安全邮件威胁防御：多重身份验证和访问控制

目录

简介

本文档介绍思科邮件威胁防御(ETD)提供的控制管理员对管理控制台的访问功能。

先决条件

要求

Cisco建议您了解以下主题，以便使用Duo配置ETD身份验证：

- Cisco ETD订用
- 访问思科安全云控制(SCC)
- 增强安全性的身份验证解决方案，在本例中为Cisco Duo。

使用的组件

本文档仅限于Email Treat Defense和Secure Cloud Control。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档重点介绍Cisco ETD如何利用Cisco SCC并与Cisco Duo集成，以提供安全身份验证和精细访问控制。

在基于云的现代解决方案中，访问控制是确保数据安全性、合规性和操作完整性的最重要组件之一

。未经授权的访问（尤其是管理员帐户）可能会导致严重的后果，例如系统受损、数据泄露和服务中断。

思科在其云产品组合中提供强大的安全功能，包括多因素身份验证(MFA)技术，该技术是Cisco ETD等服务不可或缺的一部分。MFA在传统密码之外添加了一个关键验证步骤，要求用户通过其他因素（例如移动应用批准、安全令牌或生物特征验证）进行身份验证。

为了简化和加强管理员身份验证流程，ETD利用Cisco SCC（一种集中式身份验证和策略管理服务）。

通过SCC，ETD可获得一系列广泛的安全功能，包括：

- 实施MFA以缓解凭证失窃风险。
- 与Cisco Duo、Microsoft Entra ID、Okta等第三方身份提供商集成，以支持灵活的身份验证工作流程和企业身份联合。
- 集中式策略管理，允许跨思科云服务使用一致的访问规则。

特别是Cisco Duo，它通过添加高级的基于策略的访问管理来扩展这些功能。使用SCC作为集成通道，ETD可以直接对管理员访问应用双手的精细控制，如源IP限制、设备运行状况检查和基于用户组的规则。

例如，组织可以定义仅允许从特定受信任网络范围进行访问的策略。在授权IP列表之外的任何连接尝试都可以自动阻止，如随附的图中所示。MFA和情景策略的这种组合可启用深度防御方法，确保即使凭证受到危害，攻击者仍然可以访问系统，除非他们也符合其他安全标准。

通过将Cisco ETD、Cisco SCC和Cisco Duo相结合，企业可以实施安全、可扩展且用户友好的访问控制模型，与行业最佳实践保持一致，同时加强对关键云服务的保护。

场景

ETD可以实施多种身份验证和访问控制方案，以保护管理访问：

1. 嵌入式MFA — 使用思科的内置MFA或集成Microsoft MFA。
2. Cisco SCC与Cisco Duo — 将Cisco SCC的集中式身份验证与Duo的高级MFA功能相结合。
3. 带有外部身份提供商（例如，Microsoft Entra ID）的Cisco SCC — 通过与企业身份解决方案集成来扩展身份验证策略。

本文档介绍场景2的配置步骤：采用Cisco Duo的Cisco SCC，但此过程可适用于其他技术。

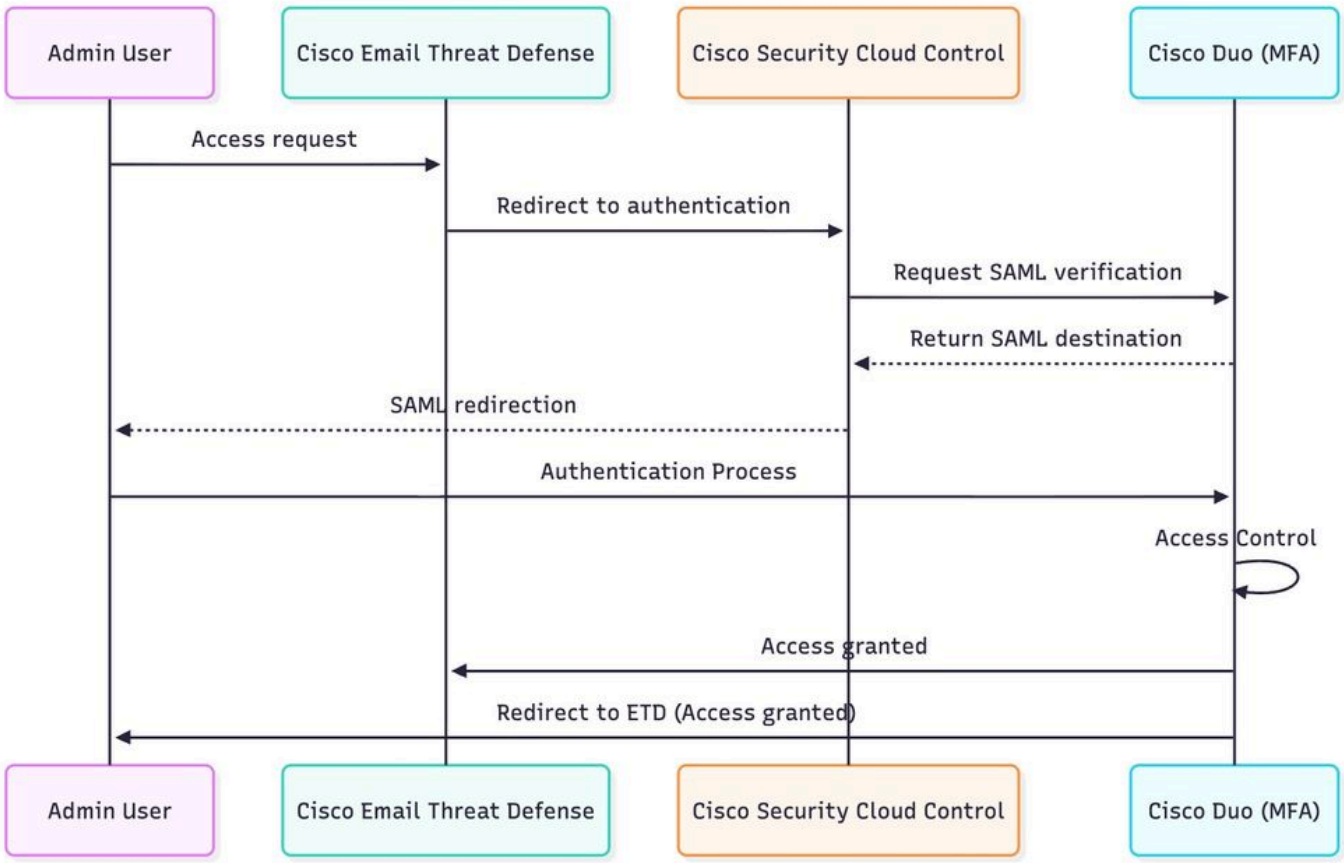
注意：本文档概述了在邮件威胁防御(ETD)中使用思科双核的多因素身份验证功能启用访问控制所需的基本步骤。实施Duo集成有助于增强安全性，因为这样可以确保只有授权用户才能访问该平台。有关综合指南、配置选项和高级部署方案，请参阅正式产品文档：

