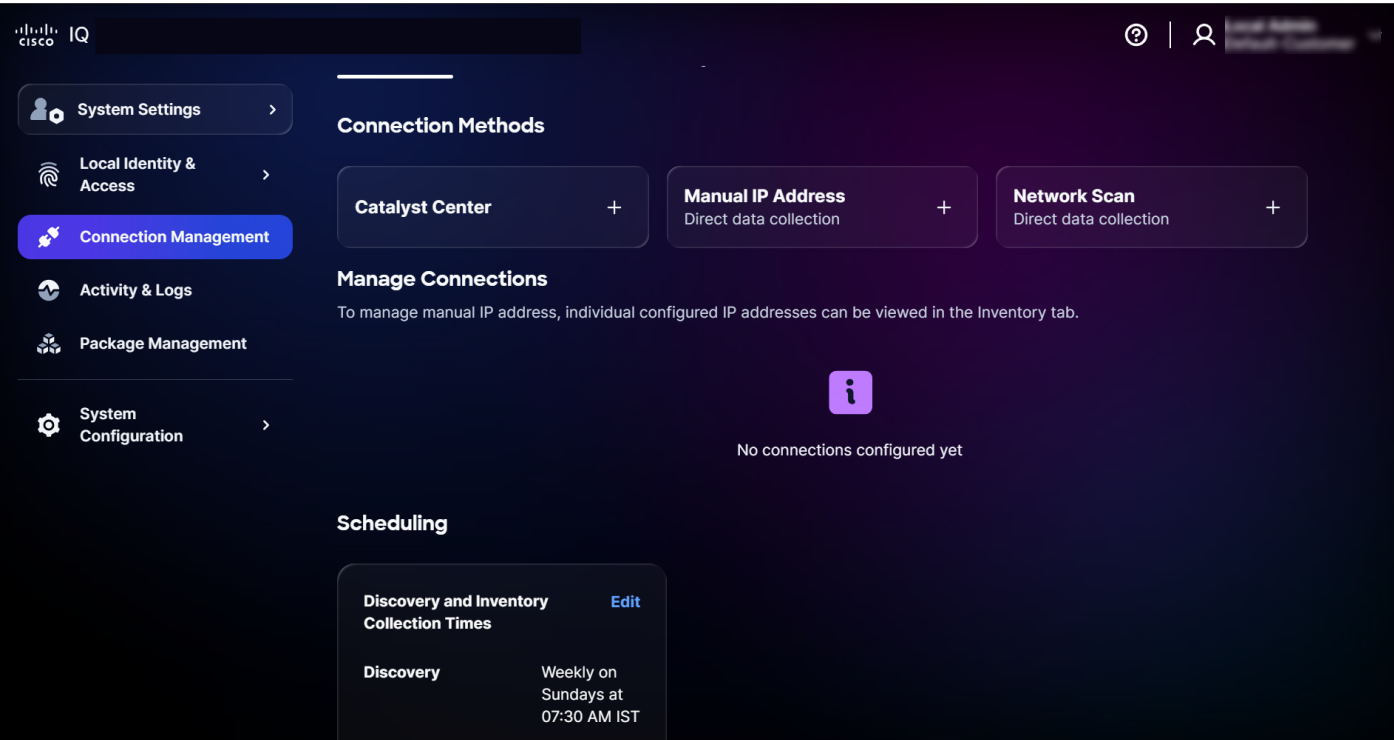
- 指定单个设备:输入单个主机名、IP地址或逗号分隔的主机名和/或IP地址列表

- 单击 submit。成功提交后，系统会将您重定向到Assets选项卡。
- 计划收集。有关详细信息，请参阅[计划](#)。

 注意：Cisco IQ VA预配置了自动计划设置，系统启动默认自动收集计划。强烈建议您编辑计划，使其符合组织的要求和维护窗口。

网络扫描

- 从系统设置中选择连接管理。系统随即会显示Connection Management页面。



网络扫描

- 单击Network Scan。Connect Assets by Network Scan页面显示三(3)个选项。

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

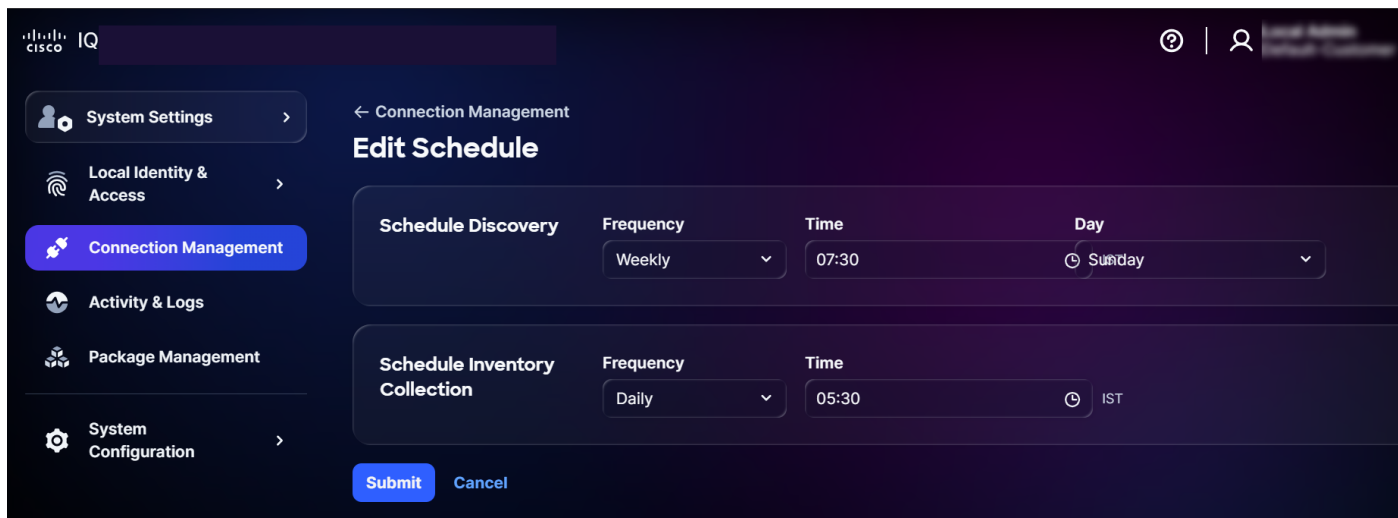
- 指定IP范围:为网络发现或管理任务定义该范围内的目标设备的IP地址范围
- 指定发现协议(CDP/LLDP):选择要使用的网络发现协议
- 文件上传:上传文件，例如配置文件或数据

3. 输入姓名.
4. 输入IP Start和IP End。
5. 在计划扫描下，选择频率和时间。
6. 单击Connect assets。

安排

调度允许您定义Cisco IQ VA何时执行自动数据收集。要计划收集，请执行以下操作：

1. 在Connection Management页面的Scheduling部分中，针对要修改的计划，单击Edit。系统将显示Edit Schedule页面。



编辑计划

2. 在Schedule Discovery部分中，从下拉列表中选择首选的Frequency和Day，并输入所需的开始时间Time。
3. 在Schedule Inventory Collection部分，从下拉列表选择您的首选Frequency，并输入所需的开始时间。
4. 单击 submit。

 注意：对于对发现或收集计划所做的任何更改，留出5-10分钟时间在虚拟设备中进行同步和准确反映。

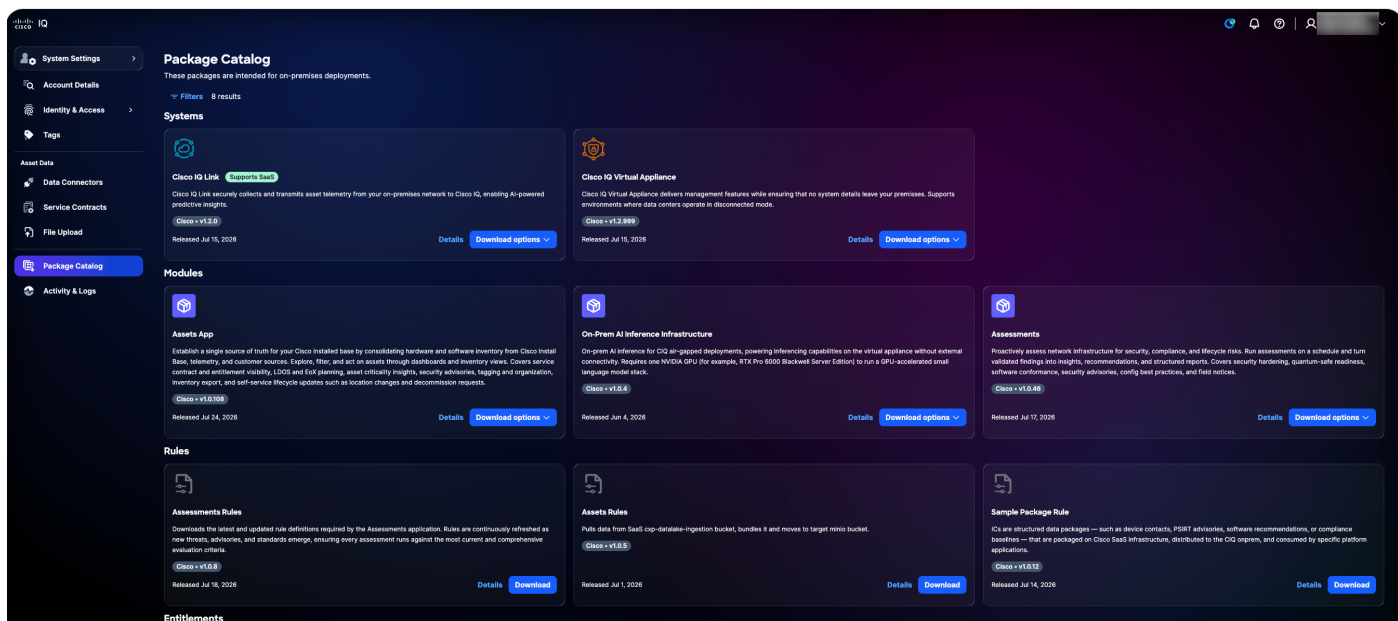
安装包（模块、规则和授权）

您可以管理VA内运行模块、规则、授权和专门的AI支持的功能的软件生命周期（即安装和配置）。您可以通过导航至软件包目录，从Cisco IQ(SaaS)下载最新版本来安装它们。包目录显示可供您使用的软件实例。它使您能够无缝地监控和管理更新，确保高效地跟踪和管理您的系统实例。

添加模块

模块是独立软件包，在VA内提供核心功能。它是一种独立的服务，具有自己的生命周期，允许进行安装、维护和调整大小。资源消耗(包括CPU、图形处理单元(GPU)和RAM)是根据初始安装期间选择的部署大小（小、中或大）动态分配的。

1. 登录到[Cisco IQ](#)。
2. 导航到系统设置 > 程序包目录。

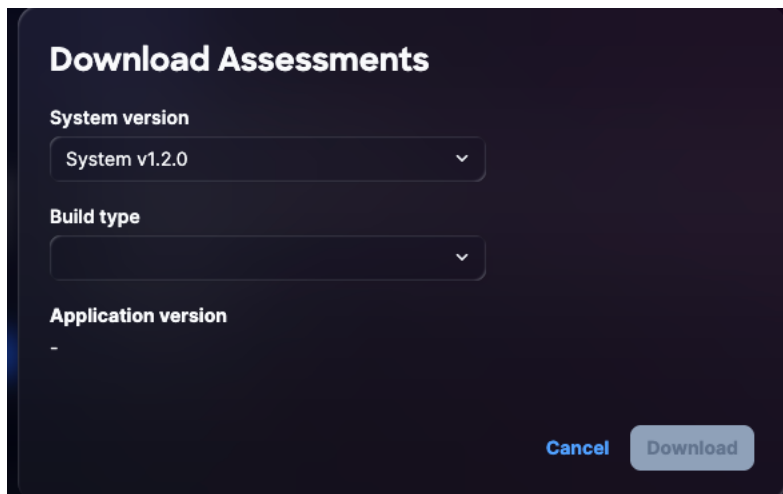


包目录

3. 从所需的模块卡中，单击Download options > Installation packages。Download窗口打开。



注意：“评估”模块用于示例图像。



下载

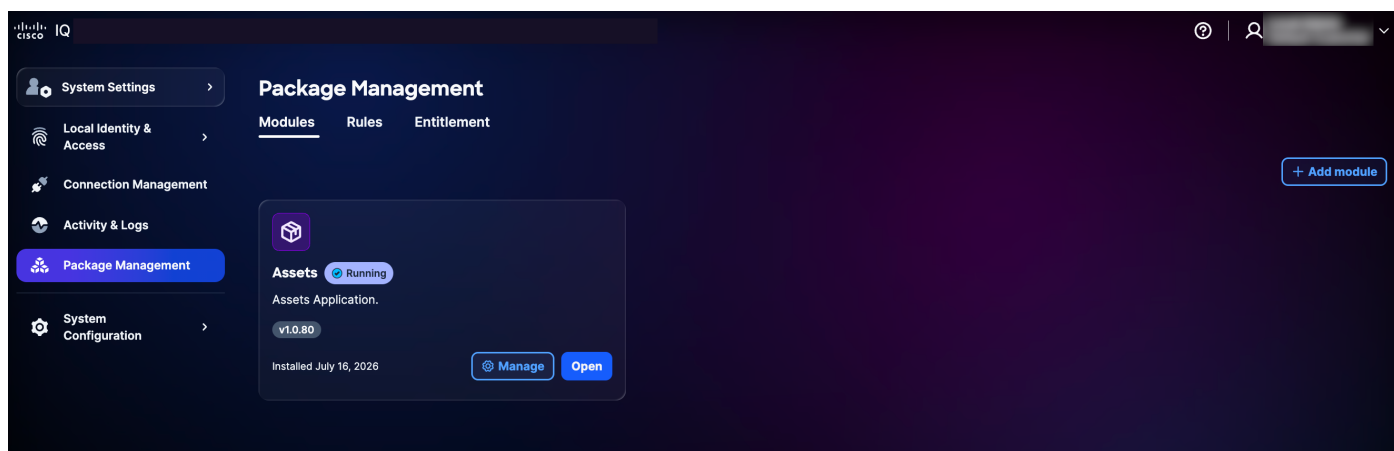
4. 从下拉列表中选择System Version。
5. 从下拉列表中选择Build type。
6. 单击Download将文件保存到本地。

 注意：安装文件很大(10-25 GB);在下载之前，请确保您有足够的磁盘空间。

7. 导航至VA。

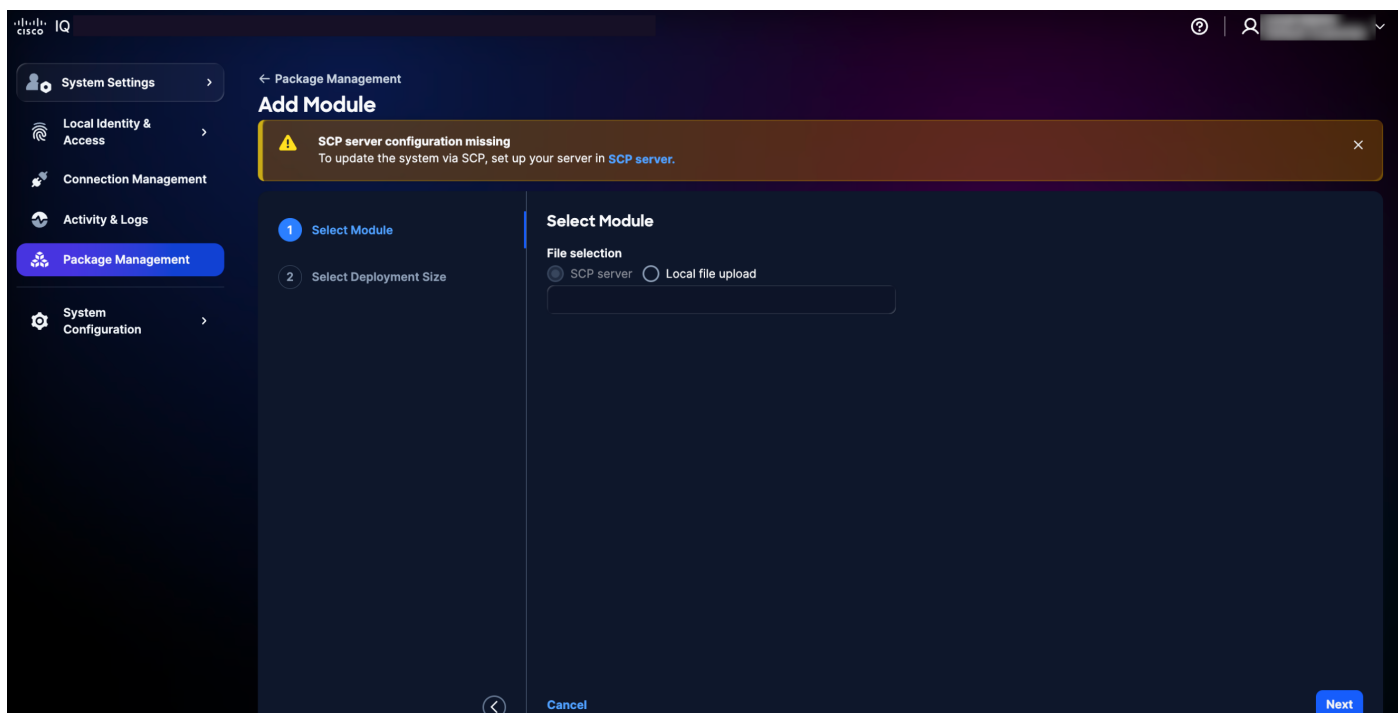
8. 导航到主页 > 系统设置 > 软件包管理。系统随即会显示Package Management页面，其中包含以下选项卡：

- 模块
- 规则
- 授权



模块

9. 单击Add module。

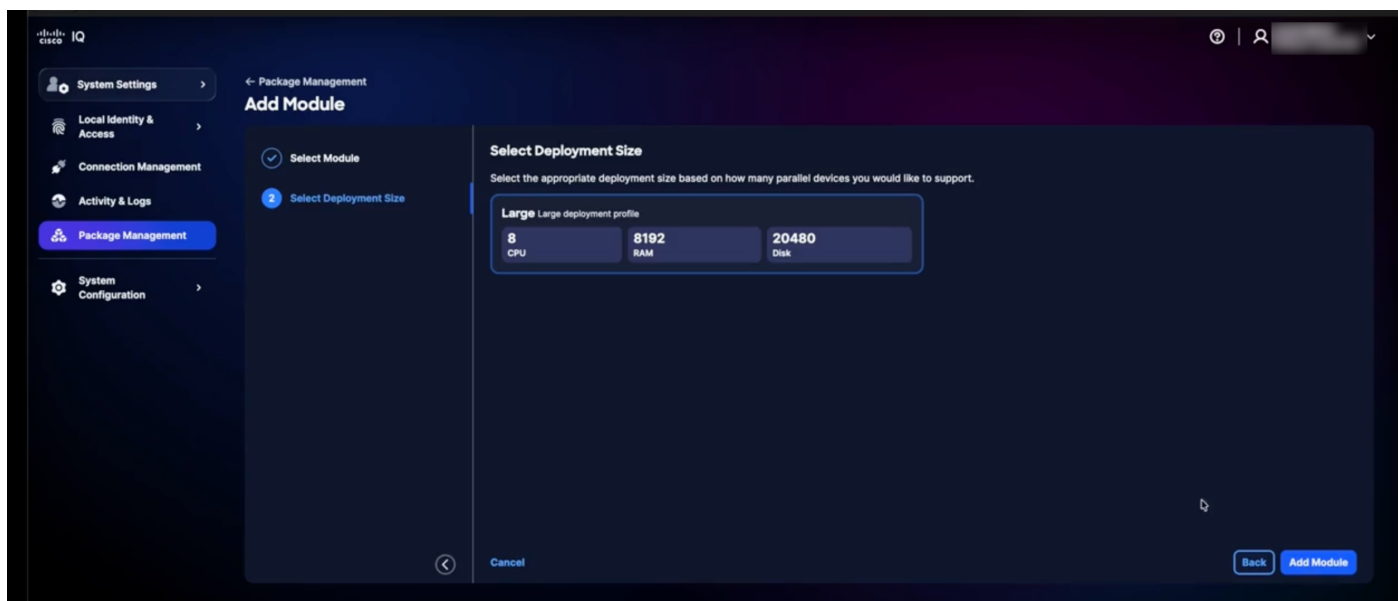


添加模块

10. 选择您的首选文件选择选项：

- SCP服务器:输入安装软件包的确切文件名（建议用于大文件）
- 本地文件上传:拖放下载的安装文件（由于上载时间的原因，不建议对30 GB或更大的文件使用）

11. 单击 Next。

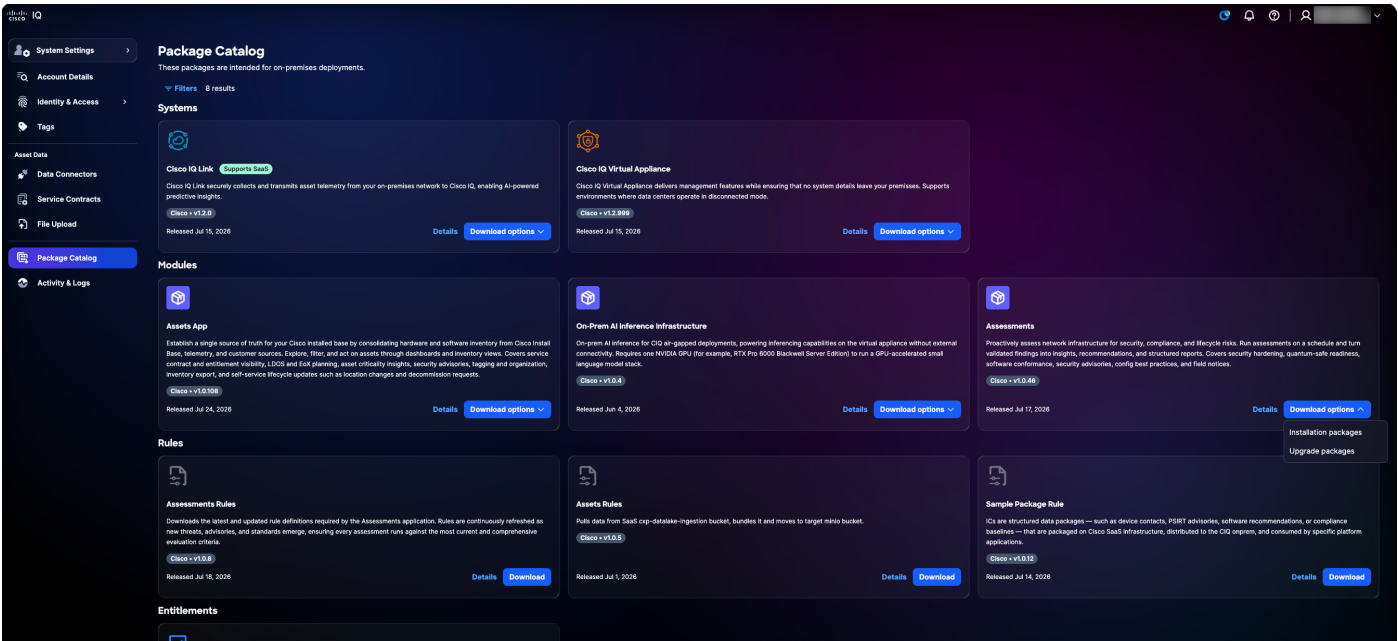


部署规模

- 12. 选择Deployment Size (例如 , Small、Medium或Large) 。 这些大小是预先定义的 , 规定了资源需求。
- 13. 单击Add Module。新安装的模块显示在包管理的模块选项卡上。完成后 , 模块状态更改为“正在运行” , 打开按钮变为可用。

升级模块

最新的模块在软件包目录 (在Cisco IQ中) 中不断更新。 要升级到最新版本 , 请执行以下操作 :



通过网络扫描连接资产

- 1. 从所需的模块卡中 , 单击Download options > Upgrade packages。Download窗口打开。

 注意 : “评估”模块用作图像的示例。

Upgrade Assessments

System version

System v1.2.0



Current app version



Build type



Application version

-

Cancel

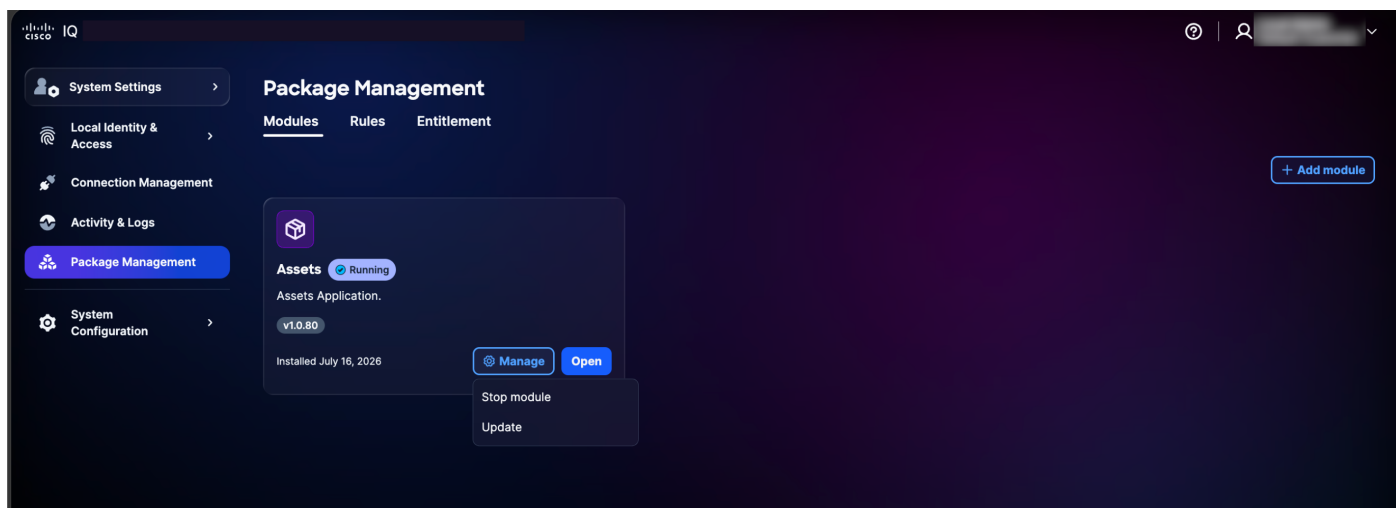
Download

下载

2. 从下拉列表中选择System version。
3. 从下拉列表中选择Current app version。
4. 从下拉列表中选择Build type。
5. 单击Download将文件保存到本地。
6. 导航至VA并完成下载文件的安装。

管理模块

添加模块后，您可以点击Manage，从Package Management页面对其进行修改。可用的修改选项包括调整大小和升级到更高版本。管理模块的步骤：



更新类型

1. 在Package Management页面中，单击所需模块的Manage > Update。
2. 选择Update type:
 - 仅更改部署大小
 - 更新版本
3. 如果选择更改部署大小，请单击下一步，然后在下一页中选择新的部署大小。

或者

如果选择Update Version，则会显示File selection选项。选择SCP Server并输入安装软件包的确切文件名，或选择Local file upload，然后拖放下载的安装文件。

4. 单击 Next。系统随即会显示选择更新计划页。
5. 从以下单选按钮选项中选择更新计划：
 - 现在更新
 - 稍后更新



注意：有些模块支持更新，不会造成任何停机。如果需要停机，则标语会显示详细信息。

6. 如果选中Update later，请输入Date和Time。
7. 单击 Next。系统随即会显示更新摘要。

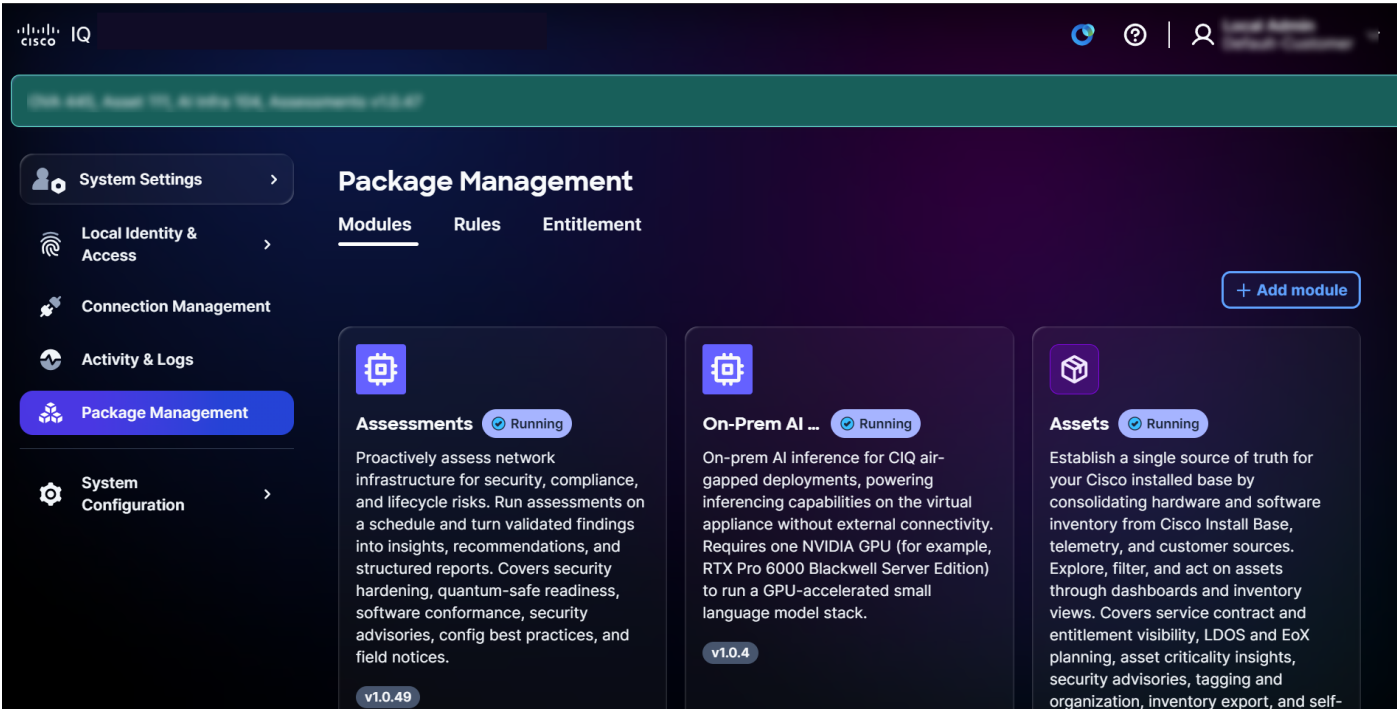


注意：您可以从更新摘要访问发行说明。

8. 单击Update Module并导航到Module选项卡。模块显示“更新已计划”状态。

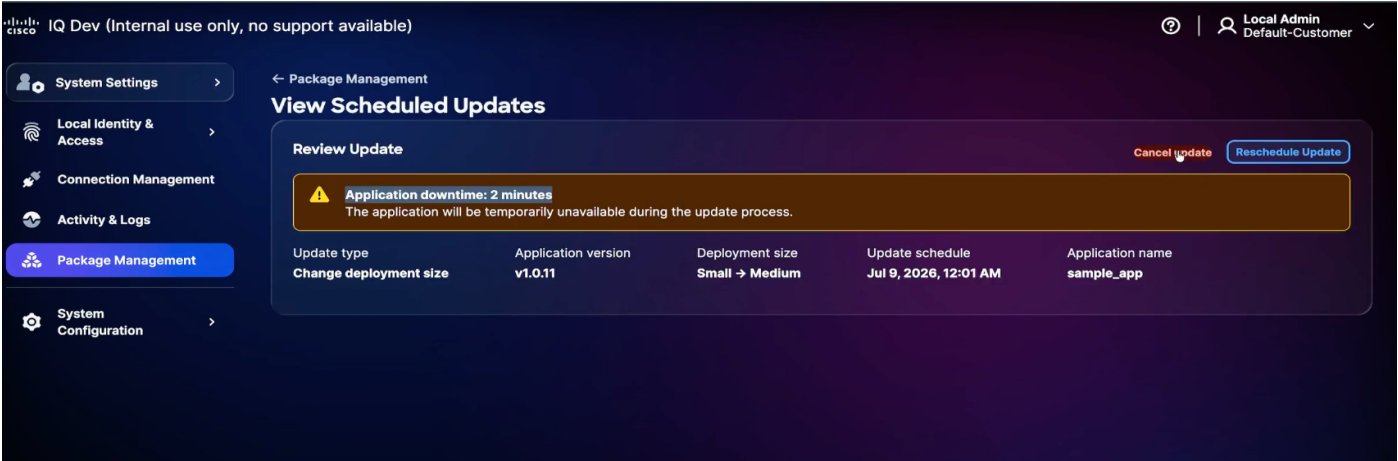
编辑计划

您还可以查看、编辑或取消计划的更新。要编辑或取消计划更新，请执行以下操作：



编辑计划

- 1. 在Package Management页面中，单击所需模块的Manage > View Scheduled update。系统将显示View Scheduled Updates窗口。



安排更新

2. 根据需要单击Cancel Update或Reschedule Update。
3. 按照屏幕上的说明完成操作。

 注意：如果模块操作（例如，安装、升级或调整大小）失败，请选择以下选项之一：

重试: UI将显示“重试”按钮，允许您再次尝试该操作。 日志: 如果错误仍然存在，请点击Logs查看详细的诊断信息。这是确定安装或运行时故障原因的主要方法。

安装规则

规则是扩展或修改现有模块功能的专用组件或“附加组件”。规则不是作为独立程序运行的；它们“插入”模块以提供特定的规则、逻辑或功能。规则与特定模块关联。安装规则后，规则会链接到其支持的模块。规则允许更新或自定义系统，而无需对核心模块进行完全升级。如果需要一组新的规则或功能，只需将新规则添加到现有模块即可。

要下载规则，请执行以下操作：

1. 登录到[Cisco IQ](#)。
2. 导航到System Settings（系统设置）> Package Catalog（软件包目录）。
3. 从所需的规则卡中，单击Download。

 注意：以下示例图像用于Assets规则。

Download Assets Rules

Target app version

assets v1.0.0



Cancel

Download

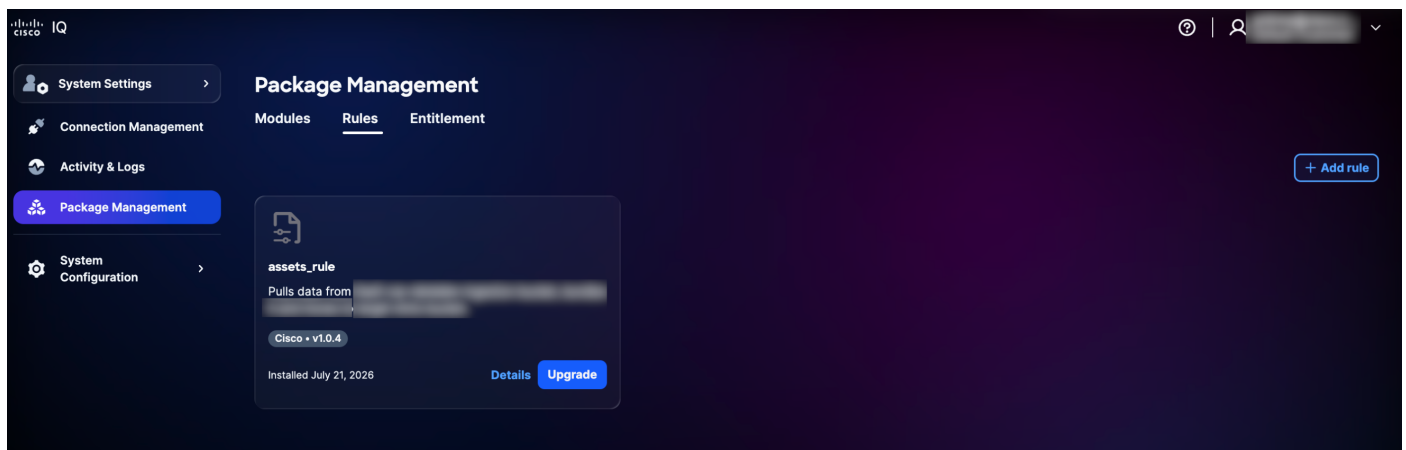
下载

4. 从下拉列表中选择目标应用版本。
5. 单击Download将文件保存到本地。



注意：安装文件很大(10-25 GB);在下载之前，请确保您有足够的磁盘空间。

6. 导航至VA。
7. 导航到主页 > 系统设置 > 软件包管理。系统随即会显示Package Management页面，其中包含以下选项卡。
 - 模块
 - 规则
 - 授权
8. 单击Rules选项卡。



包管理

9. 单击Add rule。

Add rule



SCP server configuration missing



To update the system via SCP, set up your server in [SCP server](#).

