思科IQ链路操作指南v1.1.1

简介

Cisco IQ™为客户提供增强功能和特性，旨在改善资产可视性、在整个环境中提供更智能的见解，并简化案例管理。此外，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，使用户能够主动做出明智的决策，并简化客户参与和成功的流程。

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

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

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

设置本地管理员安全

您可以通过System Configuration中的Local Admin Security菜单更改密码并设置安全问题。

您有三(3)次尝试在十(10)分钟内输入正确的密码。如果所有三(3)次尝试均失败，您的帐户将临时锁定60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。

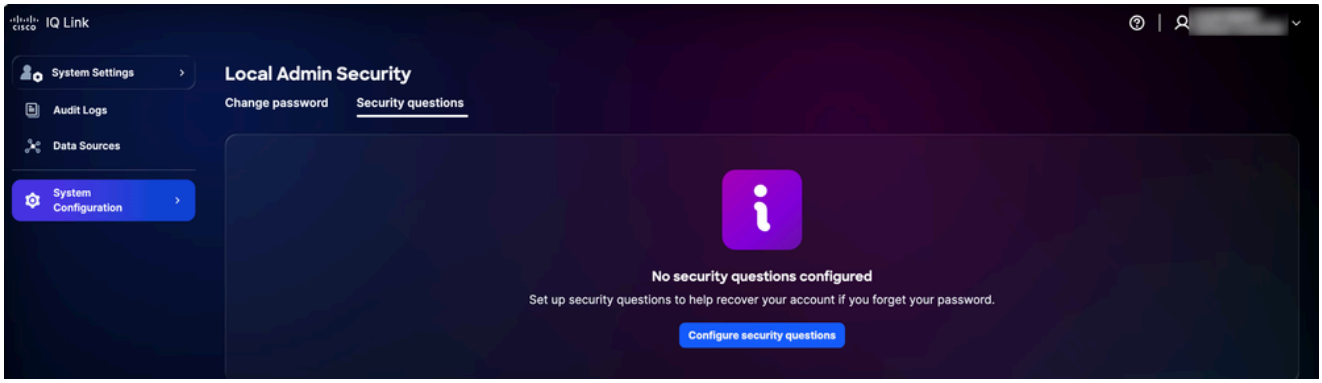
您的帐户将在60分钟后自动解锁，此时您可能会尝试登录或重置密码。

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。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。

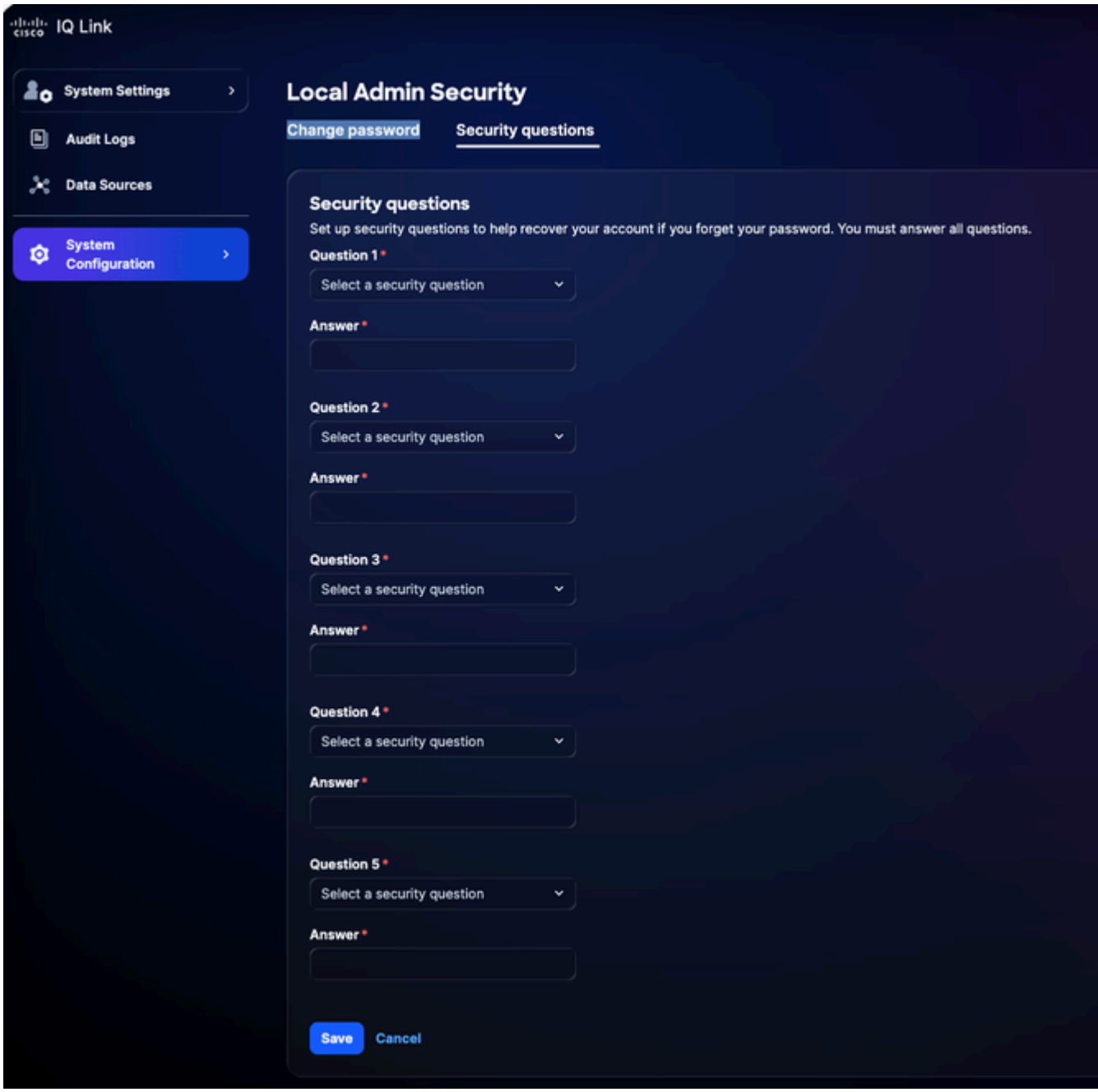
要设置安全问题，请执行以下操作：

1. 从System Settings中选择System Configuration > Local Admin Security > Security Questions。



安全问题

2. 单击配置安全问题。



安全问题

3. 从下拉列表中选择任意五(5)个安全问题。

4. 输入每个问题的回答。

5. 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，意味着“Smith”和“Smith”被相同地处理

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

只有本地管理员可以管理Cisco IQ的密码。

先决条件

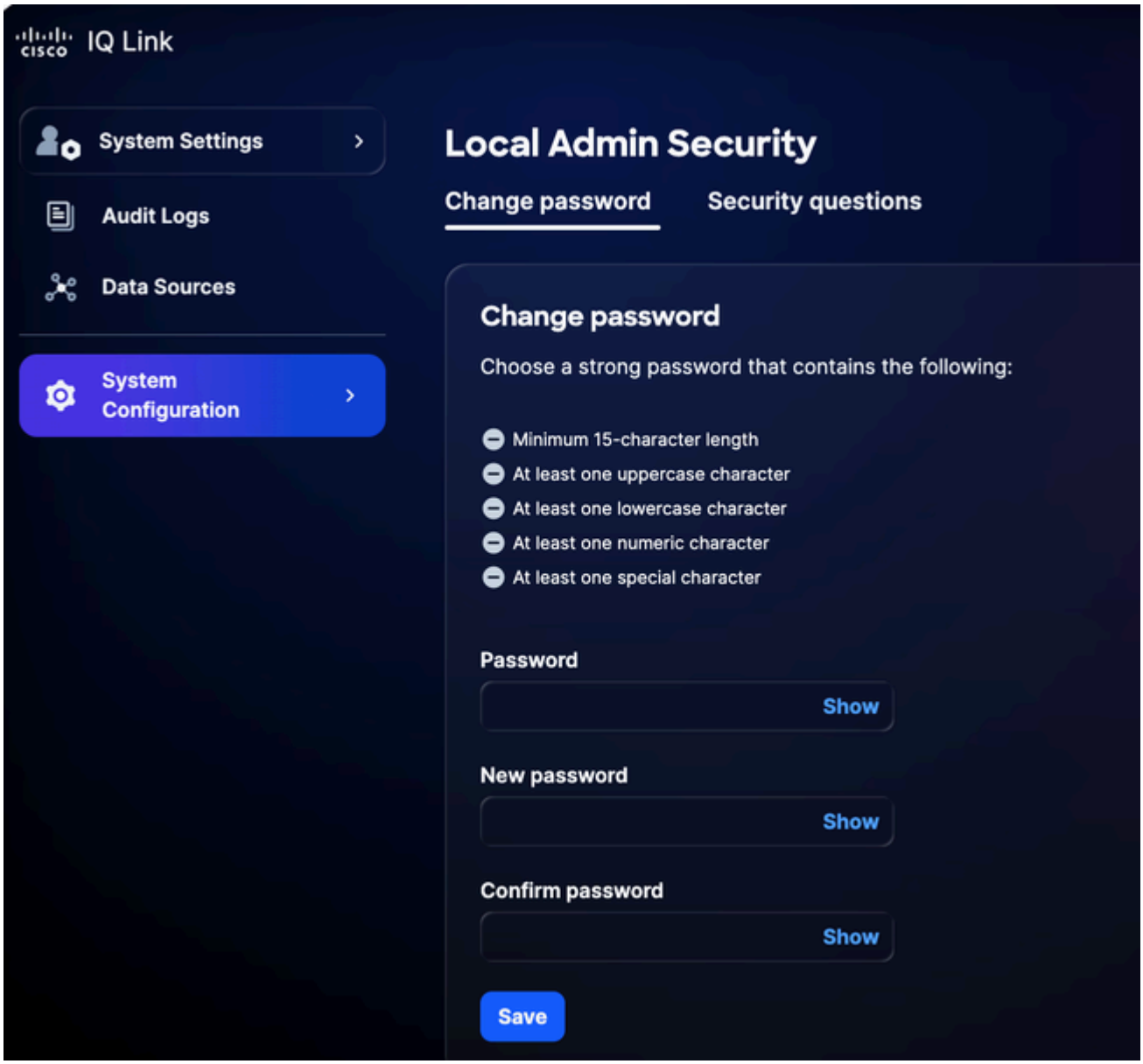
要管理密码，必须满足以下条件：

- 您是本地管理员
- 您使用的是本地管理员帐户(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. 从System Settings，导航到System Configuration > Local Admin Security > Change Password。