— 用于集中式安全策略和访问管理。

Cisco Duo -了解有关多因素身份验证设置和最佳实践的详细说明。

Cisco SCC配置

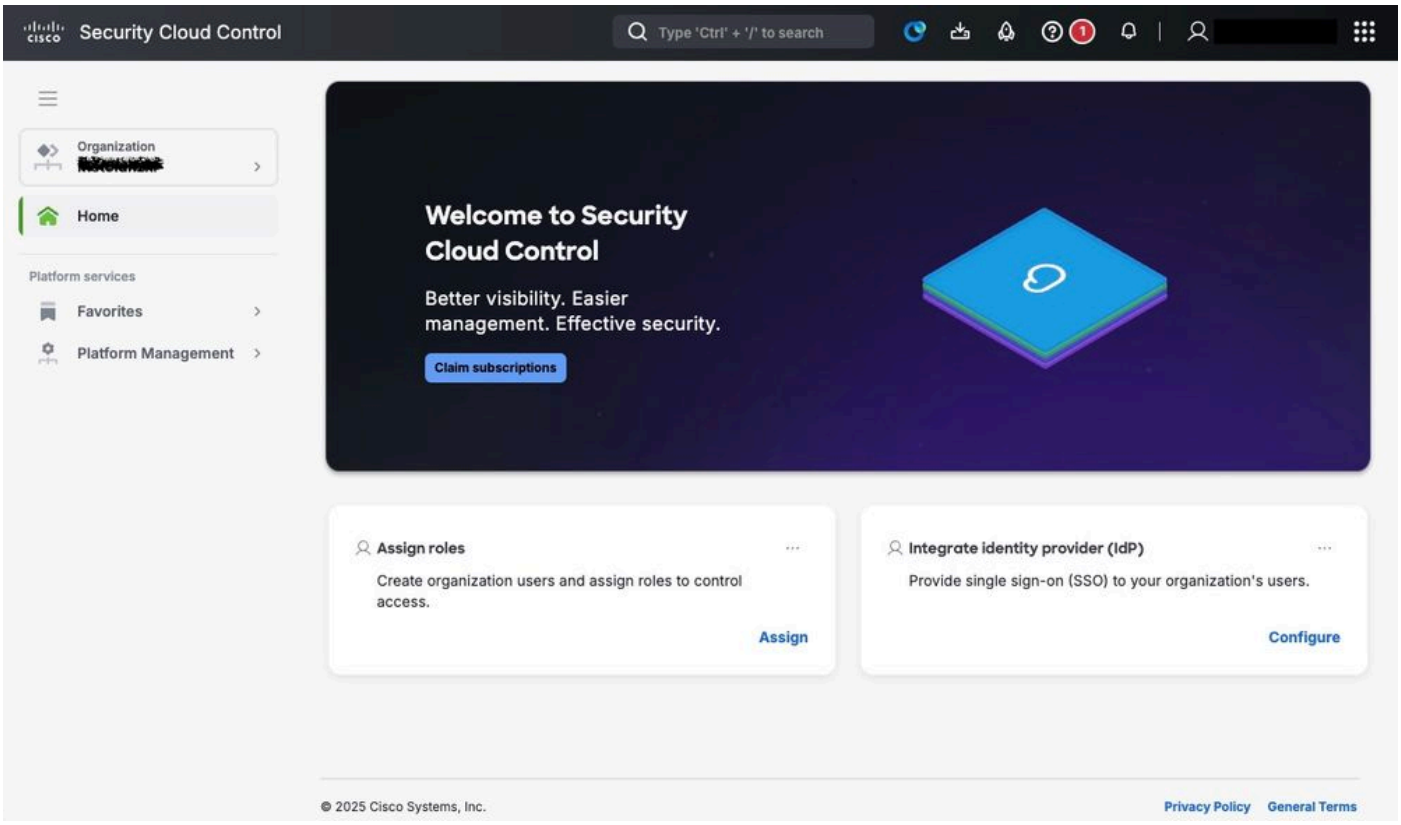
为了将Cisco ETD与Cisco Duo集成，第一步是在Cisco SCC中配置身份验证域。这样可以建立信任关系，使思科SCC能够与外部身份和MFA提供商合作。