File selection



SCP server



Local file upload

Cancel

Add

添加规则

10. 选择您的首选文件选择选项：

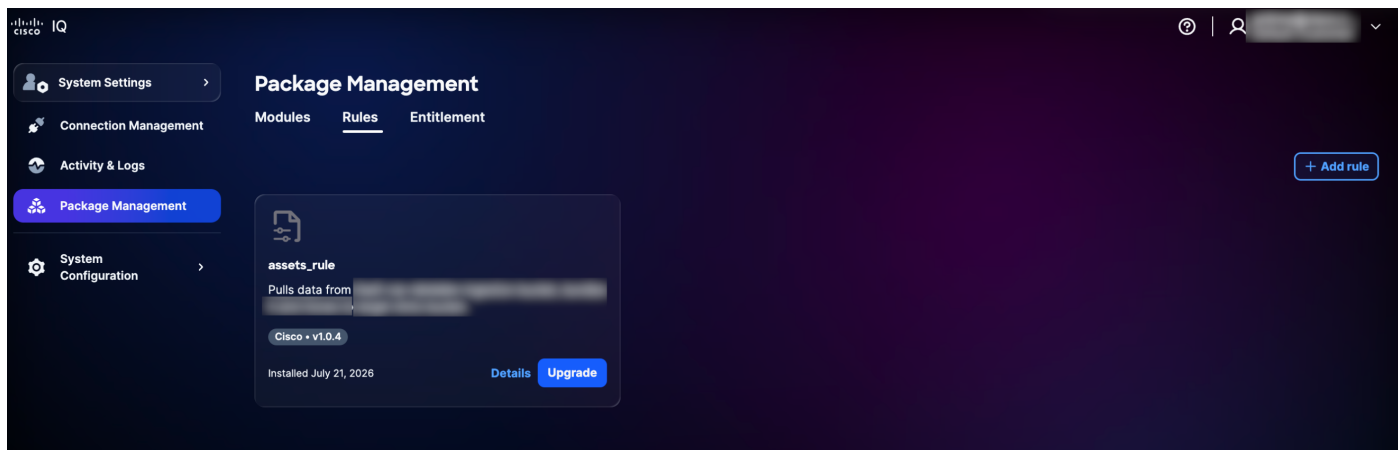
- 安全复制协议(SCP)服务器:输入安装软件包的确切文件名。对于大型文件，建议使用此方法。
- 本地文件上传:拖放下载的安装文件。

11. 单击 Add。添加的规则显示在包管理中。

升级规则

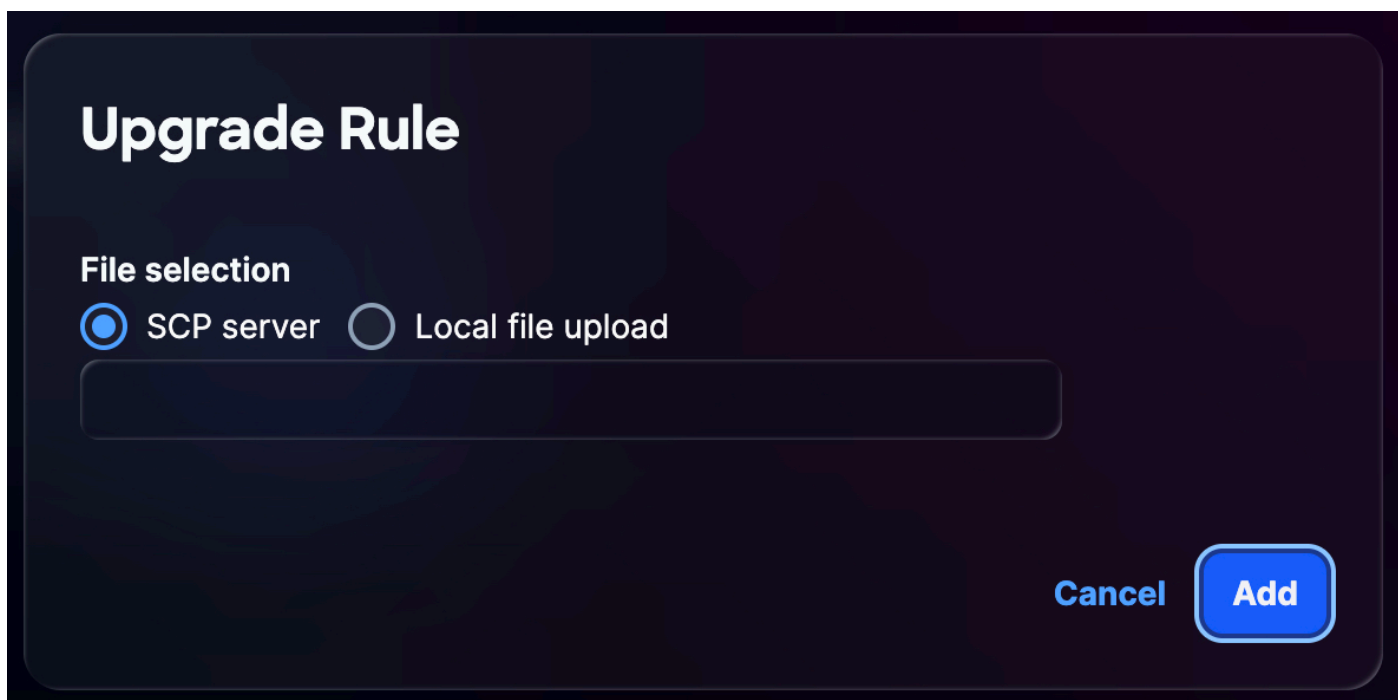
要升级规则，请执行以下操作：

1. 在VA中导航到System Settings > Package Management。



升级

2. 在所需规则中，单击Upgrade。Upgrade Rule窗口打开。



升级规则

3. 选择您的首选文件选择选项：

- 安全复制协议(SCP)服务器:输入安装软件包的确切文件名。对于大型文件，建议使用此方法。
- 本地文件上传:拖放下载的安装文件。

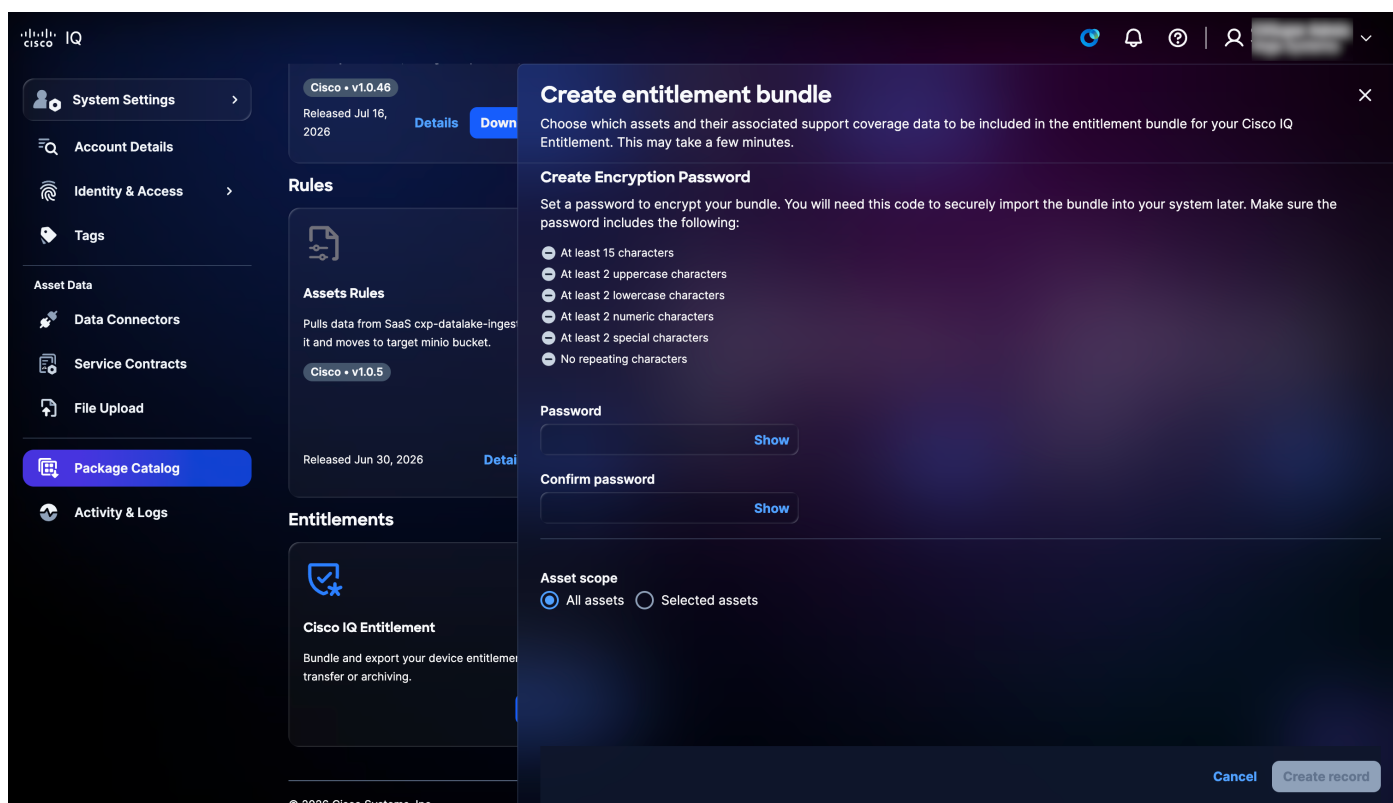
4. 单击 Add。

 注意：这些规则应用于周期性计划设备遥测收集。对于即时应用，您可以手动启动设备遥测收集。

安装授权

授权可验证贵组织对特定软件功能、模块或服务的使用权。要安装授权，请执行以下操作：

1. 登录到[Cisco IQ](#)。
2. 导航到系统设置 > 程序包目录。
3. 从授权卡中，单击创建记录。Create entitlement bundle窗口打开。



创建授权捆绑包

4. 输入密码.请参阅屏幕上显示的密码创建规则。
5. 在Confirm Password中再次输入相同的密码。
6. 选择首选的资产范围单选按钮。
 - 所有资产:包括链接到您的所有资产
 - 选定资产：允许您选择与您的环境一致的特定设备；如果选中此选项，则选中所有适用

资产的复选框

7. 单击Create record以本地保存文件。

 注意：创建授权捆绑包后，请勿离开当前屏幕。如果导航到其他页面，则捆绑包将失效，您必须重新生成该捆绑包才能启用下载选项。

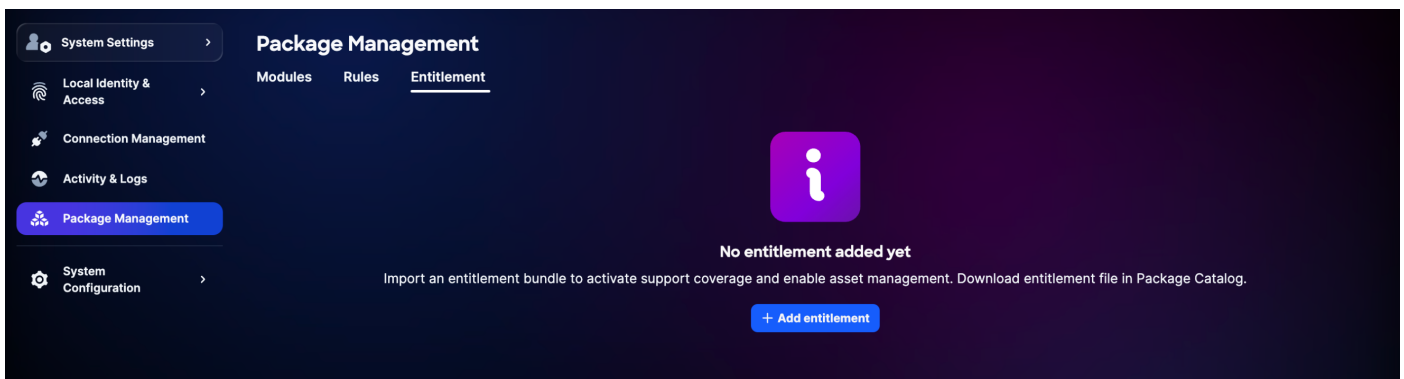
 注意：安装文件很大(10-25 GB);在下载之前，请确保您有足够的磁盘空间。

8. 登录到VA。

9. 导航到主页 > 系统设置 > 软件包管理。Package Management页面包含以下选项卡：

- 模块
- 规则
- 授权

10. 单击Entitlements选项卡。



Entitlement选项卡

11. 单击Add Entitlement。

Add Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

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

添加授权

12. 选择首选的文件选择选项。

- 安全复制协议(SCP)服务器:输入安装软件包的确切文件名；对于大型文件，建议使用此方法
- 本地文件上传:拖放下载的安装文件

13. 输入密码。

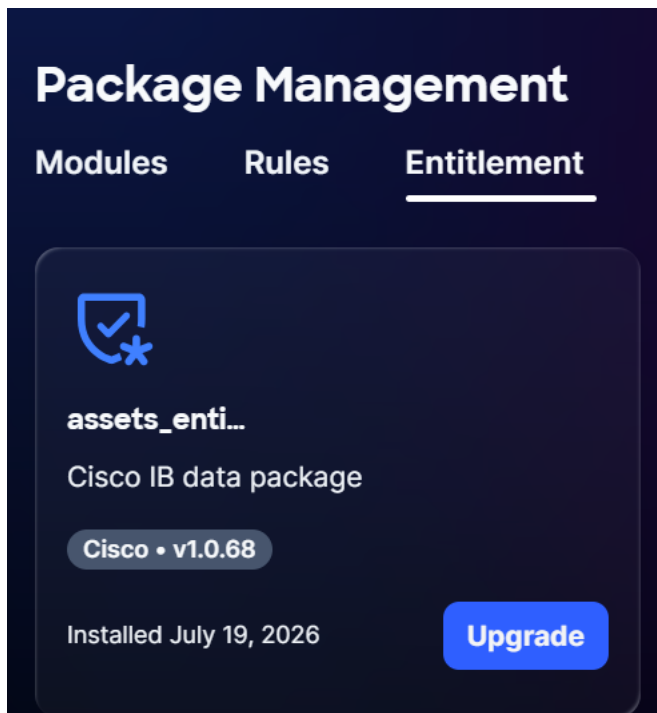
14. 单击 Add。新安装的授权显示在程序包管理的授权选项卡上。

15. 要启用授权，请在添加授权后等待5到10分钟，然后启动设备遥测收集。

 注意：在授权过程中添加服务合同会将链接到该合同的所有设备添加到本地设备资产清单。您可以选择按序列号过滤设备、使用多个帐户ID或选择特定设备来管理授权。

升级授权

要升级授权，请执行以下操作：



授权升级

1. 从所需的授权中，单击Upgrade。

Upgrade Entitlement

File selection

☒ SCP server

☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

Enter password

Show

Cancel

Add

升级授权

2. 选择您的首选文件选择选项：

• 安全复制协议(SCP)服务器:输入安装软件包的确切文件名；对于大型文件，建议使用此方法

• 本地文件上传:拖放下载的安装文件

3. 输入密码.

4. 单击 Add。

AI支持的功能

内置AI推理基础设施模块在VA中启用内置AI支持的功能。它在本地运行小型语言模型(SLM)，使系统能够响应AI驱动的提示。安装后，您可以直接在VA界面中与其交互。

支持以下查询类型：

- 资产:确定由于寿命终止状态、软件货币或不合规、安全漏洞和合同覆盖范围差距造成的风险资产
- 资产:请求对您的资产进行AI驱动的分析

本地AI推理基础设施安装包可从Cisco IQ包目录获得，其分发方式与其他模块（如资产）相同。

 注意：每个GPU一次只能运行一(1)个内部AI推理基础设施。完成安装大约需要40-45分钟。安装文件很大（约30 GB）；在下载之前，请确保您有足够的磁盘空间。

本地AI推理基础设施的必备条件

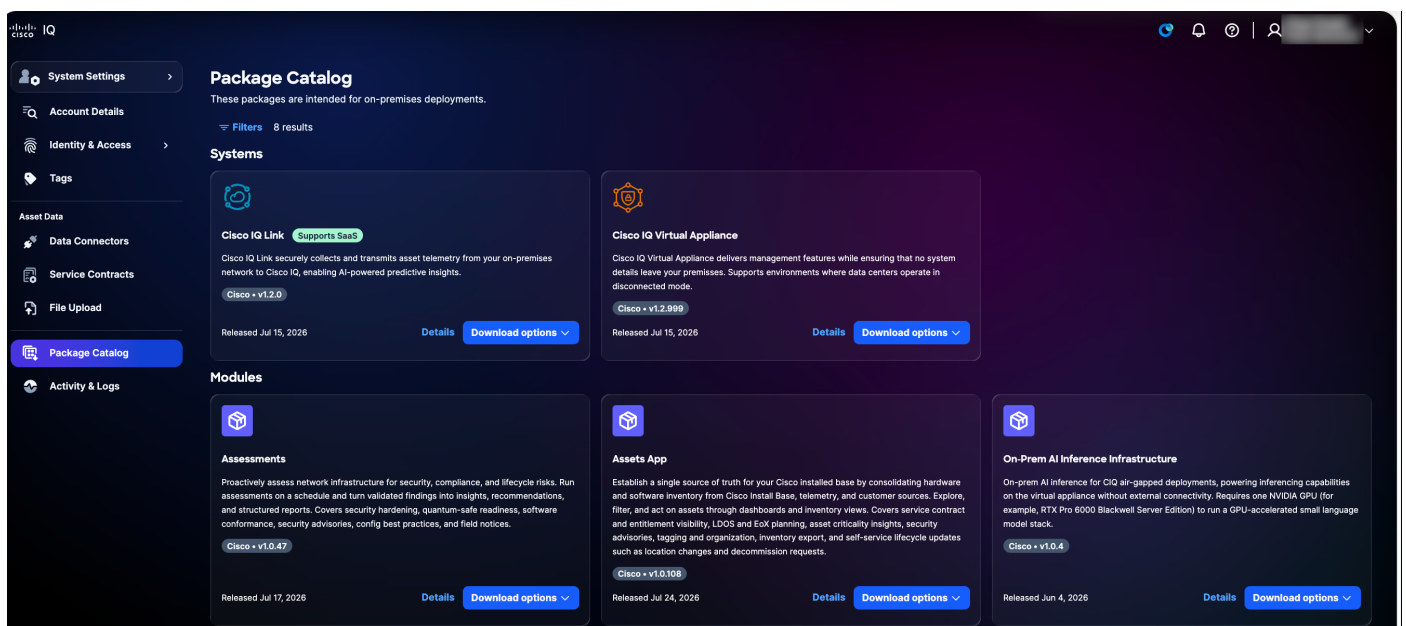
在安装本地AI推理基础设施之前，必须满足以下条件：

- VA必须包括具有GPU访问权限的VM;sIm需要一个GPU，如果没有一个GPU，则无法运行
- GPU VM必须有80GB或更多GPU VRAM可用

安装本地AI推理基础设施

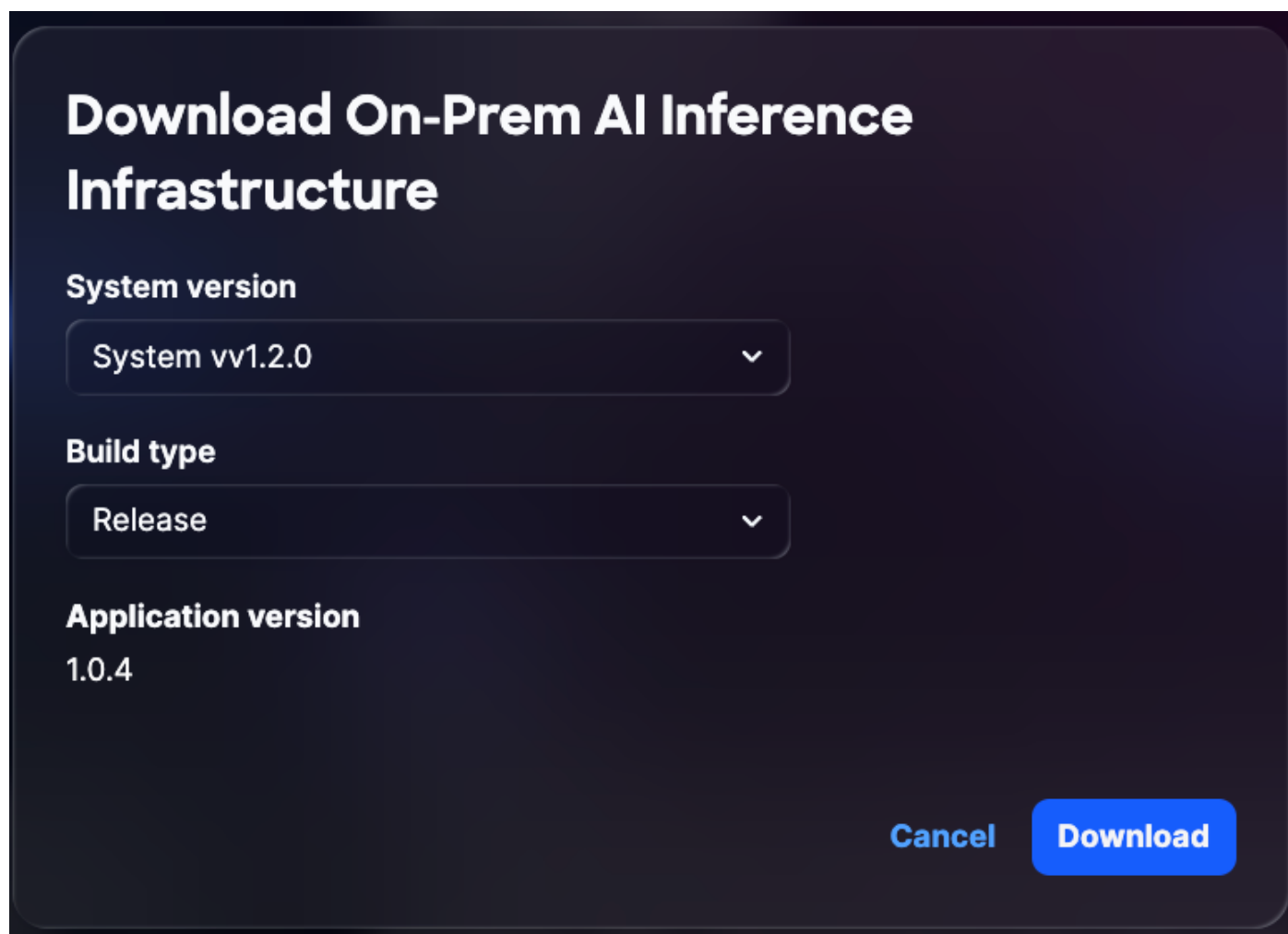
要在VA上安装内部AI推理基础设施，请从Cisco IQ SaaS下载内部AI推理基础设施模块：

1. 登录到[Cisco IQ](#)。
2. 导航到系统设置 > 程序包目录。



安装软件包

3. 从本地AI推理基础设施卡中，点击下载选项>安装包。Download Application窗口打开。



The image shows a dark-themed dialog box titled "Download On-Prem AI Inference Infrastructure". It contains three sections: "System version" with a dropdown menu showing "System vv1.2.0", "Build type" with a dropdown menu showing "Release", and "Application version" showing "1.0.4". At the bottom right, there are two buttons: "Cancel" and "Download".

Download On-Prem AI Inference Infrastructure

System version

System vv1.2.0

Build type

Release

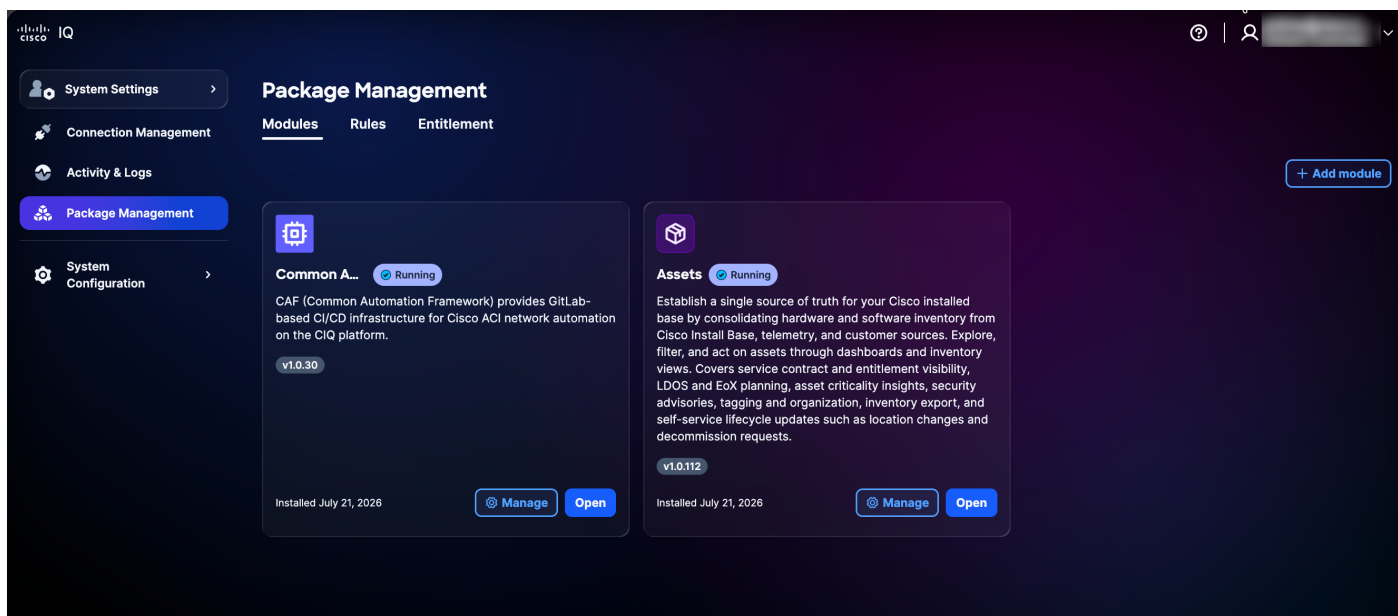
Application version

1.0.4

Cancel Download

下载AI推理基础设施

4. 从下拉列表中选择System version。
5. 从下拉列表中选择Build type。
6. 单击 Download。
7. 导航至VA。

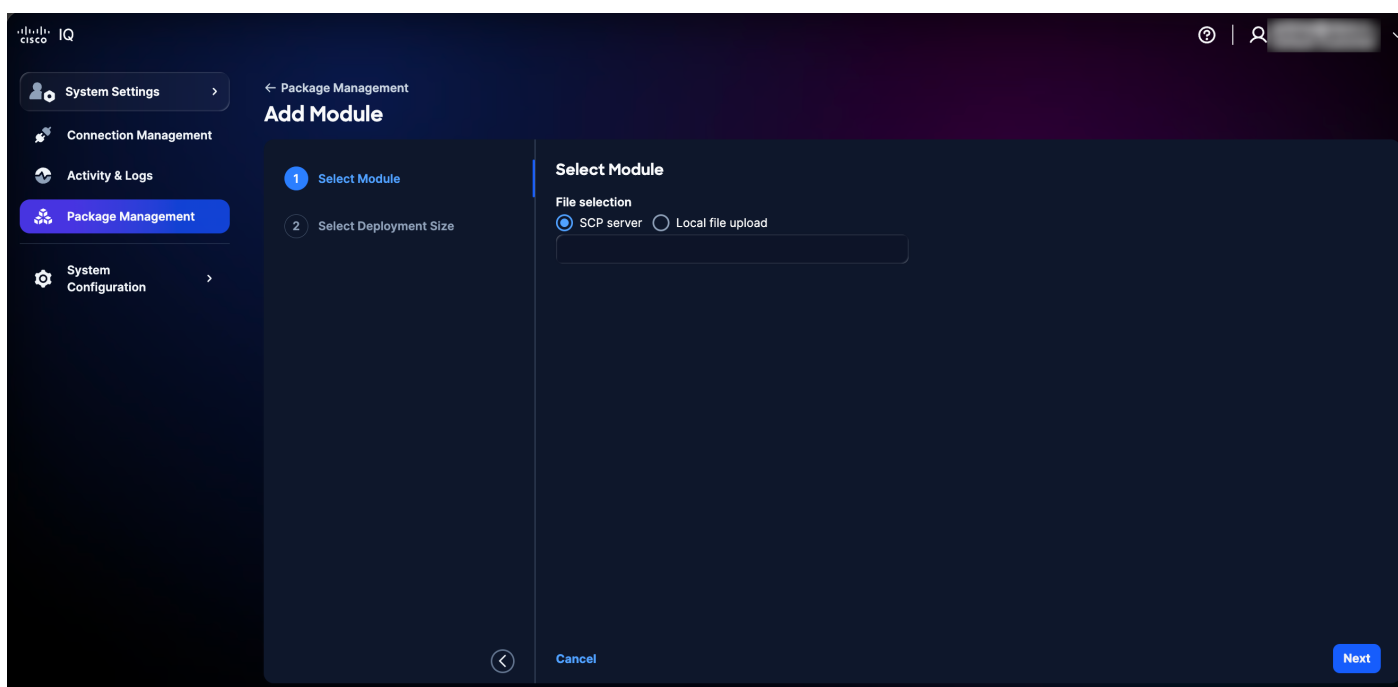


包管理

8. 导航到主页 > 系统设置 > 软件包管理。系统随即会显示Package Management页面，其中包含以下选项卡：

- 模块
- 规则
- 授权

9. 在Modules选项卡中，单击Add modules。



选择模块

10. 选择您的首选文件选择选项：
- SCP服务器:输入安装软件包的确切文件名（ 建议用于大文件 ）。

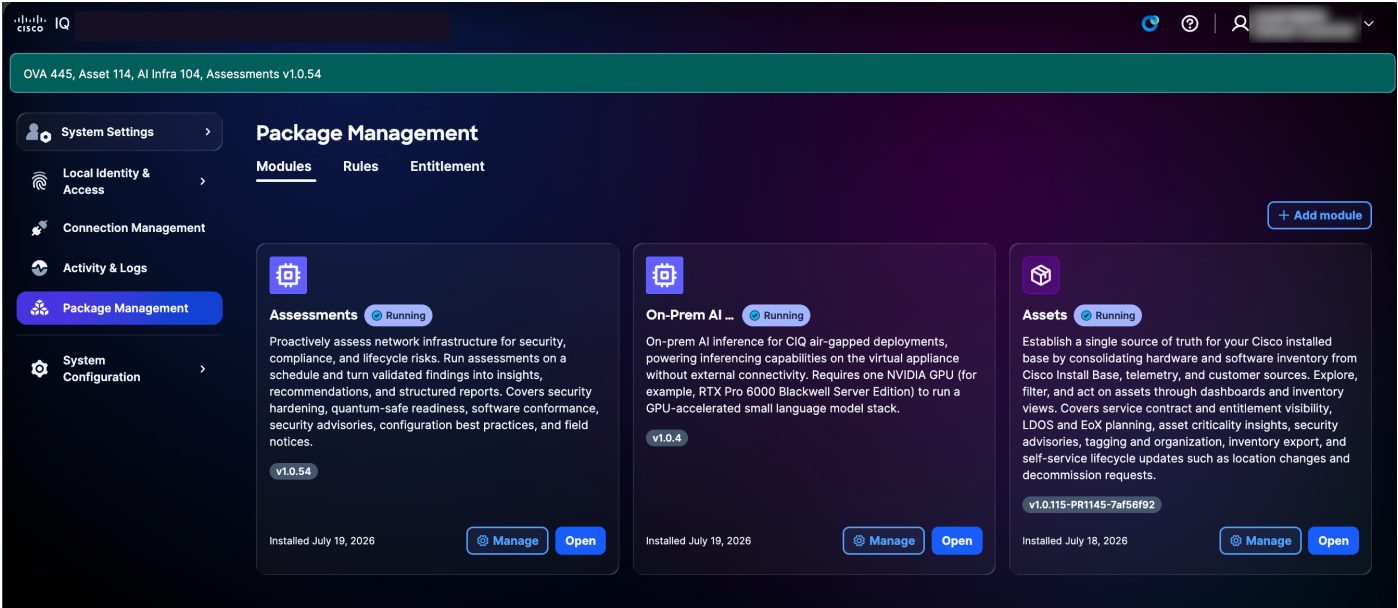
• 本地文件上传:拖放下载的安装文件（ 由于上载时间的原因，不建议对30 GB或更大的文件使用 ）。
- 注意：本地文件上传方法具有20分钟阈值。如果上传过程超过此持续时间，安装将失败。使用SCP服务器是确保成功且稳定安装的首选方法。
11. 单击 Next。系统开始上传文件。
12. 选择Deployment Size（ 例如， Small、Medium或Large ）。
13. 单击Add Module。安装开始，大约需要40-45分钟才能完成。

安装完成后，本地AI推理基础设施将显示在Package Management的Module选项卡上。

 注意：每个GPU只能运行一个内部AI推理基础设施模块。模块使用约90%的GPU VRAM。不支持在同一GPU上安装其他实例。

管理内部AI推理基础设施模块

安装后，可以从Package Management中的Applications选项卡管理本地AI推理基础设施模块。



编辑AI推理基础结构

要管理模块，请点击On-Prem AI Inference Infrastructure模块旁边的Manage。有关详细信息，请参阅[管理模块](#)。

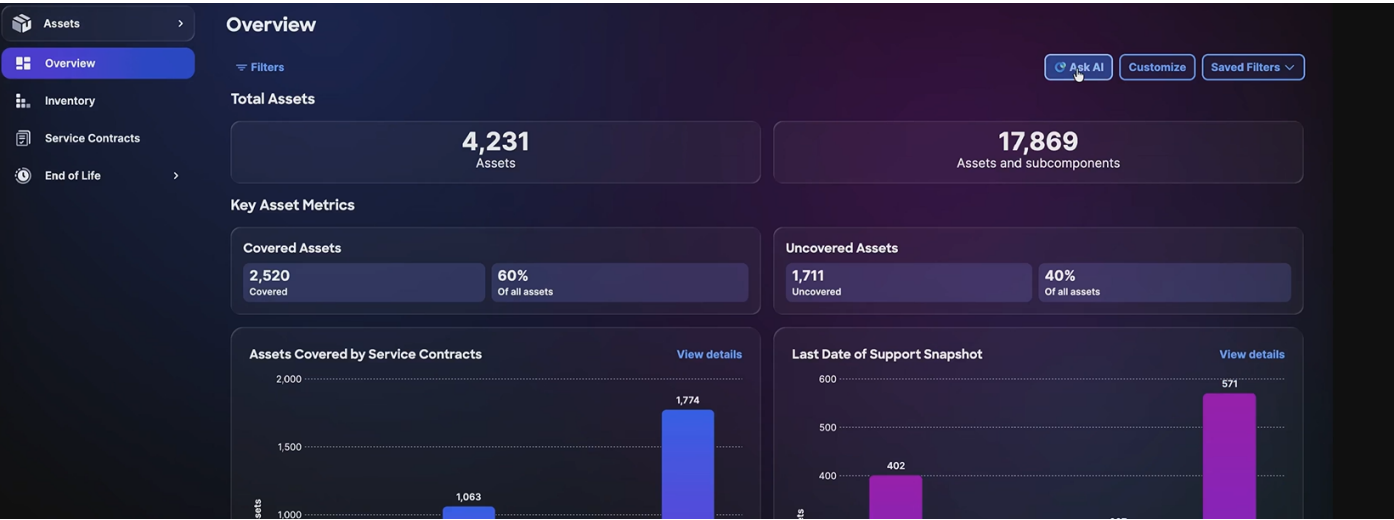
使用AI支持的功能

成功安装本地AI推理基础设施模块后，VA界面中将出现Ask AI按钮。

询问资产中的AI

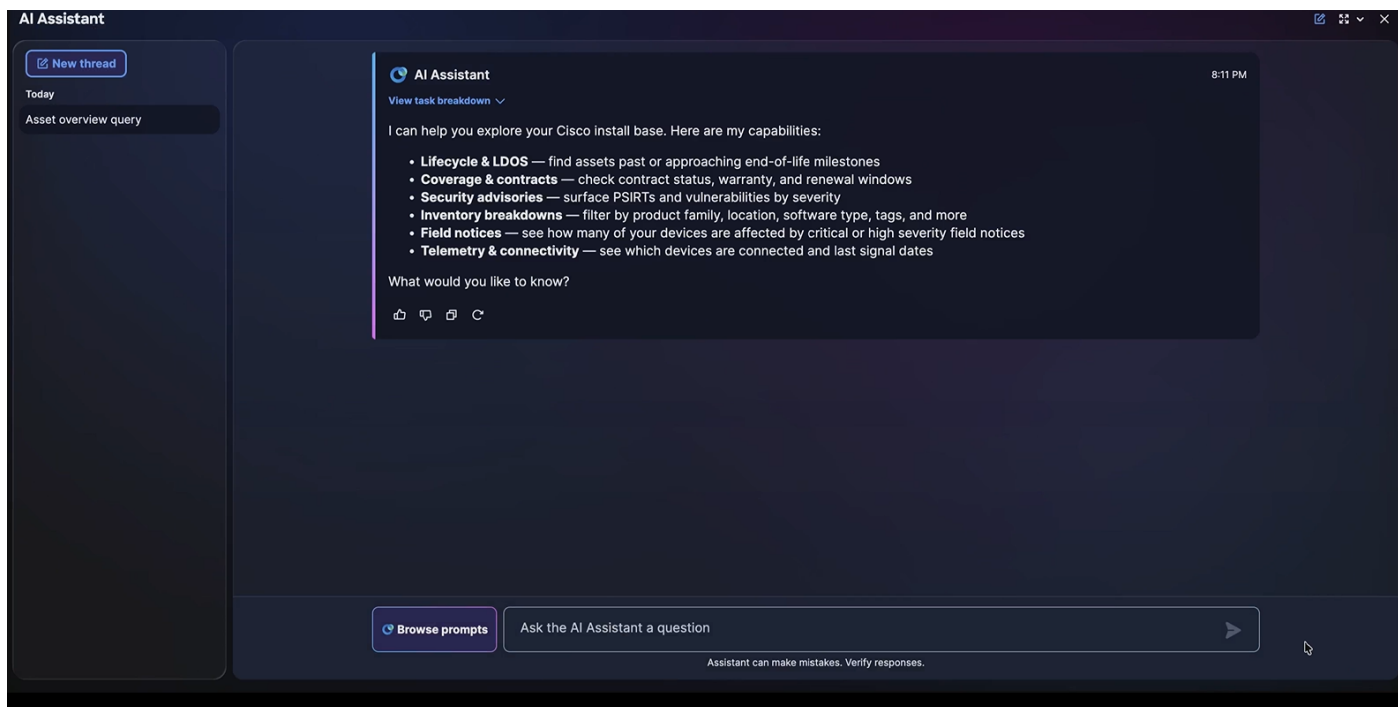
要在资产中使用Ask AI，请执行以下操作：

1. 选择Home菜单> Assets。系统随即会显示Assets页面。



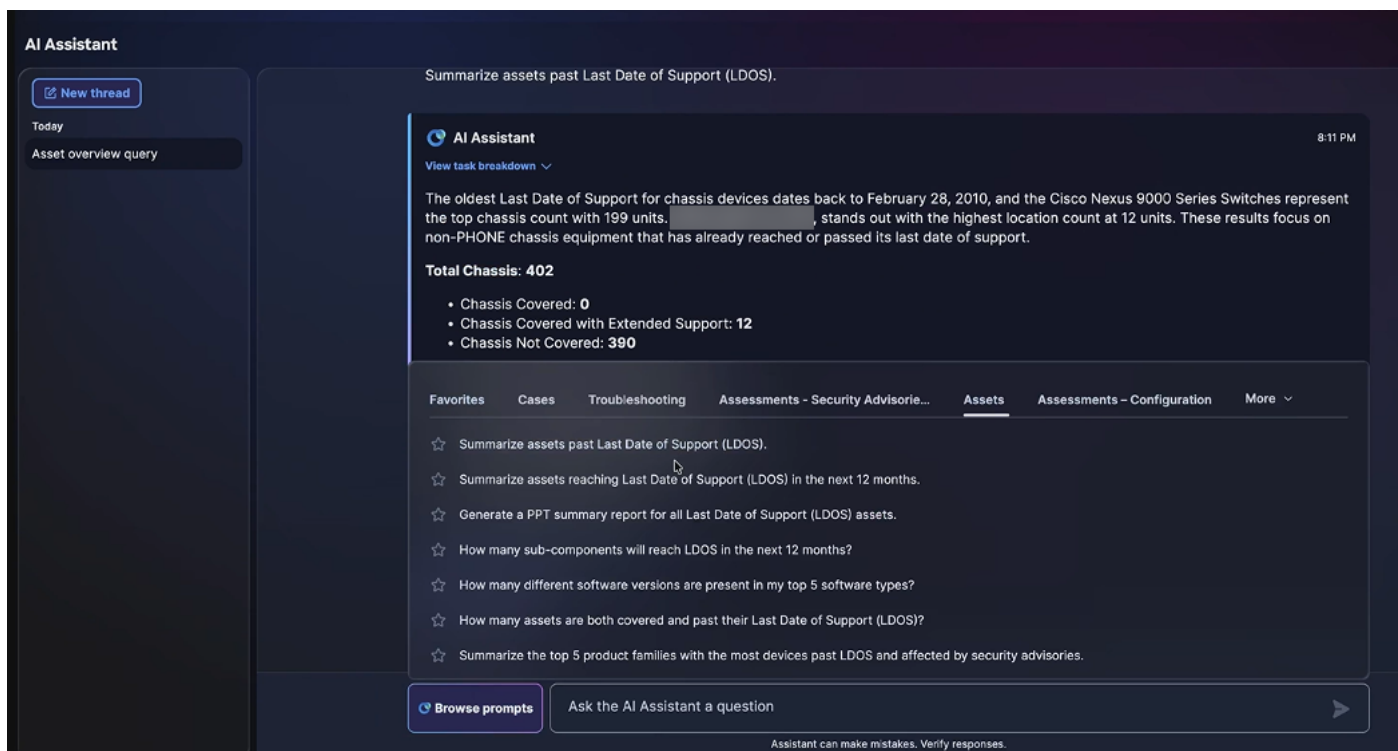
资产页面

2. 单击Ask AI。内部AI推理基础设施启动。



浏览提示

3. 单击Browse prompts查看可用的提示，或在向AI助理询问问题字段中输入自定义问题。



提示集

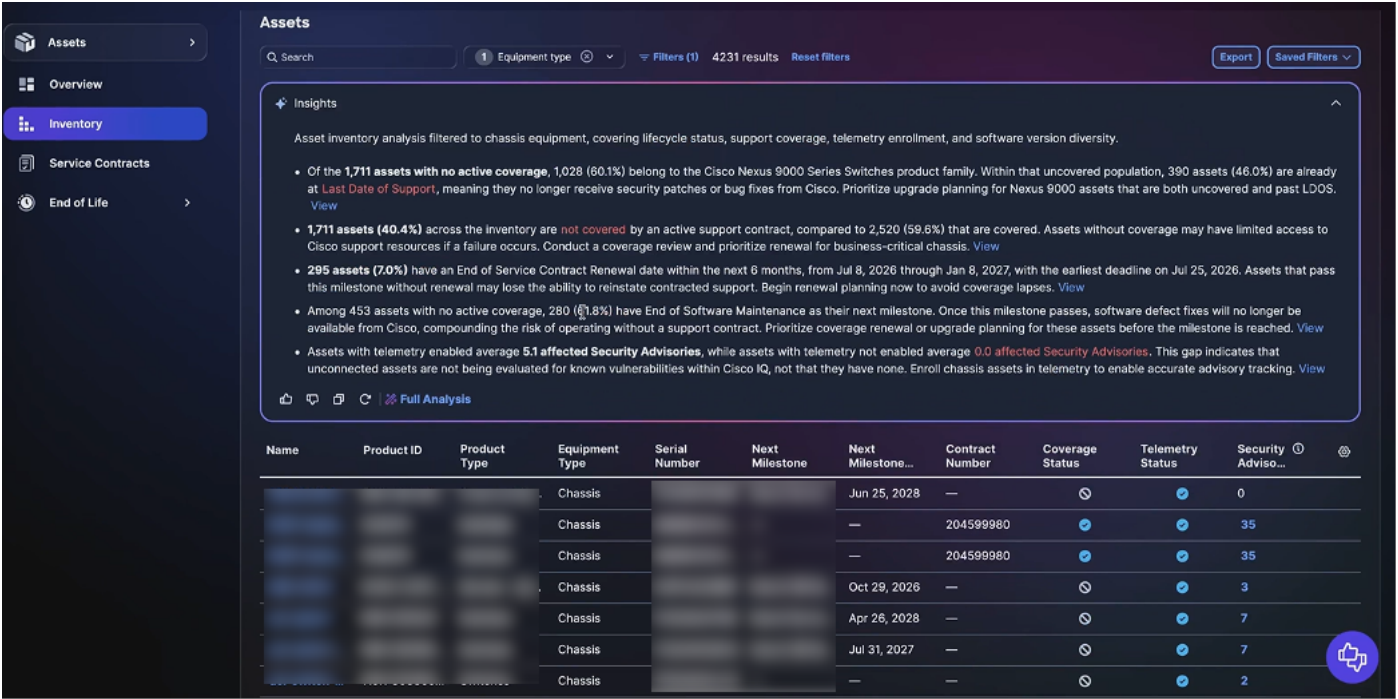
4. 单击所需的提示或按Enter。本地SLM生成响应。

库存中的AI分析

本地AI推理基础架构模块在库存部分提供由AI驱动的自动化分析。一旦填充库存数据，分析结果会自动显示。

要查看库存中的AI分析，请执行以下操作：

- 1. 选择Home菜单> Inventory。系统随即会显示Inventory页面。



资产

- 2. 查看AI生成的分析。数据可用后，结果将显示在资产视图中。

 注意：单击Full Analysis可查看图形、控制面板和图表等可视化内容，这些内容可提供更多见解。

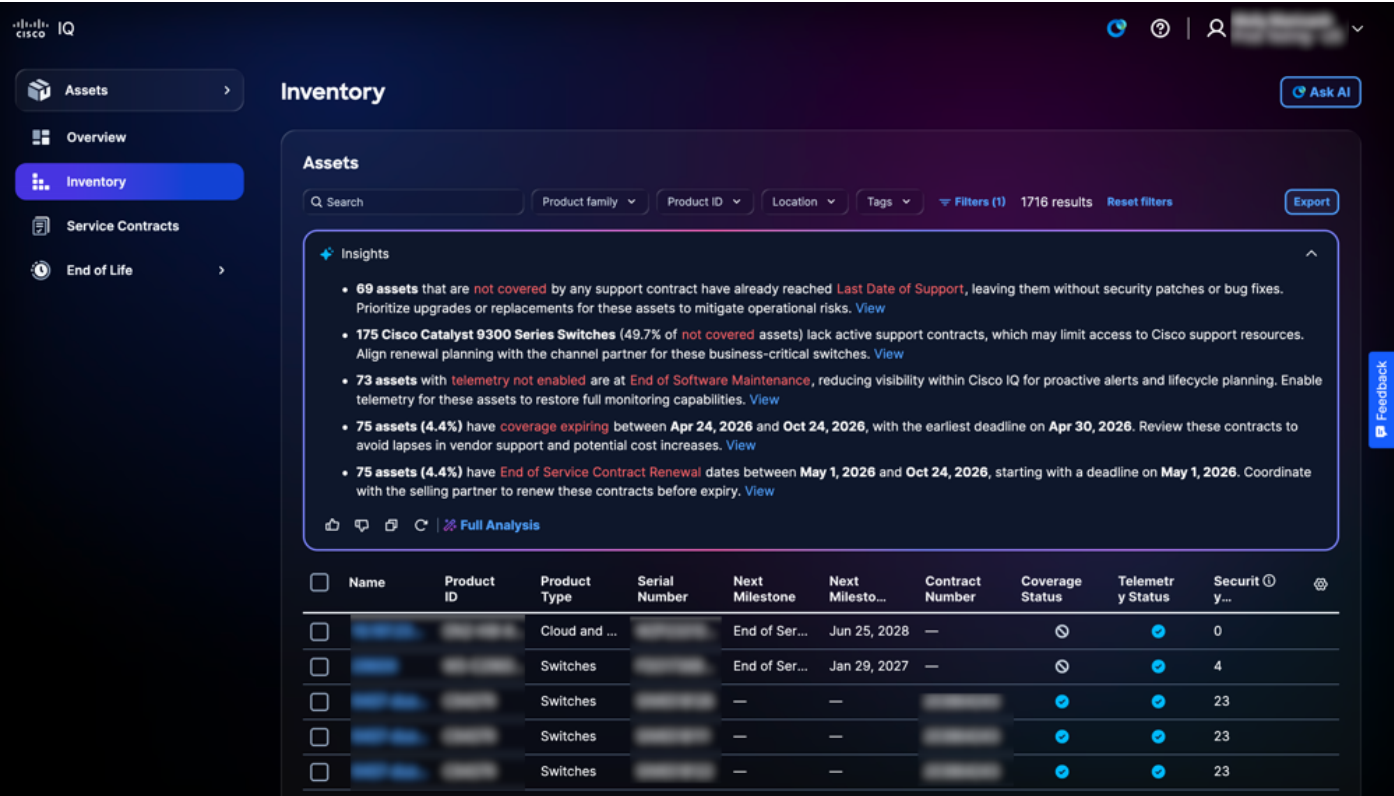
模块的常见功能

本节详细介绍所有模块共享的核心功能。这些功能提供一致的用户体验、优化系统性能并简化管理工作流程

分析数据

Insights面板提供该页面上数据的AI驱动分析，提供切实可行的见解，以改善网络环境的安全性和运行状况。

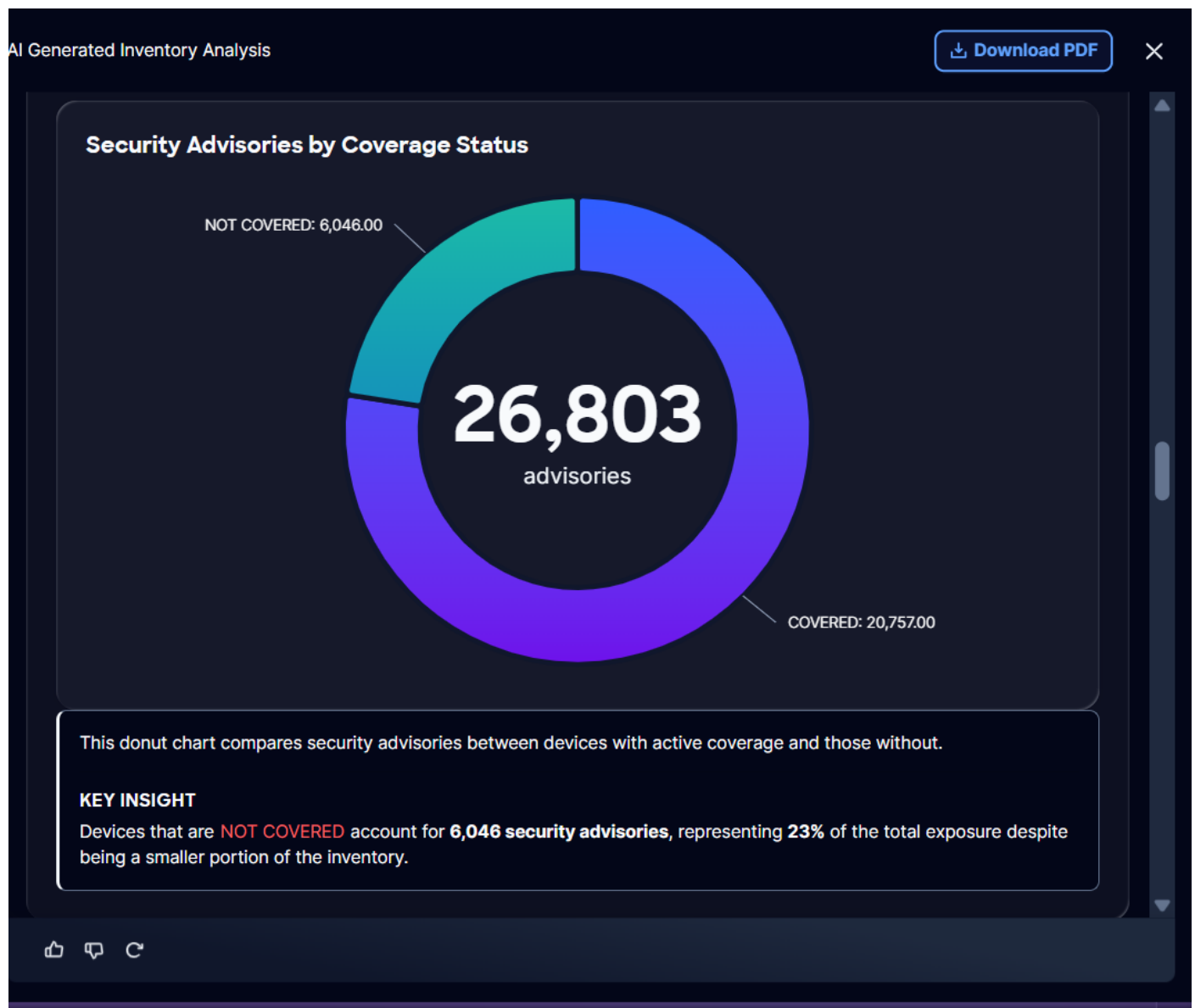
 注意：“分析”(Analysis)功能仅在选取页面上可用。



Insights面板

以下选项在“见解”面板中可用：

- 单击Expand图标展开面板并显示其他见解
- 单击Thumbs Up或Thumbs Down图标提供有关AI生成的信息的反馈
- 单击Full Analysis可显示其他信息、更深入的分析以及图形、控制面板和图表等可视化内容



