在 Cisco Secure Workload 中设置系统配置

根据您的角色，您可以使用系统级设置。例如，只有具有**站点管理员**和**客户支持用户**角色的用户才能查看**用户 (Users)** 选项。

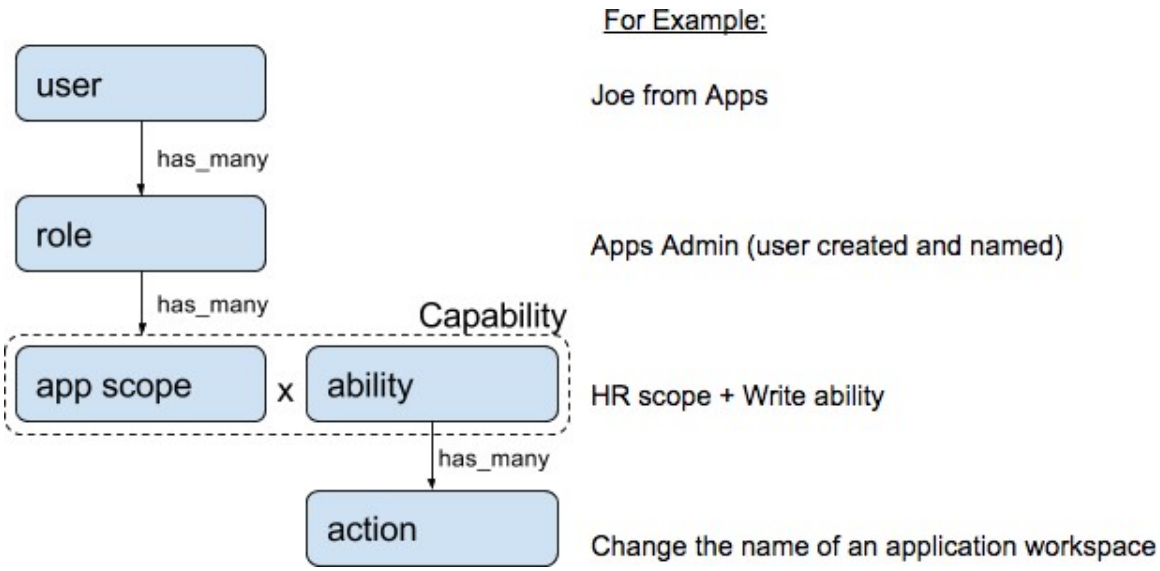
- 角色, on page 1
- 变更日志, on page 9
- 收集规则, on page 11
- 收集器, on page 12
- 会话配置, on page 12
- 公司, on page 12
- 联合 ， 第 34 页
- 空闲会话, on page 50
- 偏好设置, on page 51
- 范围, on page 55
- 租户, on page 55
- 用户, on page 57

角色

您可以使用基于角色的访问控制 (RBAC) 模型来限制对功能和数据的访问。

- 用户 - 对思科 Cisco Secure Workload 具有登录访问权限的用户。
- 角色 - 由用户创建并分配给用户的一组功能。
- 功能 - 范围 + 功能对
- 能力 - 操作的集合
- 操作 - 低级别用户操作，例如“更改工作空间名称”

Figure 1: 角色模型



用户可以具有任意数量的角色。角色可以具有任意数量的功能。例如，“力资源搜索工程师”角色可以有两种功能：“读取 HR 范围“可提供可视性和上下文，而”执行 HR 搜索"功能可让分配给该角色的工程师做出与其应用相关的特定更改。

使用**用户 (Users)** 页面为用户分配不同的角色。角色有多种功能，您可以为用户分配任意数量的角色。

定义系统角色是为了让用户能够更快地开始使用。它们定义了对**所有范围**（即系统上的所有数据）的不同访问级别。这些系统角色定义如下。

角色	说明
代理安装程序	提供管理代理生命周期（包括安装、监控、升级和转换）的功能，但**无法**删除代理和访问代理配置文件。
客户支持	获取技术支持或高级服务。提供对集群维护功能的访问权限。允许与站点管理员相同的访问权限，但**不能**修改用户。
客户支持只读	获取技术支持或高级服务。提供对集群维护功能的访问权限。允许与站点管理员相同的访问权限，但**不能**修改用户。
站点管理员	提供管理用户、代理等的功能。可以查看和编辑所有功能和数据。必须至少有一个站点管理员。
全局应用执行	在每个范围内提供执行功能。
全局应用管理	在每个范围上提供执行功能。
全局只读	在每个范围内提供读取功能。

能力和功能

角色由功能组成，其中包括范围和能力。这些定义了允许的操作及其适用的数据集。例如，(HR, Read) 功能应被阅读并解释为“HR 范围的阅读能力”。此功能将允许访问 HR 范围及其所有子范围。

能力	说明
安装程序	安装、监控和升级软件代理。
审核	支持全局设备数据读取和更改日志访问。
读	读取所有数据，包括流、应用和资产过滤器。
写	对应用和资产过滤器进行更改。
执行	执行自动发现策略并发布策略以供分析。
执行	执行与给定范围关联的应用工作空间中定义的策略。
所有者	将应用工作空间从辅助工作空间切换为主工作空间所必需。访问数据分流管理员功能，例如管理用户应用会话、添加数据分流以及创建可视化数据源。

Important 功能是继承的，例如，执行功能允许所有读取、写入和执行操作。

Important 功能适用于范围及其所有子项。

按角色访问菜单

您在导航窗格中看到和使用的菜单项取决于分配的角色：

Table 1: 概述菜单

菜单	选项	站点管理员	客户支持	客户支持只读	全局应用执行	全局应用管理	全局只读	代理安装程序
概述	概述	兼容	兼容	兼容	兼容	兼容	是	否

Table 2: 整理菜单

菜单	选项	站点管理员	客户支持	客户支持只读	全局应用执行	全局应用管理	全局只读	代理安装程序
整理	范围和资产	兼容	兼容	兼容	兼容	兼容	是	否
整理	标签管理	兼容	兼容	兼容	兼容	兼容	是	否
整理	资产过滤器	兼容	兼容	兼容	兼容	兼容	是	否

Table 3: 防御菜单

菜单	选项	站点管理员	客户支持	客户支持只读	全局应用执行	全局应用管理	全局只读	代理安装程序
防御	分段	兼容	兼容	兼容	兼容	兼容	是	否
防御	执行状态	兼容	兼容	兼容	兼容	兼容	是	否
防御	策略模板	兼容	兼容	兼容	兼容	兼容	是	否
防御	取证规则	兼容	兼容	兼容	兼容	兼容	是	否

Table 4: 调查菜单

菜单	选项	站点管理员	客户支持	客户支持只读	全局应用执行	全局应用管理	全局只读	代理安装程序
调查	流量	兼容	兼容	兼容	兼容	兼容	是	否
	警报	兼容	兼容	兼容	兼容	兼容	是	否
	漏洞	兼容	兼容	兼容	兼容	兼容	是	否
	取证	兼容	兼容	兼容	兼容	兼容	是	否

Table 5: 报告菜单

菜单	选项	租户所有者	代理安装程序	
报告	报告控制面板	是	否	

Table 6: 管理菜单

菜单	选项	站点管理员	客户支持	客户支持只读	全局应用执行	全局应用管理	全局只读	代理安装程序
管理	警报配置	兼容	兼容	兼容	兼容	兼容	是	否
管理	变更日志	是	否	是	否	不兼容	不兼容	不兼容
管理	连接器	兼容	是	否	不兼容	不兼容	不兼容	不兼容
管理	外部协调器	兼容	是	否	不兼容	不兼容	不兼容	不兼容
管理	安全连接器	兼容	是	否	不兼容	不兼容	不兼容	不兼容
管理	虚拟设备	兼容	是	否	不兼容	不兼容	不兼容	不兼容
管理	用户	兼容	是	否	不兼容	不兼容	不兼容	不兼容
管理	角色	兼容	兼容	是	否	不兼容	不兼容	不兼容
管理	威胁智能	兼容	兼容	是	否	不兼容	不兼容	不兼容
管理	许可证	是	否	不兼容	不兼容	不兼容	不兼容	不兼容
管理	收集规则	兼容	兼容	兼容	兼容	兼容	是	否
管理	会话配置	兼容	是	否	不兼容	不兼容	不兼容	不兼容
管理	使用分析	兼容	是	否	不兼容	不兼容	不兼容	不兼容
管理	数据分流管理员	是	否	不兼容	不兼容	不兼容	不兼容	不兼容

Table 7: 平台菜单

菜单	选项	站点管理员	客户支持	客户支持只读	全局应用执行	全局应用管理	全局只读	代理安装程序
平台	租户	兼容	是	否	不兼容	不兼容	不兼容	不兼容
平台	集群配置	兼容	是	否	不兼容	不兼容	不兼容	不兼容
平台	出站 HTTP	兼容	是	否	不兼容	不兼容	不兼容	不兼容
平台	收集器	兼容	是	否	不兼容	不兼容	不兼容	不兼容

菜单	选项	站点管理员	客户支持	客户支持只读	全局应用执行	全局应用管理	全局只读	代理安装程序
平台	外部身份验证	兼容	是	否	不兼容	不兼容	不兼容	不兼容
平台	SSL 证书	兼容	是	否	不兼容	不兼容	不兼容	不兼容
平台	登录页消息	兼容	是	否	不兼容	不兼容	不兼容	不兼容
平台	联合	参见下文	参见下文	否	不兼容	不兼容	不兼容	不兼容
平台	数据备份	参见下文	参见下文	否	不兼容	不兼容	不兼容	不兼容
平台	数据恢复	参见下文	参见下文	否	不兼容	不兼容	不兼容	不兼容
平台	升级/重启/关闭	兼容	是	否	不兼容	不兼容	不兼容	不兼容

Note

- 启用**联合 (Federation)** 选项，使联合可用于**站点管理员**和**客户支持**角色。
- 启用**数据备份和恢复 (Data Backup and Restore)** 选项，使**站点管理员**和**客户支持**角色可以使用数据备份和恢复。

Table 8: 故障排除菜单

菜单	选项	站点管理员	客户支持	客户支持只读	全局应用执行	全局应用管理	全局只读	代理安装程序
故障排除	服务状态	兼容	兼容	是	否	不兼容	不兼容	不兼容
故障排除	集群状态	参见下文	参见下文	否	不兼容	不兼容	不兼容	不兼容
故障排除	虚拟机	兼容	兼容	是	否	不兼容	不兼容	不兼容
故障排除	快照	兼容	是	否	不兼容	不兼容	不兼容	不兼容
故障排除	维护资源管理器	兼容	是	否	不兼容	不兼容	不兼容	不兼容
故障排除	Resque	兼容	是	否	不兼容	不兼容	不兼容	不兼容
故障排除	Hawkeye（图表）	兼容	兼容	是	否	不兼容	不兼容	不兼容
故障排除	Abyss（管道）	兼容	兼容	是	否	不兼容	不兼容	不兼容

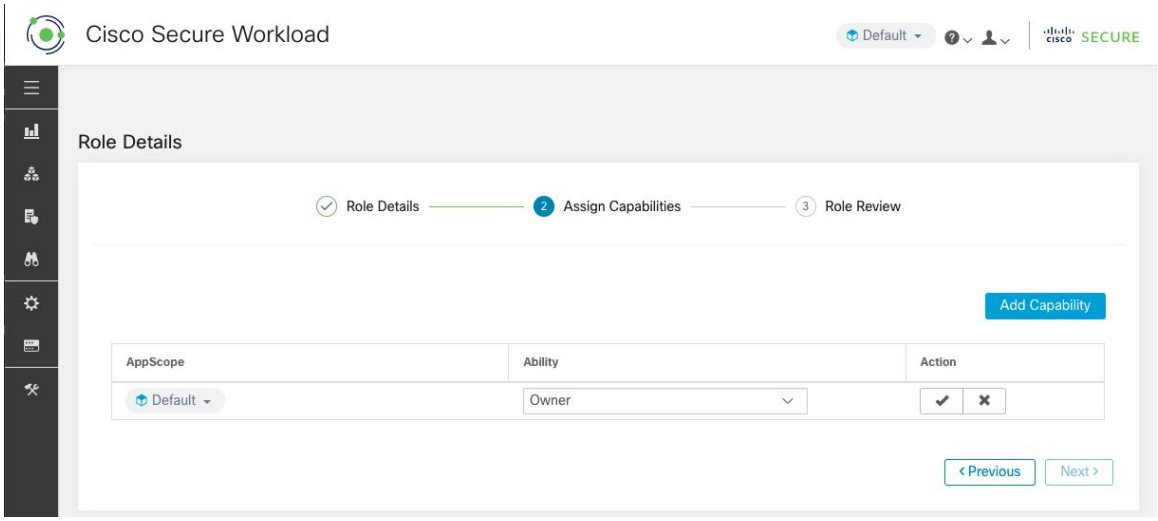
Note 集群状态选项可用于站点管理员和客户支持角色，具体取决于集群类型。

创建角色

Before you begin

您必须已拥有**站点管理员**或**客户支持**用户角色。

1. 在左侧的导航栏中，点击**管理 (Manage)** > **用户访问权限 (User Access)** > **角色 (Roles)**。
2. 点击**创建新角色 (Create New Role)**。系统将显示**角色 (Roles)** 面板。



使用“创建角色向导”(Create Role Wizard) 创建角色的过程分为三步。

Procedure

步骤 1 a) 在以下字段中输入适当的值：

字段	说明
名称 (Name)	用于标识角色的名称。
说明 (Description)	用于添加有关角色的背景信息的简短说明。

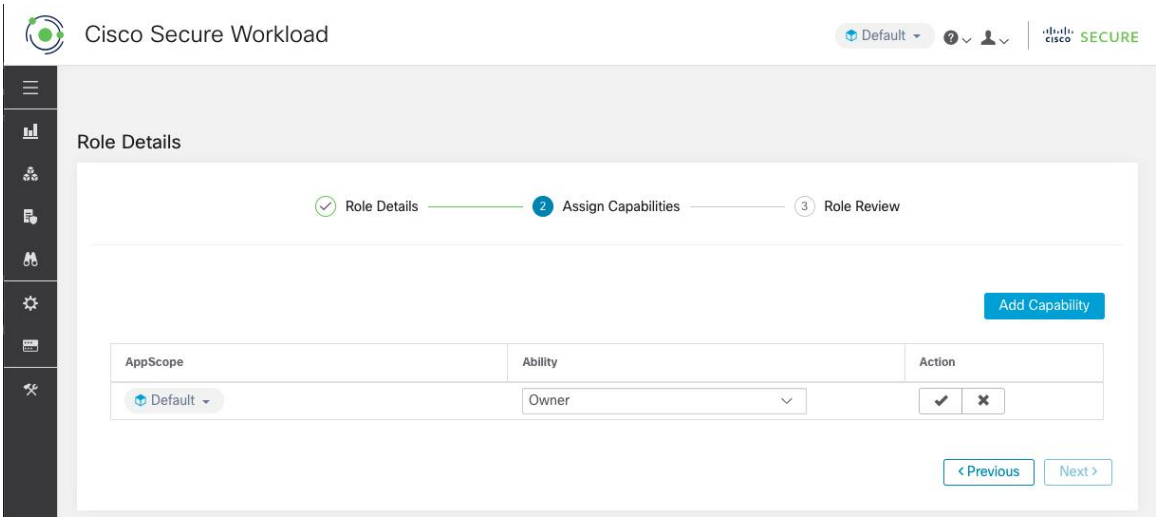
b) 点击**下一步 (Next)** 按钮移至下一步，或点击**返回角色页面 (Back to Roles Page)** 返回“角色”(Roles) 页面。

步骤 2 a) 点击**添加功能 (Add Capability)** 按钮，以便在第一行显示创建表单。

b) 选择范围和功能。

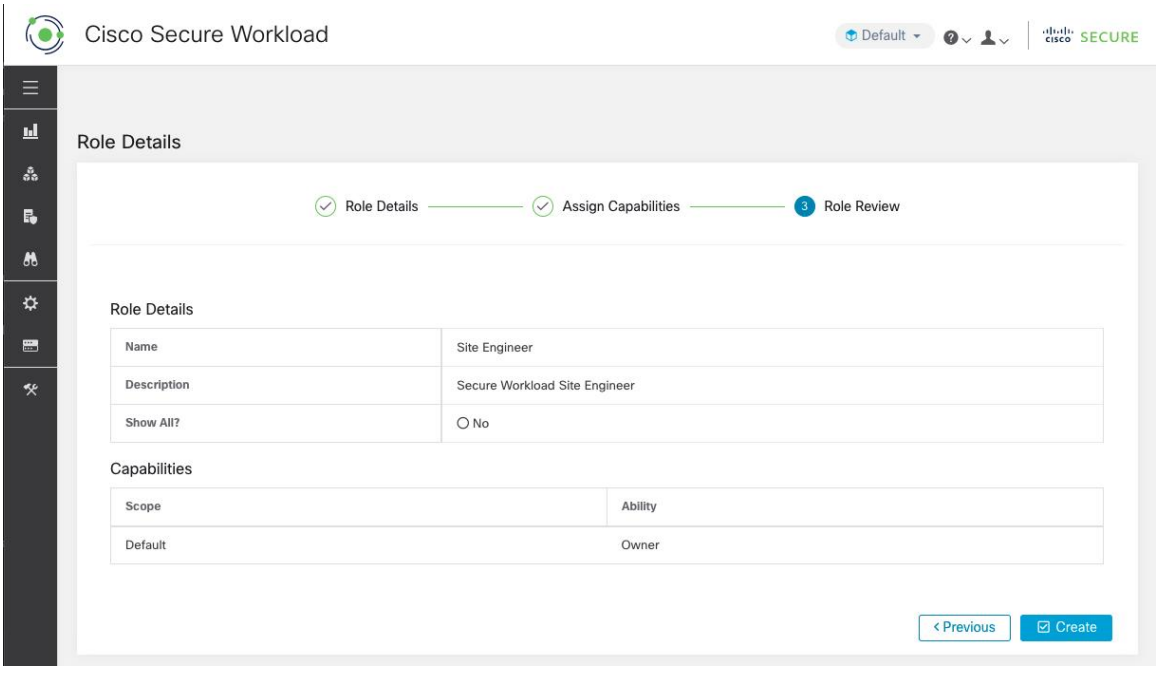
c) 点击**复选标记 (Checkmark)** 按钮创建新功能，或点击**取消 (Cancel)** 按钮取消。
d) 点击**下一步 (Next)** 查看角色详细信息，或点击**上一步 (Previous)** 返回并进行编辑。

Figure 2: 功能分配



步骤 3 a) 查看角色详细信息和功能。
b) 点击**创建 (Create)** 以创建角色。

Figure 3: 角色审核



编辑角色

本部分介绍**站点管理员**和**客户支持用户**如何编辑角色。

Before you begin

您必须是站点管理员或客户支持用户。

1. 在左侧的导航栏中，点击**管理 (Manage)** > **用户访问权限 (User Access)** > **角色 (Roles)**。
2. 在要编辑的角色的行中，点击右列中的**编辑 (Edit)** 按钮。系统将显示**角色 (Roles)** 面板。

使用“编辑角色向导”(Edit Role Wizard) 来编辑角色的过程可分为三步。

Procedure

步骤 1 a) 如有需要，请更新名称或说明。
b) 点击**下一步 (Next)** 按钮移至下一步，或点击**返回角色页面 (Back to Roles Page)** 返回“角色”(Roles) 页面。

步骤 2 a) 根据需要删除任何功能。在要删除的功能的行中，点击右列中的**删除 (Delete)** 图标。
b) 要添加功能，请点击**添加功能 (Add Capability)** 按钮以便在第一行显示创建表单。
c) 选择范围和功能。
d) 点击**下一步 (Next)** 查看角色详细信息，或点击**上一步 (Previous)** 返回并进行编辑。

步骤 3 a) 查看角色详细信息和功能。
b) 点击**更新 (Update)** 创建角色，或点击**上一步 (Previous)** 返回并进行编辑。在**更新**后，系统会保存对角色详细信息和功能分配所做的更改。

