思科IQ链路操作指南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、在整个环境中提供更智能的见解，并简化案例管理。此外，AI Assistant等AI功能通过提供情景理解来优化运营成果和思科IQ用户体验，使您能够主动做出明智的决策，并简化流程，促进客户参与和成功。

思科IQ Link可安全地从您的内部网络收集资产遥感勘测数据并将其传输至思科IQ，从而支持人工智能驱动的预测性洞察，帮助您提高网络可视性、预测问题并提高运营效率。

本地 认证

帐户管理员应使用以下凭证登录到Cisco IQ Link:

- 默认用户名：admin
- 默认密码：在Cisco IQ Link安装过程中设置的密码；有关详细信息，请参阅Cisco IQ Link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)。

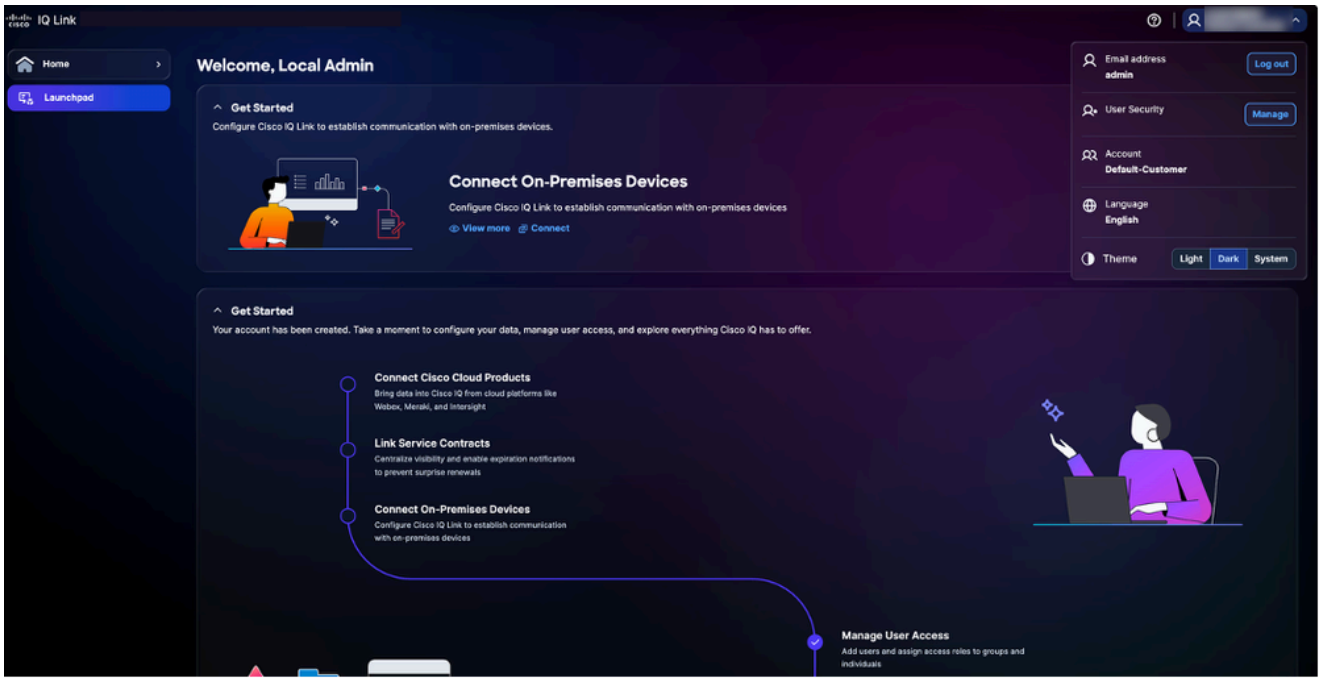
注意：在15分钟内，您有三(3)次尝试输入正确的密码。如果所有三(3)次尝试均失败，您的帐户将临时锁定30分钟以保护您的安全。
在锁定期间无法尝试登录。系统将显示以下消息："由于尝试失败次数过多，帐户被锁定。请稍后重试。"，包括锁定到期的时间。
您的帐户会在30分钟后自动解锁，此时您可能会尝试登录或重置密码。

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。

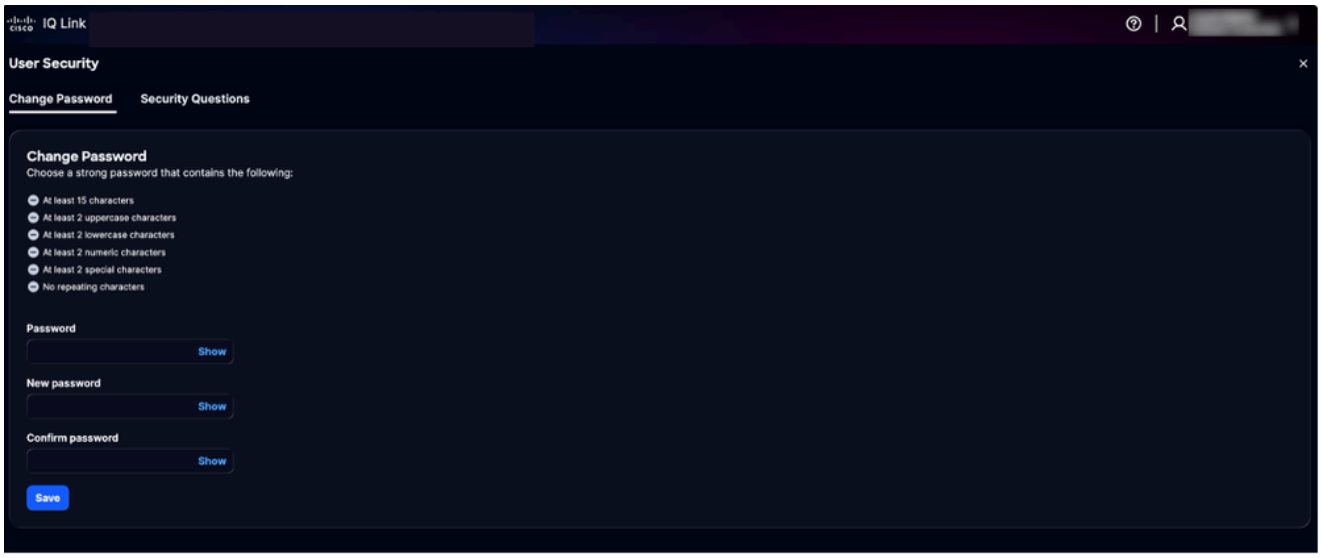
要设置安全问题，请执行以下操作：

1. 在Home(主页)中，点击User Profile（用户配置文件）。此时将打开下拉菜单。



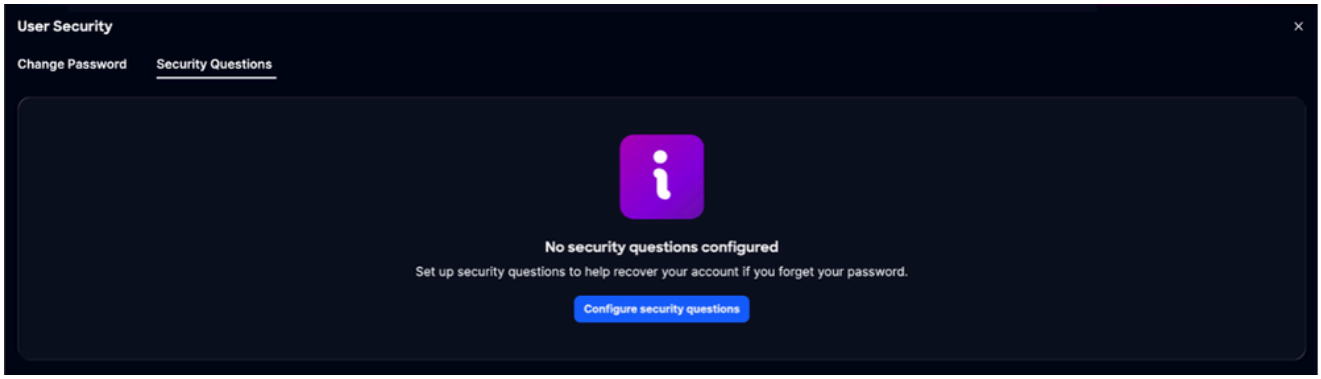
用户配置文件菜单

2. 在用户安全中单击管理。系统随即会显示User Security页面。



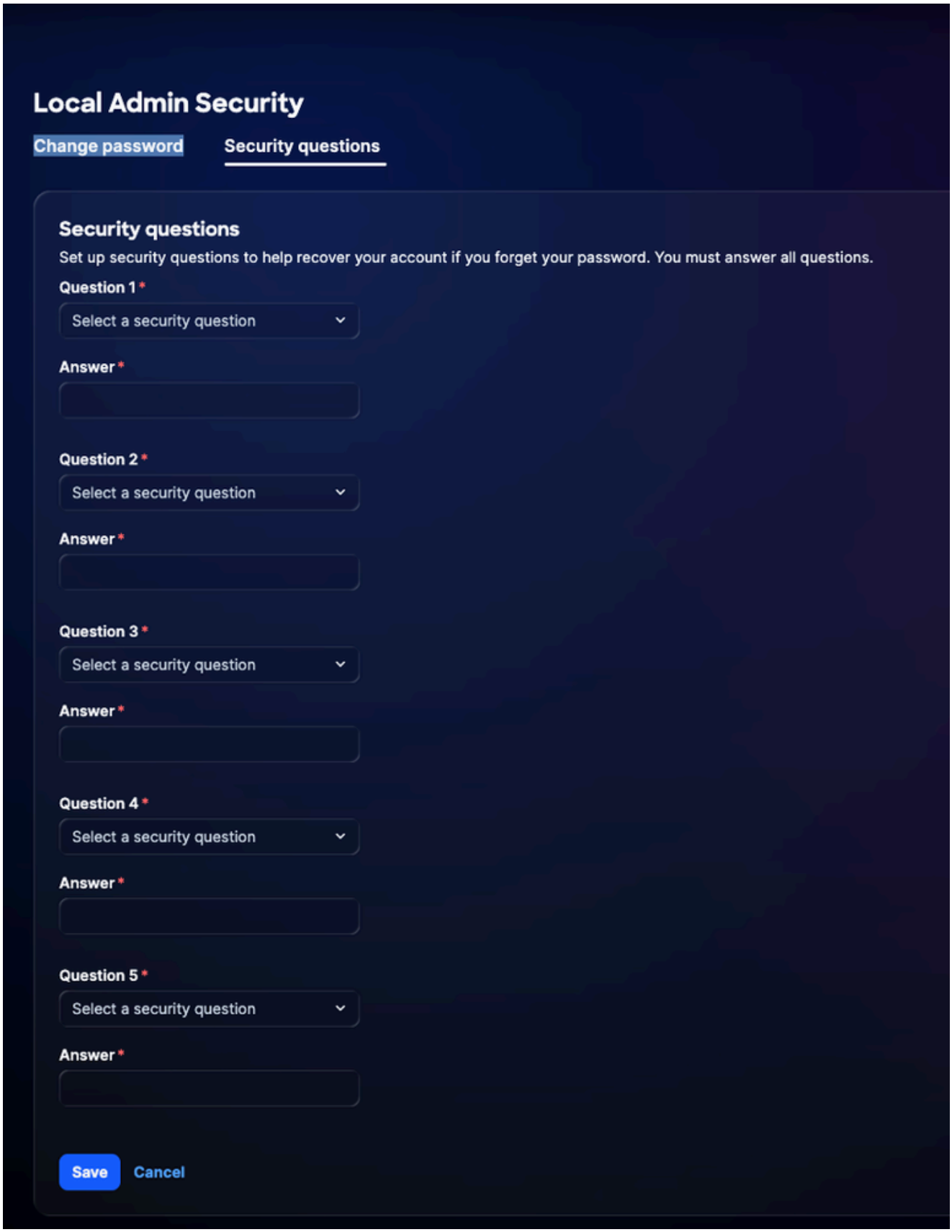
更改密码

3. 单击Security Questions以打开选项卡。



安全问题

4. 单击配置安全问题。



安全问题

5. 从下拉列表中选择任意五(5)个安全问题。
6. 输入每个问题的回答。

7. Click Save.

注意：答案不区分大小写，例如，“SMITH”和“smith”被视为相同。
忽略多余的空格，例如，“Smith”和“smith”被视为相同。

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。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，则禁用密码过期。）

先决条件

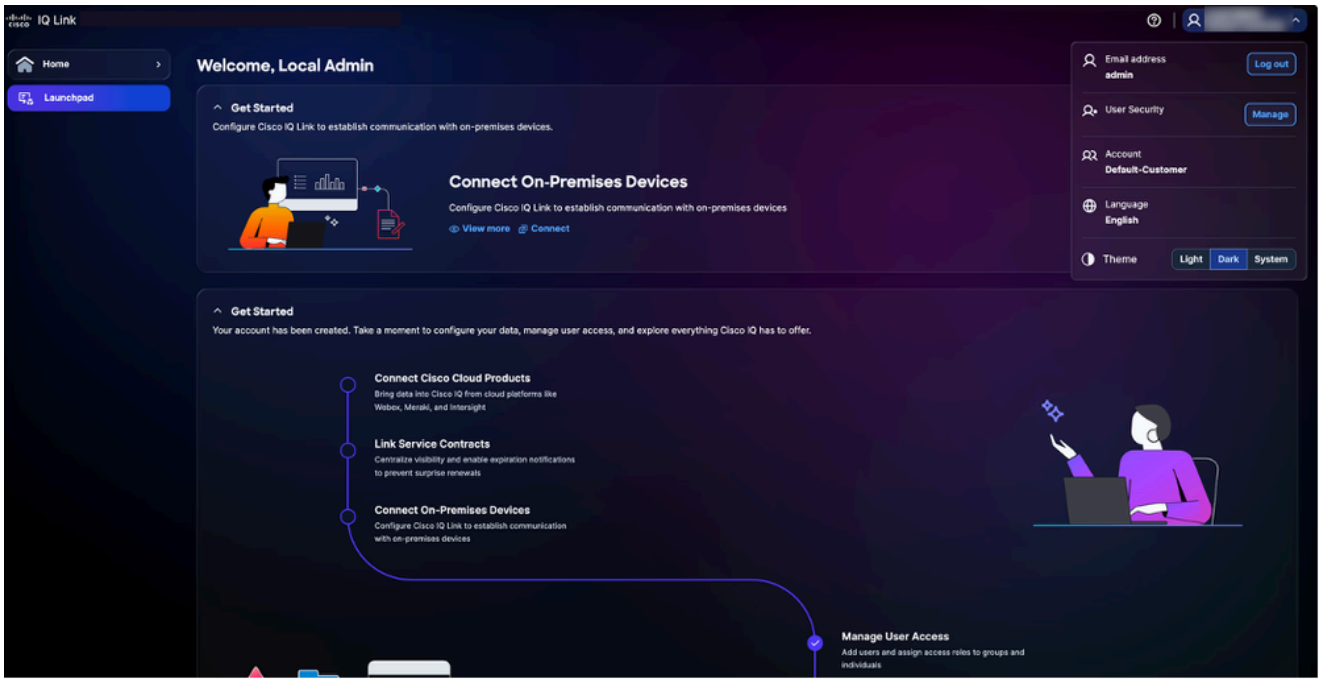
要管理密码，必须满足以下条件：

- 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 Link
- 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Home(主页)中，点击User Profile（用户配置文件）。此时将打开下拉菜单。



用户配置文件菜单

2. 在用户安全中单击管理。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.

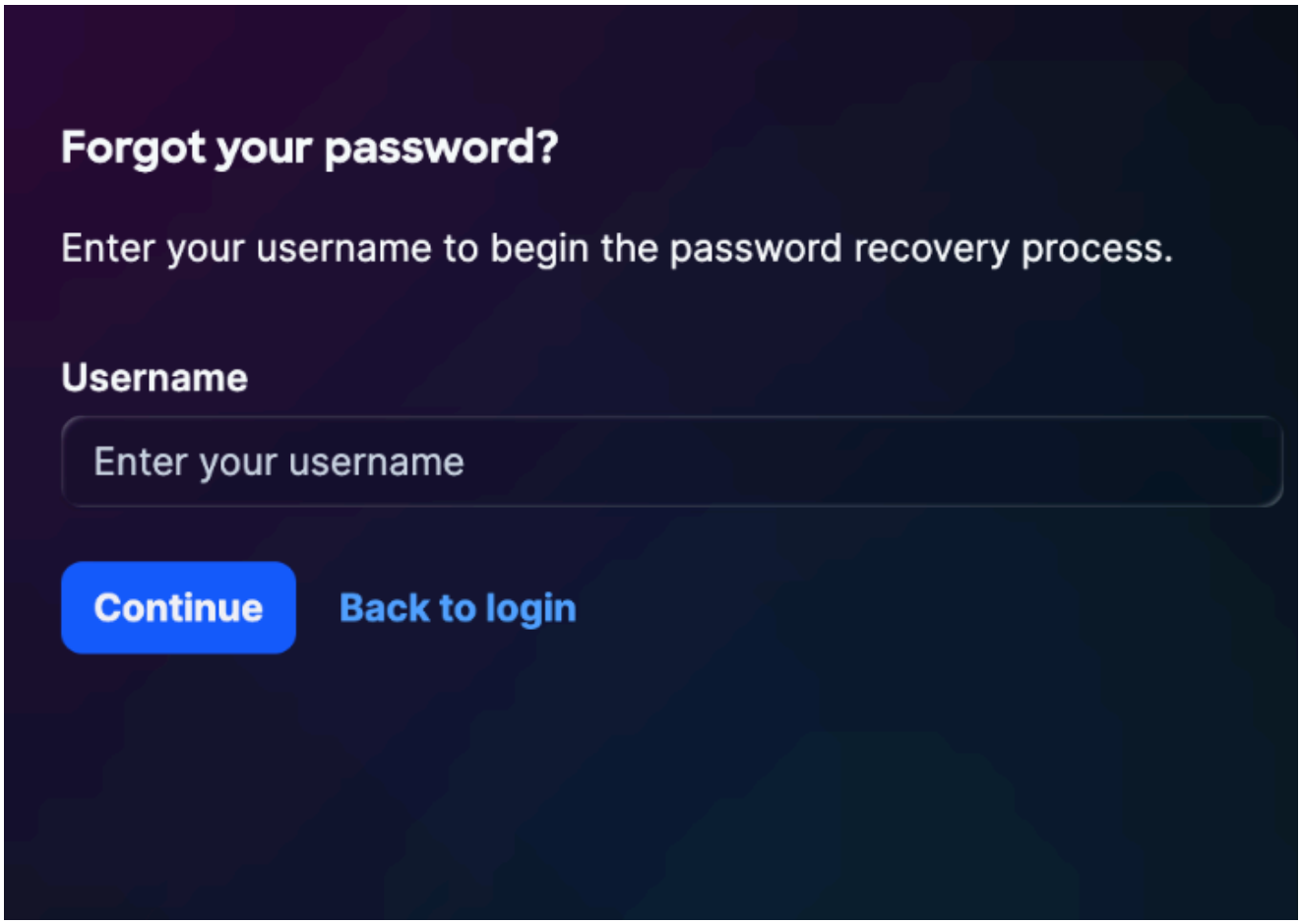
密码在Cisco IQ系统中更新，包括Cisco IQ虚拟机(VM)。

重置忘记的密码

如果之前设置了安全问题，可以使用安全问题验证过程重置忘记的密码。有关详细信息，请参阅设置安全问题和答案。

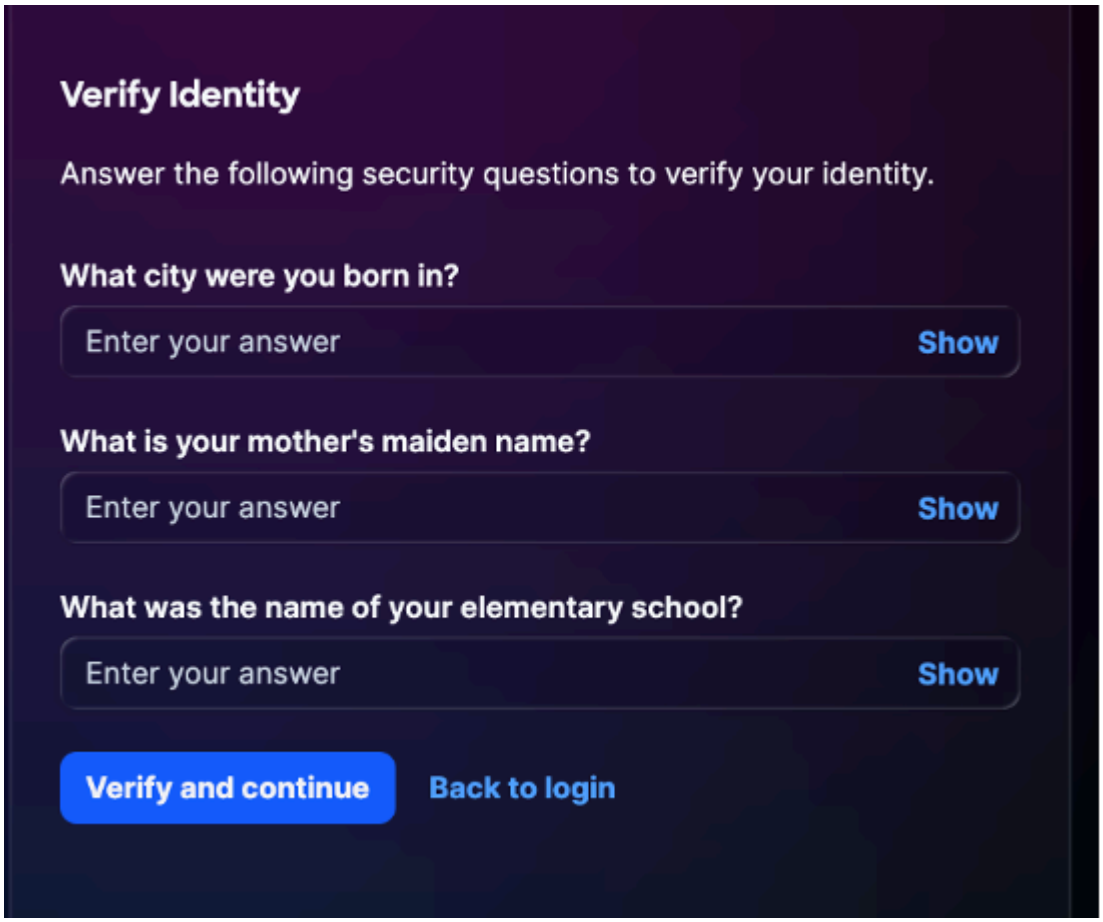
要重置忘记的密码，请执行以下操作：

1. 导航到Cisco IQ Link登录页面。
2. 单击忘记密码。



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。

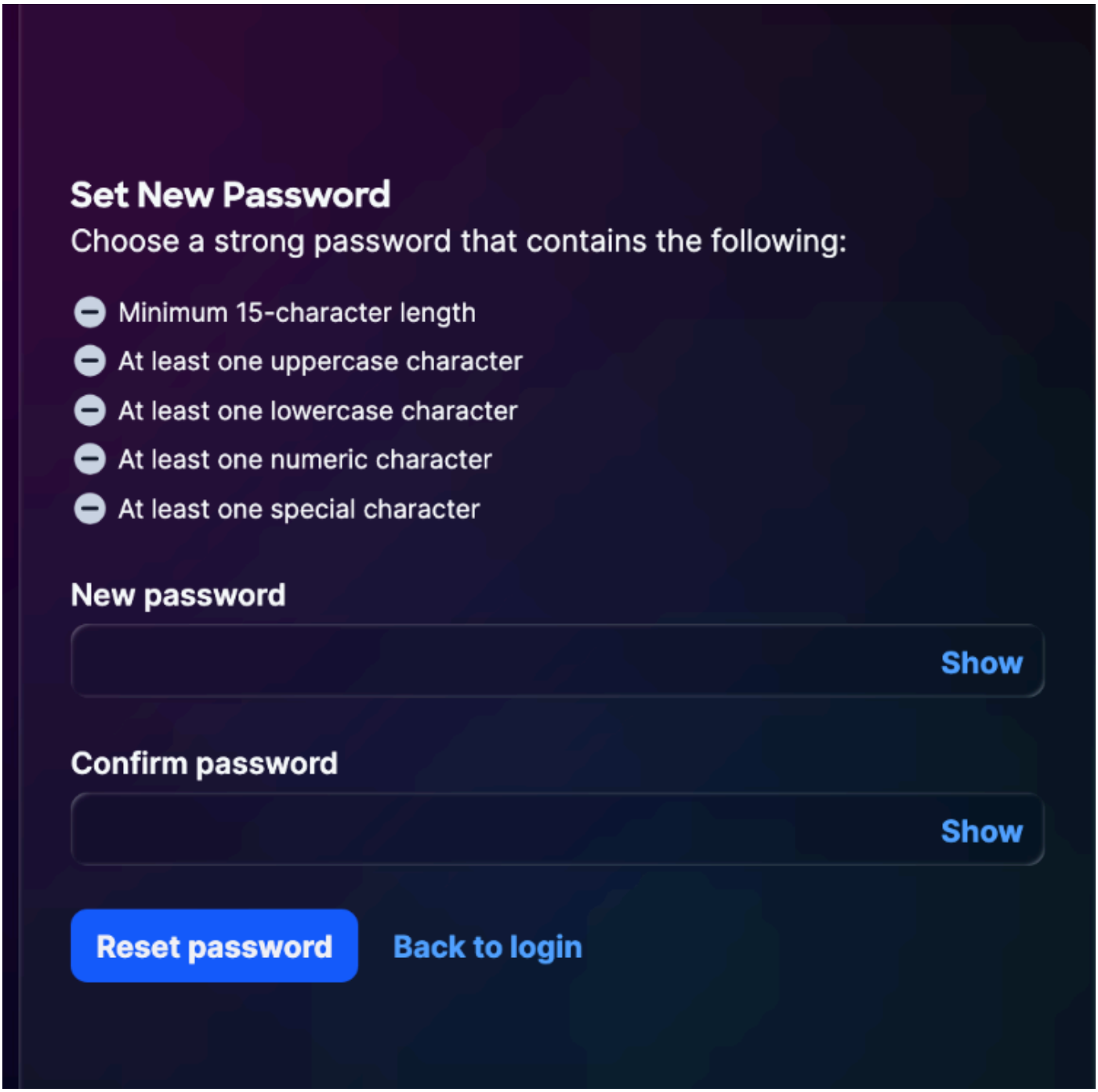


验证身份

注意：上面显示的安全问题是特定于用户的，因用户而异。

5.输入所有三(3)个显示问题的答案。

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。



重置密码

您在15分钟内进行了三(3)次尝试正确回答安全问题。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。您无法在锁定期间重置密码。
系统将显示以下消息：“由于验证尝试失败次数过多，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New password。