图解

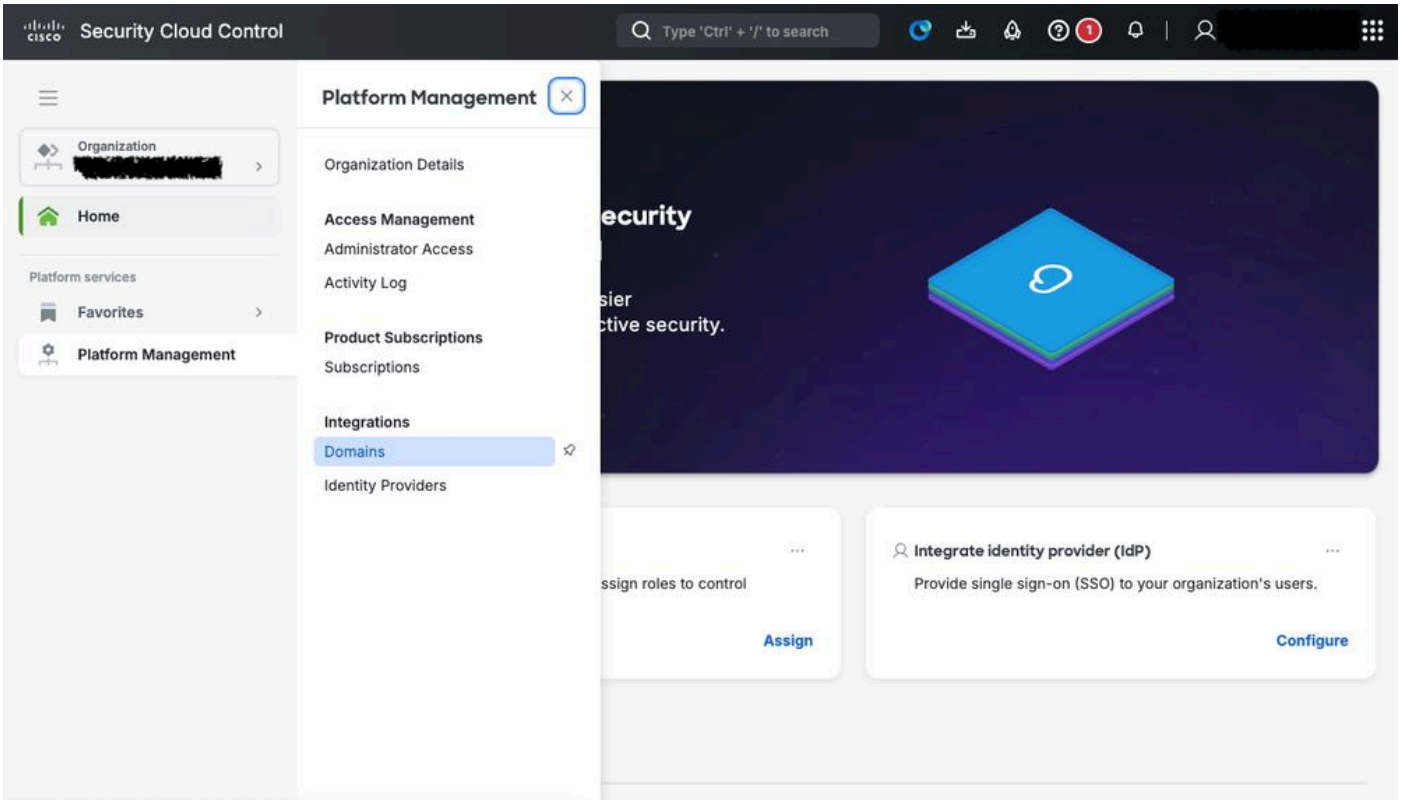
步骤1.访问Cisco SCC控制台。

登录到Cisco SCC门户https://security.cisco.com/。



步骤2.导航到域管理。

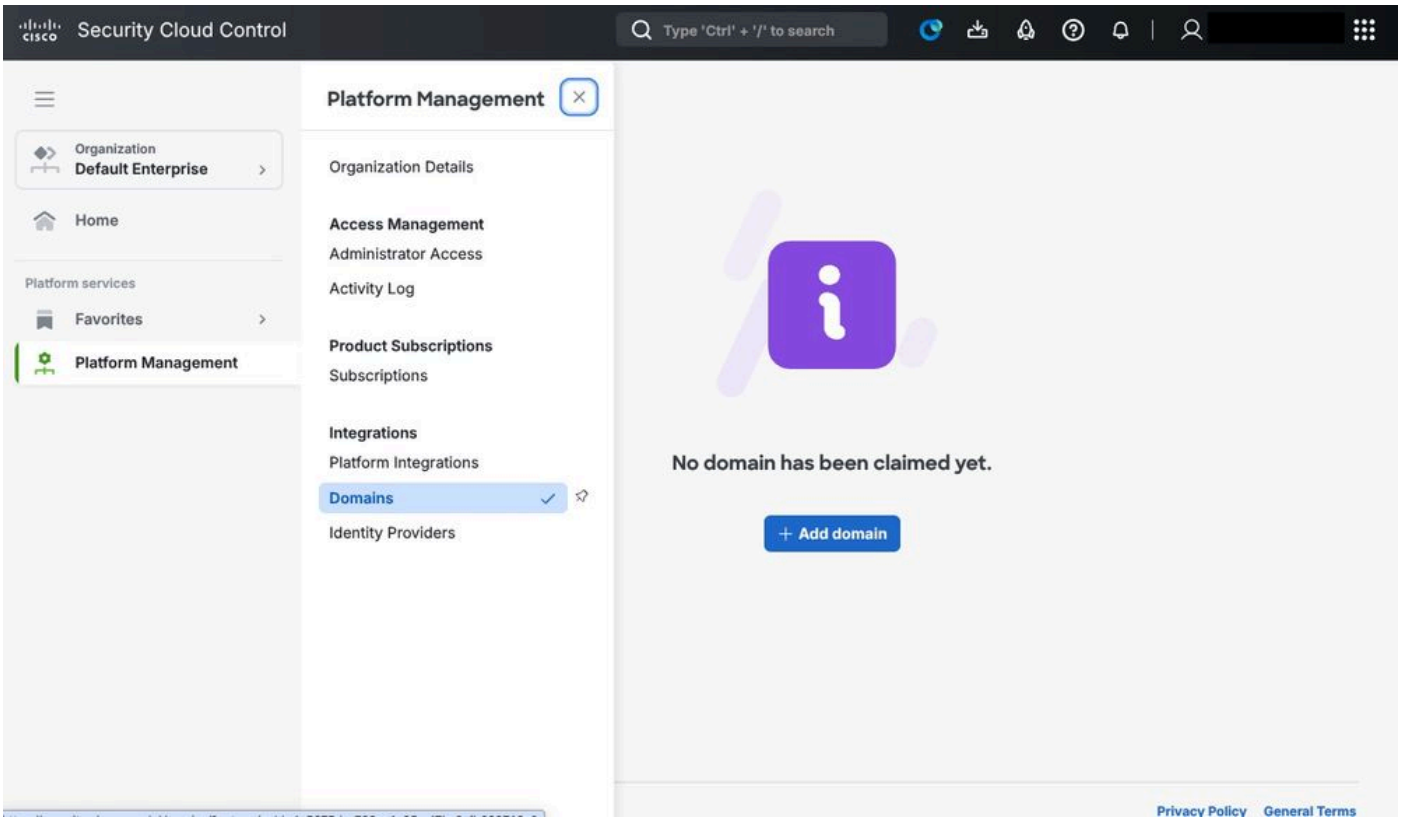
从主菜单中，导航到平台管理>域。



安全云控制域配置

步骤3.添加新域。