全面分析

以下选项在完整分析中可用：

- 单击下载PDF，为您的记录或协作保存分析的脱机副本

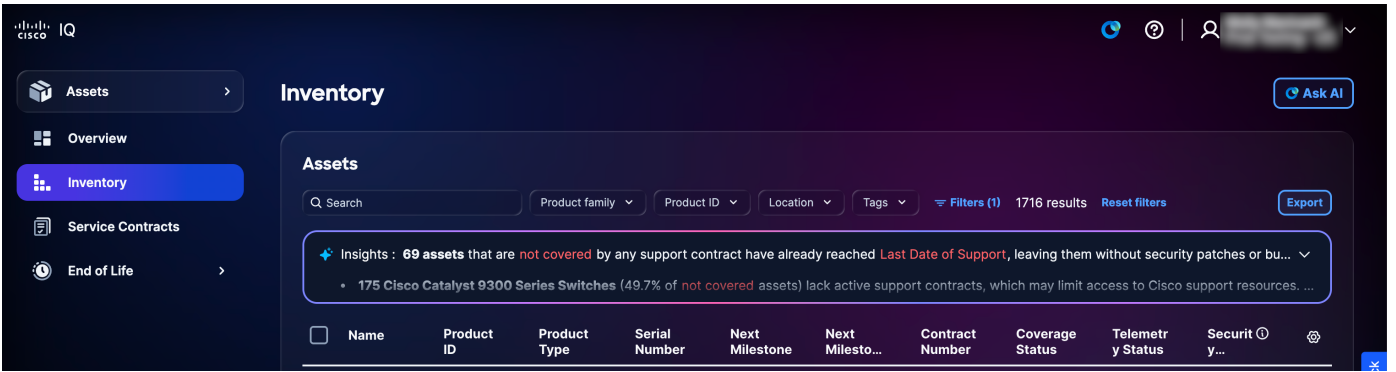
导出信息

导出功能允许您以.xls或.csv格式导出资产和安全信息的自定义视图。

 **注意：**导出功能仅适用于所选页面。

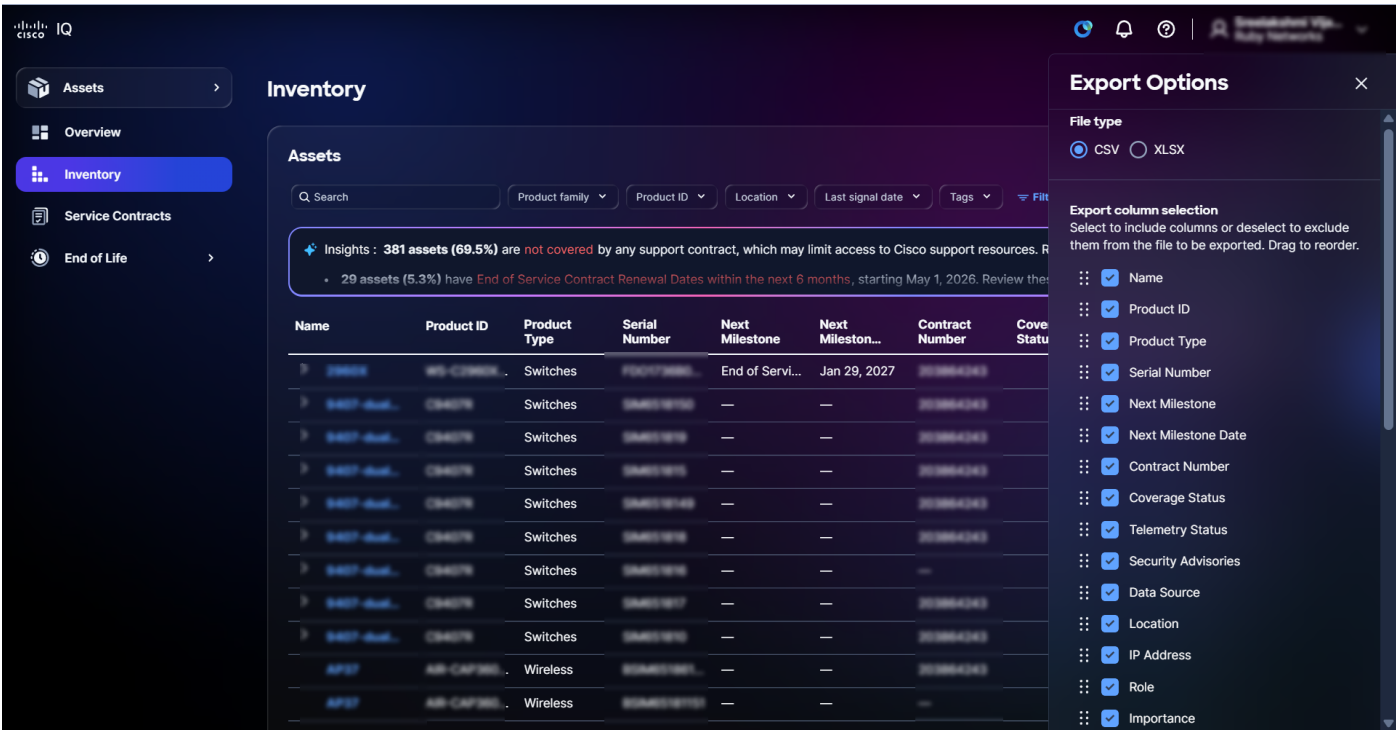
要从页面导出信息，请执行以下操作：

1. 导航到页面。



在资产模块中导出库存

2. 单击Export。系统随即会显示Export Options。

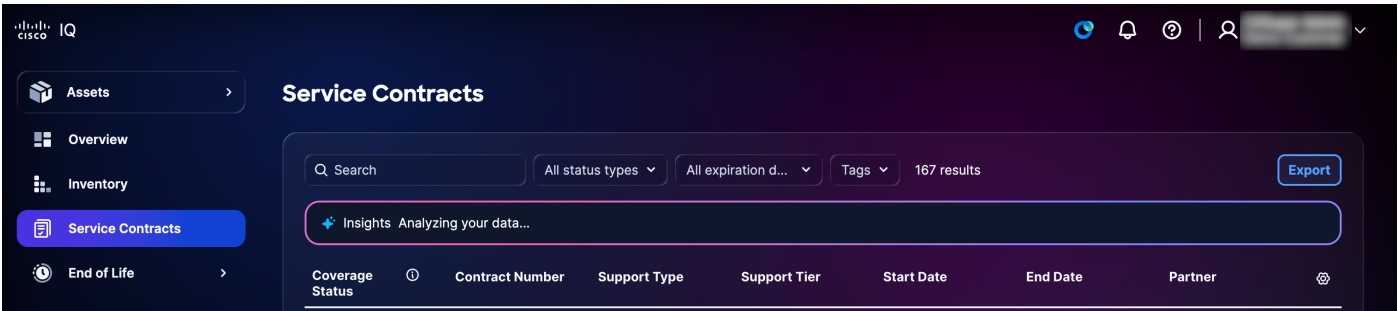


导出选项

3. 选择文件类型。
4. 选中所需列中的复选框。
5. 单击Export。文件下载到浏览器的本地下载文件夹。

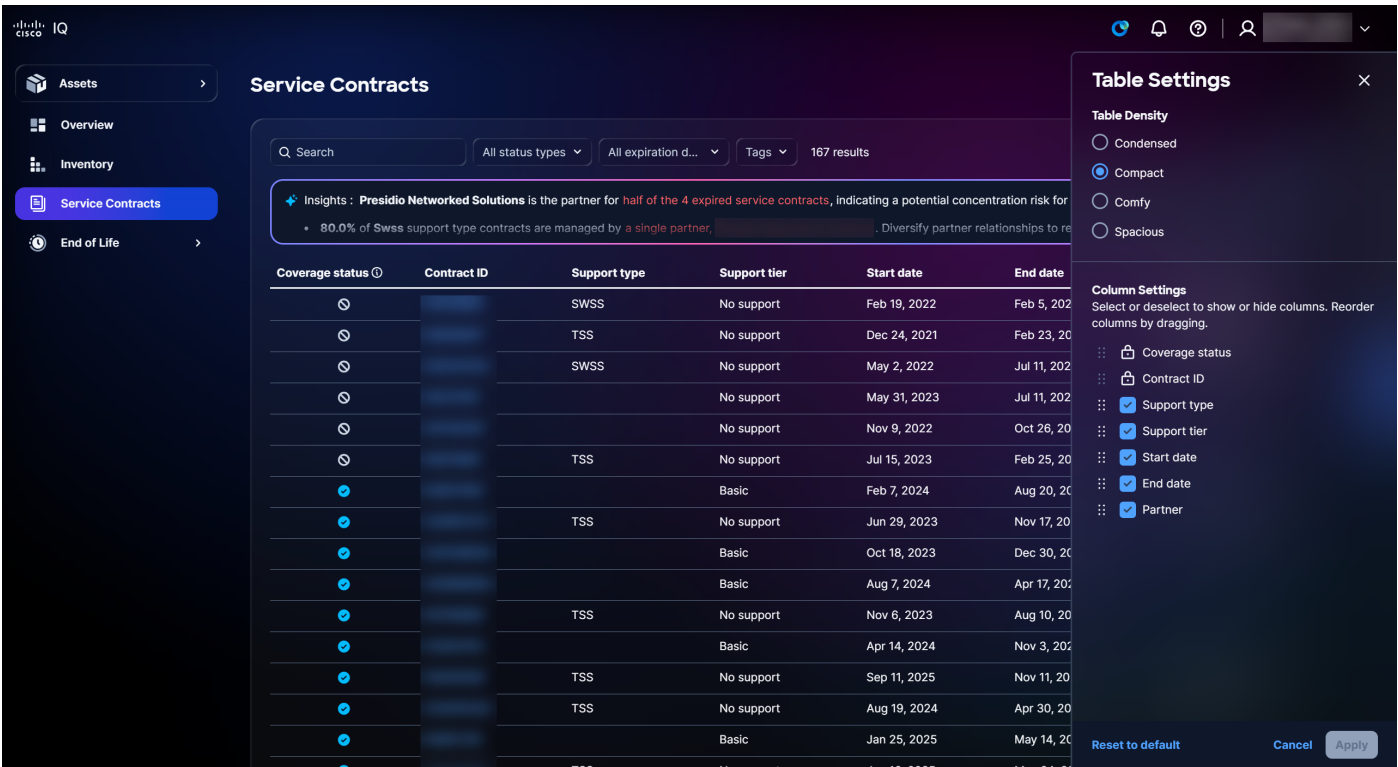
表设置

您可以配置表设置，为不同的模块功能创建自定义和细化视图。



表设置

要更改在选定页面上显示的列，请点击表设置图标。系统随即会显示表设置。



表设置选项

更改表视图

要更改表视图，请执行以下操作：

1. 选择以下表密度选项之一：

- 压缩:最小化可视元素和间距以显示更多信息
- 紧凑:减少空白并缩小UI元素之间的间距
- 舒适:在元素之间使用更多空白和更大的间距
- 宽敞:强调丰富的空白和更大的UI元素

2. 单击 Apply。

添加和删除列

要添加或删除列，请执行以下操作：

1. 选中或清除列设置复选框。
2. 单击 Apply。



注意：无法从表视图中删除Name列。

更改列顺序

要更改列顺序，请执行以下操作：

1. 拖放列名，按所需顺序排列项目。
2. 单击 Apply。

自定义控制面板

自定义控制面板功能使您能够通过一系列直观的自定义选项来个性化标准控制面板：

- 使用拖放功能重新排列控制面板构件或面板
- 删除与工作流程无关的任何组件
- 您的个性化控制面板布局可安全地存储到您的用户配置文件中，并自动应用于所有会话和设备
- 使用简单的重置选项恢复原始控制面板布局

要自定义控制面板，请执行以下操作：

1. 导航至控制面板。



自定义

2. 点击自定义。



编辑控制面板

3. 根据需要更改控制面板：

- 重新排列：将构件拖放到所需的布局中
- 删除:单击Delete图标可删除构件
- Reset:单击Reset to default将控制面板重置为其原始布局

4. Click Save.系统随即会显示Dashboard Saved消息。

控制面板布局会自动应用于所有会话和设备。

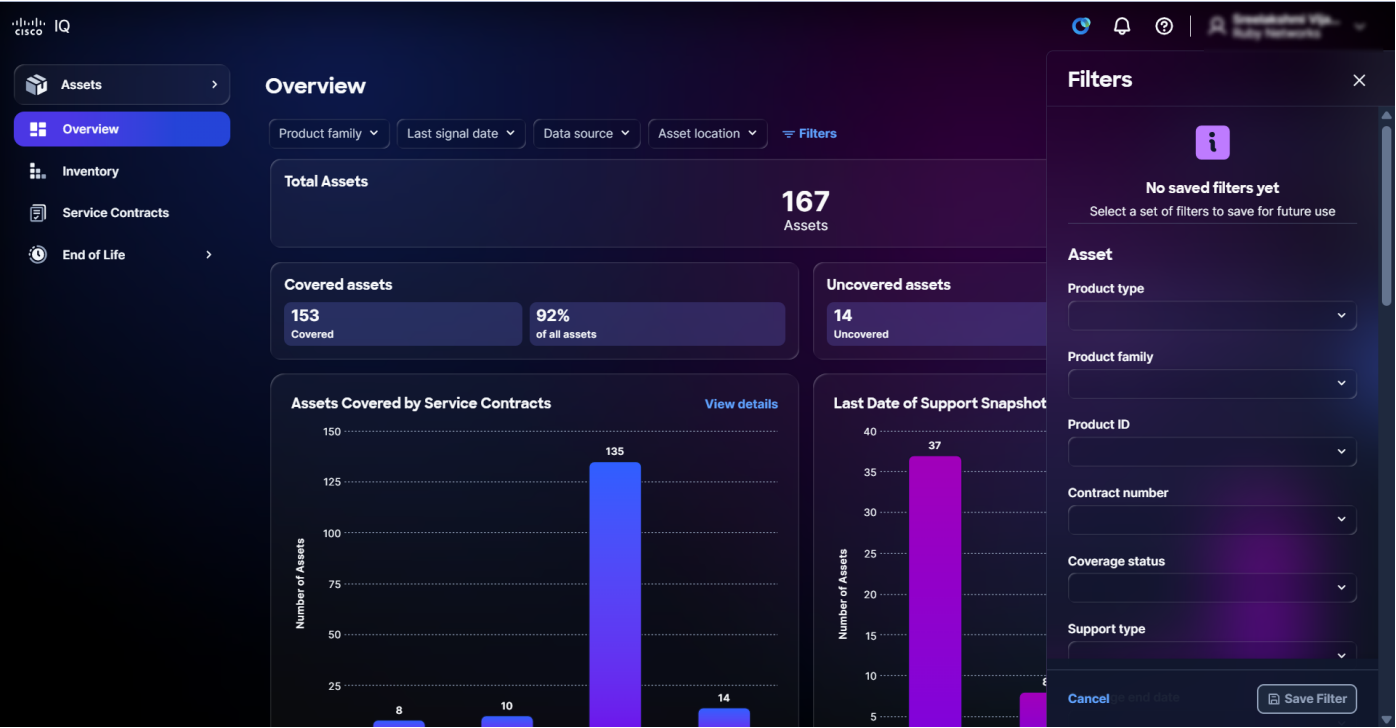
自定义过滤器

您可以保存任何控制面板视图的自定义过滤器配置，使您能够根据需要轻松返回首选设置。所有过滤器首选项都以每个用户、每个帐户的方式安全地存储，从而确保每次访问Cisco IQ时都能获得个性化和一致的体验。

创建过滤器

要创建自定义过滤器，请执行以下操作：

1. 导航至控制面板。
2. 单击Filters。



过滤器

3. 从下拉列表中选择所需的过滤器。
4. 单击Save Filter。“名称保存的过滤器”(Name Saved Filter)窗口打开。

Name saved Filter

Filter name *

Custom Filter |

Cancel

Save Filter

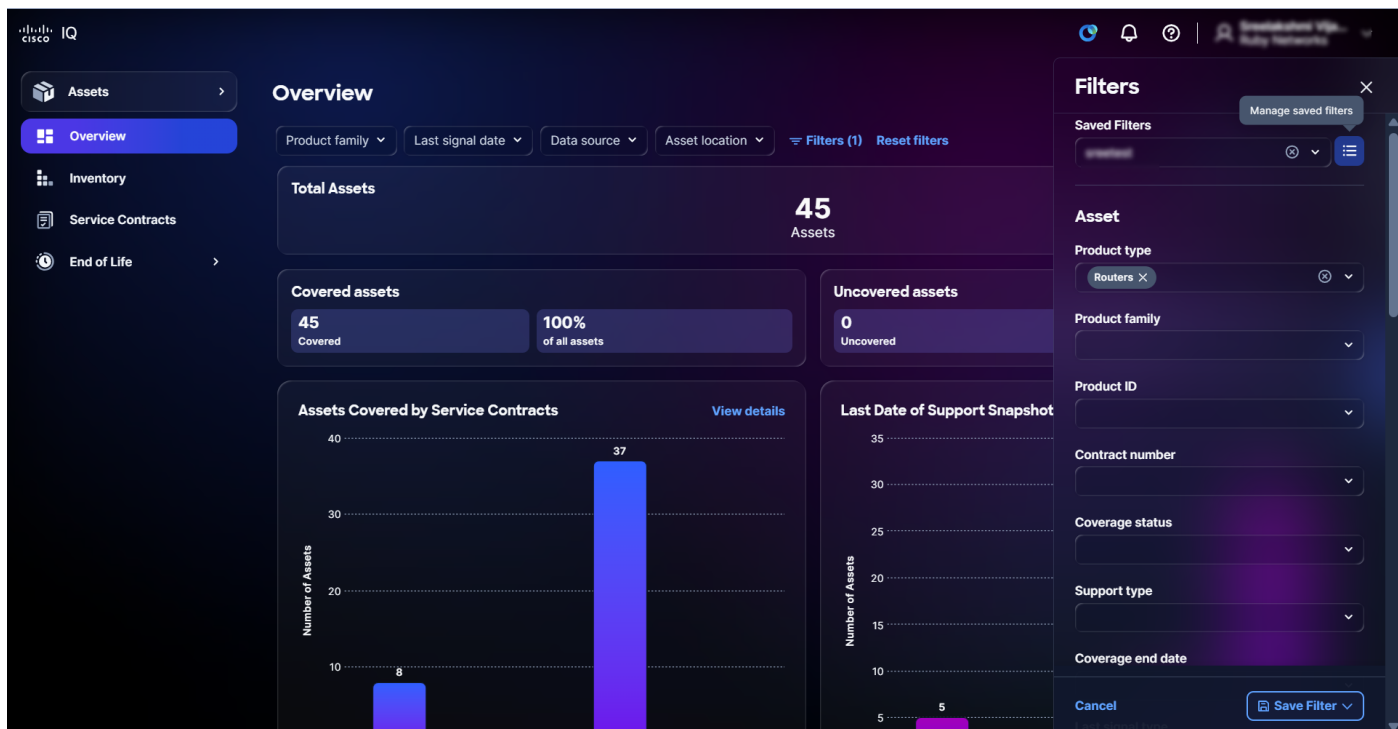
过滤器名称

5. 输入过滤器名称。
6. 单击Save Filter进行确认。

编辑过滤器名称

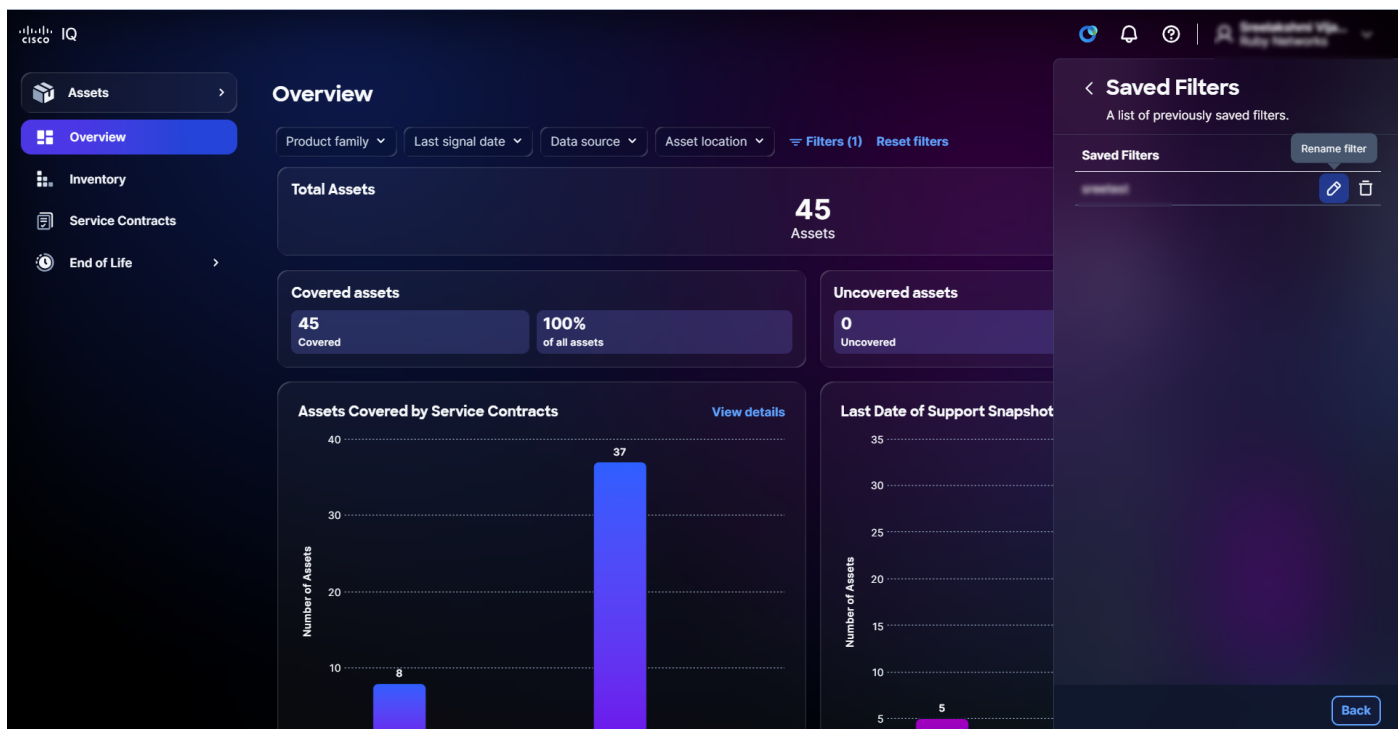
要编辑自定义过滤器，请执行以下操作：

1. 单击Filters。



管理已保存的过滤器

2. 点击Manage saved filters (管理保存的过滤器) 图标。
3. 导航到过滤器。



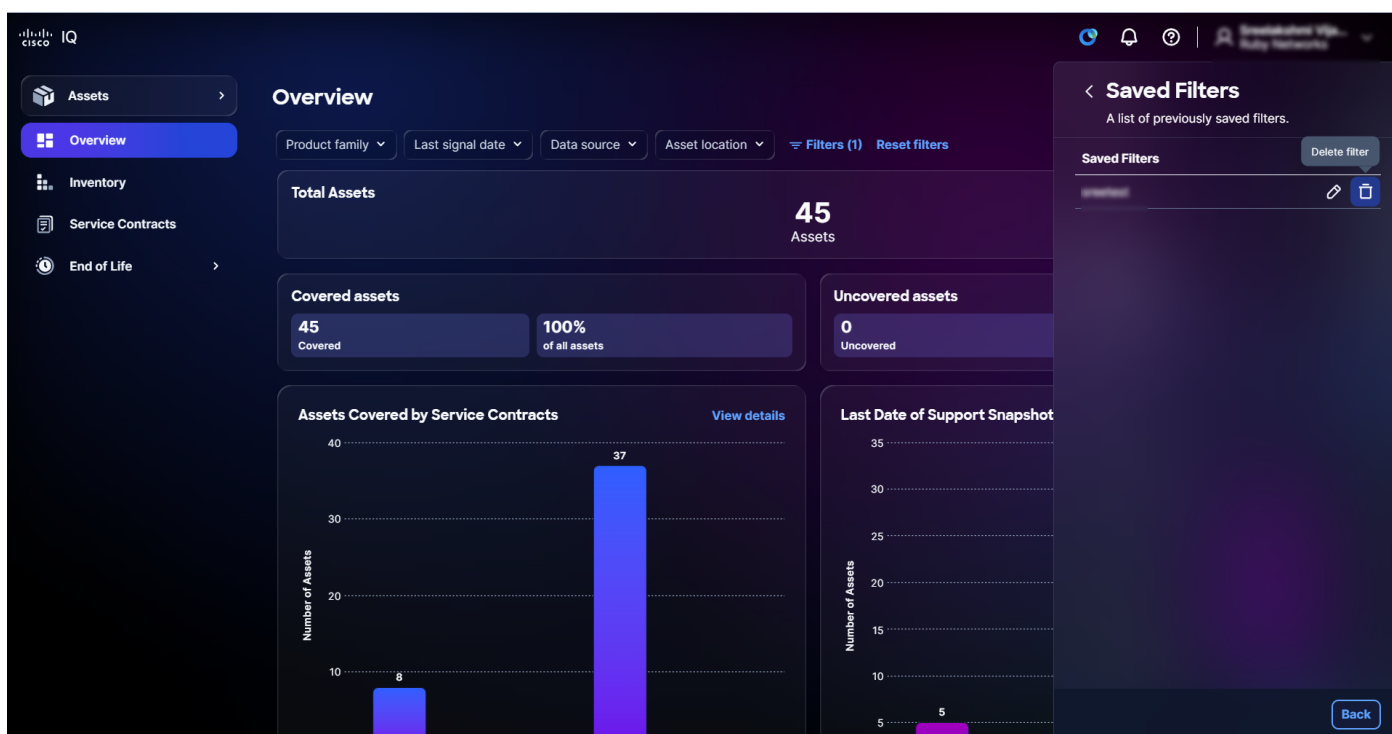
编辑过滤器

4. 单击Edit图标。将打开Name saved Filter窗口。
5. 编辑过滤器名称。
6. 单击Save Filter进行确认。

删除过滤器

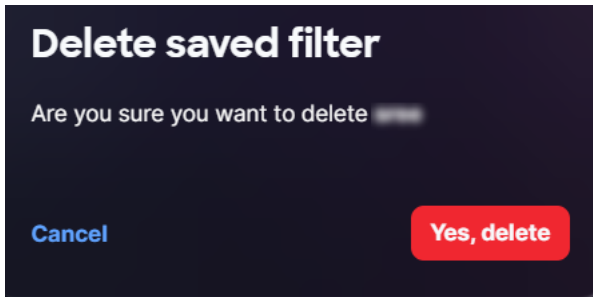
要删除自定义过滤器，请执行以下操作：

1. 单击Filters。
2. 点击“托管保存的过滤器”图标
3. 导航到过滤器。



删除已保存的过滤器

4. 单击Delete图标。将打开Delete saved filter窗口。



删除保存的过滤器确认

5. 单击Yes , delete进行确认。

资产模块

资产模块为思科资产提供全面的可视性和管理功能，是思科IQ的基础，可提供组织内所有设备的集中列表。通过从多个来源收集信息，它可以作为设备资产的一个单一数据源。维护完整且准确的资产列表至关重要，因为思科IQ中的其他模块（如“评估”模块）会依赖此数据来评估设备的健康 and 安全性。

核心概念

资产模块基于以下核心概念：

- 资产:作为思科服务交付的一部分进行库存和管理的任何物理设备、硬件或软件，并详细跟踪其身份、功能、服务覆盖范围和生命周期
- 合同来源资产:直接从链接的服务合同数据而不是通过遥感勘测数据纳入库存的资产。Cisco IQ从合同数据获取以下设备类型：机箱、模块、电源和风扇。即使不存在遥测连接，这些资产在资产中也是可见的
- 最后支持日期(LDOS):思科产品的生命周期终止和支持终止里程碑跟踪
- 服务范围:与特定硬件或软件相关的有效支持合同、保修和授权级别
- 资产标签:分配给资产的用于组织、过滤和操作工作流程的用户定义标签
- 设备信号:是指思科根据设备遥测、支持案例和合同续订最后一次观察设备（按序列号）的时间；通过多层数据管道吸收和丰富资产遥测数据

访问资产模块

要访问Cisco IQ中的资产管理功能，请选择Home menu > Assets，或者从Home page > Launchpad选项卡的Application部分中点击Assets。系统随即会显示Overview页面。

资产概述

Overview页面显示一个控制面板，通过该控制面板，您可以快速评估设备的运行状况和状态。

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

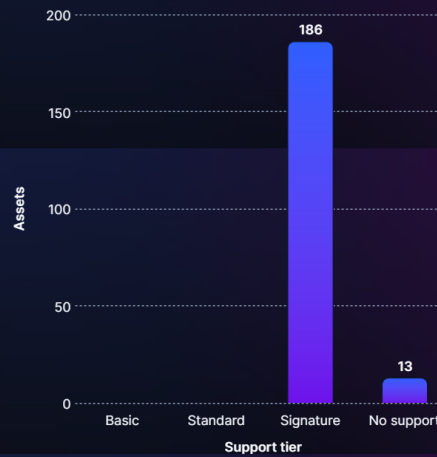
13

Uncovered

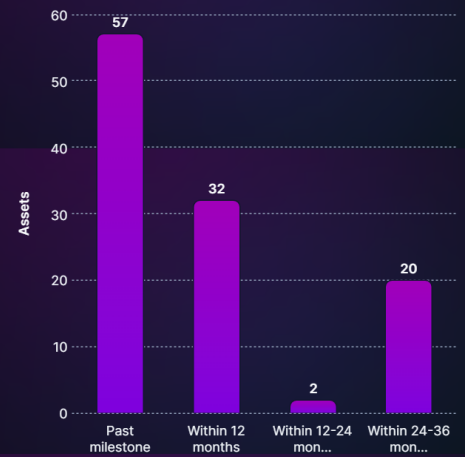
7%

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

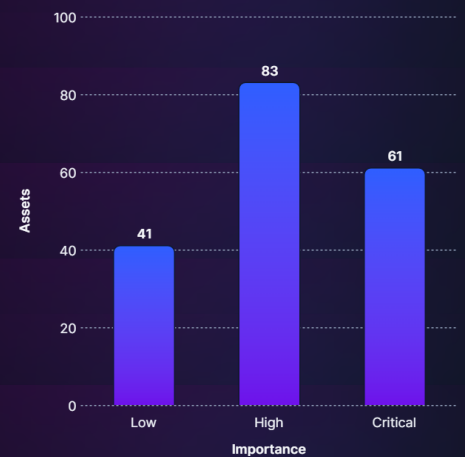
Assets With Critical or High Security Advisories [View details](#)



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](#)



资产概述

控制面板显示以下信息：

- 总资产:思科IQ帐户内的资产总数
- 关键资产指标:其他关键指标，如遥测状态、关键安全建议和LDOS信息
- 覆盖资产:服务合同覆盖的资产总数和百分比
- 未覆盖资产:服务合同未覆盖的资产总数和百分比
- 服务合同涵盖的资产:服务合同涵盖的资产（硬件或软件）数量的细分，按授权级别分类
- 最后支持日期快照:超过LDOS或达到LDOS的资产数量的细分
- 已启用遥测的资产：启用遥测的资产总数和百分比
- 未启用遥测的资产：未启用遥测的资产总数和百分比
- 具有关键或高安全性建议的资产:已启用遥感勘测、具有重要或高度安全建议的总资产的百分比
- 按重要性划分的资产：相对于网络中其他设备而言，分配给设备的优先级的细分。
- 资产细分:详细显示资产信息，例如产品系列、安装位置、软件版本和资产角色

筛选资源的视图

您可以通过从下拉列表中选择一个过滤器或点击Filters并从可用过滤器列表选择一个选项来过滤控制面板视图。

 注意：某些过滤器可能会根据屏幕缩放设置而隐藏。根据您的角色和权限，可使用不同的过滤器。

查看资产的详细信息

单击View Details时，页面重定向到Inventory页面。有关详细信息，请参阅[资产](#)。

资产重要程度见解

思科IQ包括Asset Criticality Insights，这是资产模块中的新功能，可预测网络设备的功能角色和业务重要性。通过分析设备配置和启用的功能，Asset Criticality Insights可帮助您确定哪些资产对网络的影响最大，以便您确定这些资产的优先级，以便进行安全补救、软件升级、生命周期终止(EOL)规划和覆盖决策。

 注意：资产重要度见解仅适用于具有有效遥测连接的标准或签名级别的资产。请确保您的资产满足配置要求，以便在控制面板中填充这些见解。

资产重要程度分析可在以下领域的资产应用中获得：

- 资产概述:按资产重要程度分析属性过滤和查看摘要细分
- 资产库存:按角色和重要性显示、搜索、过滤和排序设备
- 资产详情:查看各个设备的角色和重要性，并提供说明每个值的信息工具提示

覆盖角色和重要性分类

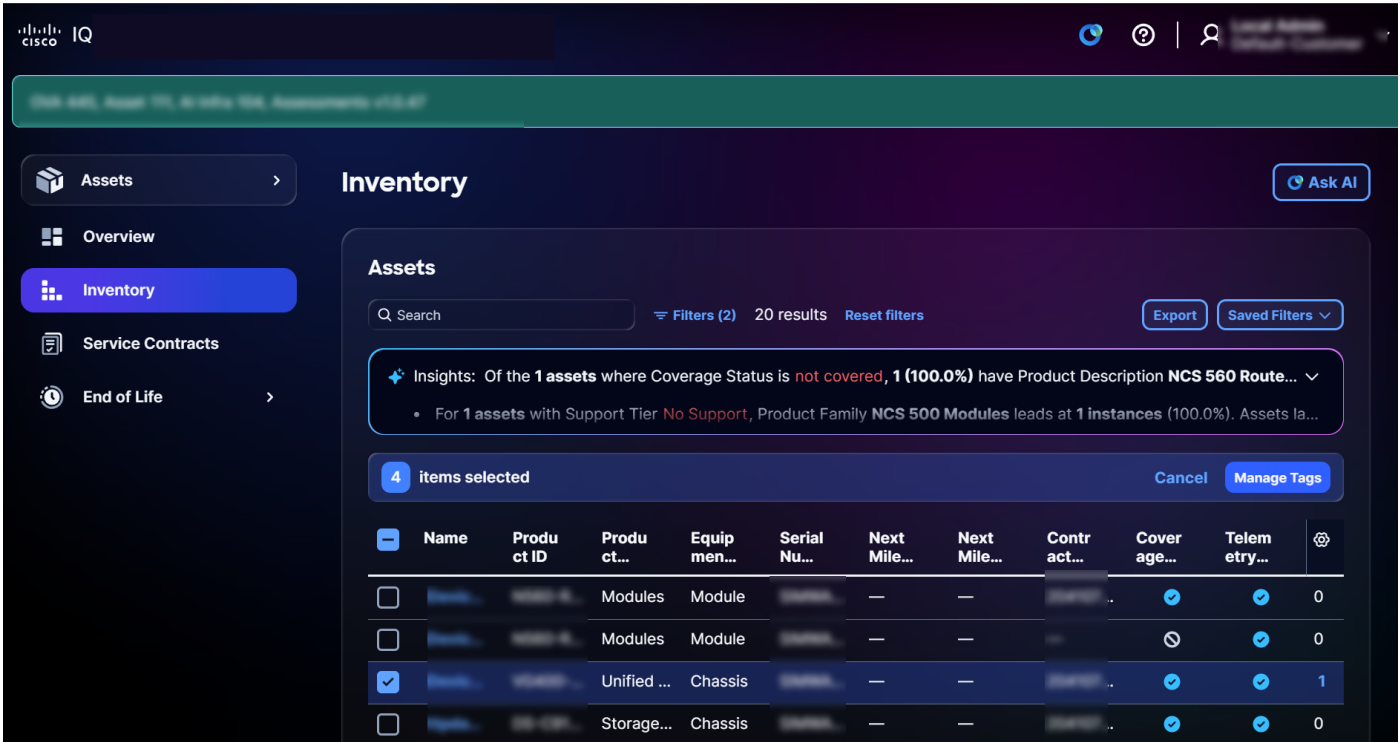
思科IQ根据遥测数据自动预测每项资产的角色和重要性。当自动预测无法准确反映资产在网络中的功能或重要性时，帐户管理员可以手动更正这些分类。

 注意：覆盖控制仅适用于帐户管理员。对于所有其他用户角色，Role和Importance值均为只读。

从库存表改写分类

要覆盖一个或多个资产的角色或重要性，请执行以下操作：

1. 导航到资产 > 库存。
2. 点击所需资产行的复选框。要同时更新多个资源，请选择多个复选框。



角色和重要性

3. 在角色或重要性列中，从资产行下拉列表中选择正确的值。
4. 单击Apply确认覆盖。

具有手动覆盖值的资产会在“角色”或“重要性”列中显示一个可视指示器。

 注意：要删除先前配置的覆盖并返回自动预测，请从Role或Importance下拉列表中选择短划线 (—)选项。

覆盖资产明细中的分类

要从资产详细信息视图改写职责或重要性，请执行以下操作：

1. 导航到资产 > 库存，然后点击资产。
2. 在资产详细信息面板中，找到角色和重要性字段。
3. 点击要更新的字段的下拉框并选择正确的值。
4. 单击Apply进行确认。

资产的详细信息视图还显示遥测属性的说明，该说明通知原始自动预测，以帮助确定覆盖是否合适

查看覆盖审计追踪

1. 选择Home > System Settings > Activity & Logs。
2. 选择Filters > Action Type > override以仅显示覆盖事件。