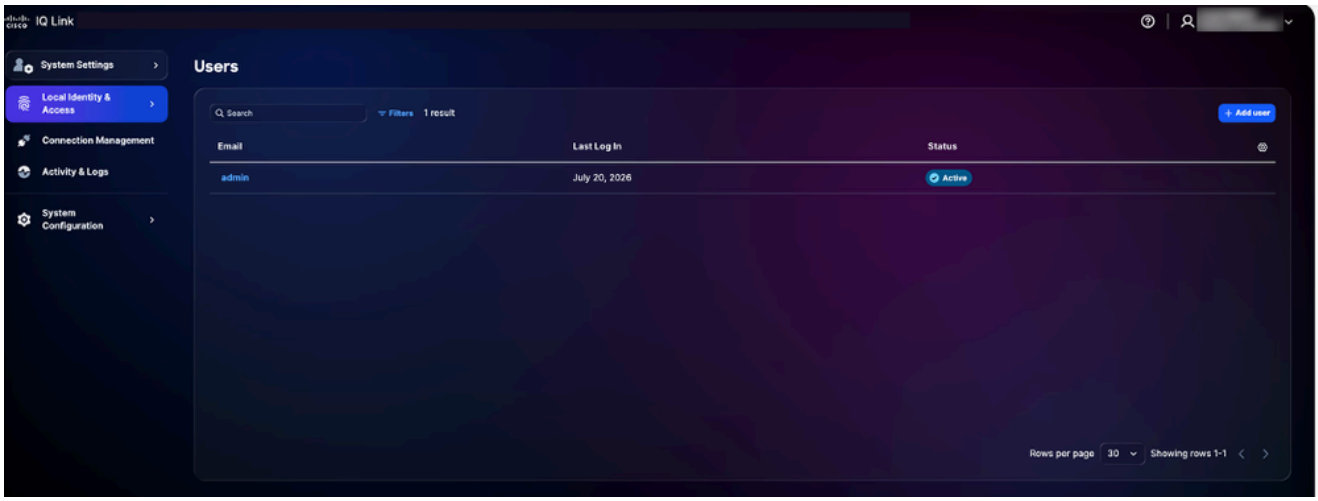
8.再次输入密码进行确认。

9.单击提交。

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：

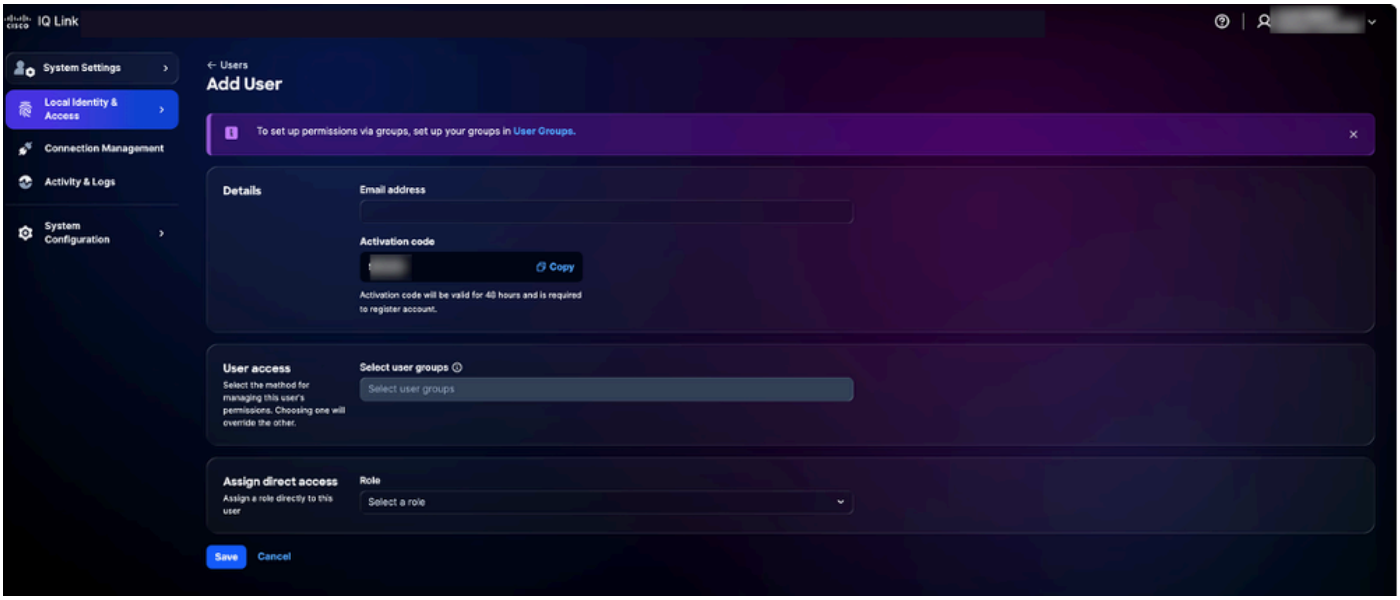
1. 导航到系统设置 > 本地身份和访问 > 用户。系统随即会显示Users页面。它列出所有现有本地用户及其状态。



“用户”页

注意：帐户管理员不显示更多选项图标（如上图所示）。

2.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。根据完成注册的要求，与用户共享。

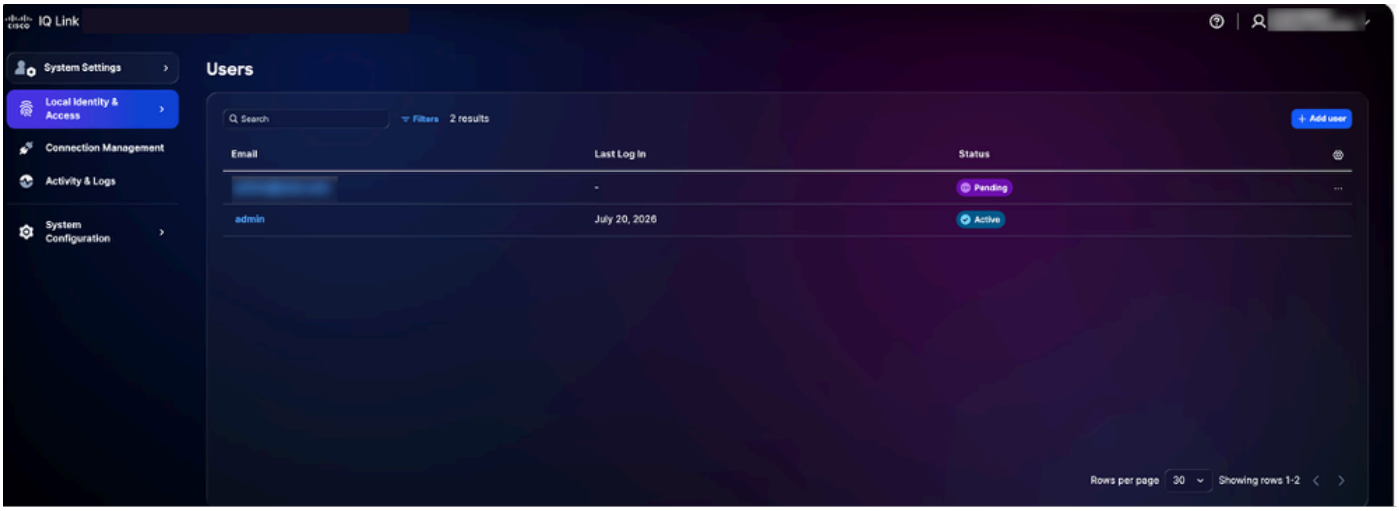
5.在用户访问中，从选择用户组下拉列表中选择用户组。

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：

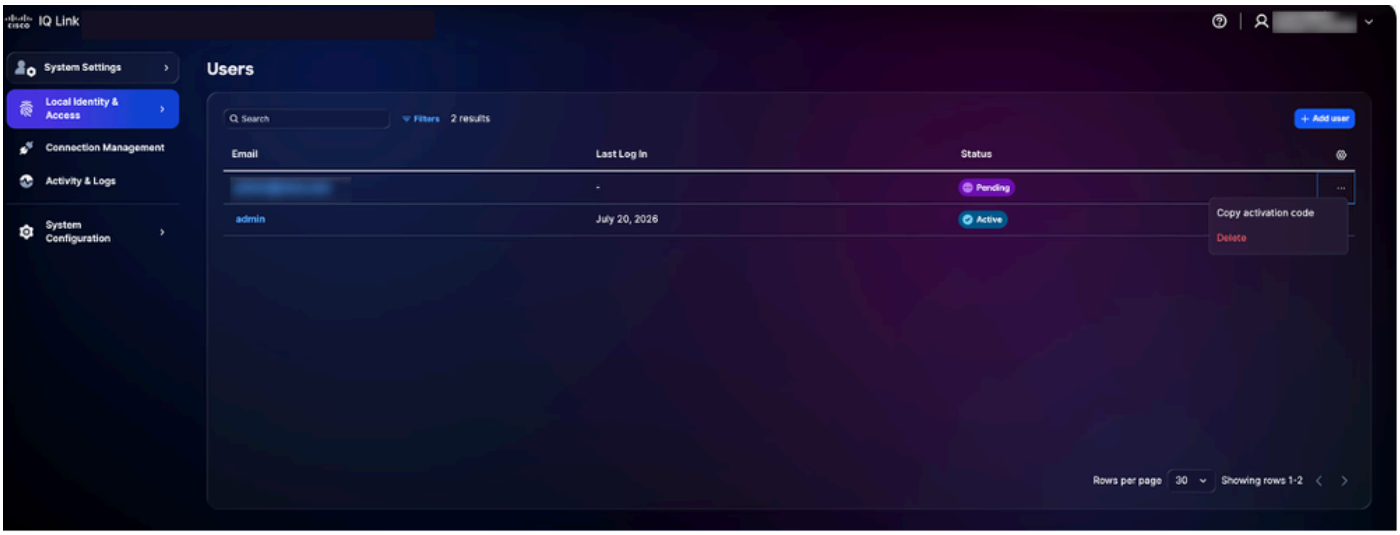
- 查看器:查看和访问应用程序
- 管理员:访问应用并管理系统设置，但系统管理和IDP除外

7.单击保存。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。



新添加的用户

8.在列表中找到新创建的用户，并确认“状态”列显示为待定。



复制激活代码

9.单击More Options图标>复制新创建用户旁的激活代码。激活代码会复制到您的剪贴板。

10.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

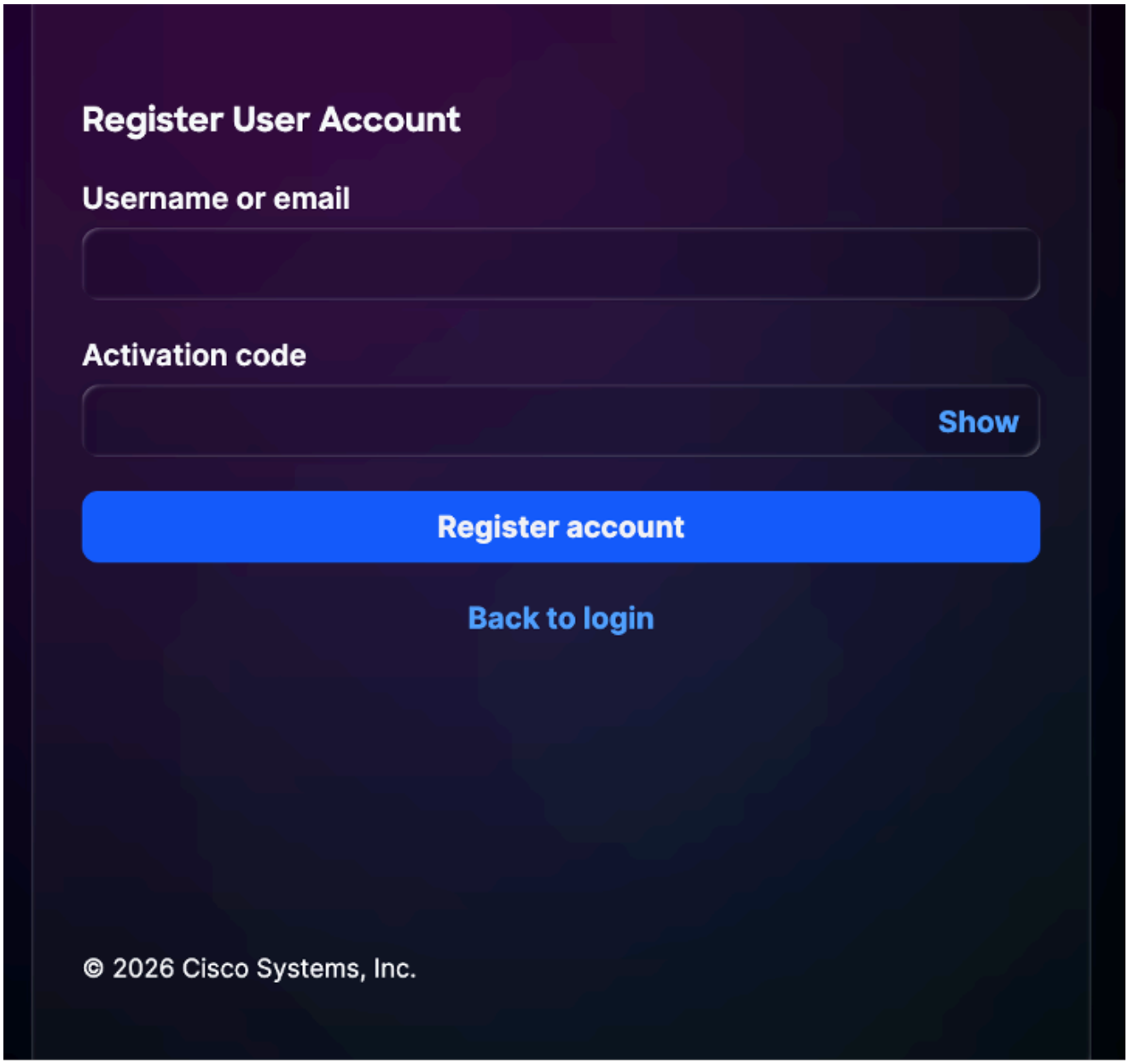
注：激活代码的有效期为48小时。如果您的代码过期，请与您的帐户管理员联系以申请新的代码。

11.要注销，请单击右上角的User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。

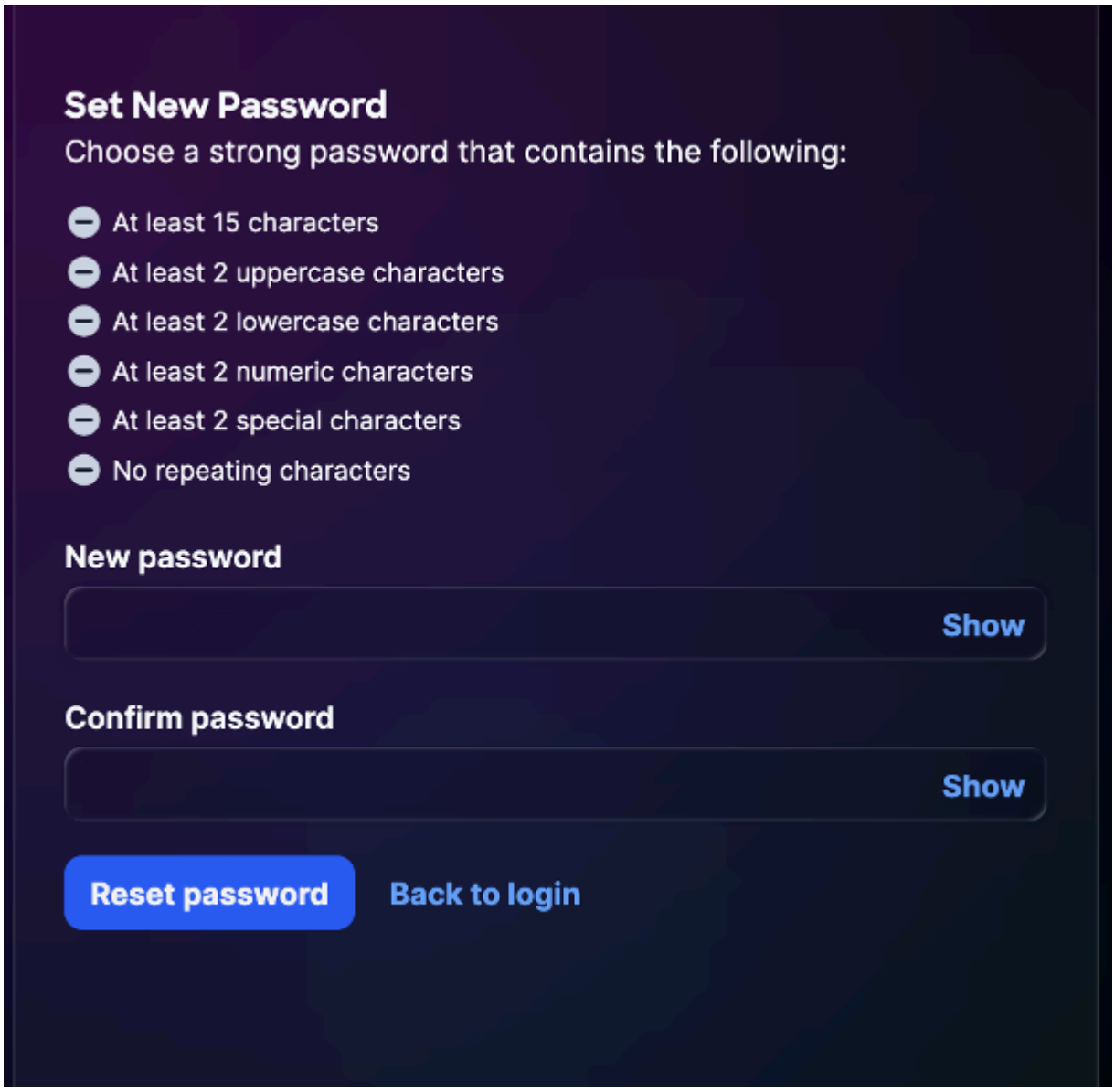


新用户帐户

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。



新用户帐户密码

5. 输入New password。
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(有关详细信息，请参阅设置安全问题和答案)。

管理本地用户组

用户组使帐户管理员能够一起管理多个本地用户的角色。帐户管理员可以创建一个组、附加一个角色和一组用户，并在一个位置更新该角色或成员身份，而不是分别为每个用户分配一个角色。所有用户组管理都从Local Identity & Access页面进行执行。

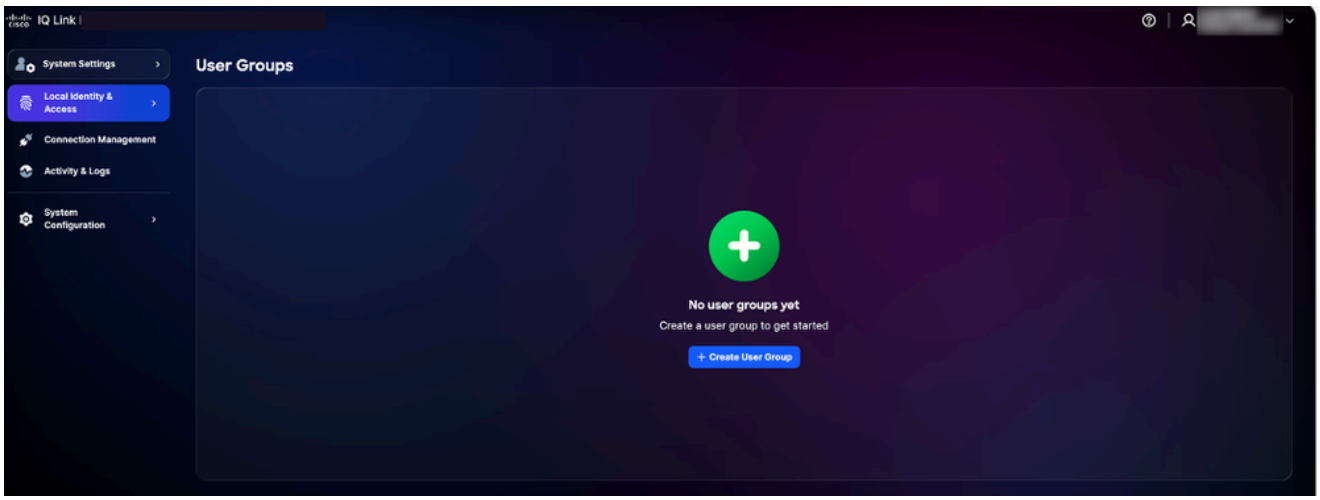
✎ 注意：只有帐户管理员可以创建、编辑或删除用户组。组由现有本地用户组成；必须先创建用

户，然后才能将其添加到组。

创建用户组

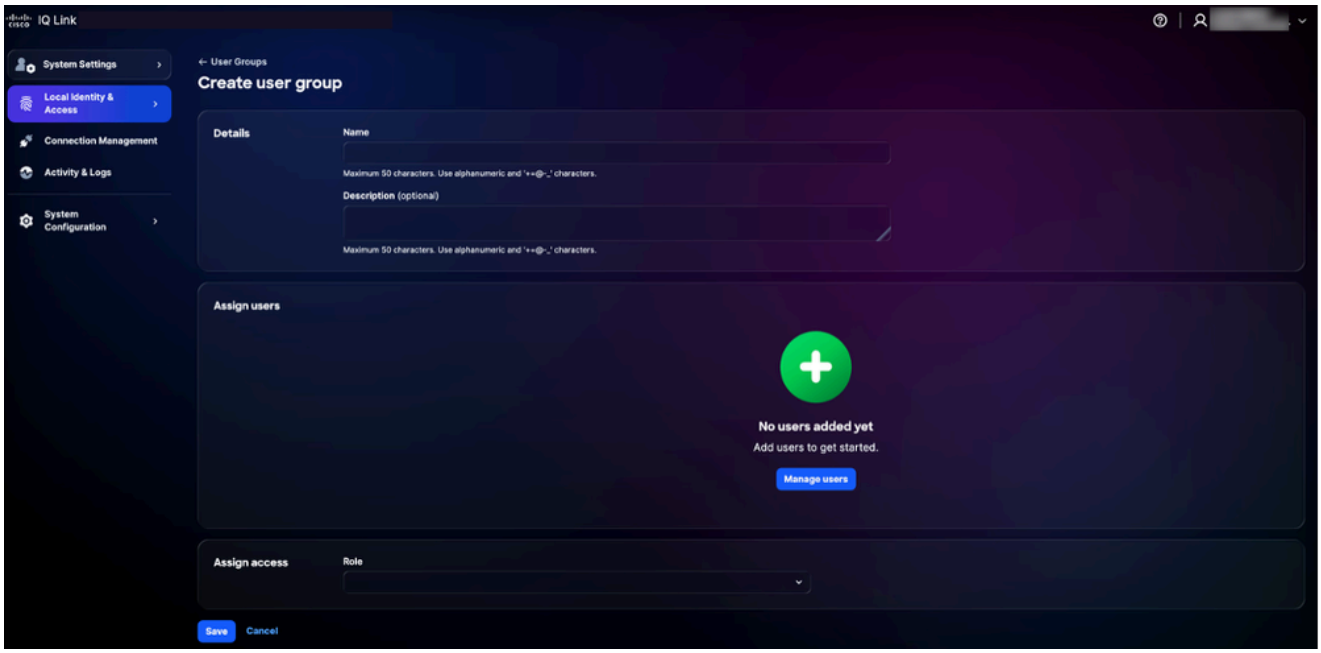
要创建用户组，请执行以下操作：

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+ = @ - _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:查看和访问应用程序（只读）
    - 管理员:访问应用并管理系统设置