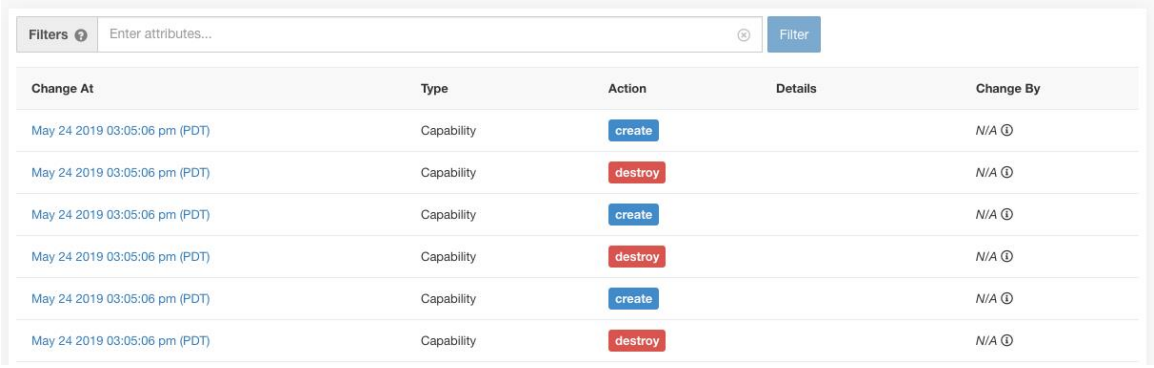
Note 无法编辑功能，必须删除并重新创建功能。

变更日志

站点管理员可以访问窗口左侧导航栏中**管理 (Manage)** 菜单下的**变更日志 (Change Log)** 页面。此页面显示在思科 Cisco Secure Workload 中进行的最新更改。

Note **变更日志保留期：** Cisco Secure Workload 可在 SaaS 和本地部署集群上管理持续时间长达一年的变更日志。每小时作业会删除超过一年时间范围的更改日志。

Figure 4: 更改日志页面

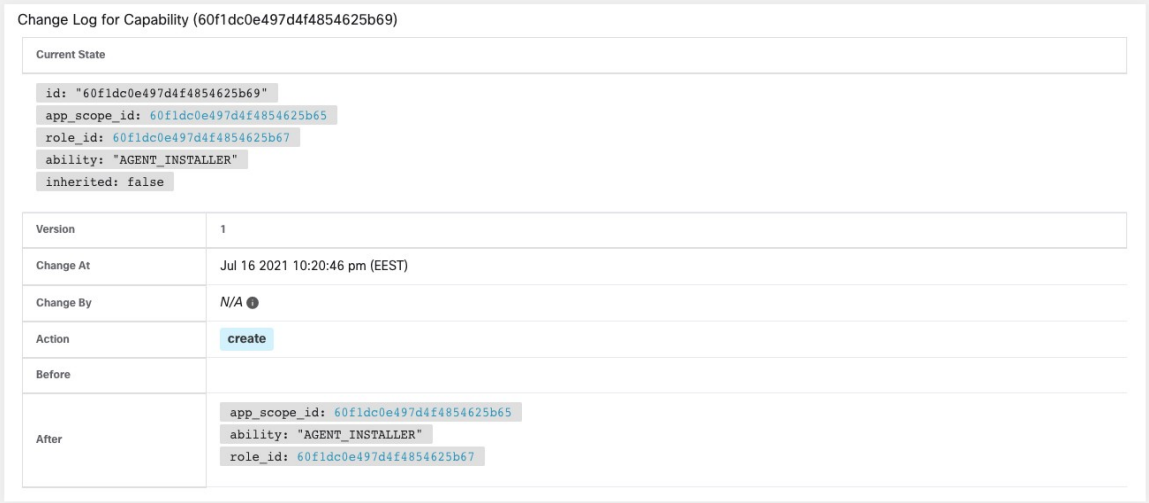


点击**更改时间 (Change At)** 列中的链接，可以查看每个更改日志条目的详细信息。此页面包括字段更改**之前**和**之后**的快照。字段可能包含技术名称，需要对其进行一些解释，以了解它们在整个Cisco Secure Workload 中的其他地方是如何出现的。

Figure 5: “更改日志详细信息” ***(Change Log Details)*** 页面

点击右上角标题为**此<实体类型>的完整日志 (Full log for this <entity type>)** 的按钮可查看实体更改的完整列表。此页面将显示每项更改的详细信息。它还包括实体的**当前状态**（如果可用）。

Figure 6: 实体的完整变更日志



收集规则

站点管理员和**客户支持用户**可以访问窗口左侧导航栏中**管理 (Manage) > 服务设置 (Service Settings)** 菜单下的**收集规则 (Collection Rules)** 页面。此页面将按运行思科 Cisco Secure Workload 代理的交换机使用的 VRF 来显示硬件收集规则。每个 VRF 在表中都有一行。

规则

点击 VRF 上的**编辑 (Edit)** 按钮以修改其收集规则。默认情况下，每个 VRF 都配置了两个默认捕获全部规则，一个用于 IPv4 (`0.0.0.0/0 INCLUDE`)，另一个用于 IPv6 (`::/0 INCLUDE`)。可以删除这些默认规则，但要保持谨慎。

可以添加额外的包含和排除规则。输入有效的子网，选择包含或排除，然后点击**添加规则 (Add Rule)**。这些规则的优先级可通过拖放来进行调整。点击并按住列表中的规则，然后拖动调整其顺序。

更改可能需要几分钟才能传播到交换机。点击右上角的**后退 (Back)** 按钮以返回到 VRF 列表。

优先级

收集规则按优先级降序排列。确定优先级时不会进行最长前缀匹配。最先出现的规则优先于后面的所有规则。示例：

1. 1.1.0.0/16 INCLUDE
2. 1.0.0.0/8 EXCLUDE
3. 0.0.0.0/0 INCLUDE

在前面的示例中，属于 1.0.0.0/8 子网的所有地址都被排除在外，只有子网 1.1.0.0/16 包括在内。

更改顺序的另一个示例：

1. 1.0.0.0/8 EXCLUDE
2. 1.1.0.0/16 INCLUDE
3. 0.0.0.0/0 INCLUDE

在上例中，属于 1.0.0.0/8 子网的所有地址都被排除在外。规则 2 在这里没有被执行，因为已经为其子网络定义了一条更高级别的规则。

收集器

站点管理员和**客户支持用户**可以访问窗口左侧导航栏中**平台 (Platform)** 菜单下的**收集器 (Collectors)** 页面。此页面显示当前配置的收集器。Cisco Secure Workload 代理会将流数据发送到委托收集器，因此所有委托收集器都必须可用，这一点很重要。默认情况下，所有收集器都会定期检查其运行状况，并根据其运行状况进行调试或下线。您可以使用切换**自动调试选择退出 (Auto Commission Opt Out)** 来选择退出此自动化过程。启用此开关后，最右列下的**开始**和**停止**图标可用于分别进行调试和下线。

Figure 7: 收集器页面

Name	IP	TCP Port	UDP Port	Health	Health Details	Status	Auto Commission Opt Out	Manual Action
collectorDatamover-1	172.21.156.182	5640	5640	Healthy		Commissioned		
collectorDatamover-2	172.21.156.183	5640	5640	Healthy		Commissioned		

会话配置

可在此处配置UI用户身份验证空闲会话超时。此配置适用于设备的所有用户。默认空闲会话持续时间为 1 小时。空闲会话持续时间的设置范围为 5 分钟至 24 小时。保存此值后，会话超时将对用户的验证会话生效。

站点管理员和**客户支持用户**可以访问此设置。在左侧导航窗格中，点击**管理 (Manage)** > **服务设置 (Service Settings)** > **会话配置 (Session Configuration)**。

公司

您可以设置公司范围内的以下（每个 Cisco Secure Workload 集群）配置。

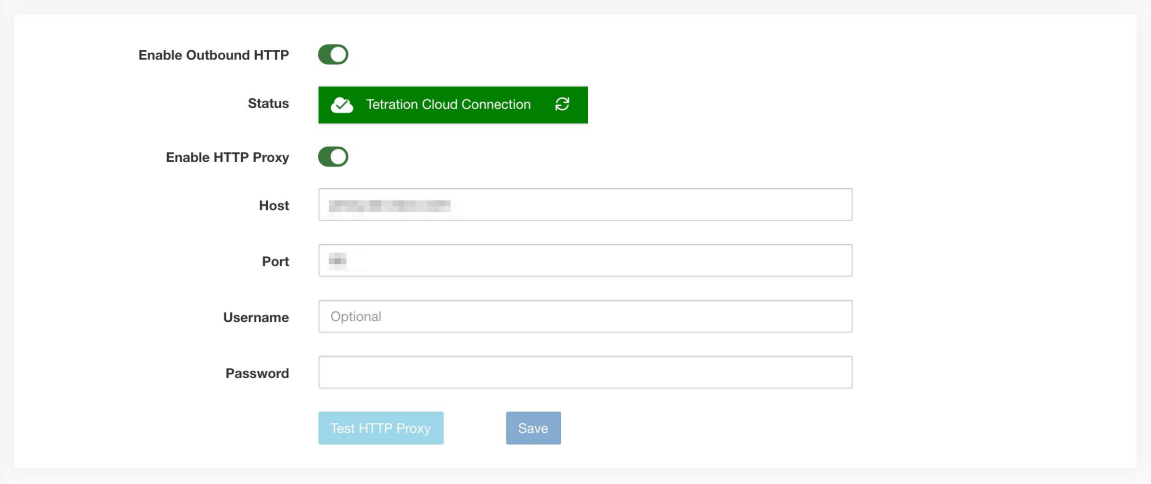
出站 HTTP 连接

为确保从思科云检索最新的威胁智能数据集，强烈建议您设置出站 HTTP 连接。

Warning 除了设置如下所示的 HTTP 代理之外，您的企业出站 HTTP 请求可能需要允许来自企业防火墙出站规则的流量发往 **periscope.tetrationcloud.com** 和 **uas.tetrationcloud.com**。

与 **peri scope.tetrationcloud.com** 的 TLS 连接将被用于传输威胁智能数据，以识别已知漏洞。因此，思科 Cisco Secure Workload 必须根据 Cisco Secure Workload 中包含的信誉良好的根 CA 证书来验证域的 X.509 证书的签名 CA 证书，从而验证域名的真实性。篡改 X.509 信任链会导致该功能无法正常工作。

Figure 8: 出站 ***HTTP*** 连接



站点管理员和**客户支持用户**可以访问出站 HTTP 设置。在左侧的导航栏中，点击**平台 (Platform)** > **出站 HTTP (Outbound HTTP)**。

字段	说明
状态 (Status)	指明 Cisco Secure Workload 设备是否可以访问 Cisco Secure Workload 云以检索威胁智能数据集更新。可以通过点击刷新按钮来重新触发状态检查。以下 HTTP 代理设置可用于根据 Cisco Secure Workload 部署配置 HTTP 代理设置。
启用 HTTP 代理 (Enable HTTP Proxy)	如果启用此选项，所有外部 HTTP 连接都会使用 HTTP 代理
主机 (Host)	HTTP 代理主机地址

字段	说明
端口 (Port)	HTTP 代理端口号
用户名 (Username)	仅当 HTTP 代理服务器使用基本身份验证时才需要
密码 (password)	仅当 HTTP 代理服务器使用基本身份验证时才需要

登录页消息

站点管理员和**客户支持用户**可以输入用户在登录页面上看到的消息，最多 1600 个字符。

要创建或更改登录页面消息，请执行以下操作：

1. 在左侧导航页面中，点击**平台 (Platform)** > **登录页面消息 (Login Page Message)**。
2. 输入或编辑消息。字符数限制为小于或等于 1600 个字符。
3. 点击**保存 (Save)**。

配置外部身份验证

如果启用此选项，则身份验证会被移交给外部系统。当前的身份验证选项包括轻量级目录访问协议 (LDAP) 以及单点登录 (SSO)。这意味着启用此功能后，所有登录用户都将使用所选机制进行身份验证。确定LDAP连接配置是否正确非常重要，尤其是在“使用本地身份验证”(Use Local Authentication) 选项上没有用户的情况下。建议的方法是，通过打开“使用本地身份验证”(Use Local Authentication) 选项，让至少一个本地身份验证用户拥有**站点管理员**凭证。此用户可以确保 LDAP 配置的设置正确无误。成功设置连接后，还可以通过取消选中用户编辑流程中的“使用本地身份验证”(Use Local Authentication) 选项来将此用户转换为外部身份验证。

站点管理员可以启用更多调试消息，而这些消息对于调试外部连接问题、用户登录失败等非常有用。这可以通过选中“外部身份验证调试”(External Auth Debug) 选项来启用。启用此选项后，更多描述性日志消息将被写入名为“external_auth_debug.log”的单独日志文件。建议在调试完成后关闭“外部身份验证调试”(External Auth Debug)，以防止将额外日志写入日志文件。

Note 按照“使用本地身份验证”(Use Local Authentication) 选项中的指明，按用户启用外部身份验证后，用户即可绕过外部身份验证。在启用外部身份验证时，也可以通过警告消息从链接转到用户编辑流，从而启用此选项。

如果启用了联合，则建议使用 SSO 外部身份验证。

Note 从 3.7.1.5 及更高版本开始，用于逐出的外部身份验证会话从 6 小时增加到了 9 小时。此设置仅适用于外部身份验证或本地身份验证。

站点管理员和客户支持用户均可配置外部身份验证。在左侧导航栏中，点击**平台 (Platform)** > **外部身份验证 (External Authentication)**。