注意：可以按日期范围、用户和资产名称过滤审计追踪。

资产

Inventory页面提供了Cisco IQ帐户中所有思科资产的列表。

资产

搜索和筛选资产清单视图

可以通过从下拉列表中选择一个过滤器或点击Filters并从可用过滤器列表选择一个选项来过滤列表视图。您也可以通过在Search字段中输入资产名称来搜索资产。

 注意：

- 根据屏幕缩放设置，某些过滤器可能会隐藏。
- 根据您的角色和权限，可使用不同的过滤器。

库存分析

Inventory页面上的Insights面板显示AI驱动的分析，该分析提供资产摘要，重点关注支持覆盖范围、连接和里程碑。单击Full Analysis可查看图形、控制面板和图表等可视化内容，这些内容可提供更多见解。有关详细信息，请参阅[分析通用模块功能中的数据](#)。

导出库存

单击Export以.xls或.csv格式保存已过滤的资产列表。有关详细信息，请参阅[导出通用模块功能中的信息](#)。

查看资产详细信息

点击资产可查看资产详细信息。系统随即会显示资产的详细信息视图，其中包含以下选项卡：

- 详细信息:显示资产详细信息，例如产品、信号数据、身份、位置、保修和覆盖信息

Assets

Overview

Inventory

Service Contracts

End of Life

Inventory

10.197.238.131

Cisco Catalyst Center Appliance (Gen 2) - 44 Core

DetailsProduct AlertsHardwareSoftware

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

资产详细信息

- 产品风险通告:显示相关产品风险通告，如安全建议和现场通知

- Hardware:提供硬件EOL详细的时间表视图(例如销售终止、最后发货和最后支持日期等)
- 软件：提供软件EOL的详细时间表视图

资产标签

资产标签是您在Cisco IQ中分配给资产资产的自定义标签。标记是您定义的key:value对，例如，Environment:Prod或Label:Campus。您可以一次为单个资产或多个资产分配标签，而且您可以按标签过滤资产以快速找到您关心的资产。

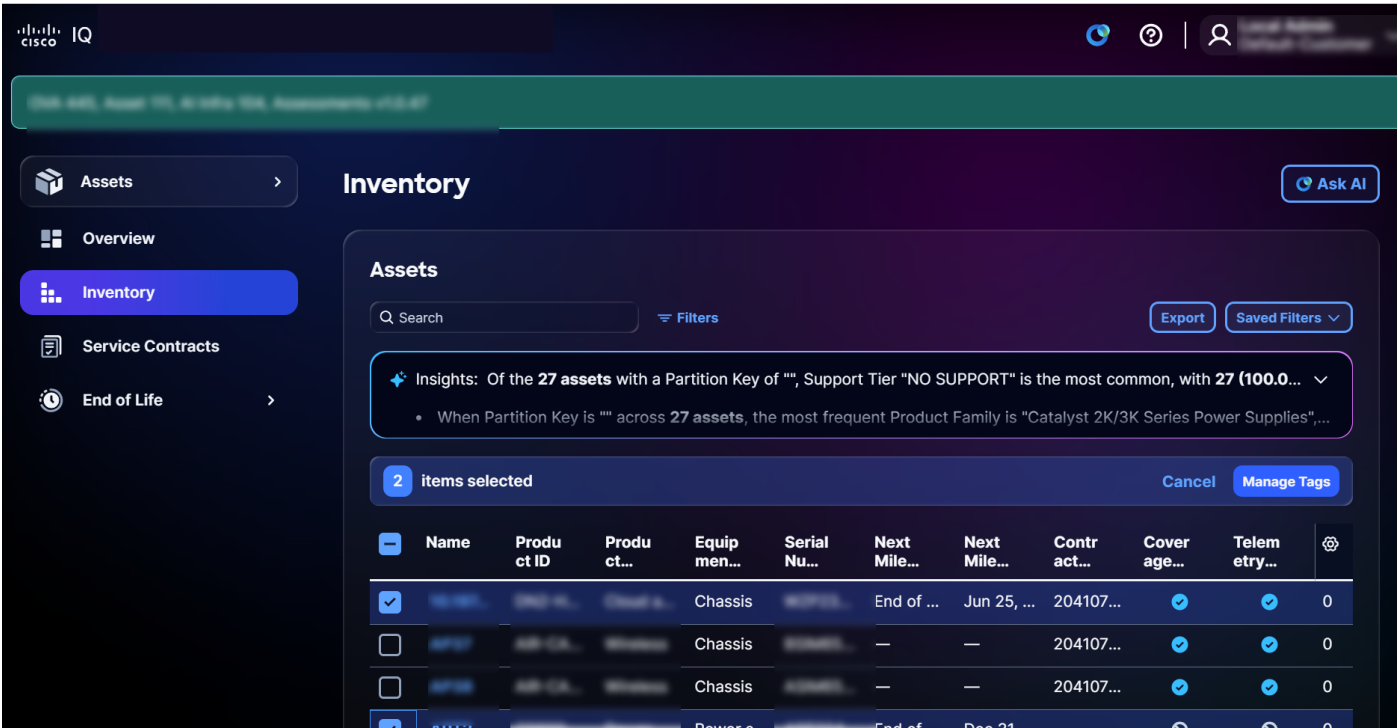
 注意：在帐户管理员创建标记后，用户可以将标记分配到资产。

分配标记

在Inventory视图中向选定资产分配标记，可以组织和分类资产，从而增强过滤、报告和管理。

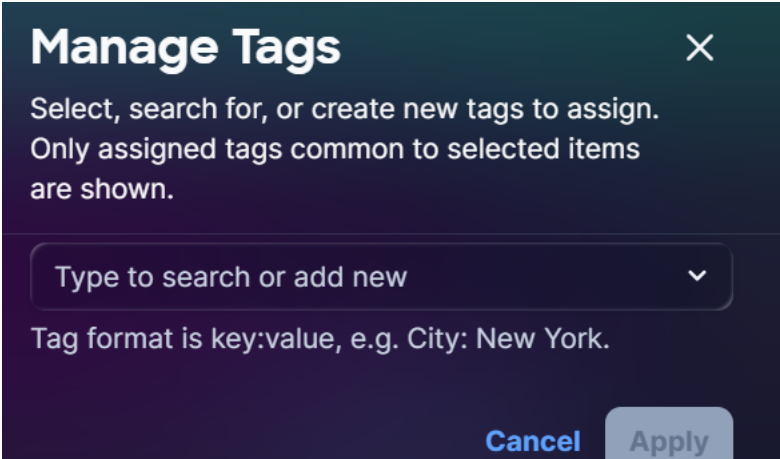
要将标签分配给资产，请执行以下操作：

1. 导航到资产 > 库存。



标记资产

- 2. 选中所需资源的复选框。
- 3. 点击管理标记。Manage Tags窗口打开。



分配标记

- 4. 在文本字段中，输入标签名称或从现有选项中选择标签名称，然后按Enter。

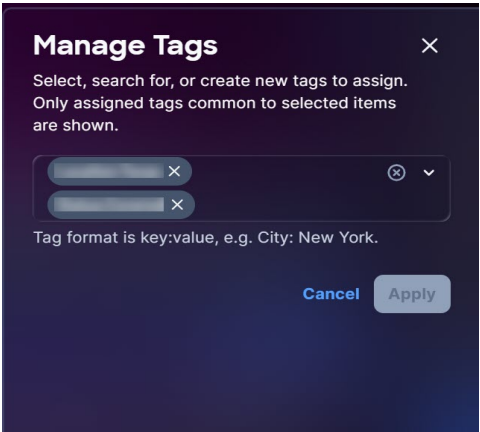
 注意：标签采用key:value格式（例如，City:NYC）。

- 5. 单击 Apply。

删除资产标记

要从一个或多个资源中删除标签，请执行以下操作：

- 1. 导航到资产 > 库存。
- 2. 选中一个或多个资源旁边的复选框。
- 3. 单击Manage tags。Manage tags窗口打开。



删除标记

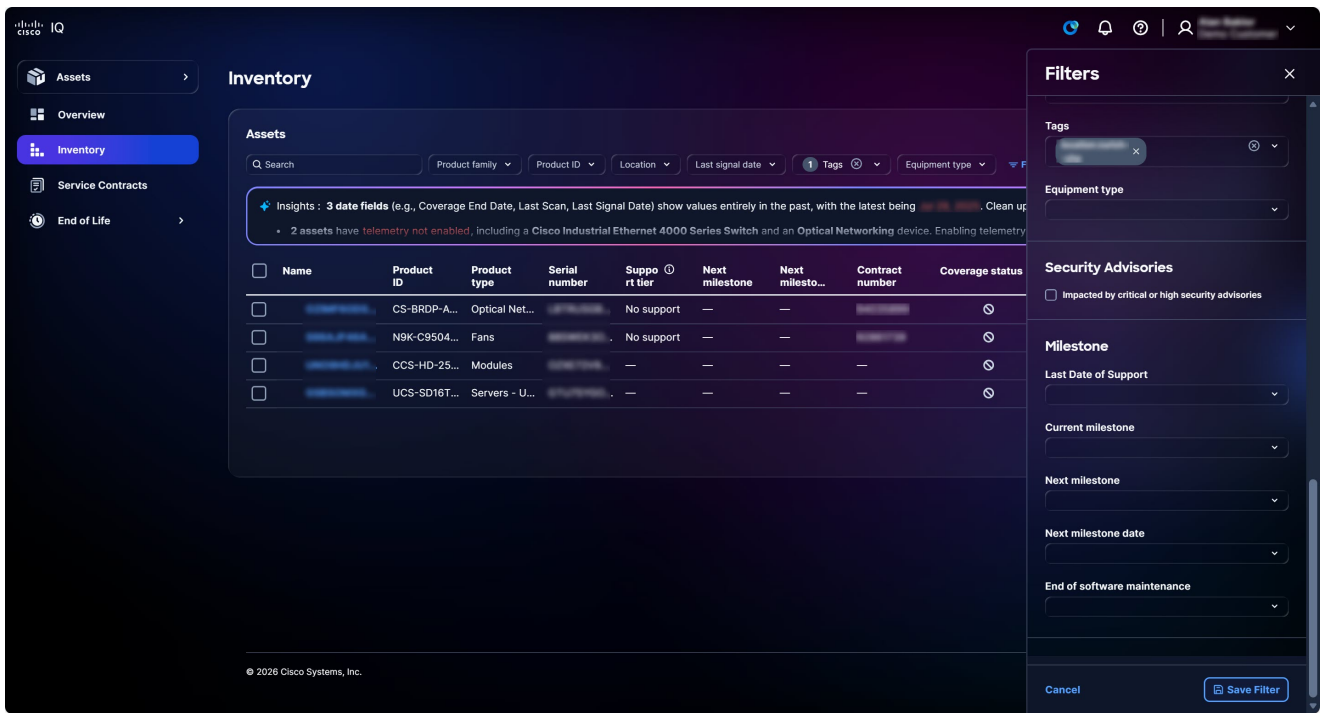
- 4. 单击任何标签上的X，将其从选择中删除。
- 5. 单击 Apply。

使用资产标签作为过滤器

创建标签后，您可以将该标签用作过滤器。

要将标签用作过滤器，请执行以下操作：

- 1. 导航到资产页。
- 2. 单击Filters。Filters窗口打开。



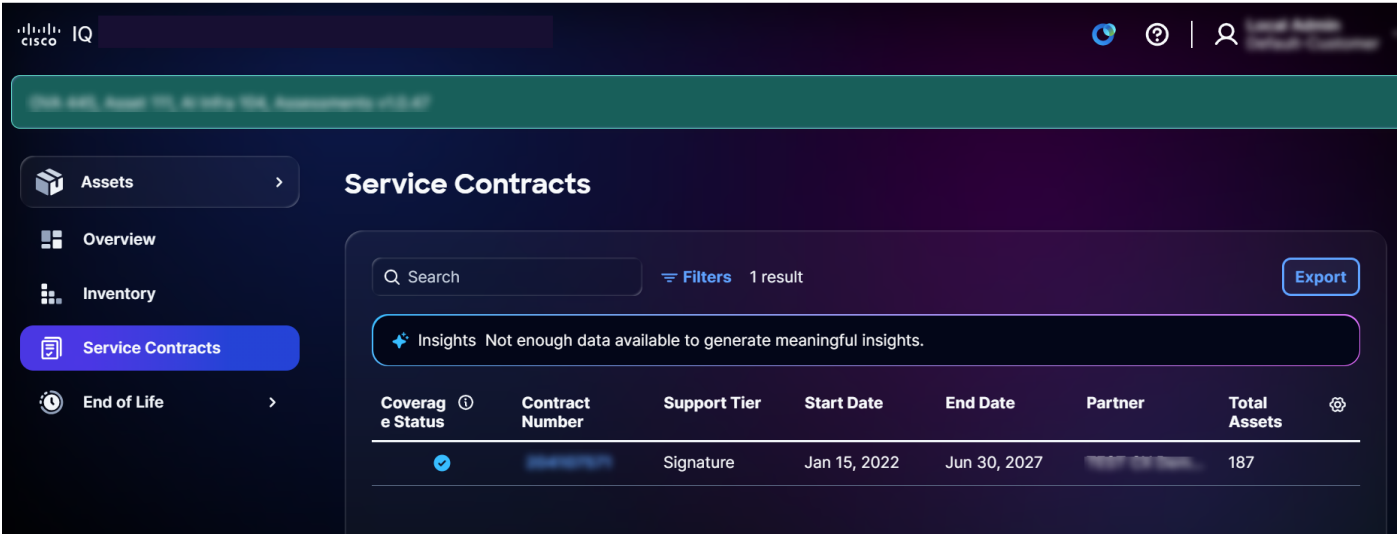
使用标签作为过滤器

- 3. 从Tags下拉列表中，选中所需标记的复选框。选择标记后，Inventory页面上的视图将更新为已过滤视图。

服务合同

服务合同页面通过提供摘要和详细的合同信息，支持有效的续约规划和覆盖范围战略，简化了合同

监督支持。



服务合同

搜索和筛选服务合同视图

您可以通过从下拉列表中选择过滤器来过滤列表视图。您也可以通过在Search字段中输入合同编号来搜索服务合同。

导出服务合同

单击Export以.xls或.csv格式保存已过滤的合同列表。有关详细信息，请参阅[导出通用模块功能中的信息](#)。

服务EA摘要

Services Enterprise Agreement(EA)Summary页提供了资产组合中客户群增长的整合视图。数据直接来源于思科的客户群记录，让您和客户团队能够一致地了解产品组合随时间推移的变化。

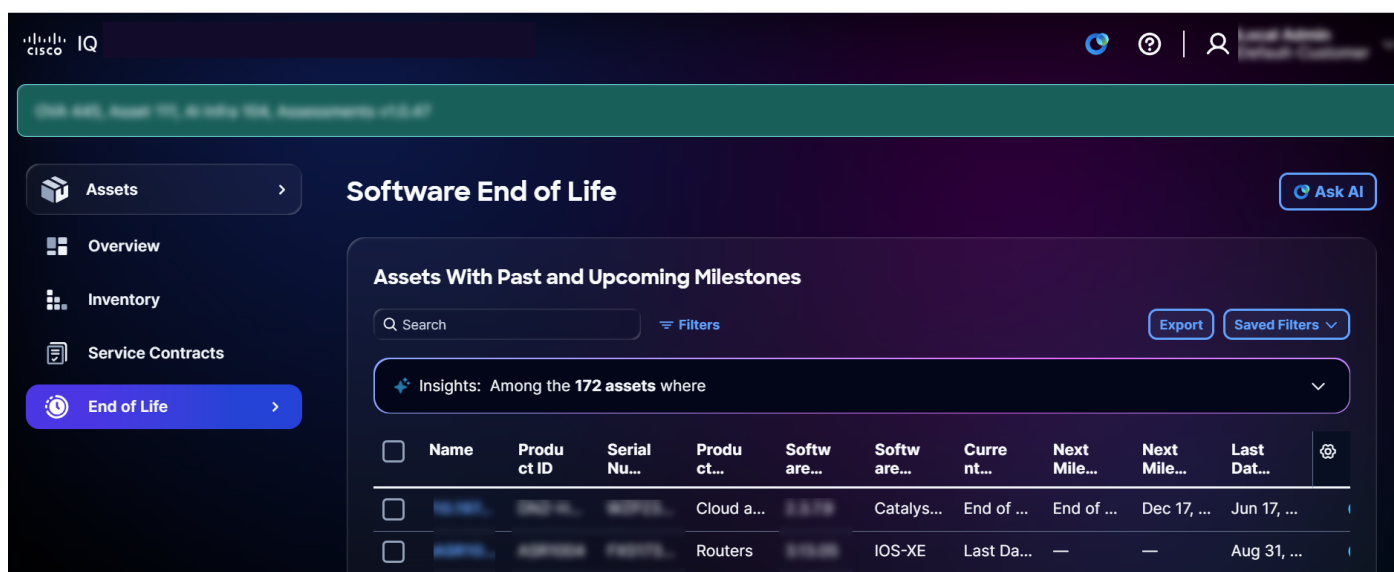
服务EA摘要页面显示以下信息：

- 添加的资产：报告期内添加到客户群的新资产
- 净变化:报告期内客户群规模的总体变化

 注意：访问服务EA摘要页面可能受角色和权限要求的约束。如果此页面在您的导航中不可见，请与您的帐户管理员联系。

生命周期结束

硬件寿命终止和软件寿命终止页提供详细的EOL信息，为用户提供主动管理产品更新周期和支持覆盖范围所需的支持。点击“寿命终止”(End of Life)页面上的资产会将您重定向到“资产”(Inventory)页面上的相关资产。



☐	Name	Product ID	Serial Nu...	Product...	Software...	Software...	Current...	Next Mile...	Next Mile...	Last Dat...	
☐	Cloud a...			Cloud a...	2.2.18	Catalys...	End of ...	End of ...	Dec 17, ...	Jun 17, ...	
☐	Routers			Routers	2.2.18	IOS-XE	Last Da...	—	—	Aug 31, ...	

软件寿命终止

寿命终止分析

End of Life页面上的Insights面板显示由人工智能驱动资产概述，其中定义了最后支持日期。单击Full Analysis可查看图形、控制面板和图表等可视化内容，这些内容可提供更多见解。有关详细信息，请参阅[分析通用模块功能中的数据](#)。

导出寿命终止

单击Export以.xls或.csv格式保存已过滤的EOL资产列表。有关详细信息，请参阅[导出通用模块功能中的信息](#)。

评估模块

“评估”模块提供了一个评估框架，使您能够主动调查并降低与安全性、稳定性、容量、合规性和老化相关的风险，从而保持网络安全、稳定和可靠。

核心概念

“评估”模块基于以下核心概念：

- **评估:**根据预定义的标准对基础设施实体进行系统评估，以衡量性能、合规性、安全性或运营能力；评估按需求、按时间表或由事件触发
- **评估执行:**评估的实例或单个运行；每次执行都会创建一个新的执行记录，用于跟踪评估生成的范围、触发机制、时间戳和结果数据
- **查找结果：**一个经过验证的、可操作的观察结果，可标识差距、风险、问题或值得注意的状态。调查结果表示评价期间的地面数据
- **见解:**从多个调查结果的模式或趋势中得出的更高级的分析结论。洞察力解释在更广泛的业务或运营环境中发现结果的意义
- **建议:**与发现或洞察力相联系的特定的、可操作的处方；这些建议提供了解决已发现问题或把握机遇的必要步骤的明确指导
- **报告:**一个结构化的文档，汇总了针对目标受众的调查结果、见解和建议；报告是向客户、高管和技术团队传达评估结果的主要交付内容

访问评估模块

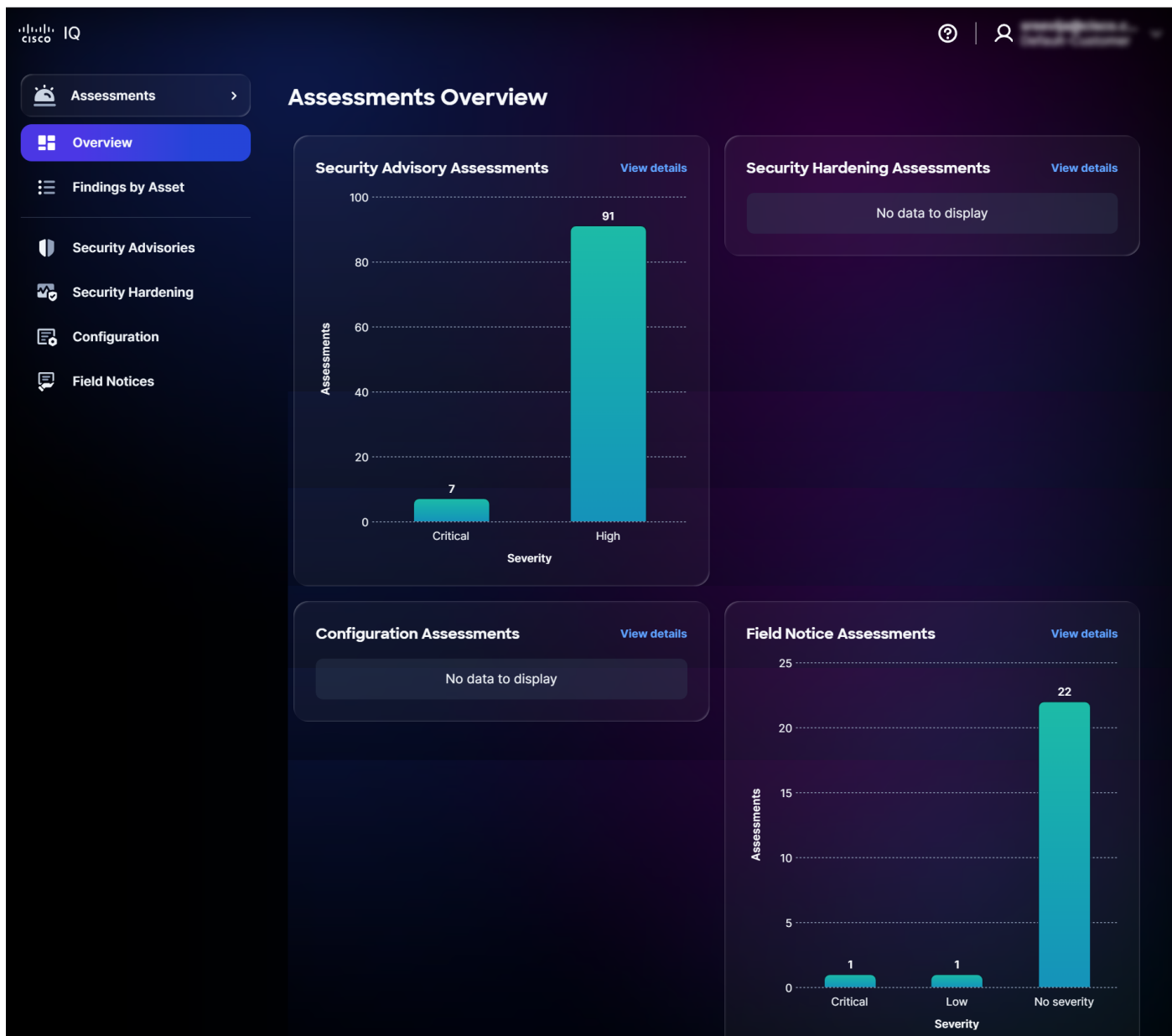
要访问Virtual Appliance中的安全和评估功能，请选择“主页”(Home)菜单>“评估”(Assessments)，或者从“主页”(Home)页面>“启动板”(Launchpad)选项卡的“应用”(Application)部分中单击“评估”(Assessments)。系统随即会显示Assessments Overview页面。



注意：也可以从System Configuration > Package Management启动评估模块。

评估概述

Assessments Overview页面显示以下控制面板：



评估概述

控制面板显示以下信息：

- 安全咨询评估:显示安全建议评估，按“严重”和“高”严重性分类
- 安全强化评估:显示未通过安全强化规则的资产，按“高”、“中”、“低”和“信息”严重性分类
- 配置评估:显示配置合规性规则失败的资产，按“严重”、“高”、“中”、“低”和“信息”严重性分类
- 现场通知评估:显示现场通知评估，按“严重”、“高”和“不适用”严重性进行分类



注意：您只能查看您有权访问的资产。

按资产列出的结果

按资产列出的结果页提供了已使用以下至少一个评估评估的资产的列表：安全建议、安全加固、配置和现场通知。

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Findings by Asset

Q Search

Filters 208 results

Export

Saved Filters

Name	Impo rtan...	IP Address	Serial Number	Security Adviso...	Security Harde...	Configu ration...	Field Notice...	S ⓘ u	
Device A	Low	10.10.1.100	1000000000	5	11	32	1	Signature	
Device A	Low	10.10.1.100	1000000000	5	11	32	1	Signature	
Device A	Low	10.10.1.100	1000000000	5	11	32	1	Signature	
Device A	Low	10.10.1.100	1000000000	5	11	32	1	Signature	
Device A	Low	10.10.1.100	1000000000	5	11	32	1	Signature	

按资产列出的结果

按资产搜索和筛选查找结果的视图

可以通过从下拉列表中选择一个过滤器或点击Filters并从可用过滤器列表选择一个选项来过滤列表视图。您还可以在Search（搜索）字段中按资产搜索结果。

 注意：

- 根据屏幕缩放设置，某些过滤器可能会隐藏。
- 根据您的角色和权限，可使用不同的过滤器。

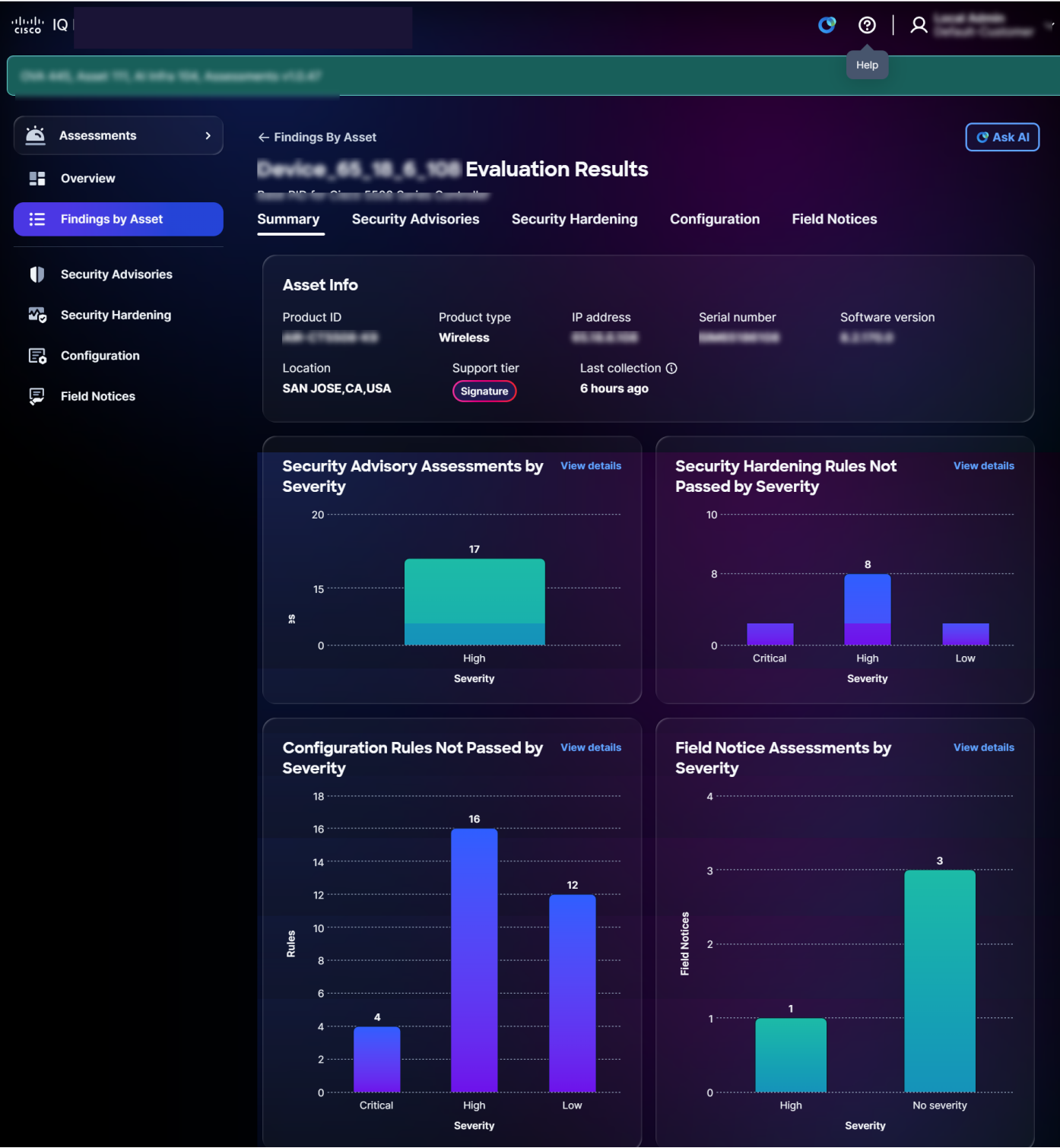
按资产导出结果

要导出“按资产列出的查找结果”列表视图，请单击导出。有关详细信息，请参阅[导出信息](#)。

按资产详细信息查看结果

要按资产详细信息查看结果，请点击资产。以下选项卡显示所选资产的详细信息：

- 摘要:提供详细的资产信息，包括安全建议、安全强化、配置和现场通知的数量
- 安全性建议:提供相关安全建议评估的列表
- 安全强化:提供不符合安全强化规则的资产的列表
- 配置:提供未通过配置最佳实践规则的资产的列表
- 现场通知:提供相关的Field Notice评估列表



按资产详细信息列出的结果

在磁贴上单击View Details时，页面重定向到模块中的相关页面。

单击查看全部资产详细信息时，系统将显示资产详细信息视图页面。

Security Advisories

安全咨询评估可识别漏洞，并根据其风险、严重性和重要性确定漏洞优先级，从而增强组织的风险管理能力。安全建议可提供关于漏洞的精细见解，帮助加快关键威胁的缓解，并确保与合规性和业务目标保持一致。这可以增强安全状态、优化资源分配，并增强恢复能力，以应对整个企业中不断演变的威胁。安全建议发布后，即会在思科IQ中自动更新。

Security Advisories页提供组织内检测到的具有漏洞的所有安全咨询的列表。单击“安全建议评估”(Security Advisory Assessments)列表中的建议会导航到相应的详细视图。

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

Search

Filters98 results

Export

Saved Filters

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

Security Advisories

搜索和过滤安全建议视图

您可以通过从下拉列表中选择过滤器来过滤列表视图。您也可以通过在Search字段中输入评估名称来搜索安全建议评估。

 注意：根据屏幕缩放设置，某些过滤器可能会隐藏。根据屏幕缩放设置，某些过滤器可能会隐藏。根据您的角色和权限，可使用不同的过滤器。缺少的严重性值显示为“—”，带有描述性工具提示。

导出安全建议

要导出安全建议评估，请点击导出。有关详细信息，请参阅[导出信息](#)。

查看安全建议评估详细信息

单击Assessment以查看有关它的其他详细信息。详细信息页面提供常见漏洞评分系统(CVSS)得分、常见漏洞和风险(CVE)、严重性等信息，以及指向参考思科安全顾问的链接。

您可以在“测评结果”(Assessment outcome)表格中查看以下类型的结果：

- 影响:表示该资产或组件具有已被确认的漏洞，可被攻击者利用，需要补救
- 可能受影响的:表示该资产或组件显示可能导致漏洞的迹象，但未得到最终确认；可能还需要进一步调查

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

← Security Advisories

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

About the Assessment

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

Severity	CVE	CVSS score
High		
Version	First published	Last updated
1.1	Sep 25, 2019	Oct 4, 2019

References

[Security Advisory](#)

Asset Results

Q Search

Filters 12 results

Export

Saved Filters

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

安全建议详细信息

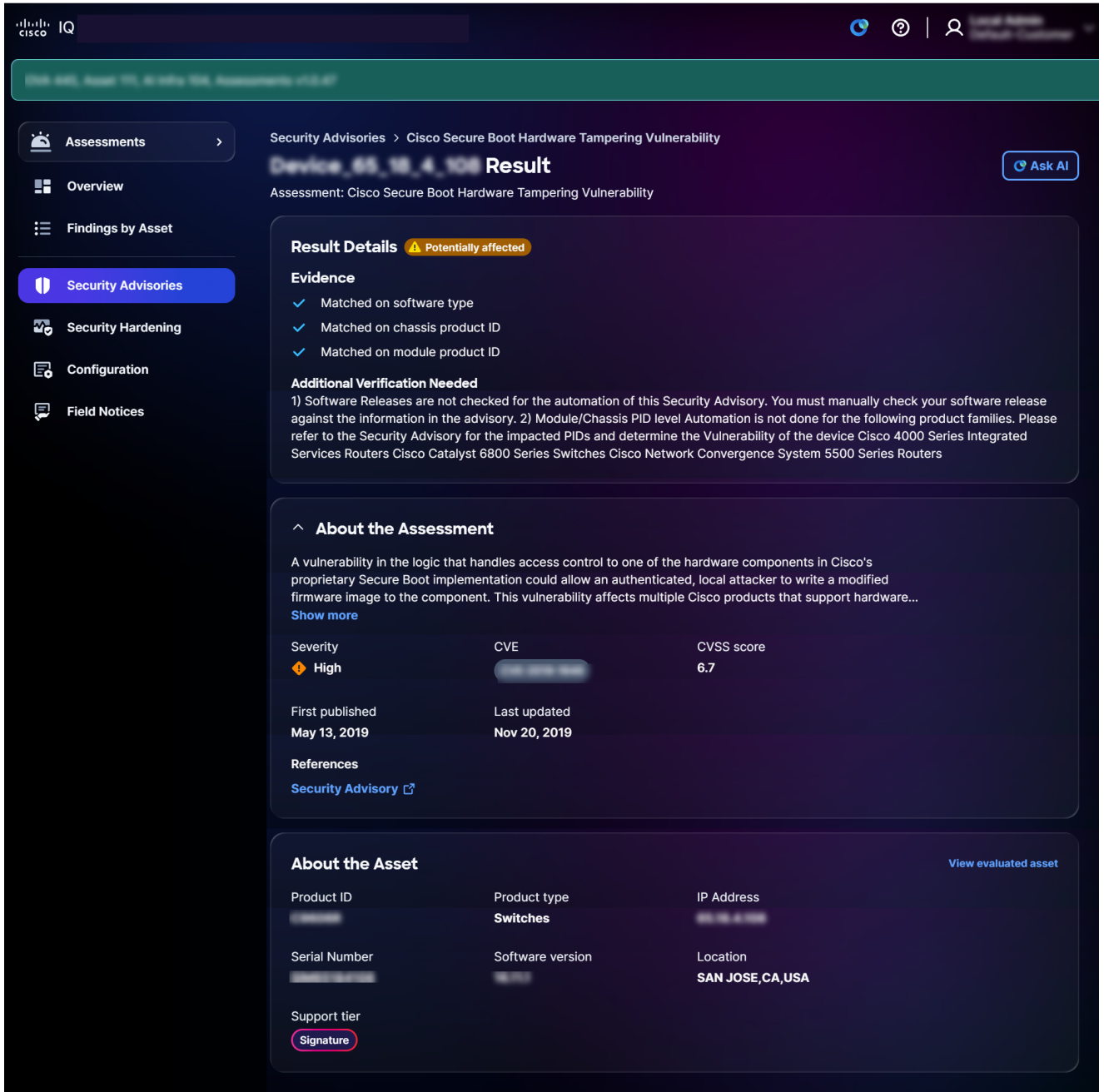
搜索和筛选资产评估结果的视图

可以通过从下拉列表选择一个过滤器或点击Filters并从可用过滤器列表选择一个选项来过滤列表视图。您也可以通过在Search字段中输入资产名称来搜索资产。

 注意：根据屏幕缩放设置，某些过滤器可能会隐藏。根据您的角色和权限，可使用不同的过滤器。

查看资产评估结果

要查看考试结果的详细信息，请单击“考试结果”表中的资产。系统随即会显示资产的评估结果详细信息页面。



The screenshot displays the Cisco IQ interface for a security advisory. The left sidebar contains navigation options: Assessments, Overview, Findings by Asset, Security Advisories (selected), Security Hardening, Configuration, and Field Notices. The main content area shows the 'Result' for the 'Cisco Secure Boot Hardware Tampering Vulnerability' assessment. It includes a 'Result Details' section with a 'Potentially affected' warning, an 'Evidence' section listing matches on software type, chassis product ID, and module product ID, and an 'Additional Verification Needed' section with instructions. Below this is the 'About the Assessment' section, which describes the vulnerability and provides details such as Severity (High), CVE (CVE-2019-11464), CVSS score (6.7), First published (May 13, 2019), and Last updated (Nov 20, 2019). The 'References' section links to the 'Security Advisory'. The 'About the Asset' section provides details for the evaluated asset, including Product ID, Product type (Switches), IP Address, Serial Number, Software version, Location (SAN JOSE, CA, USA), and Support tier (Signature).