更改密码

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

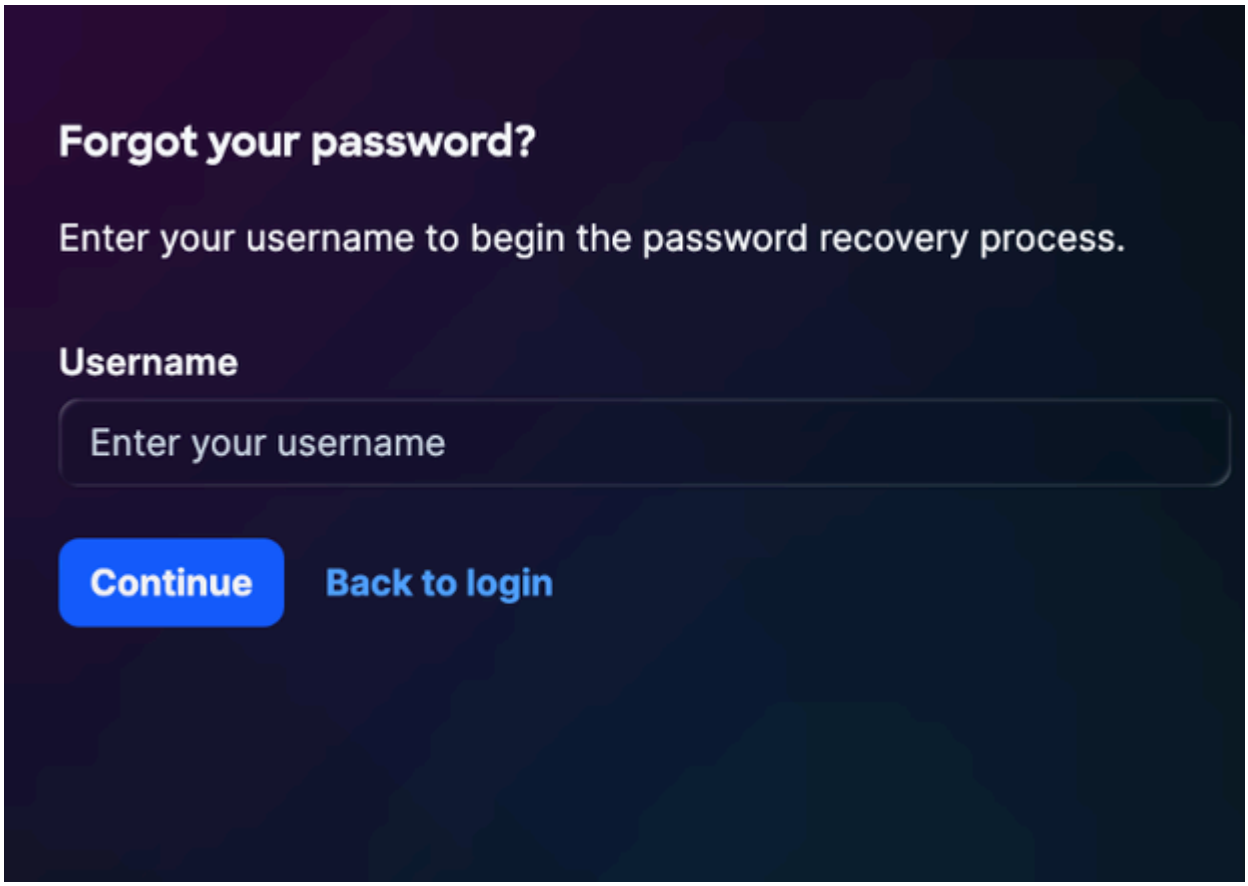
密码在Cisco IQ系统中更新，包括Cisco IQ虚拟机(VM)。

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。

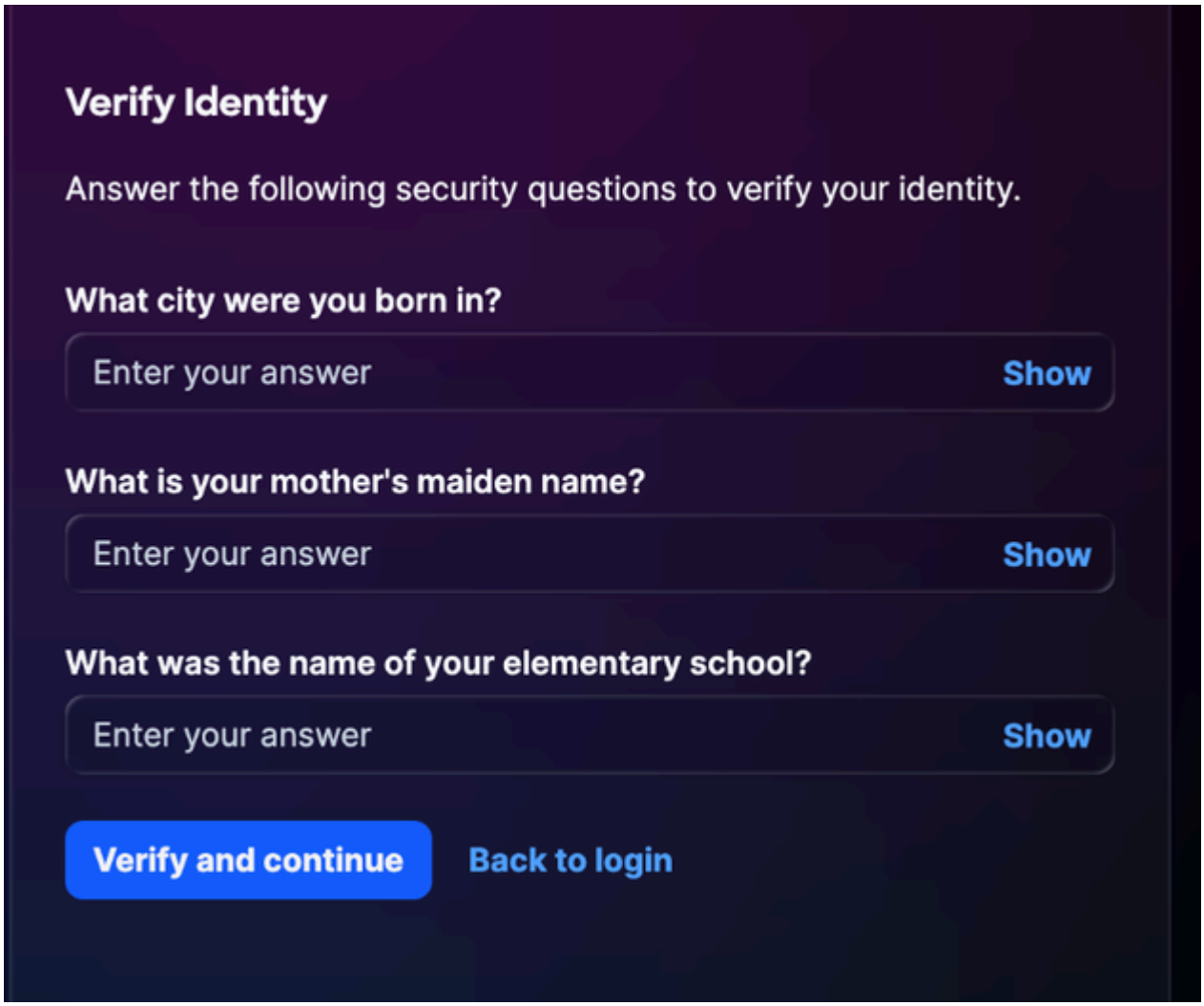
要重置忘记的密码，请执行以下操作：

1. 导航到Cisco IQ Link登录页面。
2. 单击忘记密码。



忘记了密码

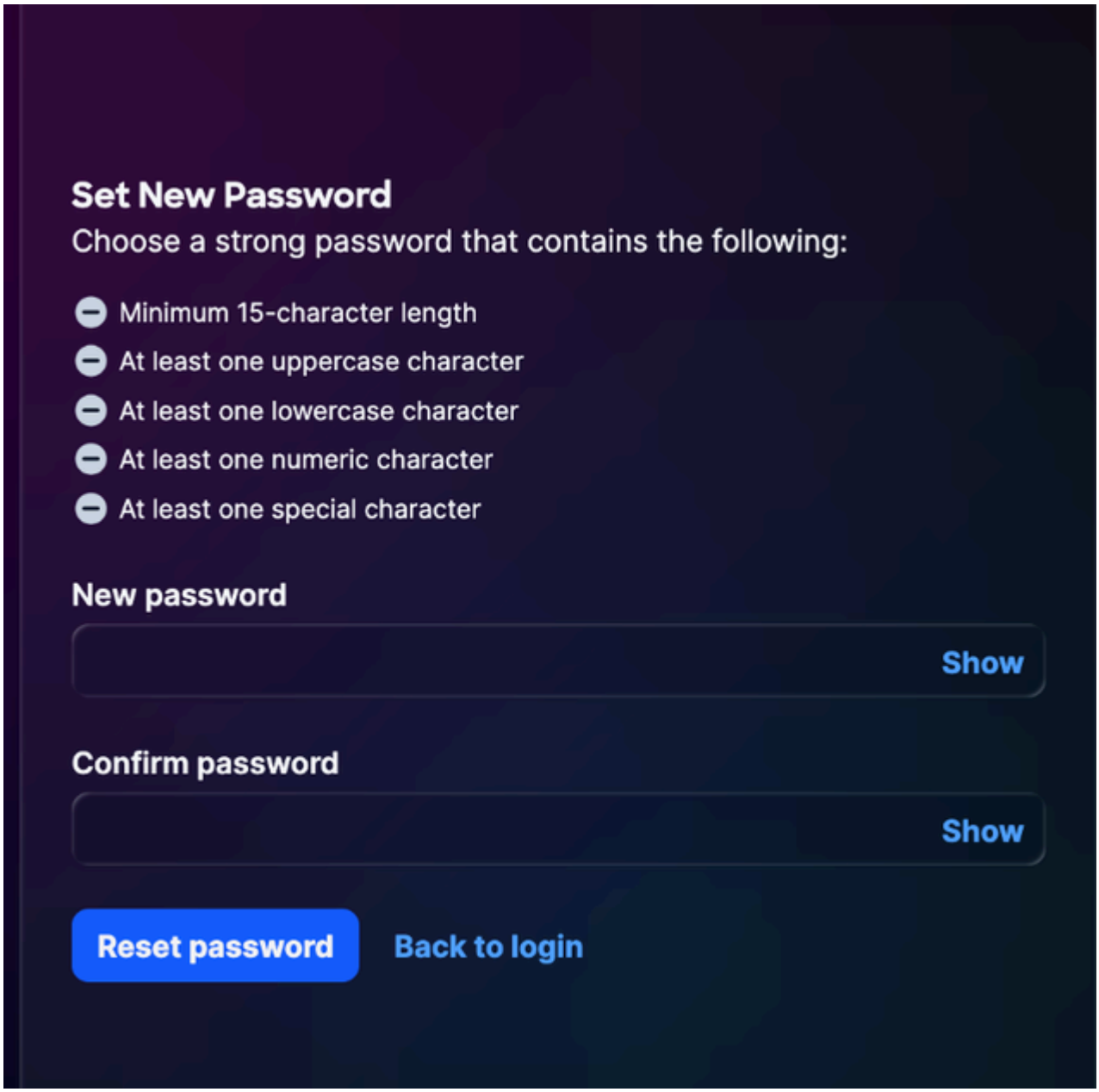
3. 输入用户名。
4. 单击 Continue。Verify Identity页显示先前配置的五(5)个问题中的三(3)个随机安全问题。



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)个显示问题的回答。
6. 单击Verify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

注意：
·在十(10)分钟内，您有三(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60分钟以保护您的安全。
·在锁定期间无法重置密码。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。
·您的帐户将在60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。

配置身份提供程序

登录到Cisco IQ Link后，管理员可以配置各种设置。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 Link。

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 Link
- 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。

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”

SAML配置参数

参数	配置	示例
受众（实体ID）	FQDN名称	mymanagementhost.mydomain.com
单点登录URL	SAML ACS终端	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. 在应用中配置单一注销(SLO)设置。

SLO配置设置

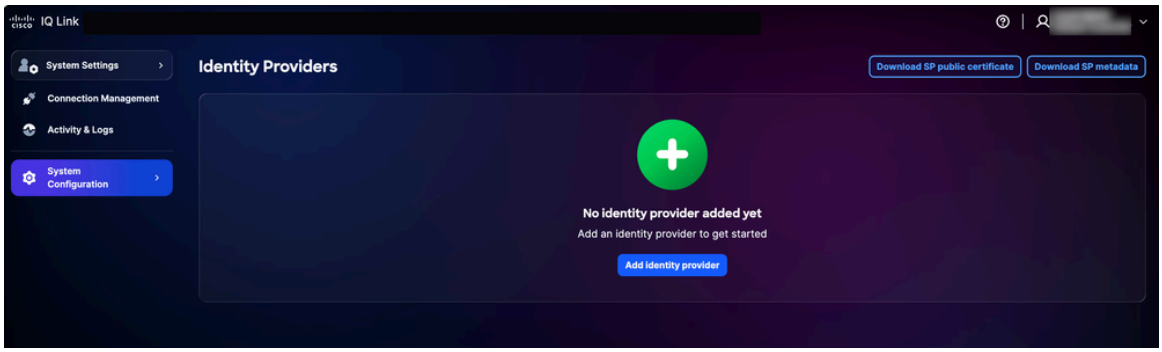
字段	价值
签名证书	对于Okta，只有当您选择启用SLO时，才需要此证书。使用身份提供程序中的下载SP证书下载签名证书。将文件另存为sp-public-key.crt。有关详细信息，请参阅单一注销配置。
SP元数据	仅ADFS IDP需要SP元数据（Okta不需要）。
是否要启用单一注销	是或否
单一注销URL	https://mymanagementhost.mydomain.com/saml/logout
SP颁发者（受众/实体ID或ACS URL）	https://mymanagementhost.mydomain.com

5. 单击Download图标下载“SP Metadata”文件。
6. 根据提供商的要求调配或创建应用。

添加IDP

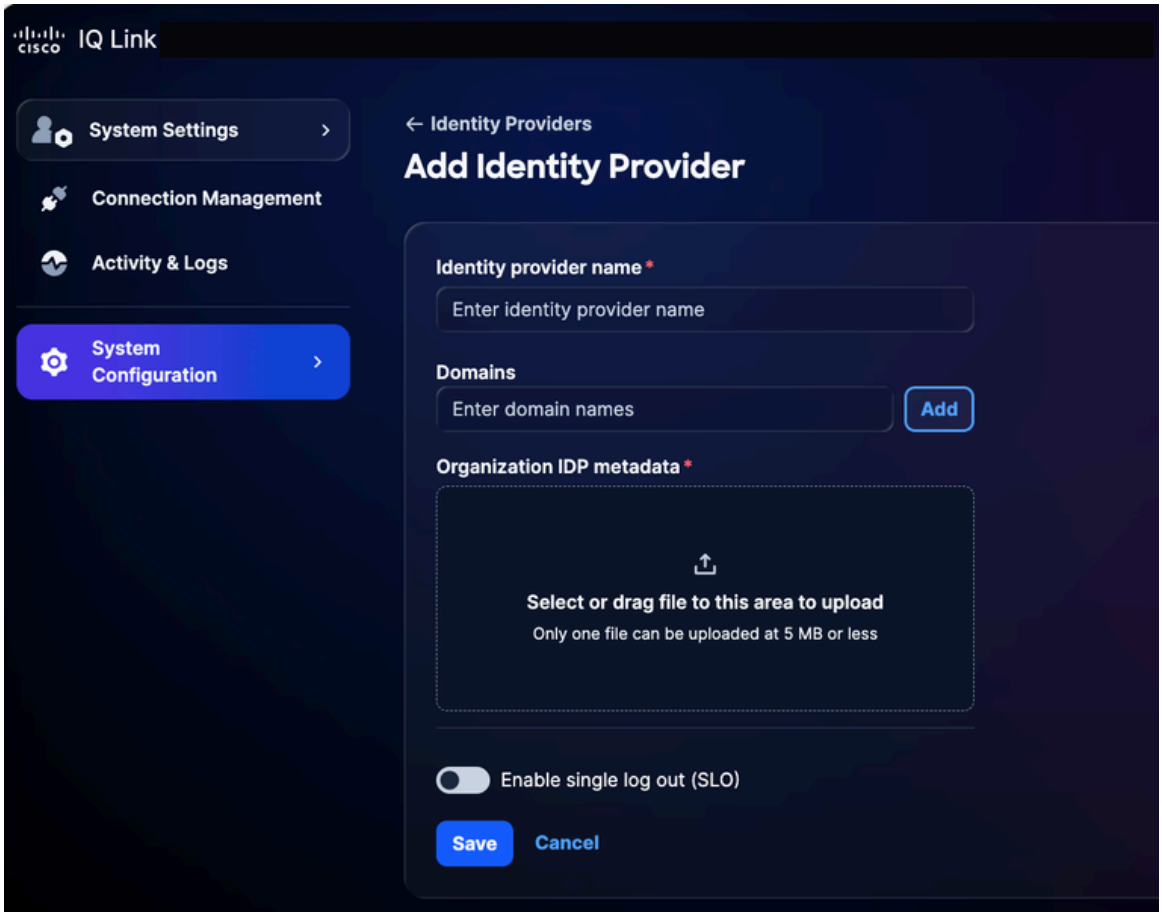
要在Cisco IQ链路中添加IDP，请执行以下操作：

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。

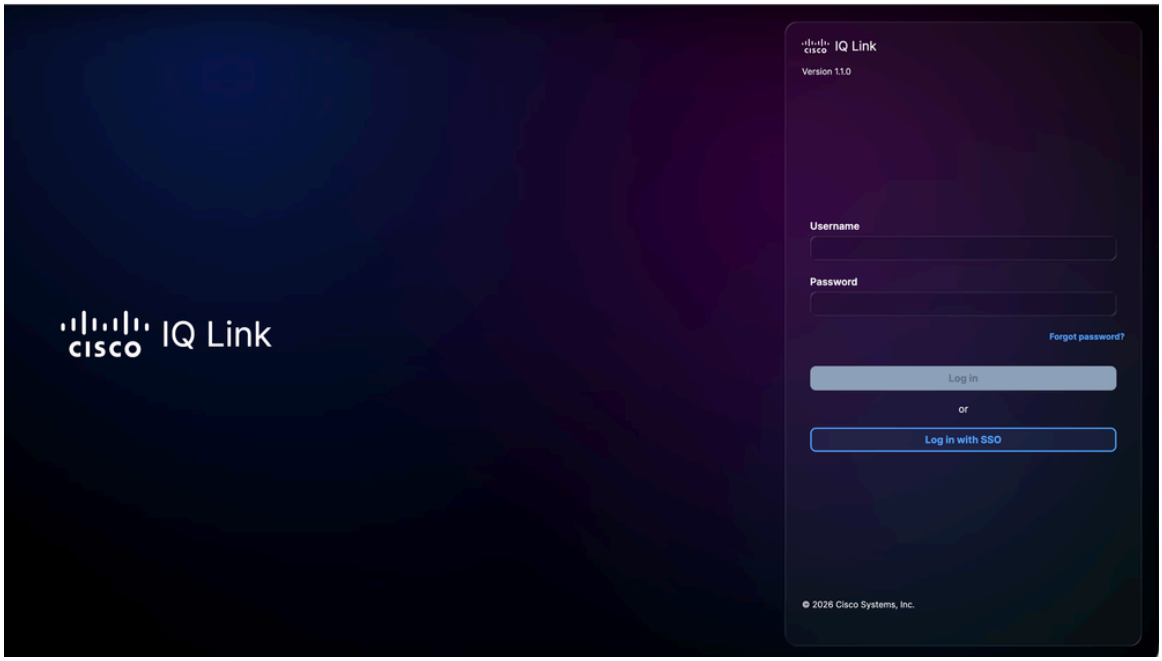
4. 点击Add以将已配置的Cisco IQ Link域名添加到Domains字段。

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. Click Save.