Figure 9: 配置外部身份验证

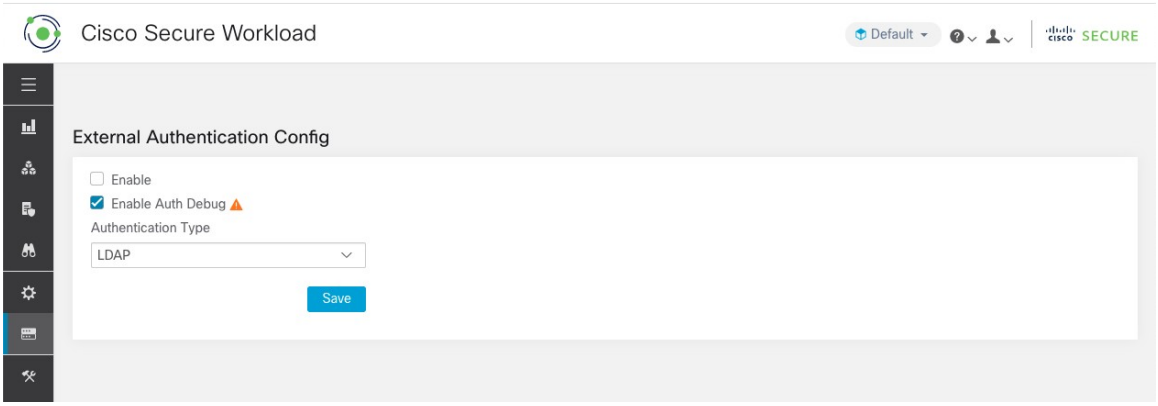


Figure 10: 配置外部身份验证（续）

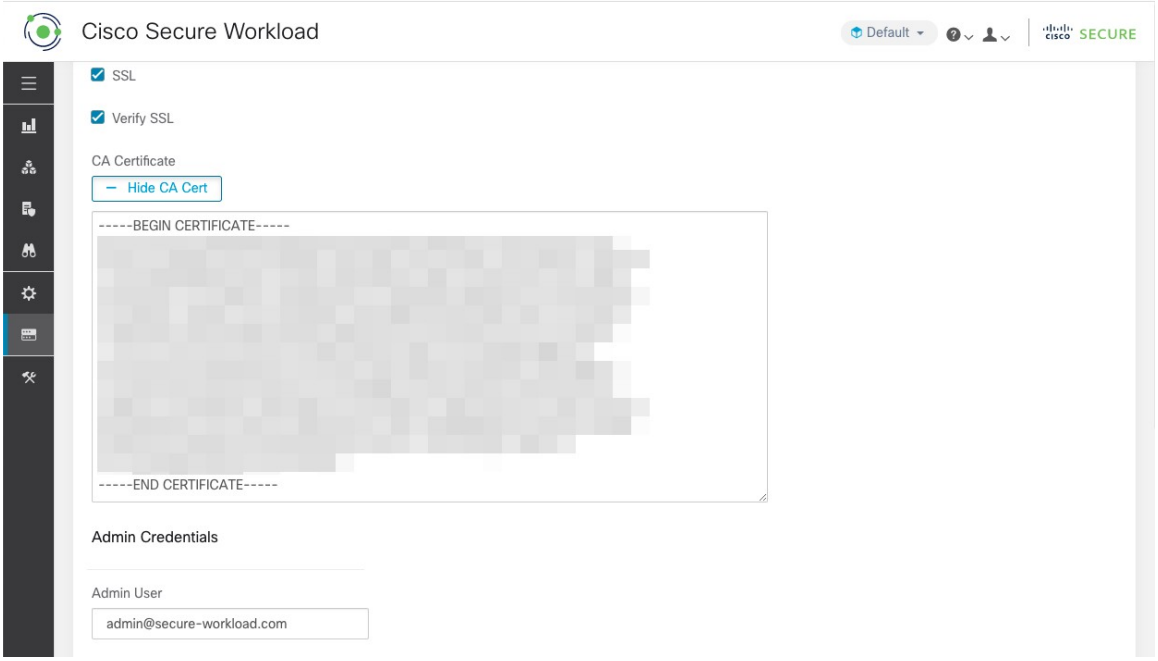


Figure 11: 配置外部身份验证（续）

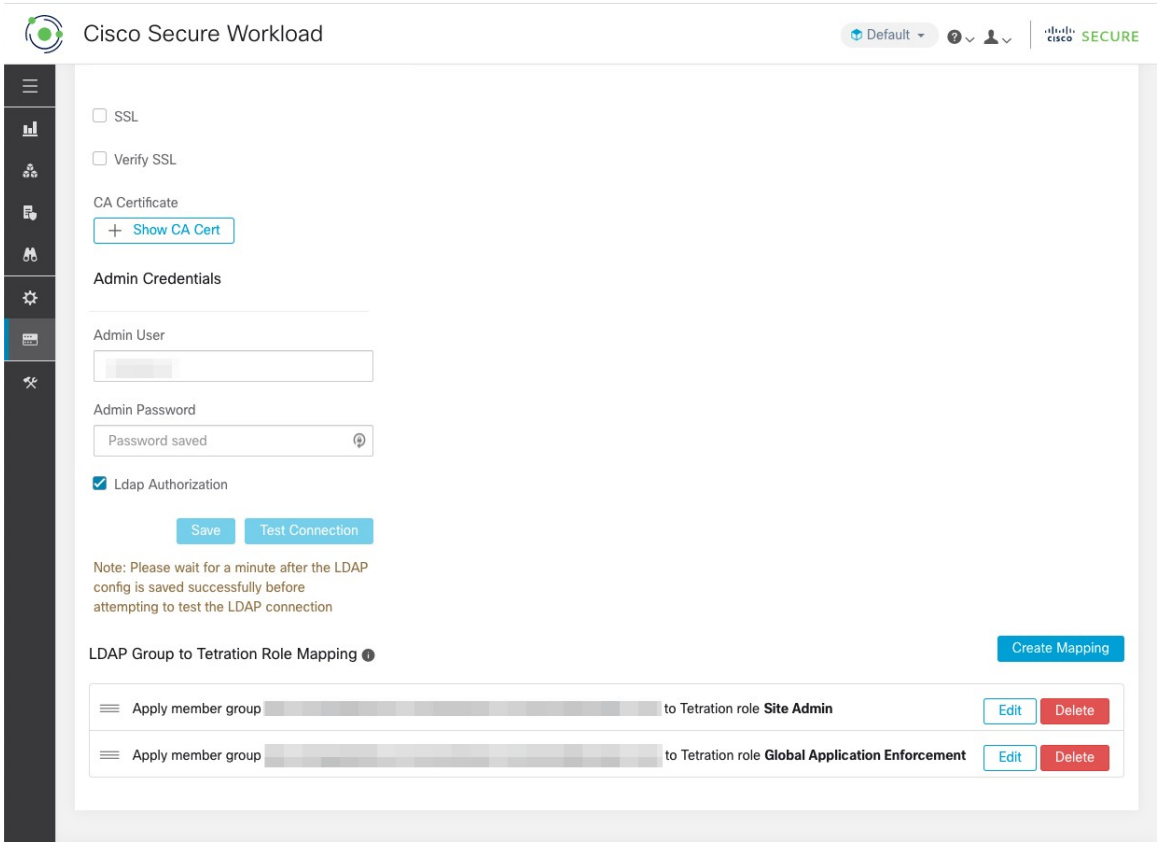
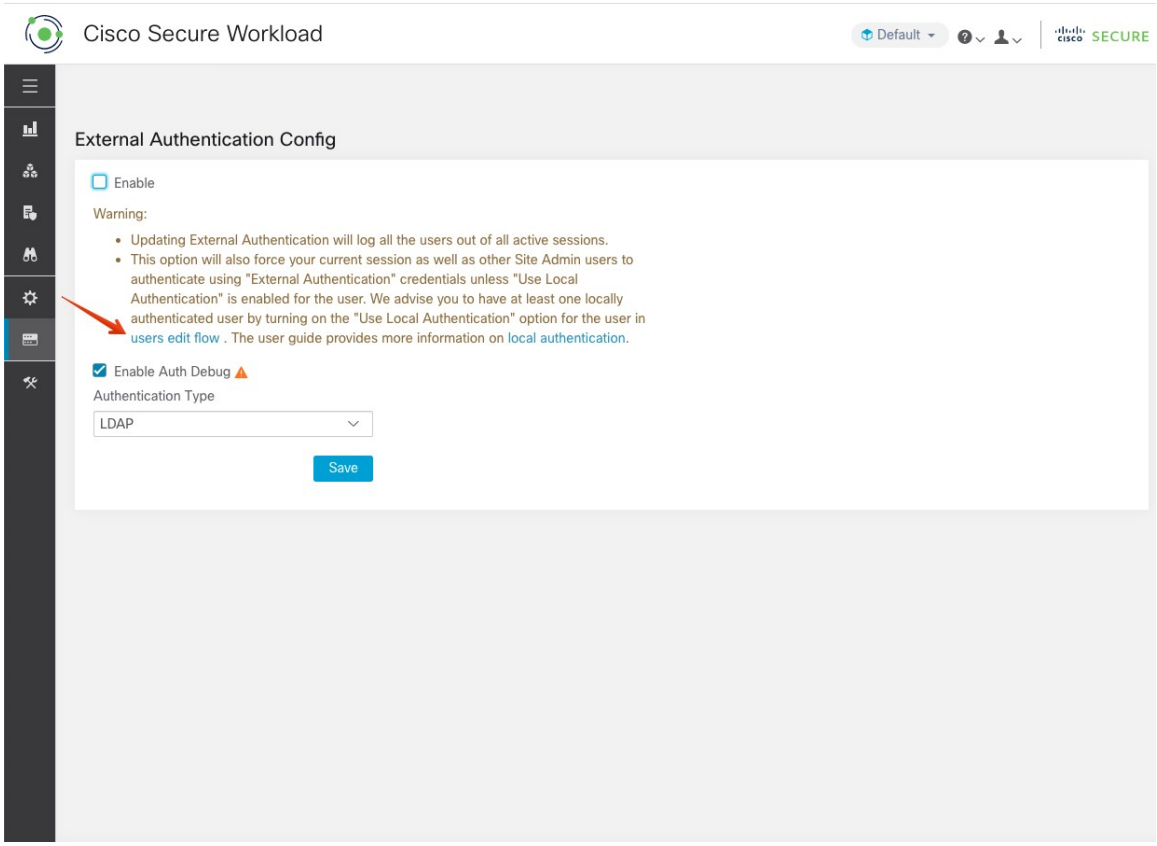


Figure 12: 外部身份验证警告



配置轻量级目录访问协议

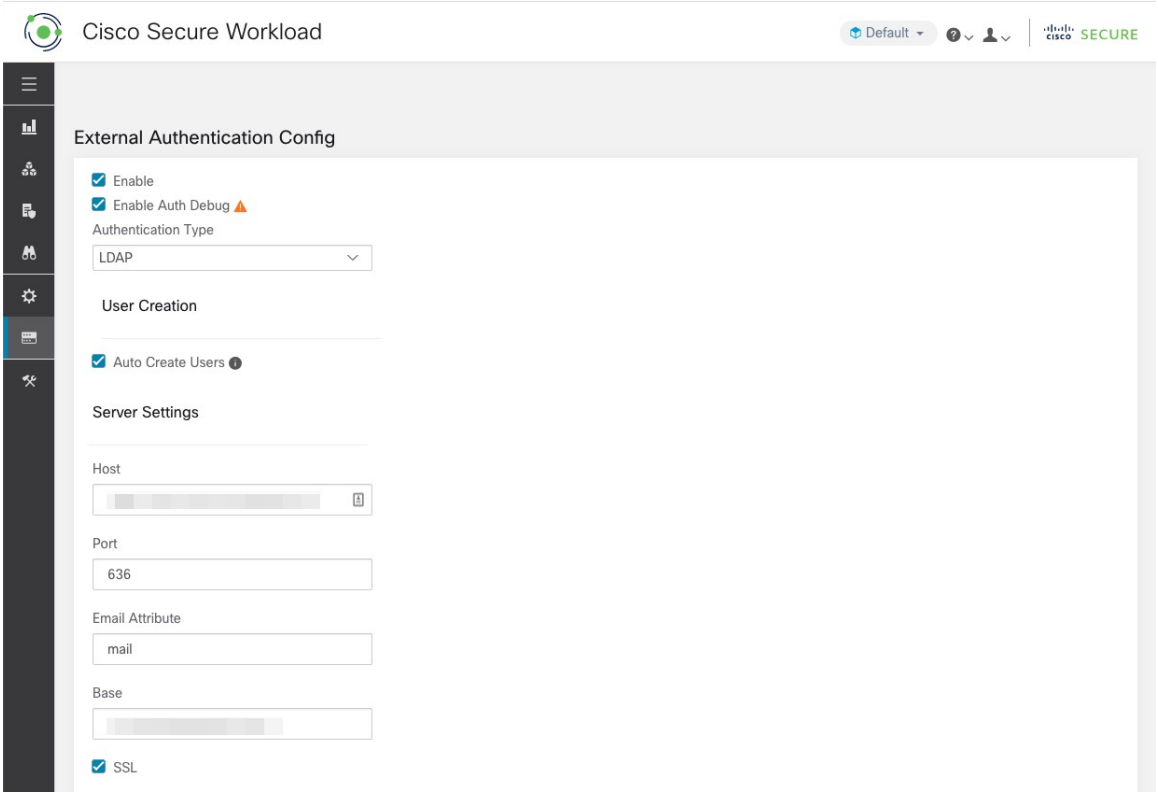
选择轻量级目录访问协议 (LDAP) 选项对用户进行身份验证。这意味着，启用此功能后，所有用户都将注销，后续登录将使用其 LDAP 电子邮件和密码进行身份验证。

如果启用了“联合”，目前不建议将 LDAP 作为身份验证机制。

如果启用了 LDAP，则建议的新用户创建工作流程如下。

鼓励**站点管理员**首先使用其邮件创建新用户，并在新用户首次通过LDAP登录之前，通过配置 LDAP 授权（AD 授权）来分配适当的角色。如果新用户通过 LDAP 登录时没有相应的角色，则不会为该用户分配默认角色。

Figure 13: 配置轻量级目录访问协议



字段	说明
自动创建用户 (Auto Create Users)	启用“自动创建用户”(Auto Create Users) 后，系统将创建首次登录时不存在的用户。这样，站点管理员就不必在允许用户登录之前预调配用户。如果应将 Cisco Secure Workload 访问权限限制为在“用户”(Users) 页面上手动创建的用户，则应关闭此选项。
主机 (Host)	将用于身份验证的 LDAP 主机。
端口 (Port)	将用于身份验证的 LDAP 端口。
邮件属性 (Email Attribute)	代表组织的邮件地址的 LDAP 属性名称。
基本 (Base)	用于搜索用户的 LDAP 基本 DN。
SSL	启用加密并使用“ldaps://”。
SSL 验证 (SSL Verify)	根据服务器证书验证服务器的 SSL 属性，如完全限定域名 (FQDN)。
SSL 证书颁发机构证书 (SSL Certificate Authority Cert)	LDAP 服务器的 SSL 证书的签名证书。如果服务器证书链无法公开验证，则此字段为必填。

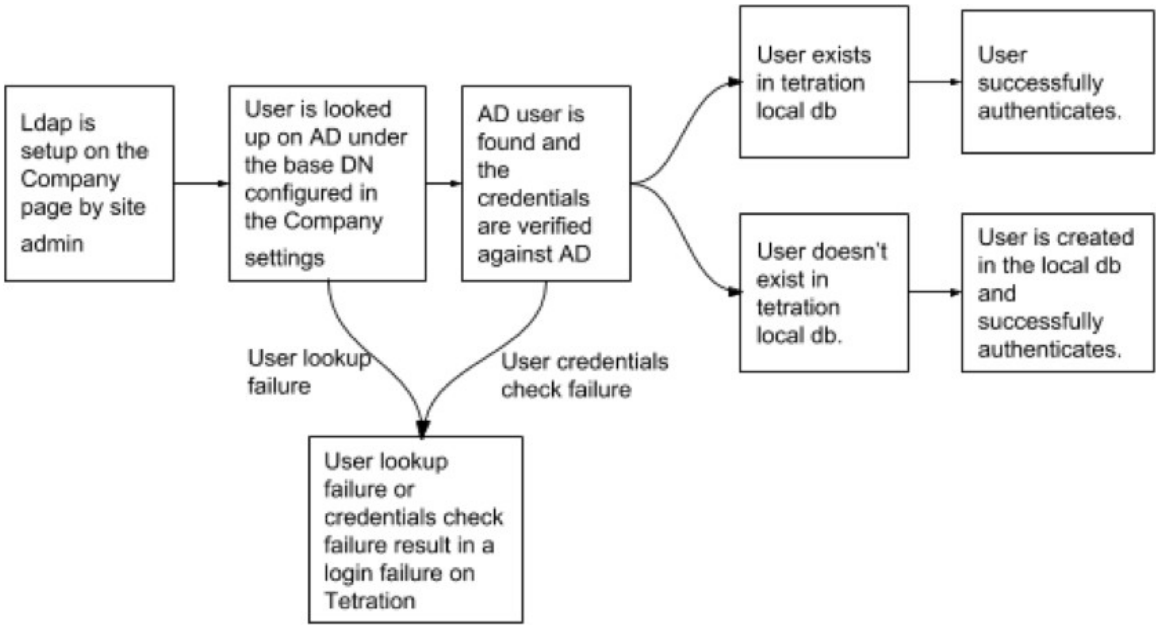
字段	说明
管理员用户 (Admin User)	用于与 LDAP 服务器绑定的 LDAP 管理员用户（而非 Cisco Secure Workload 用户）名称。例如：[User]@[Domain] 或 [Domain]\[User]
管理员密码 (Admin Password)	用于与 LDAP 服务器绑定的 LDAP 管理员密码。
Ldap 授权 (Ldap Authorization)	可以按照配置 LDAP 授权（AD 授权）中的说明来启用和配置 LDAP 授权。

启用 LDAP 配置后，除启用了“使用本地身份验证”(Use Local Authentication) 选项的用户之外，所有用户都将从其会话中注销。

点击**保存 (Save)** 按钮后，即可保存 LDAP 配置。建议您在成功保存 LDAP 配置后等待一分钟，然后再尝试测试 LDAP 连接。

保存 LDAP 配置后，可以使用**测试连接 (Test Connection)** 按钮测试 LDAP 连接。这将尝试使用输入的管理员凭证与 LDAP 服务器进行绑定。

Figure 14: 身份验证工作流程



对 LDAP 问题进行故障排除

如果在测试 ldap 连接时发生错误，请检查以下内容：

- 检查 LDAP 管理员凭证是否正确。
- 检查连接参数，例如主机、端口、SSL 等。
- 检查是否可以从 Cisco Secure Workload UI VIP 访问 LDAP 服务器。

- 检查 AD 服务器是否已启动。
- 将“**ldapsearch**”等命令行工具与连接详细信息一起使用，以查看是否可以进行绑定。

如果用户登录时出现错误，请检查以下内容：

- 检查用户能否使用 LDAP 凭证登录使用 LDAP 身份验证的其他公司网站。
- 检查公司 LDAP 设置中指定的“基本”dn 是否正确。这可以通过使用“**ldapsearch**”等命令行工具根据基本 DN 查找用户来完成。

通过邮件搜索用户的“**ldapsearch**”查询示例：

```
ldapsearch -H "ldap://<host>:<port>" -b "<base-dn>" -D "<ldap-admin-user>" -w
<ldap->admin-password> "(mail=<users-email-address>)"
```

配置 LDAP 授权（AD 授权）

可以通过启用外部身份验证 LDAP 配置的“管理员凭证”(Admin Credentials) 部分中的“LDAP 授权”(LDAP Authorization) 复选框来配置 Active Directory 授权。启用此设置后，站点管理员必须设置 LDAP ‘MemberOf’ 组到以下部分中的 Cisco Secure Workload 角色的映射。默认情况下，如果没有此配置，则必须在尝试登录之前为 Active Directory 用户预配置一个或多个 Cisco Secure Workload 角色。

如果已启用 LDAP 外部身份验证，则必须设置 LDAP MemberOf 组到 Cisco Secure Workload 角色的映射。“创建映射”允许设置要映射到 Cisco Secure Workload 角色的 LDAP MemberOf 组值。角色下拉列表中的角色是根据在范围选择器中选择的范围预先填充的。一旦保存了这些映射，所有用户在以后登录时都会根据这些值获得授权。

这些映射可以重新排序、编辑或删除。对映射的任何修改都将反映在用户以后登录时分配给他们的角色上。最多可以创建 50 个 LDAP MemberOf 组到 Cisco Secure Workload 角色的映射。

不允许重复的 LDAP MemberOf 组名称。但多个 LDAP MemberOf 组可以映射到同一角色。如果多个组映射到同一角色，则最后一个映射将作为与 Cisco Secure Workload 角色匹配的 LDAP MemberOf 存储在用户中。

***Figure 15: LDAP** 组至 **Cisco Secure Workload** 角色设置*

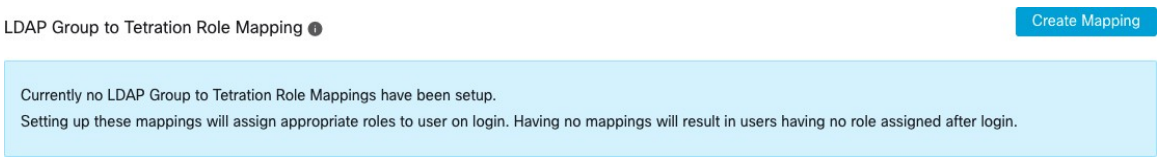
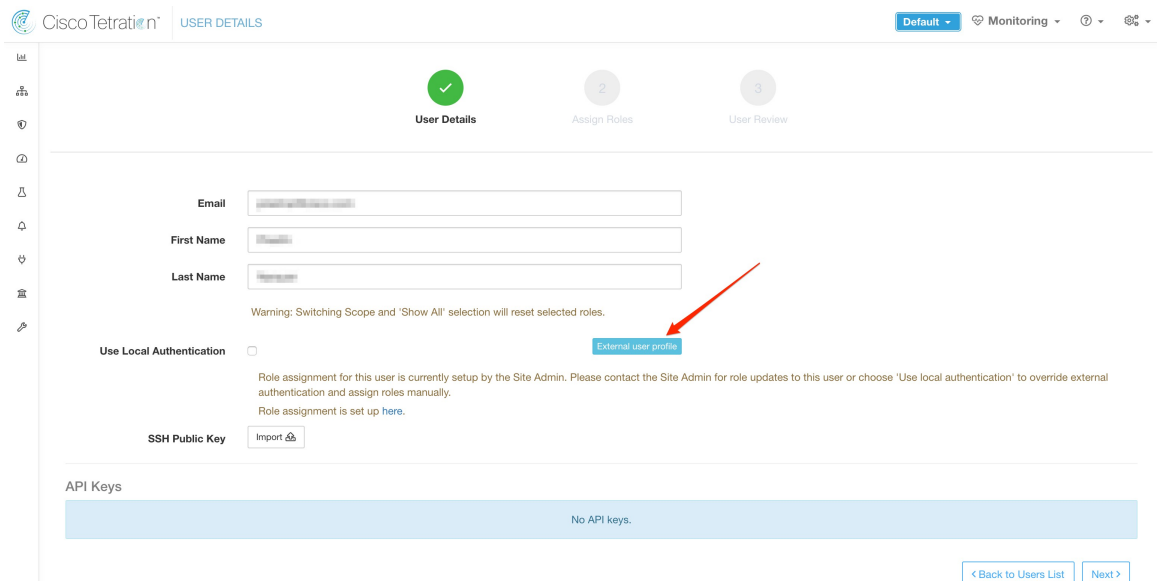


***Figure 16: LDAP** 组到 **Cisco Secure Workload** 角色的映射*

网站管理员用户可以根据上述角色映射，借助从用户上次成功登录时获得的外部用户信息来协调角色分配。

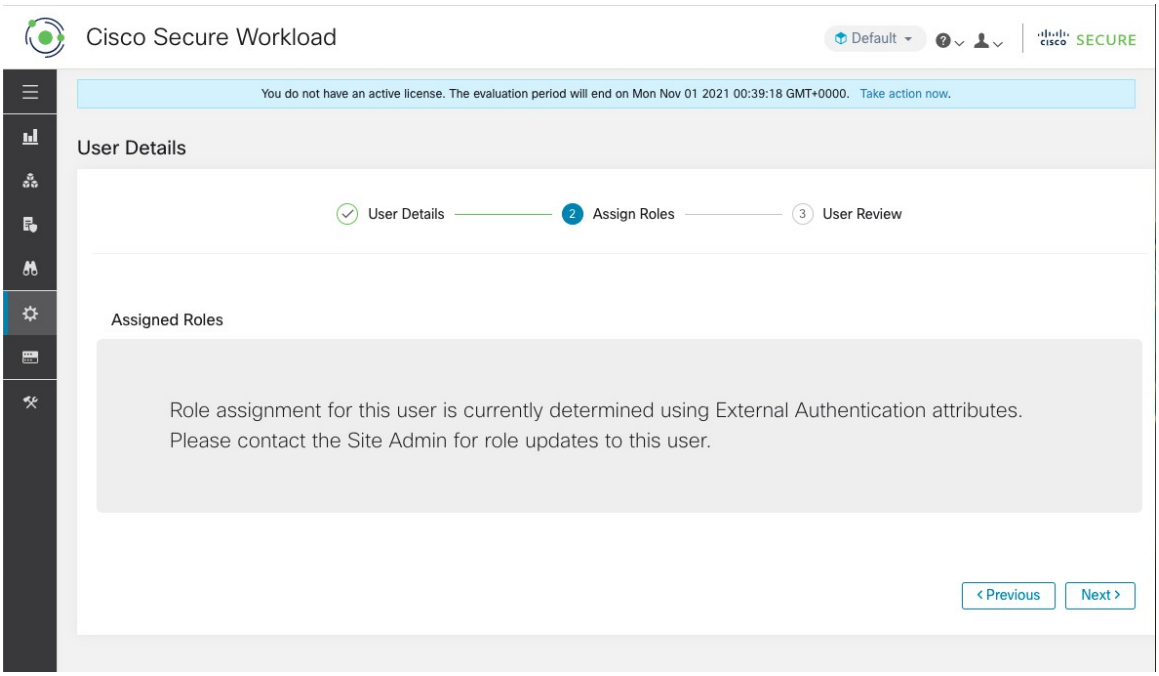
Note 按照“使用本地身份验证”(Use Local Authentication) 选项中的指明，按用户启用外部身份验证后，用户即可绕过外部身份验证。这些用户还将绕过为 AD 授权设置的授权流程。

Figure 17: 外部用户信息



启用授权后，将**不允许**在用户创建流 (添加用户, on page 57) 和用户编辑流（编辑用户详细信息或角色）中手动选择 Cisco Secure Workload 角色。