单击Add Domain开始注册身份验证域的过程。

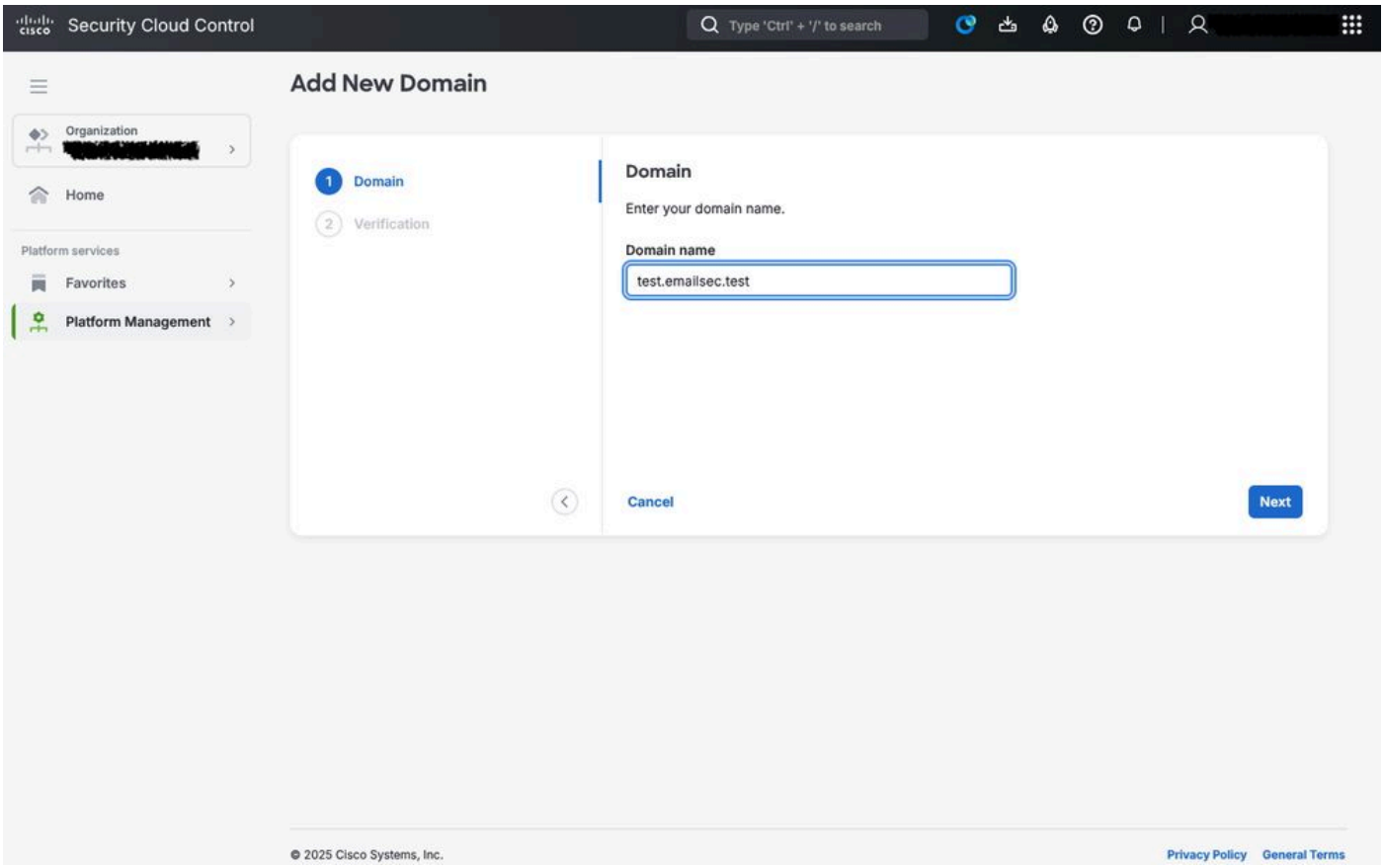


安全云控制：域

步骤4.提供域信息。

填写包含用于身份验证的域详细信息的表格。这通常包括：

- 域名(例如test.emailsec.test)
- 联系信息（管理和技术）
- 身份验证参数，取决于所选的身份提供程序