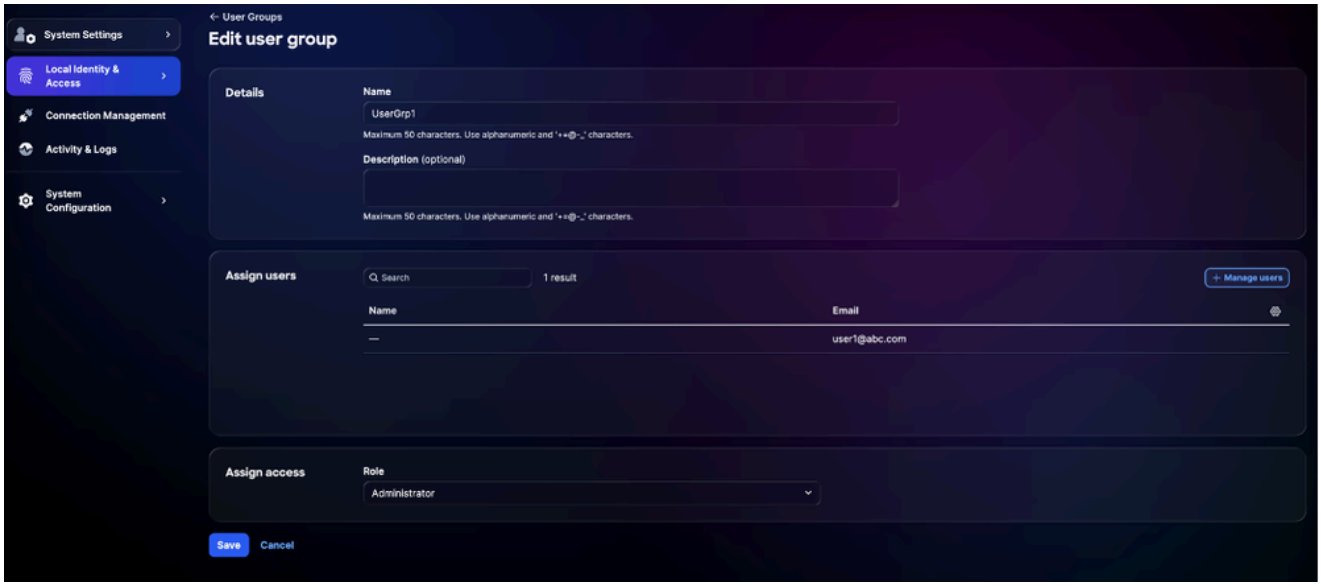
4.单击保存。

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. 点击组旁边的More图标，然后选择Edit。系统将显示“编辑用户组”页。



编辑用户组

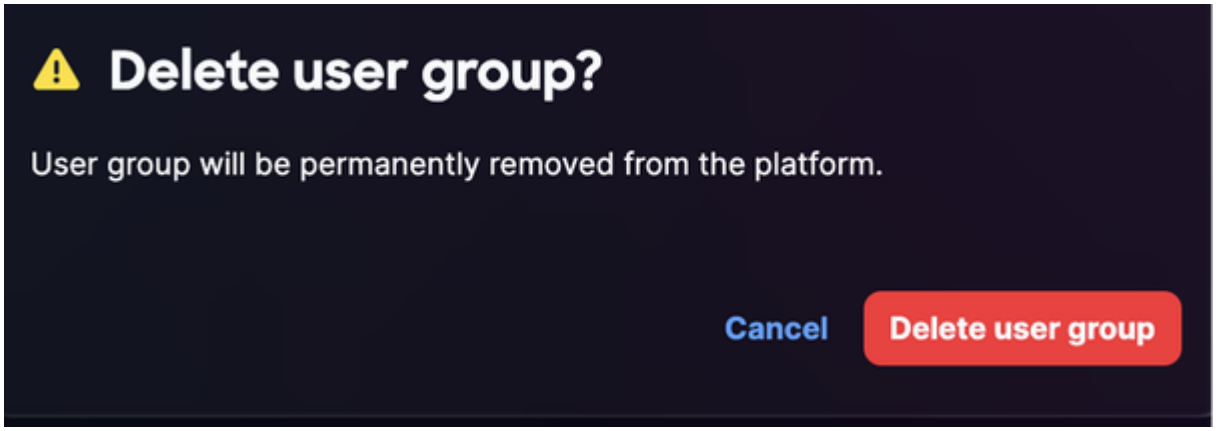
3. 进行所需的更改。
4. Click Save.

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。



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Cisco IQ Link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身份提供程序(IDP)配置登录到Cisco IQ链接。

SSO的Okta IDP SAML配置

配置IDP SAML的先决条件

- 本地帐户管理员访问Cisco IQ链路的权限
- 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。

2.为Cisco IQ Link实例设置以下属性。
表 1：Cisco IQ链路属性

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
受众	非员工
入职类别	选择“New Onboarding”

表 2：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断言消费者服务(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

3.配置以下必需属性语句。

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：.*

4.配置应用程序中的单一注销(SLO)设置。

表 3：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

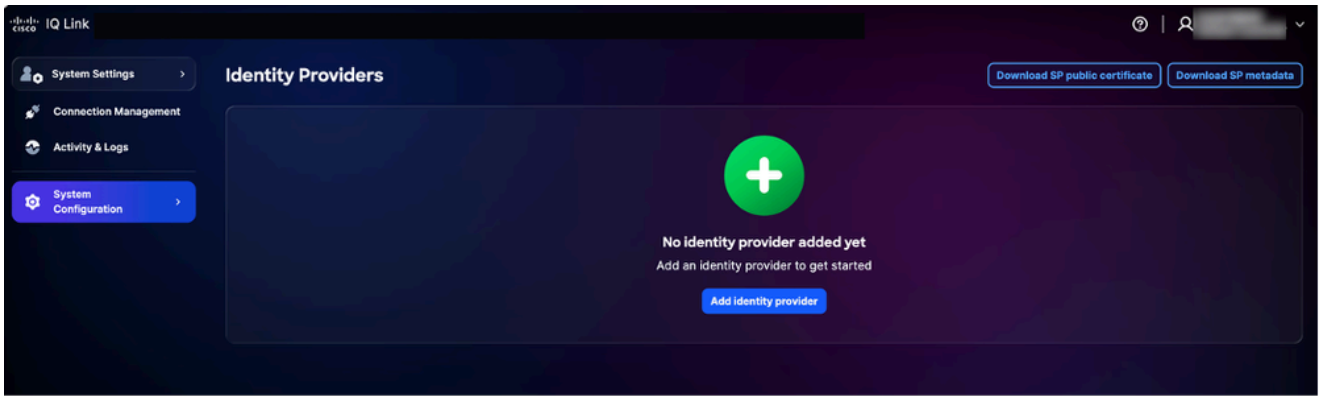
5.单击Download图标下载“SP元数据”文件。

6.按提供商的要求调配或创建应用程序。

添加Okta IDP

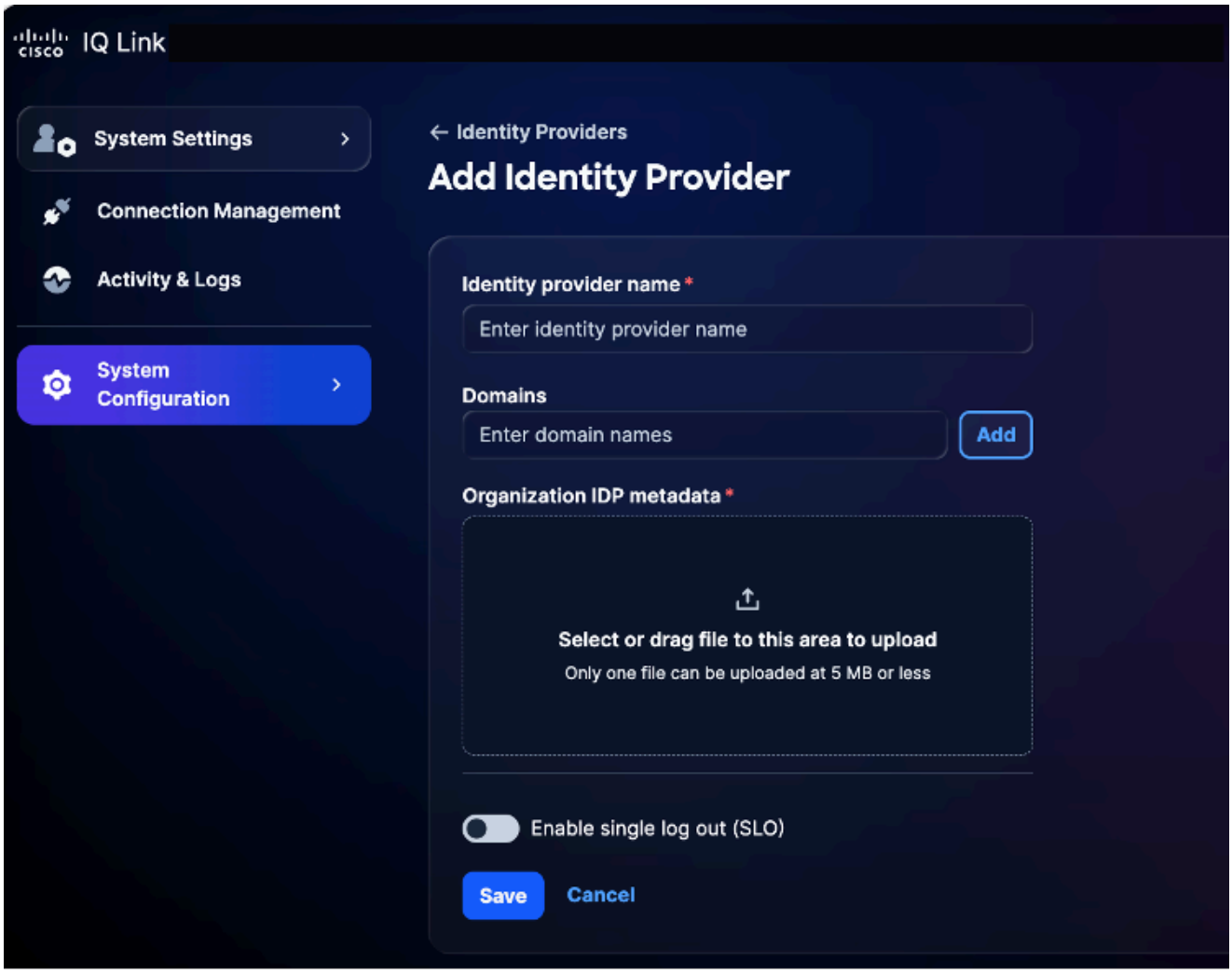
要在Cisco IQ链路中添加IDP，请执行以下操作：

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



IDP主页

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



添加身份提供程序

注意：在给定时间只能添加一(1)个IDP。

3.输入身份提供程序名称。

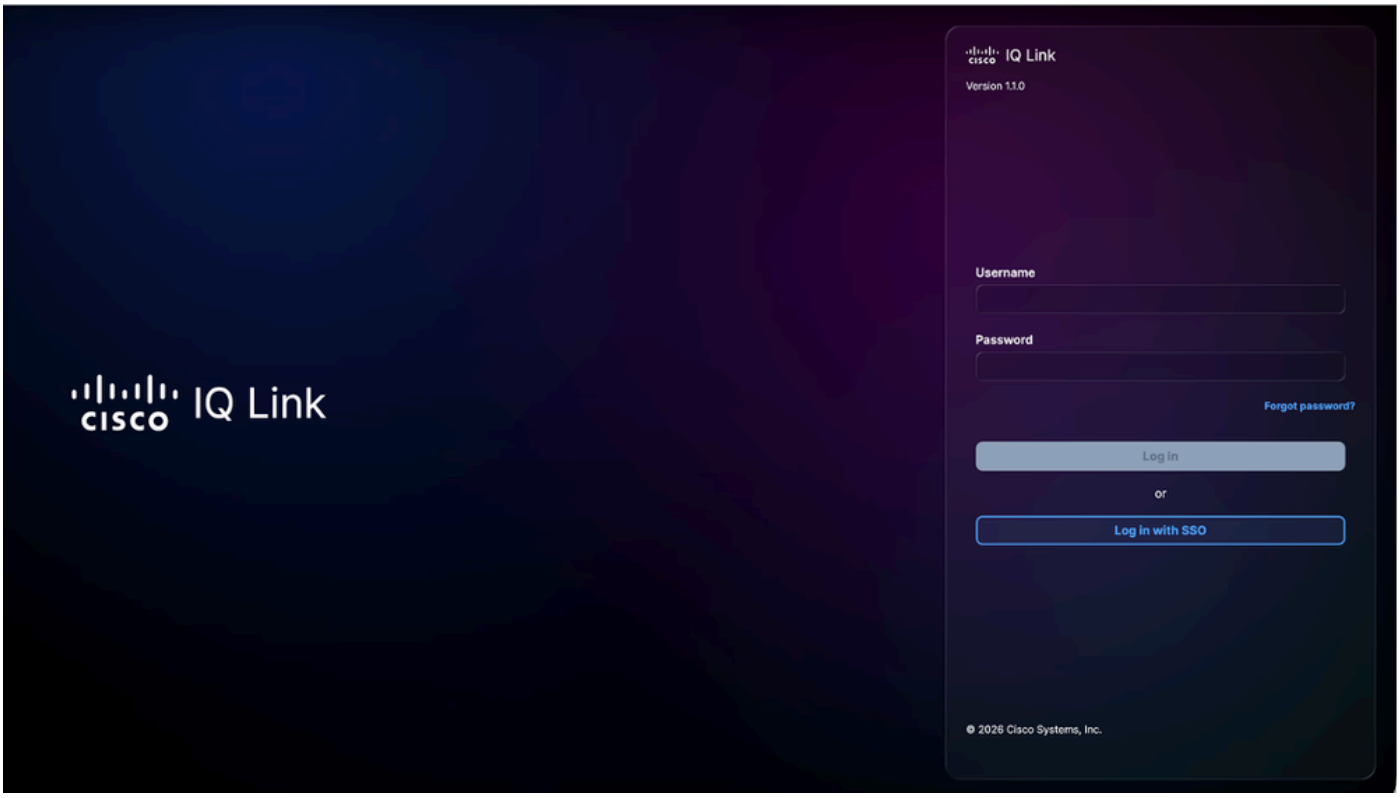
4.单击Add将已配置的Cisco IQ Link域名添加到Domains字段。

5.在组织IDP元数据字段中拖放或上传从IDP应用获取的SAML元数据文件。此文件包含证书详细信息和服务提供商(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.单击保存。

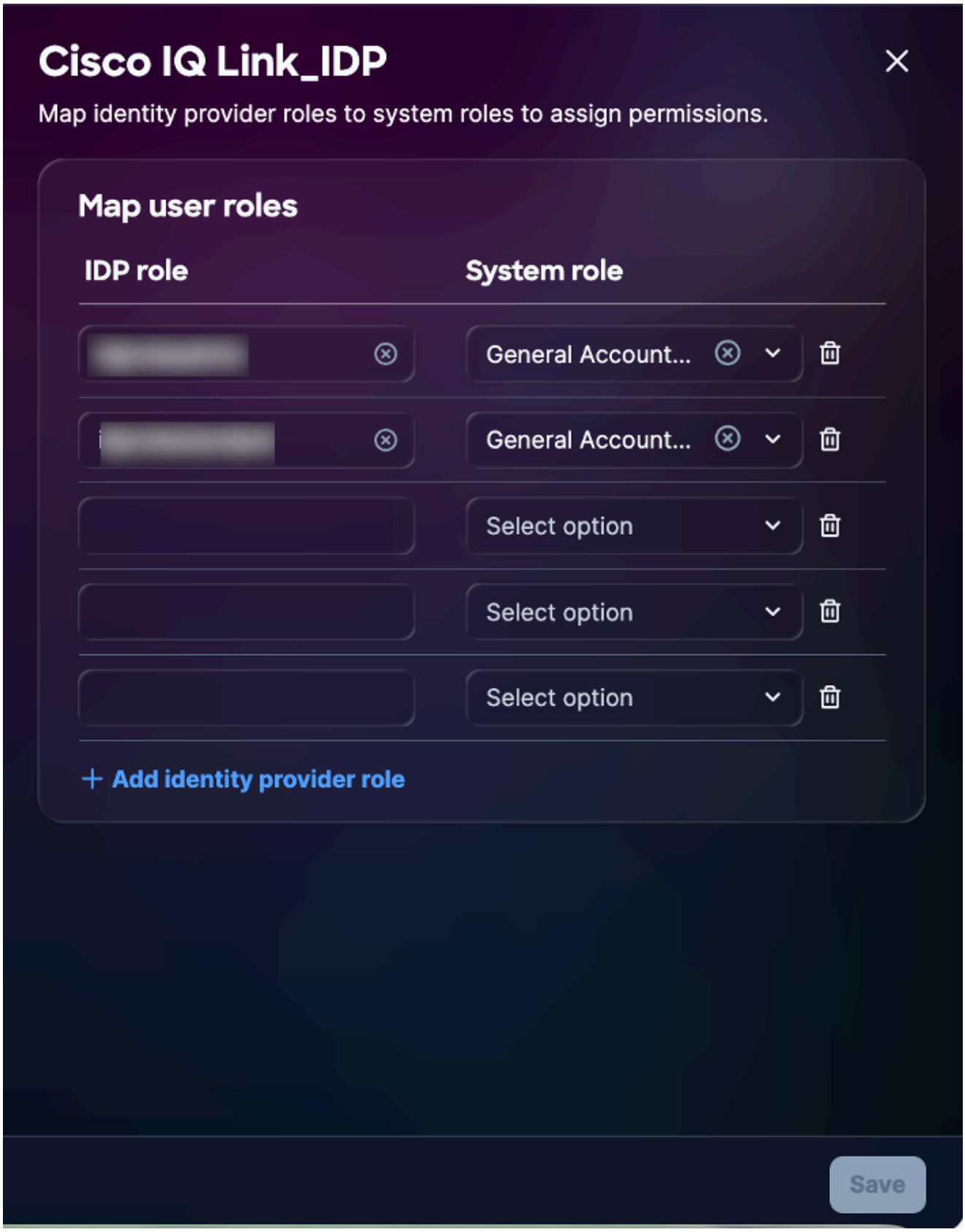
配置后，登录页面会显示一个选项，用于通过IDP登录SSO。



Cisco IQ链路登录

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。



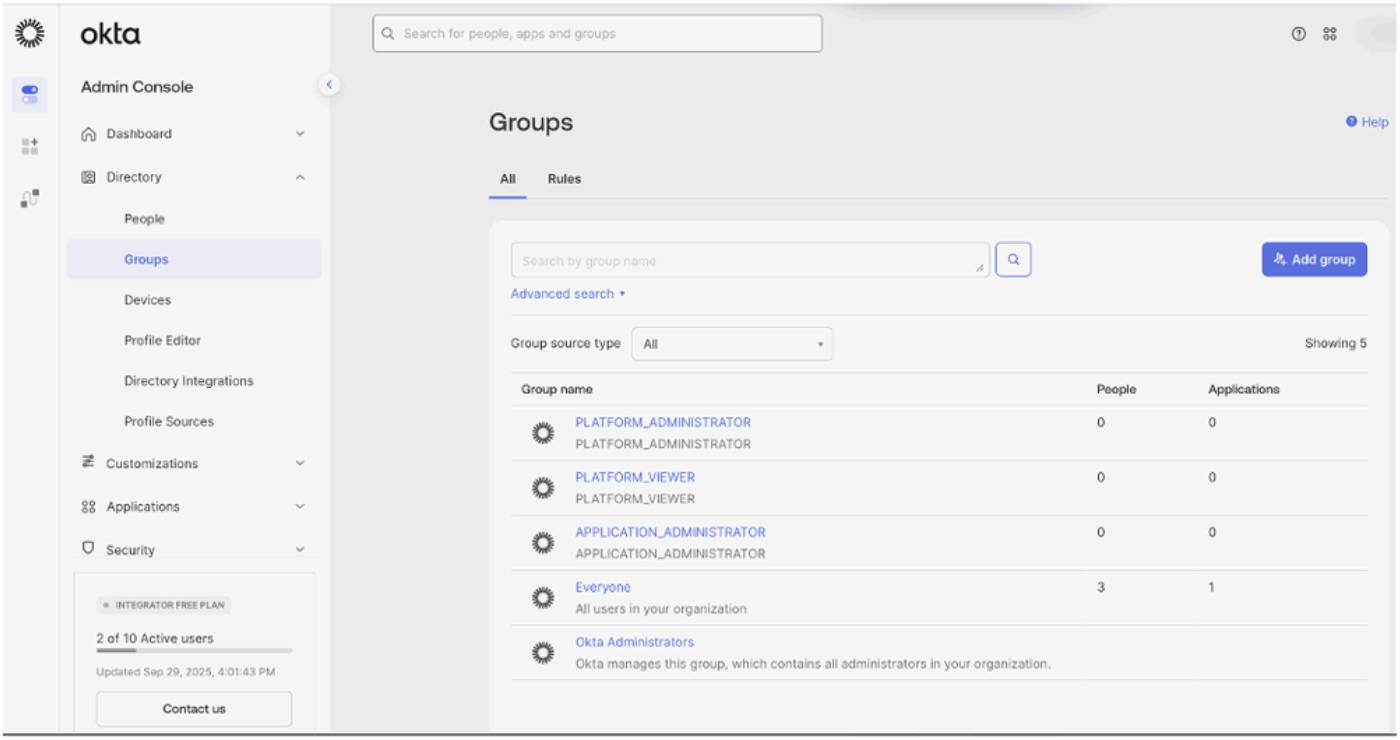
用户角色映射

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者角色根据需要映射其他角色。

4.单击保存。

单一注销配置

如果选择启用单一注销配置(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. 从身份提供程序页面，单击下载SP公共证书。

下载公共证书

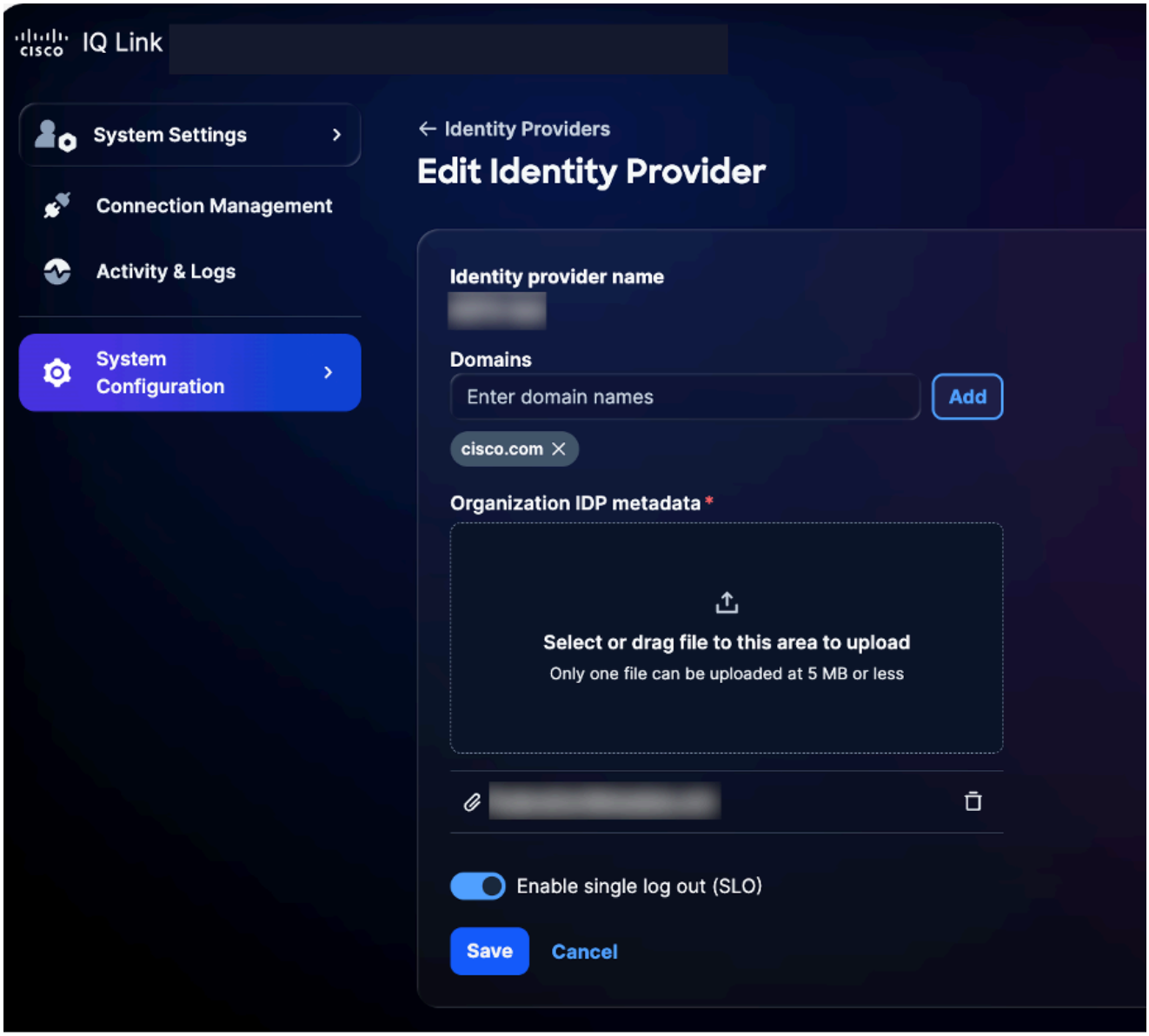
2. 将下载文件另存为sp-public-key.crt。

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. 再次下载IDP元数据文件。

6. 在Identity Providers页上，选择添加的IDP的More Options图标> Edit。



编辑身份提供程序

7. 打开Enable single log out(SLO)切换按钮。
8. 上传新下载的元数据文件。
9. 使用以下核对表验证SSO和SLO功能：

验证核对表：

- 本地帐户管理员登录成功
- 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/SLO流

排除IDP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IDP状态、证书错误、SSO登录失败和SLO配置相关的问题：