Security Advisories > Cisco Secure Boot Hardware Tampering Vulnerability

Device_65_10_4_108 Result [Ask AI](#)

Assessment: Cisco Secure Boot Hardware Tampering Vulnerability

Result Details ⚠ Potentially affected

Evidence

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

Additional Verification Needed

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

About the Assessment

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

[Show more](#)

Severity	CVE	CVSS score
High	CVE-2019-11464	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
6510-4-108	Switches	10.10.10.108
Serial Number	Software version	Location
6510-4-108	10.10.10.108	SAN JOSE, CA, USA
Support tier		
Signature		

结果详细信息

导出安全建议的资产结果

要导出资产结果，请单击导出。有关详细信息，请参阅[导出信息](#)。

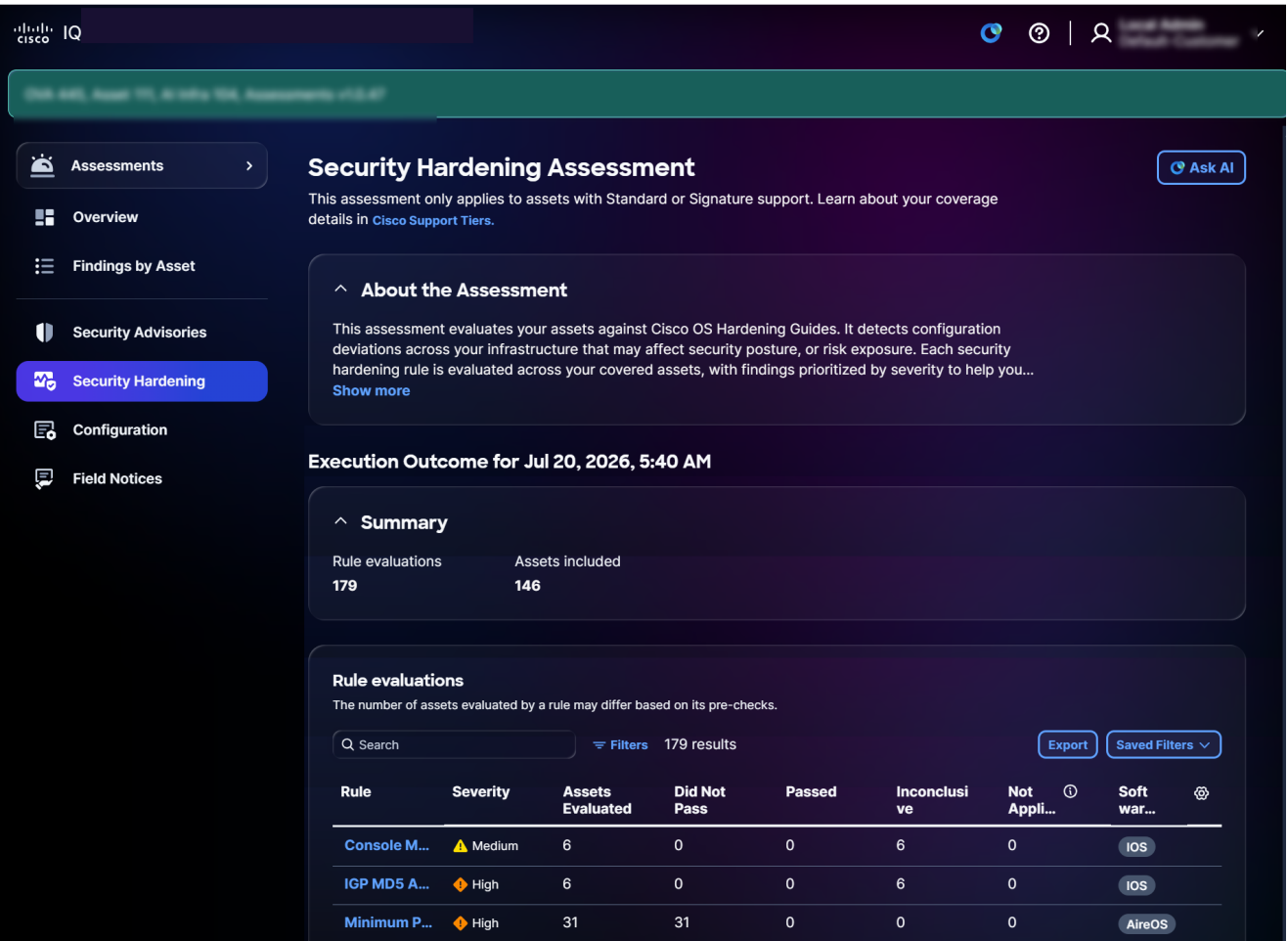
安全强化

安全强化功能可针对行业标准基准持续评估路由器、交换机和防火墙，从而近乎实时地自动了解网络基础设施的安全状态。它可识别配置差距并提供切实可行的补救指导，使客户管理员能够有效地缩小攻击面，并保持与思科严格的安全最佳实践的一致一致。通过集中合规性监控和简化强化流程，该模块将安全管理从被动任务转变为主动的、数据驱动的战略，从而确保恢复力和安全的企业网络。

 注意：安全强化评估仅适用于具有标准支持层的资产。

查看安全强化评估

安全强化评估页面显示以下信息：



Security Hardening Assessment

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

About the Assessment

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

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

Summary

Rule evaluations	Assets included
179	146

Rule evaluations

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

Search: Filters: 179 results [Export](#) [Saved Filters](#)

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

安全强化

- 关于评估:通过概述考试目的提供其他详细信息
- 执行结果:提供资产评估结果的摘要，包括规则评估和所包含资产的总数
- 规则评估:提供有关规则的详细信息，包括严重性、评估资产、未通过、通过、无结论、不适用和软件类型

- 严重级别:提供规则评估的重要性或影响级别
- 评估资产:提供根据规则条件评估的资产总数
- 未通过:提供评估期间不符合规则条件的资产
- 通过:提供评估期间符合规则标准的资产
- 无结论:提供评估无法确定故障的资产
- 不能应用:指示规则不适用或不相关的资产或方案
- 软件类型:提供软件资产类型

搜索和过滤规则的视图

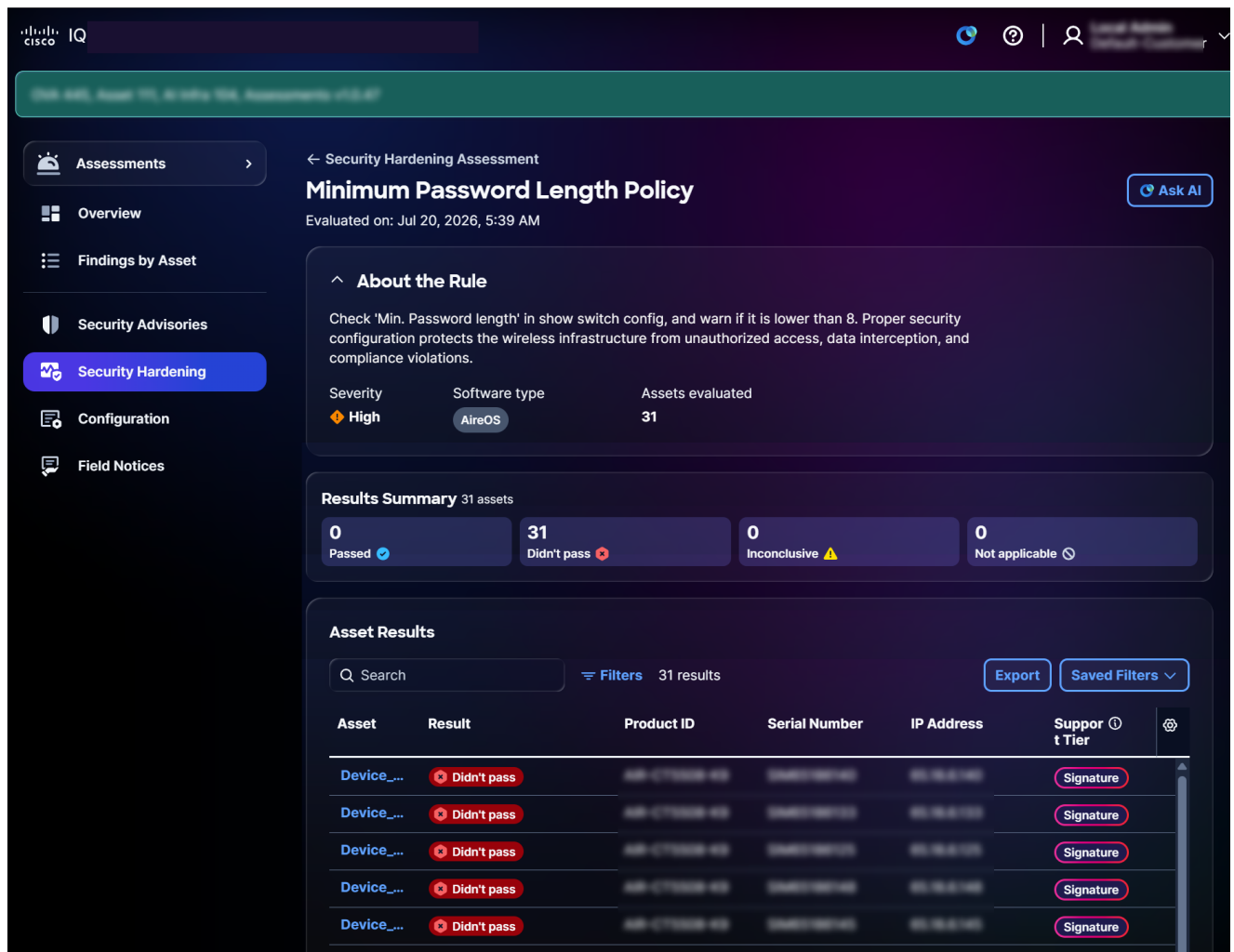
可以通过从下拉列表中选择一个过滤器或点击Filters并从可用过滤器列表选择一个选项来过滤列表视图。您也可以通过在Search字段中输入规则名称来搜索规则。



注意：根据屏幕缩放设置，某些过滤器可能会隐藏。根据您的角色和权限，可使用不同的过滤器。

查看规则评估详细信息

要查看有关规则评估的其他详细信息，请点击规则。系统随即会显示规则的评估详细信息页面，其中包含以下信息：



规则视图

- 关于规则:提供有关规则的详细信息，例如Severity、Software type、Version和Assets evaluated，并包含指向相关源文档的描述性标记链接
- 结果摘要:提供与规则相关的资产结果摘要，例如Passed、Not pass、Inconsistinal和Not applicable
- 资产业绩:提供资产列表，其中包含资产、结果、产品ID、序列号、IP地址和支持层等详细信息

 **注意：**思科IQ可在评估结果“无结论”时提供明确的指导，解释原因（例如，缺少遥测或不支持操作系统），并建议验证数据收集、更新凭证或刷新数据等步骤。此外，还提供了贴有标签的相关文档链接，以帮助解决问题。

搜索和筛选资产规则的视图

可以通过从下拉列表选择一个过滤器或点击Filters并从可用过滤器列表选择一个选项来过滤列表视图。您也可以通过在Search字段中输入资产名称来搜索资产评估结果。

 注意：根据屏幕缩放设置，某些过滤器可能会隐藏。根据您的角色和权限，可使用不同的过滤器。

导出资产结果

要导出规则的评估结果，请单击导出。有关详细信息，请参阅[导出信息](#)。

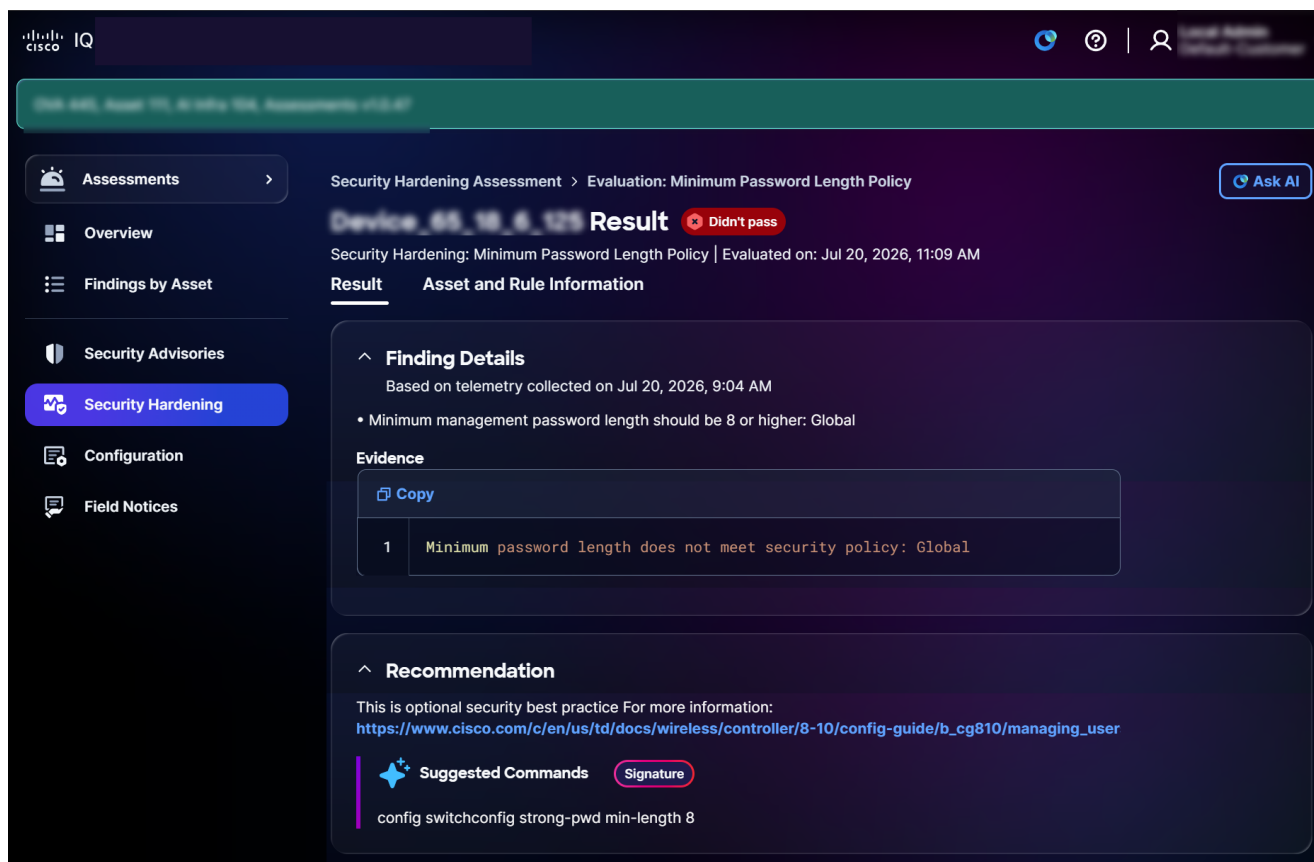
搜索和筛选资源结果视图

可以通过从下拉列表中选择一个过滤器或点击Filters并从可用过滤器列表选择一个选项来过滤列表视图。您也可以通过在Search字段中输入资产名称来搜索资产结果。

 注意：根据屏幕缩放设置，某些过滤器可能会隐藏。根据您的角色和权限，可使用不同的过滤器。

查看安全加固的资产结果

单击Asset Results中的资产可查看其详细信息。资产的结果详细信息页面根据您的权限级别或层显示信息。



The screenshot displays the Cisco IQ interface for a Security Hardening Assessment. The left sidebar contains navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening (selected), Configuration, and Field Notices. The main content area shows the 'Security Hardening Assessment > Evaluation: Minimum Password Length Policy' results. A 'Result' badge indicates 'Didn't pass'. The finding details state: 'Based on telemetry collected on Jul 20, 2026, 9:04 AM' and 'Minimum management password length should be 8 or higher: Global'. The evidence section shows a single finding: '1 Minimum password length does not meet security policy: Global'. The recommendation section provides a link to Cisco documentation and suggests the command 'config switchconfig strong-pwd min-length 8'.

安全强化标准层

- 标准层

- 查找详细信息:提供评估期间确定的配置偏差信息以及证据日志
- 建议:提供指导以解决发现问题并确保配置一致性

查看资产和规则信息以进行安全强化

要查看资产及其规则的详细信息，请点击Asset and Rule Info选项卡。系统随即会显示Asset and Rule Info页面。

关于资产:提供资产的详细信息，例如产品ID、产品类型、IP地址、序列号、软件版本、位置和支持层

- 关于规则:提供规则详细信息(包括Severity和Software type)以及特定强化检查的重要性

配置

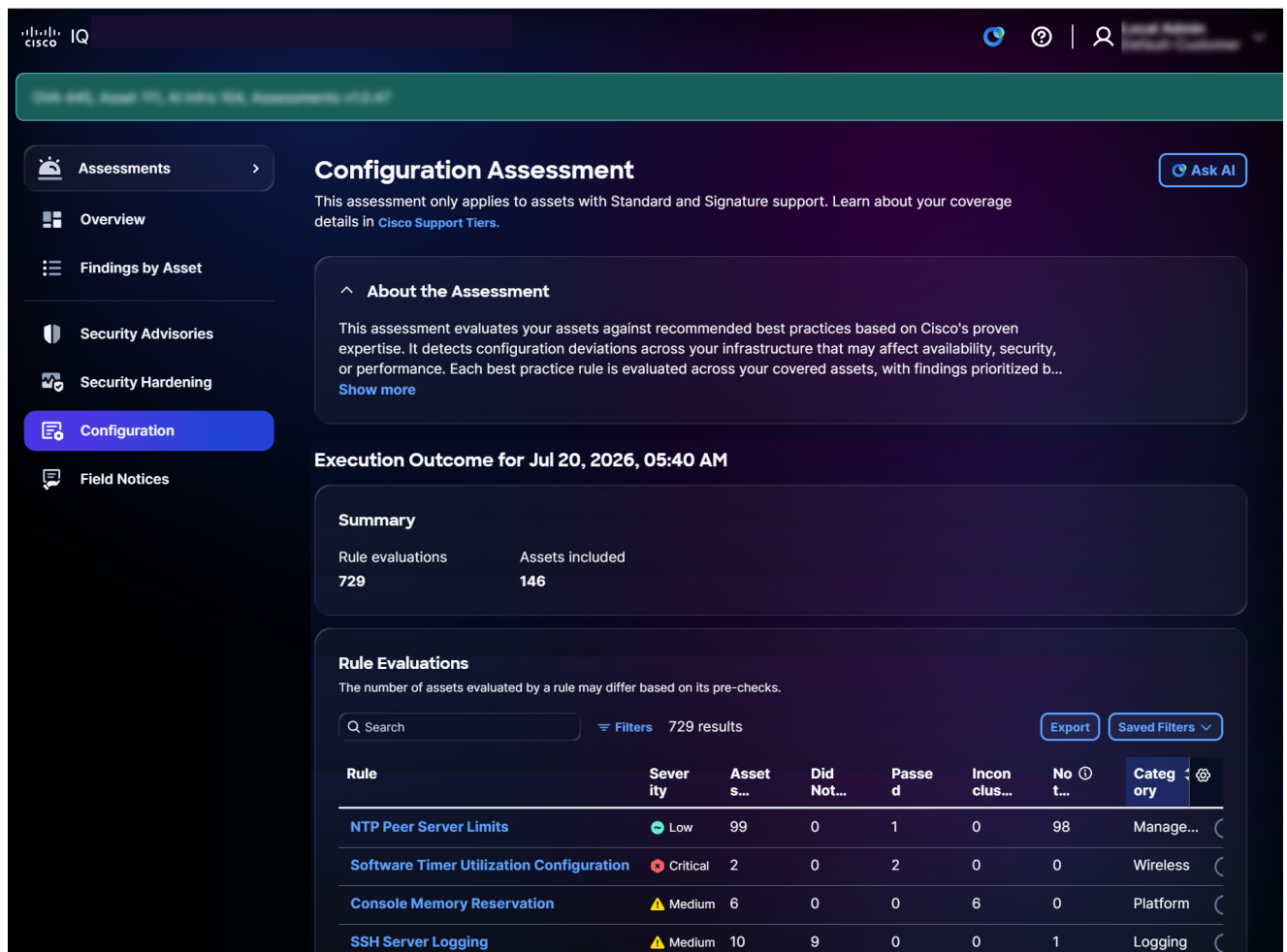
配置评估根据思科久经考验的专业知识，按照建议的最佳实践来评估您的资产，以检测可能会影响整个基础设施的可用性、安全性或性能的配置偏差。每个最佳实践规则都会在您覆盖的资产中进行评估，并将结果按照严重性进行优先级排序，以确保配置一致性、增强可复原性并降低运营风险。



注意：配置评估仅适用于具有标准支持层的资产。

查看配置评估

Configuration Assessment页面显示以下信息：

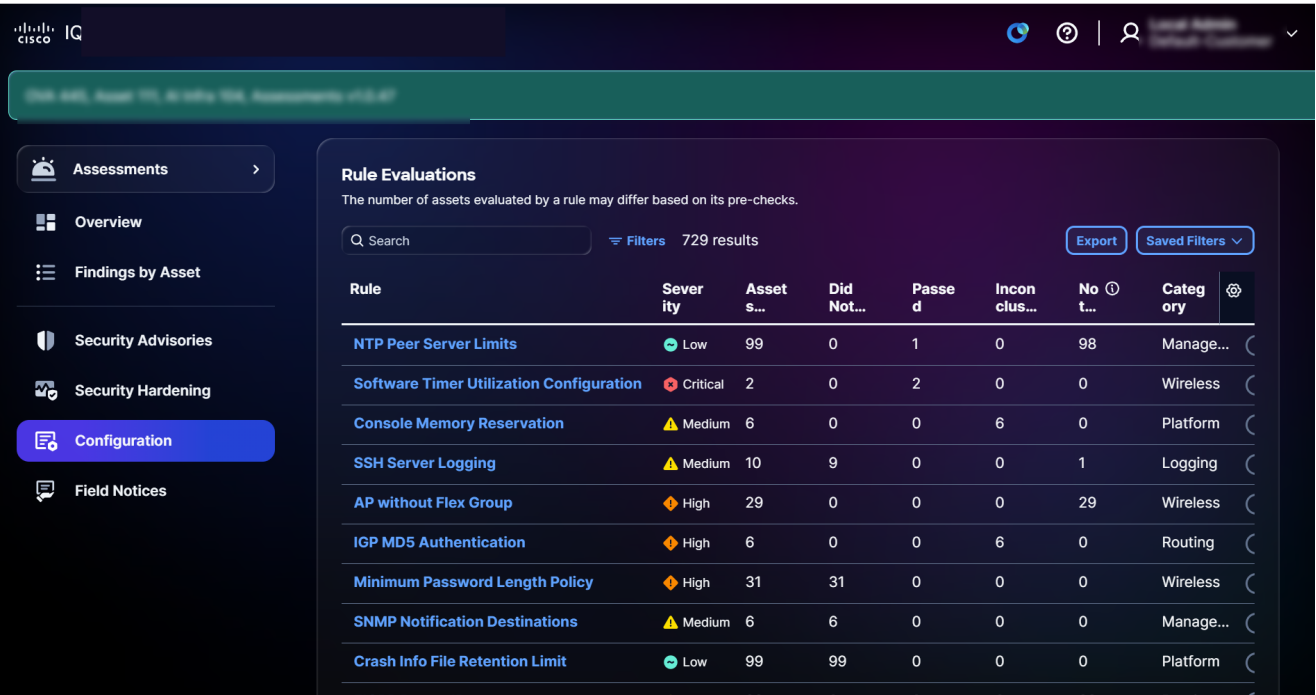


配置评估

- 关于评估:通过概述考试目的提供其他详细信息
- 摘要:提供配置执行摘要，例如Rules evaluated和Assets evaluated
- Insights:深入了解通过模式分析和发现结果关联产生的已识别配置差距；它们以智能分组密钥卡的形式显示，以突出显示需要注意的最关键领域
- 规则评估:提供有关规则的详细信息，包括严重性、评估资产、未通过、通过、不确定、不适用、Category和软件类型
- 严重级别:提供规则评估的重要性或影响级别
- 评估资产:提供根据规则条件评估的资产总数
- 未通过:提供评估期间不符合规则条件的资产总数
- 无结论:提供无法运行评估的资产总数
- 通过:提供评估期间符合规则标准的资产
- 不能应用:指示规则不适用或不相关的资产或方案
- 分类:提供规则所属的域区域

- 软件类型：指示应用规则的软件资产的类型

搜索和过滤规则的视图



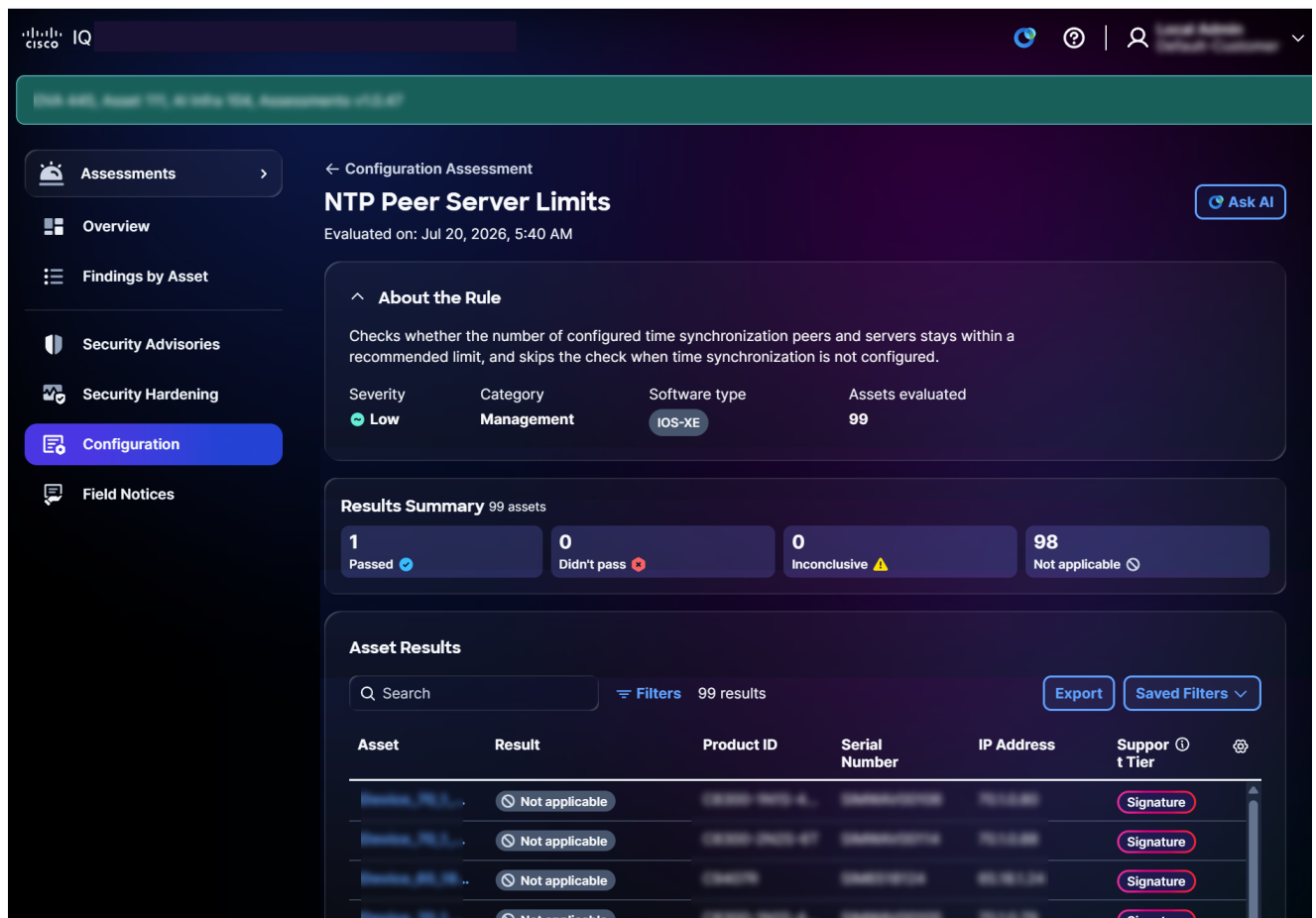
规则评估

可以通过从下拉列表中选择过滤器或点击Filters并从可用过滤器列表中选择一项来过滤列表视图。您也可以通过在Search字段中输入规则名称来搜索规则。

 注意：根据屏幕缩放设置，某些过滤器可能会隐藏。根据您的角色和权限，可使用不同的过滤器。

查看规则评估详细信息

要查看有关规则评估的其他详细信息，请点击任意规则。系统随即会显示规则的评估详细信息页面，其中包含以下信息：



评估

- 关于规则:提供有关Severity、Category、Software type和Assets evaluated等规则的详细信息，并包含指向相关源文档的描述性标记链接
- 结果摘要:通过显示通过、未通过、不确定和不适用状态的资产数，提供总体资产结果
- 资产结果:提供受所选规则影响的资产列表以及结果状态

 注意：思科IQ可在评估结果“无结论”时提供明确的指导，解释原因（例如，缺少遥测或不支持操作系统），并建议验证数据收集、更新凭证或刷新数据等步骤。此外，还提供了贴有标签的相关文档链接，以帮助解决问题。评估模块支持规则的多类别选择，支持同时处理多个规则类别并进行评估。

导出资产结果

要导出规则的资产结果，请单击导出。有关详细信息，请参阅[导出信息](#)。

搜索和筛选资源结果视图

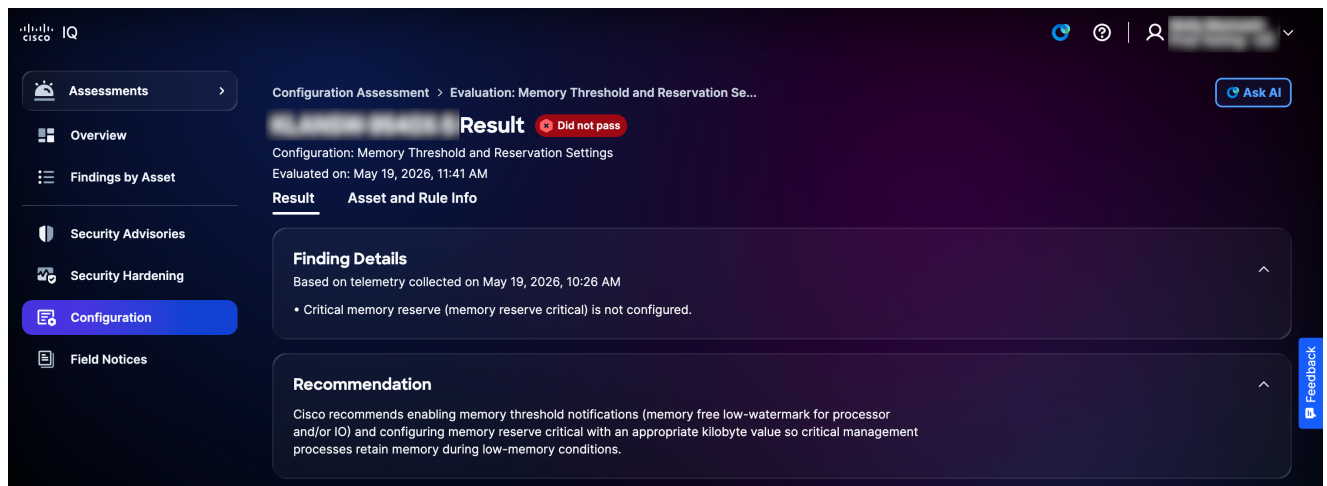
可以通过从下拉列表选择一个过滤器或点击Filters并从可用过滤器列表选择一个选项来过滤列表视图。您也可以通过在Search字段中输入资产名称来搜索资产结果。

 注意：根据屏幕缩放设置，某些过滤器可能会隐藏。根据您的角色和权限，可使用不同的过滤器。

查看配置评估的资产结果

要查看资产结果的详细信息，请点击资产结果中的资产。

资产的结果详细信息页面根据您的权限级别或层显示信息。

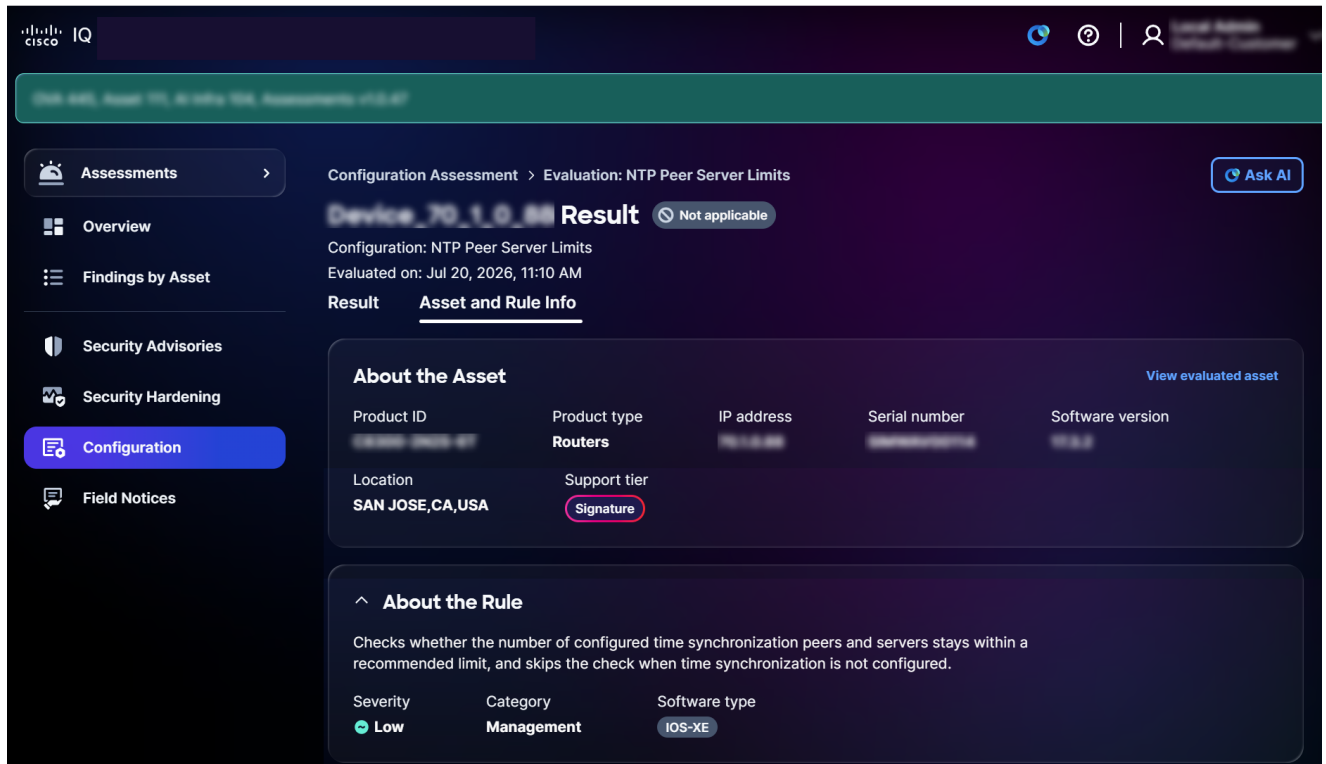


配置标准层

- 标准层
- 查找详细信息:提供评估期间确定的配置偏差信息以及证据日志
- 建议:提供指导以解决发现问题并确保配置一致性

查看配置评估的资产和规则信息

要查看资产和规则信息详细信息，请点击资产和规则信息选项卡。



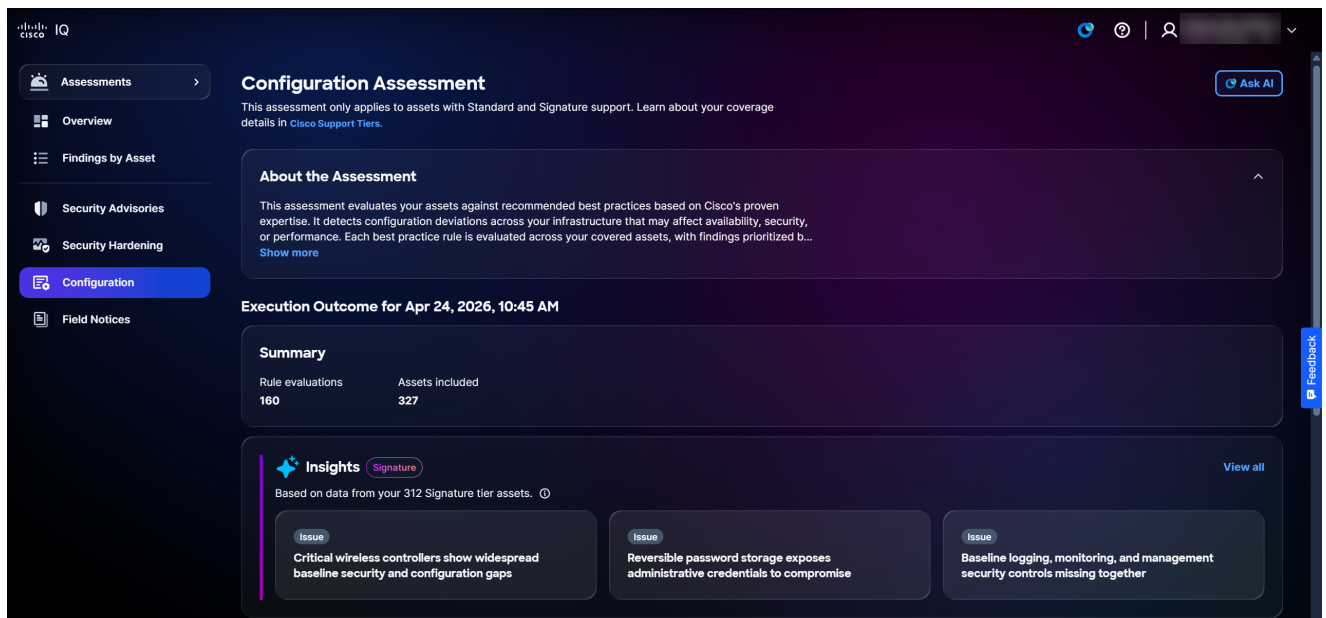
资产和规则信息

系统随即会显示Asset and Rule Info页面，其中包含以下信息：

- 关于资产:提供资产的详细信息，如产品ID、产品类型、IP地址、序列号、软件版本、位置和支持层
- 关于规则:提供规则的详细信息，例如Severity、Category和Software类型

查看见解

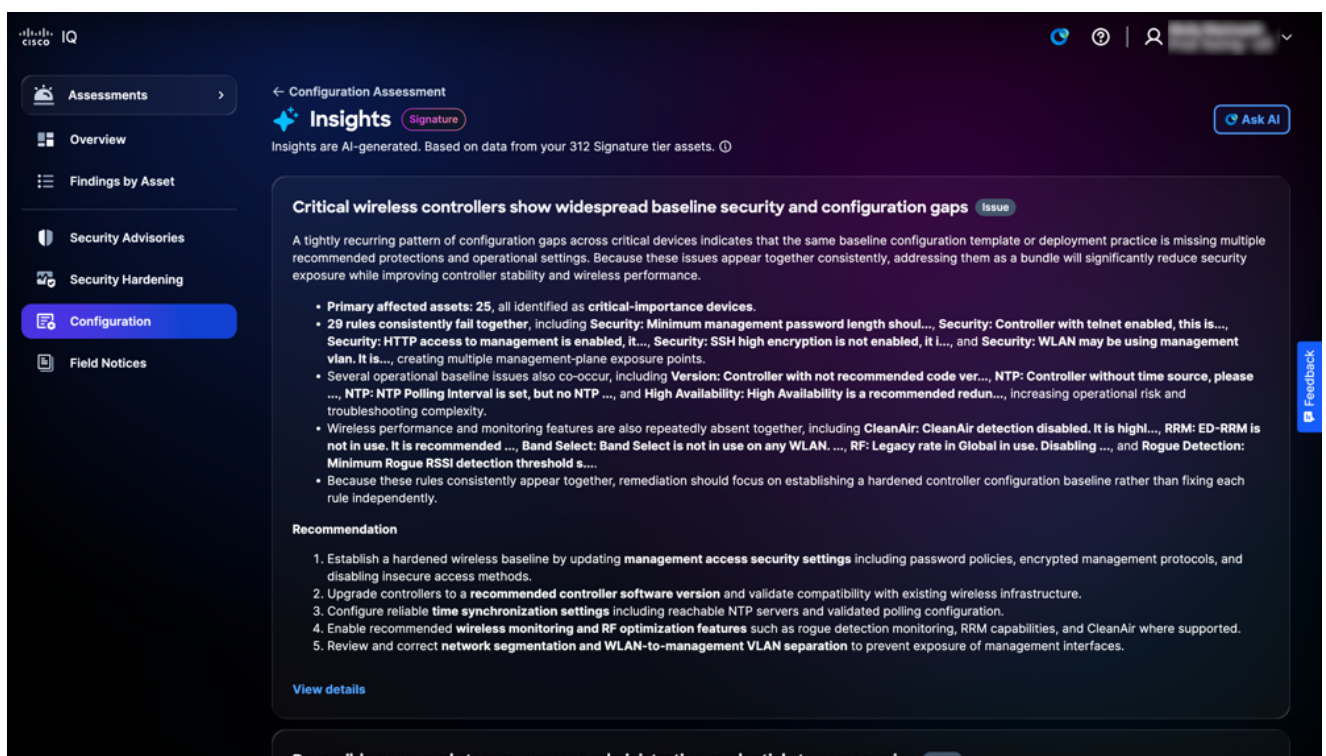
见解由AI生成，可用作智能仪表板，将评估数据综合到按优先顺序排列的关键卡中，突出显示多个调查结果之间的关键配置差异。它让您能够专注于这些紧急领域，从而有效地应对影响最大的基础设施风险。它还根据最佳实践确定您的基础设施正在执行的领域，从而突出优势。



Insights

要查看见解详细信息，请执行以下操作：

1. 在“见解”面板中，单击查看全部。Insights页面显示所有见解。



Insights页面

2. 单击View details或单击任意卡。系统随即会显示“Insights”详细信息页面，其中包含以下信息：

Configuration Assessment > Insights

Critical wireless controllers show widespread baseline security and configuration gaps

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

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

Details **Source Findings**

Insight

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

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

Recommendation

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

Affected Assets

Q Search Product type Product family Product ID [Filters](#) 25 results [Export](#)

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

见解详情

- **见解:**提供摘要，重点介绍通过跨多个调查结果的分析确定的重复出现的配置偏差模式，以及您的基础设施中与最佳实践一致的卓越领域
- **建议:**提供可操作的步骤，以修复已确定的配置差距
- **受影响的资产：**提供已按照Insight部分中的定义标识配置偏差的特定设备的列表

3. 单击Source Findings。Source Findings页面显示支持您的见解的具体查找结果。

Configuration Assessment > Insights

Critical wireless controllers show widespread baseline security and configuration gaps

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

Details Source Findings

Search: [] Severity: [] Result: [] 725 results [Export]

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

源结果

您可以通过从Severity和Result下拉列表中选择过滤器来过滤表视图。

注意：建议和受影响资产是可选的，具体取决于每项见解输出。

Field Notices

现场通知可确定与安全无关的重大产品问题，并根据其影响的严重性和重要性对其进行组织，从而提高组织管理产品风险的能力。现场通知提供对产品缺陷的可行性见解，通过推荐的升级或变通方法加速缓解，并确保与运营和业务目标保持一致。这增强了产品的可靠性，优化了资源分配，并提高了可复原性，以应对企业中不断变化的产品挑战。

Field Notices

Ask AI

About the Assessments

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

Field Notice Assessments

Search: [] Filters 47 results [Export] [Saved Filters]

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

Field Notices

搜索和筛选字段通知视图

您可以通过从下拉列表中选择过滤器来过滤列表视图。您也可以通过在Search字段中输入考试名称来搜索现场通知考试。

查看现场通知的评估

要查看有关现场通知的其他详细信息，请点击评估。系统将显示以下考试详细信息：

- 关于评估:通过概述考试目的提供其他详细信息
- 现场通知评估:显示受所选现场通知影响的资产的列表，包括检测到漏洞的资产

The screenshot shows the Cisco IQ interface for Field Notices. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration, and Field Notices (highlighted). The main content area displays a specific field notice titled "FN74223 - Some Cisco NCS 540 Series Medium Density Routers May Become Unresponsive After Upgrade to Cisco IOS XR Software Release 7.11.1 or Later - Workaround Provided". Below the title, there is an "About the assessment" section with a description, severity (Critical), last updated date (Dec 11, 2024), and a link to the field notice. The "Asset Results" section shows a table with 3 results, filtered by "Potentially affected". The table columns are Asset, Result, Product ID, Serial Number, Product Type, Product Family, and Sup po... (Support point). The table lists three devices, all with a "Potentially affected" result and a "Signature" link.

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

查看现场通知的评估

搜索并筛选字段通知的资产结果视图

可以通过从下拉列表选择一个过滤器或点击Filters并从可用过滤器列表选择一个选项来过滤列表视图。您也可以通过在Search字段中输入资产名称来搜索资产结果。

 **注意：**根据屏幕缩放设置，某些过滤器可能会隐藏。根据您的角色和权限，可使用不同的过滤器。

导出现场通知的资产结果

要导出现场通知的评估资产结果，请单击导出。有关详细信息，请参阅[导出信息](#)。

查看现场通知的资产评估结果

要查看资产的评估结果详细信息，请从“资产评估结果”(Asset Assessment Results)中点击资产。系统随即会显示资产的评估结果详细信息页面。

您可以查看以下类型的结果：

- 影响:表示符合现场通知自动检查的所有条件且无需其他手动验证即可确认受影响的资产
- 可能受影响的:表示符合现场通知的所有自动检查条件，但需要额外手动验证以确认其是否真正受到影响的资产

Assessments - Security Hardening选项卡下提供以下提示：

- 思科针对网络设备的安全强化最佳实践是什么？
- 如何强化Cisco IOS XE设备？
- 列出路由器和交换机的关键安全强化步骤。
- 思科设备的建议基线强化设置是什么？
- 有多少资产违反了安全强化最佳实践？

本地 认证

帐户管理员应使用以下凭证成功登录到VA:

- 默认用户名：admin
- 默认密码：在VA安装过程中设置的密码；有关详细信息，请参阅入门指南
- 默认帐户上下文:默认客户

登录后，默认用户“admin”和帐户名称“Default-Customer”将显示在主页上。

设置本地管理员安全

您可以通过主页中的User Profile菜单更改密码并设置安全问题。

锁定设置

以下帐户锁定设置可在部署期间配置：

- 锁定状态：启用或禁用帐户锁定功能。

- Maximum Login Attempts：设置帐户锁定前允许的最大连续失败尝试次数(默认值：3;范围：0–10)。
- 滚动时间窗口：定义跟踪失败尝试的时间段(默认值：15分钟；范围：0-60分钟)。
- Duration：设置达到最大尝试次数后帐户保持锁定状态的持续时间(默认值：30分钟；范围：0-60分钟)。

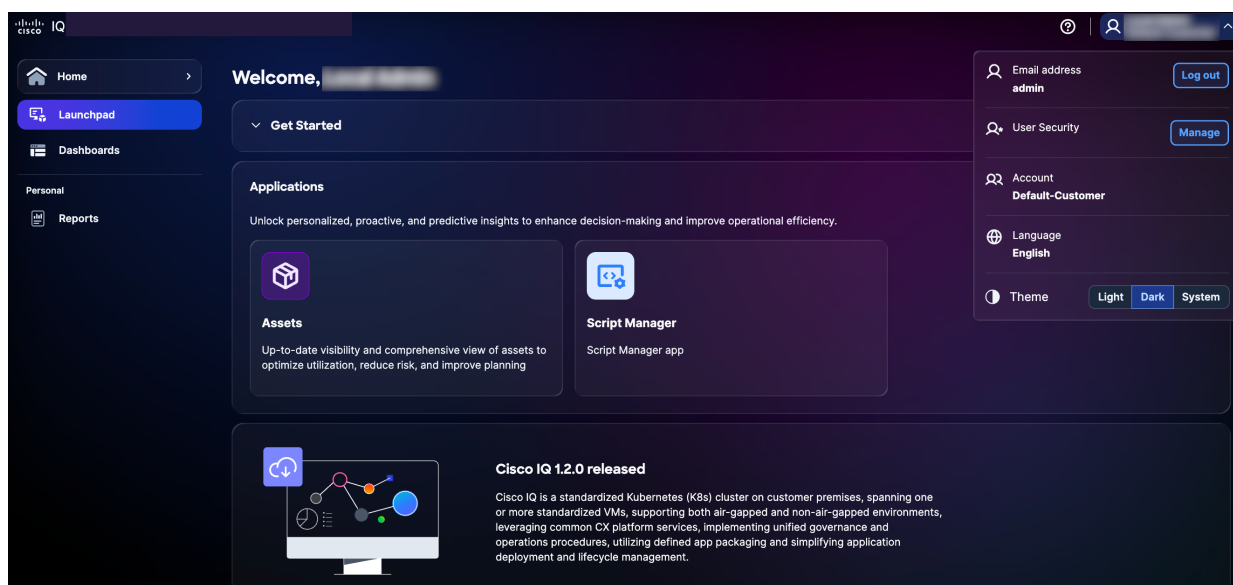
 注意：在15分钟内，您有三(3)次尝试输入正确的密码。如果所有三(3)次尝试均失败，您的帐户将临时锁定30分钟以保护您的安全。在锁定期间无法尝试登录。系统将显示以下消息：“由于尝试失败次数过多，帐户被锁定。请稍后重试。”，包括锁定到期的时间。您的帐户会在30分钟后自动解锁，此时您可能会尝试登录或重置密码。

设置安全问答

如果您忘记了密码，安全问题有助于验证您的身份。帐户管理员必须设置五(5)个安全问题的答案才能启用密码重置功能。这是一次性设置。

要设置安全问题，请执行以下操作：

1. 在Home页中，单击User Profile图标。将打开下拉菜单。



使用安全性

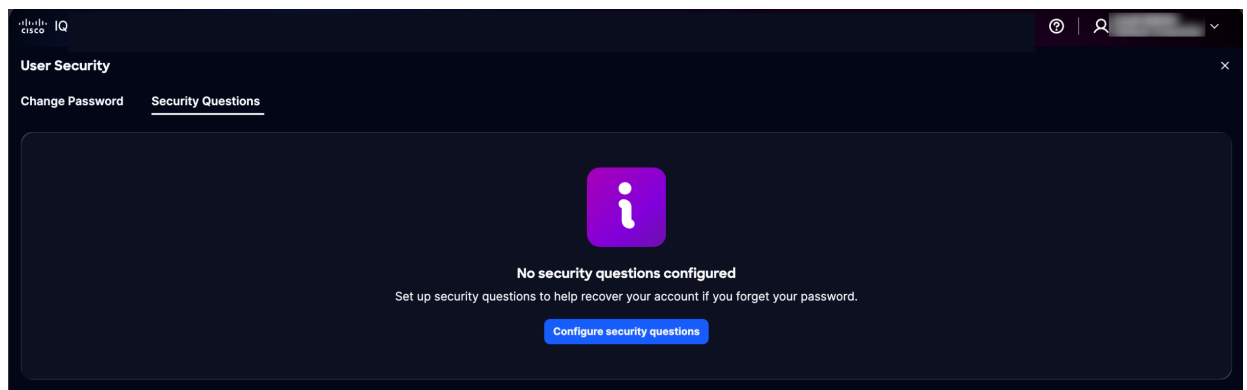
2. 点击Manage in User security. 系统随即会显示User Security页面。



The screenshot shows the 'User Security' interface in Cisco IQ. The 'Change Password' tab is selected. It lists password requirements: at least 15 characters, at least 2 uppercase characters, at least 2 lowercase characters, at least 2 numeric characters, at least 2 special characters, and no repeating characters. There are input fields for 'Password', 'New password', and 'Confirm password', each with a 'Show' button. A 'Save' button is at the bottom.