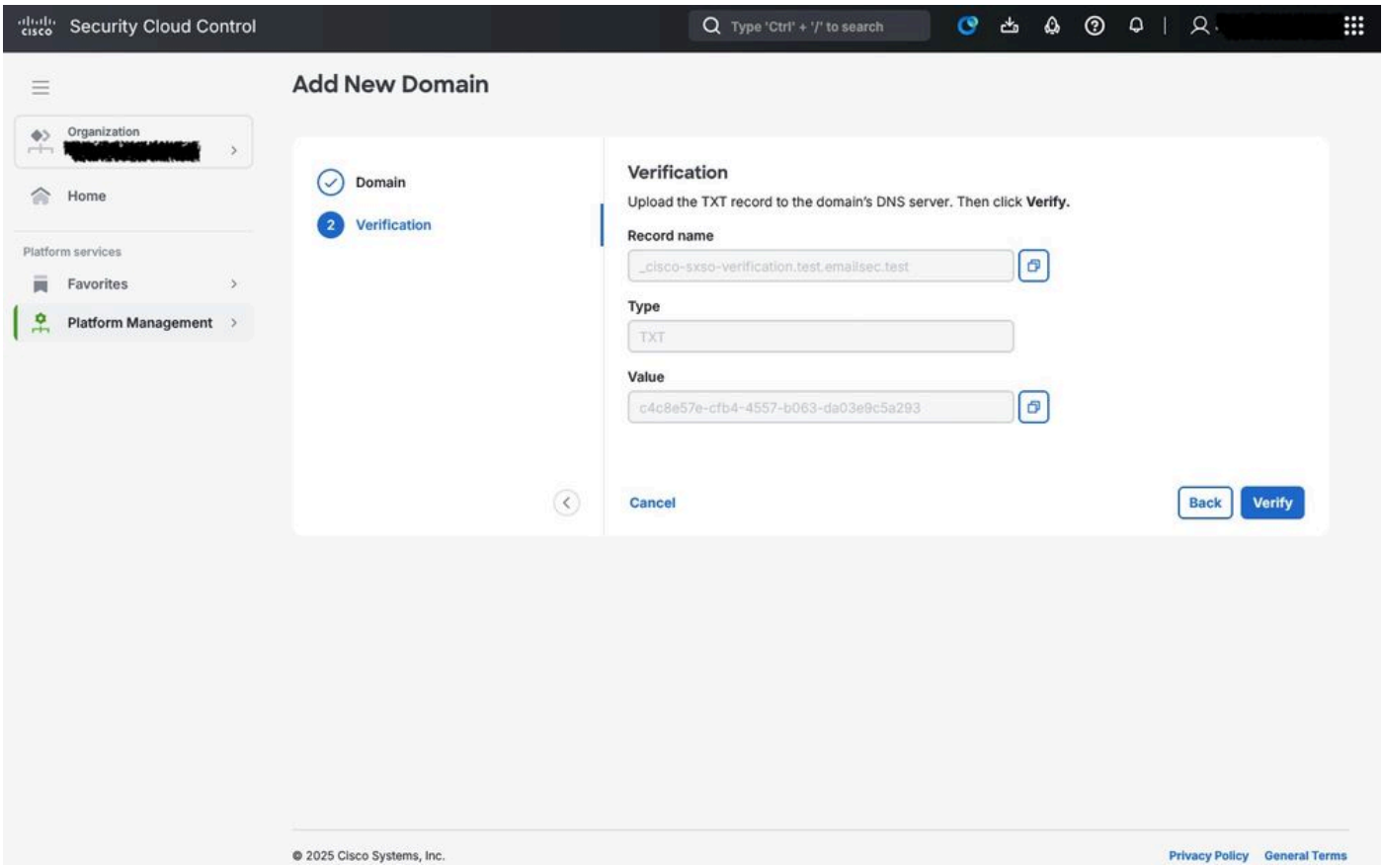


步骤5.通过DNS进行域验证。

注册域后，思科需要所有权证明。

- CSCC提供验证记录
- 此记录必须添加到域的DNS配置中（通常作为TXT记录）
- 思科安全云会自动验证DNS条目以确认该域属于您的组织

⚠ 警告：验证过程必须成功完成，才能继续集成。根据DNS传播，验证需要几分钟到几小时。



使用Cisco SCC将ETD与Cisco Duo连接