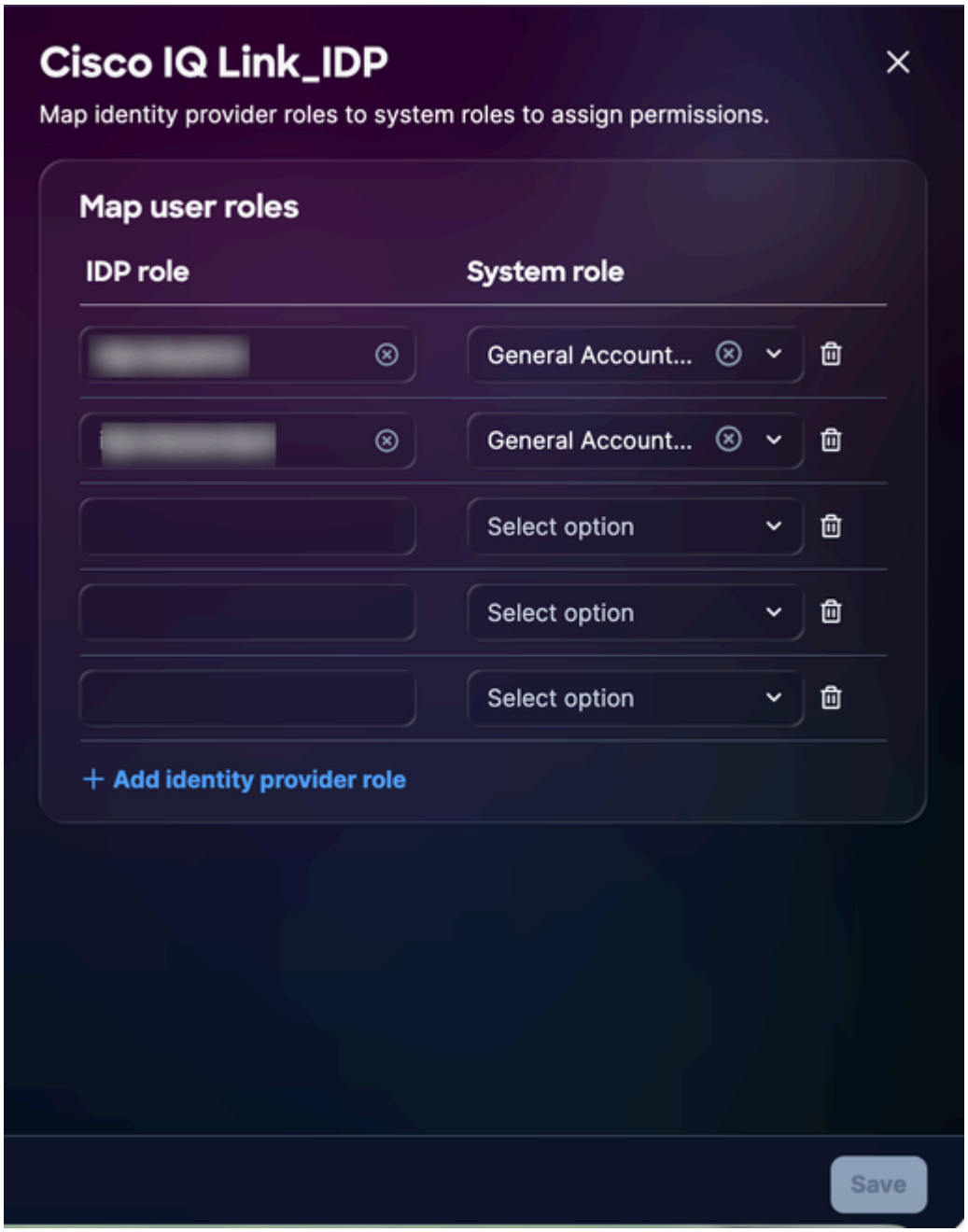
8. 配置后，登录页面会显示一个选项，用于通过IDP登录SSO。



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。

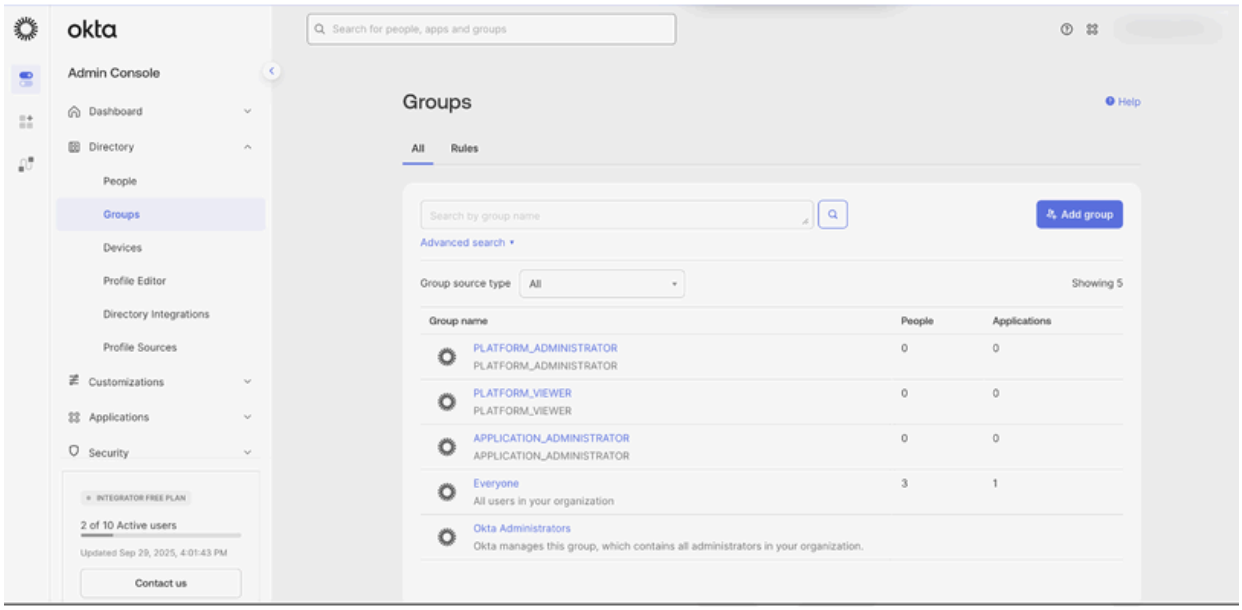


用户角色映射

2. 输入所选系统角色的IDP角色。支持以下系统角色：

   - general_account _administrator:一般帐户管理员具有执行产品中所有操作的完全权限
   - general_account _viewer: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

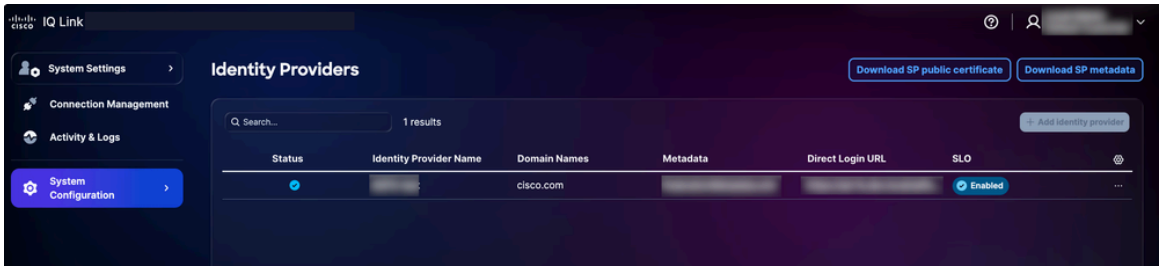
3. 通过点击添加身份提供程序角色根据需要映射其他角色。

4. Click Save.

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

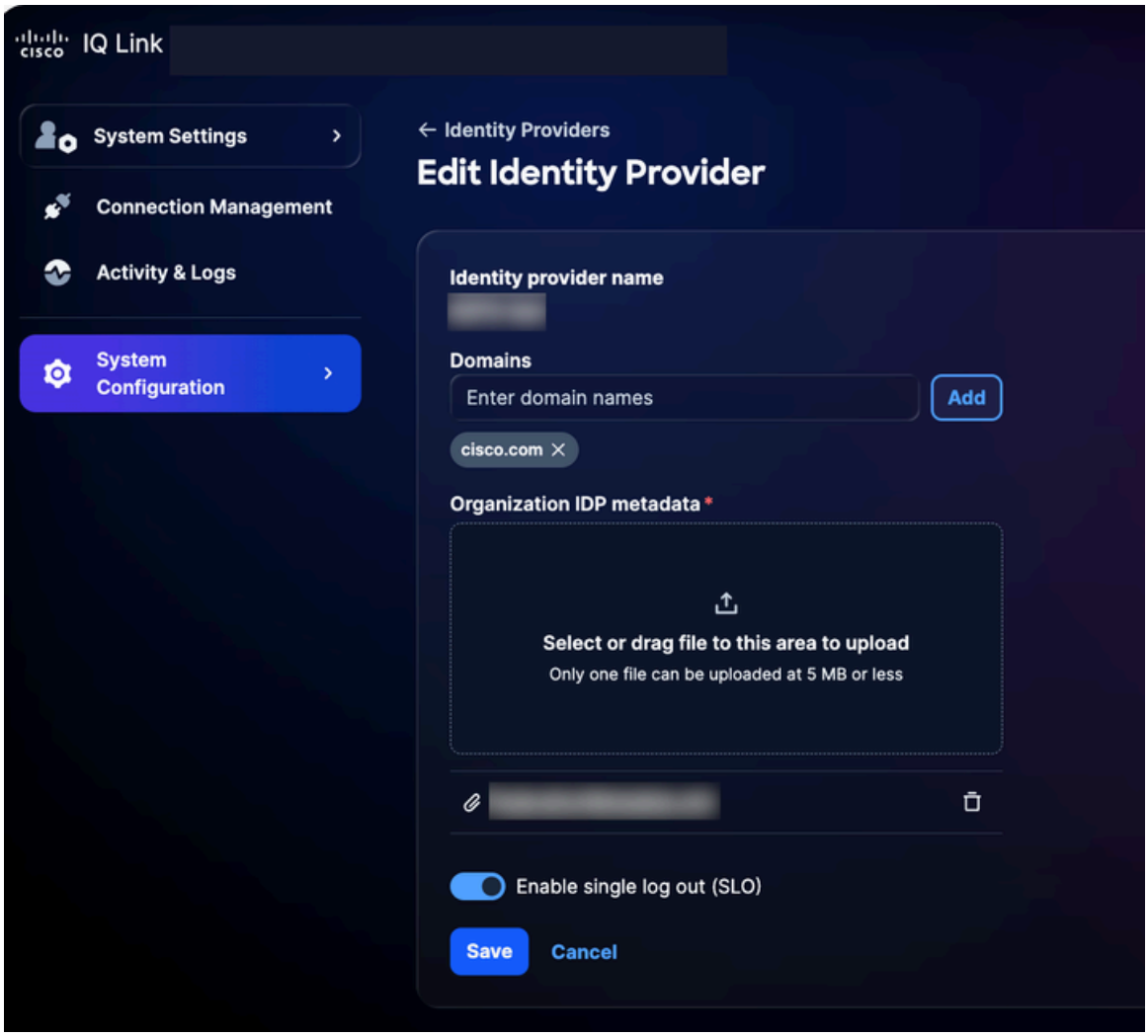
2. 将下载文件另存为sp-public-key.crt。

3. 导航到您的IDP门户。

4. 上传IDP SAML Configuration for SSO部分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：

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+
- 已配置的Active Directory集成

- ADFS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
- ADFS服务器配置详细信息（如下表所示）

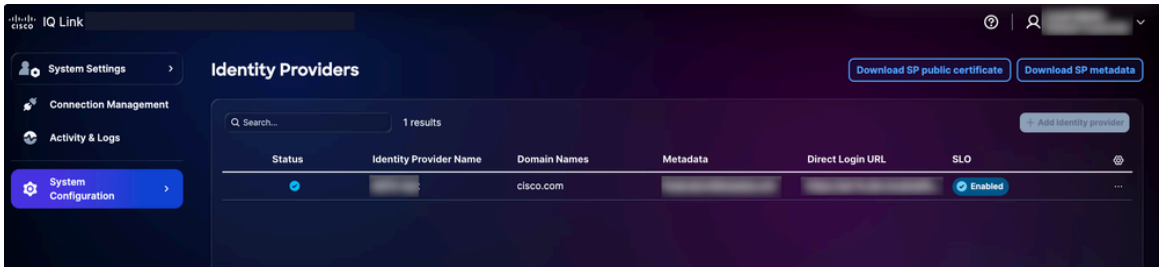
ADFS服务器配置

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	Active Directory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，从文件导入有关信赖方的数据。
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“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。

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。

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

领款申请	目的	来源
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”, Issuer == “AD A
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/ws/2005/05/identity/claims/ema

@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.Issu

@RuleName = “Send Group Membership”
c:[Type == “http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname”, Issuer == “AD A
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/claims/Group”), query = “;memb
’@@
```

3. 通过运行以下命令应用声明规则：

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

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. 选择下列选项之一：

注意：SP证书由内部证书颁发机构颁发，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

- 将颁发CA证书导入受信任的根证书颁发机构库