表 4：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(ADFS)配置为Cisco IQ的SAML IDP的指导。

为SSO配置ADFS IDP SAML的先决条件

- 建议使用ADFS 6.0+
- Windows Server 2012 R2+
- 配置的AD集成
- ADFS上的SSL/传输层安全(TLS)证书
- 帐户管理员访问Cisco IQ
- 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
- ADFS服务器配置详细信息（如下表所示）

表 5：ADFS服务器配置

项目	描述	示例
思科IQ FQDN	用户部署主机名	devxx-23.cx-xxx-xxx.cisco.com
ADFS服务器URL	用户ADFS服务器地址	https://ad-fs.dev.local
公司域	电子邮件域	company.com
AD组	AD组域名(DN)	CN=Role - CXIQ开发人员

配置ADFS服务器

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目录（例如，C:-certificate.crt）。
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 从文件中导入有关信赖方的数据，以从作为步骤3的一部分保存的文件中获取详细信息。
10. 单击Browse以选择SP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“CIQ-Stage”），添加任何相关备注，然后点击Next。
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重身份验证(MFA)适配器(例如，已配置Azure MFA或*基于时间的一次性密码(TOTP))，否则不要选择“允许每个具有MFA的用户”。
如果未配置任何MFA提供程序而启用此策略，ADFS将对用户进行身份验证，但最终会拒绝状态为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
```

要设置“允许所有人”（无MFA要求），请运行以下命令：

```
Set-AdfsRelyingPartyTrust -TargetName “

     ” -AccessControlPolicyName “Permit everyone”
```

您还可以通过PowerShell创建信赖方信任：

```
Add-AdfsRelyingPartyTrust `
    -Name “

     ” `
    -Identifier “

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

       ”) `
    -AccessControlPolicyName “Permit everyone” `
    -IssuanceAuthorizationRules ’=> issue(Type = “http://schemas.microsoft.com/authorization/claims/per
```

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 6：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	公钥基础设施(PKI)/证书身份验证	ADFS通过用户主体名称(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 - Stage”）。

```
$relyingPartyName = “Cisco IQ - Stage”
```

2.定义将用户信息和组成员身份发送到Cisco IQ的声明规则。

```
$claimRules = @’

@RuleTemplate = “LdapClaims”

@RuleName = “Send Email and Name”

c:[Type == “http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname ”, Issuer == “AD
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/ws/2005/05/identity/claims/em

@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.Iss

@RuleName = “Send Group Membership”
c:[Type == “http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname ”, Issuer == “AD
```

```
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/claims/Group”), query = “;mem
’@@
```

3.通过运行以下命令应用索赔规则：

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

Write-Host “Claim rules configured successfully!” -ForegroundColor Green
```

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. 设置用户名以检查用户的组成员身份。

```
$username = “testuser”
```

2.运行以下命令查找用户帐户：

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

$user = $searcher.FindOne()
```

3.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.选择以下选项之一：

注意：SP证书由内部证书颁发机构(CA)颁发，ADFS无法通过标准信任链进行验证。

- 全局为此信赖方禁用链验证

```
Set-AdfsRelyingPartyTrust `
    -TargetIdentifier “


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

或者

- 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:-iq-onprem-ca.cer” -CertStoreLocation “Cert:”
```

3.通过重新启动ADFS服务应用更改。

```
Restart-Service 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.运行以下命令进行安装：

```
certutil -ca
```

5.通过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, Thumbprint, NotAfter -AutoSize
```

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：

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

Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificatetransport

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

Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificatetransport
```

2.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 AddressPath, Enabled, Proxy -AutoSize
```

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”, “FormsAu
-PrimaryExtranetAuthenticationProvider @(“CertificateAuthentication”, “FormsAuthentication”, “Microsoft
```

2.使用以下命令验证两个列表是否都包括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TlsClientPort未启用，49443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CERT_E_UNTRUSTEDROOT(0x800B0109)错误，这些错误会阻止证书身份验证工作。

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=

     :49443 `
    certhash=

        `
    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：

```
netsh 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:
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 7：Schannel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SystemCertificatesstore中，以确保正确识别该证书。

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LocalMachinestore中已存在CA证书：

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

如果未找到证书，请将其导入到LocalMachinestore:

```
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 Metadata”}).FullUrl
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。
2. 用ADFS服务器的主机名替换<your-adfs-server>。
3. 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。

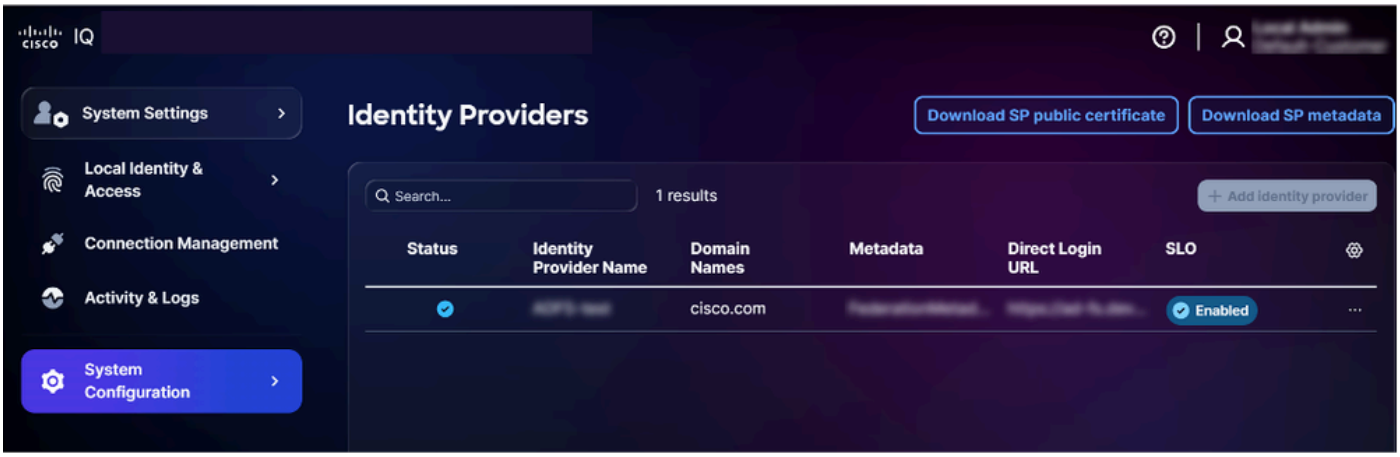
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = “(&(objectClass=group)(cn=Role - CXIQ*))”
$searcher.PropertiesToLoad.Add(“distinguishedName”) | Out-Null
$searcher.PropertiesToLoad.Add(“cn”) | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties[“distinguishedname”]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

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开发人员，OU=Groups，DC=dev，DC=example，DC=com CN=Role - CXIQ Viewers，OU=Groups，DC=dev，DC=example，DC=com

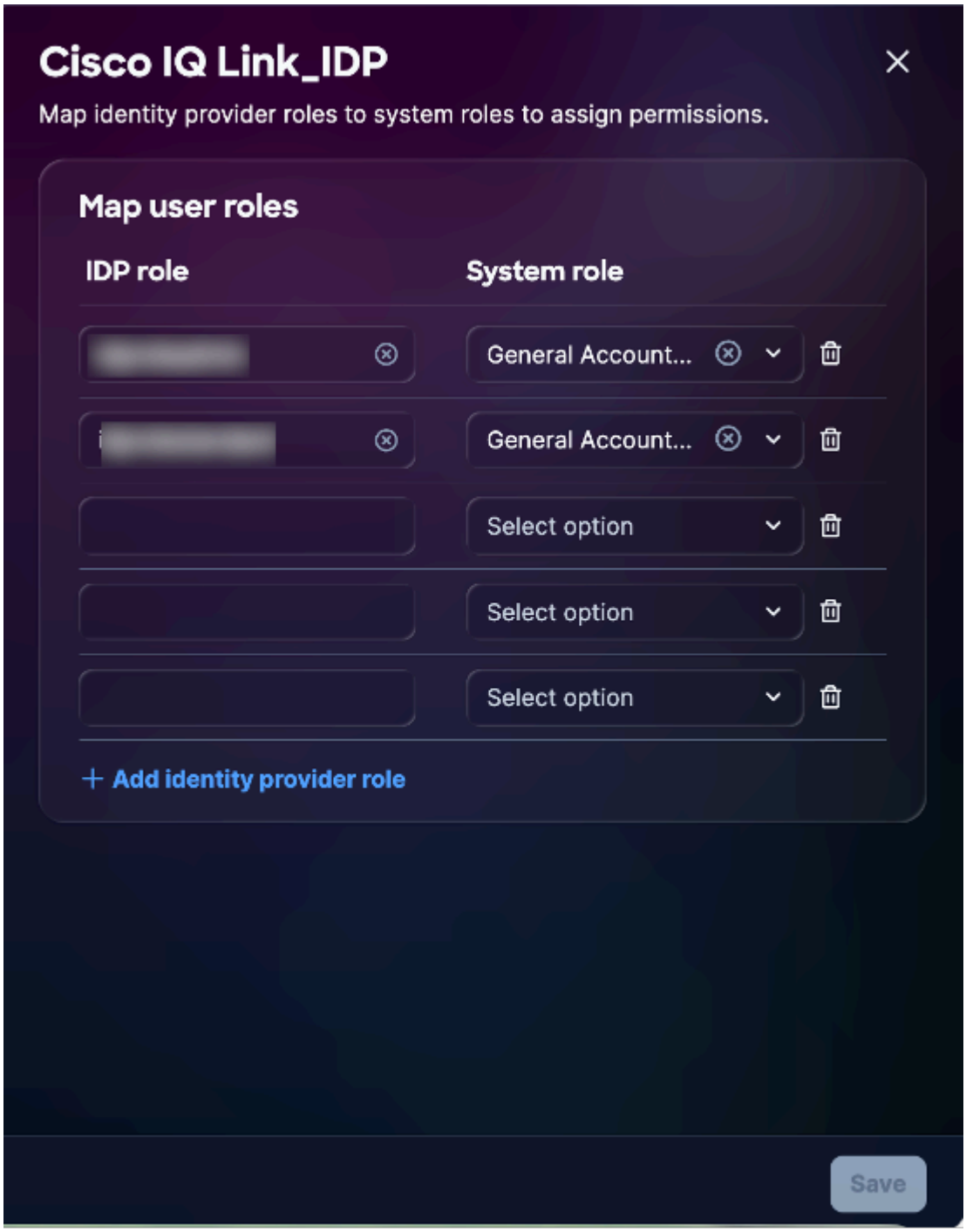
如果未列出所需的组，则必须在帐户管理员在AD中创建这些组，然后才能完成ADFS角色映射。

要配置角色映射，请执行以下操作：



映射角色

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。



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）而不是完整的域名。

3.单击保存。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，请确保用户证书已安装在macOS密钥链中(有关详细信息，请参阅配置基于证书的身份验证下的"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. 选择证书身份验证。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. 确认登录成功。

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8 ：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 • 错误的组属性:必须为http://schemas.xmlsoap.org/cla ims/Group • 用户不在AD组中
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 - Stage” | 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 - Stage” | 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和PKI/基于证书的身份验证(CBA)。

为SSO配置Entra ID SAML的必备条件

- Microsoft 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9 ：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

项目	描述	示例
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)(集成在画廊中找不到的所有其他应用程序（非画廊）)。
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。您可以通过从虚拟设备(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。上传成功后，SP元数据文件中的数据将自动填充到基于SAML的单点登录屏幕中。

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：

1. 在企业应用中，导航到单点登录并选择SAML。
2. 在基本SAML配置部分中，单击编辑，然后输入以下内容：
    a. 标识符（实体ID）:<YOUR-CIQ-FQDN>
    b. 回复URL(ACS URL):https://<YOUR-CIQ-FQDN>/saml/acs
    c. 登录URL:https://<YOUR-CIQ-FQDN>/saml/login
    d. 注销URL:https://<YOUR-CIQ-FQDN>/saml/logout
3. 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。

4.要配置SAML属性和声明，请在属性和声明部分中单击编辑。

5.配置以下声明：

表10 ：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/claims

领款申请	源属性	命名空间
givenname	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
姓	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
名称	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
组	user.assignedroles	（EMPTY — 清除命名空间）

注意：对于组声明：
— 使用user.assignedroles作为源 — 不 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. 导航到身份 > 应用 > 应用注册。
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、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，转至单点登录 > SAML签名证书部分。
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. 请注意设置部分中的以下值：

- 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11 ：系统角色

系统角色	IDP角色（应用角色值）	描述
普通帐户管理员	CXIQ管理员	所有操作的完全权限
常规帐户查看器	CXIQ开发人员	只读访问
常规帐户查看器	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App Role Value字符串(有关详细信息，请参阅配置Entra ID SAML应用下的“配置应用角色”)。

3.单击保存。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，并且是否显示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 successful|Extracted group|To
```

预期输出

```
SAML 2.0 compliant authentication successful for user: user@domain.com with full name: N/A and 1 groups
Extracted group: CXIQ Admins (original: CXIQ Admins)
Total groups extracted: 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

- Windows Server，带AD证书服务(CS)，配置企业CA（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.将<USER-UPN>替换为您的Entra ID 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
```

在客户端计算机上导入用户证书(macOS)

- 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 -P "


     "
```

- 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，然后点击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登录页面上，输入用户的电子邮件并单击下一步。

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12 ：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Entra ID SAML应用下的配置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，请参阅配置Entra ID SAML应用下的“将用户分配给应用角色”(Assigned Users to App Roles))。
重复的组领款申请	user.groups和user.assignedroles均处于活动状态	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Entra ID SAML应用下的配置应用角色)。
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，请参阅实验室环境的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，请参阅配置基于证书的身份验证下的导入客户端计算机上的

问题	原因	修复程序
		用户证书(macOS))，使用所需设置在Entra ID中启用CBA(有关详细信息，请参阅配置基于证书的身份验证下的在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	在插件配置中增加clock_skew_seconds(默认值为300，实验使用30000)。
VA中的“未完成”状态	尚未配置角色映射	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中添加身份提供程序
- 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
- 签发用户证书与UPN匹配的Entra ID用户
- 将用户证书导出为PFX并在客户端计算机上安装
- 信任客户端计算机上的CA证书

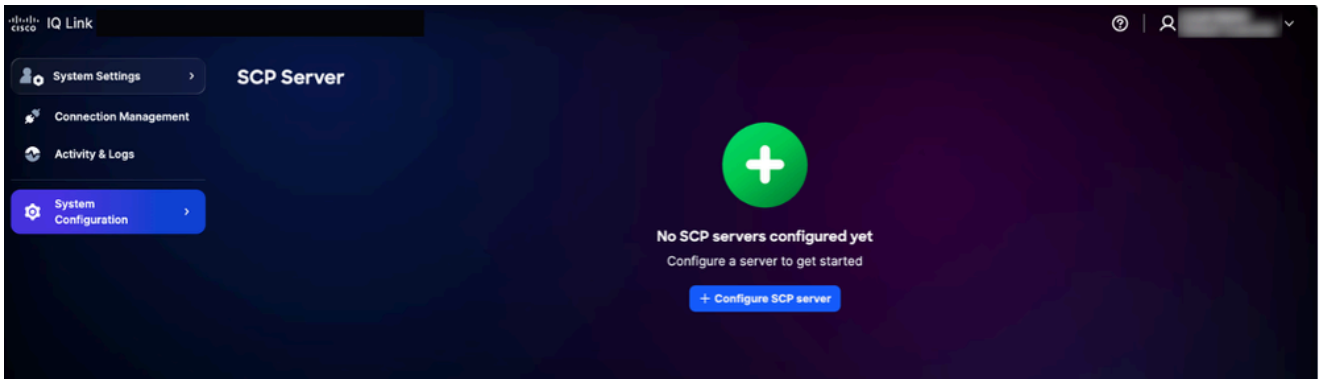
- 在Protection > Certificate authorities下将CA根证书上传到Entra ID
- 在身份验证方法中启用CBA
- 配置用户名绑定(PrincipalName和userPrincipalName)
- 验证CBA登录端到端正常工作

添加SCP服务器

此安全复制协议(SCP)服务器是导入升级文件的必备条件，这些文件对于添加、升级或修补思科IQ安装至关重要。

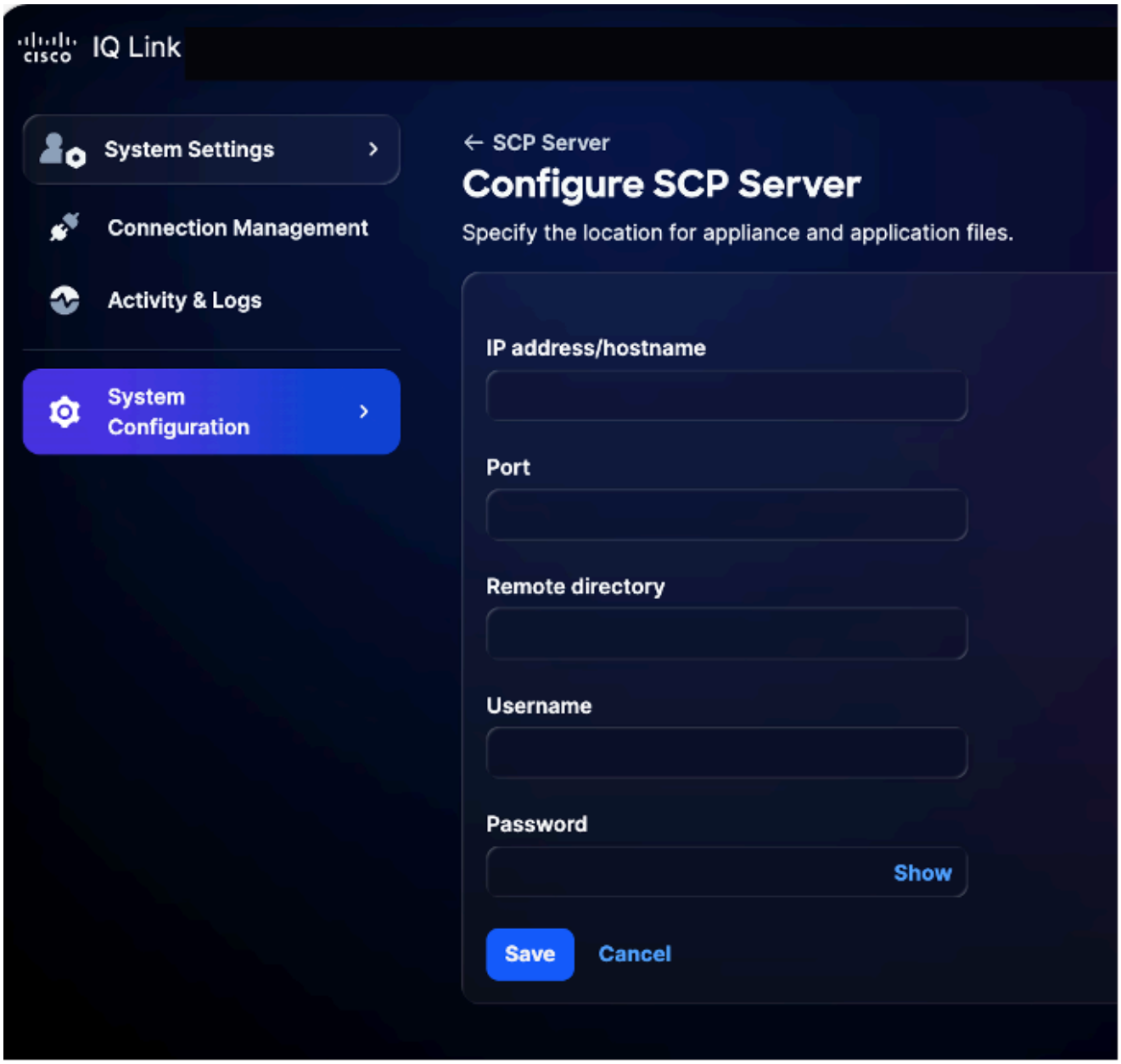
添加SCP服务器的步骤：

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。



配置SCP服务器

3. 输入IP地址/主机名。
4. 请输入一个端口号。
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。