成功配置管理员的域（作为应用更严格的访问控制和管理权限的基础）后，下一步是集成约定的MFA服务。

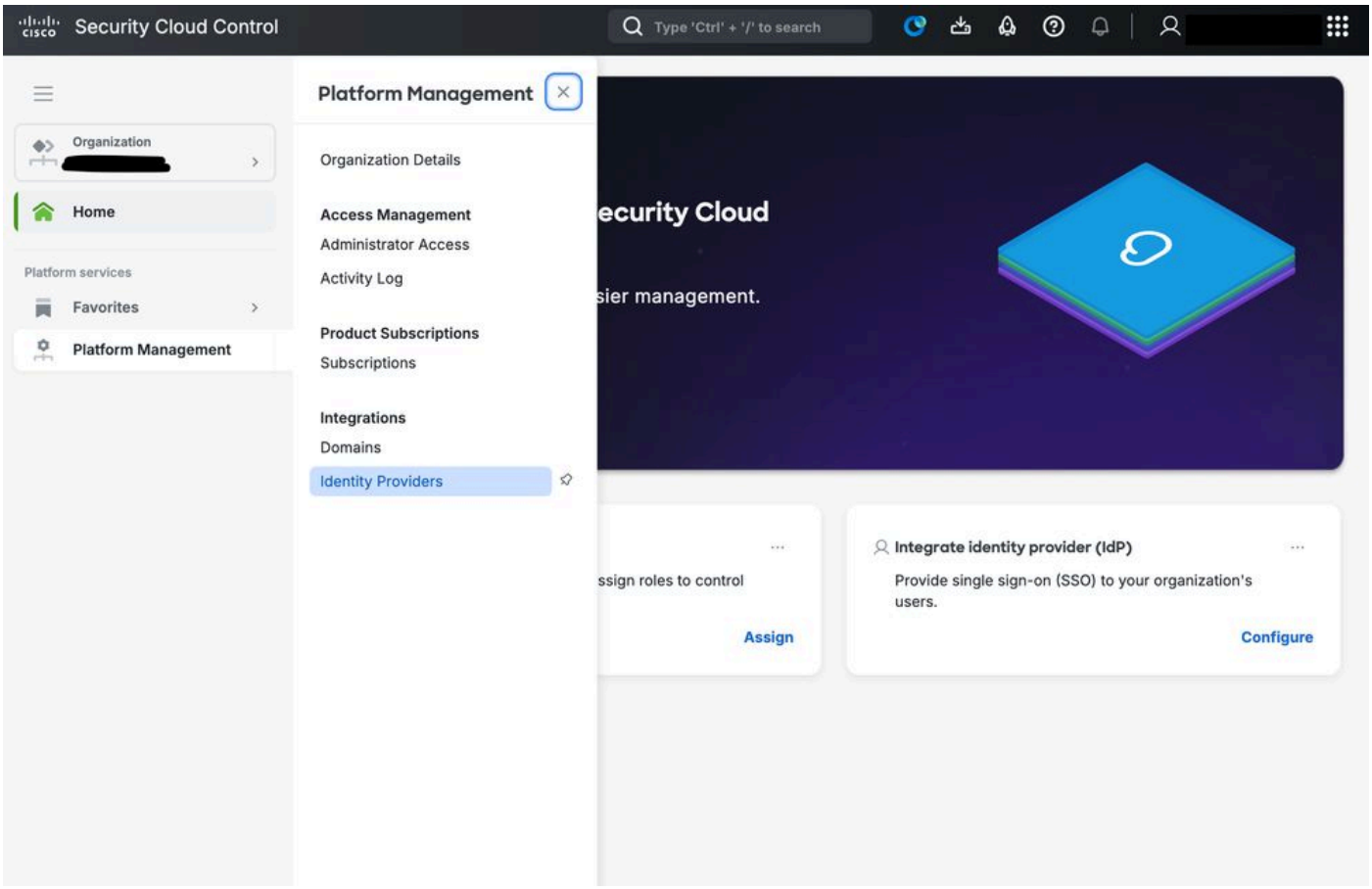
在此场景中，Cisco Duo被实施为访问控制、安全登录和MFA验证的主要解决方案。此集成要求管理员通过多个验证步骤验证其身份，从而增强环境的安全状态，降低未经授权的访问风险，并确保遵守组织安全策略。