```
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
```

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。

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。

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）如果需要，请打开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Active Directory中找到用于映射的组。要从Active Directory中查找组，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LDAP查询Active Directory，无需其他模块。组信息以完整的可分辨名称(DN)格式返

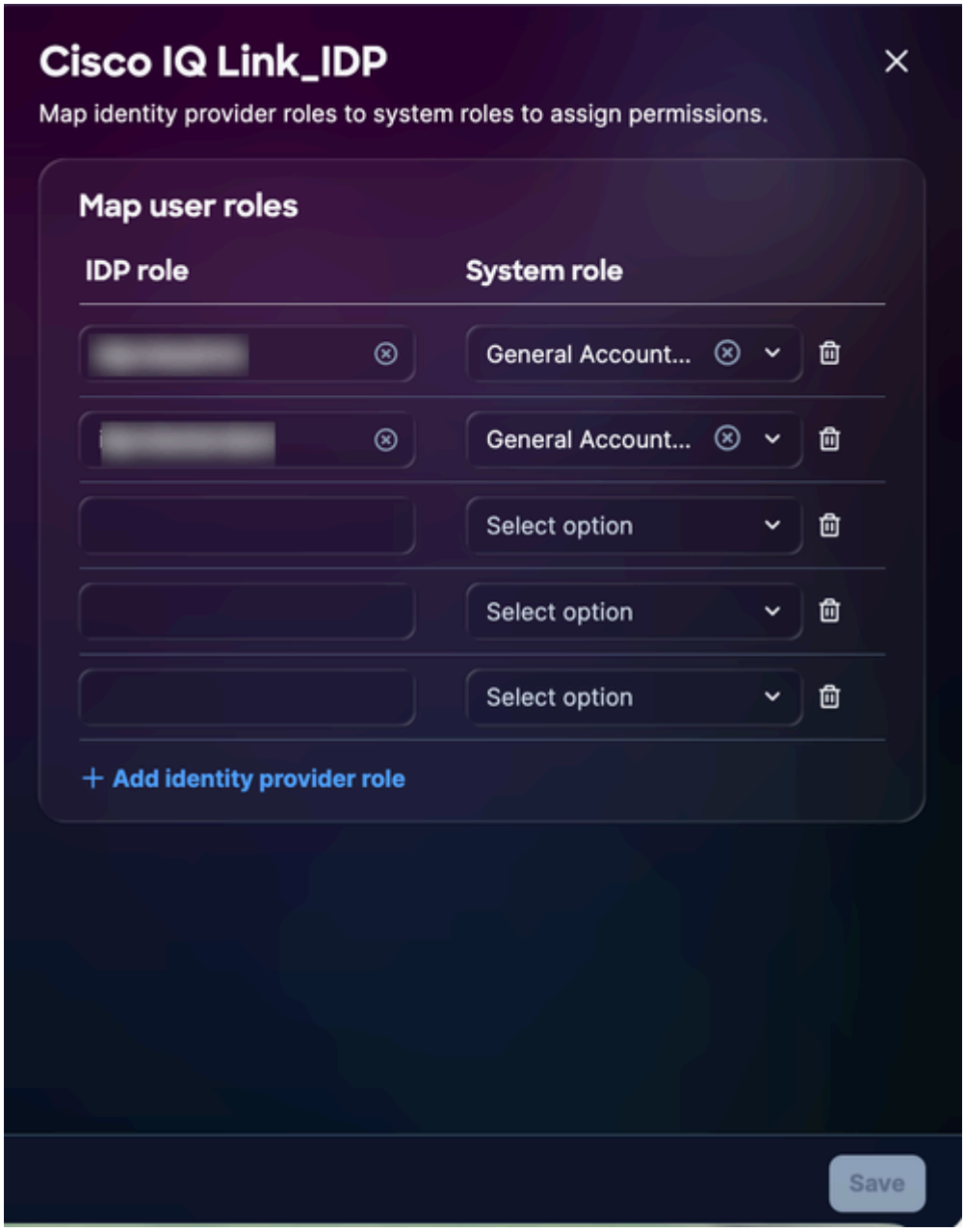
回，例如：

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

如果所需的组未列出，则管理员必须在Active Directory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：

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：

   - general_account _administrator: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。
   - general_account__viewer:常规帐户查看器具有只读访问权限。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. Click Save.状态更新为Success。

验证和测试

测试验证

1. 在Incognito或Private模式浏览器中，导航至https://your-cisco-iq-domain.com/login。
2. 使用域\用户名或user@domain.local格式的Active Directory凭证登录。
3. 验证您已被重定向到Cisco IQ主页（在身份验证成功后）。
4. 确认已分配的角色在用户配置文件中显示正确解析的组名（例如，CXIQ开发人员）。

测试注销

要测试注销，请点击从Cisco IQ注销。系统随即会显示“Logging out， please wait..”（注销，请稍候……）消息，您将被重定向到Cisco IQ Login页面。系统还会终止ADFS会话。如果您尝试直接访问ADFS，系统会提示您重新登录。

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。

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	●缺少索赔规则:重新运行配置ADFS声明规则中的说明 ●错误的组属性:必须是http://schemas.xmlsoap.org/claims/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