Figure 18: *“用户”(User)* 页面



映射到 Cisco Secure Workload 角色的 LDAP MemberOf 组会显示在用户配置文件页面上。

Figure 19: *“用户配置文件”(User Profile)* 页面

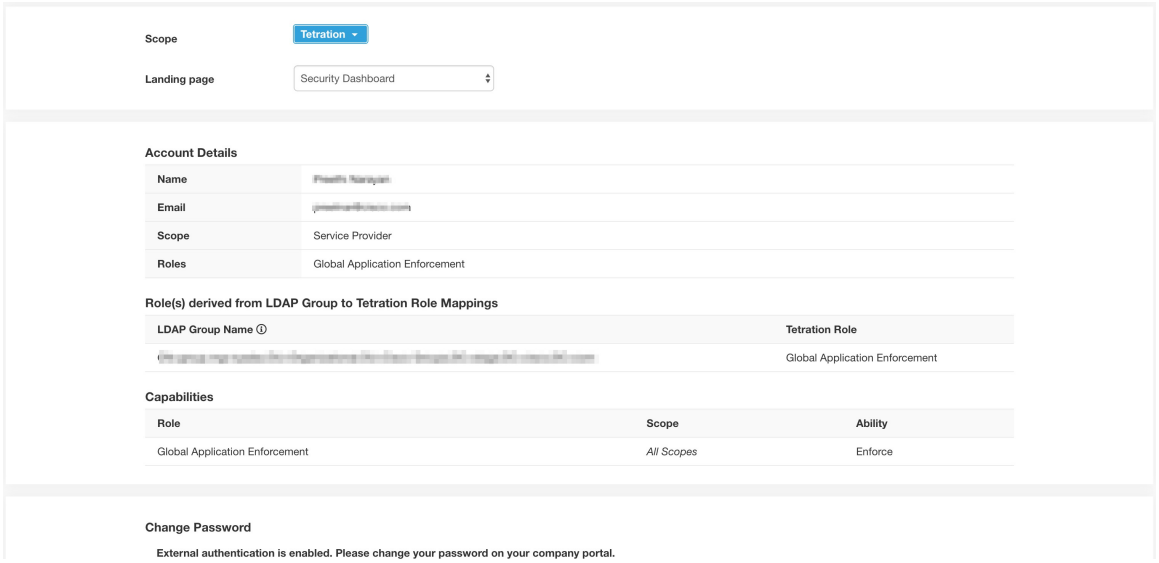
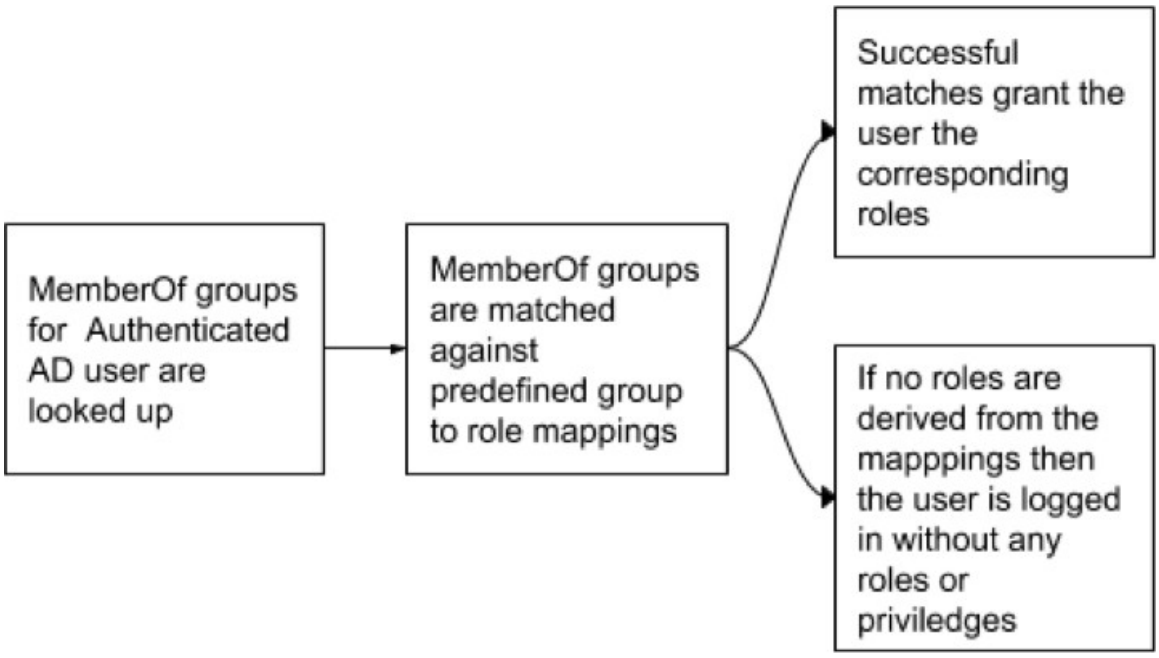


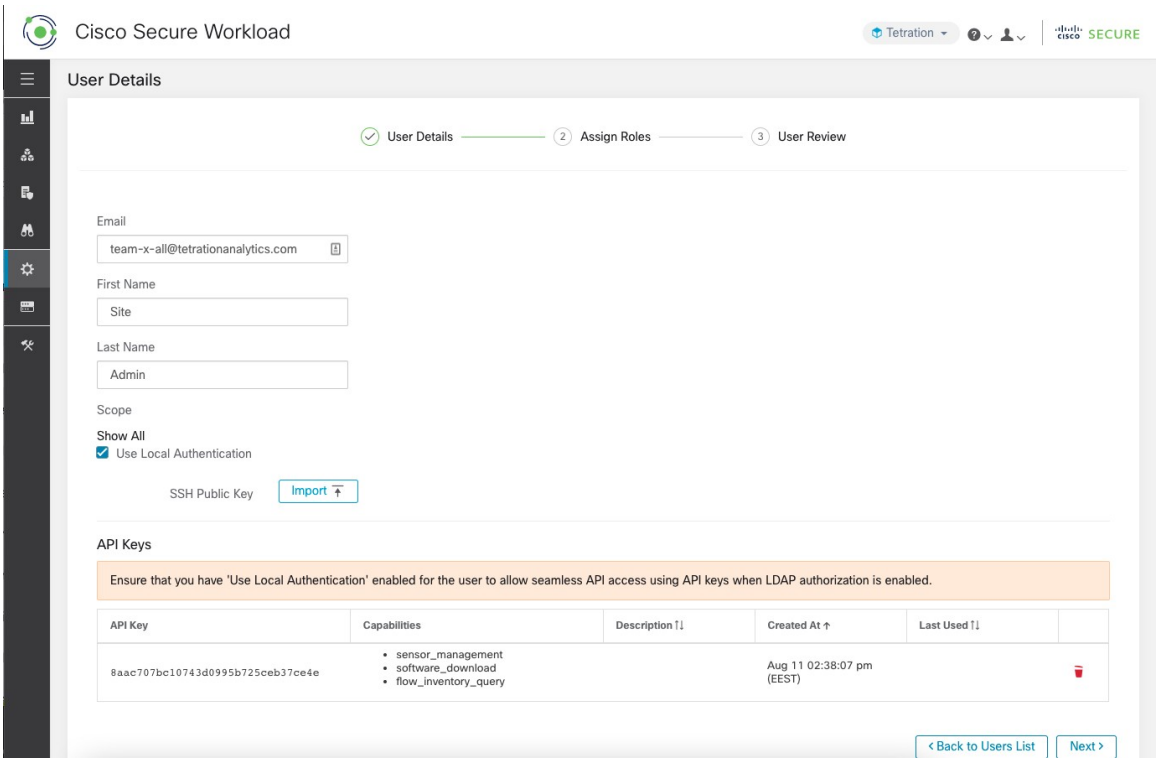
Figure 20: 授权工作流程



如果启用 LDAP 授权，则通过 API 密钥对 OpenAPI 的无缝访问将停止，因为当用户会话终止后，就会从 LDAP MemberOf 组派生的 Cisco Secure Workload 角色重新评估。因此，为确保 OpenAPI 访问不会中断，建议拥有 API 密钥的用户启用“使用本地身份验证”(Use Local Authentication) 选项。

Figure 21: LDAP 授权 *API* 密钥警告

Figure 22: “用户” *(Users)* 页面上的 *LDAP* 授权 *API* 密钥警告



对 LDAP 授权问题进行故障排除

如果角色没有根据“外部身份验证”、“LDAP 组到角色映射 ”部分中定义的映射分配给用户，请再次检查角色映射的设置和格式。

- 组字符串必须为字符串格式。例如：CN=group.jacpang,OU=Organizational,OU=Cisco Groups,DC=stage,DC=cisco,DC=com
- 组名必须与 AD 中的组名完全一致，并且不能有空格或多余字符。
- 必须从角色选择器中选择组的角色映射。

用户角色映射调试步骤

- 您必须有两个用户，一个是站点管理员，此用户的邮件地址不应与 AD 用户相同。
- 在以下步骤中，此用户称为“SA 用户”。
  - 如前所述，SA 用户已在“公司”(Company) 页面的“外部验证配置”(External Auth Config) 中设置了角色映射配置。假设“SA 用户”将使用 [site-admin]@[Domain] 登录。
  - 我们假设“AD 用户”为 [ad-user]@[Domain]。我们假设 LDAP 设置已完成，AD 用户可以登录，但无法获得分配的角色。
- 使用隐身浏览器会话作为 AD 用户登录。这会将浏览器状态从 SA 用户会话中分离出来。

- 以 SA 用户身份登录并转到“用户”(Users) 页面。
- 点击必须配置角色映射的 AD 用户的编辑图标。
- 点击“用户配置文件”(User Profile) 页面上的“外部用户配置文件”(External User Profile) 按钮。
- 您将看到一个包含“memberof”部分的外部身份验证配置文件表。
- 这是可用于“公司”(Company) 页面、“外部身份验证配置”(External Auth Config)、“LDAP 组到角色映射”(LDAP Group to Role-Mapping) 部分上的角色映射的“memberof”值之一。
- 您必须提供完整的“memberof”每行字符串进行匹配。创建角色映射后，拥有相同属性“memberof”的任何人都会被分配到映射的角色。
- 要授予AD用户新映射的角色，用户需要注销，然后重新登录，以便重新评估该映射配置文件。
- 用户登录并具有由于组角色映射而成功分配的角色后，匹配规则将在该用户的“首选项”(Preferences) 页面上可见。

配置单点登录

如果选择了此选项，则可使用单点登录 (SSO) 来验证用户身份。这意味着启用该功能后，所有用户都将被重定向到身份提供者登录页面进行身份验证。启用“使用本地身份验证”(Use Local Authentication) 选项的用户可以使用登录页面中的邮箱和密码登录表单进行身份验证。

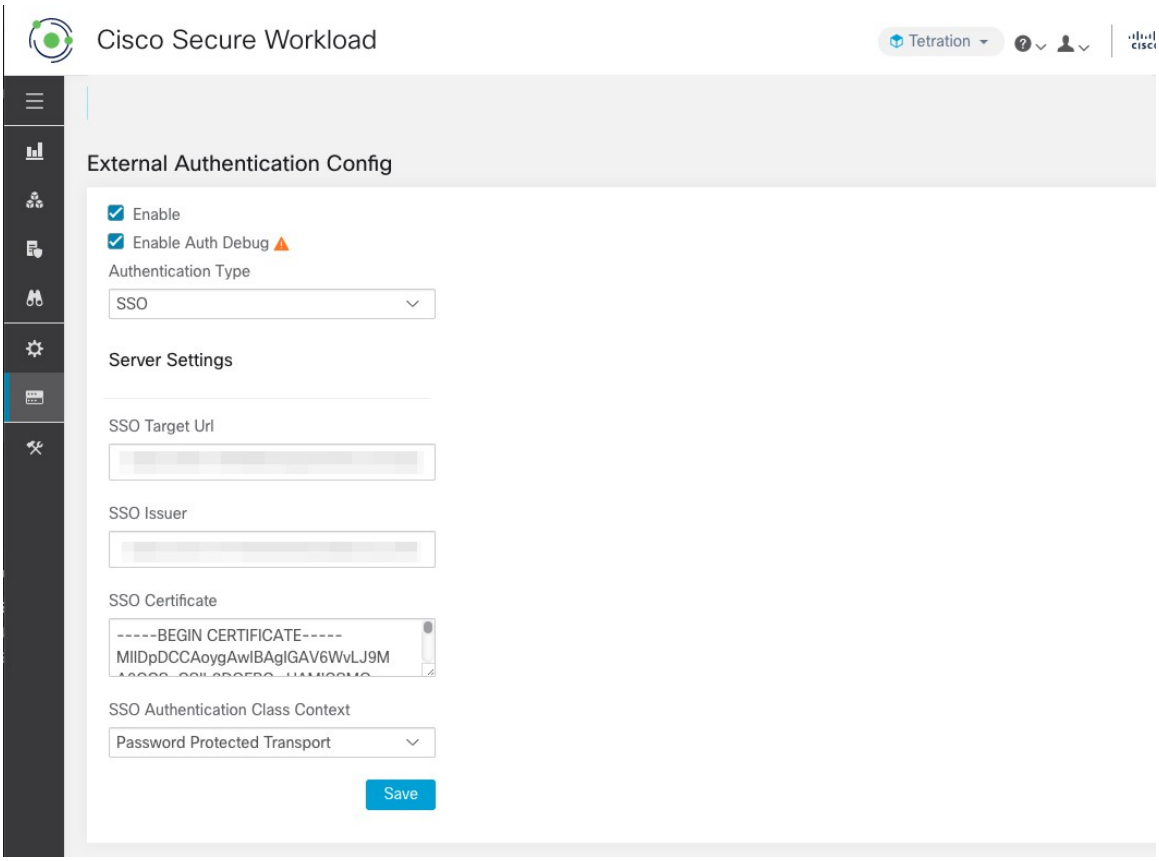
确定 SSO 配置是否设置正确非常重要，尤其是在“使用本地身份验证”(Use Local Authentication) 选项上没有用户的情况下。建议的方法是，通过打开“使用本地身份验证”(Use Local Authentication) 选项，让至少一个本地身份验证用户拥有**站点管理员**凭证。此用户可以确保SSO配置设置正确。成功设置连接后，还可以通过取消选中用户编辑流程中的“使用本地身份验证”(Use Local Authentication) 选项，将此用户转换为外部身份验证。

如果启用了 SSO，建议创建新用户的工作流程如下。

我们鼓励**站点管理员**和**范围所有者**首先使用其邮件地址创建新用户，并在新用户首次通过 SSO 登录之前分配适当的角色和范围。如果新用户通过 SSO 登录时没有相应的角色，则不会为该用户分配默认角色。

下表介绍为了在 Cisco Secure Workload上配置 SSO 而必须设置的字段。在本例中，Cisco Secure Workload 是运营商 (SP)。

Figure 23: 配置单点登录

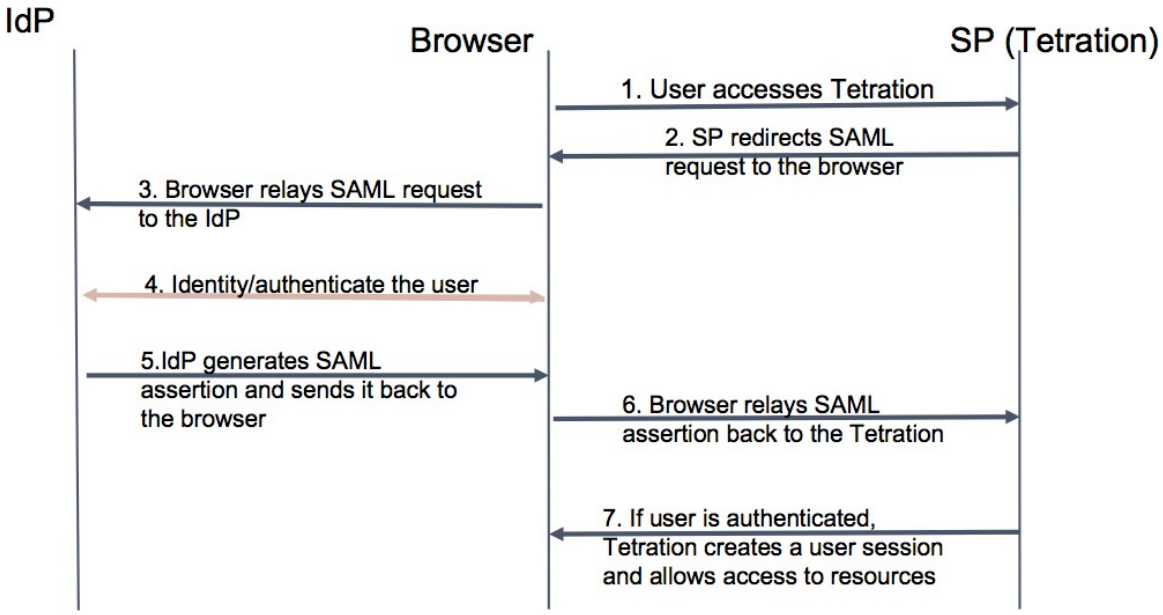


字段	说明
SSO Target Url	用户登录时将被重定向到的 SSO IdP 目标 URL。
SSO Issuer	您的 SP 的 SSO 实体 ID，用于唯一标识您的 SP 的 URL。这通常是 SP 的元数据。在本例中为： `https://<tetration-cluster-fqdn>/h4_users/saml/metadata`
SSO Certificate	由身份提供者 (IdP) 提供的 SSO 证书。
SSO AuthN Context	在 SAML 请求中指定的 SSO AuthN 情景的选项。默认选项为“受密码保护的传输”(Password Protected Transport)。对于 Windows 和基于 PIV 的身份验证，其他选项包括“集成 Windows 身份验证”(Integrated Windows Authentication) 和“X.509 证书”(X.509 Certificate)。

启用 SSO 配置后，除已启用“使用本地身份验证”(Use Local Authentication) 选项的用户之外，所有其他用户都将从其会话中注销。

点击**保存 (Save)** 按钮后，系统会保存 SSO 配置。

Figure 24: 身份验证工作流程



与身份提供者 (IdP) 共享的信息

IdP 需要来自 Cisco Secure Workload (SP) 的一些信息来设置 SSO，以便进行身份验证。下表描述了必须设置的字段。

字段	说明
SSO Url	用于接收 SAML 断言（来自 IdP 的响应）的身份验证终端 (url)。在我们的示例中，它将是： `https://<tetration-cluster-fqdn>/h4_users/saml/auth`
Entity Id	这是 SP 的元数据。在本例中为： `https://<tetration-cluster-fqdn>/ h4_users/saml/metadata`
Name ID format	NameId 是邮箱，即 `'urn:oasis:names:tc:SAML:1. 1:nameid-format:emailAddress'`
Attributes	从 IDP 获取用户属性。我们在身份验证过程中获取这些属性： • email • firstName • lastName 确保属性名称与之前指定的名称相同。