Cisco Duo与Cisco Cloud Control集成

步骤1.访问Cisco SCC控制台。

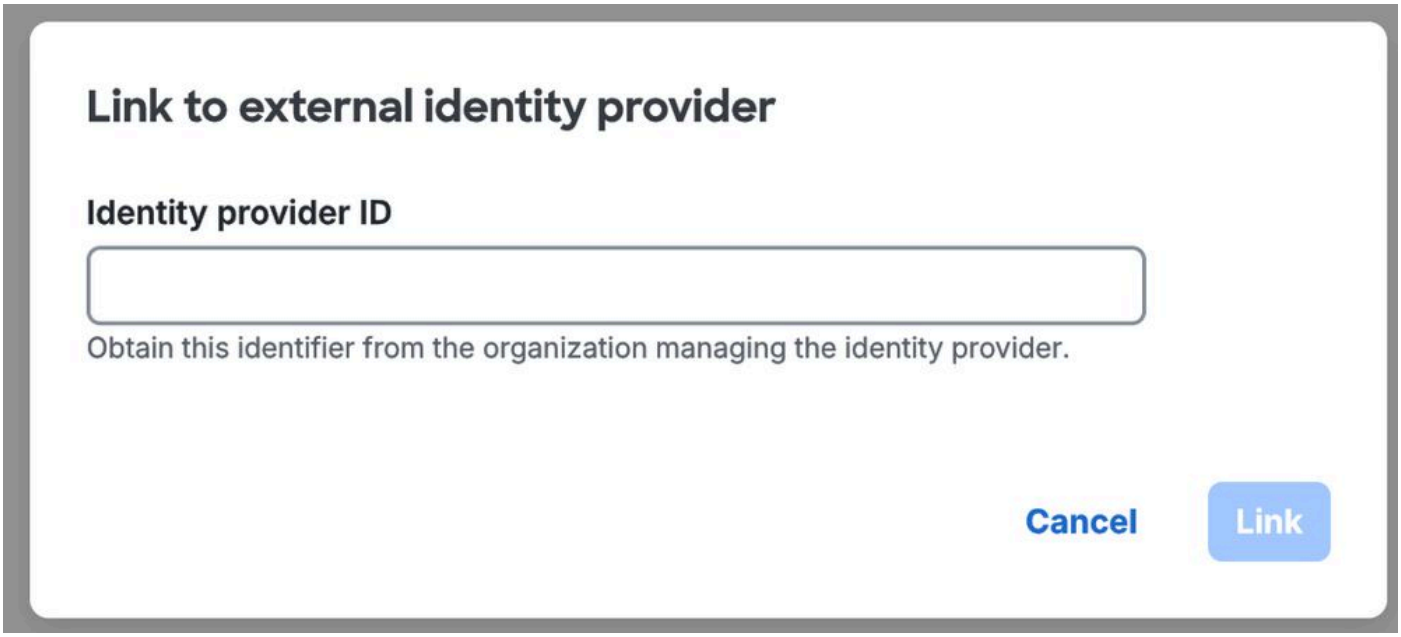
登录思科安全云控制门户https://security.cisco.com/。

导航到平台管理，然后单击身份提供程序。



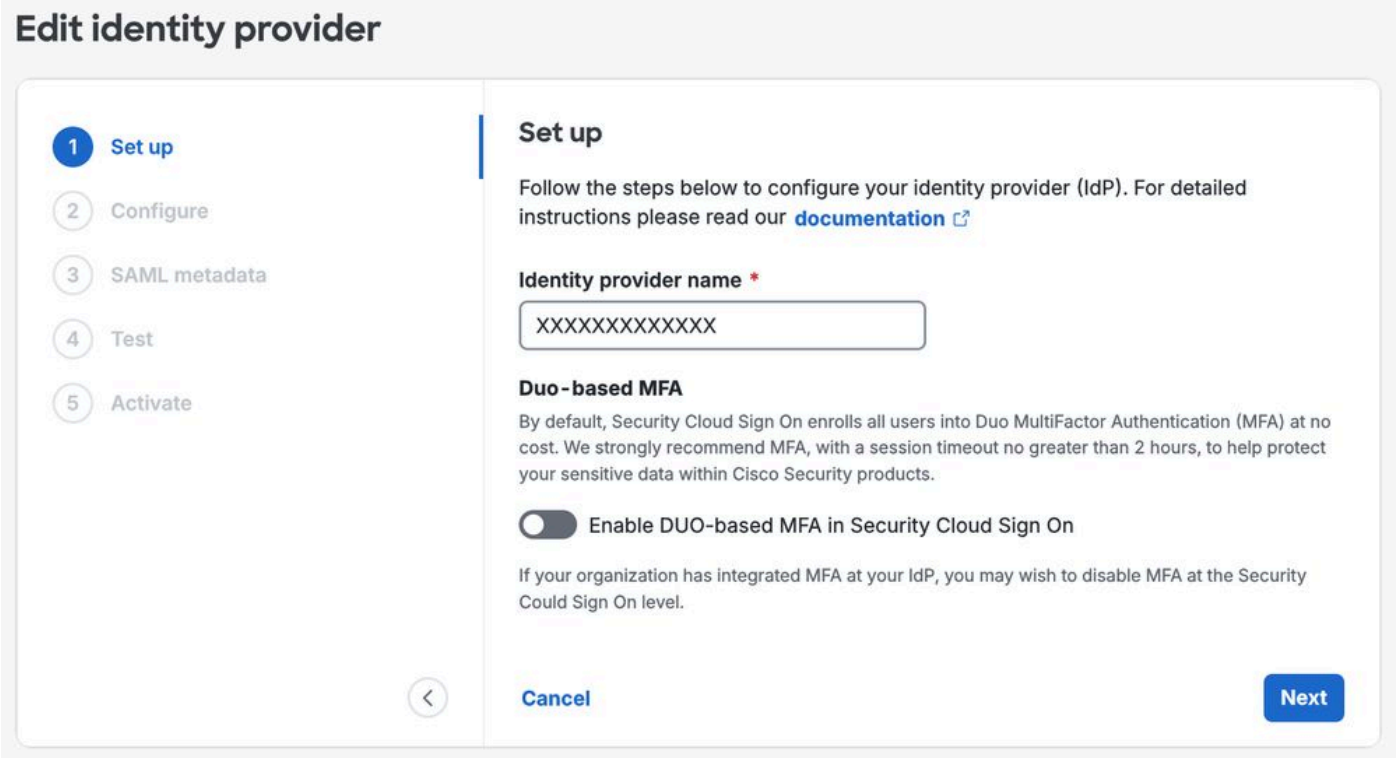
SCC IDP配置