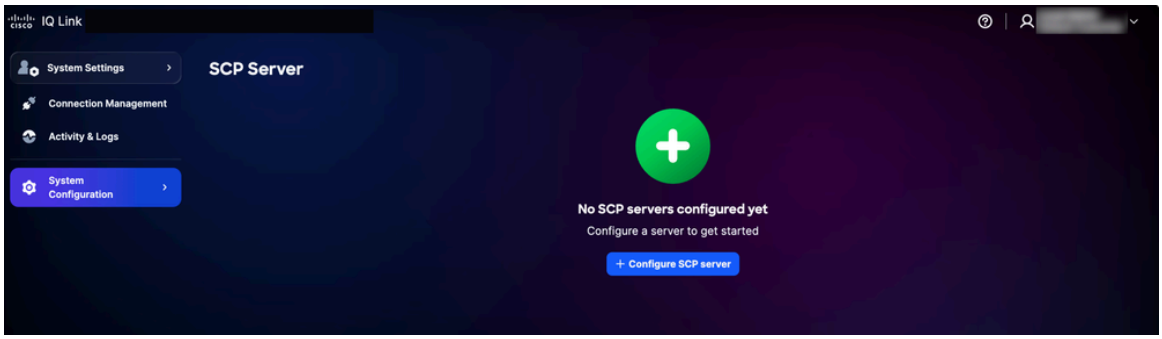
```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object SamlEndpoints
```

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先决条件，这些文件对于添加、升级或修复Cisco IQ安装至关重要。

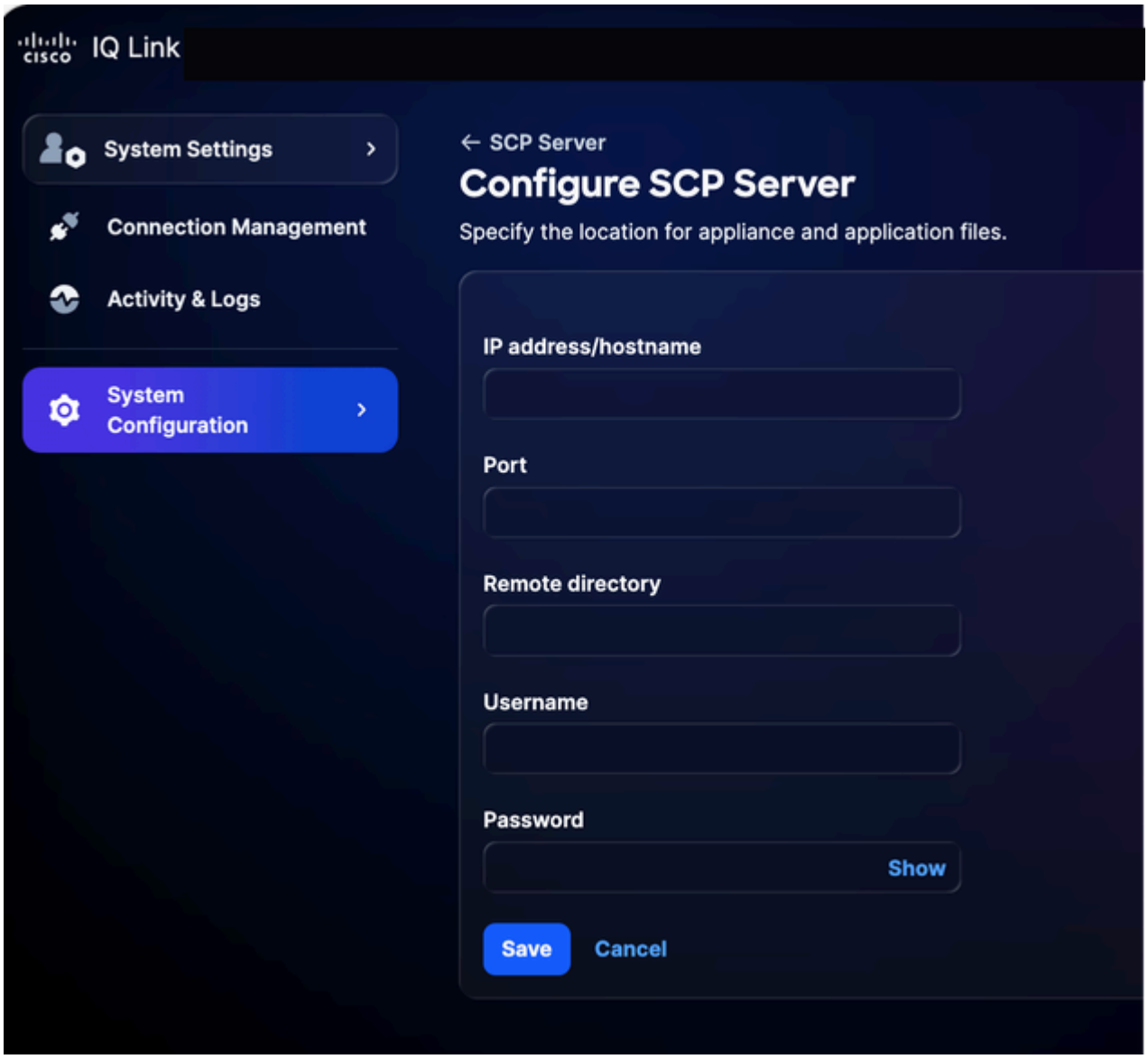
添加SCP服务器的步骤：

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。



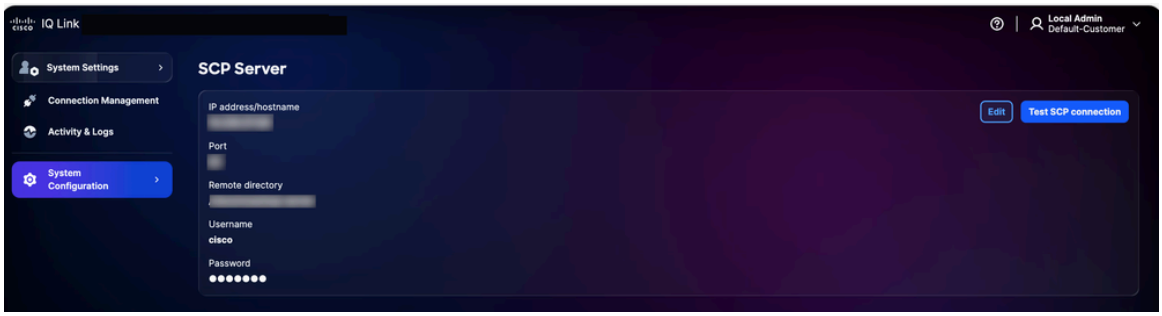
配置SCP服务器

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

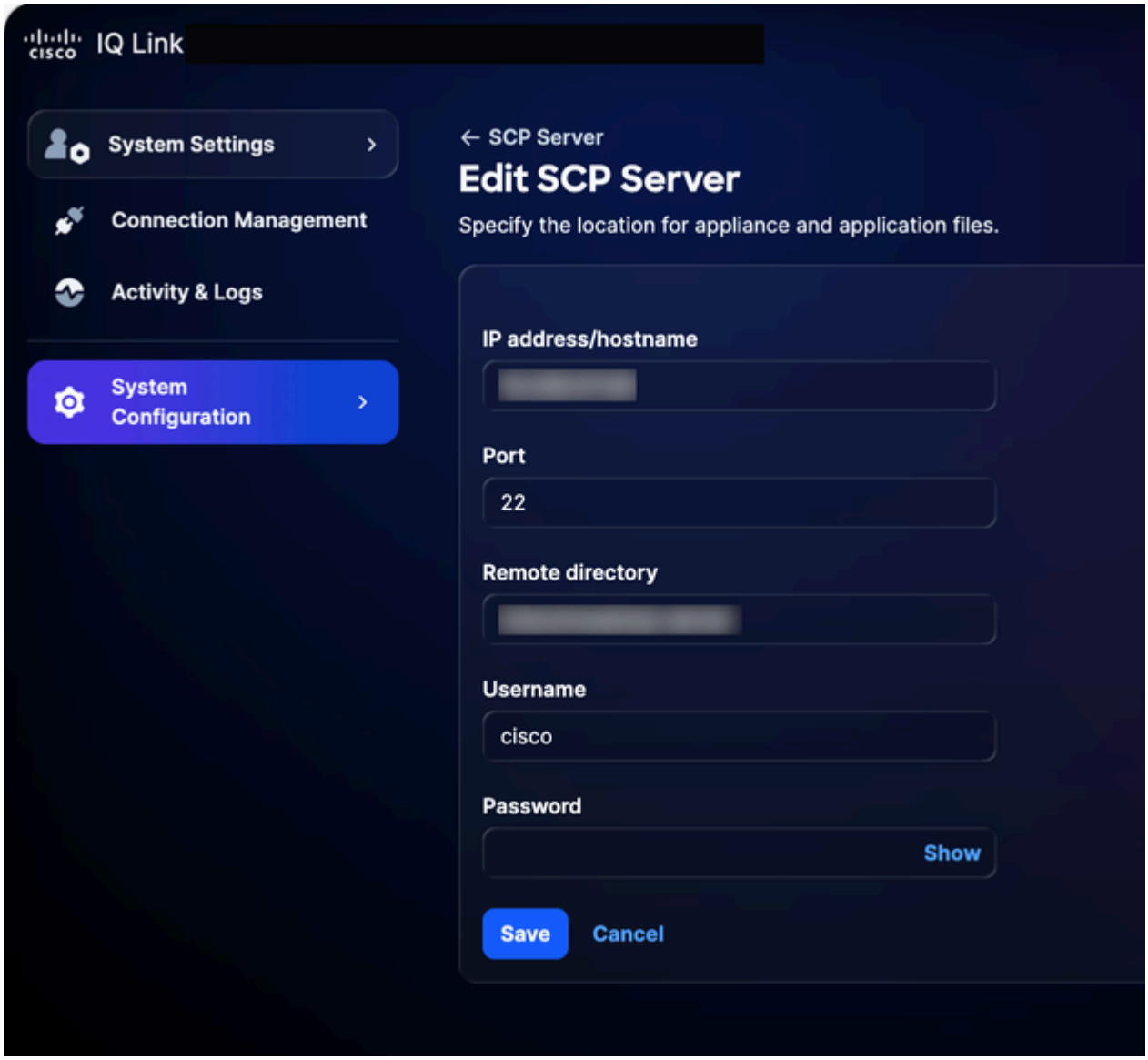
要编辑现有SCP服务器，请执行以下操作：

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.

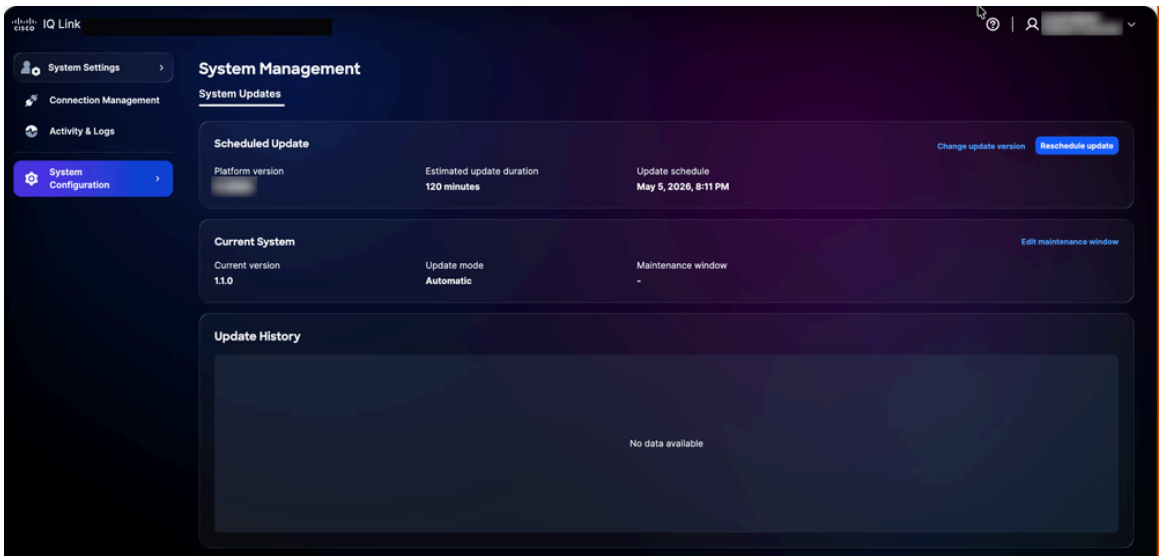
系统管理更新

客户可以通过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

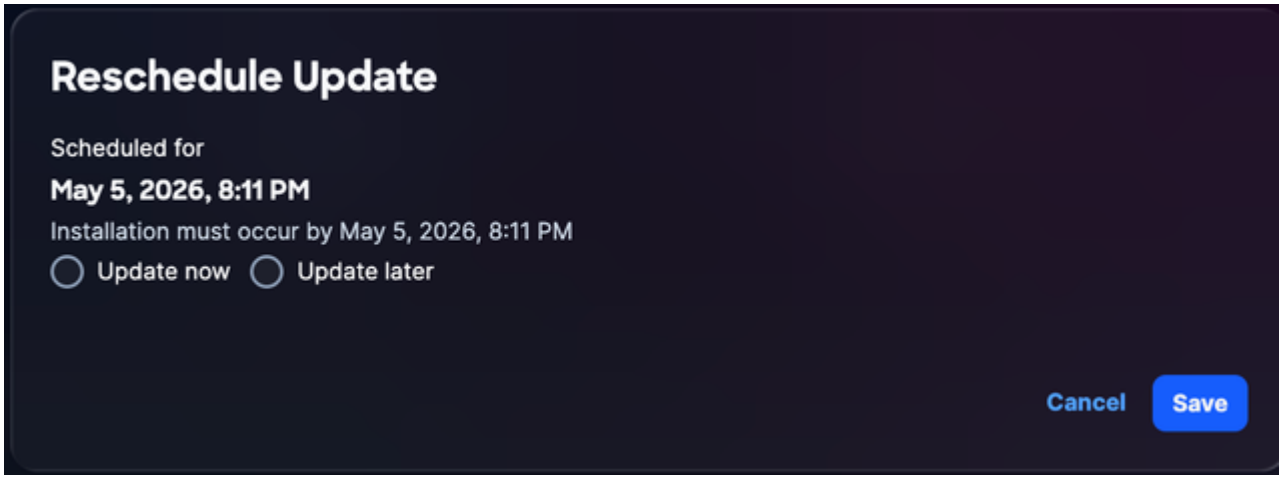
要重新计划系统更新，请执行以下操作：

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。



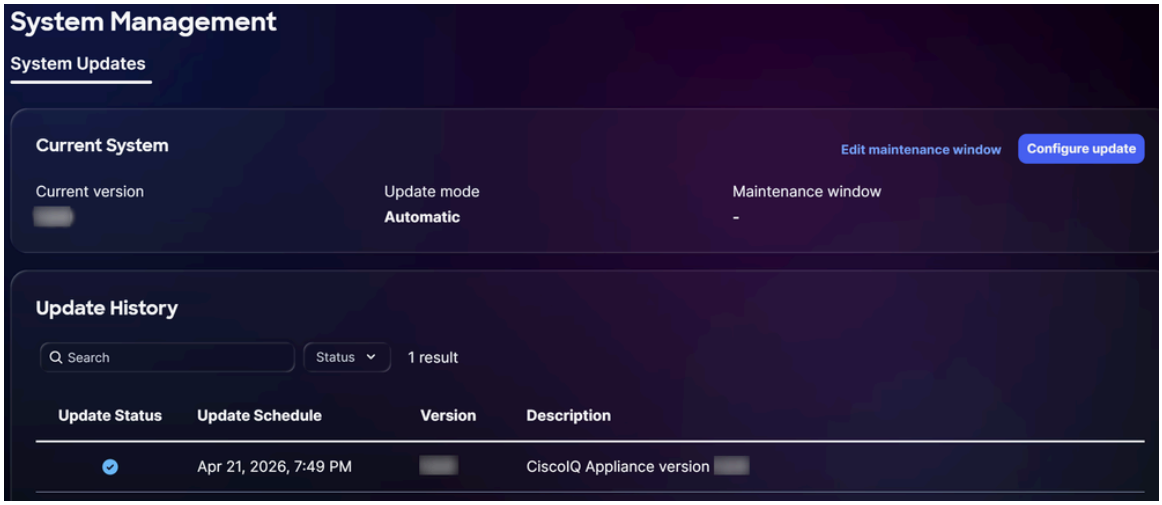
系统升级

2. 单击Reschedule update。



重新安排升级

3. 单击Update Now立即重新计划，或单击Update Later安排其他时间。
4. Click Save.系统将显示一个确认消息，您将被重定向到系统更新主页。



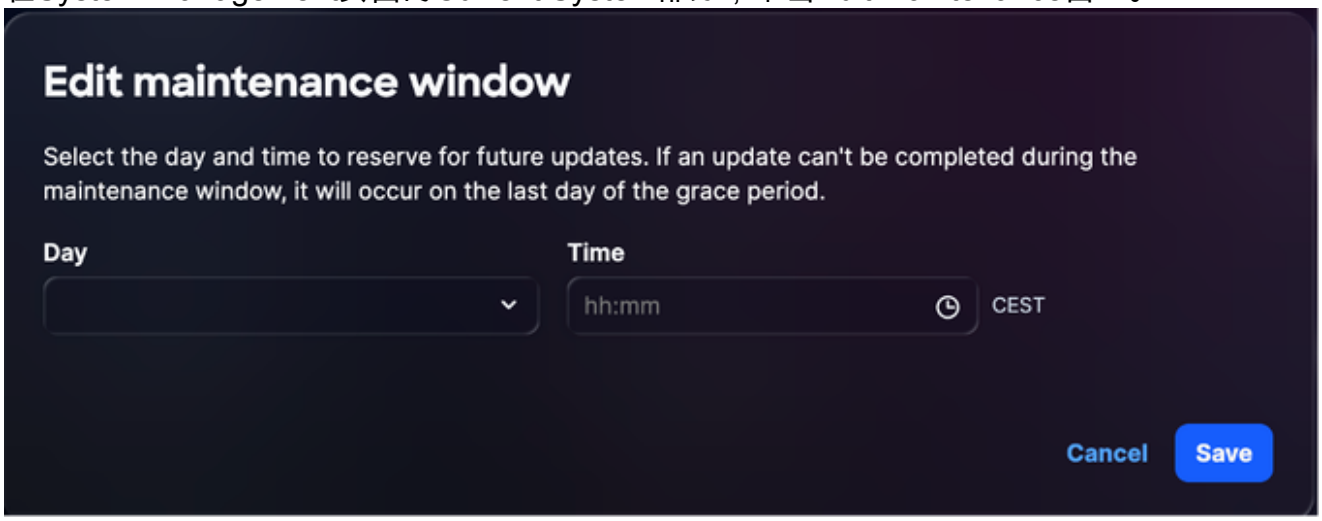
升级成功

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。

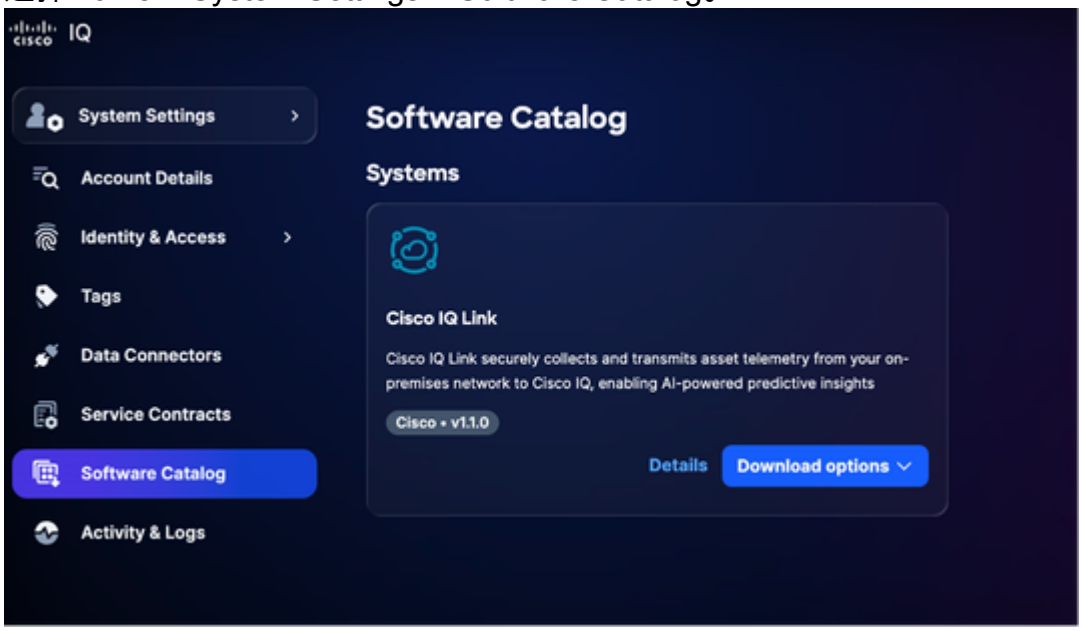
注意：
·如果未配置升级计划，系统默认为两(2)周（对于非重启升级）和四(4)周（对于需要重启的升级）的宽限期。在这些宽限期之后，必须手动执行更新。
·如果升级失败，系统最多执行两(2)次自动重试。已安排第三次尝试，但需要手动启动。

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。

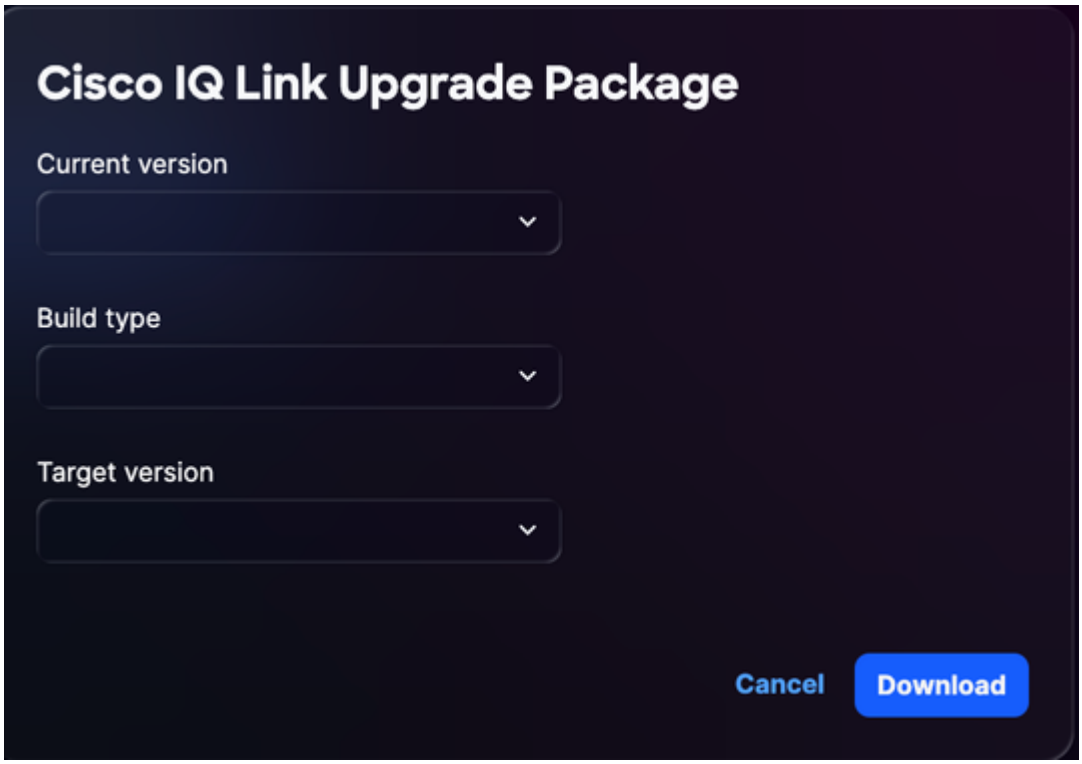
要手动升级系统，请执行以下操作：

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



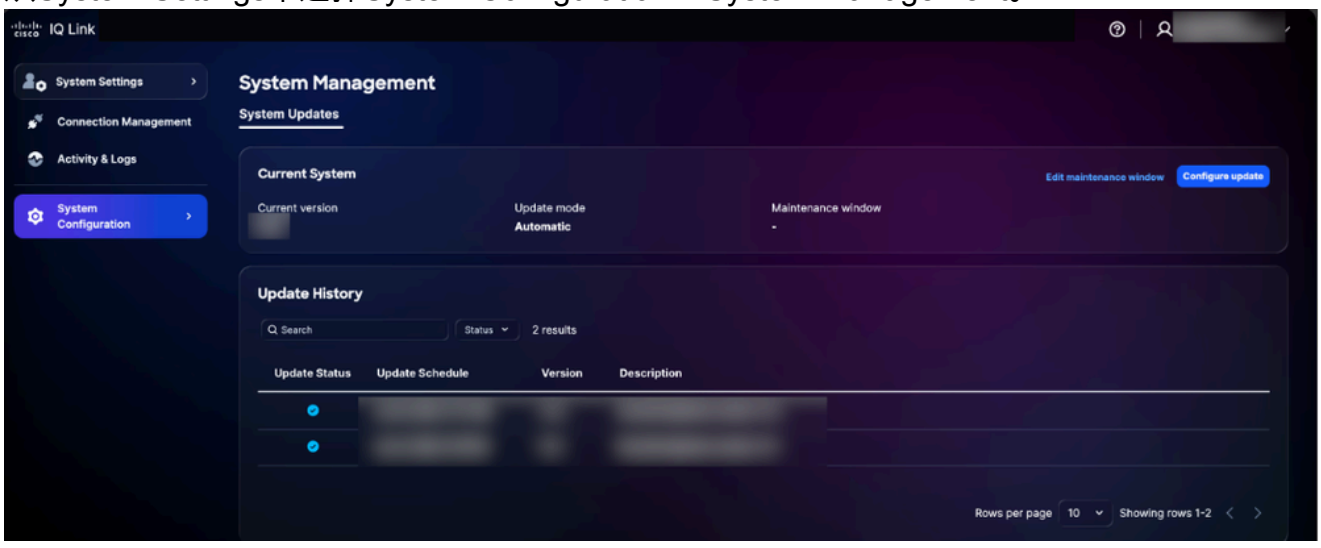
软件目录

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