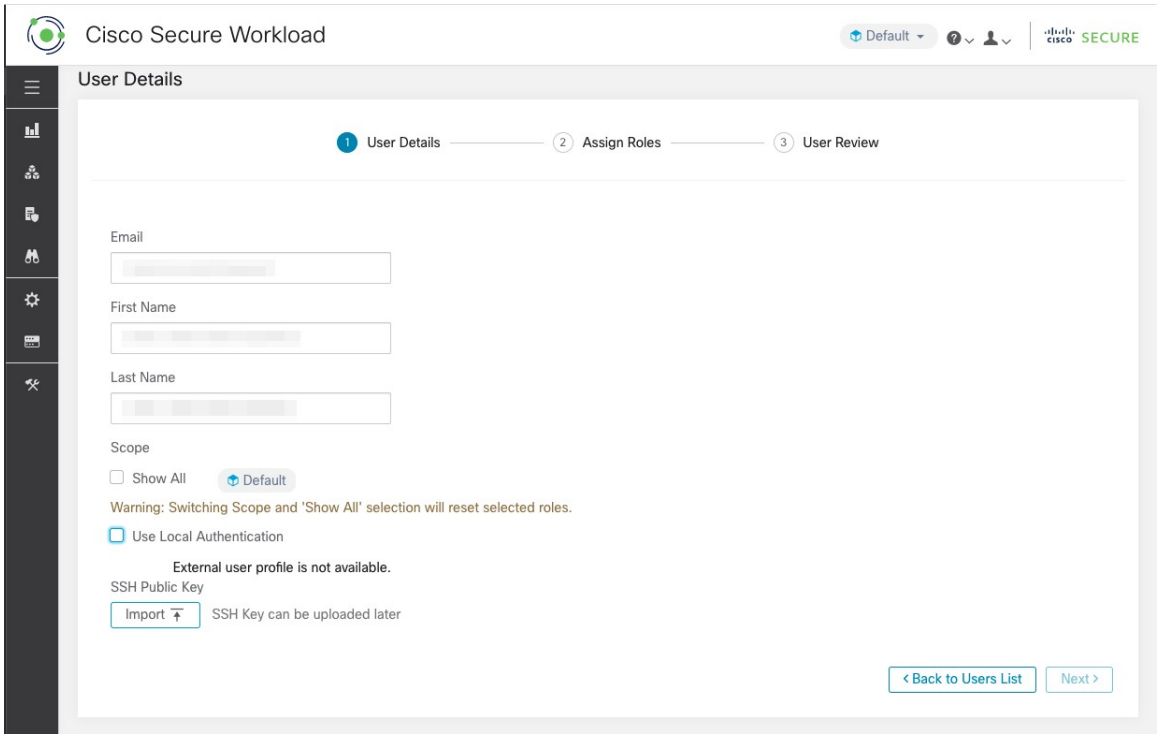
排除 SSO 问题

- 为此 SSO 配置设置设置一些停机时间，因为（从运营商）验证身份验证是否有效的唯一方法是在设置之后进行。
- 检查并验证生成的 IdP 元数据。
- 检查 IdP 与 SP 之间交换的所有配置参数。
  - IdP 上的配置 - SSO URL、受众、名称 ID、属性等
  - Cisco Secure Workload 公司页面上的配置 - SSO 目标 URL、SSO 颁发者和 SSO 证书。
- 从服务器应用日志中获取从 IdP 返回的示例 SAML 断言。根据 SAML 验证器对其进行验证，以确保其是有效的 SAML 响应。
- 运营商 SSO 设置中的错误可能会导致从 IdP 生成错误。通过使用浏览器检查元素，您可以查看正在发出的网络请求。
- 如果用户在登录时遇到问题，请让 IdP 管理员检查该用户是否有权访问 Cisco Secure Workload 应用。

“使用本地身份验证”(Use Local Authentication) 选项

设置配置后，站点管理员可以允许用户不使用外部身份验证。这可以通过在用户编辑部分启用标志“使用本地身份验证”(Use Local Authentication) 来逐个用户完成。为用户选择该字段将使该用户从所有会话注销。

Figure 25: 使用本地身份验证



Warning **确保至少一位用户具有本地身份验证访问权限！**

如果为某个用户删除了“(Use Local Authentication) 使用本地身份验证”选项（即取消选中），并且此用户恰好是使用该选项的最后一个用户，则没有用户具有登录到 Cisco Secure Workload 的本地身份验证访问权限。这意味着，如果外部身份验证系统出现任何中断（如配置问题、连接问题等），任何用户都无法登录。如果尝试删除最后一个经过本地身份验证用户，则会看到一条警告。

通过外部身份验证进行日志记录的用户的会话较短，当会话到期时，系统会提示用户进行登录。通过外部身份验证登录的用户无法在站点上重置密码（必须在公司网站上重置）。但是，如果为用户设置了“使用本地身份验证”(Use Local Authentication) 标志，则可以重置密码。

SSL 证书和密钥

要启用对 Cisco Secure Workload UI 的完全可验证的 HTTPS 访问，可将 UI 域名专用的 SSL 证书和与 SSL 证书公钥匹配的 RSA 私钥上传到集群。

SSL 证书有两种获取方式，取决于用于引用 Cisco Secure Workload UI 虚拟 IP (VIP) 地址的完全合格域名 (FQDN) 的格式。如果 Cisco Secure Workload FQDN 基于企业域名（例如 tetration.cisco.com），则拥有该基本域的企业证书颁发机构 (CA) 会向您颁发一个 SSL 证书。否则，您可以使用信誉良好的 SSL 证书供应商为您的 FQDN 颁发 SSL 证书。

Note 值得注意的是，虽然 Cisco Secure Workload UI 支持服务器名称指示 (SNI)，但证书中指定的主题替代名称 (SAN) 将无法匹配。例如，如果证书的通用名 (CN) 是 tetration.cisco.com，而证书中包含一个 tetration1.cisco.com 的 SAN，那么使用 SNI 兼容浏览器向以 tetration1.cisco.com 为主机名的集群发送的 HTTPS 请求将无法通过该证书获得服务。使用 CN 中指定的主机名以外的主机名向集群发出的 HTTPS 请求，将使用集群上安装的默认自签名证书提供服务。这些请求会导致浏览器警告。

站点管理员和**客户支持用户**可以使用 SSL 证书。在左侧的导航栏中，点击**平台 (Platform)** > **SSL 证书 (SSL Certificate)**。

要导入证书和密钥，请点击**导入新证书和密钥 (Import New Certificate and Key)** 按钮。

Note SSL 认证和私钥的首次导入应通过与集群的可信网络连接进行，这样私钥就不会被可访问传输层的恶意方截获。

输入 SSL 证书和密钥的以下信息：

NAME 可以是证书密钥对的任何名称。此名称有助于您查看安装的 SSL 证书。

X509 证书 (X509 Certificate) 字段接受隐私增强邮件 (PEM) 格式的 SSL 证书字符串。如果您的 SSL 证书需要中间 CA 捆绑包，请在证书之后连接 CA 捆绑包，以便让 Cisco Secure Workload FQDN 的 SSL 证书位于证书文件的开头。

其格式如下：

```
-----BEGIN CERTIFICATE-----
< Certificate for Cisco Secure Workload FQDN >
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
< Intermediary CA 1 content >
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
< Intermediary CA 2 content >
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
< Root CA content >
-----END CERTIFICATE-----
```

RSA 私钥 (RSA Private Key) 字段应该是在前一个证书中签名的公钥的 RSA 私钥。其格式如下：

```
-----BEGIN RSA PRIVATE KEY-----
< private key data >
-----END RSA PRIVATE KEY-----
```

Note RSA 私钥必须未加密。如果 RSA 私钥已加密，则会导致“500 内部服务器错误”。

导入后将执行验证步骤，以确保证书中签名的公钥和私钥确实是RSA密钥对。如果验证成功，我们将显示证书捆绑包的 SHA-1 摘要（SHA-1 签名和创建时间）。

重新加载浏览器，以查看与 Cisco Secure Workload UI 的 SSL 连接现在正在使用新导入的 SSL 证书。

集群配置

此部分显示有关客户网络和管理联系人的 Cisco Secure Workload 集群的运行配置。可编辑的值以铅笔图标表示。

Note a. 用于代理连接的强 SSL 密码：启用此选项后，在 SSL 协商期间，Cisco Secure Workload 集群不会接受 TLS-1.0 和 TLS-1.1 协议及以下密码：DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA

后续连接会遵守这一规定，并在 TLS 握手过程中使用强密码：

1. 与 Cisco Secure Workload 的所有 API 和 UI 连接。
2. 与 Cisco Secure Workload 的所有可视性和执行代理连接。

请注意，较旧的 SSL 库可能不支持此选项。

站点管理员和**客户支持用户**可以访问此设置。在左侧导航栏中，点击**平台 (Platform)** > **集群配置 (Cluster Configuration)**。

编辑配置后，新配置需要一些时间才能应用到整个集群，并通过高亮显示特定配置来表示。

外部 IPv6 集群连接

物理思科 Cisco Secure Workload 集群可以配置为连接到外部 IPv4 和 IPv6 网络。IPv4 连接为必需，但 IPv6 连接为可选。IPv6 连接一经配置就无法禁用。只能在部署或升级期间为集群的外部网络启用 IPv6 连接。有关在升级期间启用外部 IPv6 集群连接的详细信息，请参阅《思科 Cisco Secure Workload 升级指南 》；有关在部署期间启用外部 IPv6 集群连接的详细信息，请参阅《思科 Cisco Secure Workload 硬件部署指南》。

Before you begin

让代理在双堆栈模式下运行（同时支持 **IPv4** 和 **IPv6**）

前提条件

- 集群必须启用 IPv6。
- 在 DNS 中为 FQDN 创建 A 和 AAAA 记录（适用于 IPv4 和 IPv6），并等待域名解析。

为代理配置“Sensor VIP FQDN”，使其在双堆栈模式下运行

Procedure

步骤 1 从左侧导航栏中选择**平台 (Platform)** > **集群配置 (Cluster Configuration)**。

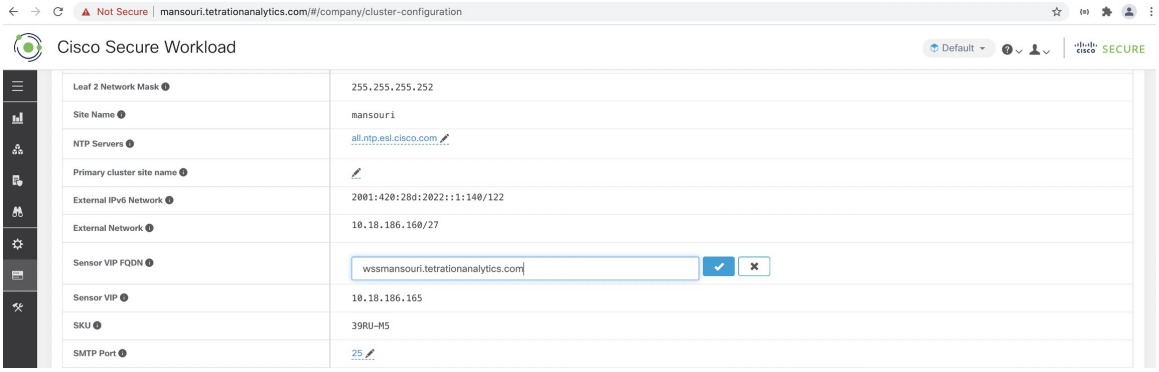
步骤 2 查找“Sensor IPv6 VIP”、“Sensor VIP”和“Sensor VIP FQDN”字段。“Sensor IPv6 VIP”和“Sensor VIP”应已设置。

步骤 3 如果未设置“Sensor VIP FQDN”，请将其设置为上面创建的 FQDN。在执行此操作之前，必须解析 FQDN 的 DNS 中的 A 和 AAAA 记录。

步骤 4 如果已设置“传感器 VIP FQDN”(Sensor VIP FQDN)，请确保在 DNS 中存在“传感器 VIP FQDN”(Sensor VIP FQDN) 字段中设置的 FQDN 的 A 和 AAAA 记录，然后点击“传感器 VIP FQDN”(Sensor VIP FQDN) 字段并将其保存到同一值，以便更新。

步骤 5 字段完成更新后（大约 20 分钟后，状态会自动更新），代理将能够通过 IPv4 和 IPv6 连接到集群。

步骤 6 有效的“传感器 VIP FQDN”只能设置一次。



Note AIX 不支持 IPv6 执行。有关双栈模式要求和限制的详细信息，请参阅《思科 Cisco Secure Workload 升级指南》

NTP 身份验证

Cisco Secure Workload 本地版本支持网络时间协议版本 (NTP) 版本 4 和 SHA-1 身份验证。使用“设置”(Setup) 用户界面配置 NTP 服务器，或使用“集群配置”(Cluster Configuration) 页面在 Cisco Secure Workload 上部署设备。

要使用 Cisco Secure Workload 用户界面配置 NTP 身份验证，请执行以下操作：

Procedure

步骤 1 配置NTP服务器：运行CentOS 7的系统会提供以下配置作为参考，而这些配置会因操作系统而异。

a) 确保 /etc/ntp.conf 下提供了以下条目。

```
# Key file containing the keys and key identifiers used when operating with symmetric
key cryptography.
keys /etc/ntp/keys

# Specify the key identifiers which are trusted.
trustedkey 1
controlkey 1
requestkey 1
```

b) 在 /etc/ntp/keys 下输入服务器端密钥。

```
# For more information about this file, see the man page ntp_auth(5).
# id type key
1 SHA1 <password>
```

c) 重启 NTP 服务器：`# service ntpd restart`

d) 启动 NTP 服务器的服务：

```
# ntpq -p
     remote           refid      st  t  when  poll  reach  delay  offset  jitter
==============================================================================
<ntp.server.com> <refid>      5  u  17     64     377  0.000  0.000   0.000
```

步骤 2 在 Cisco Secure Workload UI 上，导航至**平台 (Platform)** > **集群配置 (Cluster Configuration)**。

步骤 3 在**已通过身份验证的 NTP 服务器 (Authenticated NTP Server)** 字段中，输入 NTP 服务器的名称或 IP 地址。

步骤 4 在**已通过身份验证的 NTP 服务器密码 (Password For Authenticated NTP Server)** 字段中，输入 NTP 服务器密码。

配置并验证 NTP 服务器后，已验证的 NTP 服务器优先于在 Cisco Secure Workload 中输入的任何未验证的 NTP 服务器。

使用分析

站点管理员和**客户支持用户**可以启用或禁用使用情况分析。在导航栏中，点击**管理 (Manage)** > **服务设置 (Service Settings)** > **使用情况分析 (Usage Analytics)**。

Cisco Secure Workload 收集数据，通过单向散列匿名呈现，然后将其发送到服务器。为本地设备按设备配置隐私设置，为思科 Cisco Secure Workload SaaS 按租户配置隐私设置。您还可以在此页面启用数据收集并切换收集。

联合

联合提供了一种将多个 Cisco Secure Workload 设备连接在一起，并将其大部分管理整合到指定为**领导者**的单台设备的方法。

注释

- 此功能要求联合中的所有设备都运行版本 3.4.x 或更高版本。
- 请联系思科技术支持中心以启用联合选项。

设置联合

过程

步骤 1 在指定的**领导者**上，导航至 **平台 (Platform)** > **联合 (Federation)**，然后点击**创建新联合 (Create New Federation)** 按钮。

步骤 2 要添加第一个**跟随者**设备，请输入其名称和完全限定域名 (FQDN)，然后点击**添加 (Add)** 按钮。

步骤 3 点击链接以下载加入证书文件。

步骤 4 在**跟随者**上，导航至**平台 (Platform)** > **联合 (Federation)**，然后点击**加入现有联合 (Join Existing Federation)**，并选择上面创建的加入证书。

步骤 5 对将成为联合的一部分的每个**跟随者**重复步骤 2-4。

图 *26:* 创建或加入联合

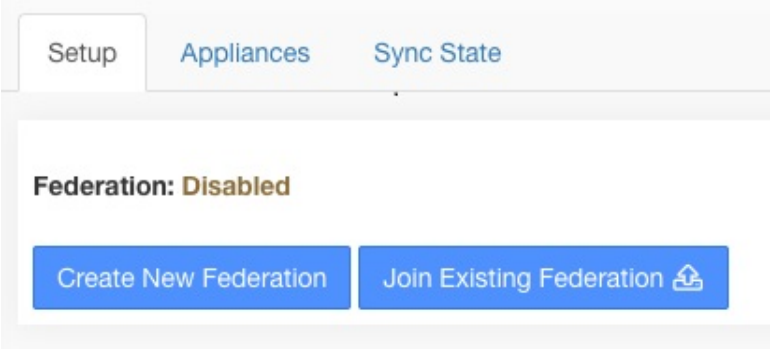
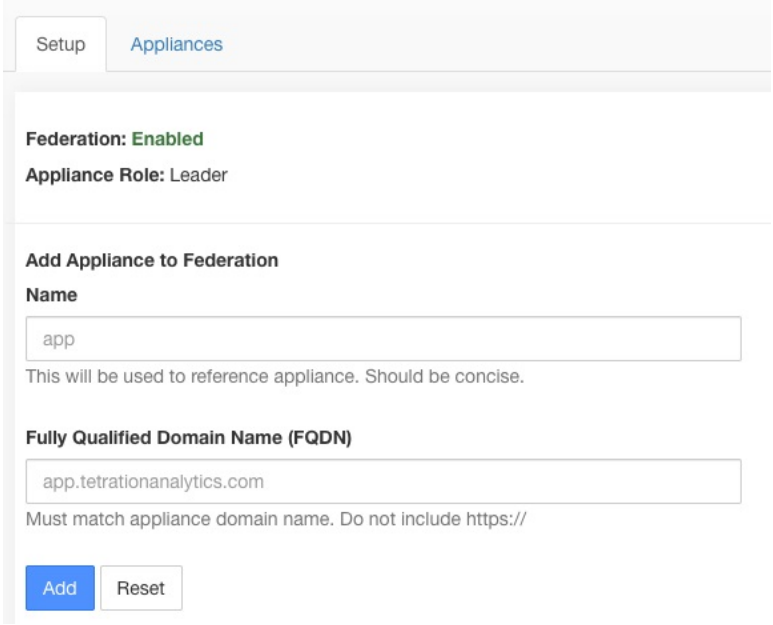
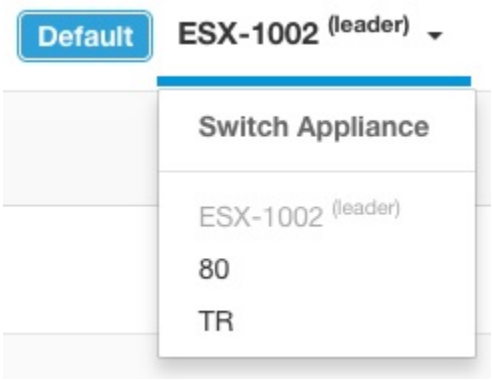


图 *27:* 联合添加跟随者表单



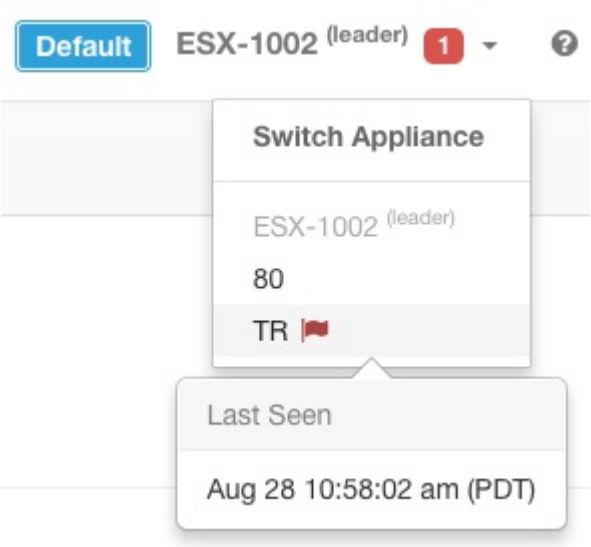
启用联合后，标头包括设备名称和用于更改设备的选择器。

图 *28:* 设备选择器



如果联合中的一个或多台设备在超过10分钟内未被领导者发现，则设备选择器中会显示警报，并且有问题的设备将被标记。将光标悬停在上面将显示它们上次与领导者同步的时间。

图 *29:* 带警报的设备选择器



身份验证设置

使用单点登录 (SSO) 设置启用了联合的身份验证。必须在联合的每台设备部分上配置 SSO。如在每台设备上配置单点登录 (SSO) 所示，在**平台 (Platform)** > **外部身份验证 (External Authentication)** 页面上的领导者和每个跟随者上配置 SSO 设置。