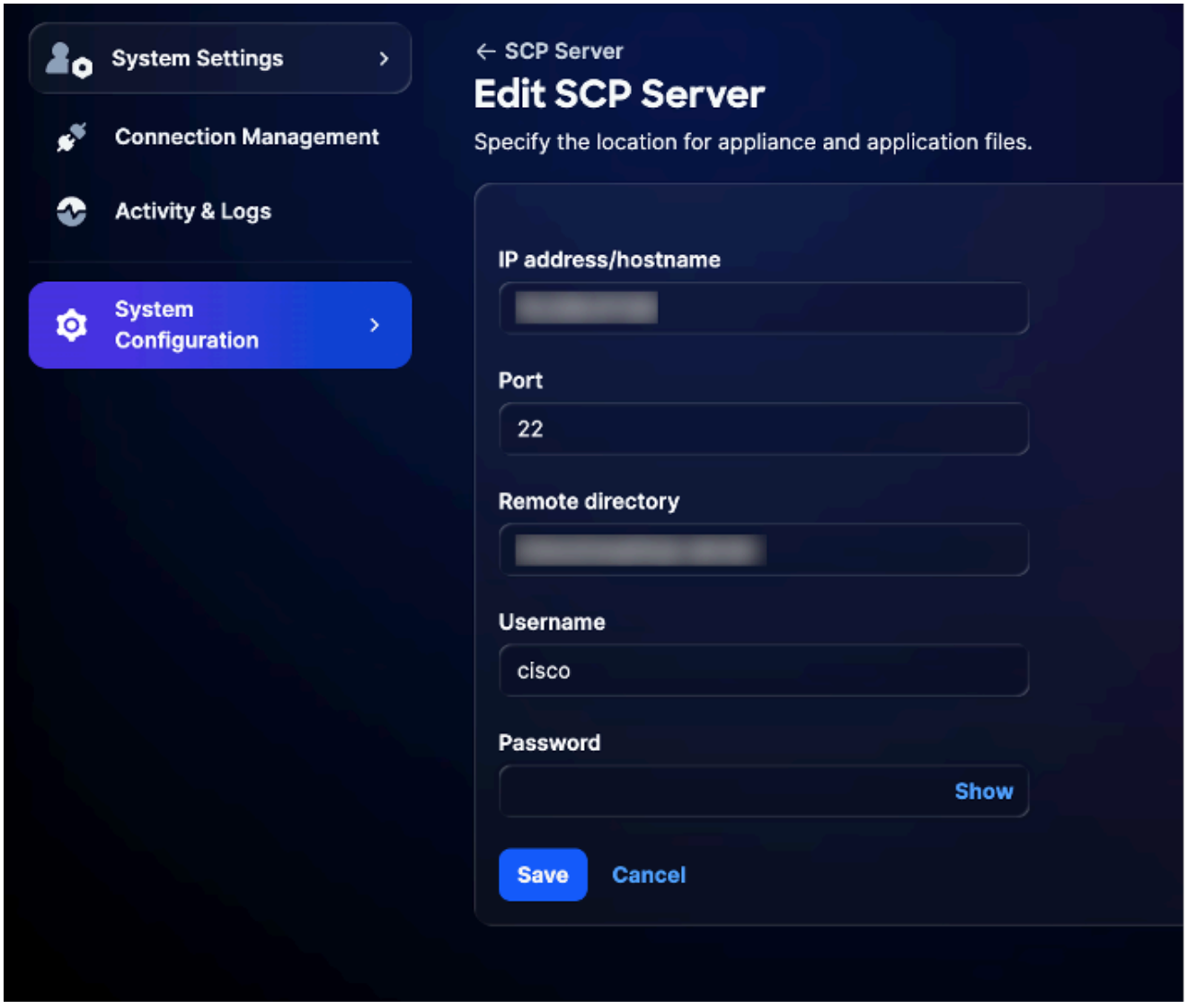
编辑现有SCP服务器

要编辑现有SCP服务器，请执行以下操作：

1. 导航到SCP Server页面。

SCP服务器

2. 对于所需的现有SCP服务器，单击Edit。



编辑SCP服务器

3. 根据需要修改详细信息。

4. Click Save.

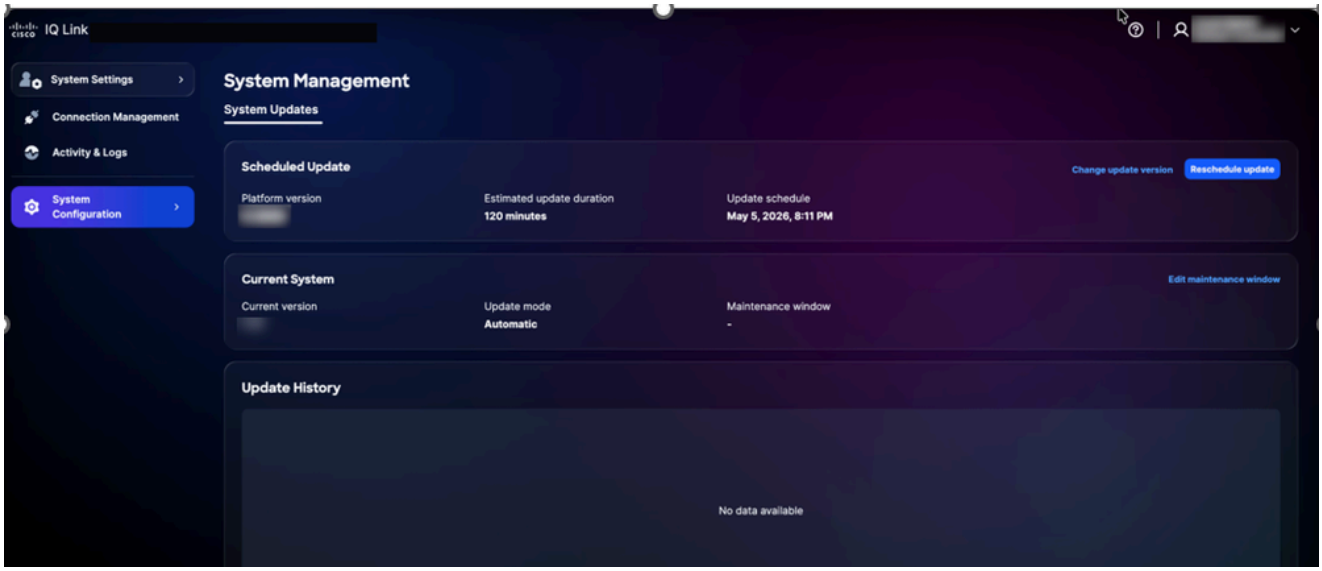
系统管理

您可以通过UI升级到最新的Cisco IQ Link版本。您还可以从Cisco IQ Data Connectors页面进行验证。

重新计划系统更新

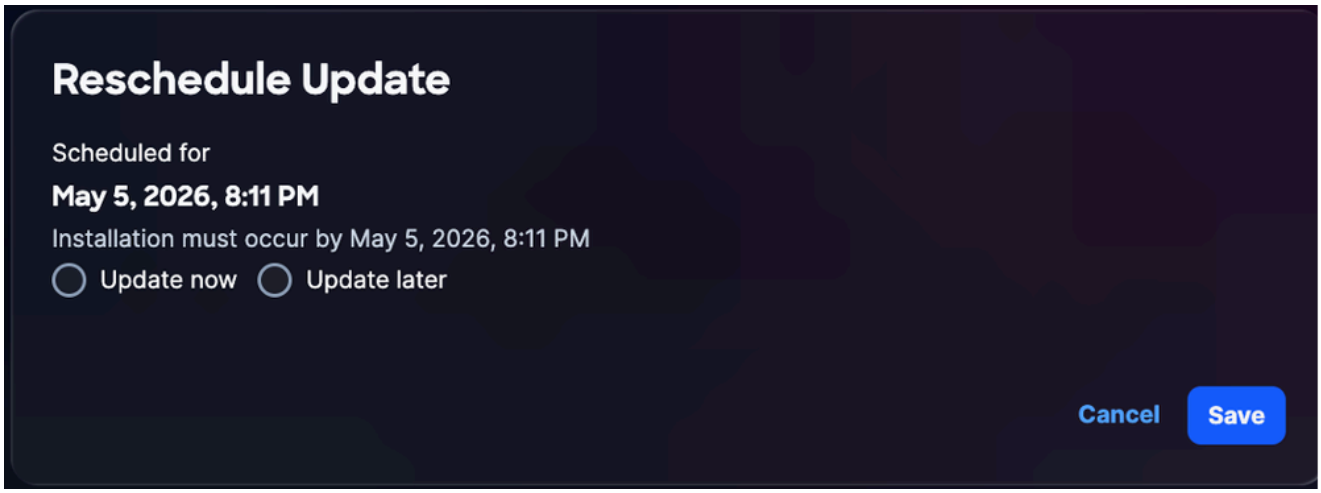
要重新计划系统更新，请执行以下操作：

1. 从Administration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。



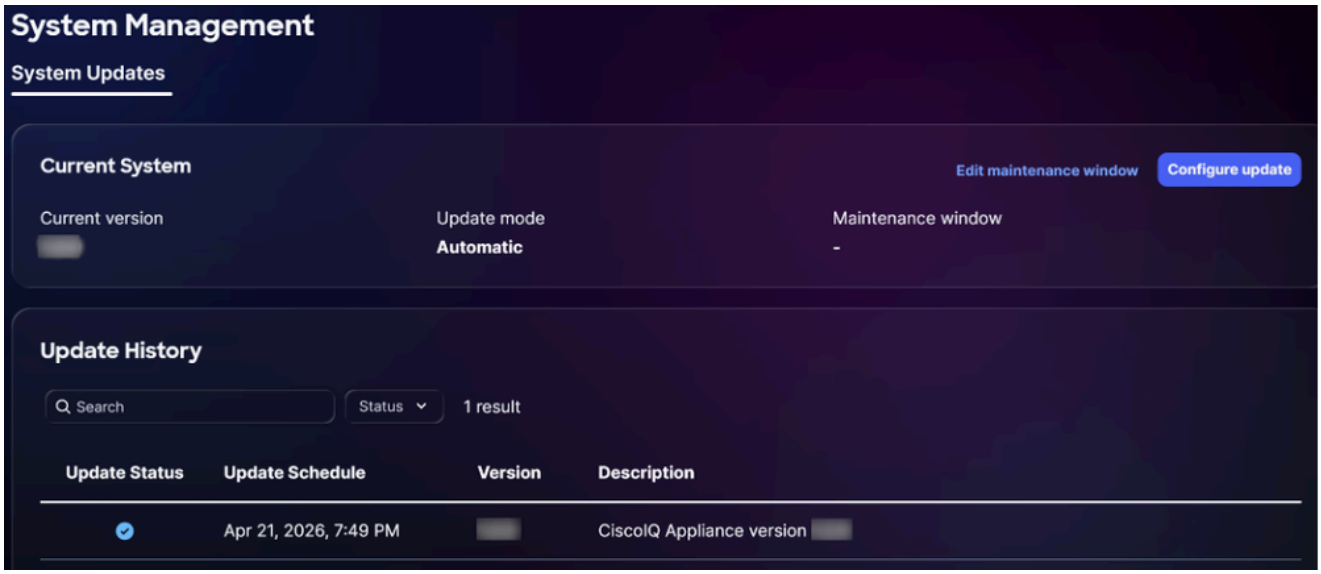
系统升级

2. 单击Reschedule update。



重新安排升级

3. 选择Update Now单选按钮以立即重新安排，或选择Update Later单选按钮以安排其他时间。
4. Click Save.系统将显示一条确认消息，您将被重定向到系统更新主页。

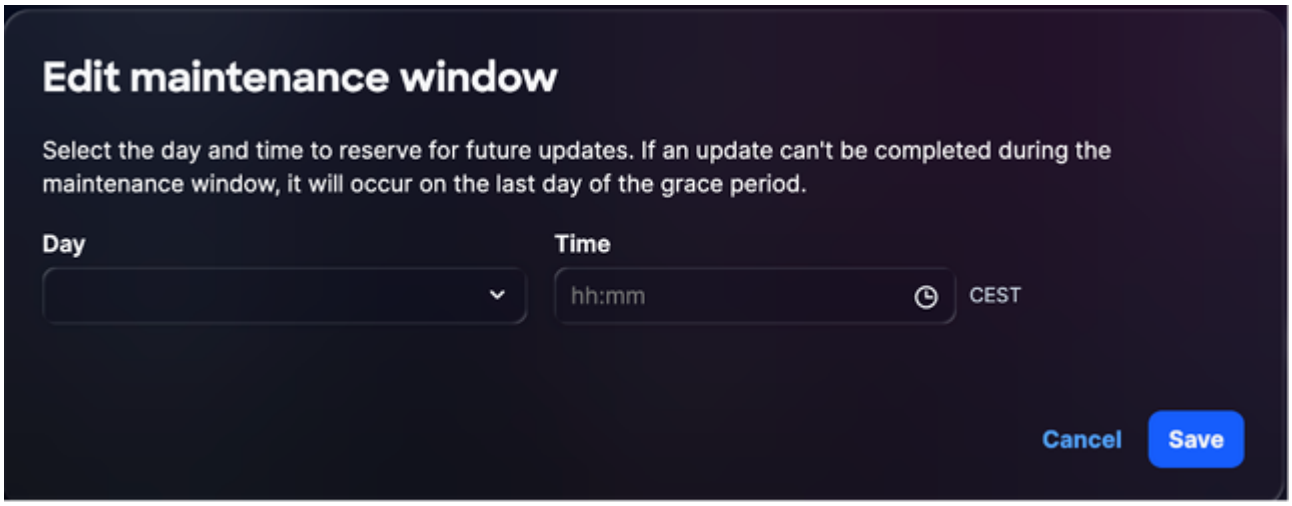


升级成功

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：

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。

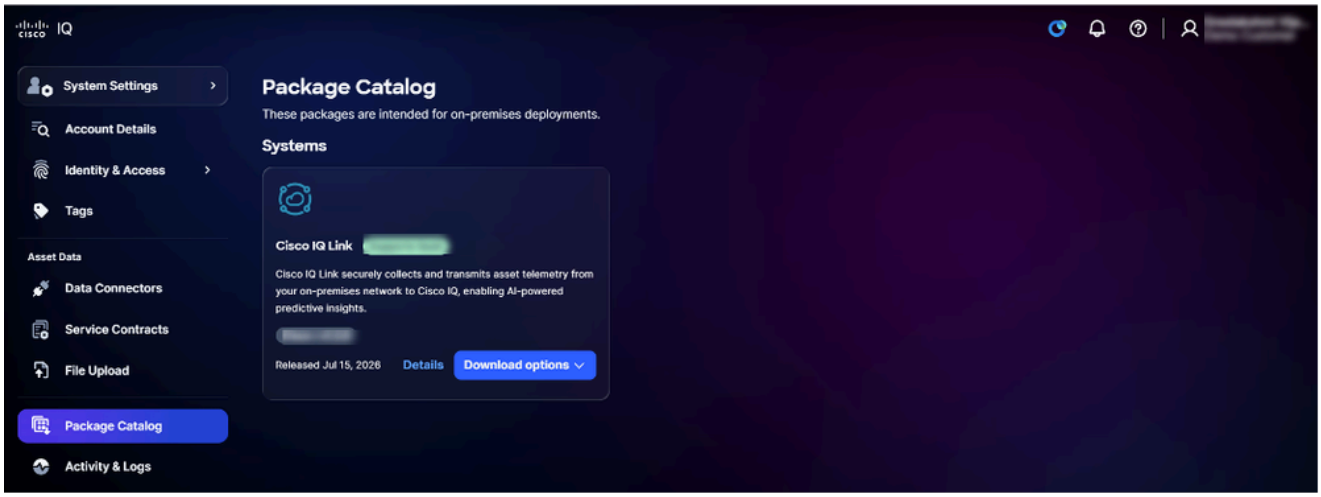
3. 单击保存。已成功计划维护窗口。根据显示的计划触发更新。

注意：
— 如果未配置升级计划，对于不重新启动的升级，系统默认为两(2)周的宽限期；对于需要重新启动的升级，系统默认为四(4)周的宽限期。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。

手动升级系统

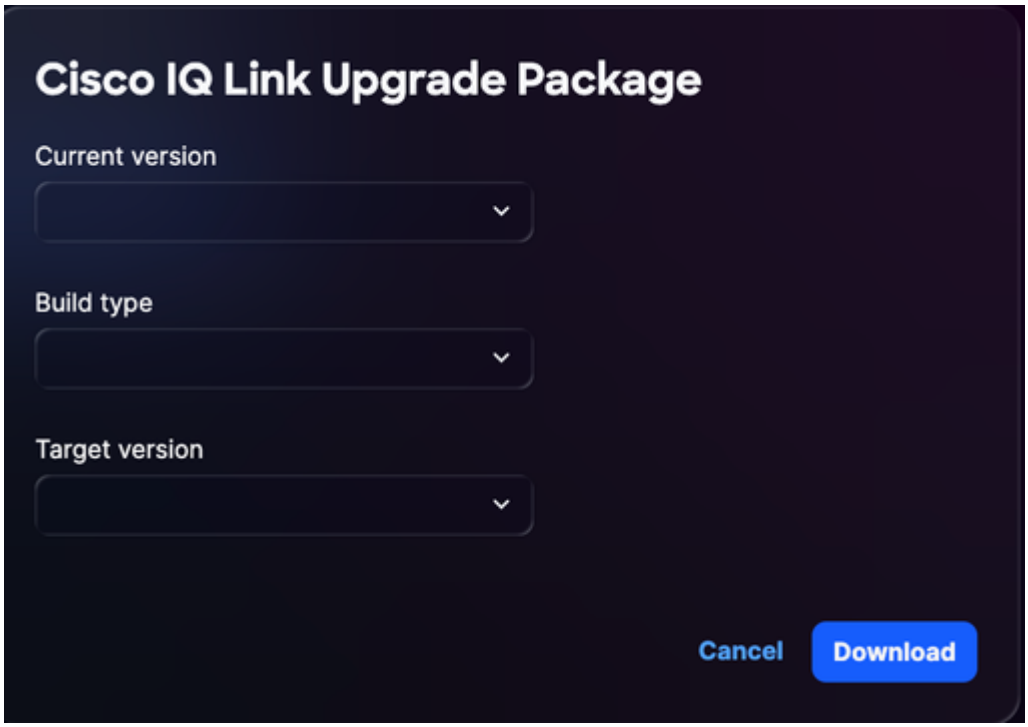
在无法自动从Cisco IQ SaaS分发或延迟分发的情况下，您可以直接从Cisco IQ SaaS下载升级捆绑包来手动执行系统升级。要手动升级系统，请执行以下操作：

1. 登录Cisco IQ SaaS 选择Home > System Settings > Package Catalog。



包目录

2. 在Cisco IQ Link部分中，单击Download options > Upgrade packages。



升级包

3. 从下拉列表中选择Current version。

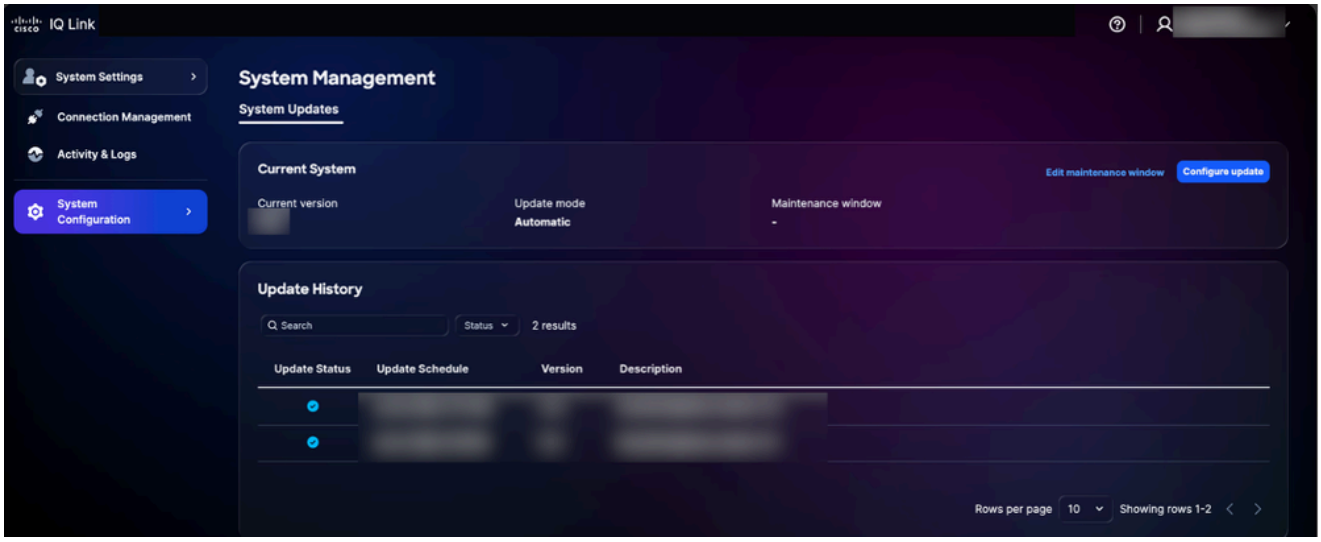
4. 从下拉列表中选择Build type。

5. 从下拉列表中选择Target version。

6. 单击 Download。下载升级捆绑包。

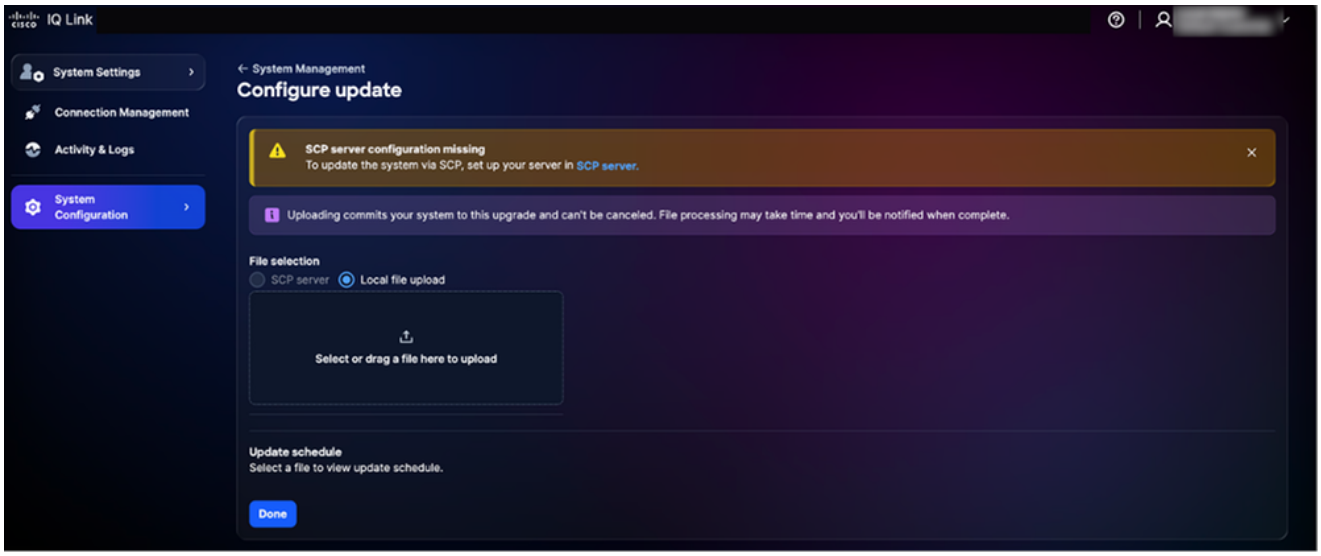
7. 导航到Cisco IQ Link。

8. 从System Settings中选择System Configuration > System Management。



配置更新

9. 单击Configure update。



本地文件上传

10. 单击Local file upload单选按钮。

11. 选择下载的升级捆绑包文件并将其拖到上传字段中。
12. 单击Done。系统成功更新后，系统会显示确认消息。

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。

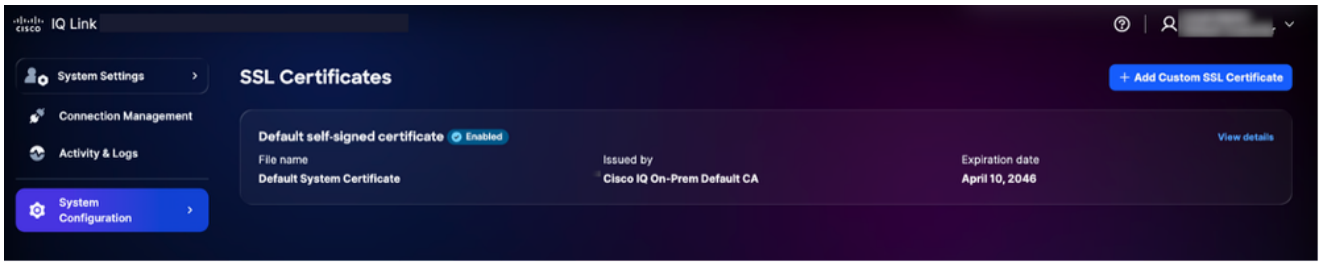
注意：证书的有效期必须至少为90天。如果证书到期前的剩余天数少于90天，则认为该证书“即将到期”。

添加、编辑或删除SSL证书后，必须按照Okta IDP或ADFS IDP的单一注销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：

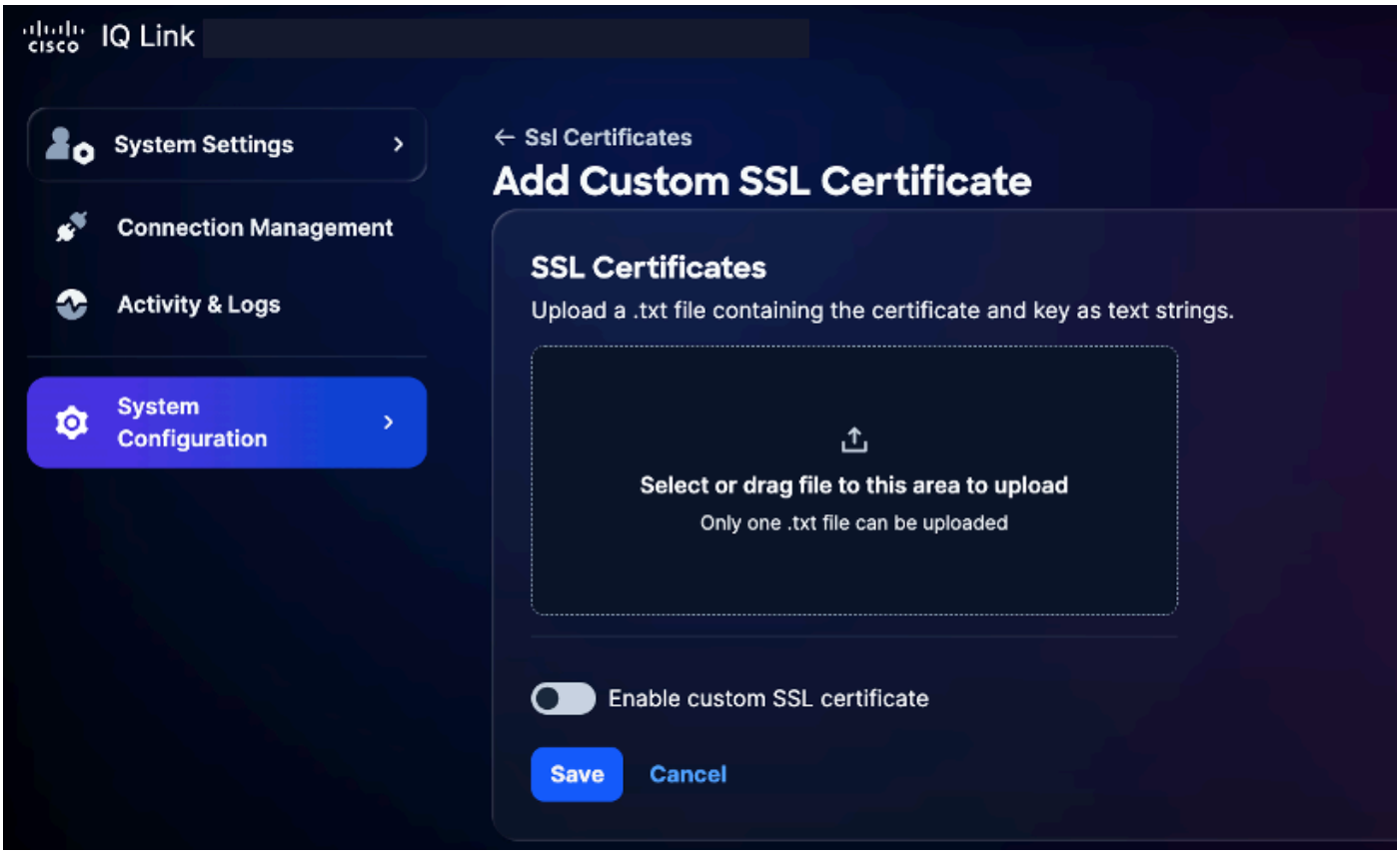
1. 从System Settings中，选择System Configuration > SSL Certificates。系统将显示SSL Certificates页面，其中列出了系统的所有SSL证书。