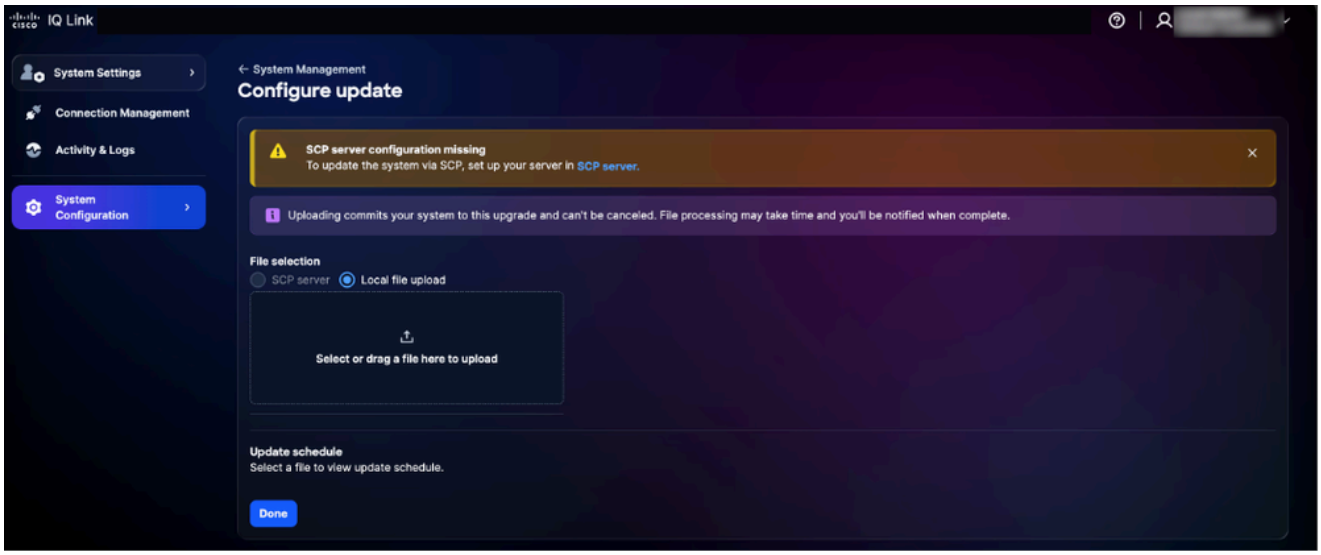
升级包

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. 导航到Cisco IQ Link。
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. 单击Done。系统成功更新后，系统会显示确认消息。

SSL证书配置

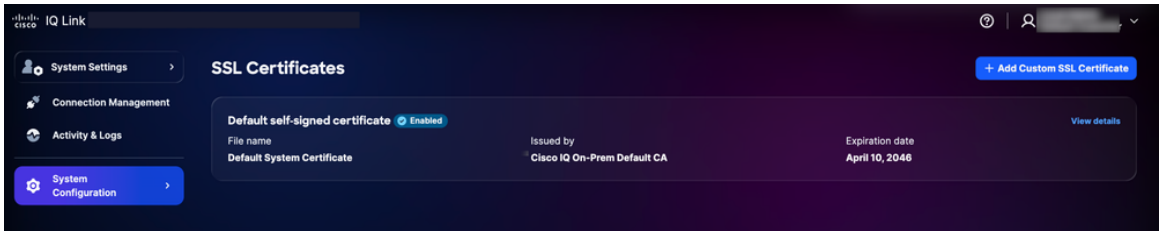
Cisco IQ中预安装并启用了默认自签名证书，但用户可以上传自定义SSL证书。启用自定义SSL证书时，该证书用于HTTPS连接；如果证书被禁用或删除，系统会自动恢复为默认证书。

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，客户必须按照Okta IDP或ADFS IDP的完成SLO配置部分所述上传新的SSL。

添加自定义SSL证书

要添加自定义SSL证书，请执行以下操作：

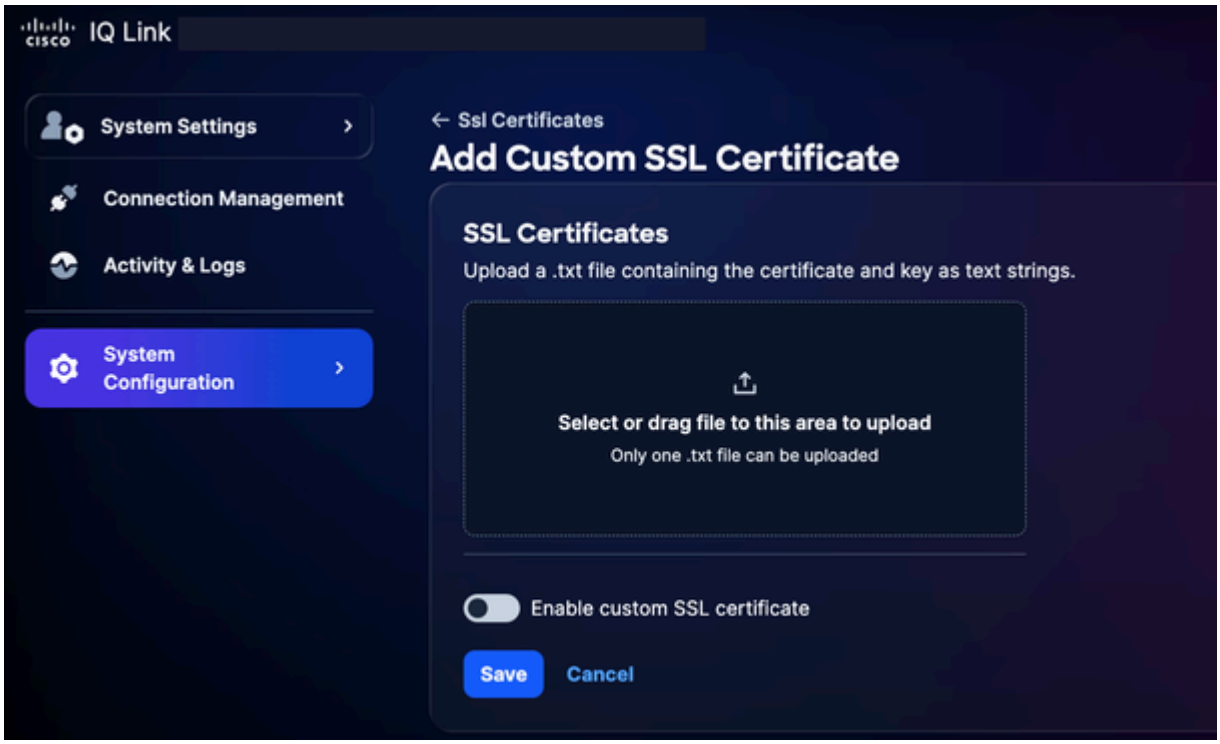
1. 从System Settings中，选择System Configuration > SSL Certificates。系统将显示SSL Certificates页面，其中列出了系统的所有SSL证书。



添加SSL证书

2. 单击Add Custom SSL Certificate。

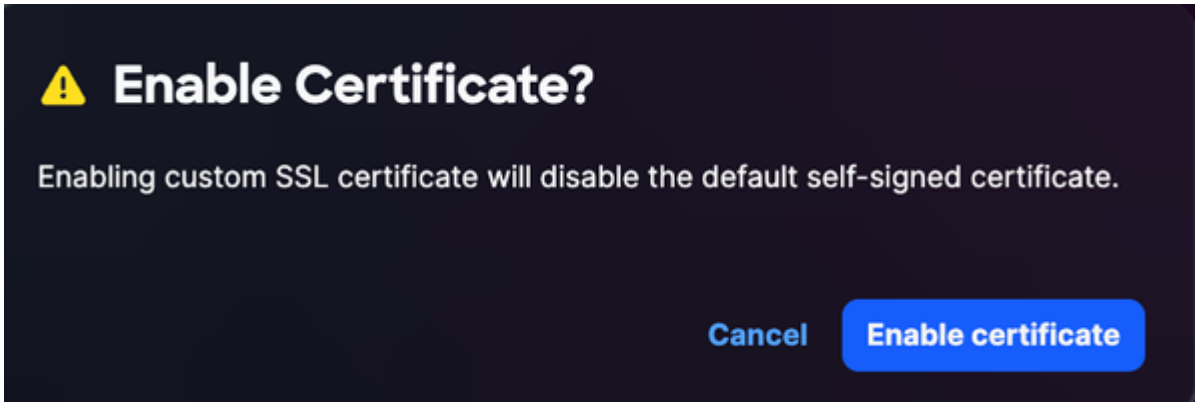
注意：
·上传包含隐私增强型邮件编码证书和密钥作为文本字符串的.txt文件
·一次只能上传一个.txt文件
·文件必须同时包含证书和私钥



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。



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. 点击启用证书。

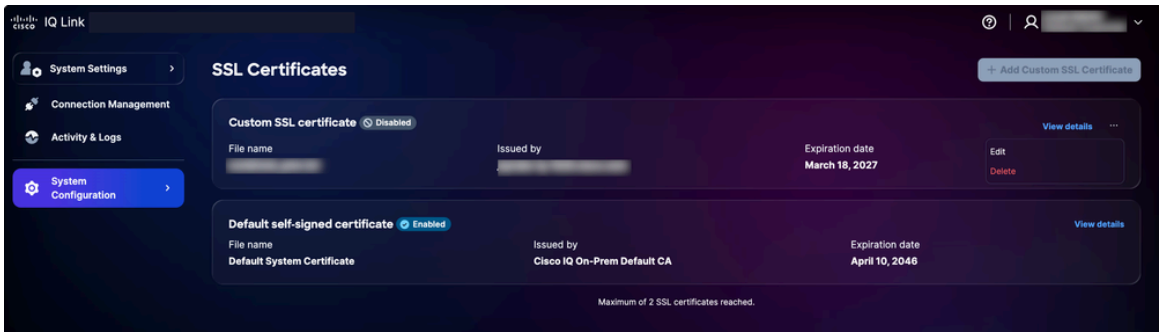
6. Click Save.

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。



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。

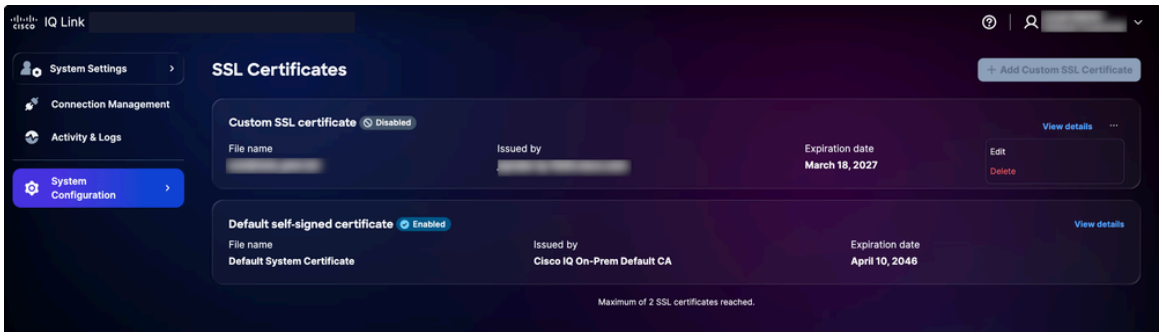
4. Click Save.

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. 导航到所需的个人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

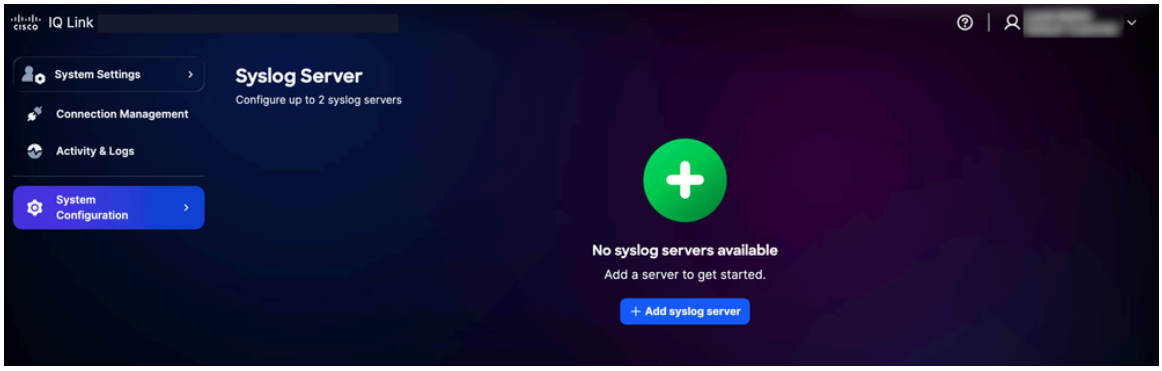
具有管理员角色的用户可以配置外部系统日志服务器以导出系统日志。最多可以配置两(2)台系统日志服务器。

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

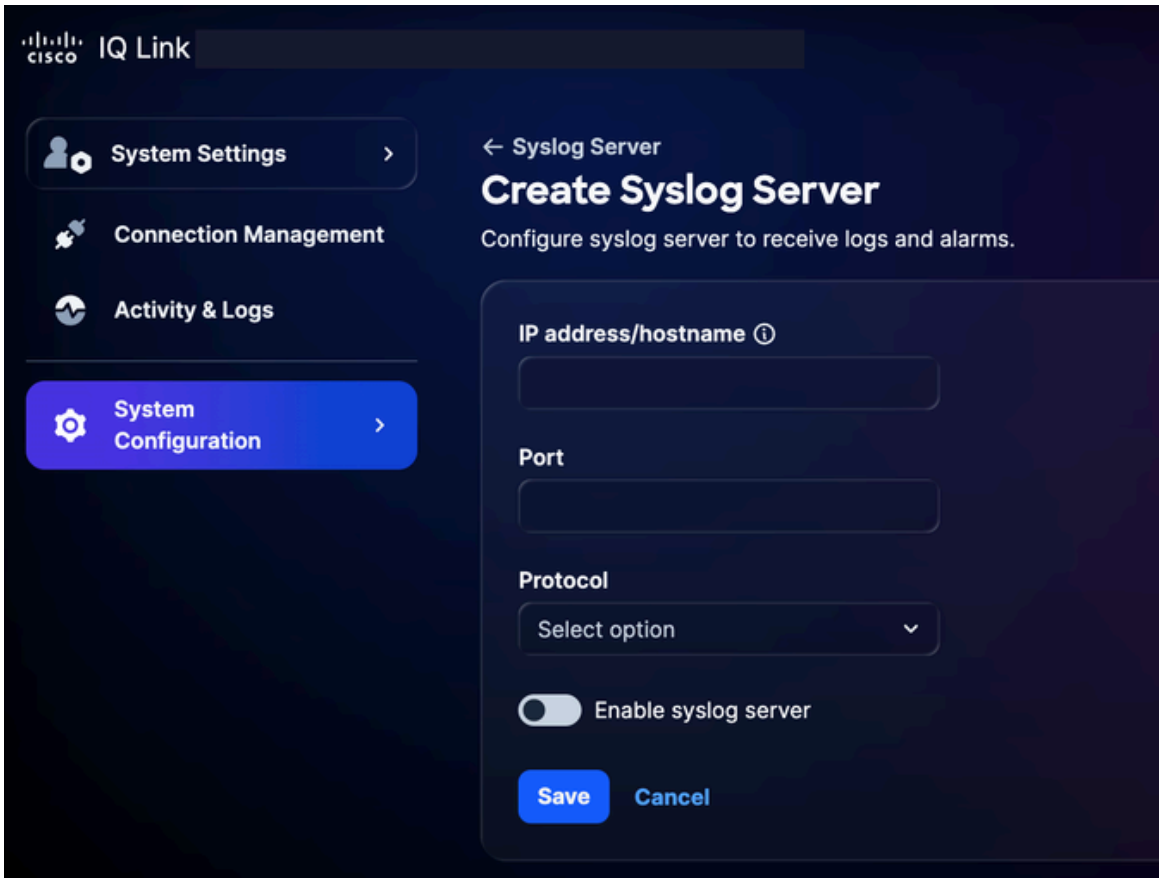
添加系统日志服务器的步骤：