管理任务

根据管理任务，有些必须在**领导者**上执行，有些则必须在**跟随者**上执行。下表列出了每项任务的设备类型。

表 *9:* 联合设备中的管理任务

任务	设备
用户	领导者
范围	领导者
角色	领导者
租户	领导者
API 密钥	领导者
收集规则	领导者
软件代理配置	领导者

任务	设备
软件代理	跟随者
软件代理升级	跟随者
软件代理降级	跟随者
资产过滤器	领导者
资产上传	领导者
默认策略发现配置	领导者
策略顺序	领导者

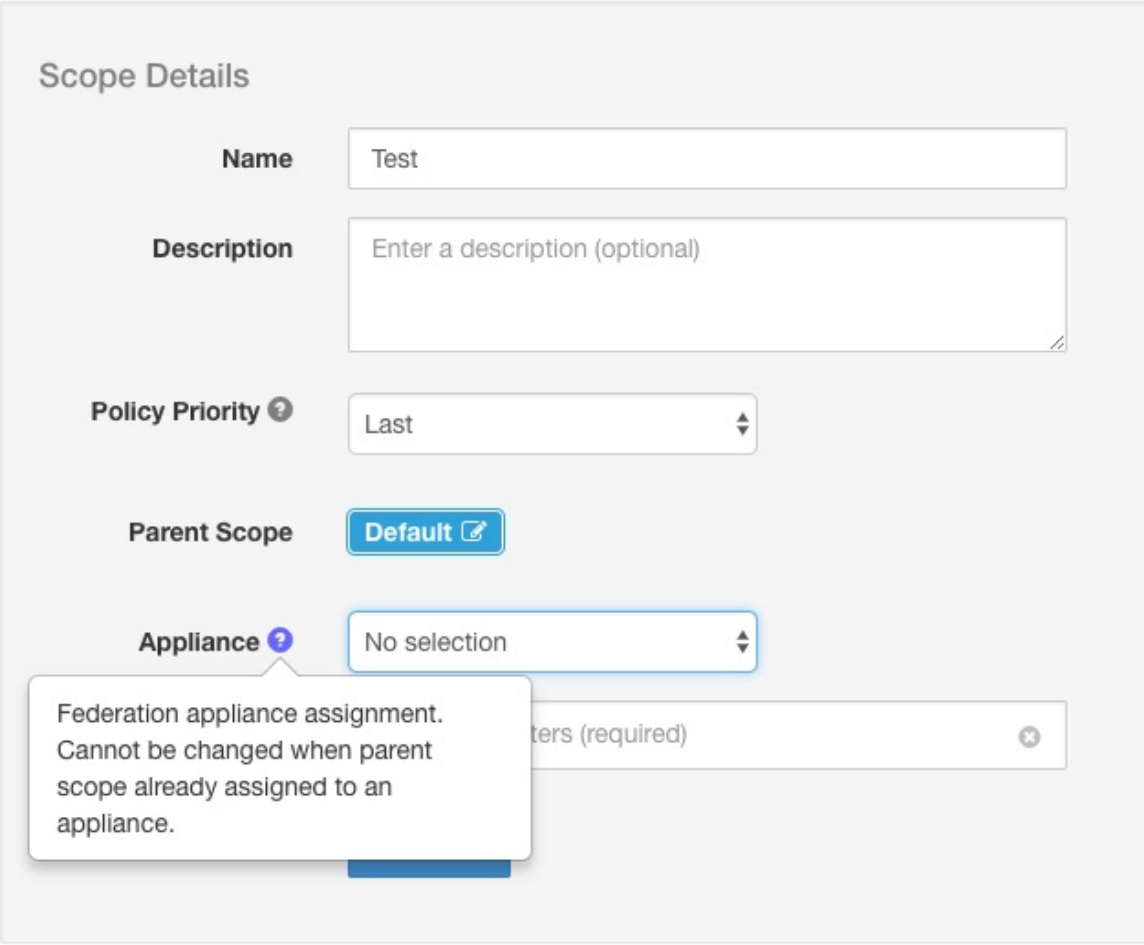
范围

当某个范围内的资产由单台设备管理时，可以将该范围分配给该设备。这可以在与该范围关联的工作空间中实现自动策略发现、策略分析和执行。它还将确保在该范围上创建的策略只适用于连接到设备的代理。

在全局范围内创建的应用（未指定给设备）不能用于自动策略发现或策略分析。但是，它们可用于在联合中的所有设备上执行策略。

可在创建过程中或通过编辑范围将设备分配给范围。所有子范围都会继承父设备的设备，并且不能分配给其他设备。

图 *30:* 将设备分配到范围



注释 根级范围（租户）总是全局性的，无法分配给设备。

工作空间

所有工作空间（“应用”）都必须在**领导者**上进行管理。但是，基于流的图表只能在相应的**跟随者**设备上查看。其中包括**策略分析 (Policy Analysis)** 和**执行 (Enforcement)** 选项卡下显示的图表。在**领导者**上，点击**查看本地设备上的图表 (View Charts on Local Appliance)** 以导航至相应的**跟随者**。

图 *31:* 领导者策略分析

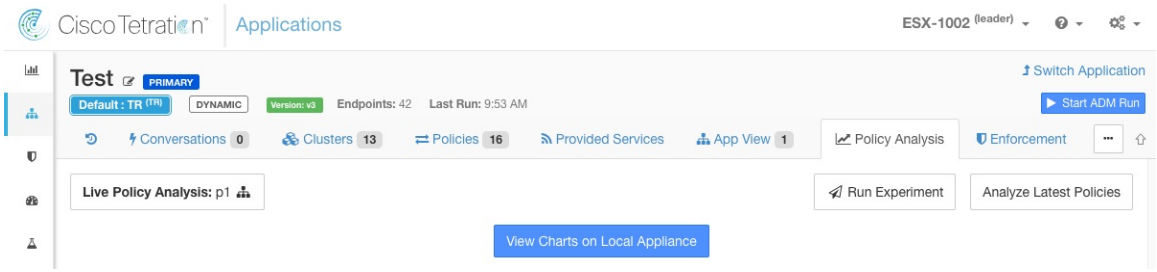
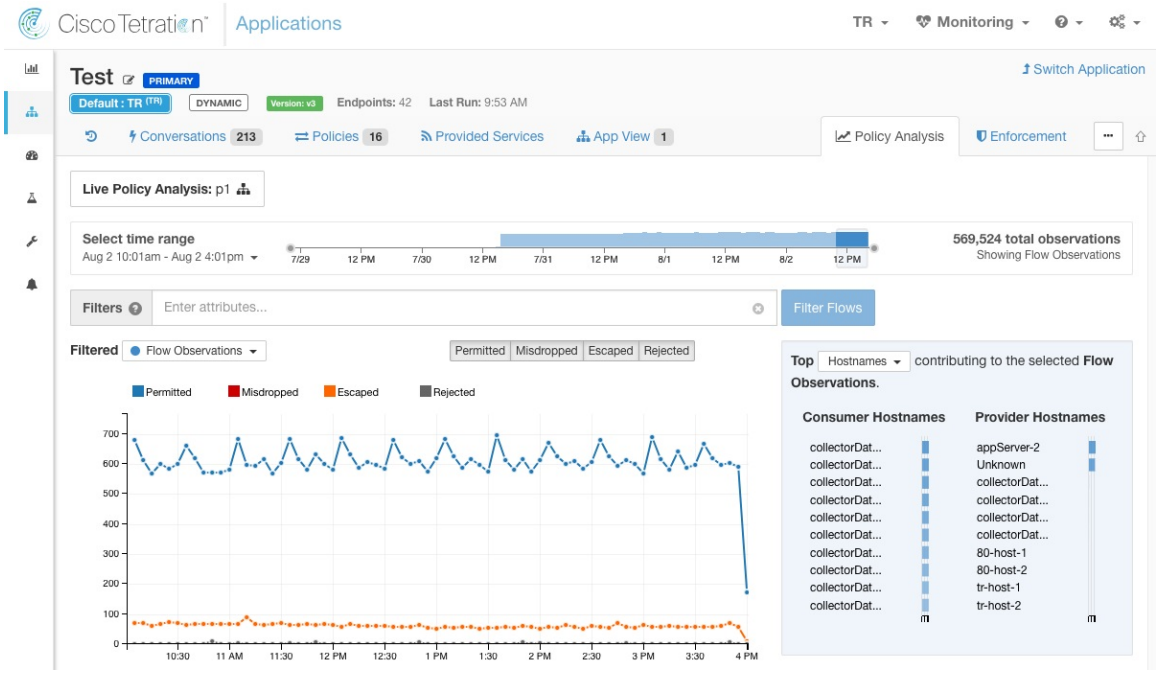
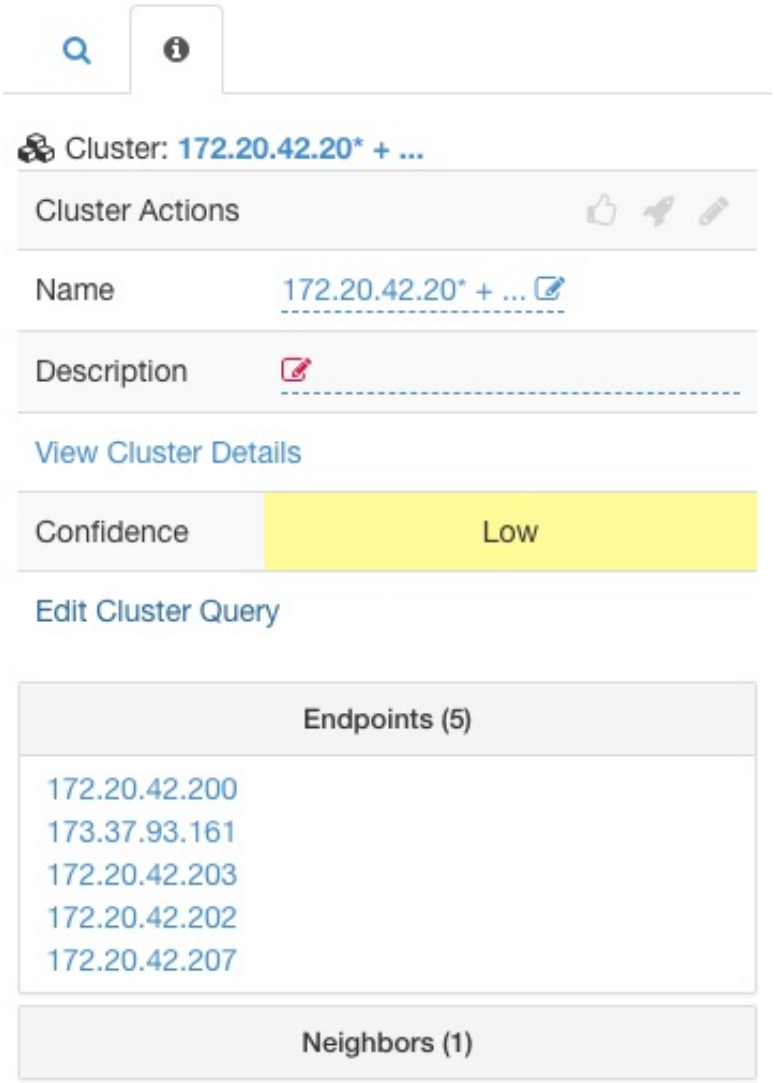


图 *32:* 对跟随者的策略分析



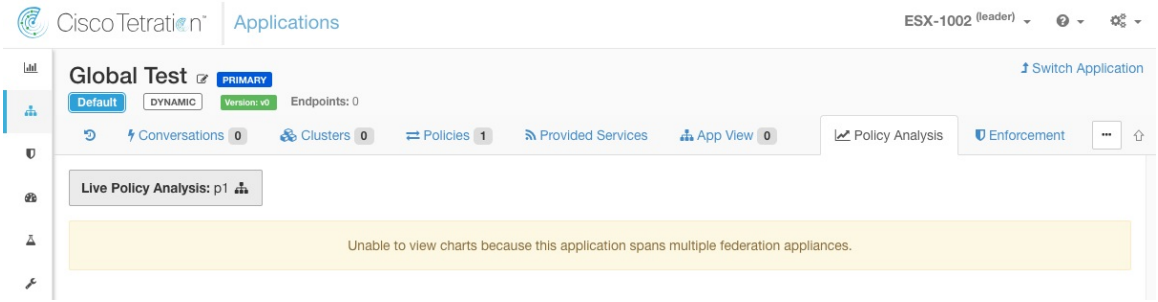
此外，始终在本地执行针对资产的搜索（自动策略发现页面除外）。因此，有必要导航至**跟随者**以查看集群、过滤器和范围终端。同样的逻辑也适用于查看集群、过滤器和范围详细信息。

图 *33:* 集群侧边栏



如上所述，在全局范围内创建的工作空间不能用于自动策略发现或策略分析。虽然可以执行策略，但基于流的执行图表不可用。

图 *34:* 已在全局范围上禁用策略分析



警告 使用与设备关联的范围或受限资产过滤器的策略将仅在该设备上执行。

软件代理

连接到联合中的任何设备的所有软件代理在**领导者**设备上可见。

过程

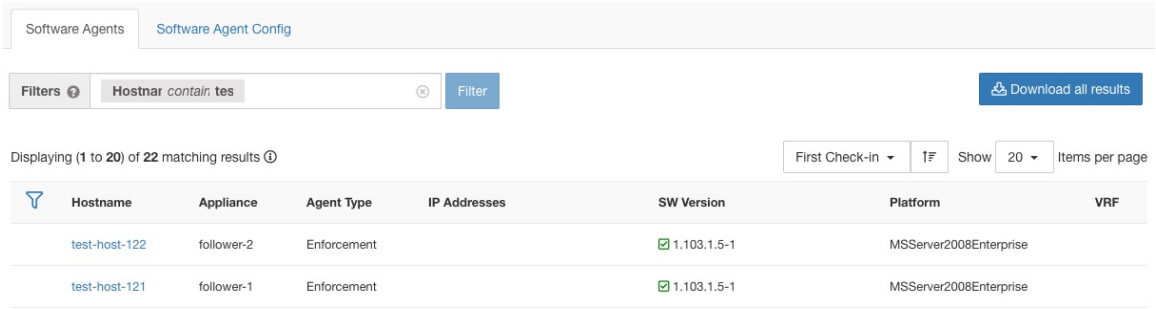
步骤 1 点击右上角的**设置菜单**。

步骤 2 选择**代理配置 (Agent Config)**。
系统将显示**代理配置 (Agent Config)** 页面。

步骤 3 点击**软件代理 (Software Agents)** 选项卡。
系统将打开**软件代理 (Software Agents)** 选项卡。

步骤 4 查找要移动的一个或多个代理，然后点击在其表行中找到的复选框。

步骤 5 **设备 (Appliance)** 列指明代理的连接位置。



在跟随者设备之间移动软件代理

软件代理可以在**跟随者**设备之间移动。在代理连接到的设备上，执行以下步骤：

过程

步骤 1 点击右上角的**设置菜单**。

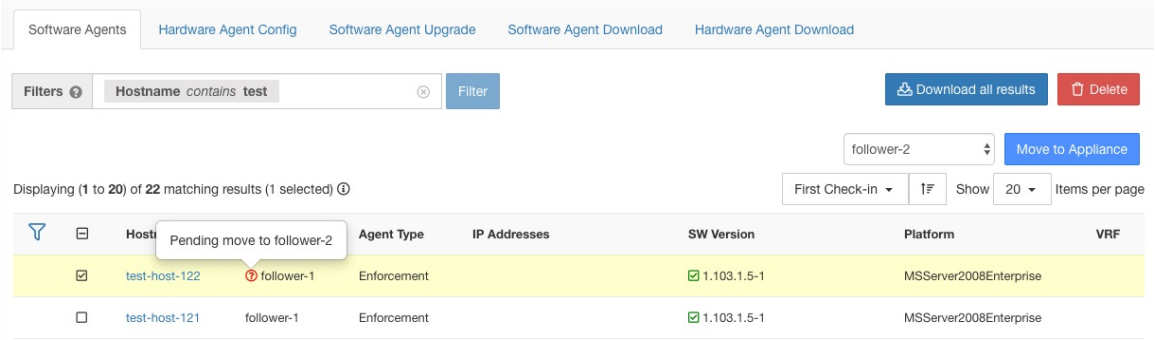
步骤 2 选择**代理配置 (Agent Config)**。将显示该页面。

步骤 3 点击**软件代理 (Software Agents)** 选项卡。系统将打开**软件代理 (Software Agents)** 选项卡。

步骤 4 查找要移动的一个或多个代理，然后点击在其表行中找到的复选框。

步骤 5 从**选择设备 (Select Appliance)** 下拉列表中，为这些代理选择所需的设备。

步骤 6 点击**移至设备 (Move to Appliance)** 按钮。



表会更新，以指明移动处于待处理状态。在代理下次签入时，就会收到移动设备的消息。移动完成后，原始设备上将不再显示代理。访问新的设备**软件代理 (Software Agents)** 页面，验证移动是否成功。

其他任务

通常，必须在**跟随者**设备上进行基于流和资产的查询。下表指明了一些常见任务的设备类型。

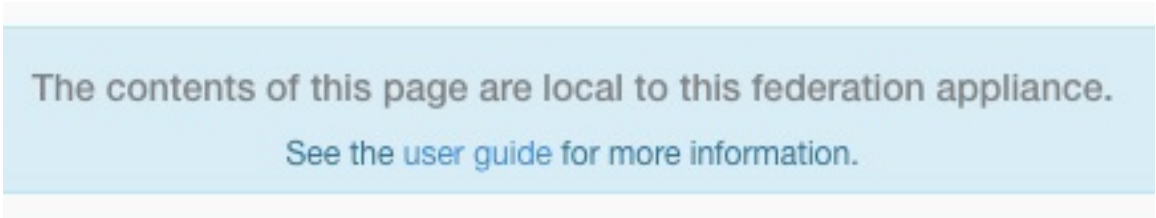
表 *10:* 常见任务的联合设备类型

任务	设备
可视性 (Visibility) > > **流搜索 (Flow Search)**	跟随者
可视性 (Visibility) > **资产搜索 (Inventory Search)**	跟随者
可视性 (Visibility) > **资产过滤器 (Inventory Filters)**	跟随者
可视性 (Visibility) > **外部协调器 (External Orchestrators)**	跟随者
分段 (Segmentation) > **自动策略发现 (Automatic Policy Discovery)**	领导者
分段 (Segmentation) > **策略分析 (Policy Analysis)**	领导者
分段 (Segmentation) > **执行历史记录 (Enforcement History)**	领导者
分段 (Segmentation) > **对话 (Conversations)**	跟随者
分段 (Segmentation) > **分析结果 (Analysis Results)**	跟随者
分段 (Segmentation) > **执行结果 (Enforcement Results)**	跟随者
监控 (Monitoring) > **代理 (Agents)**	跟随者

任务	设备
监控 (Monitoring) > **执行状态 (Enforcement Status)**	跟随者
监控 (Monitoring) > **许可证 (Licenses)**	跟随者
软件代理 (Software Agents) > **更改设备 (Change Appliances)**	跟随者

以上未包括的任何其他任务应被视为设备的本地任务。因此，所做的任何更改或显示的结果都只代表当前设备的状态，而不代表联合的状态。这些页面上将显示以下警报。

图 *35:* 本地设备警报



现有部署

以下各节提供了一套用于保存加入联合的设备数据的准则。

保留的数据

用户负责将用户、角色、收集规则、取证配置文件、用户上传的标签和代理配置从跟随者复制到领导者，然后再将其添加到联合。跟随者上未复制到领导者的数据将被擦除，并替换为领导者中的数据。