添加SSL证书

2. 单击Add Custom SSL Certificate。

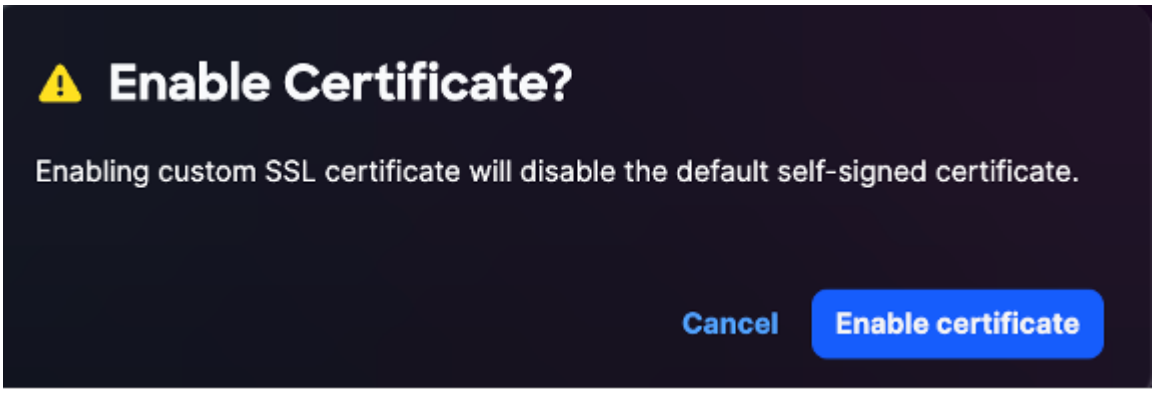
注意：
— 上传包含隐私增强型邮件编码证书和密钥作为文本字符串的.txt文件
— 一次只能上传一个.txt文件
— 文件必须同时包含证书和私钥



上传SSL证书

3.将自定义SSL证书拖放或上传到SSL Certificate字段。

4.打开Enable custom SSL certificate切换按钮。



编辑SSL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.单击启用证书。

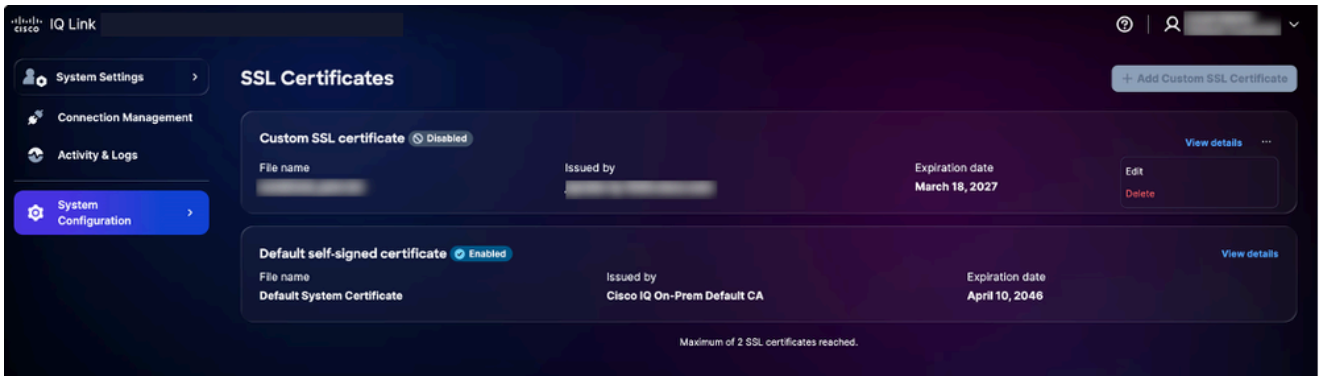
6.单击保存。

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。



编辑SSL证书

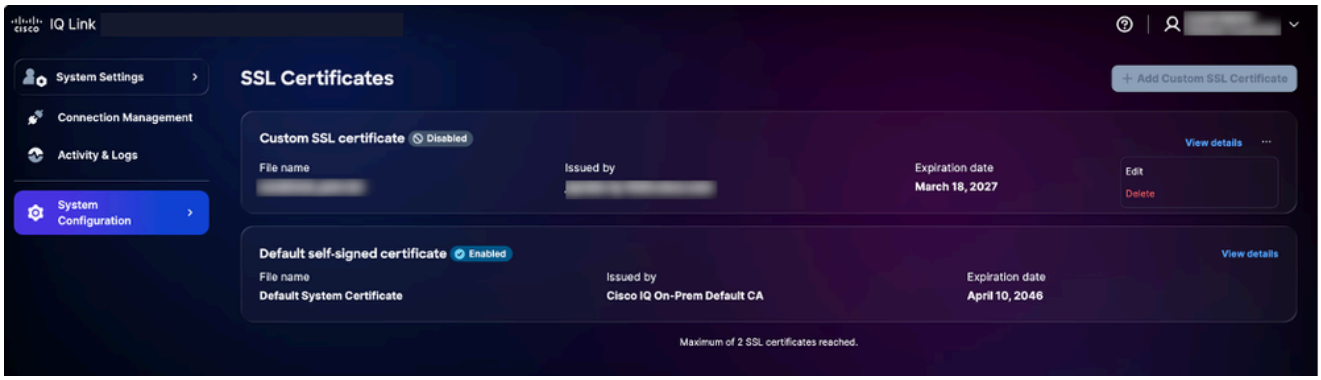
2. 选择更多选项图标> 编辑。系统将显示Edit SSL Certificate页面。
3. 根据需要编辑证书详细信息。
4. Click Save.

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. 导航到所需的自定义SSL证书。



删除SSL证书

2. 选择More Options图标> Delete。
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

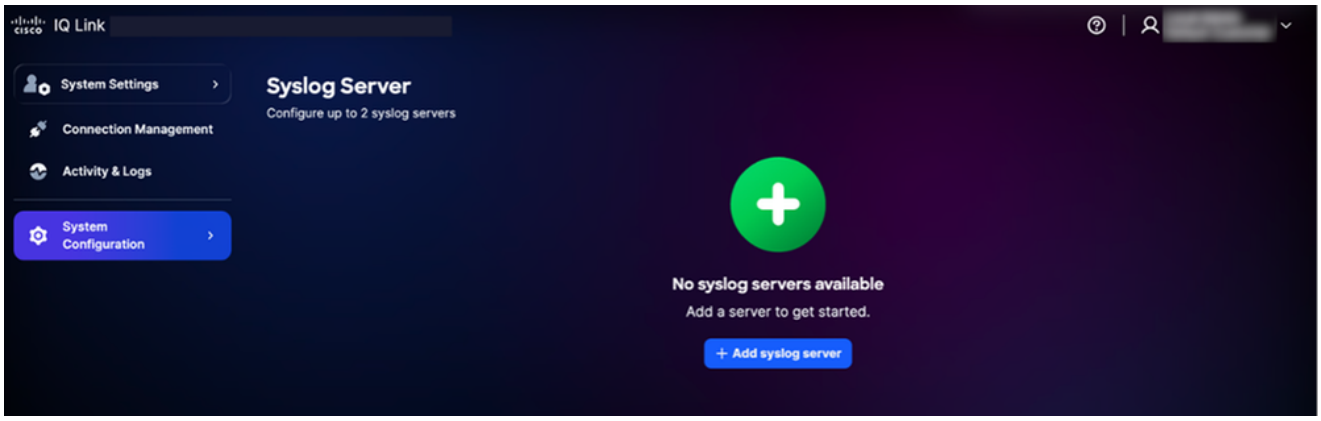
具有帐户管理员角色的用户可以配置外部系统日志服务器以导出系统日志。最多可以配置两(2)台系统日志服务器。

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

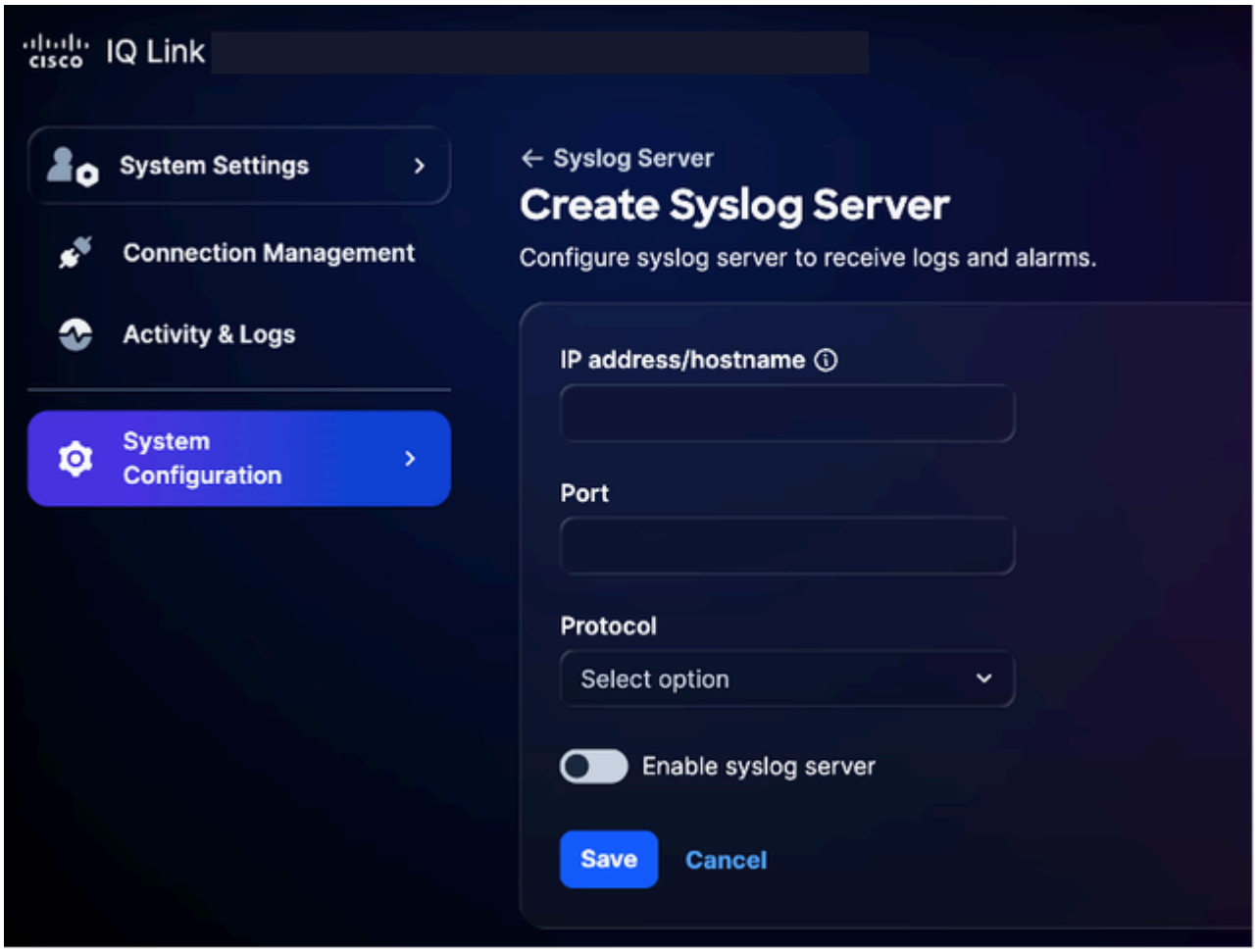
添加系统日志服务器的步骤：

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. 请输入一个端口号。

5. 从Protocol下拉列表中选择适用的协议（例如，UDP或TCP）。

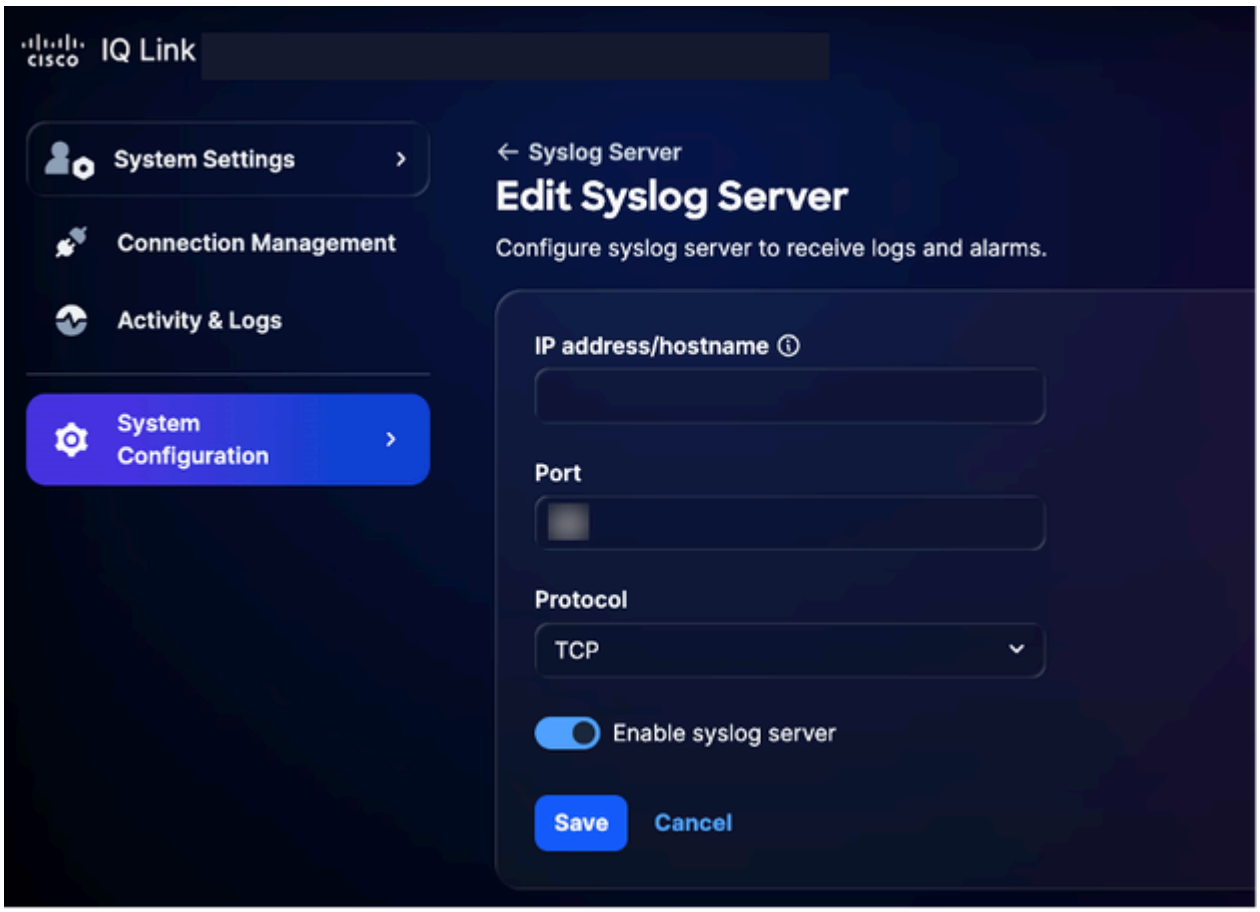
6. 打开Enable syslog server切换按钮。

7. Click Save.系统将显示确认消息，新添加的系统日志服务器会显示在系统日志服务器主页上。

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。



编辑系统日志服务器

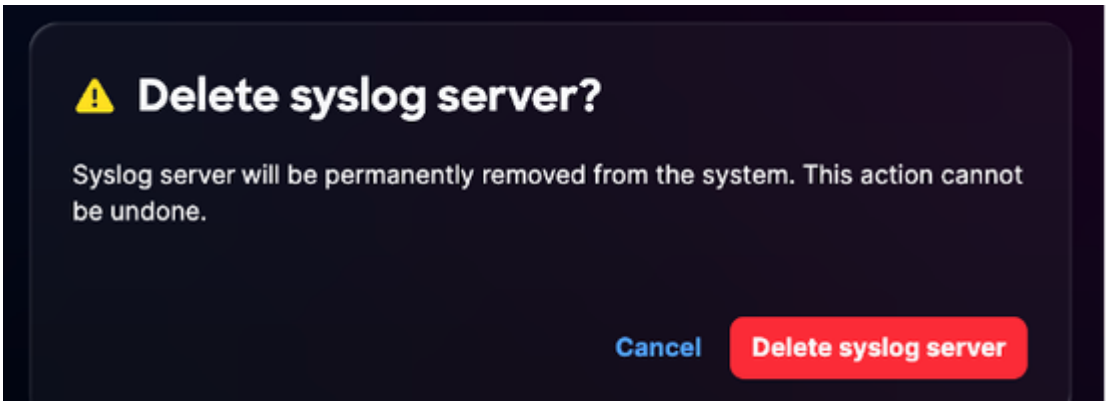
3. 根据需要编辑详细信息或关闭Enable syslog server切换。
4. Click Save.

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。

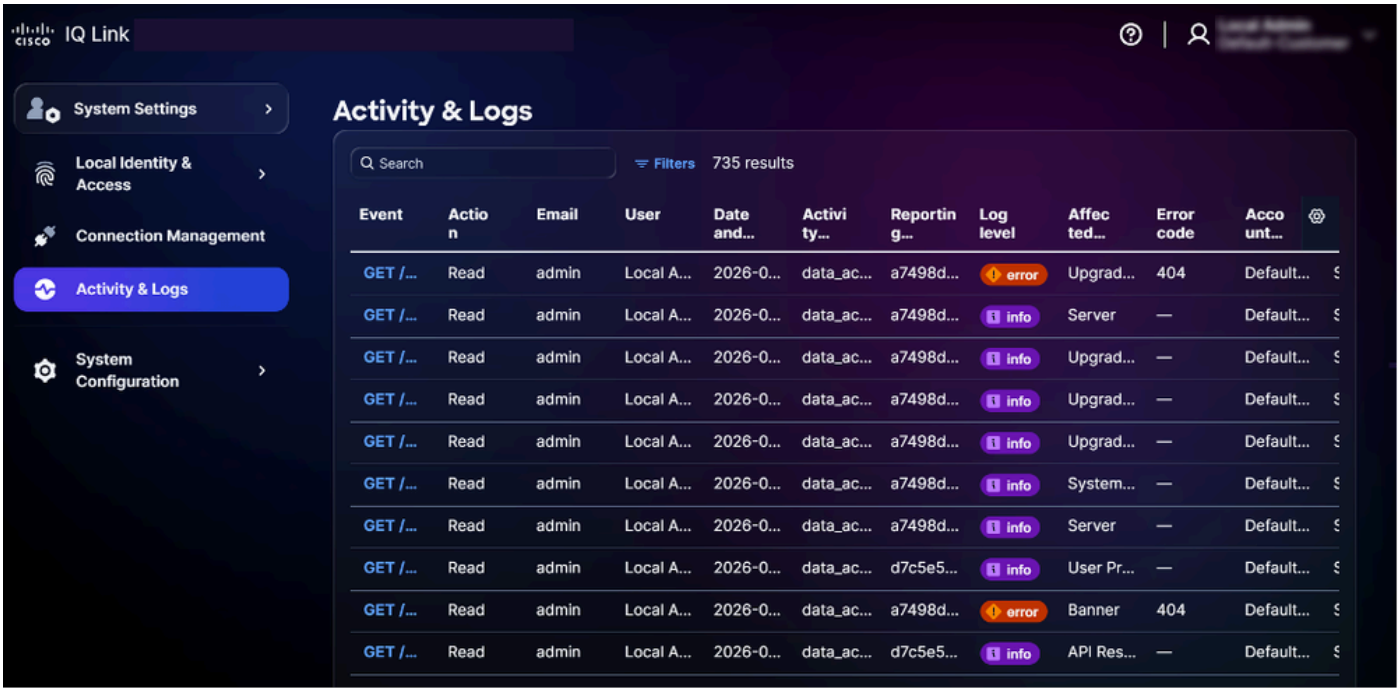


确认

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。



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：

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

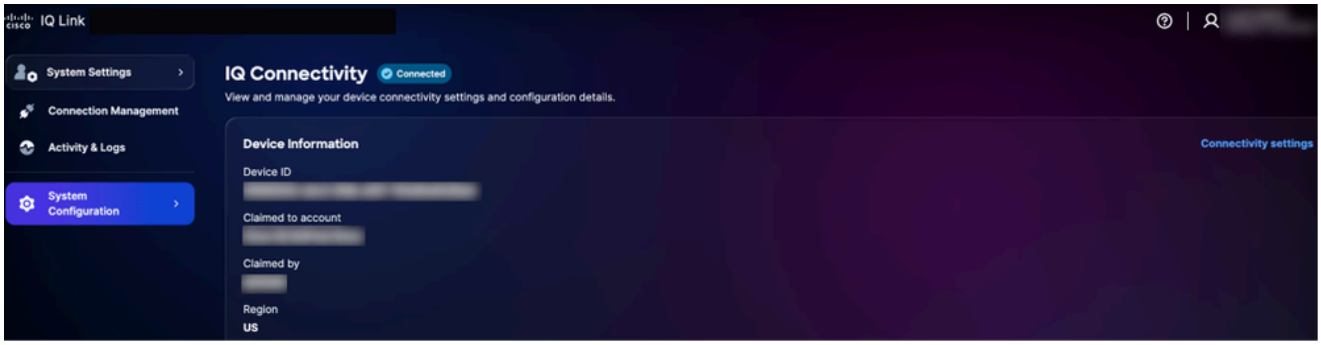
以下过滤器选项可用：

- 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:过滤特定错误代码的日志

IQ连接

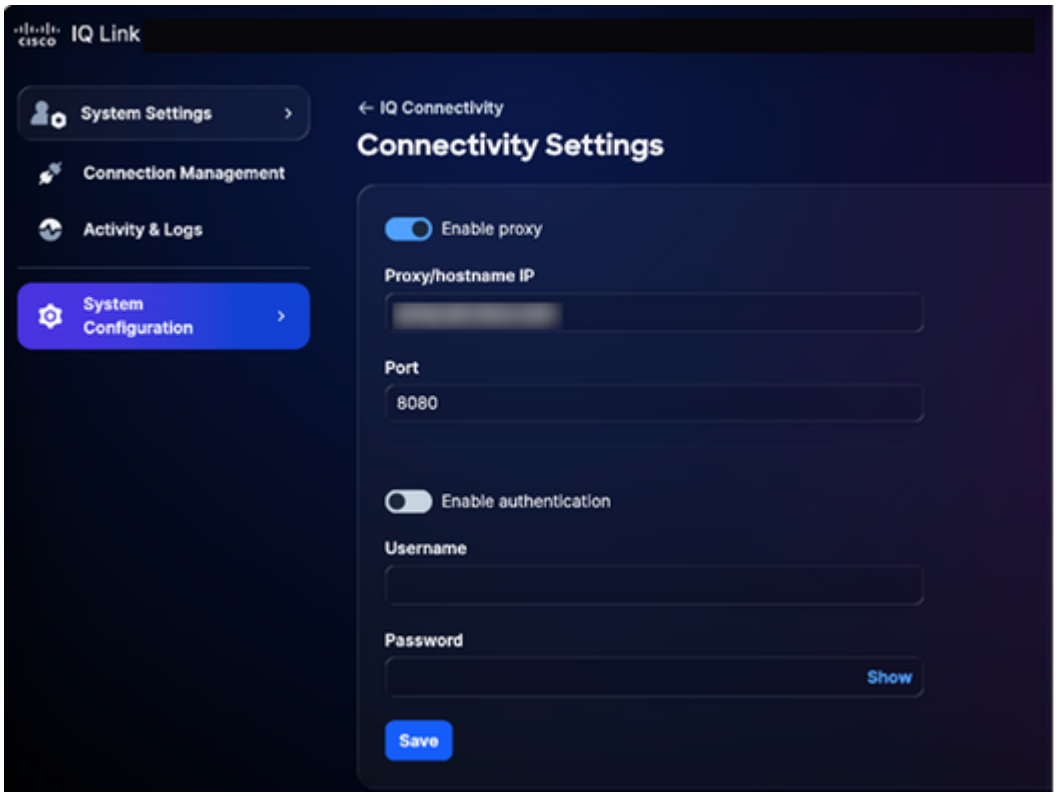
要查看和管理设备连接设置和配置详细信息，请执行以下操作：

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



IQ连接

2. 单击连接设置。



连接设置

3. 根据需要更新详细信息。
4. Click Save.