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。



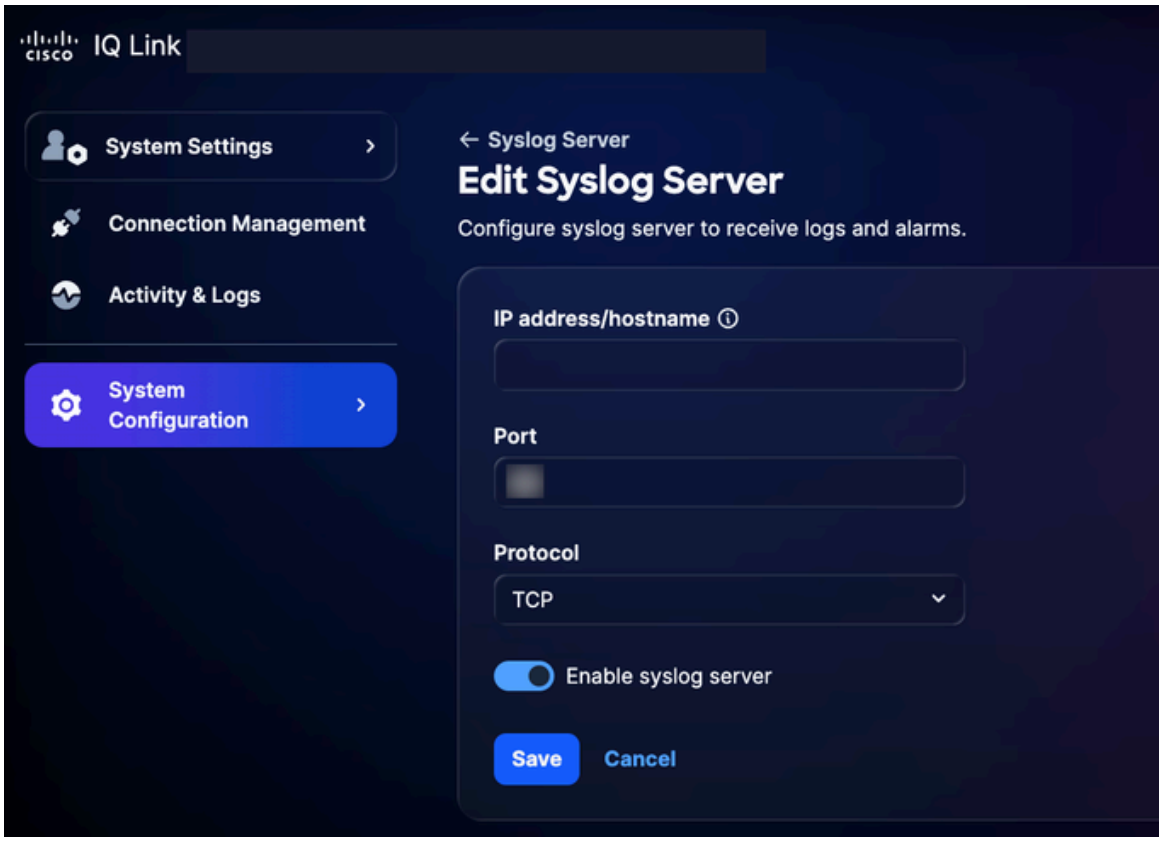
创建系统日志服务器

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。



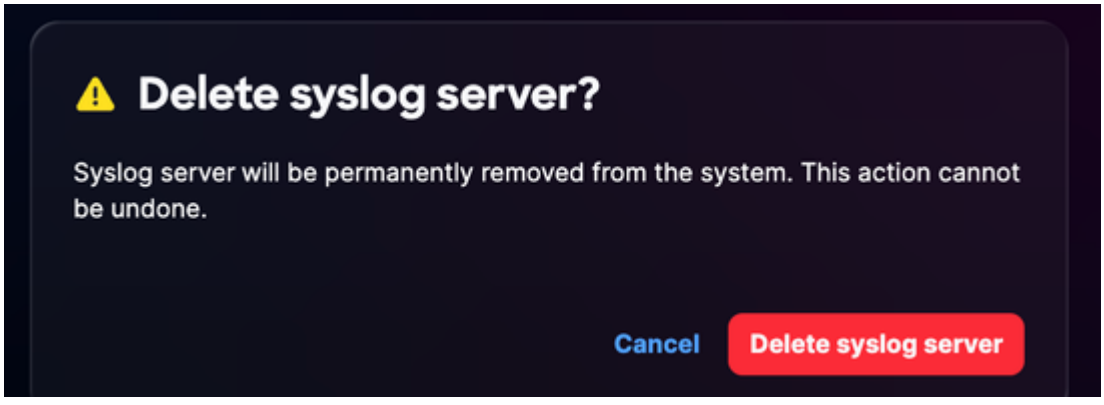
编辑系统日志服务器

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。

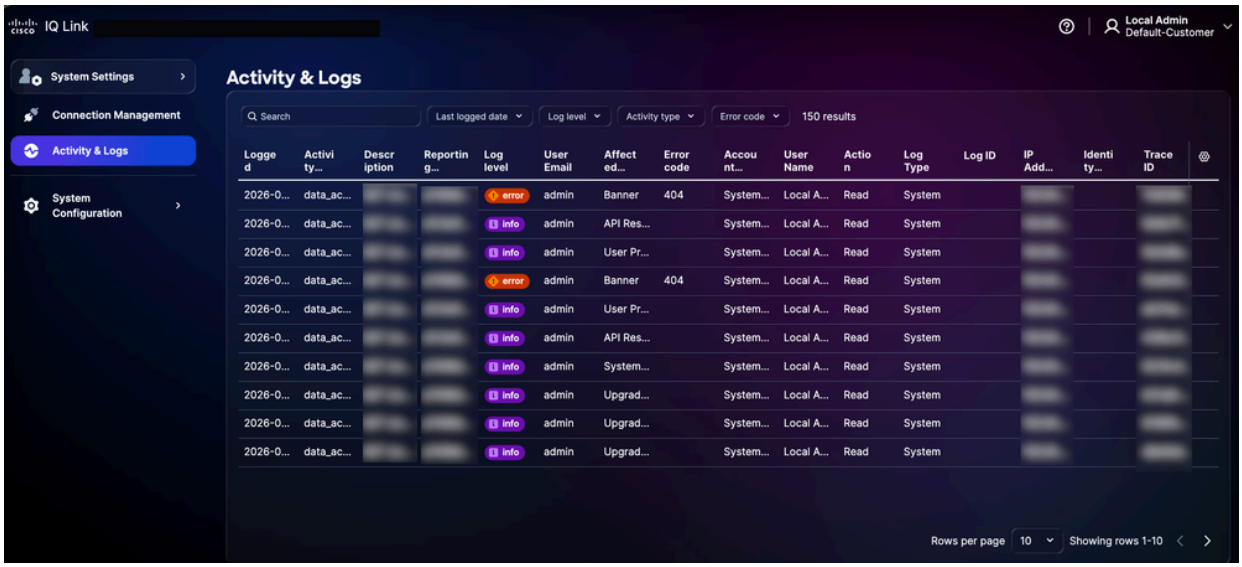


确认

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

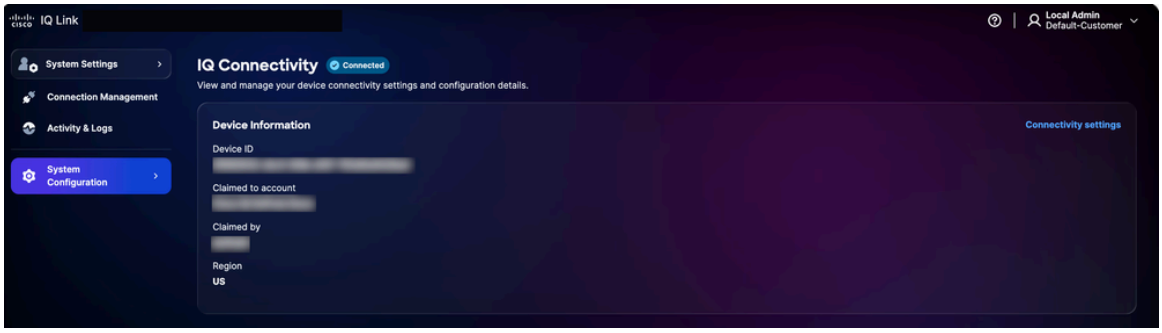
以下过滤器选项可用：

- 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

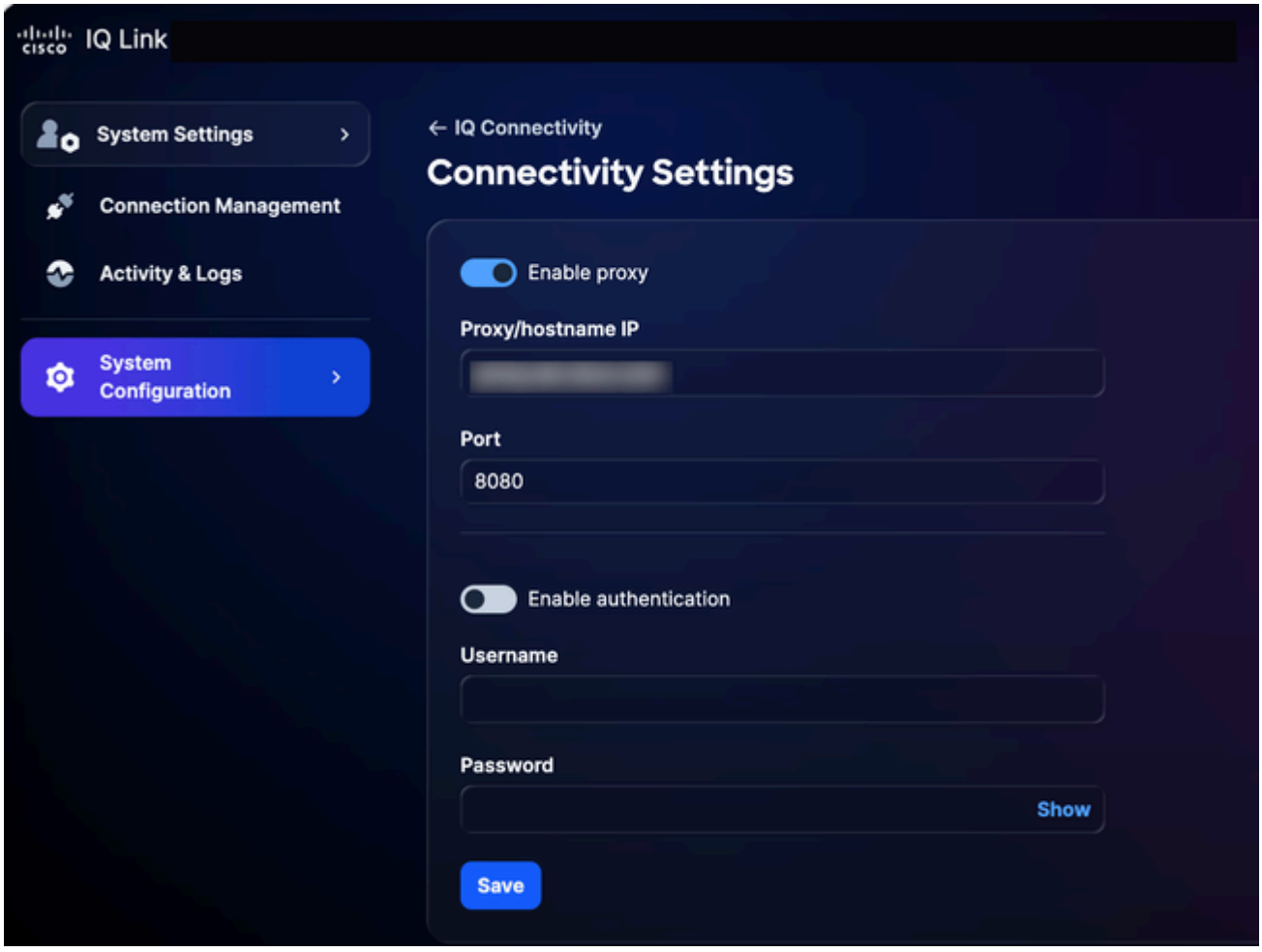
要查看和管理设备连接设置和配置详细信息，请执行以下操作：

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部署解决方案，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。配置数据收集可总结为如下共享：

- 创建凭证集:建立身份验证协议（例如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。

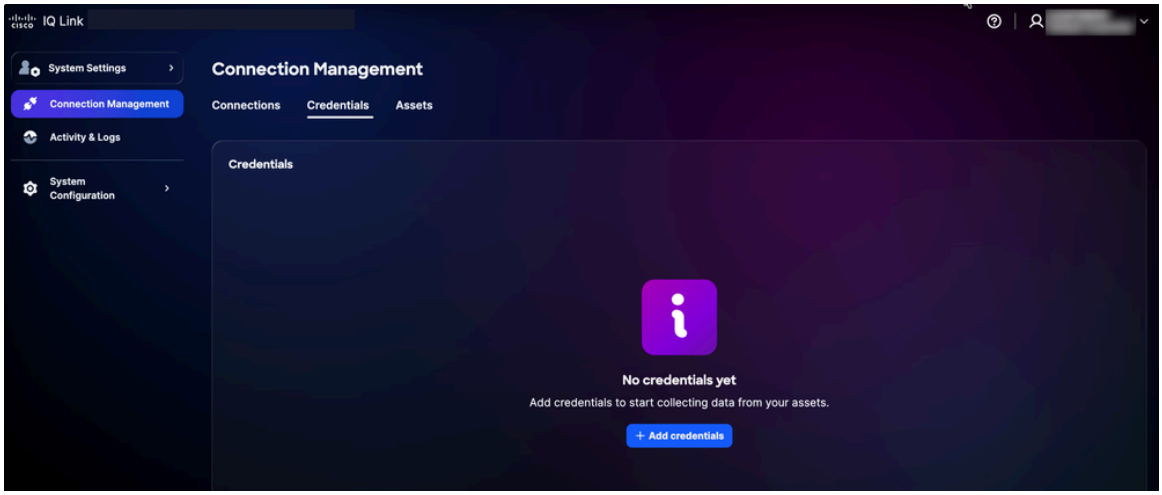
- 将凭证映射到资产:将凭证集与库存资产进行映射，以自动执行身份验证过程。通过创建将特定IP范围链接到已定义的凭证集的规则，系统在数据收集期间自动应用正确的身份验证。这消除了手动输入错误，并确保您的配置在网络扩展时保持准确。

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

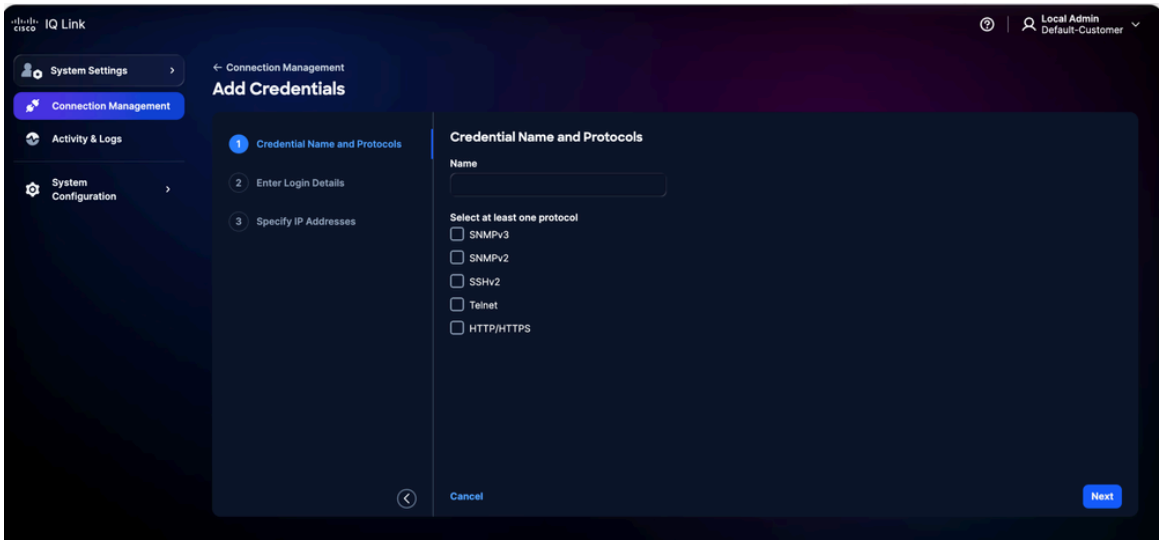
必须先添加凭据才能执行数据收集。要添加凭证，请执行以下操作：

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。

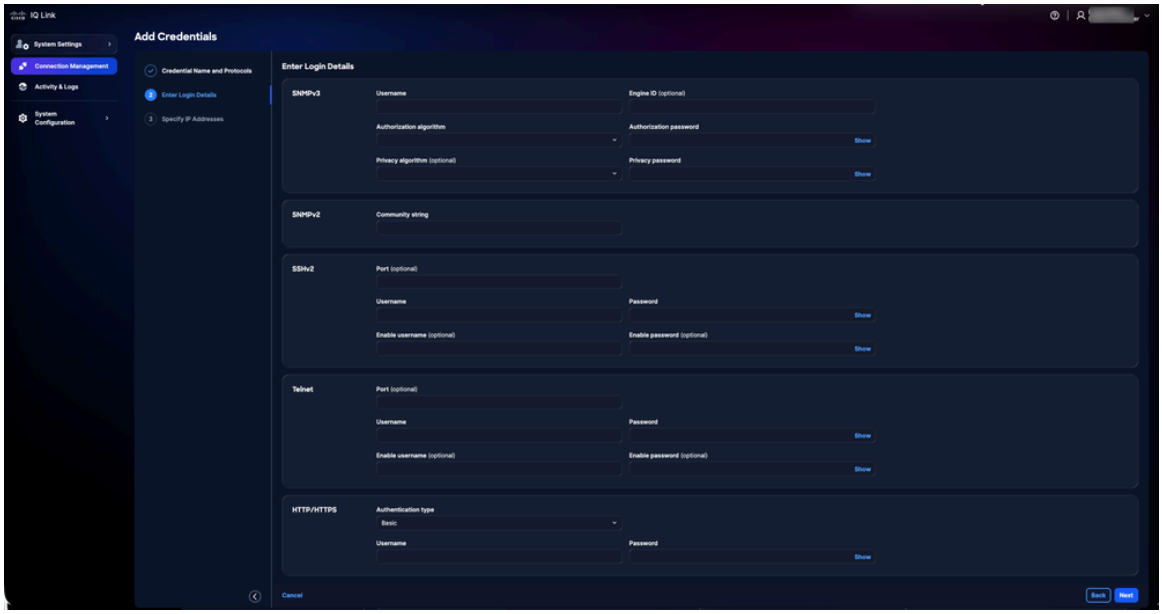


添加凭证

4. 输入姓名.

5. 选中所有适用的协议复选框。

6. 单击 Next。

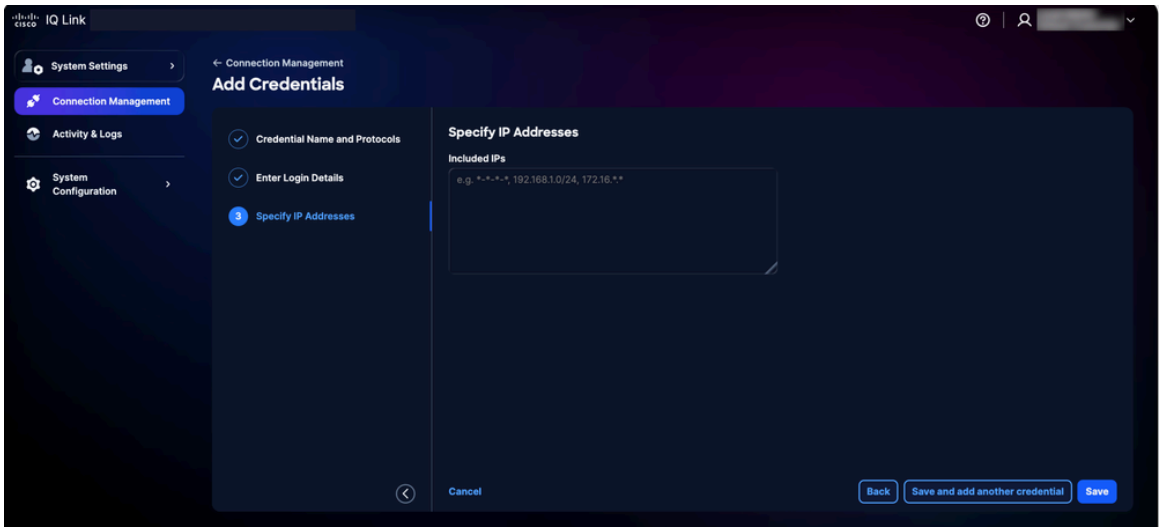


添加凭证详细信息

注意：对于上图，我们说明了在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。



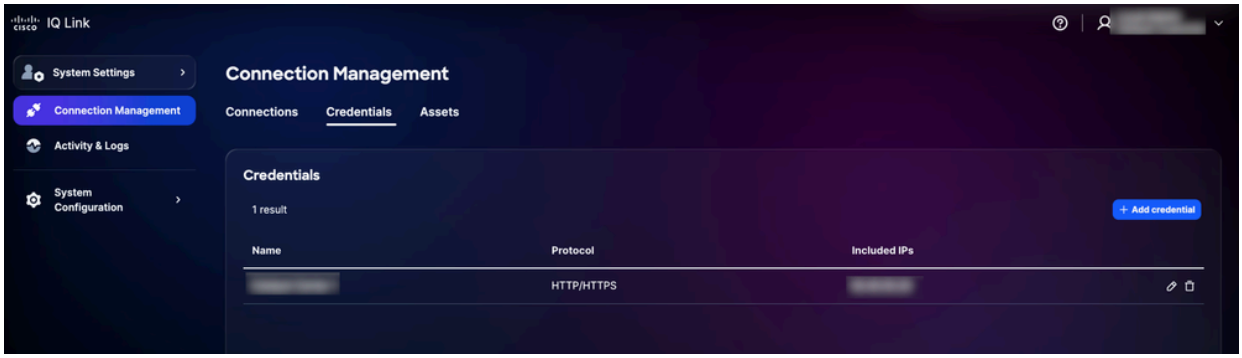
指定IP地址

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.*（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。

凭证选择示例

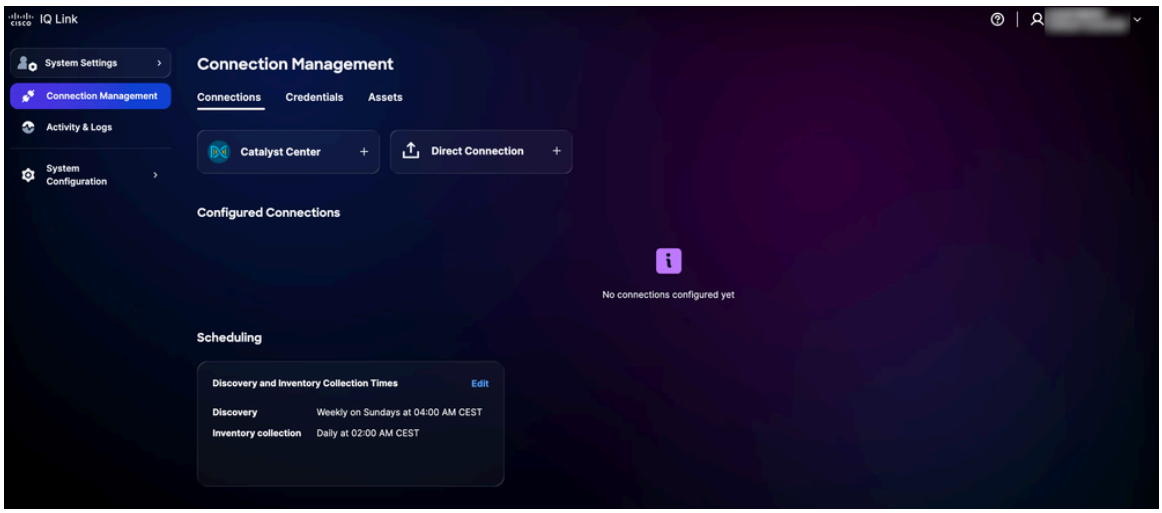