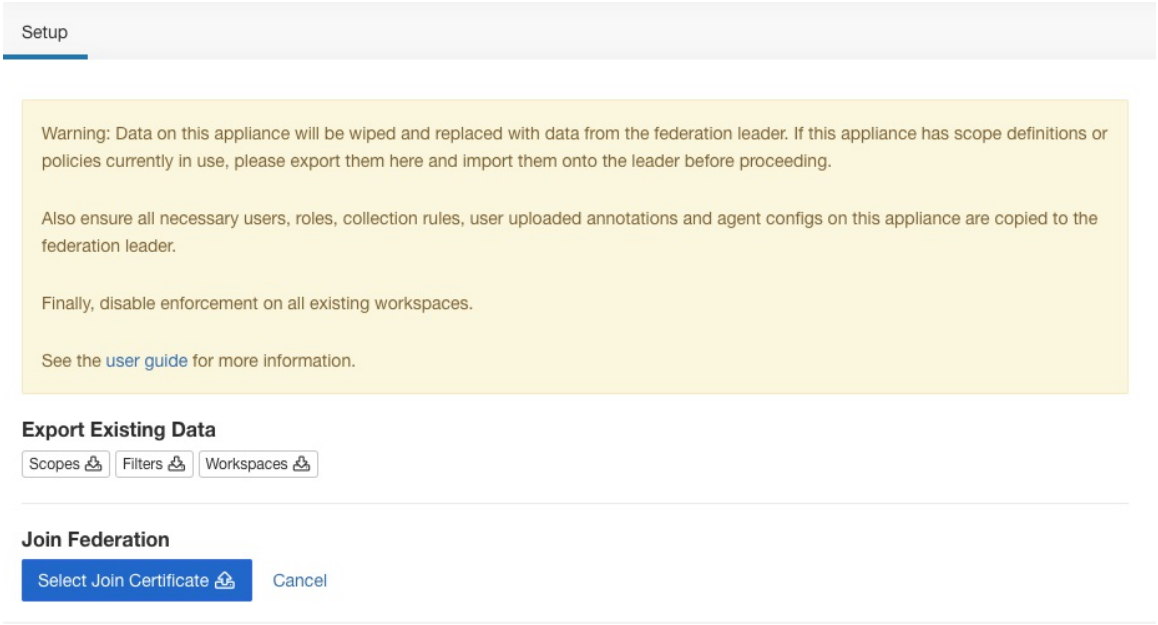
执行以下操作，通过将范围、过滤器和策略导出到随后可在 主设备上导入的文件，保留关注设备上的范围、过滤器和策略。执行以下操作，将**跟随者**的范围、过滤器和策略导出到文件中，然后导入到**领导者**中，以保存这些内容。

过程

步骤 1 在跟随者设备上，导航至**平台 (Platform)** > **联合 (Federation)**，然后点击**加入新联合 (Join New Federation)** 按钮。

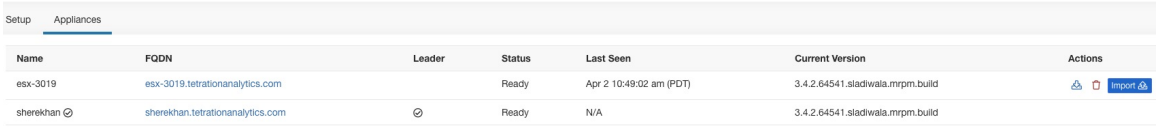
下载设备本地的范围、过滤器和工作空间。

图 *36:* 跟随者上的现有部署导出工作流程



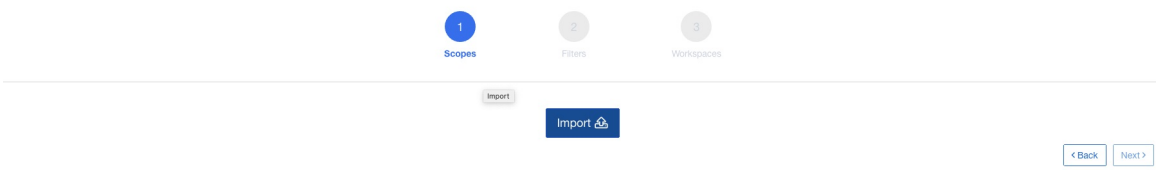
步骤 2 在**领导者**上，导航至**平台 (Platform)** > **联合 (Federation)**。通过输入跟随者的名称和完全限定域名 (FQDN) 并点击**添加 (Add)** 按钮来添加跟随者。然后切换到设备视图，并点击设备 FQDN 右侧的**导入 (Import)** 按钮。

图 *37:* 跟随者上的现有部署导入图标



您可以上传从跟随者下载的范围、过滤器和工作空间。在每个阶段解决所有冲突，然后再继续下一阶段。

图 *38:* 跟随者上的现有部署导入向导



通过比较两台设备上的条目名称，可检测出领导者和跟随者条目之间的冲突。例如，请考虑在领导者和跟随者上都存在的范围 **Default:host**。在领导者上，此范围的查询设置为 **Hostname eq foo**，在跟随者上，此范围的查询为 **Hostname eq bar**。导入向导会警告用户此范围存在冲突，并从领导者选择查询（即 **Hostname eq foo**）。

步骤 3 最后，您必须在跟随者上的所有现有工作空间上禁用执行，然后才能将其添加到联合。

步骤 4 必须对每个加入联合的跟随者重复步骤 1-3。

未保留数据

1. 虚拟设备（包括与连接器一起使用的设备）在加入联合后必须在跟随者上重新调配。
2. 对于与领导者通用的范围，无法访问跟随者加入联合时之前的流数据。

断开连接的操作模式

注释 适用于跟随者。

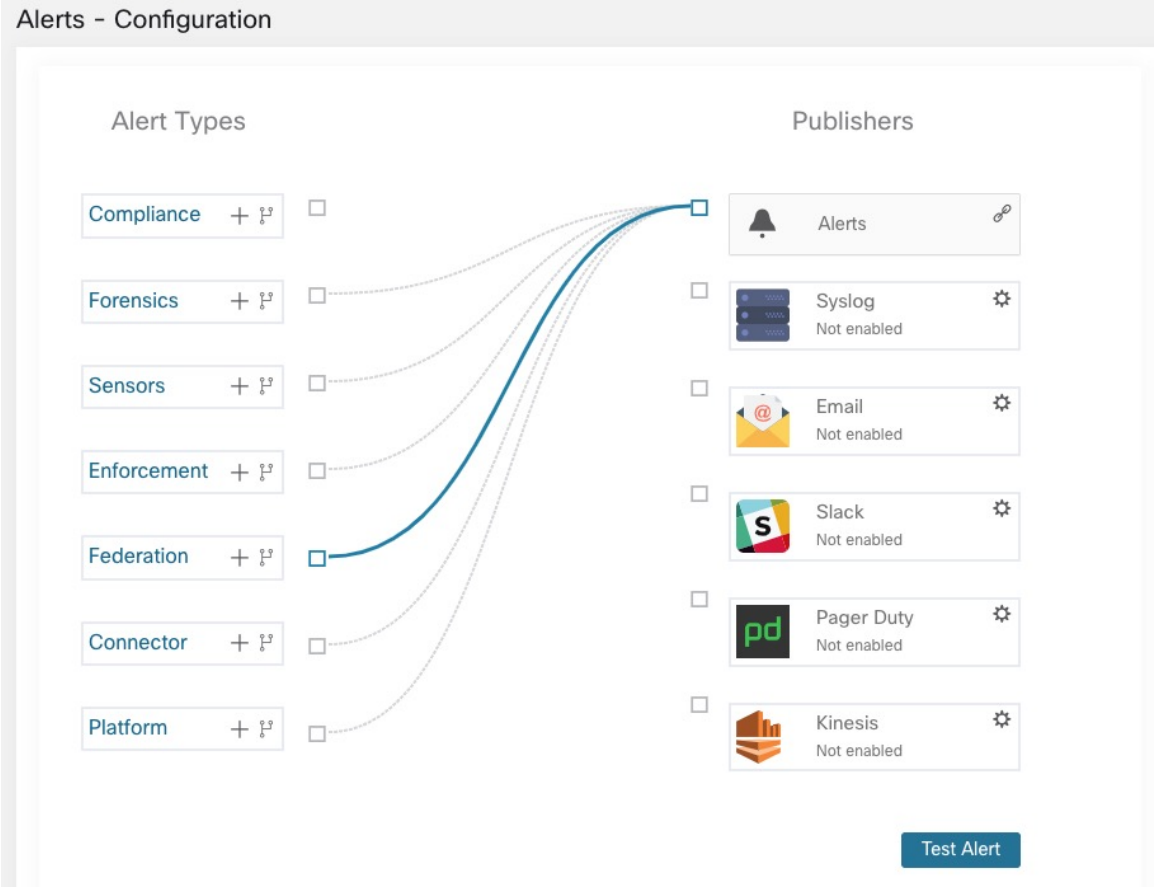
在某些情况下（例如网络分区），有必要在一个或多个**跟随者**上禁用联合，以允许它们在独立模式下运行。要执行此操作，请导航至**平台 (Platform)** > **联合 (Federation)** ，然后点击**禁用 (Disable)** 按钮。从联合断开连接的跟随者将继续作为独立集群运行。

可以通过将跟随者上的新范围、资产过滤器和工作空间导出到文件来保留这些文件，然后在领导者上导入这些文件，然后再将其添加回联合。这样会保留对现有工作空间的策略所做的更改。但是，当跟随者重新加入联合时，对领导者上已存在的范围和资产过滤器所做的更改将会丢失。

配置告警

要启用警报，请从导航窗格中选择**管理 (Manage)** > **工作负载 (Workloads)** > **警报配置 (Alert Configs)**。更新联合的警报配置。

图 *39:* 联合警报



您可以为以下事件生成警报：

- 当联合中的一个或多台设备在超过 10 分钟内未与领导者通信时，则会在严重性为 MEDIUM 的领导者上生成警报。
- 当跟随者无法联系领导者的时间超过 10 分钟时，则会在跟随者上生成严重性为 MEDIUM 的警报。

警报详细信息

有关一般警报结构和有关字段的信息，请参阅常见警报结构。*alert_details* 字段是结构化的，包含用于联合警报的以下子字段

注释 设备是触发警报的设备。

表 *11:* 联合警报详细信息

字段	警报类型	格式	说明
id	全部	字符串	设备 ID
name	全部	字符串	设备名称
fqdn	全部	字符串	设备的 FQDN
is_leader	全部	布尔值	如果设备是领导者，则为 true
status	全部	字符串	设备的状态
current_sw_version	全部	字符串	设备上的软件版本
last_seen_at	全部	整数	设备最后一次出现时的 Unix 时间戳
created_at	全部	整数	创建设备时的 Unix 时间戳
updated_at	全部	整数	更新设备时的 Unix 时间戳
created_at	全部	整数	创建设备时的 Unix 时间戳
deleted_at	全部	整数	删除设备时的 Unix 时间戳
disconnected	全部	布尔值	当跟随者与领导者断开连接时，设置为 true。对于领导者，始终设置为 false

跟随者关闭警报的 **alert_details** 示例

```
{
  "id": "5f219ad8755f024b46c2524a",
  "name": "esx-3018",
  "fqdn": "esx-3018.tetrationanalytics.com",
  "is_leader": false,
  "status": "Ready",
  "current_sw_version": "3.4.0.39.devel",
  "last_seen_at": 1596140582,
  "created_at": 1596037848,
  "updated_at": 1596140582,
  "deleted_at": 0,
  "disconnected": true
}
```

领导者关闭警报的 **alert_details** 示例

```
{
  "id": "5f219acc755f024b46c25248",
  "name": "sherekhan",
  "fqdn": "sherekhan.tetrationanalytics.com",
  "is_leader": true,
  "status": "Ready",
  "current_sw_version": "3.4.0.39.devel",
  "last_seen_at": 1596140582,
  "created_at": 1596037848,
  "updated_at": 1596140582,
  "deleted_at": 0,
  "disconnected": false
}
```


API

注释 必须在领导者上生成联合集群的凭证，并可用于查询跟随者。

本节列出了为联合添加或更新的 API：

设备

设备终端允许用户检索联合中设备的状态。

设备对象

设备对象的属性如下表所述：

属性	类型	说明
id	字符串	设备的唯一标识符。
name	字符串	用户指定的设备名称。
fqdn	字符串	用户指定的设备 FQDN。
is_leader	布尔值	指明设备是否为领导者。
status	字符串	设备的状态。
current_sw_version	字符串	设备上的 Cisco Secure Workload 软件版本。
last_seen_at	整数	领导者最后一次看到跟随者时的 Unix 时间戳。领导者的值始终为 null。
deleted_at	整数	删除设备时的 Unix 时间戳。

属性	类型	说明
disconnected	布尔值	指明跟随者是否与领导者失去联系。对于领导者，它设置为 false。

列出设备

此终端会返回联合中的设备数组。

```
GET /openapi/v1/appliances
```

参数：无

响应对象：返回设备对象数组。

示例 python 代码

```
restclient.get('/appliances')
```

范围

范围对象 现在包括与范围关联的设备的 ID。对于全局范围，它会被设置为 null。

现在，以下 API 会在创建或更新范围时接受设备 ID。

创建范围

创建范围时提供的设备 ID 会将其与特定设备关联。

```
POST /openapi/v1/app_scopes
```

参数：

名称	类型	说明
short_name	字符串	用户指定的范围名称。
description	字符串	用户指定的范围说明。
short_query	JSON	与范围关联的过滤器（或匹配条件）。
parent_app_scope_id	字符串	父范围的 ID。
policy_priority	整数	默认值为“last”。用于对工作空间优先级进行排序。请参阅审核自动发现的策略下的“策略排序”。
appliance_id	字符串	设备的唯一标识符。

示例 python 代码

```
req_payload = {
    "short_name": "App Scope Name",
    "short_query": {
        "type":"eq",
        "field":"ip",
        "value": <....>
    },
    "parent_app_scope_id": <parent_app_scope_id>,
    "appliance_id": <appliance_id>,
}
resp = restclient.post('/app_scopes', json_body=json.dumps(req_payload))
```

更新范围

此 API 允许使用设备 ID 将现有范围与设备相关联。

```
PUT /openapi/v1/app_scopes/{app_scope_id}
```

参数：

名称	类型	说明
short_name	字符串	用户指定的范围名称。
description	字符串	用户指定的范围说明。
short_query	JSON	与范围关联的过滤器（或匹配条件）。
appliance_id	字符串	设备的唯一标识符。

返回与指定 ID 关联的已修改的范围对象。

示例 python 代码

```
req_payload = {
    "short_name": "App Scope Name",
    "short_query": {
        "type":"eq",
        "field":"ip",
        "value": <....>
    },
    "appliance_id": <appliance_id>,
}
resp = restclient.put('/app_scopes/%s' % <app_scope_id>,
                      json_body=json.dumps(req_payload))
```

空闲会话

对于使用本地数据库进行身份验证的用户，本部分介绍失败的登录尝试如何锁定用户帐户：

Procedure

步骤 1 使用邮箱和密码进行五次失败的登录尝试会导致帐户被锁定。

Note 作为一项防止探测的安全措施，当尝试登录被锁定的帐户时，登录界面上将不会显示具体的锁定信息。

步骤 2 锁定间隔设置为 30 分钟。帐户解锁后，使用正确的密码登录或点击忘记密码？*(Forgot password?)*。

Note 用户成功登录后，如果一小时内处于非活动状态，用户会被注销。此超时可在**管理 (Manage)** > **服务设置 (Service Settings)** > **会话配置 (Session Configuration)** 中进行配置。

偏好设置

首选项 (Preferences) 页面将显示您的帐户详细信息，使您能够更新显示首选项、更改登录页面、更改密码以及配置双因素身份验证。

更改登录页面首选项

要更改登录时看到的页面，请执行以下操作：

Procedure

步骤 1 在窗口的右上角，点击用户图标，然后选择**用户首选项 (User Preferences)**。

步骤 2 从下拉菜单中选择登录页面。登录时，您的首选项将保存为默认页面或主页。要查看更改，请点击页面左上角的 Cisco Secure Workload 徽标。

更改密码

Procedure

步骤 1 点击右上角的用户图标。

步骤 2 选择**用户首选项 (User Preferences)**。

步骤 3 在**更改密码 (Change Password)** 窗格中的**旧密码 (Old Password)** 字段中输入当前密码。

步骤 4 在**密码 (Password)** 字段中输入新密码。

步骤 5 在**确认密码 (Confirm Password)** 字段中再次输入新密码。

步骤 6 点击**更改密码 (Change Password)** 以提交更改。

Note 密码必须为 8-128 个字符，并至少包含以下各项之一：

- 小写字母 (a b c d . . .)
- 大写字母 (A B C D . . .)
- 数字 (0 1 2 3 4 5 6 7 8 9)
- 特殊字符 (! " # $ % & ’ ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ‘ { | } ~)，包含空格

恢复密码

本部分介绍在您忘记密码时如何重置密码。

Before you begin

要重置密码，您必须先拥有一个帐户。只有**站点管理员**有权创建新帐户。

Procedure

步骤 1 将浏览器指向思科 Cisco Secure Workload URL，然后点击**忘记密码 (Forgot Password)** 链接。系统将显示**忘记密码？(Forgot your password?)** 对话框。

步骤 2 输入必须将密码发送到的邮箱 ID。

步骤 3 点击**重置密码 (Reset Password)**。

密码重置说明将被发送到您的邮箱。

Note 使用双因素身份验证找回密码时，需要联系网站管理员获取一次性的临时密码。

重置密码

本部分介绍如何为没有邮箱 ID 的用户重置密码。

Procedure

步骤 1 以**站点管理员**身份登录 Cisco Secure Workload，然后从导航窗格中选择**管理 (Manage)** > **用户访问 (User Access)** > **用户 (Users)**。

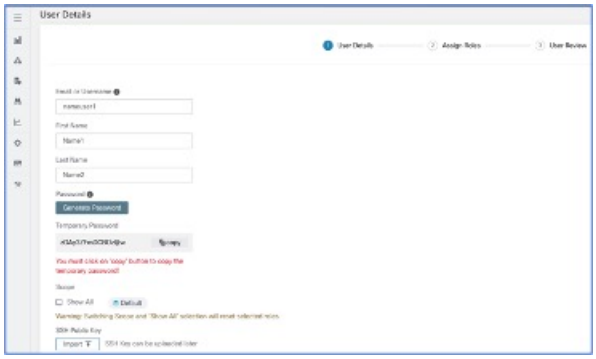
步骤 2 在**操作 (Actions)** 列下，点击**铅笔**图标。此时将显示**用户详细信息 (User Details)** 页面。

Table 12: 用户新消息字段说明

字段	说明
电子邮箱或用户名 (Email or Username)	输入用户的用户名；用户名不区分大小写，但不能包含 @ 或空格。 **Note** 作为**站点管理员**，您可以使用 用户名为要恢复临时密码的用户生成临时密码。 用户名的最大长度不能超过 255 个字符。
名字 (First Name)	输入用户的名字。
姓氏 (Last Name)	输入用户的姓氏。
范围 (Scope)	为多租户分配给用户的根范围。（可供站点管理员使用）
SSH 公钥 (SSH Public Key)	（可选）点击**导入 (Import)** 以导入 SSH 公钥，也可以稍后导入密钥。

步骤 3 点击**生成密码 (Generate Password)** 以生成一个临时密码。复制密码并与请求密码的用户共享。

Figure 40:



Note 用户可以使用用户名和临时密码登录并重置密码。

启用双因素身份验证

本部分介绍如何启用双因素身份验证。

Procedure

步骤 1 点击用户图标。

步骤 2 选择**用户首选项 (User Preferences)**。

步骤 3 点击**双因素身份验证 (Two-Factor Authentication)** 窗格中的**启用 (Enable)** 按钮。系统将显示新的**双因素身份验证 (Two-Factor Authentication)** 页面。

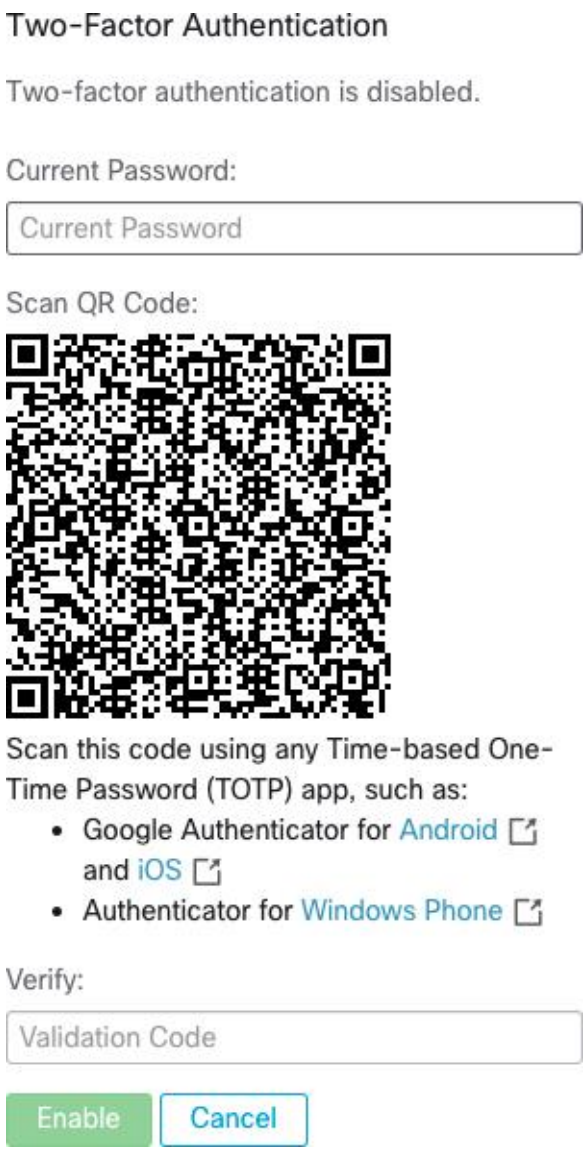
步骤 4 输入您的密码。

步骤 5 使用基于时间的一次性密码 (TOTP) 应用（如 Google Authenticator Android 或 iOS 版或 Authenticator Windows Phone 版）扫描**当前密码 (Current Password)** 字段下显示的二维码。