安全问题

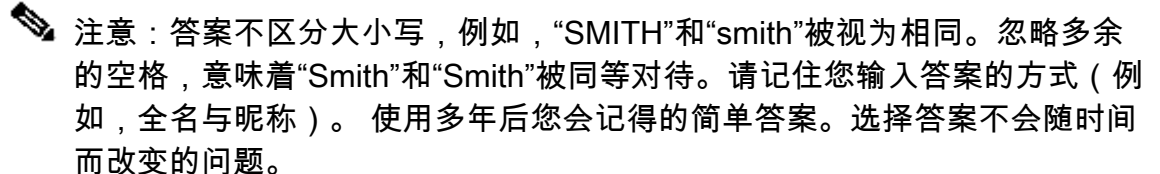
3. 单击Security Questions以打开选项卡。



The screenshot shows the 'User Security' interface in Cisco IQ with the 'Security Questions' tab selected. It displays a message: 'No security questions configured. Set up security questions to help recover your account if you forget your password.' Below the message is a 'Configure security questions' button.

“安全问题”选项卡

4. 单击配置安全问题。





注意：如果需要，您可以稍后更新您的答案。当您更新答案时，以前的所有答案都将被替换，因此您必须再次提供所有五(5)个问题的答案，而不仅仅是您要更改的问题。

管理密码

帐户管理员和本地用户可以管理Cisco IQ的密码。

为了确保您的帐户安全，将实施以下密码策略：

- 。重新使用限制：您的新密码不能与之前五(5)个密码中的任何一个匹配。此策略适用于“注册”、“忘记密码”和“更改密码”流程。
- 。字符变体：在验证时更改密码时，新密码中至少必须存在八(8)个与当前密码不同的字符。
- 。最小更改间隔：默认情况下，必须等待24小时才能再次更改密码。如果配置了不同的时间间隔，在该时间过去之前，您将无法更新密码。
- 。密码过期：密码每60天过期一次。在到期日期后首次登录时，您需要设置新密码才能访问系统（如果配置为0，则密码到期将被禁用）。

先决条件

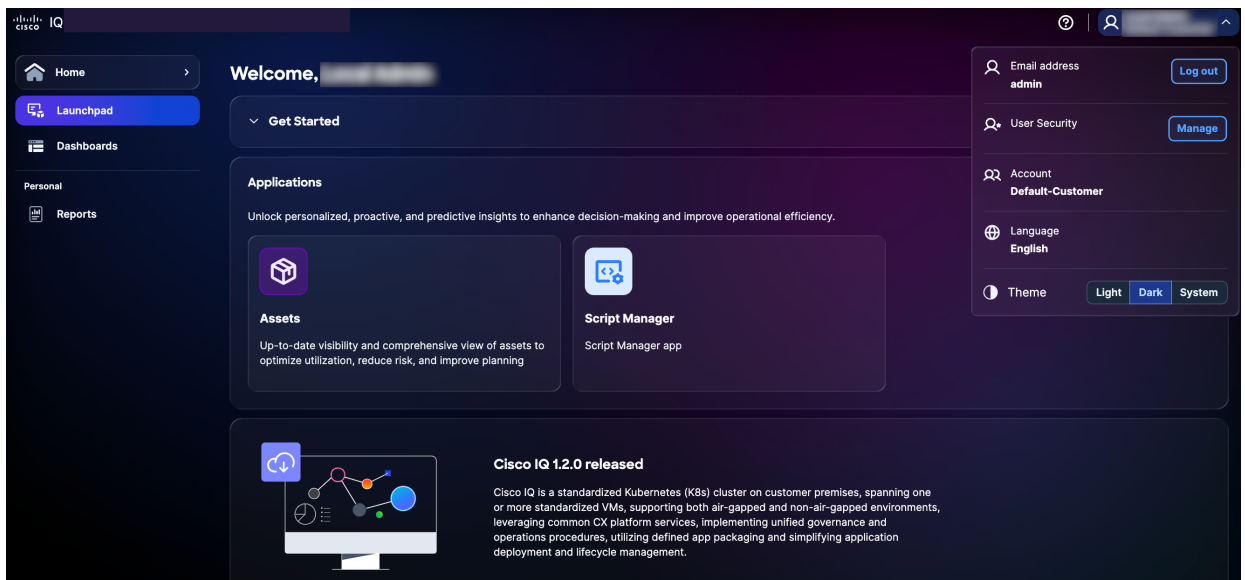
要管理密码，必须满足以下条件：

- 。您是本地帐户管理员或用户
- 。您使用的是本地帐户(不是单点登录(SSO)或外部身份验证)
- 。您已登录到Cisco IQ
- 。您知道当前密码

更改密码

要更改密码，请执行以下操作：

1. 在主页中，点击您的用户简档图标。此时将打开下拉菜单。



管理用户安全

2. 点击Manage in User security。系统随即会显示User Security页面。



更改密码

3. 输入当前的密码。
4. 输入新密码。
5. 再次输入新密码进行确认。
6. Click Save.

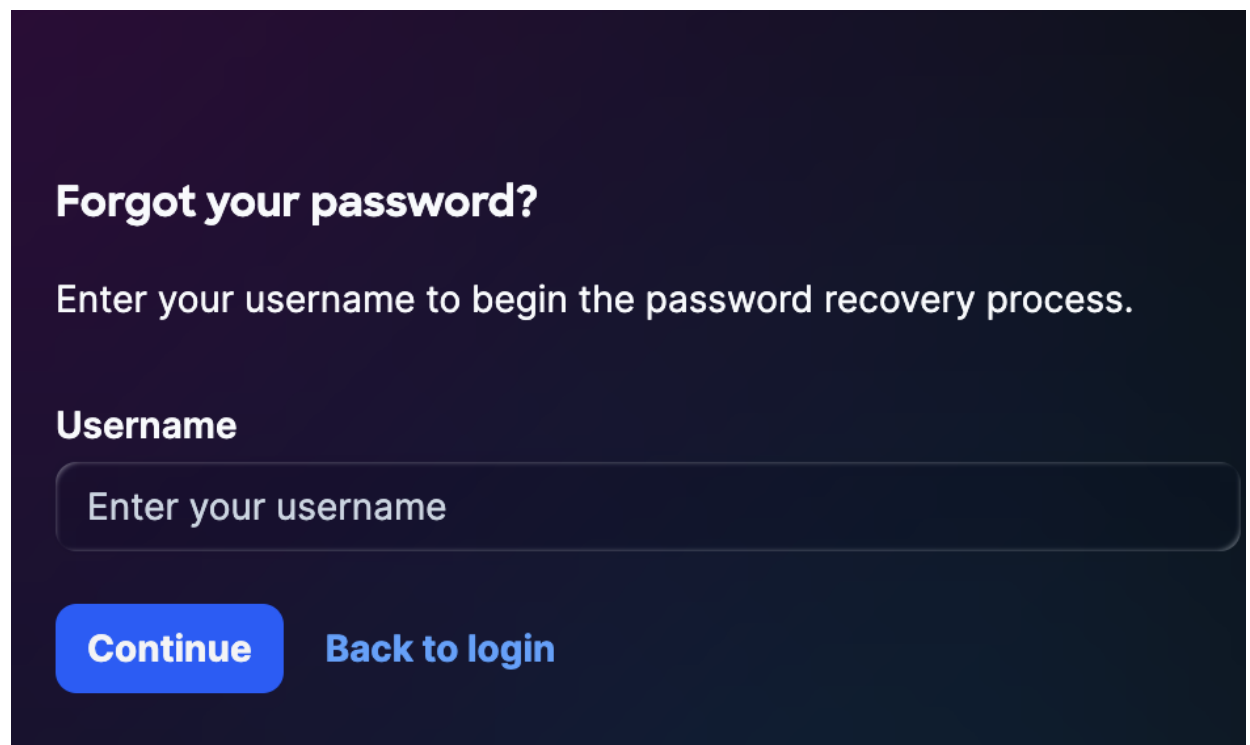
密码在Cisco IQ系统 (包括Cisco IQ VM) 中更新。

重置忘记的密码

您可以使用安全问题验证过程重置密码。

要重置忘记的密码，请执行以下操作：

1. 导航至Cisco IQ VA登录页面。
2. 单击忘记密码。



Forgot your password?

Enter your username to begin the password recovery process.

Username

Continue **Back to login**

忘记了密码

3. 输入用户名。
4. 单击 Continue。Verify Identity页显示先前配置的五(5)个问题中的三(3)个随机安全问题。

Verify Identity

Answer the following security questions to verify your identity.

What city were you born in?

[Show](#)

What is your mother's maiden name?

[Show](#)

What was the name of your elementary school?

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

验证身份

5. 输入所有三(3)个显示问题的回答。
6. 单击验证并继续。如果提交的响应与之前保存的响应匹配，系统会提示您输入新密码。

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

重置密码

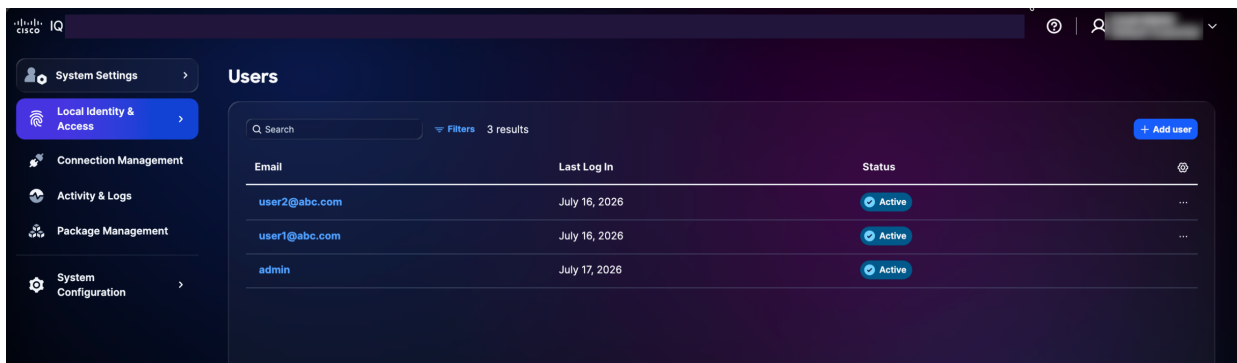
 注意：在15分钟内，您有三(3)次尝试输入正确的密码。如果所有三(3)次尝试均失败，您的帐户将临时锁定30分钟以保护您的安全。在锁定期间无法尝试登录。系统将显示以下消息：“由于尝试失败次数过多，帐户被锁定。请稍后重试。”，包括锁定到期的时间。您的帐户会在30分钟后自动解锁，此时您可能会尝试登录或重置密码。

7. 输入新密码.
8. 再次输入密码进行确认。
9. 单击 submit。

添加本地用户

帐户管理员可以将用户添加到Cisco IQ帐户。添加新用户的步骤：

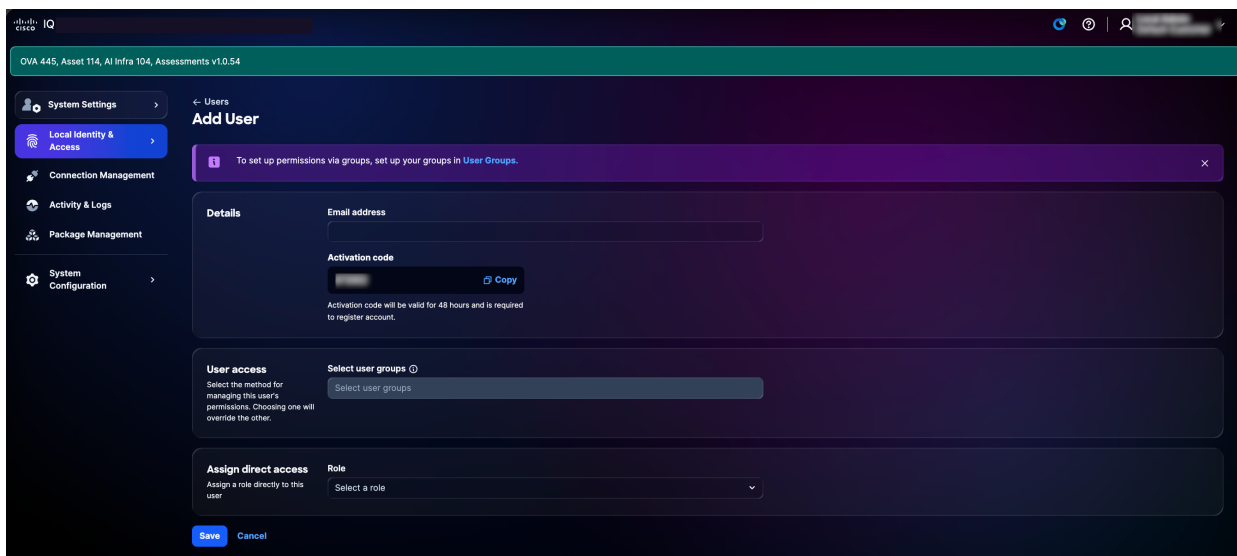
1. 导航到系统设置 > 本地身份和访问 > 用户。系统随即会显示Users页面。它列出所有现有本地用户及其状态。



“用户”页

 注意：请勿在不安全的通道上共享激活代码。如果代码丢失或受损，请使用菜单图标重新生成新的激活代码，使上一个激活代码失效。激活码的有效期为48小时。如果您的代码过期，请与您的帐户管理员联系以申请新的代码。

- 单击Add users。系统将显示Add User页面。



添加用户

3. 输入电子邮件地址。
4. 输入激活代码。

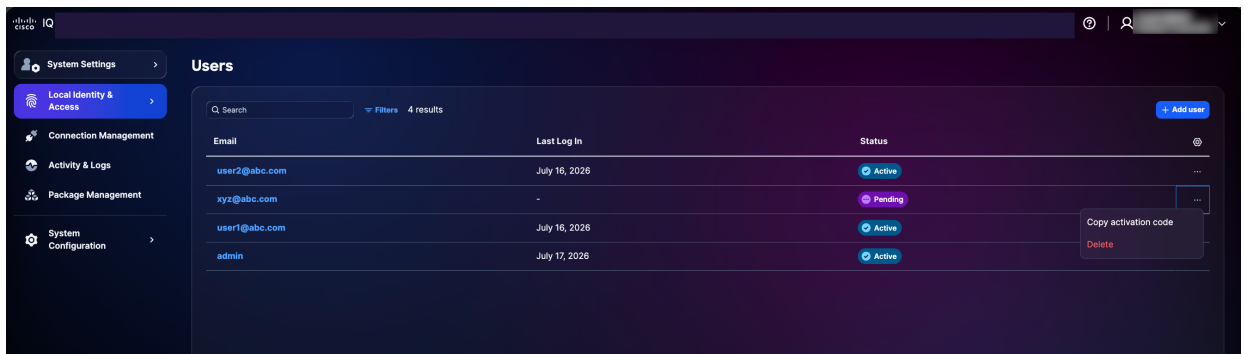
 注意：默认情况下显示激活代码。与用户共享显示的激活代码，因为注册时需要该代码。

5. 在User access中，从Select user groups下拉列表中选择用户组。

 注意：用户从所选组继承访问权限。

6. 在分配直接访问中，从角色下拉列表中选择角色。有两(2)个可用角色：

- 查看器:查看和访问应用程序
 - 帐户管理员:访问模块并管理系统设置，系统管理和身份提供程序(IDP)除外
7. Click Save.系统随即会创建新用户，并将其以待处理状态显示在用户列表中。“待定”表示用户尚未完成自激活。
 8. 在列表中找到新创建的用户，并确认Status列显示Pending。
 9. 点击新创建的用户旁边的More Options图标。



复制激活代码

10. 从下拉列表中选择Copy activation code。激活代码会复制到您的剪贴板。
11. 安全地与用户共享此代码（例如，通过安全的内部渠道）。激活码仅供一次性使用，需要该激活码才能完成注册。

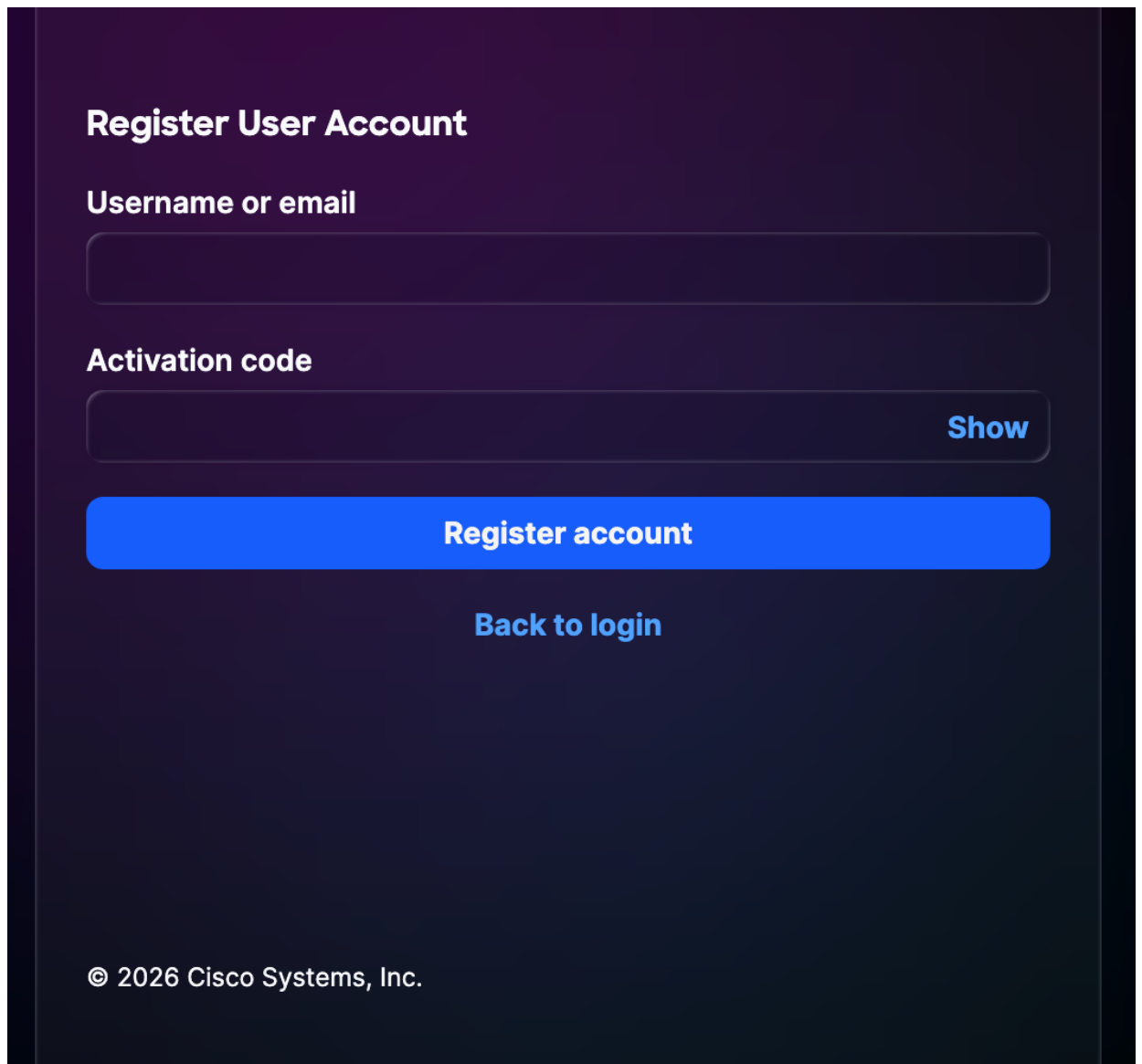
 **注意：**请勿在不安全的通道上共享激活代码。如果代码丢失或受损，请使用菜单图标重新生成新的激活代码，使上一个激活代码失效。激活码的有效期为48小时。如果您的代码过期，请与您的帐户管理员联系以申请新的代码。

12. 要注销，请点击右上角的User Profile图标，然后选择Logout。您将返回到Cisco IQ登录页面。

注册新用户帐户

要注册新用户帐户，请执行以下操作：

1. 在登录页面上，单击Register a new user account链接。

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

Register User Account

Username or email

Activation code

[Show](#)

Register account

[Back to login](#)

© 2026 Cisco Systems, Inc.

新用户帐户

2. 输入创建用户时使用的用户名或电子邮件地址(例如 , user1@abc.com)
3. 输入由帐户管理员共享的激活代码。
4. 单击Register account。系统随即会显示Set New Password窗口。

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](#)

新用户帐户密码

5. 输入新密码。
6. 在Confirm password中再次输入密码。
7. 首次成功登录时，系统会提示用户配置五(5)个安全问题。(请参阅[设置安全问题](#))。

管理本地用户组

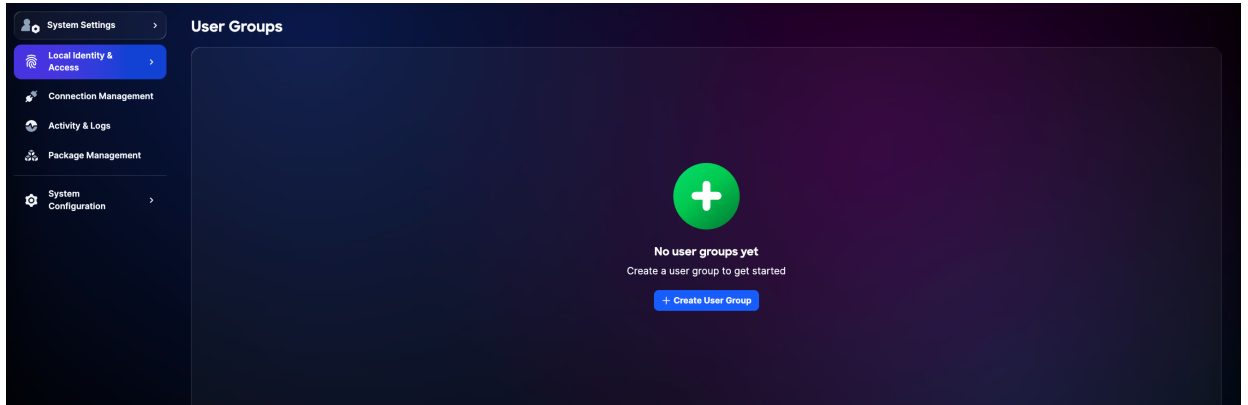
用户组使帐户管理员可以同时管理多个本地用户的角色。您可以创建一个组，向其附加一个角色和用户集，并在一个位置更新该角色或成员身份，而不是将角色单独分配给每个用户。所有用户组管理都从Local Identity & Access页面进行执行。

 注意：只有帐户管理员可以创建、编辑或删除用户组。组由现有本地用户组成；必须先创建用户，然后才能将其添加到组。有关详细信息，请参阅[添加本地用户](#)。

创建用户组

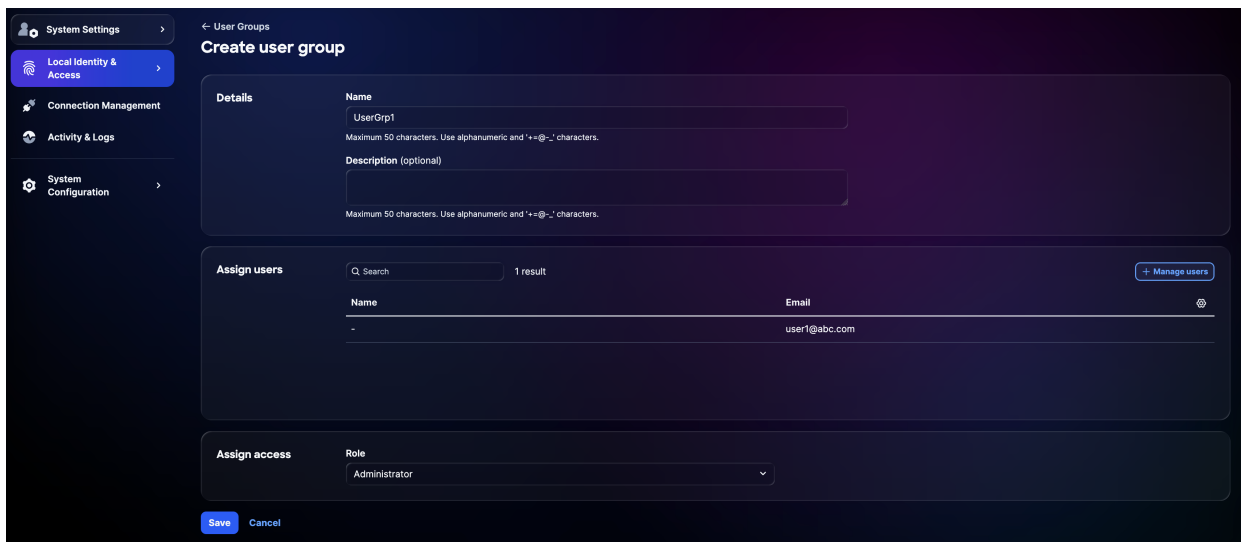
要创建用户组，请执行以下操作：

1. 从System Settings中选择Local Identity & Access > User Groups。系统随即会显示User Groups页面。



用户组

2. 单击创建用户组。系统随即会显示创建用户组页面。



创建用户组

3. 完成以下部分：

- 详细信息
- 名称：输入组的唯一名称（例如，只读运算符）
- 说明（可选）：组的简短说明(最多50个字符；允许使用字母数字和+ = @ - _个字符)
- 分配用户:搜索并选择要添加到组的一个或多个现有本地用户。注意：要添加尚未列出的用户，请单击Manage users。

- 分配访问权限
- 角色:选择要分配给此组的所有成员的系统角色。以下角色可用：
- 查看器:查看和访问模块（只读）
- 管理员:访问模块和管理系统设置

4. Click Save.

新用户组及其分配的角色和成员计数显示在User Groups列表中。

编辑用户组

要编辑用户组，请执行以下操作：

1. 从User Groups列表中找到要修改的组。
2. 选择More Options图标> Edit，选择所需的组。系统将显示“编辑用户组”页。

The screenshot shows the 'Edit user group' interface. The sidebar on the left includes 'System Settings', 'Local Identity & Access' (selected), 'Connection Management', 'Activity & Logs', and 'System Configuration'. The main panel has a header 'User Groups' and a sub-header 'Edit user group'. The 'Details' section has a 'Name' field with 'UserGp1' and a 'Description (optional)' field. The 'Assign users' section shows a search bar and a table with one user: 'user1@abc.com'. The 'Assign access' section has a 'Role' dropdown set to 'Administrator'. 'Save' and 'Cancel' buttons are at the bottom.

编辑用户组

3. 进行所需的更改。

4. Click Save.

更新的组将显示在User Groups列表中。新角色将对组的所有成员生效。

删除用户组

删除用户组的步骤：

1. 从User Groups列表中找到要删除的组。
2. 点击组旁边的更多选项图标，然后选择删除。

Delete user group?

User group will be permanently removed from the platform.

Cancel

Delete user group

删除用户组

3. 出现提示时确认删除。

该组将从User Groups列表中删除。



注意：删除用户组会从所有成员中删除基于组的角色分配。单个用户帐户不会被删除。

配置身份提供程序

登录到VA后，帐户管理员可以配置各种设置。帐户管理员可以使用本地管理或IDP配置登录。

SSO的Okta IDP SAML配置

配置IDP SAML的先决条件

- 。 本地管理员访问Cisco IQ
- 。 访问IDP门户

SSO的IDP SAML配置

要为SSO配置IDP安全断言标记语言(SAML)，请执行以下操作：

1. 导航到您的IDP门户。

表 2：思科IQ属性

字段	价值
应用程序名称	<应用程序名称>
环境	ESP业务应用
应用程序所有者组	IDP设置的所有者
团队邮件程序	团队的邮件程序

字段	价值
受众	非劳动力
入职类别	选择“New Onboarding”

表 3：SAML配置参数

参数	配置	示例
受众 (实体ID)	完全限定域名 (FQDN)	mymanagementhost.mydomain.com
单点登录URL	SAML断言客户服务(ACS)终结点	https://mymanagementhost.mydomain.com/saml/acs
名称ID格式	电子邮件地址	不适用
应用用户名	用户名	不适用

5. 配置属性语句。



注意：IDP属性更改取决于特定的提供程序和配置。下面以思科IDP及其属性为例。

- 第一个条目
 - 名称：用户名
 - 值：user.login
- 第二个条目
 - 名称：主要电子邮件
 - 值：user.email
- 组属性语句
 - 名称：组
 - 过滤器:REGEX
 - 值：.*

6. 配置应用程序中的单个注销(SLO)设置。

表 4：SLO配置设置

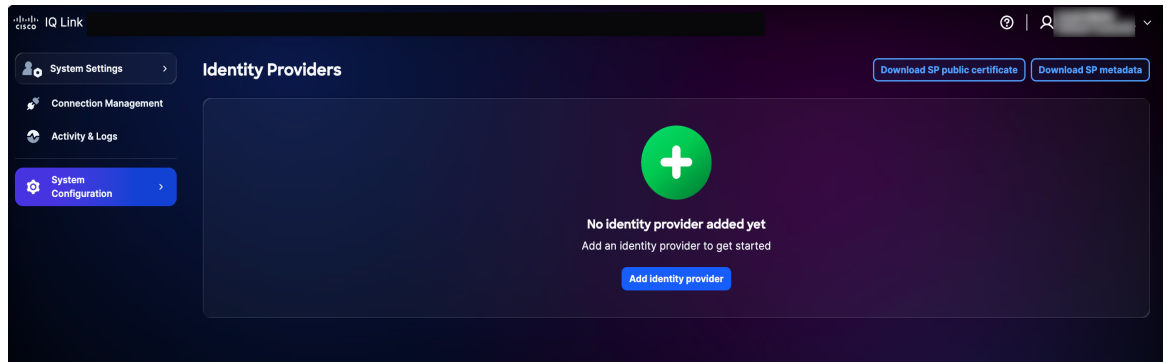
字段	价值
签名证书	对于Okta，只有当您选择启用SLO时，才需要此证书。使用身份提供程序中的下载SP证书下载签名证书。将文件另存为sp-public-key.crt。有关详细信息，请参阅 单一注销配置 。
SP元数据	仅ADFS IDP需要服务提供商(SP)元数据 (Okta不需要)。
是否要启用单一注销	是或否
单一注销URL	https://mymanagementhost.mydomain.com/saml/logout
SP颁发者 (受众/实体ID或ACS URL)	https://mymanagementhost.mydomain.com

8. 单击Download图标下载“IDP Metadata XML”文件。
9. 根据提供商的要求调配或创建应用。

添加Okta IDP

在Cisco IQ中添加IDP的步骤：

1. 从System Settings中选择System Configuration > Identity Providers。系统将显示Identity Providers页面。



IDP主页

 注意：在给定时间只能添加一(1)个IDP。

2. 单击Add Identity Provider。系统随即会显示Add Identity Provider页面。

The screenshot shows the Cisco IQ Link web interface. On the left is a navigation sidebar with four items: 'System Settings' (with a user icon), 'Connection Management' (with a plug icon), 'Activity & Logs' (with a pulse icon), and 'System Configuration' (with a gear icon and a right arrow, highlighted in blue). The main content area is titled 'Identity Providers' with a back arrow, and 'Add Identity Provider'. It contains three main sections: 1. 'Identity provider name *' with a text input field labeled 'Enter identity provider name'. 2. 'Domains' with a text input field labeled 'Enter domain names' and a blue 'Add' button. 3. 'Organization IDP metadata *' with a dashed box containing an upload icon and the text 'Select or drag file to this area to upload' and 'Only one file can be uploaded at 5 MB or less'. At the bottom, there is a toggle switch for 'Enable single log out (SLO)' which is currently off, and two buttons: 'Save' (blue) and 'Cancel' (light blue).

添加身份提供程序

3. 输入身份提供程序名称。
4. 点击Add以将Cisco IQ配置的域名添加到Domain(s)字段。
5. 在组织IDP元数据字段中拖放或上载从IDP应用获取的SAML元数据文件。此文件包含证书详细信息和SP实体详细信息。
6. (可选) 打开Enable single logout切换按钮。您也可以稍后启用SLO。
7. Click Save.

角色映射配置

1. 从添加的IDP中，选择更多选项图标> 映射角色。系统将显示Map user roles页面。

×

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

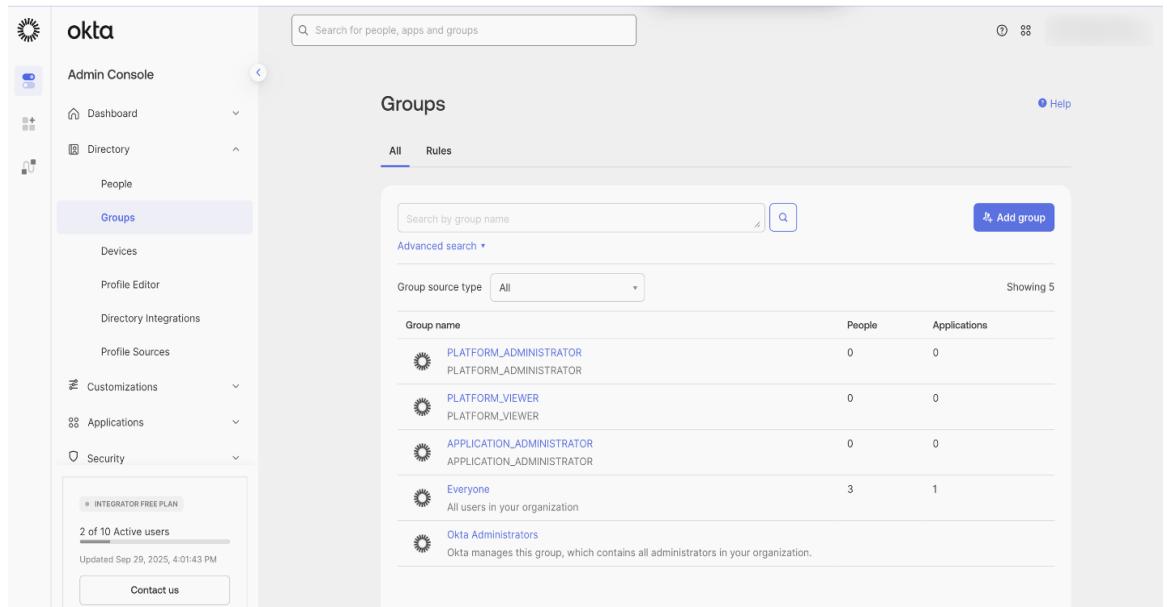
映射用户角色

2. 输入所选系统角色的IDP角色。支持以下系统角色：

- 一般帐户管理员:一般帐户管理员具有执行产品中所有操作的完全权限
- 常规帐户查看器:常规帐户查看器具有只读访问权限



注意：IDP角色是一个开放文本字段。它必须与您组织的IDP中配置的组或角色名称完全匹配。下面是Okta组的示例。



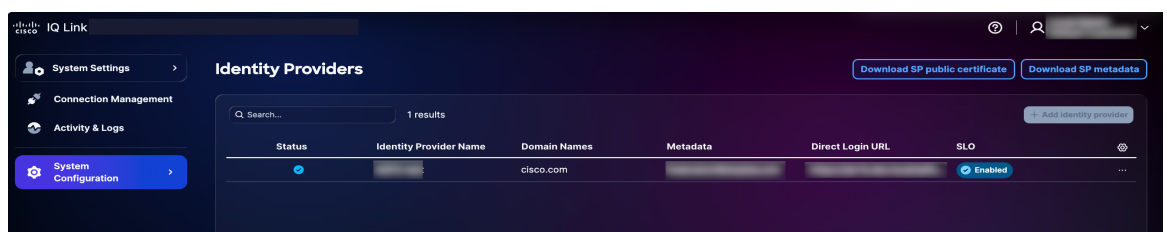
角色映射引用

3. 通过点击添加身份提供程序角色根据需要映射其他角色。
4. Click Save.配置后，登录页面会显示一个选项，用于通过IDP登录SSO。

单一注销配置

如果选择启用SLO，则必须上传包含SLO URL的元数据。您可以通过编辑身份提供程序设置并打开Enable Single Log Out来配置此设置。要完成SLO配置，请执行以下操作：

1. 从身份提供程序主页中，单击下载SP公共证书。



SP公共证书

2. 将下载的文件另存为sp-public-key.crt。
3. 导航到您的IDP门户。

4. 上传在SSO的[IDP SAML配置中生成的签名证书文件](#)。
5. 输入SLO URL(例如 , <https://ciq-xxx-xxx-37-160.cx-hub-rtt.cisco.com/saml/logout>)。
6. 输入SP颁发者(例如 , ciq-xxx-xxx-37-160.cx-hub-rtt.cisco.com)。
7. 单击 submit。
8. 再次下载IDP元数据文件。
9. 在Identity Providers页上 , 选择添加的IDP的More Options图标> Edit。
10. 打开Enable single log out(SLO)切换按钮。
11. 上传新下载的元数据文件。
12. 使用以下核对表验证SSO和SLO功能 :

验证核对表 :

- 本地管理员登录成功
- 已配置并调配IDP门户
- IDP以“成功”状态添加到思科IQ
- 配置并测试角色映射
- 下载SP元数据并提取证书
- 如果启用SLO , 则SLO配置使用实际签名证书完成
- 已成功测试端到端SSO和SLO流

排除IDP问题

下表列出了常见问题和可能的解决方案 , 以帮助快速确定和解决与IDP状态、证书错误、SSO登录失败和SLO配置相关的问题 :

表 5 : 故障排除

问题	解决方案
IDP状态显示为“未完成”	验证角色映射配置
证书错误	验证证书格式和有效性
SSO登录失败	验证属性映射和组分配
SLO未按预期工作	确保正确上传证书并配置SLO URL

ADFS IDP SAML SSO配置

本节提供将Microsoft Active Directory(AD)联合身份验证服务(FS)配置为Cisco IQ的SAML IDP的指南，支持基于密码和公钥基础设施(PKI)或基于证书的身份验证。

为SSO配置ADFS IDP SAML的先决条件

- 建议使用ADFS 6.0+
- Windows Server 2016 + (推荐2019年)
- 已配置的AD与用户帐户集成
- ADFS服务器上的SSL/TLS证书
- Cisco IQ的管理员访问权限
- 对ADFS服务器(Windows Server)的管理访问
- ADFS服务器上的PowerShell访问
- ADFS和Cisco IQ之间的网络连接
- 企业证书颁发机构(CA) (已安装或可访问)
- 域管理员或企业管理员权限 (仅PKI需要)
- ADFS服务器配置详细信息 (如下表所示)

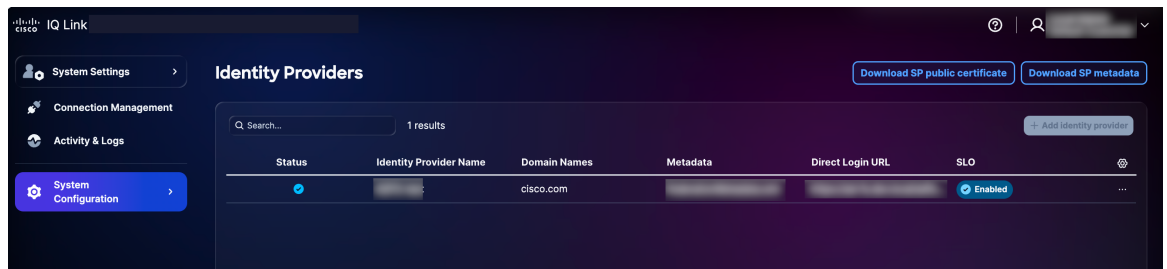
表 6：身份验证流程概述

项目	描述	示例
思科IQ FQDN	用户部署主机名	<Your-CIQ-FQDN>例如 dev35-23.cx-xxx- xxx.cisco.com
ADFS服务器URL	用户ADFS服务器地址	https://<Your-ADFS- HOSTNAME>例如 https://ad-fs.dev.local
公司域	电子邮件域	<您的域>
AD组	Active Directory组域名 (DN)	CN=Role - CXIQ开发人员 OU=Groups , DC=dev , DC=local
CA名称(PKI)	企业CA名称	<Your-CA-Name>
证书身份验证端口(PKI)	ADFS备用TLS端口	49443
SSL证书指纹	ADFS服务器SSL证书	<YOUR-SSL-CERT- THUMBPRINT>