设备IP	可用的凭据集	选定的凭证集
10.10.1.5	10.10.1.5、10.10.1、10.10.*	10.10.1.5（完全匹配）
10.10.2.15	10.10.2.、10.10..*	10.10.2.*（更详细）
10.10.5.50	10.10...	10.10..（更详细）

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

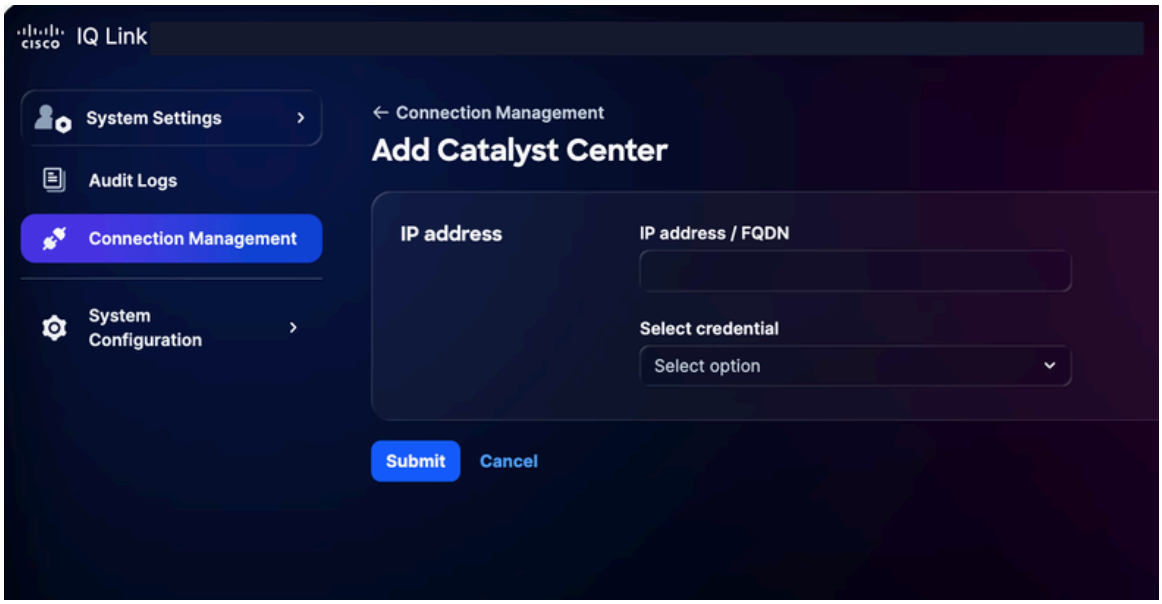
对于使用Catalyst Center的数据收集：

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



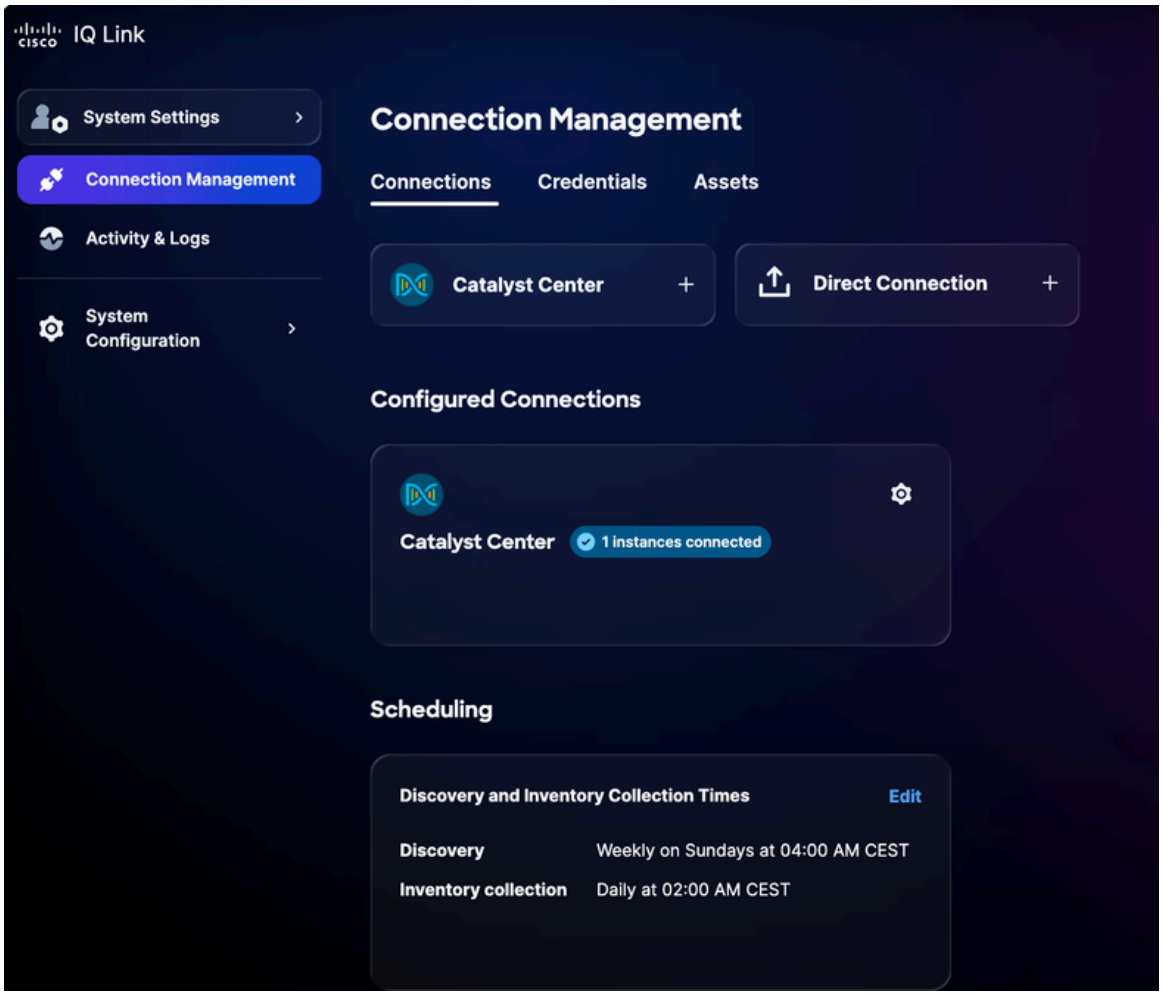
连接管理

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

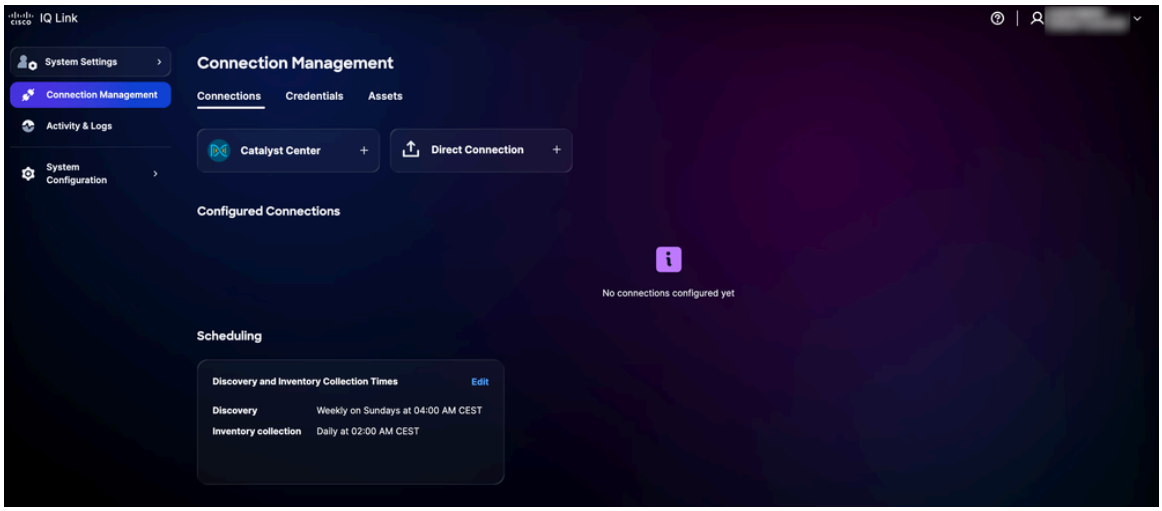
6. 计划收集。有关详细信息，请参阅计划。

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

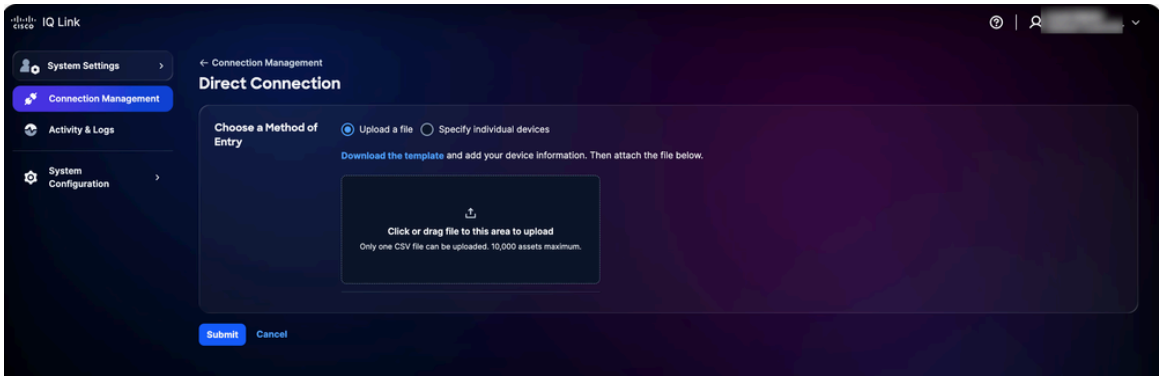
要添加直接连接的设备，请执行以下操作：

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



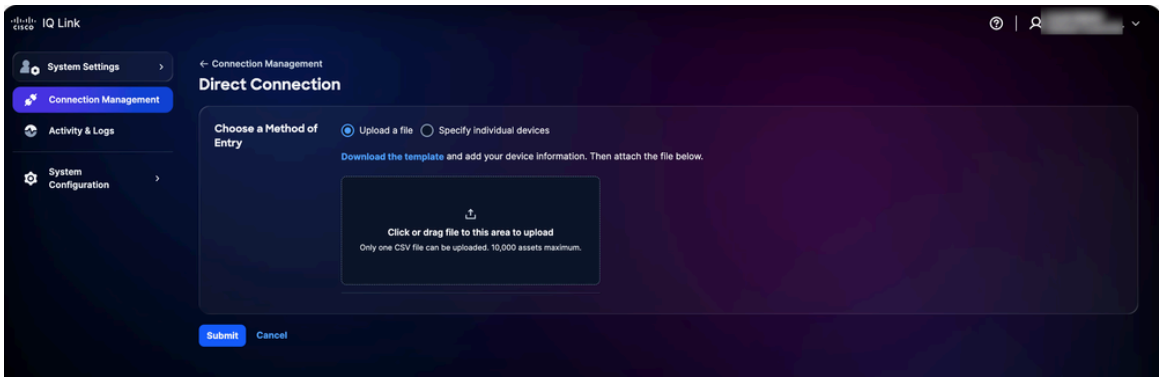
连接管理

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。



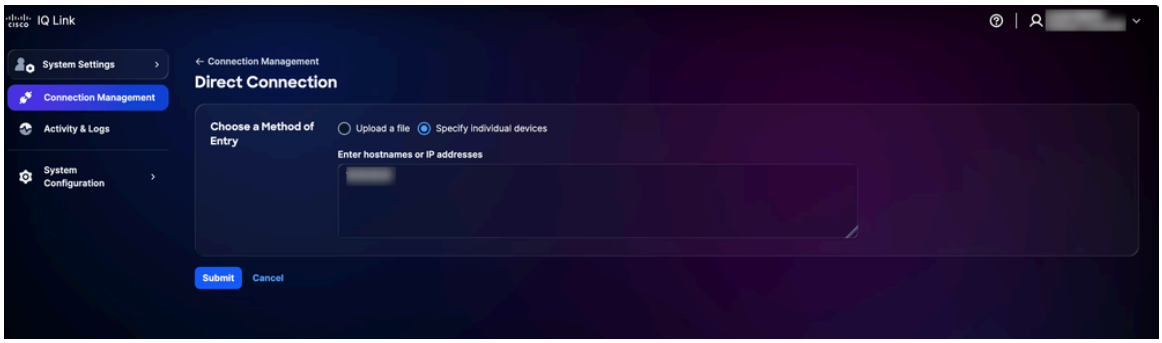
上载文件

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。

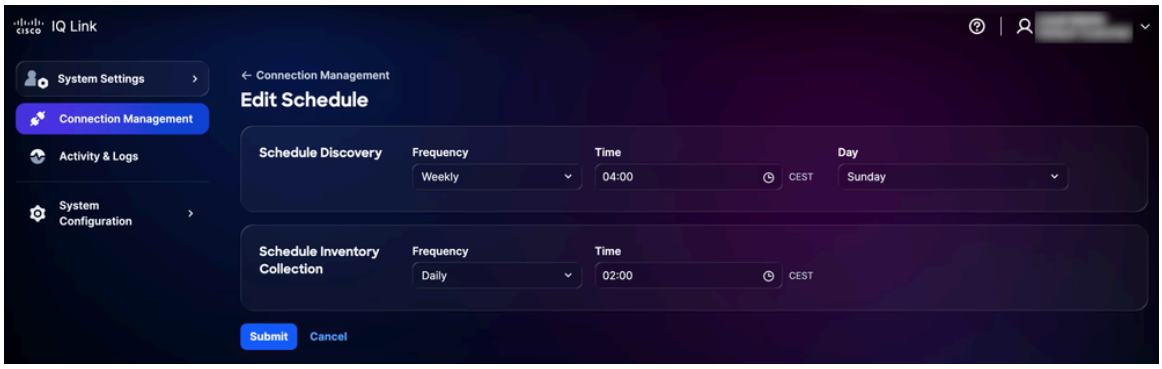
4. 计划收集。有关详细信息，请参阅计划。

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。

安排

安排允许您定义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

管理员可以配置跨应用程序显示的自定义横幅。

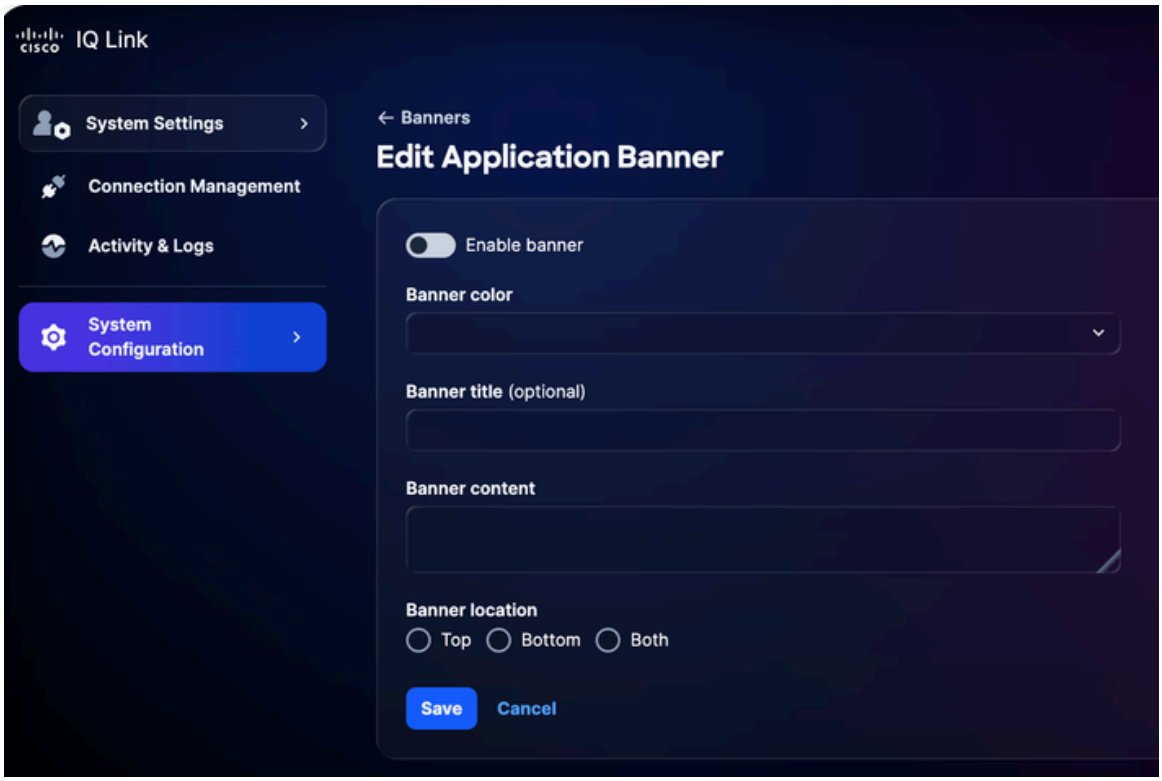
配置标语

配置标语：

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. 单击 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。

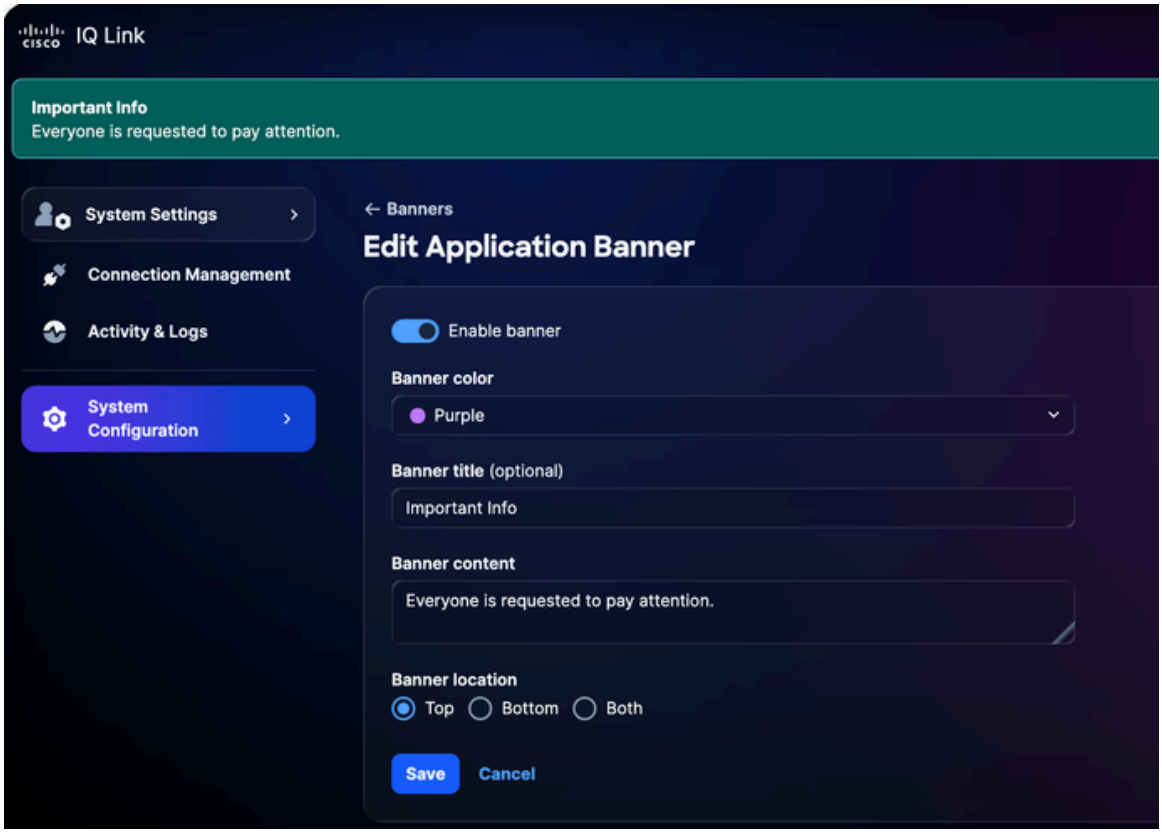
编辑横幅

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

客户可以从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CoSystem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）。