连接管理（数据收集）

Cisco IQ Link是用于网络数据收集的现场解决方案，旨在提供对您的基础设施的深入可视性。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。配置数据收集概述如下：

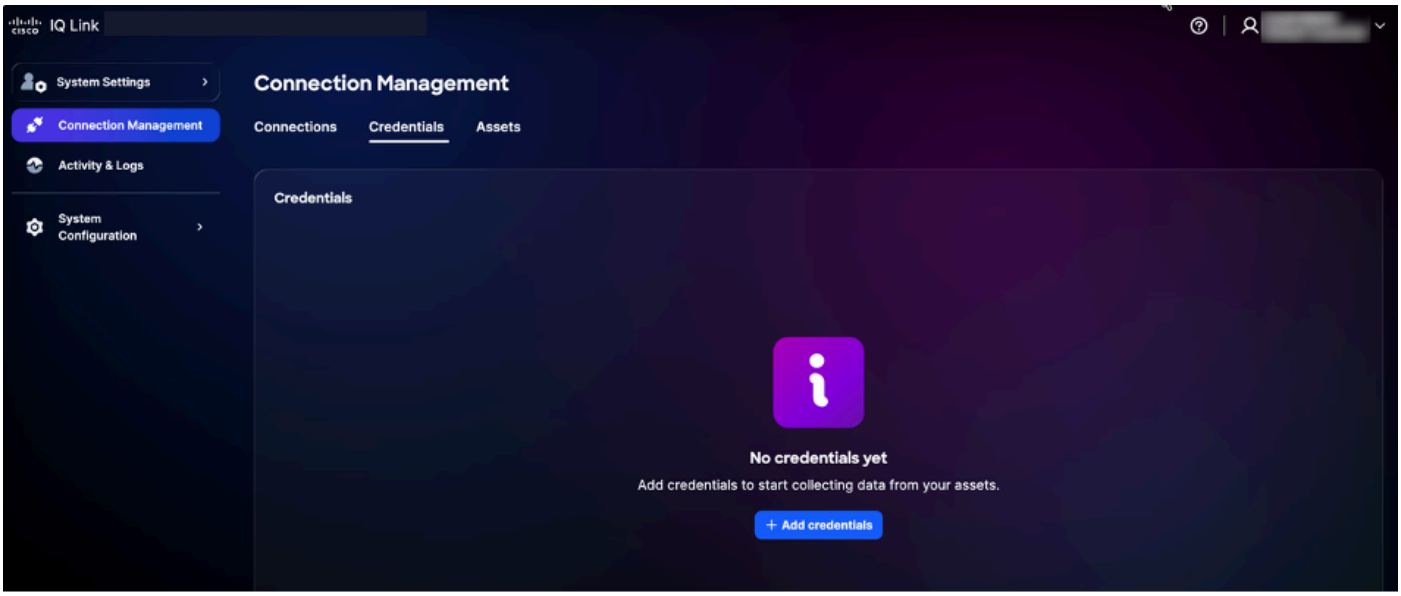
- 创建凭证集:建立身份验证协议(例如，简单网络管理协议(SNMP)v1/v2c/v3)以与网络设备通信。通过按安全区域或位置集中凭证（例如，“SanJose-SNMPv3”），您可以在一个位置更新密码，使更改自动传播到所有相关设备。
- 将凭证映射到资产:将凭证集与库存资产进行映射，以自动执行身份验证过程。通过创建将特定IP范围链接到已定义的凭证集的规则，系统在数据收集期间自动应用正确的身份验证。这消除了手动输入错误，并确保您的配置在网络扩展时保持准确。

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

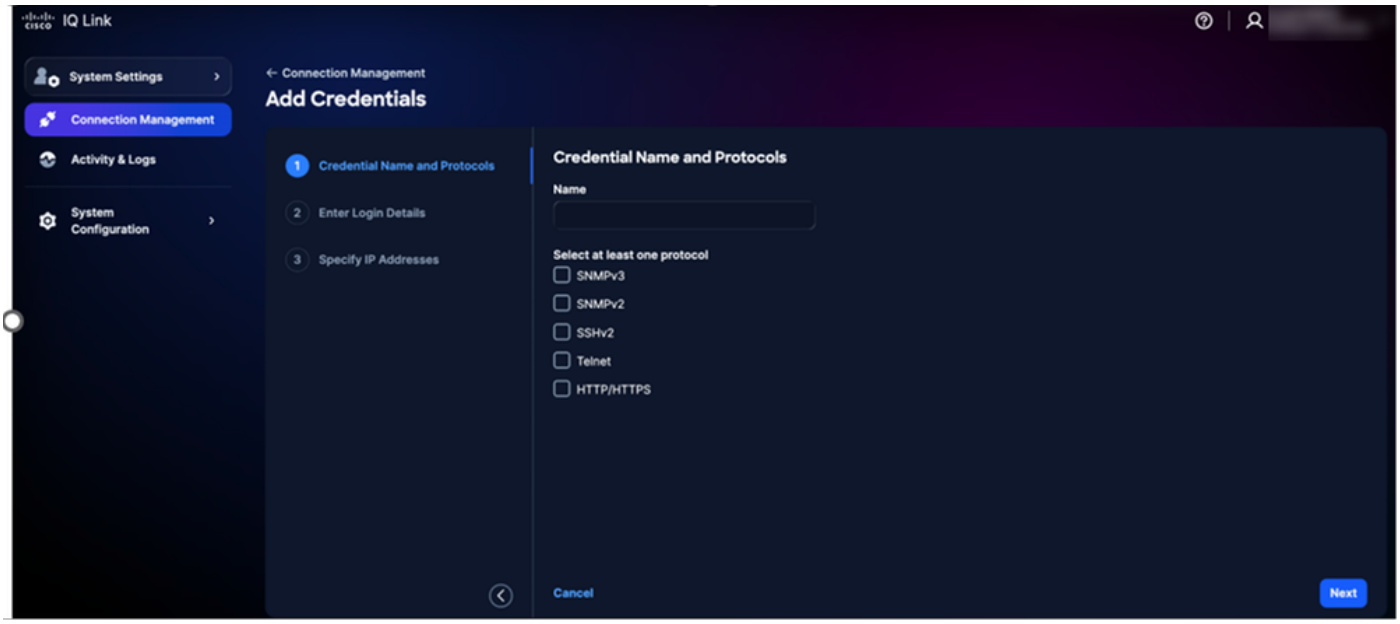
必须先添加凭据才能执行数据收集。要添加凭证，请执行以下操作：

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.单击添加凭证。

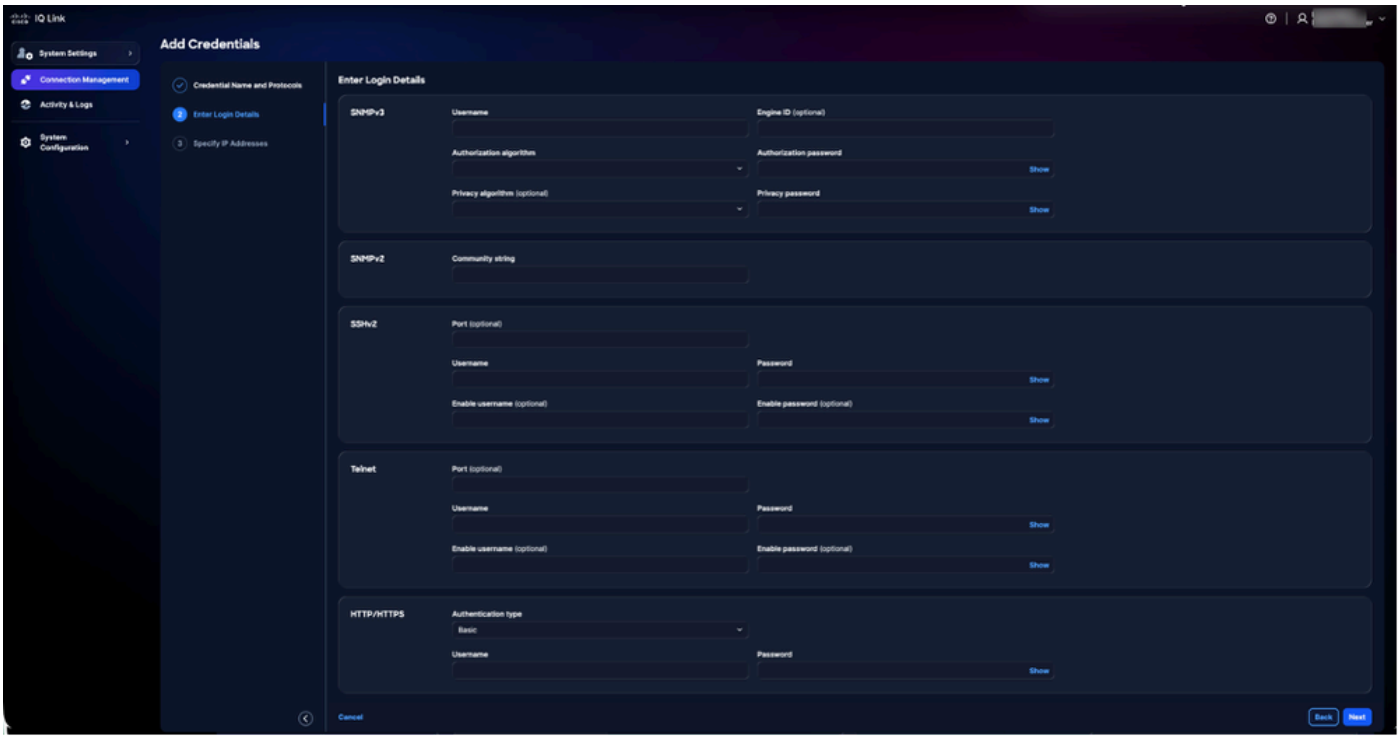


添加凭证

4.输入名称。

5.选中所有适用的协议复选框。

6.单击下一步。

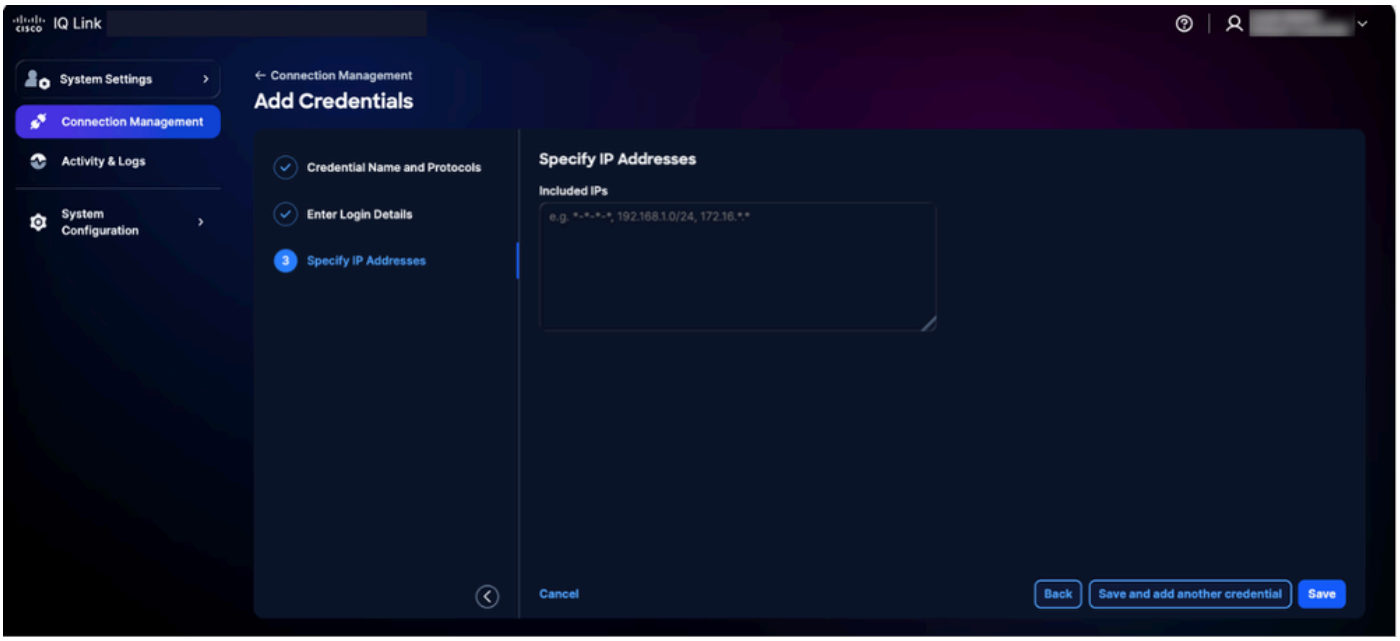


添加凭证详细信息

注意：上图显示了上一步中选择所有协议的视图。您的接口将仅显示您选择的特定协议。

7.输入每个选定协议的登录详细信息。

8.单击下一步。

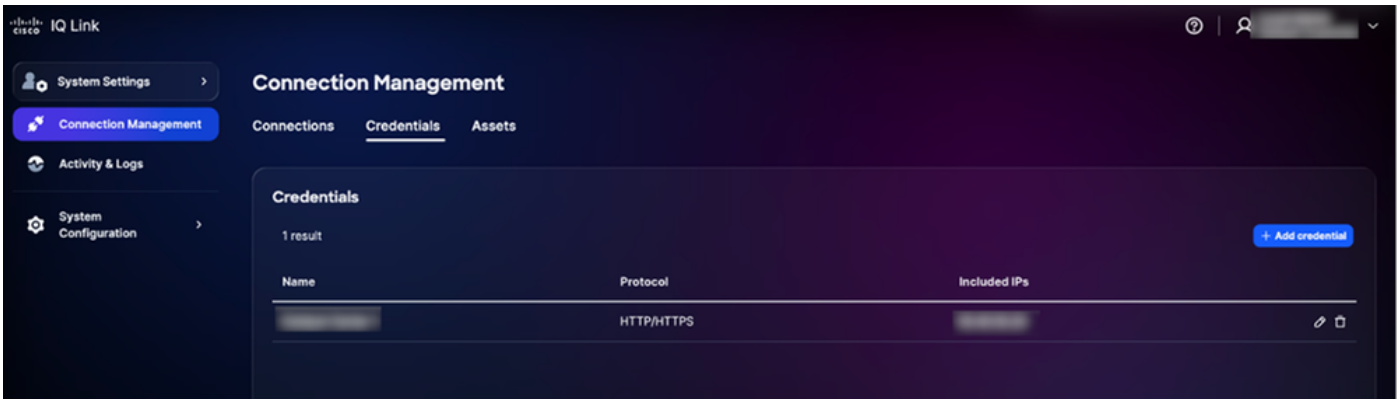


指定IP地址

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.单击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.*（通配符中的最高优先级）

    1.2.*.*

    1.*

..*.*（优先级最低）

- 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13 ：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）

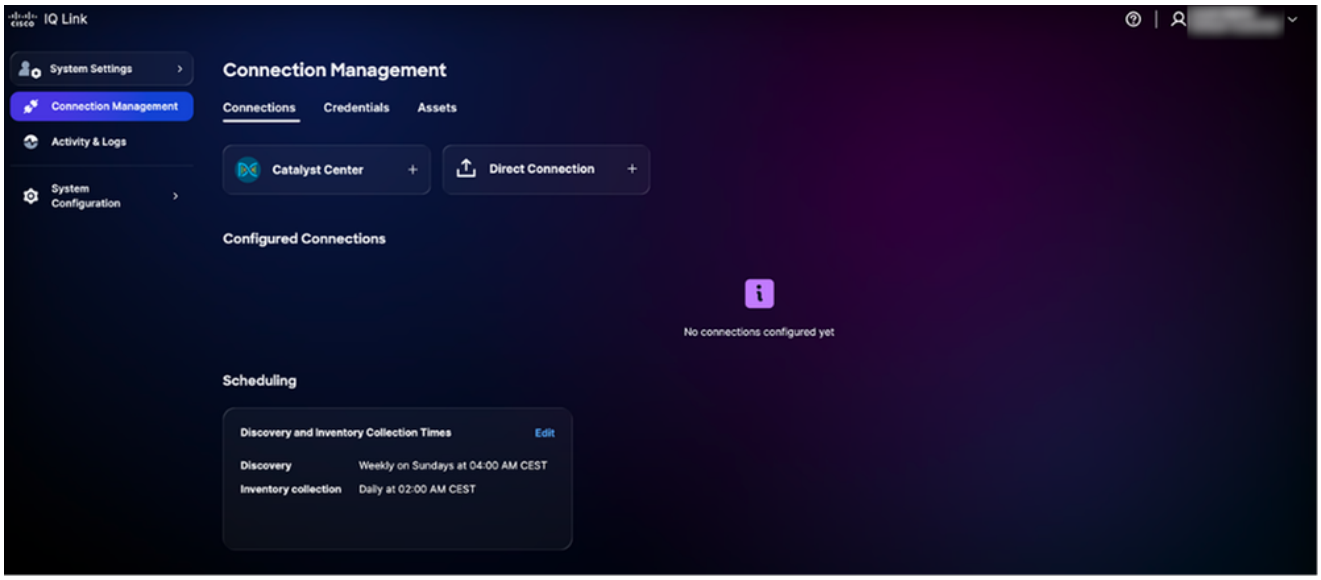
注意：如果设备属于多个重叠类别，系统始终会选择具有最高特异性的凭证集（换言之，最少的尾部通配符）。