配置基本ADFS SAML

要配置ADFS，请执行以下操作：

1. 从System Settings中选择System Configuration > Identity Providers。系统将显示Identity Providers页面。



下载选项

2. 单击下载SP公共证书和下载SP元数据以下载这些文件。
3. 将service-provider-metadata.xml和service-provider-certificate.crt文件复制并保存到ADFS服务器(例如，C:\)。
4. 登录到ADFS服务器。
5. 从ADFS Management菜单中，单击信赖方信任。
6. 从信赖方信任菜单中，单击添加信赖方信任。将打开新向导。
7. 单击Claims Aware单选按钮。
8. 单击Start继续配置。
9. 单击Import data about the relying party from a file，从作为步骤3一部分保存的文件中获取详细信息。
10. 单击Browse以选择服务提供商元数据文件并完成文件上传。
11. 单击 Next。
12. 输入显示名称（例如“Cisco IQ”），添加任何相关注释，然后点击下一步。
13. 在Choose Access Control Policy页面上，点击Permit everyone（或您的组织的安全配置所需的策略）。
14. 单击剩余屏幕中的下一步。
15. 单击Close完成信赖方信任配置。

 **注意：**除非您的ADFS服务器具有注册的多因素身份验证(MFA)适配器(例如 Azure MFA，已配置基于时间的一次性密码(TOTP))。

如果启用此策略而未配置MFA提供程序，ADFS将对用户进行身份验证，但最终拒

绝状态为urn:oasis:names:tc:SAML:2.0:status:RequestDenied的请求。由于SAML响应不包含断言，插件将失败并报告“缺少电子邮件”错误。

问题：已选择“Permit Everyone with MFA”。

解决方法：在PowerShell中，通过运行以下命令检查当前策略。

```
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”);
```

配置ADFS声明规则

要配置ADFS声明规则，请执行以下步骤。

所需领款申请

请参阅下表了解所需索赔。

表 7：所需领款申请

领款申请	目的	来源
发送邮件	用户标识符	AD邮件
显示名称	用户的全名	AD显示名称
UPN	PKI/证书身份验证	ADFS通过UPN将客户端证书映射到AD用户
名称ID	SAML主题	从电子邮件转换
组	基于角色的访问	AD组成员(memberOf)

应用领款申请规则

1. 定义信赖方信任的名称（例如，“Cisco IQ — 生产”）。

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

2. 定义声明规则以将用户信息和组成员身份发送到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. 通过运行以下命令应用声明规则：

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

写主机“声明规则配置成功！” — 前景颜色绿色

警告：每个AD用户帐户都必须填充邮件属性。如果缺少此属性，则SAML断言不包含电子邮件声明，从而导致身份验证被拒绝。

要更新用户的邮件地址，请执行以下PowerShell命令：

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

验证用户组

1. 通过运行以下命令设置用户名以检查用户的组成员身份：

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

2. 运行以下命令查找用户帐户：

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

3. 使用以下命令显示用户所属的组：

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

示例输出：

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

配置ADFS以信任SP签名证书

1. 在ADFS服务器中，将SP证书导入到TrustedPeople存储中：

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

2. 选择下列选项之一：



注意：SP证书由ADFS无法通过标准信任链验证的内部CA颁发。

- 全局为此信赖方禁用链验证

```
Set-AdfsRelyingPartyTrust `   
-TargetIdentifier "  
  
" `   
-SigningCertificateRevocationCheck None `   
-EncryptionCertificateRevocationCheck None
```

- 如果SP证书由CA颁发（非自签名），请将颁发CA证书导入根证书存储区

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

3. 通过重新启动ADFS服务应用更改。

重新启动 — 服务adfssrv

设置PKI/证书身份验证

本节介绍如何在密码中添加基于证书（即智能卡或软件证书）的身份验证。如果仅密码身份验证足够，则可跳过此部分。

安装AD CS CA角色

要安装AD证书服务(CS)CA角色，请执行以下操作：

1. 通过运行以下命令，验证域中是否已存在企业CA：

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

如果命令返回有效响应，您可以跳过本节的剩余部分。您的环境已配置。如果命令指示未找到CA，请继续执行步骤2。

2. 通过运行以下命令安装CA角色：

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

3. 通过运行以下命令配置CA角色：

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

4. 通过运行以下命令验证安装：

```
certutil -ca
```

5. 运行以下命令，确认服务处于活动状态且可以访问：

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

配置证书模板

要使用客户端身份验证增强型密钥使用(EKU)配置证书模板，请执行以下操作：

1. 打开certsrv.msc并展开CA节点。
2. 右键单击Certificate Templates > Manage。
3. 复制用户模板。



注意：仅当从内置用户模板颁发的证书包括客户端身份验证EKU时，该模板才有效或有效。

4. 配置以下选项卡上的设置：

- 一般：在名称字段中输入“CIQ用户身份验证”，有效期为一(1)年
- 请求处理:从用途下拉列表中选择签名和加密，然后选中允许导出私钥复选框
- 主题名称:选择Build from Active Directory Information，并在Subject和SAN字段中包含电子邮件

警告：Subject和SAN字段必须包含用户的用户主体名称(UPN)或与AD帐户匹配的电子邮件。ADFS使用这些字段将证书映射到AD用户。

- 分机:确保应用策略包括“客户端身份验证(1.3.6.1.5.5.7.3.2)”
- 安全:添加域用户并授予其读取和注册权限

5. 使用以下命令发布模板：

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

注册用户证书

1. 以目标用户身份登录。
2. 通过运行以下命令注册证书：

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

3. 通过运行以下命令验证证书安装：

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

从Windows导出用户证书并在客户端(Mac)上安装

要将用户证书从Windows导出到Mac:

1. 通过运行以下命令从Windows将证书导出为PFX文件：

```
$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. 将user-cert.pfx文件传输到Mac设备。

3. 通过运行以下命令将证书导入Mac密钥链：

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



注意：导入证书后，必须关闭浏览器并重新打开才能对其进行识别。

4. 通过运行以下命令信任Mac上的CA:

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

启用ADFS证书身份验证终端

要启用ADFS证书身份验证终端，请执行以下操作：

1. 通过运行以下命令启用所需的ADFS证书终端：

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

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

2. 通过运行以下命令验证所有终端均已启用：

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

启用证书身份验证作为主要

要启用证书身份验证作为主要身份验证，请执行以下操作：

1. 使用以下命令配置内联网和外联网访问的主要身份验证提供程序：

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

2. 使用以下命令验证两个列表是否包括CertificateAuthentication和FormsAuthentication:

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

3. 使用以下命令检查当前TLS客户端端口配置：

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

4. 如果未配置TlsClientPort，49443使用以下命令更新端口并重新启动ADFS服务：

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

SChannel/TLS修复（对于PKI至关重要）

以下各节中的步骤可解决阻止证书身份验证工作的CERT_E_UNTRUSTEDROOT(0x800B0109)错误。

在端口49443上绑定SSL证书

要在端口49443上绑定SSL证书，请执行以下操作：

1. 使用以下命令删除端口49443上的任何现有SSL证书绑定：

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

:49443

2. 使用以下命令创建启用客户端证书协商的新绑定：

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

```
certhash=:49443`
```

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

3. 使用以下命令验证是否已启用客户端证书协商：

```
http show sslcert
hostnameport=
```

:49443

清理证书存储区 (严重)

要清理证书存储区，请执行以下操作：

警告：如果受信任根存储中存在非自签名证书，Windows SChannel将拒绝所有客户端证书。这是PKI故障的主要根本原因。

1. 通过运行以下命令识别受信任根存储中的非自签名证书：

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

2. 通过运行以下命令，将这些证书移动到中间CA存储区：

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

3. 通过运行以下命令，验证受信任根存储中是否没有保留任何非自签名证书：

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

信道注册表修复（严重）

要配置SChannel注册表设置以确保正确的证书身份验证，请执行以下操作：

1. 使用以下命令定义注册表路径变量：

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

2. 使用以下命令应用下表中定义的注册表设置：

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

表8：信道注册表设置

设置	价值	目的
ClientAuthtrustMode	2	启用独占CA信任以更正默认验证路径。
SendTrustedIssuerList	0	防止服务器在TLS握手期间发送完全可信颁发者列表。

验证CA证书存储

要验证CA证书存储，请执行以下操作：



注意：颁发用户证书的CA证书必须位于SystemCertificates存储区中，以确保其被正确识别。

1. 使用以下命令定义CA证书的指纹：

```
$caThumbprint = "  
  
"
```

2. 使用以下命令验证CA证书已存在于LocalMachinestore*中：

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

如果未找到证书，请将其导入到LocalMachine存储区：

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

重新启动ADFS服务器（必备）

使用以下命令重新启动ADFS服务器：

```
Restart-Computer -Force
```



注意：ClientAuthTrustMode注册表更改仅在服务器重新启动后生效。

导出ADFS元数据

您可以使用PowerShell或Web浏览器下载ADFS元数据。

PowerShell

要使用PowerShell导出ADFS元数据，请执行以下操作：

1. 在ADFS服务器上打开PowerShell。
2. 运行以下命令下载元数据文件。

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

运行这些命令后，元数据文件将保存到C:-metadata.xml中。

Web 浏览器

要使用Web浏览器导出ADFS元数据，请执行以下操作：

1. 导航至<https://<your-adfs-server>/FederationMetadata/2007-06/FederationMetadata.xml>，将“<your-adfs-server>”替换为ADFS服务器的主机名。
2. 出现提示时，将元数据XML文件保存到计算机。

在Cisco IQ上配置

要在Cisco IQ上进行配置，请执行以下操作：

1. 将adfs-metadata.xml传输到工作站。
2. 在Cisco IQ中，导航到System Settings > System Configuration > Identity Providers。
3. 上传ADFS metadata文件以自动提取IDP证书、实体ID和SSO URL。
4. 保存配置。



注意：如果ADFS执行自动令牌签名证书滚动更新，您必须重新导出元数据文件并将其上传到Cisco IQ以确保继续身份验证。

添加ADFS IDP

1. 在Identity Providers页面上，单击Add identity provider。
2. 输入身份提供程序名称。
3. 输入域(例如，company.com)。
4. (可选) 根据需要打开Enable single logout切换按钮。

5. 在Upload IDP Metadata字段中拖放或上载从IDP应用程序获取的SAML元数据文件。

6. Click Save.

 注意：状态显示为“未完成”，直到角色映射完成；这是预料之中的现象。

配置角色映射

在继续配置角色映射之前，请确保可以从AD中查找要用于映射的组。要从AD查找组，请运行以下PowerShell命令：

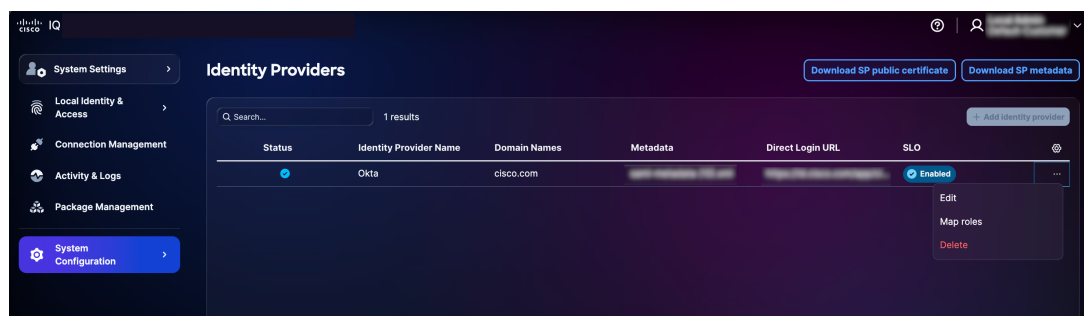
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = "(&(objectClass=group)(cn=Role - CXIQ*))"
$searcher.PropertiesToLoad.Add("distinguishedName") | Out-Null
$searcher.PropertiesToLoad.Add("cn") | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties["distinguishedname"]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

系统直接通过轻量级目录访问协议(LDAP)查询AD，无需其他模块。组信息以完整的可分辨名称格式返回，例如：

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

如果未列出所需的组，则必须在帐户管理员在AD中创建这些组，然后才能完成ADFS角色映射。

要配置角色映射，请执行以下操作：



角色映射

1. 从添加的IDP中，选择更多选项图标> 映射角色。系统将显示Map user roles页面。

Cisco IQ Link_IDP

×

Map identity provider roles to system roles to assign permissions.

Map user roles

IDP role	System role
×	General Account... × ▼ 🗑
×	General Account... × ▼ 🗑
	Select option ▼ 🗑
	Select option ▼ 🗑
	Select option ▼ 🗑

+ Add identity provider role

Save

角色映射

2. 为所选系统角色输入IDP角色。支持以下系统角色：

- 一般帐户管理员:一般帐户管理员具有执行产品中所有操作的完全权限。IDP角色（解析的名称）是CXIQ管理员。
- 常规帐户查看器:General Account Viewer具有只读访问权限。IDP角色（解析的名称）是CXIQ开发人员和CXIQ查看器。



注意：使用解析的名称（例如，CXIQ开发人员）而不是完整DN。

3. Click Save.状态更新为Success。

SChannel客户端证书测试

要验证SChannel是否正确配置为接受客户端证书，请打开一个新的PowerShell窗口并执行以下命令：

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

:49443/adfs/ls/"
```

预期输出是HTTP响应（例如，重定向或ADFS页面）。如果发生TLS握手错误，则连接失败。

PKI流的端到端浏览器测试

在开始对PKI流进行端到端浏览器测试之前，请确保用户证书安装在MacOS密钥链中(请参阅[在客户端计算机上导入用户证书\(MacOS\)](#))。要测试：

1. 导航到应用SAML登录URL。ADFS提供证书和密码选项。
2. 选择Certificate Authentication。浏览器提示输入证书。
3. 上传证书。ADFS对用户进行身份验证，使用SAML响应重定向请求，并建立新会话。

端到端浏览器测试密码流

开始端到端浏览器测试密码流之前：

1. 导航到应用SAML登录URL。ADFS提供证书和密码选项。
2. 选择密码/表单身份验证。
3. 输入Username。
4. 输入密码。
5. 验证是否成功登录。

 注意：两个流必须同时运行。

排除ADFS故障

以下列表概述了常见问题和可能的解决方案，以帮助快速确定和解决与ADFS状态、证书错误、SSO登录失败和SLO配置相关的问题。

表9：ADFS问题

问题	症状/说明	原因/检查/解决方法和修复程序
未提取的组	登录后无角色	缺少领款申请规则:重新运行配置ADFS声明规则中的说明
解密失败	“无法解密日志中的断言”	检查ADFS证书配置的配置
登录循环	停滞在身份验证或登录环路中	- 无效的ACS URL:验证：https://your-fqdn/saml/acs - Cookie不匹配:检查浏览器Cookie中的正确域

用于故障排除的诊断命令

要确保ADFS环境与Cisco IQ之间的成功集成，请使用以下诊断命令。这些命令有助于验证元数据可访问性、证书配置和终端设置。

- 验证ADFS元数据可访问性:确认可以访问和公开访问ADFS联合元数据；这是建立初始信任的关键步骤

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

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

- 验证加密证书:确保正确的加密证书与Cisco IQ信赖方信任相关联

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

- 检查SAML终端配置:验证思科IQ信任的SAML终端是否正确配置以及身

份验证请求和断言是否路由到预期的URL

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

用于SSO的Microsoft Entra ID SAML配置

本节提供将Microsoft Entra ID(Entra ID)配置为Cisco IQ的SAML IDP的指导，同时支持基于密码的身份验证、PKI身份验证或基于证书的身份验证(CBA)。

为SSO配置Entra ID SAML的必备条件

- Entra ID租户（例如，“ciqtestdev.onmicrosoft.com”）
- Cisco IQ的全局管理员或应用管理员角色访问权限
- Entra ID（云）和Cisco IQ之间的连接
- 企业CA已安装或可访问（仅PKI需要）
- 可从互联网访问的证书撤销列表(CRL)分发点（仅适用于PKI）

表10：Entra ID服务器配置

项目	描述	示例
租户Id	Entra ID租户标识符	37352d8f-0ebe-4762-8161-8775ffe897cb
思科IQ FQDN	部署主机名	<YOUR-CIQ-FQDN>
IDP实体Id	Entra ID颁发者URL	https://sts.windows.net/<TENANT-ID>/
IDP SSO URL	SAML登录终结点	https://login.microsoftonline.com/<TENANT-ID>/saml2
公司域	用户的电子邮件域	<YOUR-DOMAIN>

配置Entra ID SAML应用

创建企业应用程序

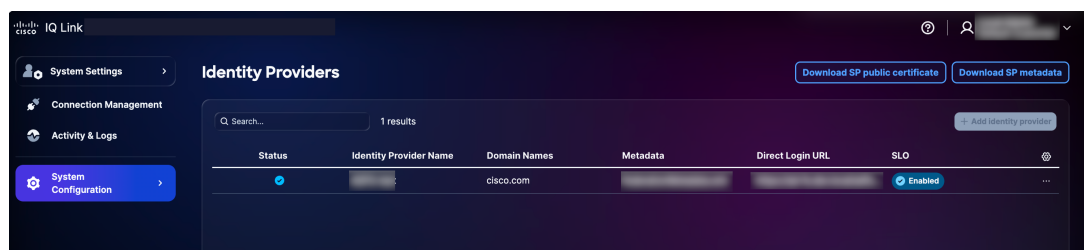
1. 登录到[Microsoft Entra管理中心](#)。
2. 导航到身份 > 应用 > 企业应用。
3. 单击New application > Create your own application。

4. 输入名称（例如“Cisco IQ”）。
5. 选择Integrate any other application you not found in the gallery(non-gallery)。
6. Click Create.

配置SAML单点登录

要配置SAML单点登录，必须上传SP元数据文件。您可以通过从VA执行以下步骤来获取它：

1. 从System Settings中选择System Configuration > Identity Providers。系统将显示Identity Providers页面。



下载选项

2. 单击Download SP metadata进行下载。上传此下载的SP元数据文件以完成SAML单点登录配置。
3. 单击Upload Metadata file按钮上载SP元数据文件。成功上传后，SP元数据文件中的数据将自动填充到基于SAML的单点登录屏幕。

您还可以选择手动输入这些详细信息以配置单点登录设置。要手动配置SAML单点登录，请执行以下操作：

4. 在企业应用中，导航到单点登录并选择SAML。
5. 在基本SAML配置部分中，单击编辑，然后输入以下内容：
 - 标识符（实体ID）:<YOUR-CIQ-FQDN>
 - 回复URL(ACS URL):https://<YOUR-CIQ-FQDN>/saml/acs
 - 登录URL:https://<YOUR-CIQ-FQDN>/saml/login
 - 注销URL:https://<YOUR-CIQ-FQDN>/saml/logout
6. Click Save.



注意：实体ID必须与思科IQ用作其SP实体ID的完全匹配。这通常是部署的FQDN。

7. 要配置SAML属性和声明，请点击属性和声明部分中的编辑。

8. 配置以下声明：

表11：所需的SAML领款申请

领款申请	源属性	命名空间
唯一用户标识符 (名称ID)	user.userprincipalname (默认)	
电邮地址	user.mail	http://schemas.xmlsoap.org/ws/2005/05/identity/
givenname	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/
姓	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity/
名称	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/
组	user.assignedroles	(EMPTY — 清除命名空间)



注意：对于组声明：

- 使用user.assignedroles作为源 — 而不是user.groups
- Namespace字段必须为空。这可确保SAML断言中的属性名称只是组，而不是完整的统一资源标识符(URI)
- 请勿使用user.groups添加重复的组声明，因为这会导致冲突

配置应用角色

应用角色在应用注册（而非企业应用）中配置；要配置应用角色，请执行以下操作：

1. 导航到Identity > Applications > App registrations。
2. 查找并选择应用程序。
3. 转至App roles > Create app role。
4. 对于每个需要的角色，配置以下内容：
 - 显示姓名：例如，Cisco IQ管理员
 - 允许的成员类型:用户/组
 - 值：例如，Cisco IQ管理员
 - 描述:例如，Cisco IQ管理员
5. 单击 Apply。

 注意：创建符合您的Cisco IQ角色映射要求的角色（例如，CXIQ管理员、CXIQ开发人员或CXIQ查看者）。

使用应用角色而不是组声明，原因如下：

- 仅云租户无法发送没有P1或P2许可证的组显示名称
- sAMAccountName仅适用于从本地AD同步的组
- 组ID源发送难以映射的通用唯一标识符(UUID)
- 应用角色发送与思科IQ角色期望完全匹配的字符串值

将用户分配到应用角色

要将用户分配给应用角色，请执行以下操作：

1. 返回企业应用 > 用户和组。
2. 单击Add user/group。
3. 选择用户并分配适当的应用角色。
4. 单击Assign。角色值在SAML声明组属性中显示为可读字符串。

下载IDP元数据和证书

下载IDP元数据和证书：

1. 从Enterprise Application中，选择Single Sign-On > SAML Signing Certificate。
2. 下载联合元数据XML（另存为entra-id-metadata.xml）。

或者

下载证书(Base64)，用于手动证书输入。

3. 请注意Set up部分中的以下值：
 - 登录URL(IDP SSO URL)
 - Azure AD标识符（IDP实体ID）
 - 注销URL(IDP SLO URL)

 注意：由于Entra ID会定期轮换签名证书，因此必须重新下载元数据，并在活动证书更改时将其上传到VA，以确保不间断的SSO服务。

添加内部ID IDP

 注意：当Cisco IQ中添加IDP时，会自动为SAML创建APISIX路由，无需手动配置路由。

添加Entra ID IDP的步骤：

- 1. 以帐户管理员身份登录到VA。
- 2. 导航到系统设置 > 系统配置 > 身份提供程序。
- 3. 单击Add identity provider。
- 4. 输入IDP的名称（例如，“Entra ID”）。
- 5. 输入域（例如，“ciqtestdev.onmicrosoft.com”或您的公司域）。
- 6. （可选）根据需要打开Enable single logout切换按钮。
- 7. 在Upload IDP Metadata字段中，拖放或上载从Entra ID获取的entra-id-metadata.xml文件。
- 8. Click Save.

 注意：在角色映射完成之前，状态将保持“未完成”；这是预料之中的行为。

配置角色映射

要配置角色映射，请执行以下操作：

- 1. 从添加的IDP中，选择更多选项图标>映射角色。系统将显示Map user roles页面。
- 2. 为每个系统角色输入IDP角色。支持以下系统角色：

表12：系统角色

系统角色	IDP角色（应用角色值）	描述
general_account_administrator	CXIQ管理员	所有操作的完全权限
general_account_viewer	CXIQ开发人员	只读访问
general_account_viewer	CXIQ查看器	只读访问

 注意：完全按照在Entra ID中配置的方式使用应用程序角色值字符串(有

 关详细信息，请参阅[配置应用程序角色](#))

4. Click Save.状态更新为Success。

检验SAML流（密码身份验证）

要验证SAML流，请执行以下操作：

1. 在Incognito或Private模式下打开浏览器。
2. 导航至https://<YOUR-CIQ-FQDN>/saml/login。
3. 验证是否已重定向到Microsoft登录页面。
4. 使用您的凭证进行身份验证（如果配置了MFA）。
5. 身份验证后，验证您是否重定向回/saml/acs并且显示Cisco IQ应用。
6. 通过运行以下命令验证组提取：

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

预期输出

符合以下条件的SAML 2.0用户身份验证成功：user@domain.com全称
：N/A和1组

提取的组：CXIQ管理员(原始：CXIQ管理员)

提取的组总数：1

配置基于证书的身份验证

本节介绍如何将CBA与密码一起添加。如果仅密码身份验证足够，则可跳过此部分。

CBA必备条件

- 配置了Enterprise CA的AD CS的Windows Server（例如，“DEV-ADCS-CA”）
- CA服务器上的PowerShell管理员访问权限
- 证书UPN必须与Entra ID userPrincipalName匹配
- CRL分发点必须可从互联网访问

在AD CS上创建证书模板

1. 在CA服务器上打开certtmpl.msc。
2. 复制用户模板并将其命名为“EntraUserCert”。
3. 配置模板：
 - 一般：显示名称EntraUserCert，有效期1-2年
 - 请求处理:目的=签名和加密
 - 主题名称:在请求中选择“供应”
 - 分机:应用策略必须包括客户端身份验证(1.3.6.1.5.5.7.3.2)
 - 安全:向通过身份验证的用户授予读取和注册权限
4. 使用以下命令发布模板：

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

请求和颁发用户证书

1. 使用以下PowerShell脚本创建证书配置(INF)文件(例如，C:-cert.inf):

```
@”
[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. 用您的Entra ID UPN替换<USER-UPN>(例如
， user@ciqtestdev.onmicrosoft.com)。

3. 要生成证书，请运行以下命令：

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

4. 要向CA提交请求，请运行以下命令：

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

5. 要将证书安装到CA，请运行以下命令：

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

导出证书

要将用户证书导出为PFX文件（用于客户端），请运行以下脚本：

```

$cert = Get-ChildItem Cert:| Where-Object { $_.Subject -like "*"
    *"} }
$password = ConvertTo-SecureString -String "

```

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

要导出CA根证书（用于Entra ID），请运行以下脚本：

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

在客户端计算机(MacOS)上导入用户证书

要导入用户证书(PFX)，请运行以下命令：

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

要导入CA根证书，请运行以下命令：

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

在Keychain Access中将CA证书设置为Always Trust:

1. 打开密钥链访问。
2. 查找CA证书并单击Get Info。
3. 在Trust下，设置为“Always Trust”。

 注意：导入后，请退出并重新打开浏览器以识别证书。

将CA根证书上传到Entra ID

1. 登录到[Microsoft Entra管理中心](#)。
2. 导航到Protection > Security > Certificate authorities。
3. 单击Upload并选择ca-root.cer文件。
4. 将其标记为根CA证书。
5. 输入CRL分发点URL（必须可公开访问）。

在Entra ID身份验证方法中启用CBA

1. 导航到Protection > Authentication methods > Policies。
2. 单击Certificate-based authentication 进行配置。
3. 启用CBA并添加目标用户或组。
4. 在Configure下，将保护级别设置为Single-factor authentication。

配置用户名绑定

在CBA配置中，转到用户名绑定选项卡并设置以下绑定：

- 证书字段：主体名称
- 用户属性:userPrincipalname

这会将证书的Subject Alternative Name(SAN)中的UPN映射到Entra ID用户。

检验CBA流程

1. 在Incognito或Private模式下打开浏览器。
2. 导航至https://<YOUR-CIQ-FQDN>/saml/login。
3. 在Microsoft登录页面，输入用户的电子邮件并点击下一步。
4. 选择Use a certificate or smart card（或者它可以自动提示）。
5. 当浏览器提示选择证书时，选择适用的用户证书。
6. 验证Entra ID验证证书，使用SAML响应重定向并创建会话。

 注意：确保选择正确的客户端证书。选择错误的证书（例如，其他用户的证书或过期的证书）会导致身份验证失败。

排除Entra ID问题

以下列表概述了常见问题和可能的解决方案，以帮助快速确定和解决与Entra ID SAML配置相关的问题。

表13：故障排除

问题	原因	修复程序
无效的SAML响应 — 缺少电子邮件	SAML断言没有NameID或电子邮件属性	验证Entra ID声明配置(有关详细信息，请参阅 配置SAML单点登录)。检查用户是否已填充邮件属性。
提取的组总数：0	组声明未配置或来源错误	使用user.assignedroles作为源。确保将用户分配给应用角色(有关详细信息，请参阅 将用户分配给应用角色)。
重复组声明	user.groups和user.assignedroles都处于活动状态	删除user.groups声明。仅保留user.assignedroles。
显示为UUID的组	源属性为“组ID”	使用应用角色方法(有关详细信息，请参阅 配置应用角色)。
属性名称显示长URI	命名空间字段不为空	清除组声明设置中的Namespace字段。
无效的SAML签名	IdP证书已轮换或不匹配	从Entra ID重新下载元数据并重新上传到Cisco IQ。
AADSTS500191	无法从互联网访问CRL	将CRL发布到可公开访问的URL，或使用自签名CA方法(有关详细信息，请参阅 可达性问题的CRL解决方法)。
未提示证书	证书不在密钥链中，CA不受客户端信任，或CBA未启用	验证是否已在MacOS Keychain Access中导入用户证书(有关详细信息，请参阅 在客户端计算机上导入用户证书(MacOS))，已使用所需设置在Entra ID中启用CBA(有关详细信息，请参阅 在Entra ID身份验证方法中启用CBA)，并重新启动Chrome以应用更改。
SAML断言已过期	系统之间的时钟偏差	增加插件配置中的clock_skew_seconds(默认值为

问题	原因	修复程序
虚拟设备中的状态“不完整”	尚未配置角色映射	300;使用30000作为实验)。 完成角色映射(有关详细信息, 请参阅 配置角色映射)。

可达性问题的CRL解决方法

如果无法从Internet访问您的CA的CRL分发点 (在实验设置中常见) , 请使用无CRL要求的自签名CA:

```
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=

"
)
```

仅将根CA证书上传到Entra ID。由于它自签名时没有思科发现协议(CDP), 因此Entra ID不会尝试CRL验证。

完成设置核对表

本节介绍使用Microsoft Entra ID SAML应用和可选CBA配置VA的完整设置核对表。

Entra ID SAML应用程序设置

- 在Entra ID中创建企业应用程序（非库）
- 通过手动输入SP元数据配置基本SAML配置
- 使用user.assignedroles配置属性和声明（包括电子邮件、名称和组）
- 在应用程序注册中创建应用程序角色
- 将用户分配到应用角色
- 下载联合元数据XML

Cisco IQ配置

- 通过上传Entra ID元数据在Cisco IQ中添加IDP
- 配置角色映射以将应用角色值映射到Cisco IQ系统角色
- 检验基于密码的登录是否端到端有效
- 验证是否在日志中正确提取了组

基于证书的身份验证（可选）

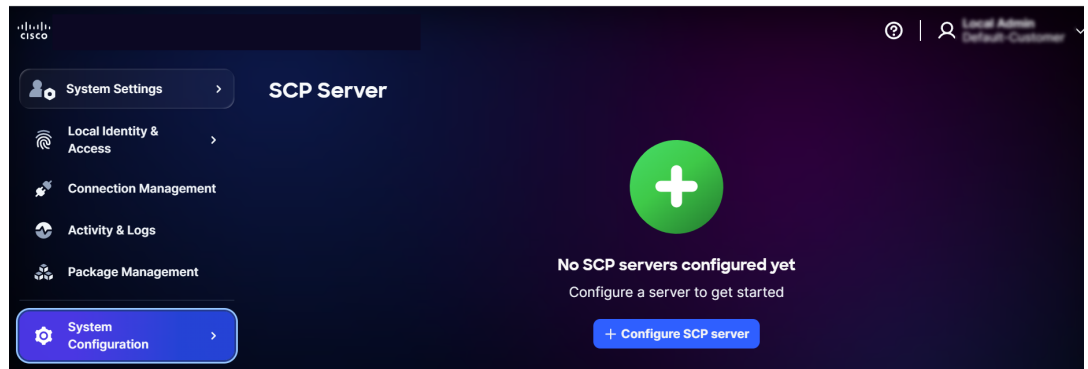
- 使用客户端身份验证EKU在AD CS上创建证书模板
- 使用与Entra ID用户匹配的UPN颁发用户证书
- 将用户证书导出为PFX文件并将其安装在客户端计算机上
- 信任客户端计算机上的CA证书
- 将CA根证书上传到Protection > Certificate authorities下的Entra ID
- 在身份验证方法中启用CBA
- 配置用户名绑定（PrincipalName和userPrincipalName）
- 验证CBA登录端到端正常工作

添加SCP服务器

SCP服务器是导入对添加、升级或修复Cisco IQ安装至关重要的升级文件的必备条件。

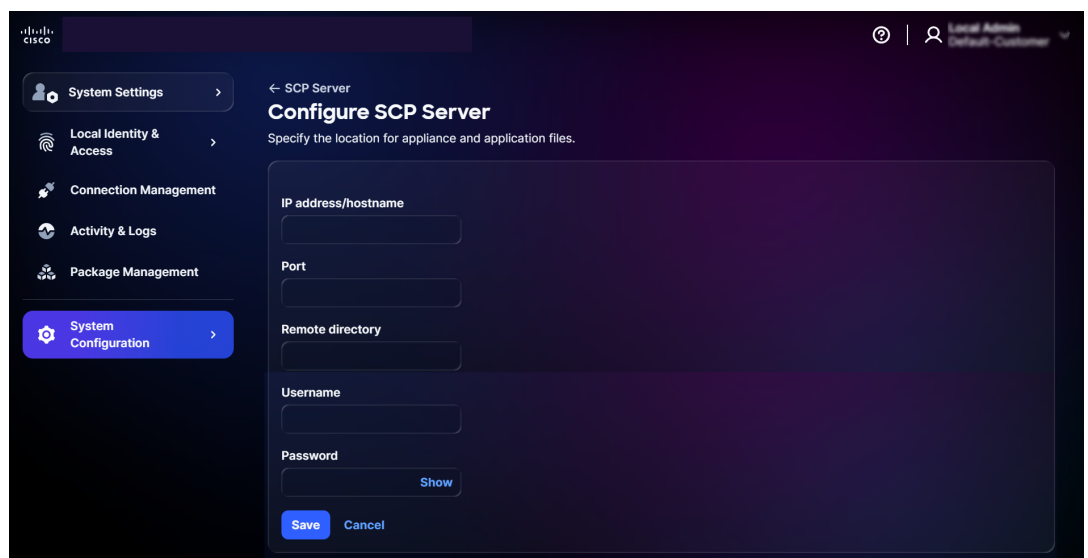
添加SCP服务器的步骤：

1. 从System Settings中选择System Configuration > SCP Server。系统随即会显示SCP Server页面。



SCP服务器主页

2. 单击Configure SCP server。系统随即会显示配置SCP服务器页面。



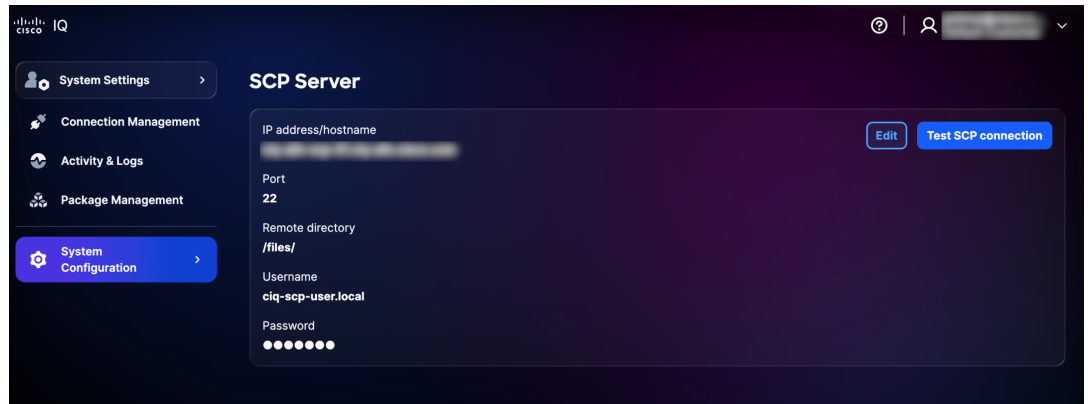
配置SCP服务器

3. 输入IP地址/主机名。
4. 输入Port。
5. 输入Remote directory。
6. 输入用户名。
7. 输入密码。
8. Click Save.系统随即会显示确认。

编辑现有SCP服务器

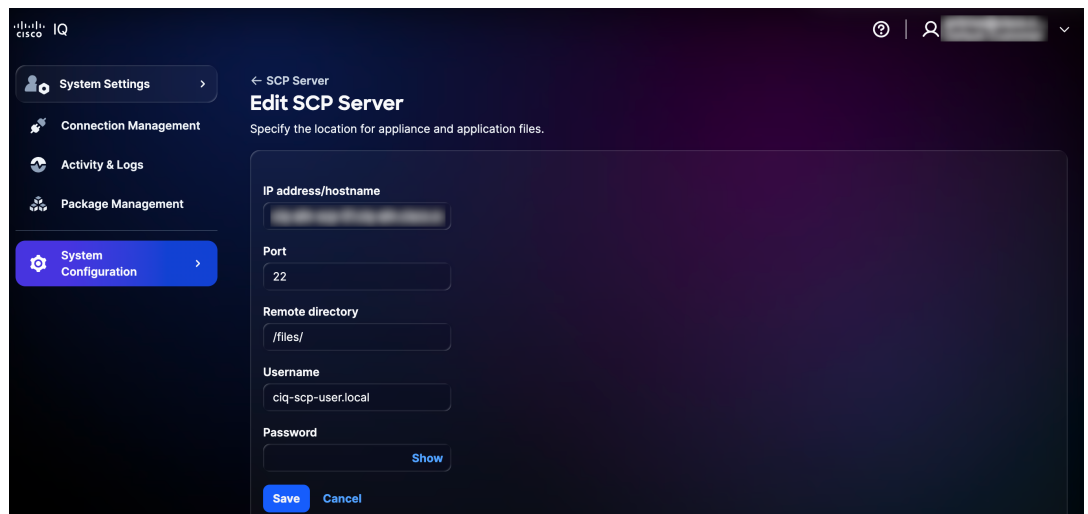
要编辑现有SCP服务器，请执行以下操作：

1. 导航到SCP Server页面。



已添加SCP服务器

2. 点击编辑所需的现有SCP服务器。



编辑SCP服务器

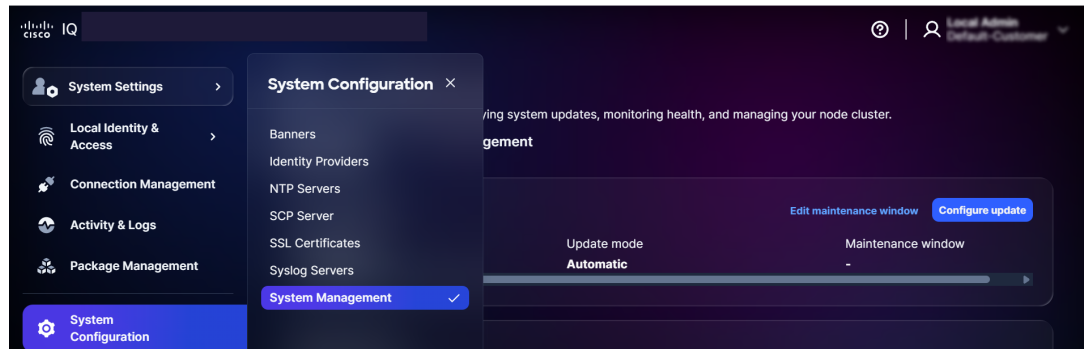
3. 根据需要修改详细信息。
4. Click Save.

系统管理

您可以通过UI升级到最新的Cisco IQ VA版本。您也可以从Cisco IQ Data Connectors页面进行验证。

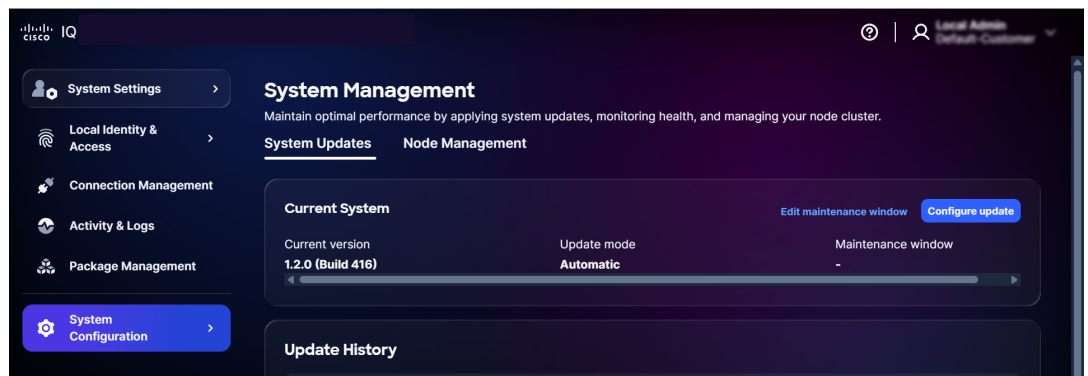
重新计划系统更新

要重新计划系统更新，请执行以下操作：



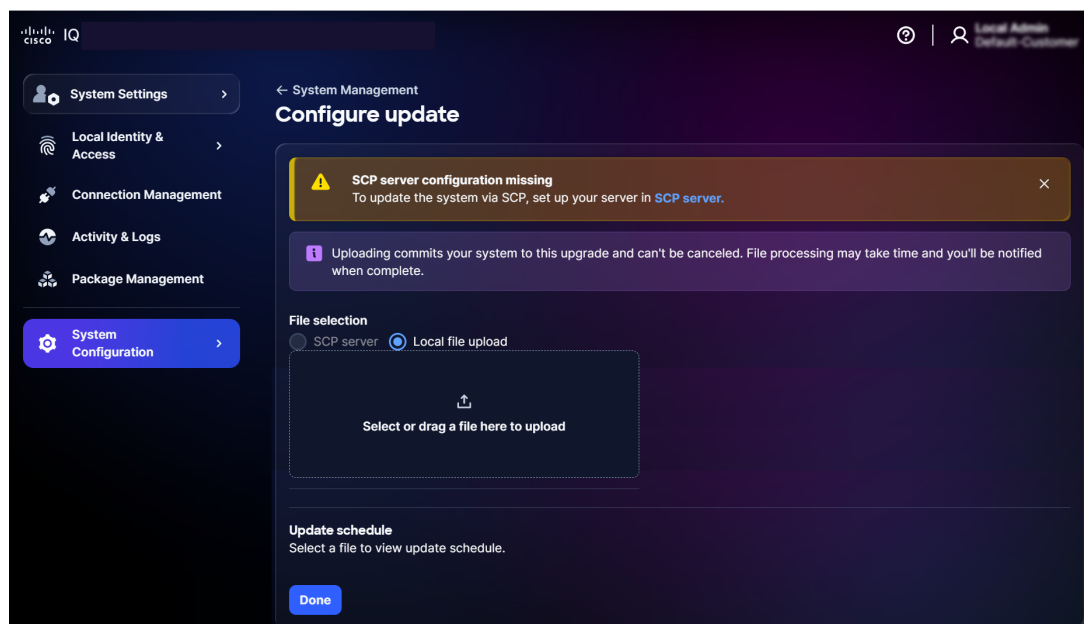
系统管理

1. 从System Settings中选择System Configuration > System Management。系统随即会显示System Management页面。此页面显示当前运行的系统版本；如果尚未配置更新，则Update History部分为空。



系统升级

2. 单击Configure update。系统随即会显示配置更新页面。



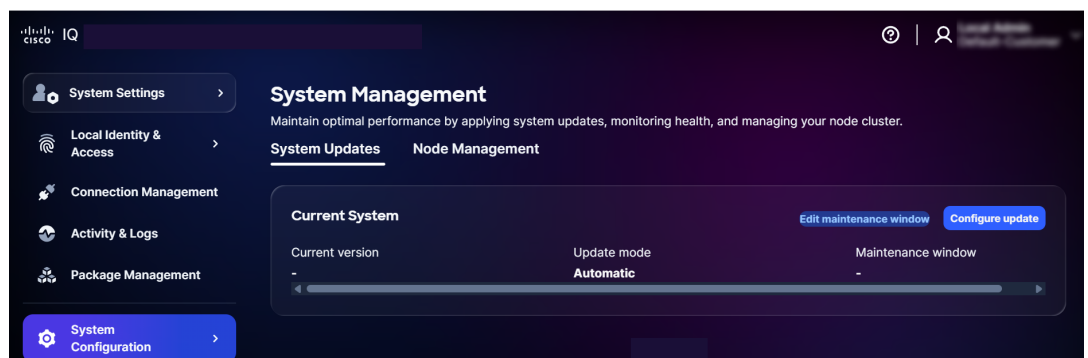
配置升级

3. 选择Update schedule以安排其他时间。
4. 等待文件上传完成；持续时间取决于捆绑包的大小和网络速度。

通过验证Update Status (更新状态) 列下显示的复选标记图标来确认更新成功。

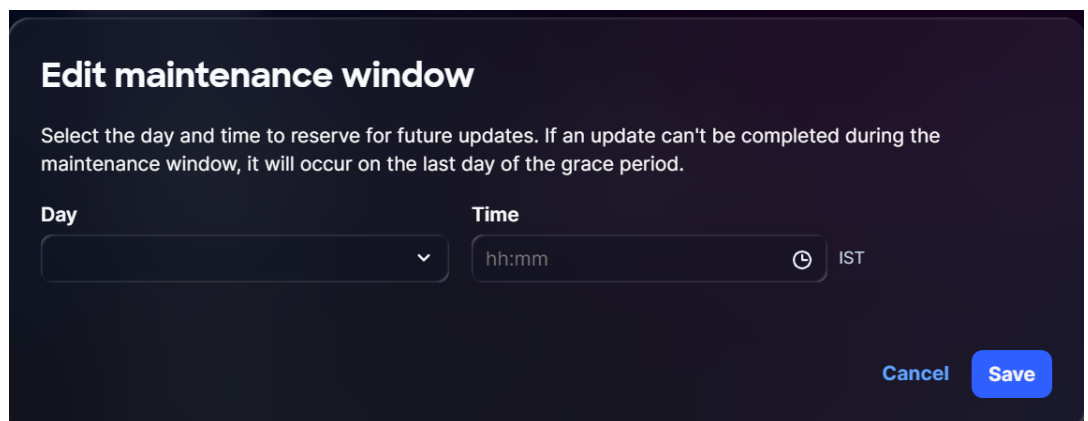
编辑系统升级计划

您可以为系统升级创建自定义计划。如果配置了自定义计划，升级将在用户定义的日期进行，前提是这些日期保持在最大宽限期内。要创建系统升级计划，请执行以下操作：



编辑维护

1. 在System Management页面的Current System部分，单击Edit maintenance窗口。



编辑维护窗口

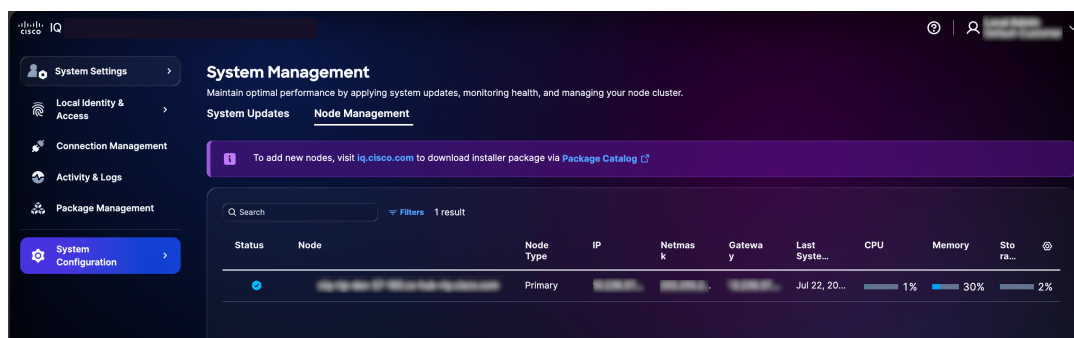
2. 从Day和Time下拉列表中选择一个选项。
3. 单击保存。已成功计划维护窗口。根据显示的计划触发更新。

 **注意：**如果未配置升级计划，系统默认为两(2)周（对于非重启升级）和四(4)周（对于需要重启的升级）的宽限期。在这些宽限期之后，必须手动执行更新。如果升级失败，系统最多执行两(2)次自动重试

。已安排第三次尝试，但需要手动启动。

节点管理

1. 导航到System Configuration > System Management > Node Management以查看和管理集群中的节点。



节点管理

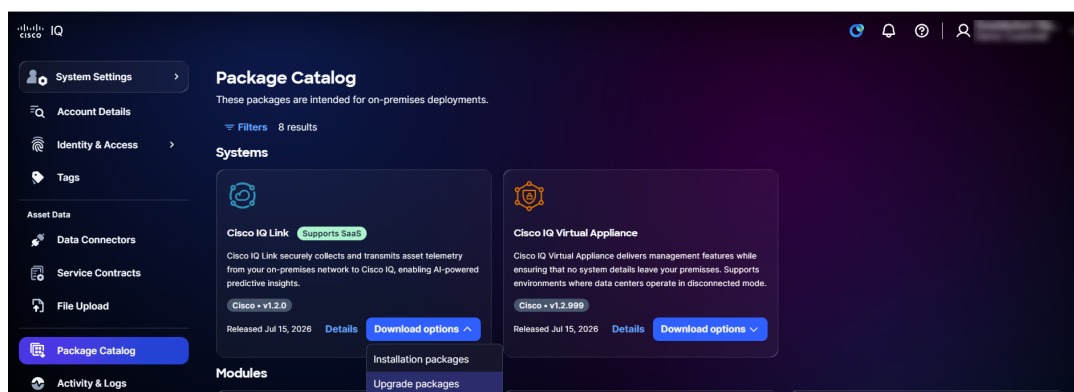
2. 节点列表显示每个节点的状态、主机名、节点类型、IP地址、网络掩码、网关和上次同步时间。

 注意：状态列中的蓝色复选标记表示节点处于活动状态。

手动升级系统

在无法自动从Cisco IQ SaaS分发或延迟分发的情况下，您可以直接从Cisco IQ SaaS下载升级捆绑包来手动执行系统升级。要手动升级系统，请执行以下操作：

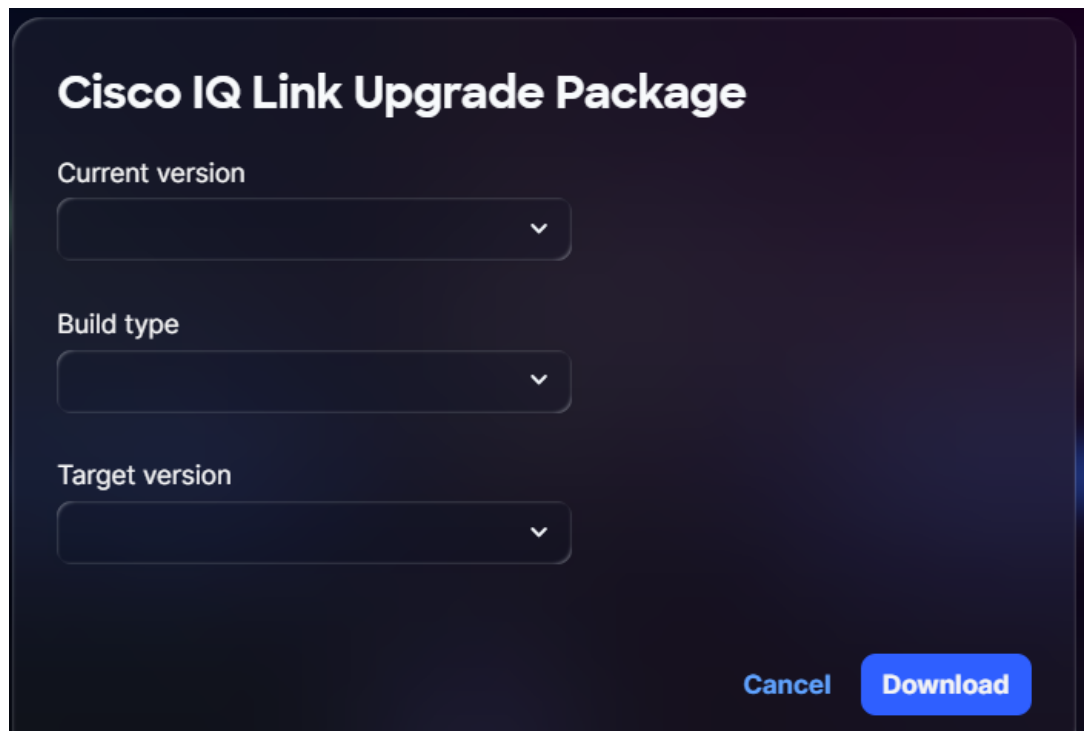
1. 登录[Cisco IQ SaaS](#)。
2. 导航到主页 > 系统设置 > 程序包目录。



软件目录

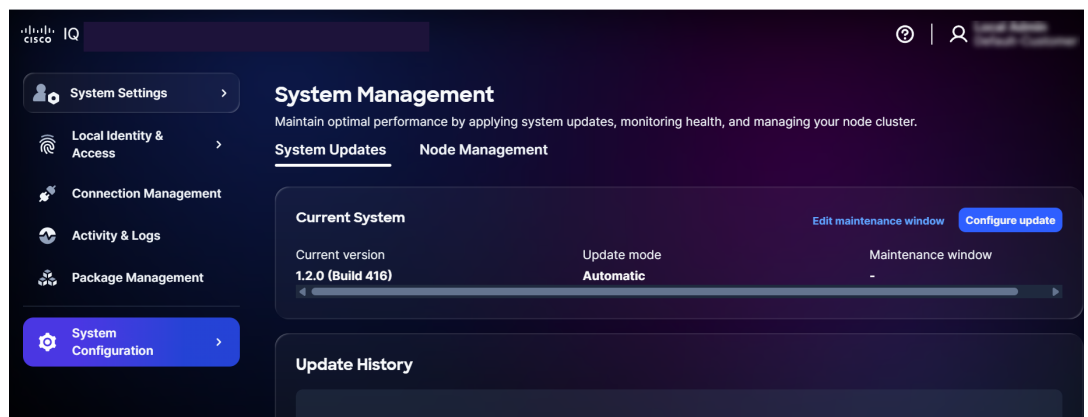
3. 在Cisco IQ Virtual Appliance卡中，单击Download options > Upgrade

packages。



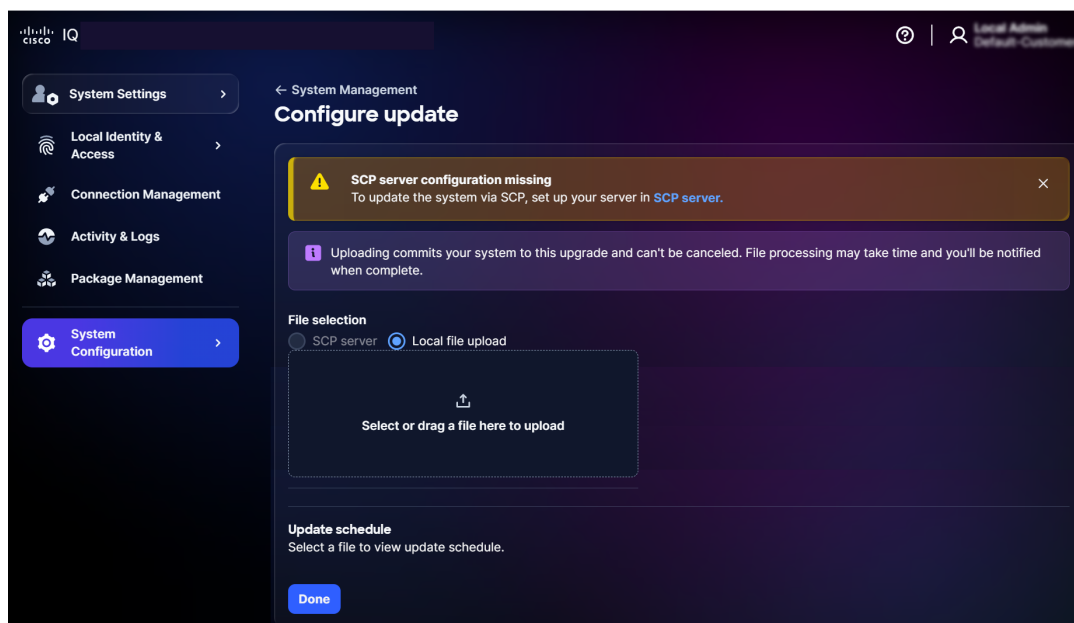
升级包

4. 从下拉列表中选择Current version。
5. 选择Build type from下拉列表。
6. 从下拉列表中选择Target version。
7. 单击 Download。下载升级捆绑包。
8. 导航至Cisco IQ VA。
9. 从System Settings中选择System Configuration > System Management。



配置更新

10. 单击Configure update。



本地文件上传

11. 单击Local file upload单选按钮。
12. 选择下载的升级捆绑包文件并将其拖到上传字段中。
13. 等待文件上传完成；持续时间取决于捆绑包的大小和网络速度。

SSL证书配置

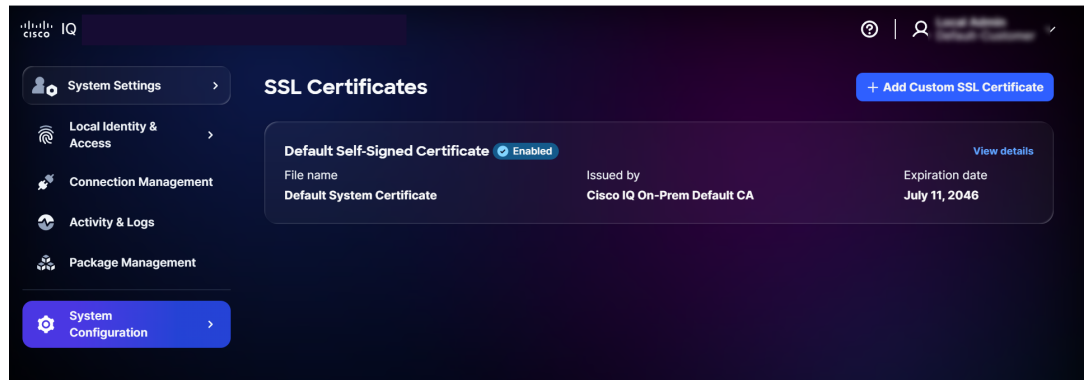
Cisco IQ中预先安装并启用了默认自签名证书，但您也可以上传自定义SSL证书。启用自定义SSL证书时，该证书用于HTTPS连接；如果证书被禁用或删除，系统会自动恢复为默认证书。无法编辑或删除默认SSL证书。

 注意：证书的有效期必须至少为90天。如果证书到期前的剩余天数少于90天，则认为该证书“即将到期”。添加、编辑或删除SSL证书后，必须按照[完成Okta IDP或ADFS IDP的SLO配置](#)中所述上传新的SSL证书。

添加自定义SSL证书

要添加自定义SSL证书，请执行以下操作：

1. 从System Settings中，选择System Configuration > SSL Certificates。系统将显示SSL Certificates页面，其中列出了系统的所有SSL证书。

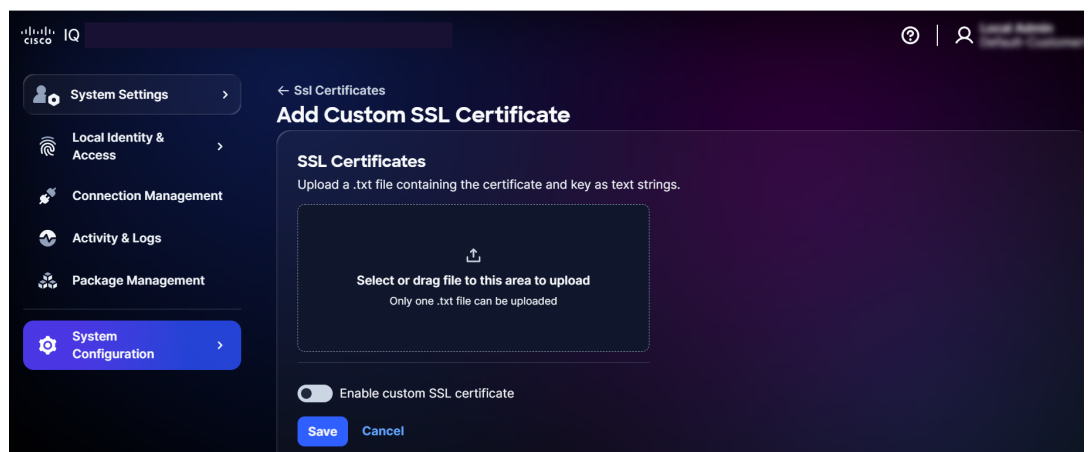


添加SSL证书

2. 单击Add Custom SSL Certificate。



注意：上传包含隐私增强型邮件编码证书和密钥作为文本字符串的.txt文件。一次只能上传一个.txt文件。文件必须同时包含证书和私钥。

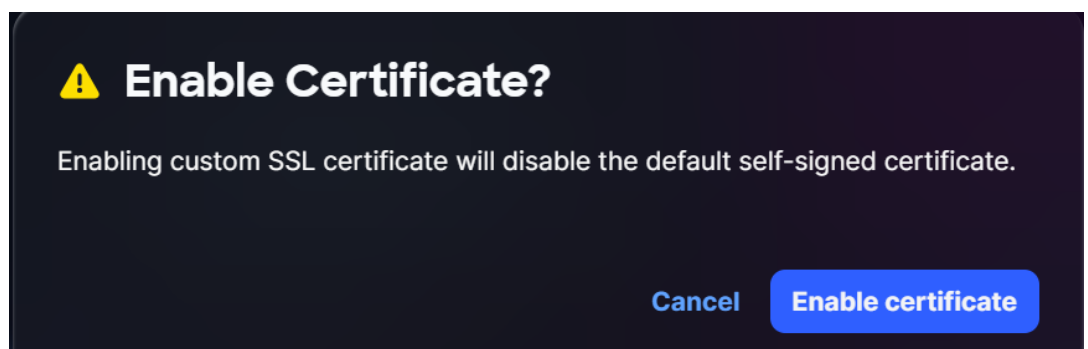


上传SSL证书

3. 在SSL Certificate部分下拖放或上传自定义SSL证书。

4. 打开Enable custom SSL certificate (启用自定义SSL证书) 切换按钮

。



启用证书

 注意：如果您要上传证书而不立即将其激活，请保持关闭切换。

5. 点击Enable certificate。

6. Click Save.

自定义SSL证书已启用且处于活动状态。默认系统证书将自动停用。

编辑自定义SSL证书

您可以编辑自定义SSL证书以上传新证书或禁用当前启用的证书。要编辑：

1. 导航到所需的自定义SSL证书。
2. 选择更多选项图标> 编辑。系统将显示Edit SSL Certificate页面。
3. 根据需要编辑证书详细信息。
4. Click Save.

删除自定义SSL证书

警告：自定义SSL证书可以随时删除，但这是不可逆操作；您可以在删除后随时上传新的自定义证书。

删除：

1. 导航到所需的个人SSL证书。
2. 选择更多选项图标> 删除。
3. 点击删除证书。系统将删除自定义证书，并自动重新激活默认证书。

系统日志服务器配置

具有帐户管理员角色的用户可以配置外部系统日志服务器以导出系统日志。最多可以配置两(2)台系统日志服务器。

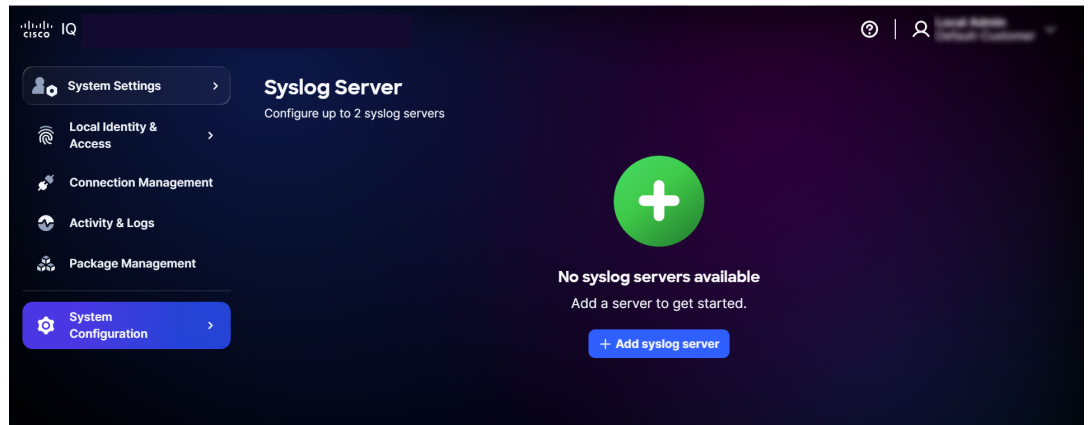
 注意：系统日志服务器必须指定为IP地址，而不是完全限定域名(FQDN)。

添加系统日志服务器

添加系统日志服务器的步骤：

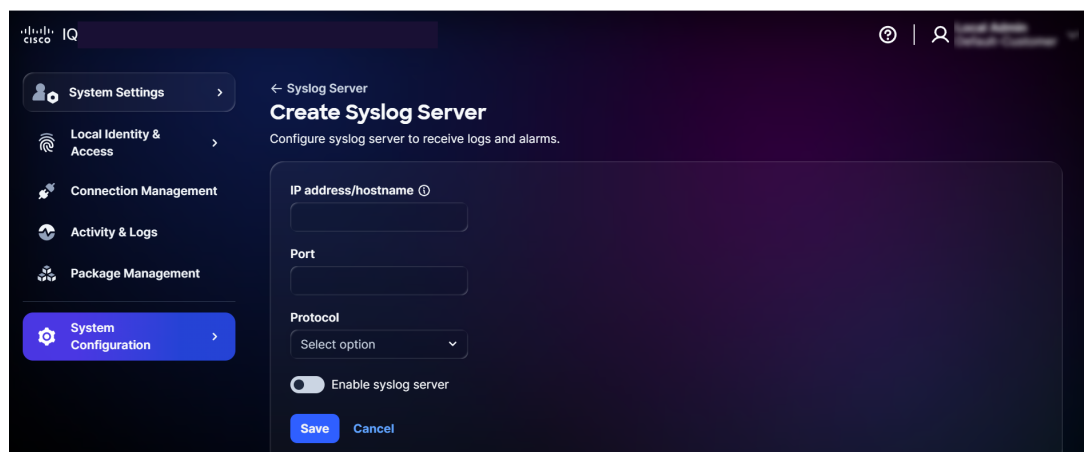
1. 从System Settings中选择System Configuration > Syslog Server。系

系统随即会显示Syslog Server页面。



添加系统日志服务器

2. 单击Add syslog server。系统随即会显示创建系统日志服务器页面。



创建系统日志服务器

3. 输入IP地址/主机名。
4. 输入Port。
5. 从Protocol下拉列表中选择适用的协议（例如UDP、TCP）。
6. 打开Enable syslog server切换按钮。
7. Click Save.系统将显示确认消息，新添加的系统日志服务器将显示在Syslog服务器主页上。

编辑配置的系统日志服务器

要编辑已配置的系统日志服务器，请执行以下操作：

1. 导航到所需的系统日志服务器。
2. 选择更多选项图标> 编辑。系统随即会显示Edit Syslog Server页面。

3. 根据需要编辑详细信息或关闭Enable syslog server切换。
4. Click Save.

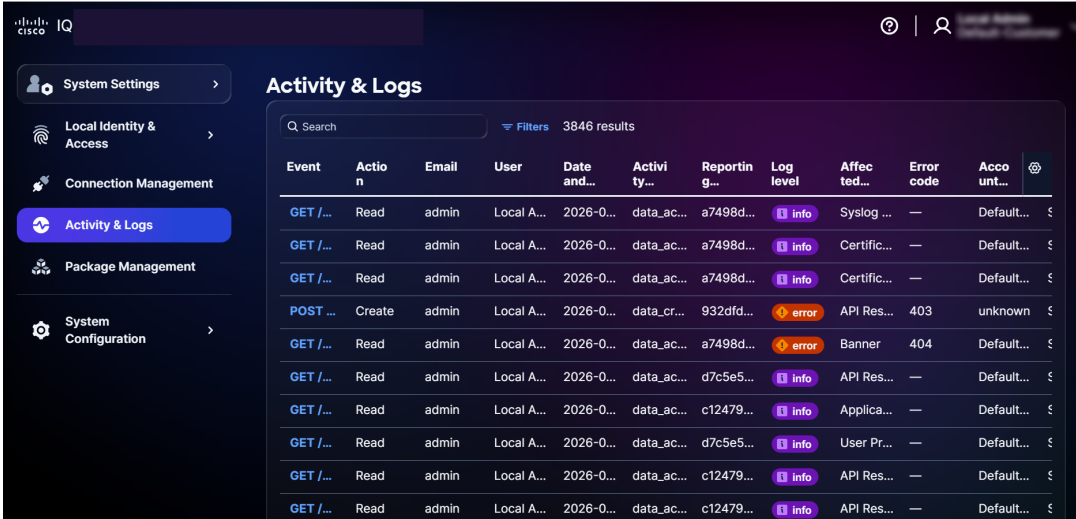
删除配置的系统日志服务器

要删除已配置的系统日志服务器，请执行以下操作：

1. 导航到所需的系统日志服务器。
2. 选择更多选项图标> 删除。系统随即会显示确认。
3. 单击Delete syslog server。

活动和日志

活动和日志详细记录了Cisco IQ中的用户操作和更改，使帐户管理员能够跟踪用户活动并保持透明度。



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

活动和日志

要查看活动和日志，请从System Settings菜单中选择Activity & Logs。

活动和日志：

- 记录网关级别的所有API操作
- 支持过滤器、分页和搜索功能，帮助您轻松查找和管理信息

以下过滤器选项可用：

- 上次记录日期:过滤日志到特定时间范围
- 日志级别:按严重性过滤日志（例如，错误、警告和信息）
- 活动类型:按系统活动类型过滤日志

- 错误代码:特定错误代码的过滤器

横幅

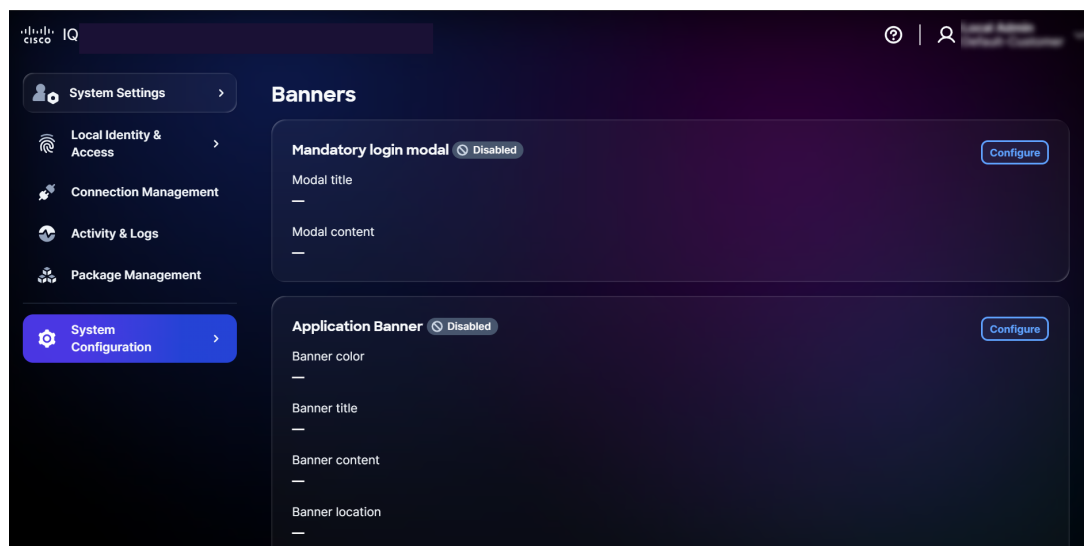
帐户管理员可以配置系统范围的横幅以符合安全和合规性标准。

- 强制登录模式:进入登录屏幕之前，必须确认必填标语。
- 应用横幅:这些是自定义横幅，在身份验证成功后横跨应用显示。

配置强制登录模式标语

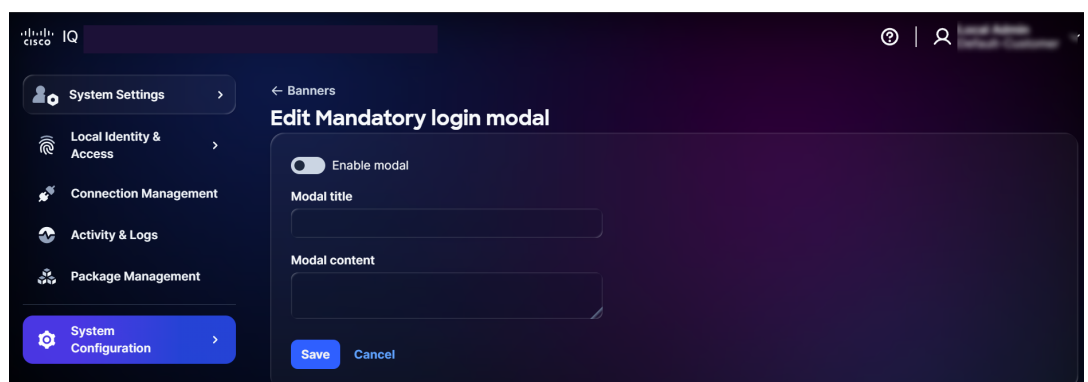
要配置强制性标语，请执行以下操作：

1. 从系统设置中选择系统配置 > 横幅。系统随即会显示Banners页面。



配置必填标语

2. 在Mandatory login modal中单击Configure。系统随即会显示Edit Mandatory login modal页面。



编辑强制登录模式横幅

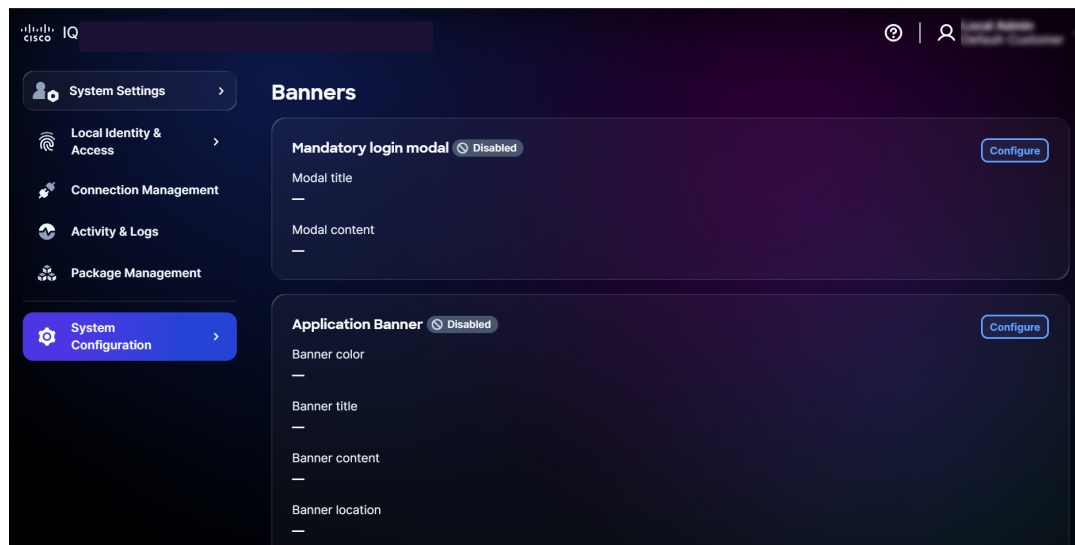
3. 点击切换以启用或禁用标语。

4. 输入模式标题。
5. 输入Modal内容。
6. Click Save.系统保存了Mandatory login modal。

配置应用横幅

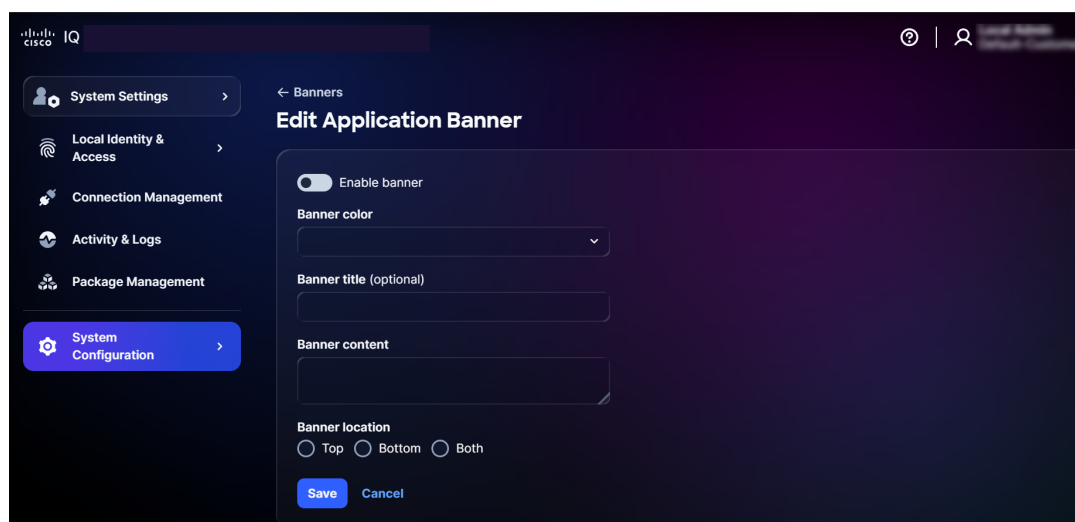
要配置应用横幅，请执行以下操作：

1. 从系统设置中选择系统配置 > 横幅。系统随即会显示Banners页面。



配置标语

2. 点击Application Banner中的Configure。系统随即会显示Edit Application Banner页面。



编辑应用横幅

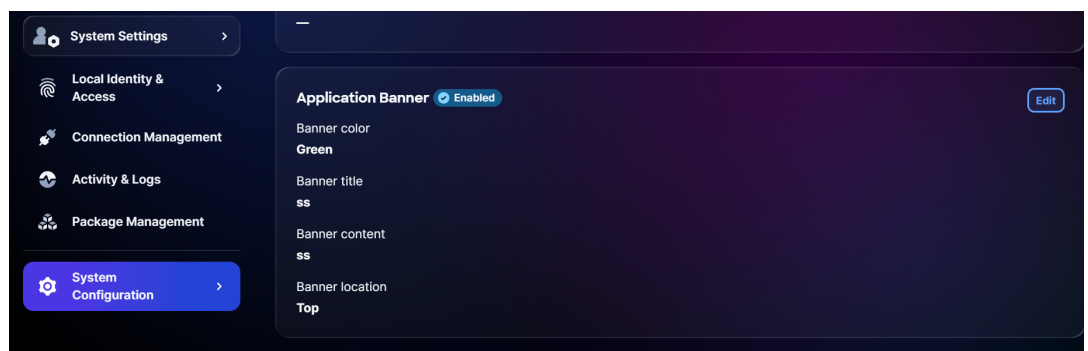
3. 点击切换以启用或禁用标语。

4. 选择Banner color。
5. 输入Banner title。
6. 输入Banner content。
7. 选择Banner location。
8. Click Save.横幅将在整个应用中显示。

编辑横幅

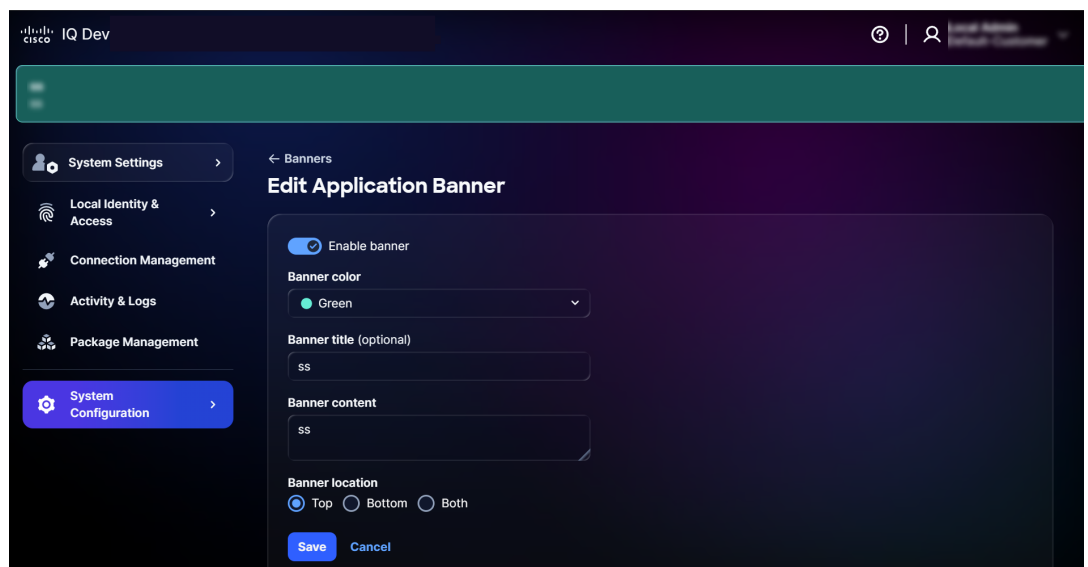
要编辑横幅，请执行以下操作：

1. 从系统设置中选择系统配置 > 横幅。系统随即会显示Banners页面。



编辑横幅

2. 单击 Edit。系统随即会显示Edit Application Banner页面。



编辑应用横幅

3. 编辑所需的详细信息。
4. 点击切换以启用或禁用标语。

5. Click Save.

故障排除

您可以从Cisco IQ系统收集诊断和日志文件，并将其安全地传输到SCP服务器。报告问题时可与支持团队共享这些文件，以提供有价值的情景并帮助进行故障排除。

要收集诊断和日志文件，请执行以下操作：

1. 登录到Cisco IQ。



主菜单

2. 从Cisco IQ主菜单中，输入“3”并按Enter选择System Diagnostics。



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):

系统诊断

3. 输入SCP/SFTP Server Address。
4. 输入SCP/SFTP Server Port。
5. 输入SCP/SFTP Server Path。
6. 选择一个协议。
7. 输入用户名。
8. 输入密码。
9. 输入“C”并按Enter继续系统诊断。

```



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...

```

系统诊断操作完成

系统开始诊断过程并执行下列操作：

- 检查连通性
- 收集系统信息
- 收集Kubernetes信息
- 收集日志
- 准备系统诊断套件
- 上传系统诊断捆绑包

完成后，系统将显示一条确认消息，指示生成的捆绑包名称。

支持模块

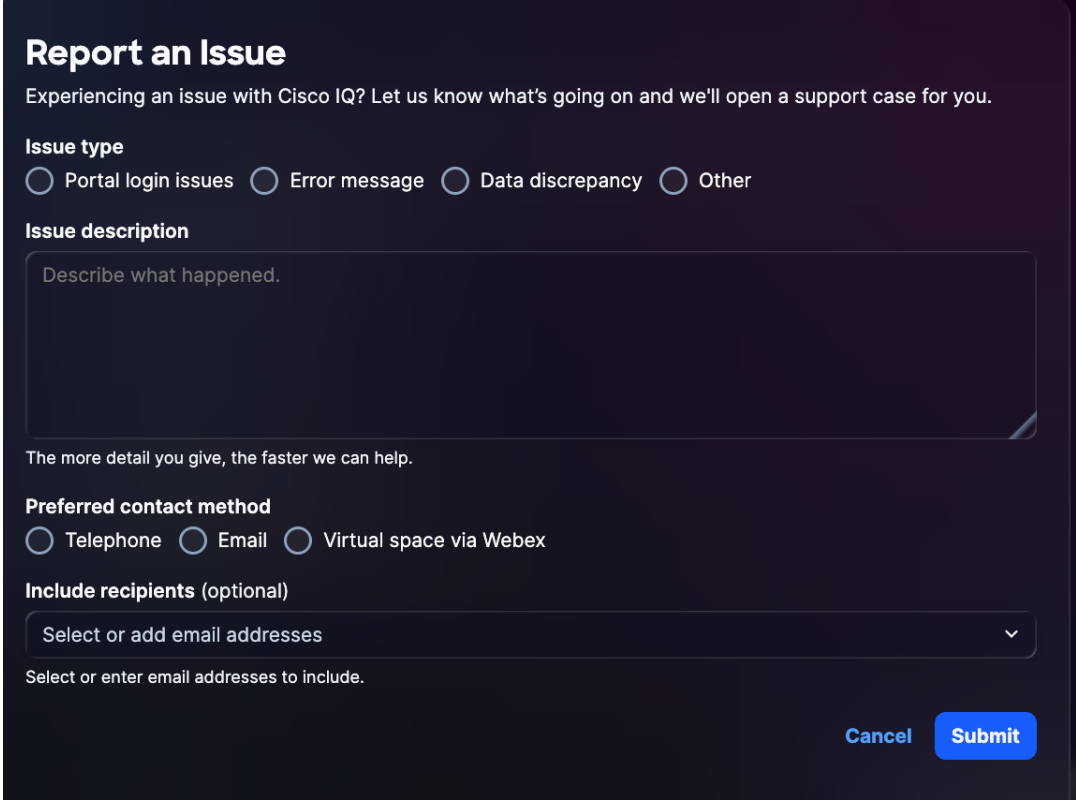
您可以通过Cisco IQ SaaS创建VA和特定于模块的支持案例。支持模块在Cisco IQ SaaS中提供，并提供支持案例的整合视图。它使您能够筛选、排序和自定义案例列表视图，让您能够查看有权访问的未结和已结案例。有关Cisco IQ SaaS中支持模块的更多详细信息，请参阅[Cisco IQ SaaS入门指南](#)。

 **注意：** Cisco IQ VA客户可以访问大多数Cisco IQ SaaS支持模块功能，包括打开与Cisco IQ VA及其模块相关的技术支持中心(TAC)案例，以及创建和管理产品案例。

创建支持案例

您可以在Cisco IQ SaaS中创建VA和模块特定案例。要创建案例，请执行以下操作：

1. 登录[Cisco IQ\(SaaS\)](#)。
2. 单击Help图标> Report an Issue。将打开“报告问题”窗口。



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

报告问题

3. 提供所需的详细信息。
4. 单击 submit。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。