步骤 6 输入您选择的 TOTP 应用显示的验证码。

步骤 7 点击**启用 (Enable)**。

Figure 41: *“双因素身份验证”(Two-Factor Authentication)* **窗格**



登录系统并输入 TOTP 应用中显示的验证码进行登录时，选中**使用双因素身份验证 (Use two-factor authentication)** 复选框。

Note 如果您需要为双因素身份验证恢复密码，请联系**站点管理员**或 Cisco Secure Workload 客户支持。

禁用双因素身份验证

本部分介绍如何禁用双因素身份验证。

Procedure

步骤 1 点击右上角的用户图标。

步骤 2 选择**用户首选项 (User Preferences)**。

步骤 3 在双因素身份验证下，点击**禁用 (Disable)** 按钮。系统将显示**双因素身份验证 (Two-Factor Authentication)** 窗格。

步骤 4 输入您的密码。

步骤 5 再次点击**禁用 (Disable)** 按钮。

您不再需要在登录过程中输入双因素验证码。

范围

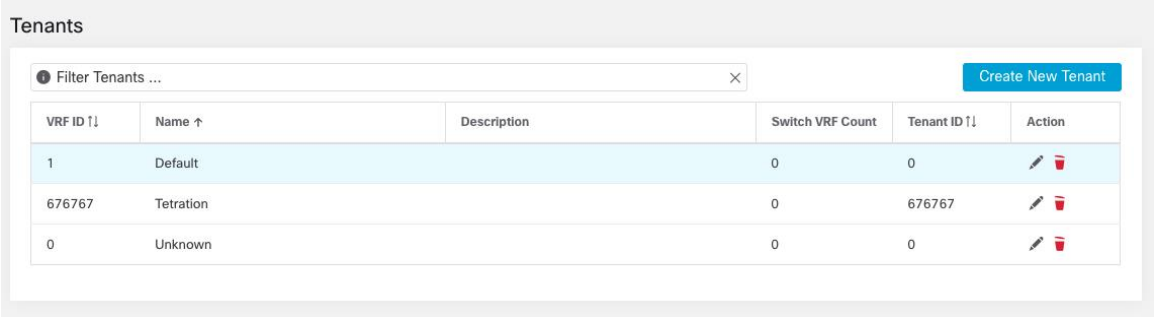
Note **范围 (Scopes)** 页面与**资产搜索 (Inventory Search)** 合并。有关详细信息，请参阅范围和资产页面。

租户

站点管理员和**客户支持用户**可以从导航窗格访问 **平台 (Platform)** > **租户 (Tenants)** 菜单下的**租户 (Tenants)** 页面。“租户”(Tenants) 页面将显示当前配置的租户和 VRF。Cisco Secure Workload 预配置了一个或多个租户和 VRF，您可以添加、编辑和删除租户。

Note 这些值会影响集群输出的结果。建议在更改这些值之前咨询思科 TAC，以了解系统影响。

Figure 42: “租户” *(Tenants)* 页面



添加租户

Before you begin

您必须是站点管理员或客户支持用户。

Procedure

步骤 1 在左侧导航窗格中，点击平台 (Platform) > 租户 (Tenants)。

步骤 2 点击创建新租户 (Create New Tenant)。

步骤 3 在以下字段中输入适当的值：

字段	说明
名称	为租户输入所需的名称。
说明	（可选）说明字段包含有关租户的其他信息。

步骤 4 点击创建 (Create)。

编辑租户

Before you begin

您必须是站点管理员或客户支持用户。

Procedure

步骤 1 在左侧导航窗格中，点击平台 (Platform) > 租户 (Tenants)。

步骤 2 找到要编辑的租户，然后点击右侧列中的铅笔图标。

字段	说明
名称	更新租户的名称。
说明	（可选）更新说明字段包含有关租户的其他信息。
VRF ID	显示此特定租户或 VRF 的 ID。
更改日志	点击更改日志图标将显示一个新页面，其中显示租户或VRF的更改日志。

步骤 3 点击**更新 (Update)**。

用户

要访问**用户 (Users)** 页面，站点管理员从导航窗格中选择管理用户访问（**管理 (Manage)** > **用户访问 (User Access)**）。

用户 (Users) 页面显示运营商用户以及与页面标题范围关联的用户。

运营商用户没有范围；系统会为用户分配允许他们跨根范围执行操作的角色。

添加用户

Before you begin

- 您必须是**站点管理员**才能在 Cisco Secure Workload 中添加用户。
- 如果为用户分配了多租户范围，则只能选择分配给同一范围的角色。
- 要恢复用户的密码，拥有邮件帐户的**站点管理员**可以使用用户的用户名生成随机密码来恢复密码。

Note 此页面会按在页眉上选择的范围首选项进行过滤。

Procedure

步骤 1 如果适用，请从页眉中选择相应的根范围。

步骤 2 从导航窗格中，选择管理用户访问用户（**管理 (Manage)** > **用户访问权限 (User Access)** > **用户 (Users)**）。

步骤 3 点击**创建用户 (Create User)**。
此时将显示**用户详细信息 (User Details)** 页面。

步骤 4 更新用户详细信息 **(User Details)** 下的以下字段。

Table 13: 用户新消息字段说明

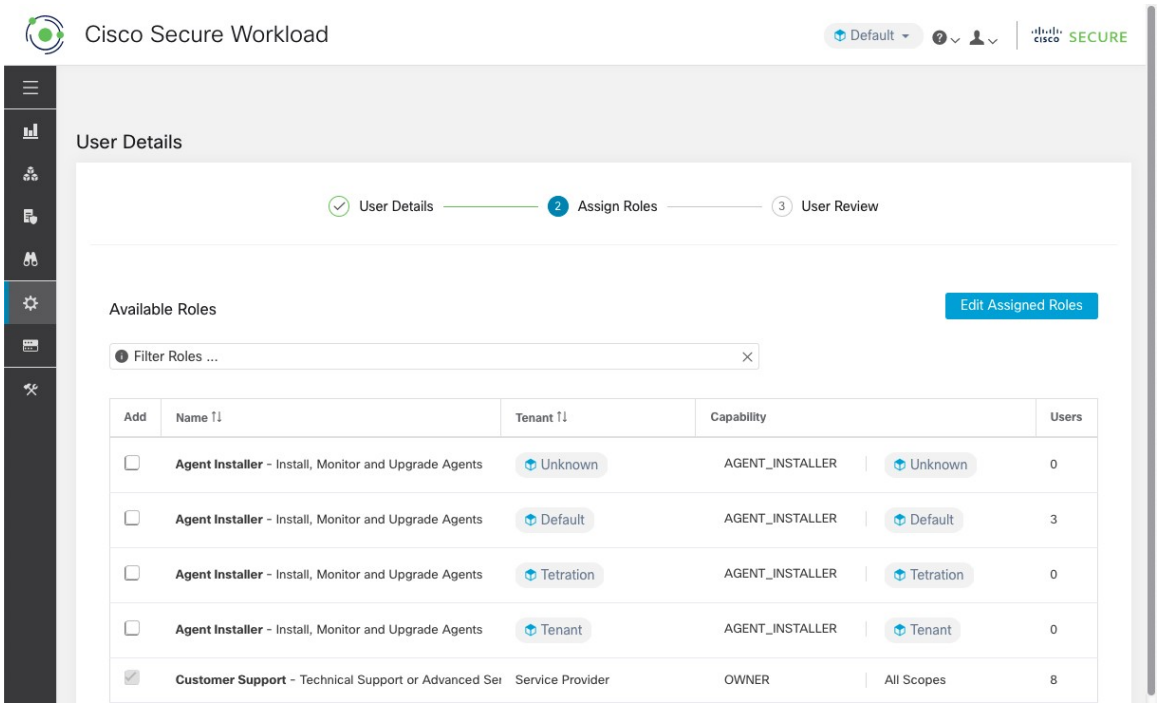
字段	说明
电子邮箱或用户名	输入用户的邮件ID。邮件地址不区分大小写。如果您的邮件包含字母，则会使用字母的小写版本。 输入用户的用户名；用户名不区分大小写，并且不能包含 @ 或空格。
名字	输入用户的名字。
姓氏	输入用户的姓氏。
范围	为多租户分配给用户的根范围。（可供**站点管理员**使用）
SSH 公钥	（可选）点击**导入 (Import)** 以导入 SSH 公钥，也可以稍后导入密钥。

步骤 5 点击**下一步 (Next)**。

步骤 6 在**分配角色 (Assign Roles)** 下，向用户添加或删除分配的角色。

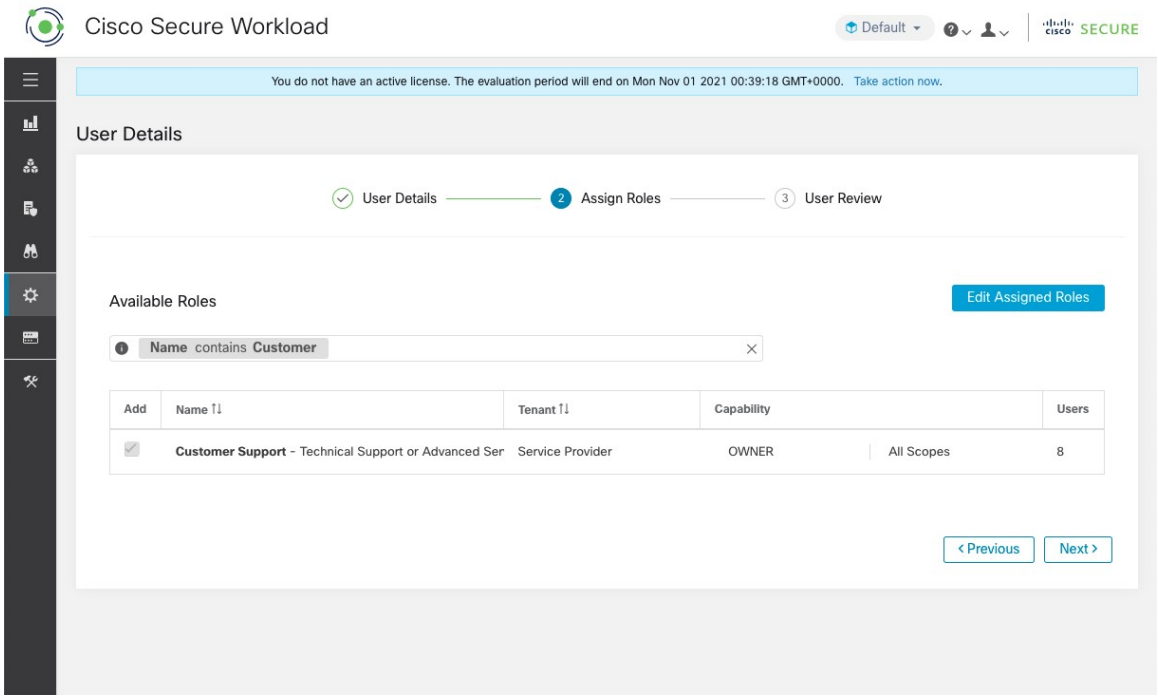
- 点击**添加角色 (Add Roles)** 以分配新角色，然后点击**添加 (Add)** 复选框。

Figure 43: 分配的用户角色



- 选择分配的角色，点击**编辑分配的角色 (Edit Assigned Roles)**，然后点击**删除 (Remove)** 图标。
- 您可以使用**名称**或**租户**来过滤用户角色。

Figure 44: 过滤用户角色



步骤 7 点击**下一步 (Next)**。

步骤 8 在**用户查看 (User Review)** 下，查看用户详细信息和分配的角色。点击**创建 (Create)**。

如果启用了外部身份验证，则会显示身份验证详细信息。

在 Cisco Secure Workload 中添加用户后，系统会向注册的电子邮件 ID 发送激活电子邮件以设置密码。

Note 没有邮箱ID的用户可以使用**站点管理员**共享的用户名和临时密码登录。首次登录时，用户会被重定向以便设置其永久密码。

编辑用户详细信息或角色

Before you begin

您必须是**站点管理员** 才能编辑 Cisco Secure Workload 中的用户。

Note 此页面会按在页眉上选择的范围首选项进行过滤。

Procedure

步骤 1 如果适用，请从页眉中选择相应的根范围。

步骤 2 从导航窗格中，选择管理用户访问用户（**管理 (Manage)** > **用户访问权限 (User Access)** > **用户 (Users)**）。

步骤 3 对于所需的用户帐户，在**操作 (Actions)** 下点击**编辑 (Edit)**。
此时将显示**用户详细信息 (User Details)** 页面。

步骤 4 编辑以下详细信息。

a) 更新**用户详细信息 (User Details)** 下的以下字段。

Table 14: 用户新消息字段说明

字段	说明
电子邮箱或用户名	更新用户的邮件ID。用户名不区分大小写，用户名中不能包含 @ 或空格。 **Note** 对于没有邮件 ID 的用户，**站点管理员**将使用用户的用户名。用户名的最大长度为 255 个字符。
名字	更新用户的名字。
姓氏	更新用户的姓氏。
范围	为多租户分配给用户的根范围。（可供**站点管理员**使用）

b) 点击**下一步 (Next)**。

c) 在**分配角色 (Assign Roles)** 下，向用户添加或删除分配的角色。

- 点击**添加角色 (Add Roles)** 以分配新角色，然后点击**添加 (Add)** 复选框。
- 选择分配的角色，点击**编辑分配的角色 (Edit Assigned Roles)**，然后点击**删除 (Remove)** 图标。

d) 点击**下一步 (Next)**。

e) 在**用户查看 (User Review)** 下，查看用户详细信息和分配的角色。点击**更新 (Update)** 以更新用户帐户。

如果启用了外部身份验证，则会显示身份验证详细信息。

停用用户帐户

Note 为了保持变更日志审计的一致性，只能停用用户，而不能从数据库中删除用户。

Before you begin

您必须是**站点管理员**或**根范围所有者**用户。

Note 此页面会按在页眉上选择的范围首选项进行过滤。

Procedure

步骤 1 在左侧的导航栏中，点击**管理 (Manage)** > **用户访问权限 (User Access)** > **用户 (Users)**。

步骤 2 如果适用，请从页面右上角选择相应的根范围。

步骤 3 在要停用的帐户行中，点击右列中的**停用 (Deactivate)** 按钮。

要查看已停用的用户，请切换**隐藏已删除的用户 (Hide Deleted Users)** 按钮。

重新激活用户帐户

如果用户已被停用，您可以重新激活该用户。

Before you begin

您必须是**站点管理员**或**根范围所有者**用户。

Note 此页面会按在页眉上选择的范围首选项进行过滤。

Procedure

步骤 1 在左侧的导航栏中，点击**管理 (Manage)** > **用户访问权限 (User Access)** > **用户 (Users)**。

步骤 2 如果适用，请从页面右上角选择相应的根范围。

步骤 3 切换**隐藏已删除用户**以显示所有用户，包括已停用的用户。

步骤 4 对于所需的已停用帐户，请点击右列中的**恢复**以重新激活该帐户。

导入 SSH 公钥

要通过其中一个收集器 IP 地址以 **ta_guest** 用户身份启用 SSH 访问，则可以为每位用户导入 SSH 公钥。此菜单仅对**站点管理员**和在根范围具有 `SCOPE_OWNER` 功能的用户可用。SSH 公钥在 7 天后自动到期。

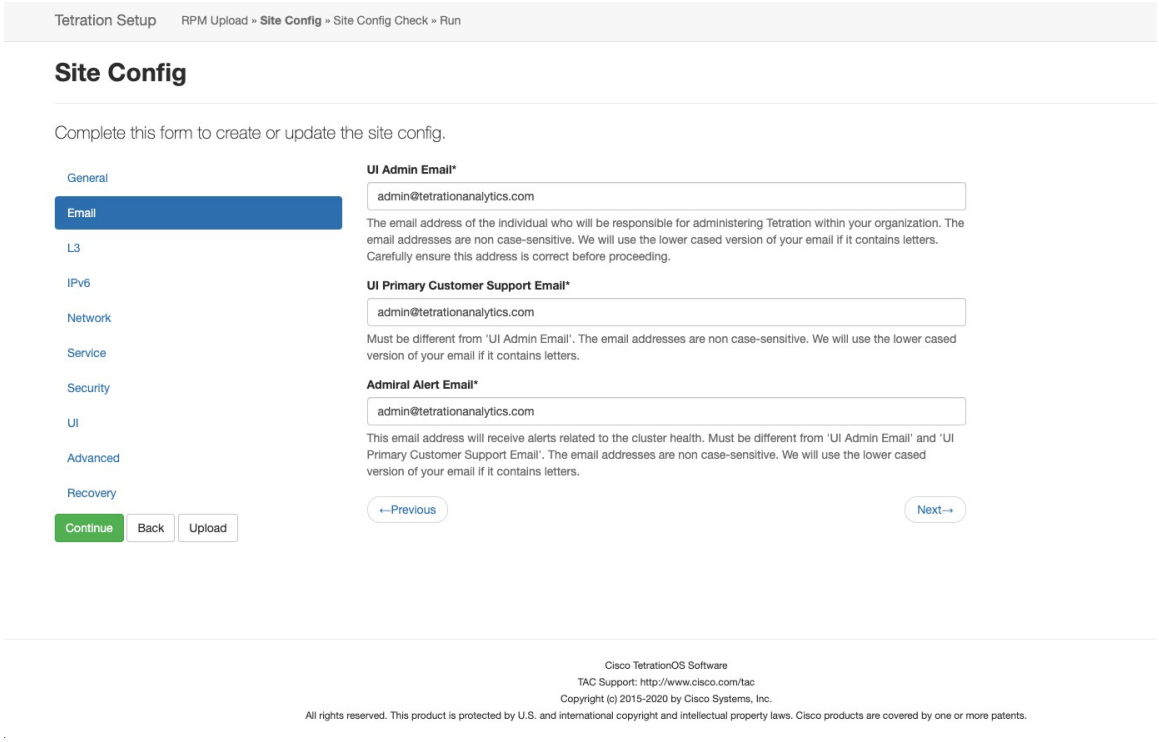
Cisco Secure Workload 设置中的站点配置

本部分介绍**站点管理员**如何在 Cisco Secure Workload 设置过程中设置站点。

字段	说明
UI 管理员邮件 (UI Admin Email)	在您的组织内负责管理 Cisco Secure Workload 的人员的邮件地址。
UI 主要客户支持邮件 (UI Primary Customer Support Email)	主要支持人员的邮件地址。必须与“UI 管理员邮件”(UI Admin Email) 不同。
Admiral 警报邮件 (Admiral Alert Email)	此邮件地址接收与集群运行状况相关的警报。必须与“UI 管理员邮件”(UI Admin Email) 和“UI 主要客户支持邮件”(UI Primary Customer Support Email) 不同。

邮箱地址不区分大小写。如果邮件包含字母，则会使用小写版本。

Figure 45: 配置 ***UI*** 管理员、主要客户支持和 ***Admiral*** 管理员警报邮件



变更日志 - 用户

站点管理员和在根范围上具有**范围所有者**能力的用户可以通过点击**操作 (Actions)** 列下的**更改日志 (Change Log)** 图标来查看每位用户的更改日志。

有关详细信息，请参阅变更日志。根范围所有者只能查看属于其范围的实体的变更日志条目。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。