使用Catalyst Center进行数据收集

对于每个Cisco IQ Link实例，最多可连接20个Catalyst Center（非集群）。

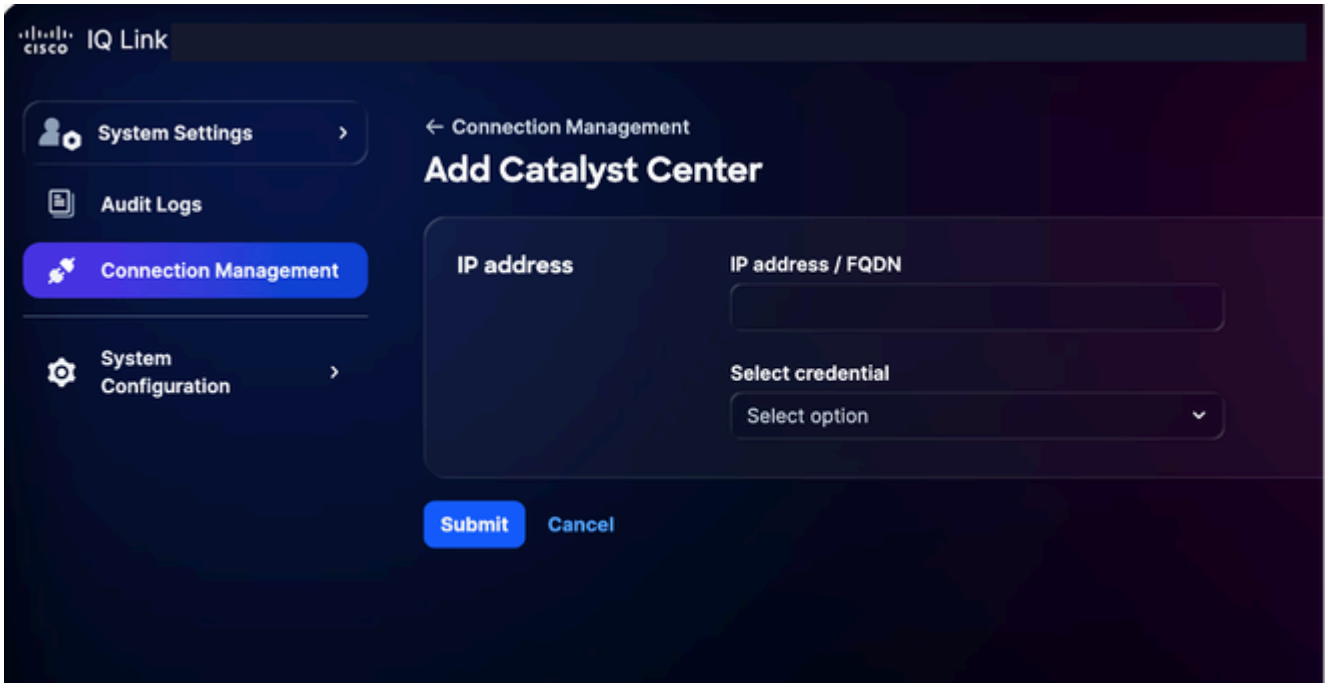
对于使用Catalyst Center的数据收集：

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。

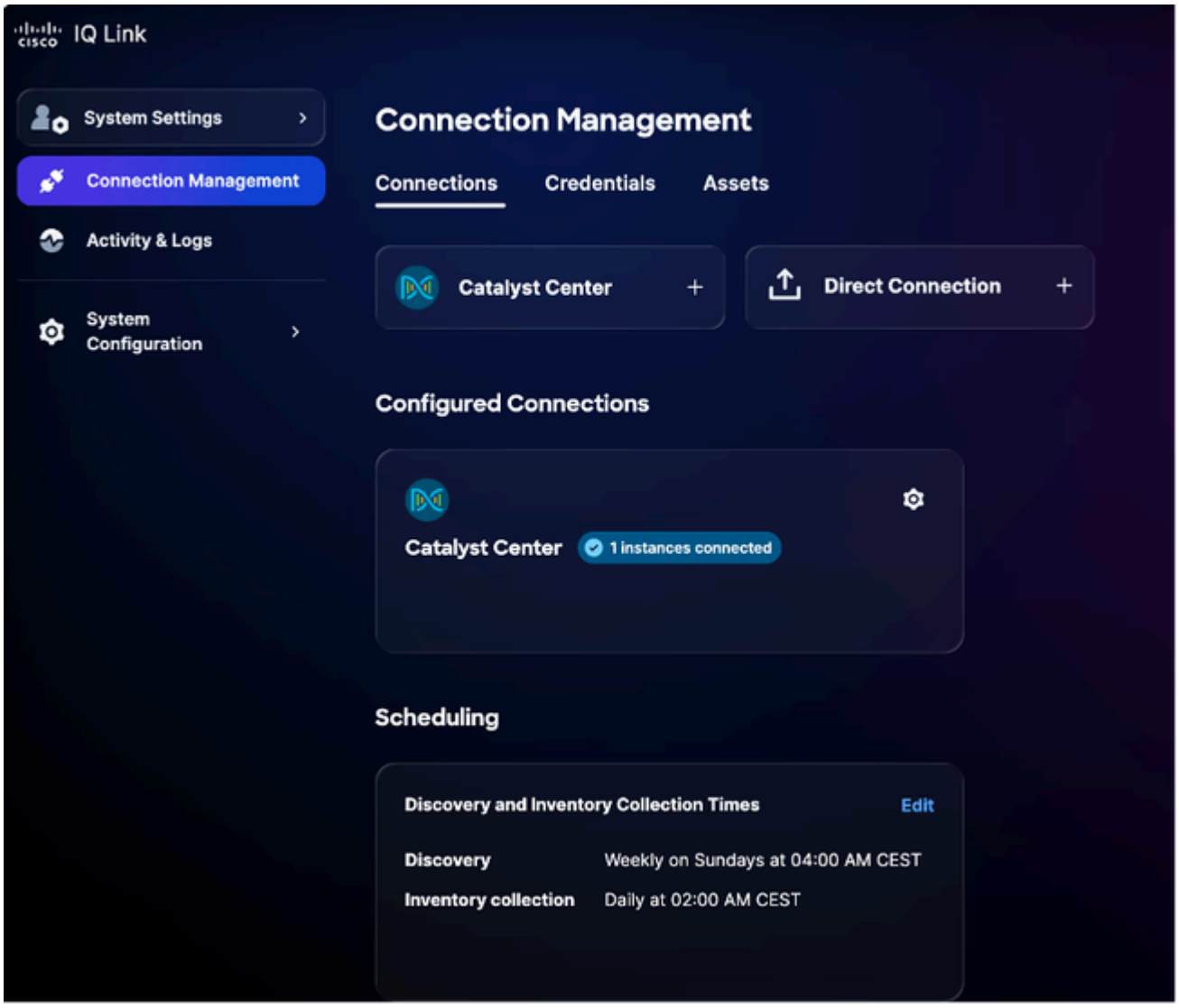


添加Catalyst Center

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。



已成功添加Catalyst Center

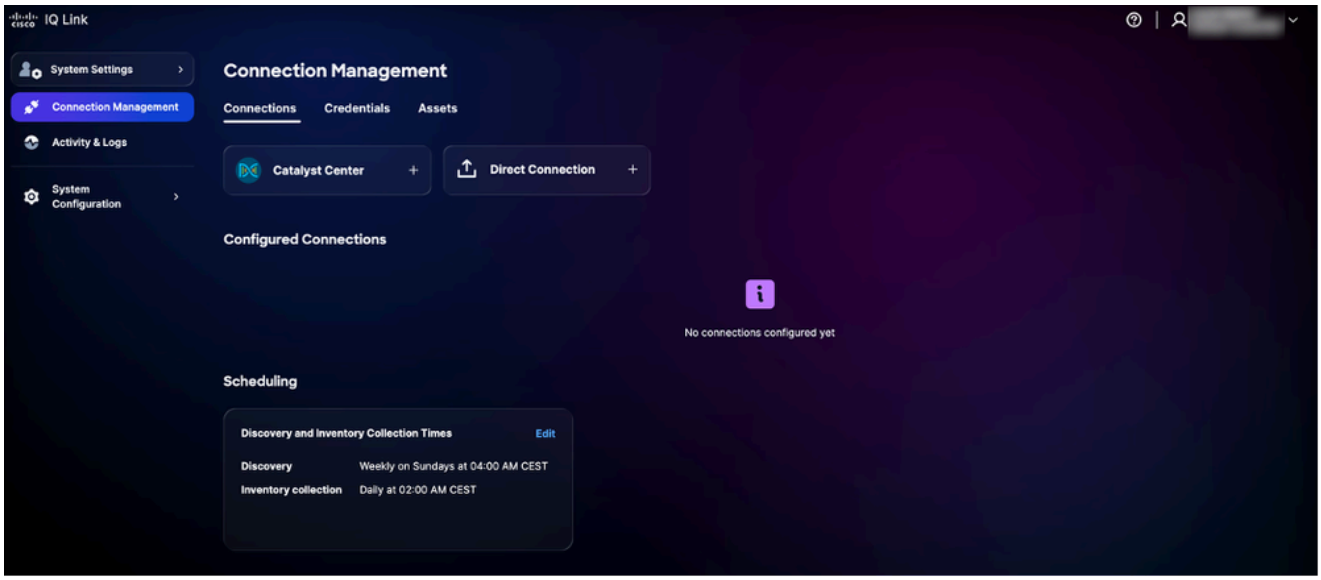
6. 计划收集。有关详细信息，请参阅计划。

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

直接连接

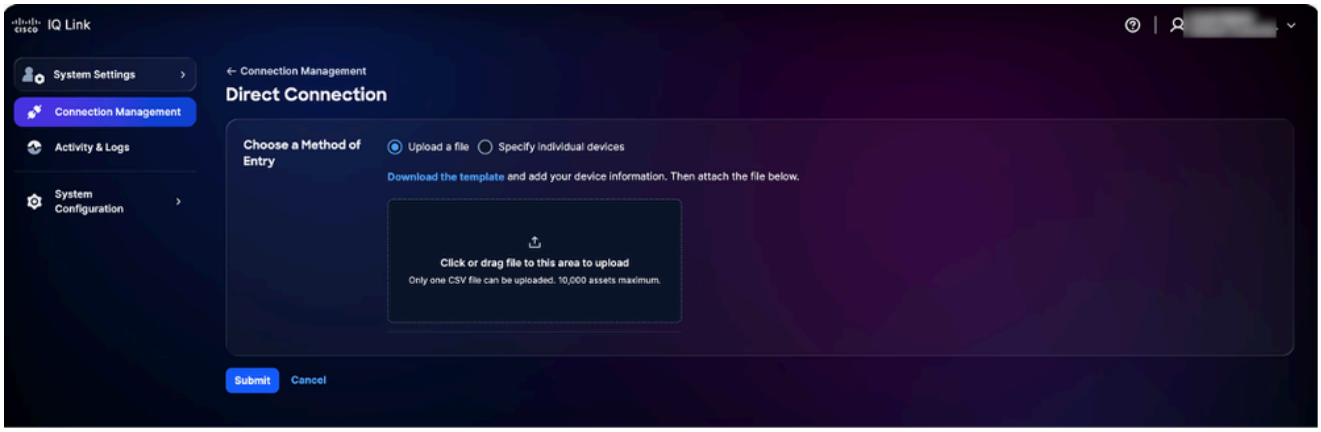
要添加直接连接的设备，请执行以下操作：

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



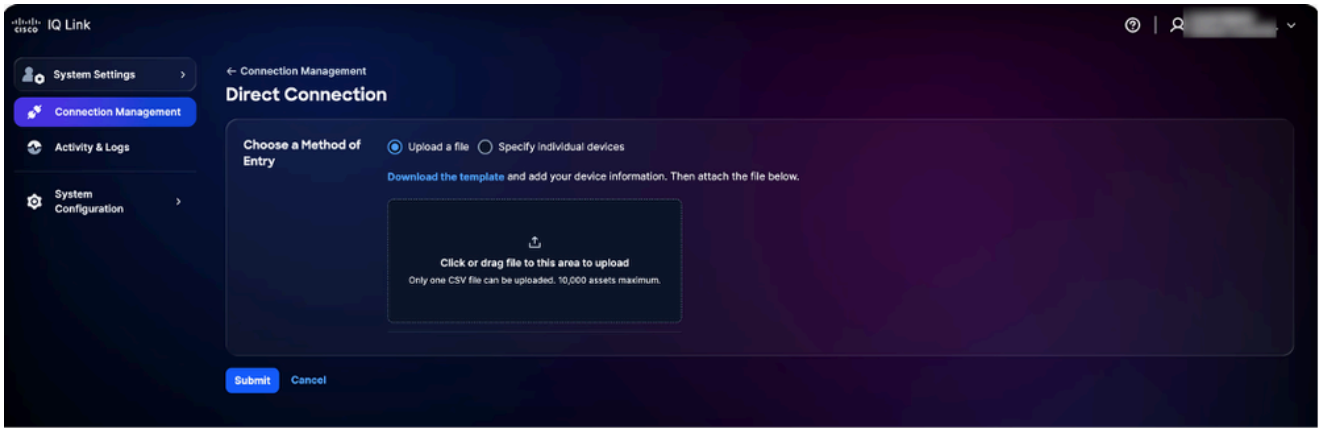
连接管理

2. 单击Direct Connection。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。



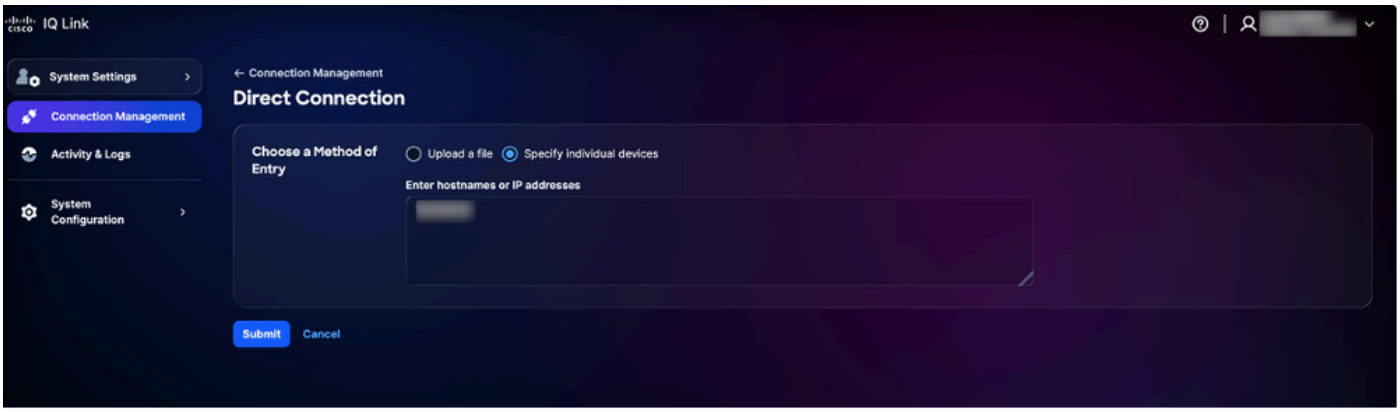
上载文件

3. 单击Choose a Method of Entry的首选选项，然后使用以下方法之一提交设备：



上载文件

- 上载文件:单击或拖放文件，然后单击Submit



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，然后单击Submit

成功提交后，系统会将您重定向到Assets选项卡。

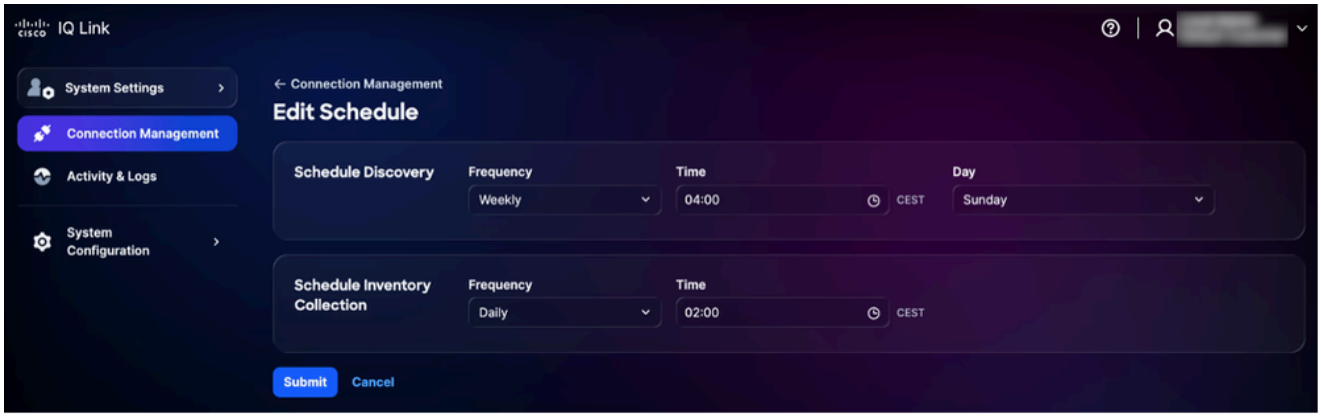
4.安排收集。有关详细信息，请参阅计划。

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

安排

调度允许您定义Cisco IQ Link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：在Cisco IQ Link中，为对发现或收集计划所做的任何更改留出5-10分钟的时间进行同步和准确反映。

横幅

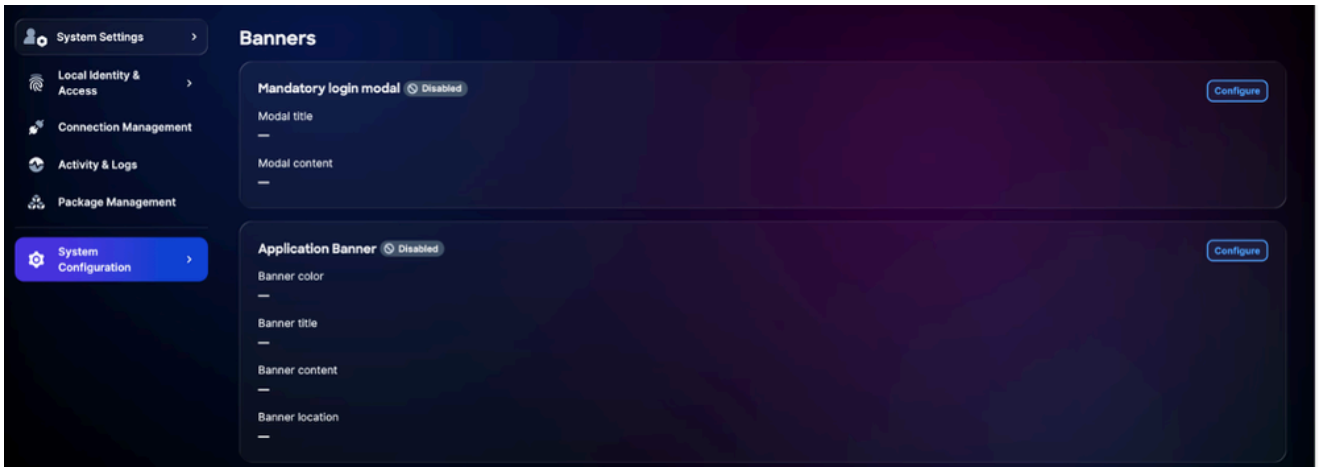
帐户管理员可以配置系统范围的横幅以符合安全和合规性标准。

- 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

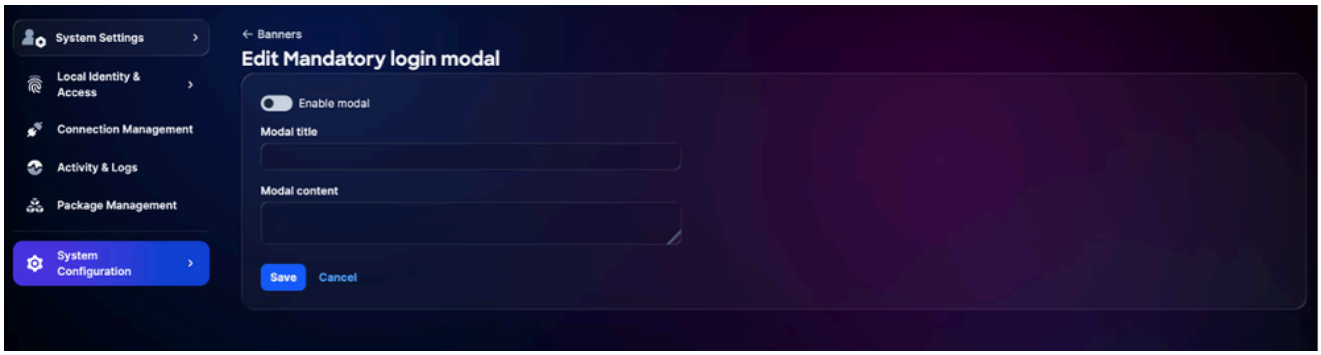
要配置强制性标语，请执行以下操作：

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。



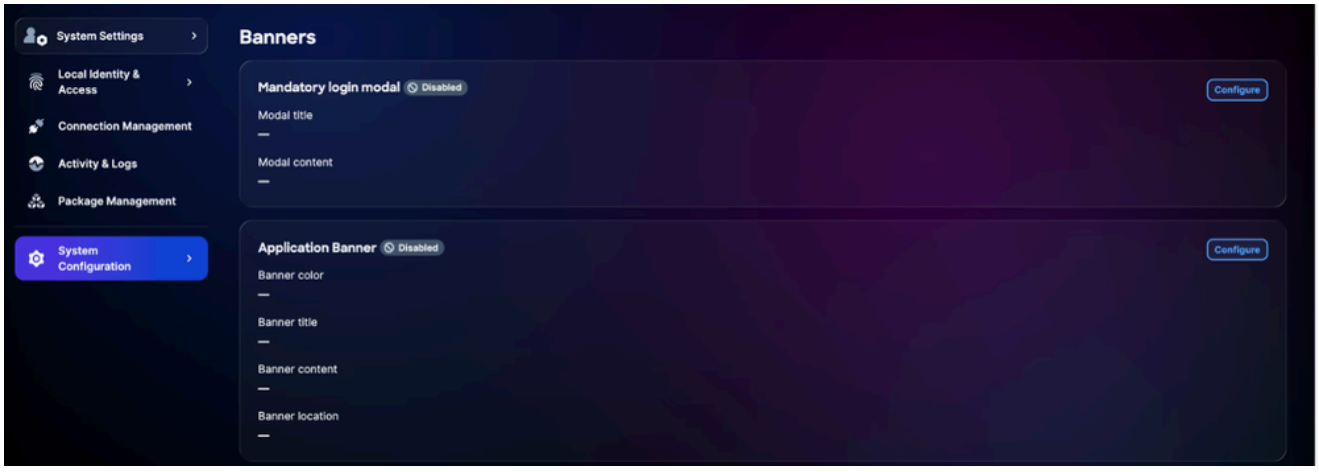
编辑强制登录模式横幅

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

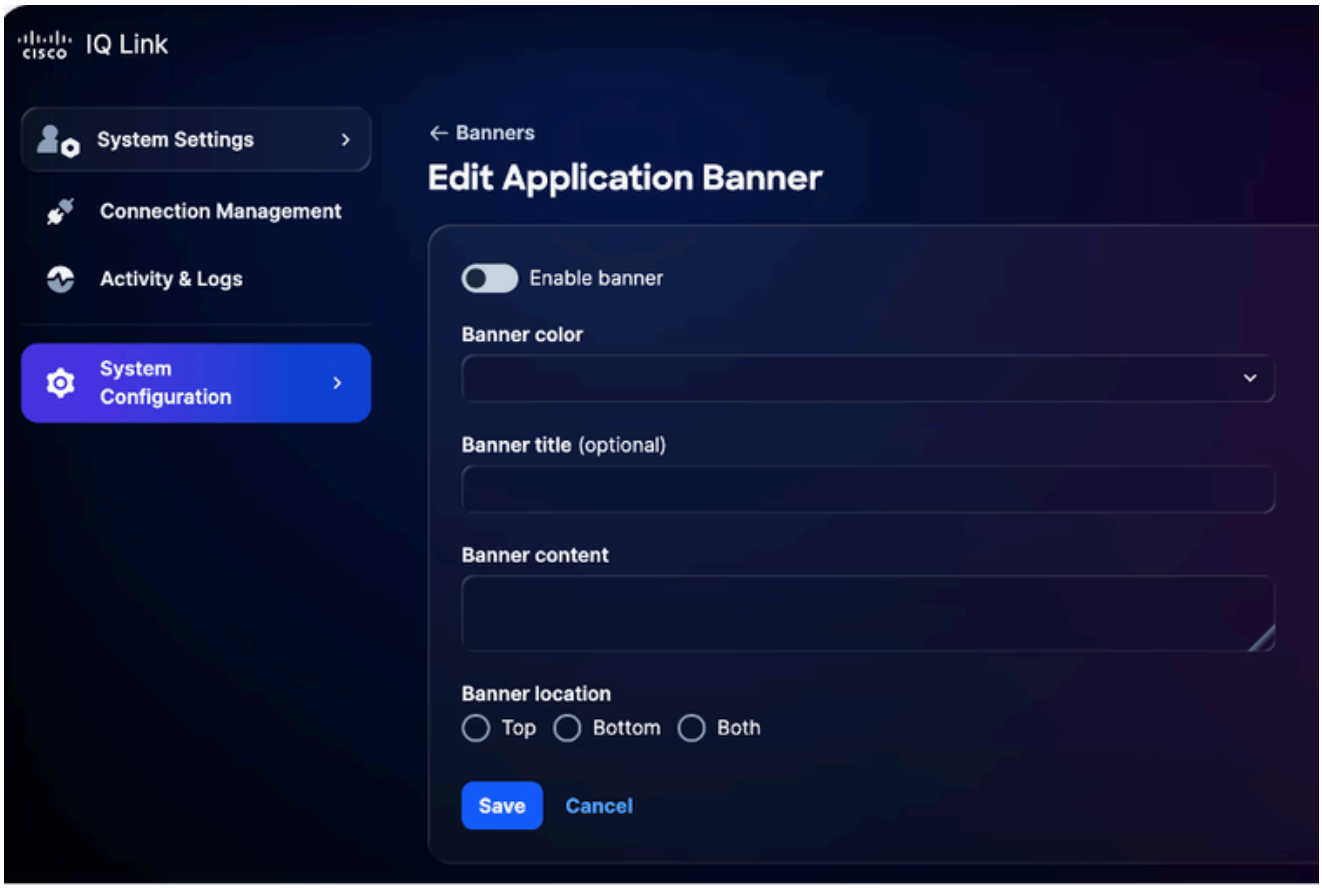
要配置应用横幅，请执行以下操作：

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

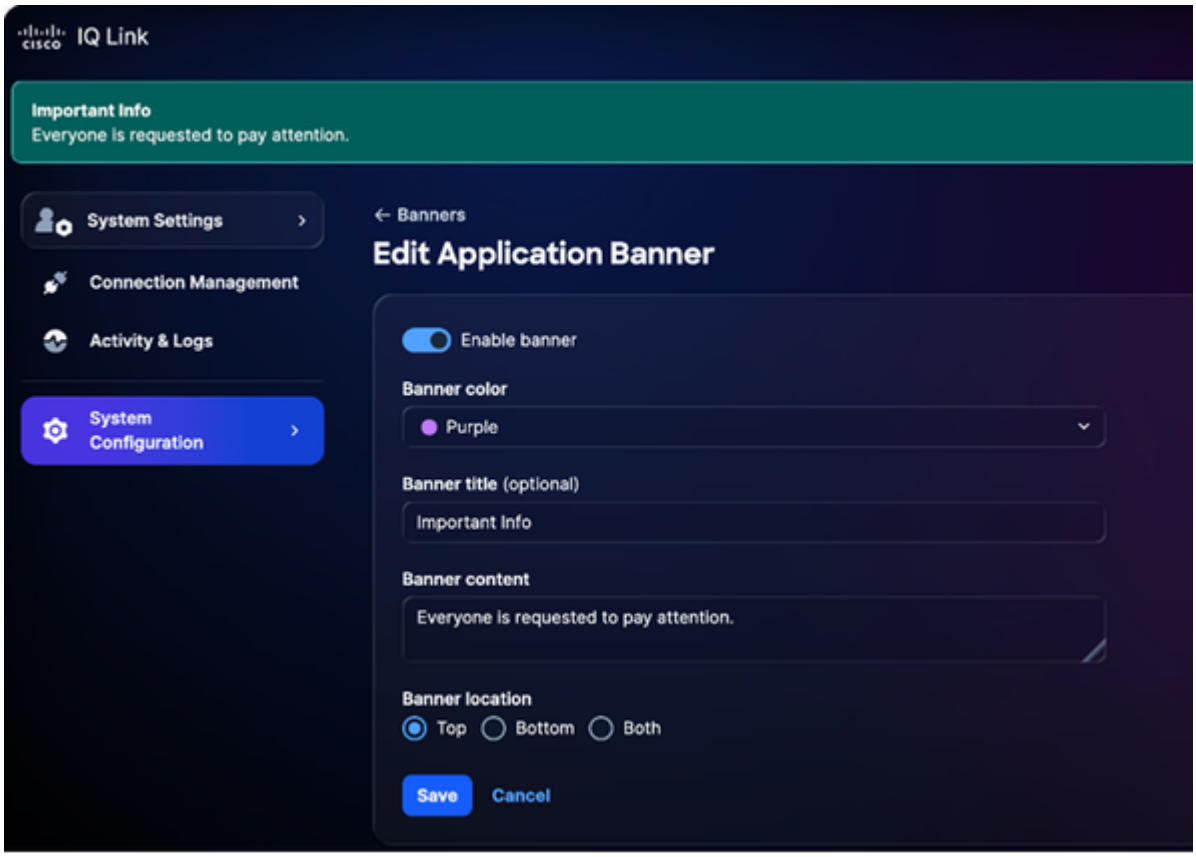
3. 点击切换以启用或禁用标语。
4. 选择Banner color。
5. 输入Banner title。
6. 输入Banner content。
7. 选择Banner location。
8. Click Save.横幅将在整个应用中显示。

编辑横幅

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。

编辑应用横幅

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：

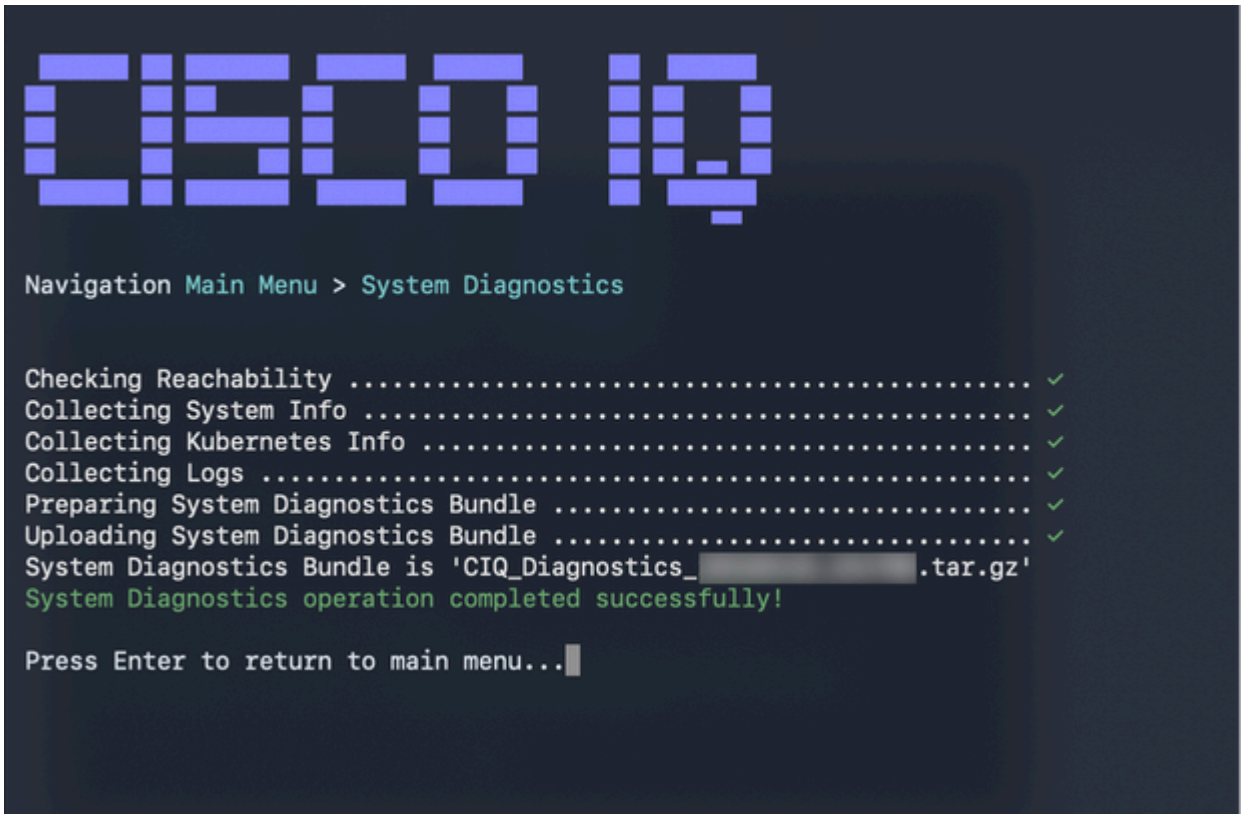
1. 登录到Cisco IQ。

主菜单

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

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。



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。

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）。