使用自定义名称以标识身份提供程序。



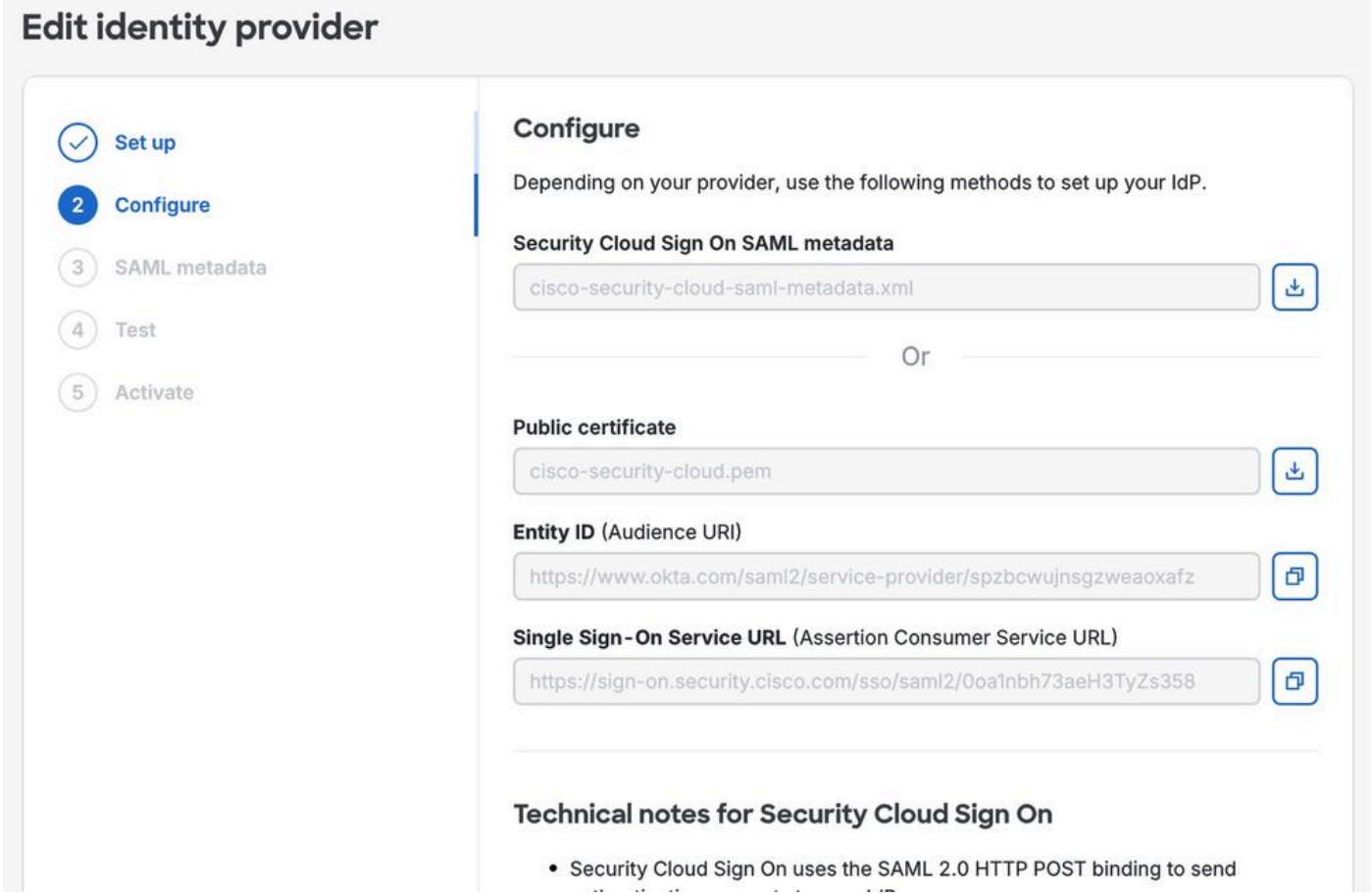
现在开始安装。此时，您可以访问Cisco SCC和Cisco Duo。

第2步：在SCC中，禁用Enable DUO-based MFA in Security Cloud Sing On（如图所示），然后点击Next。

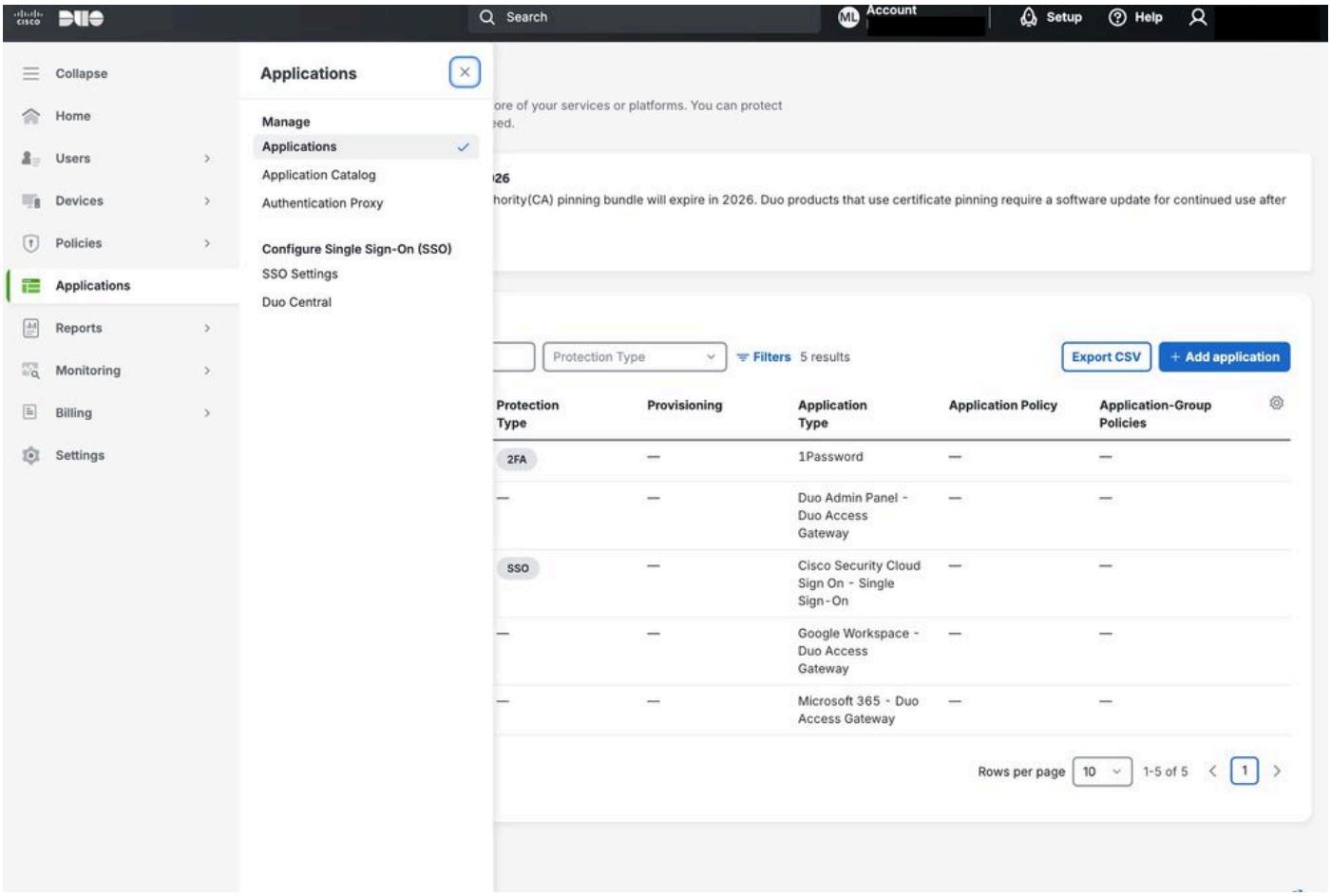


身份提供程序配置

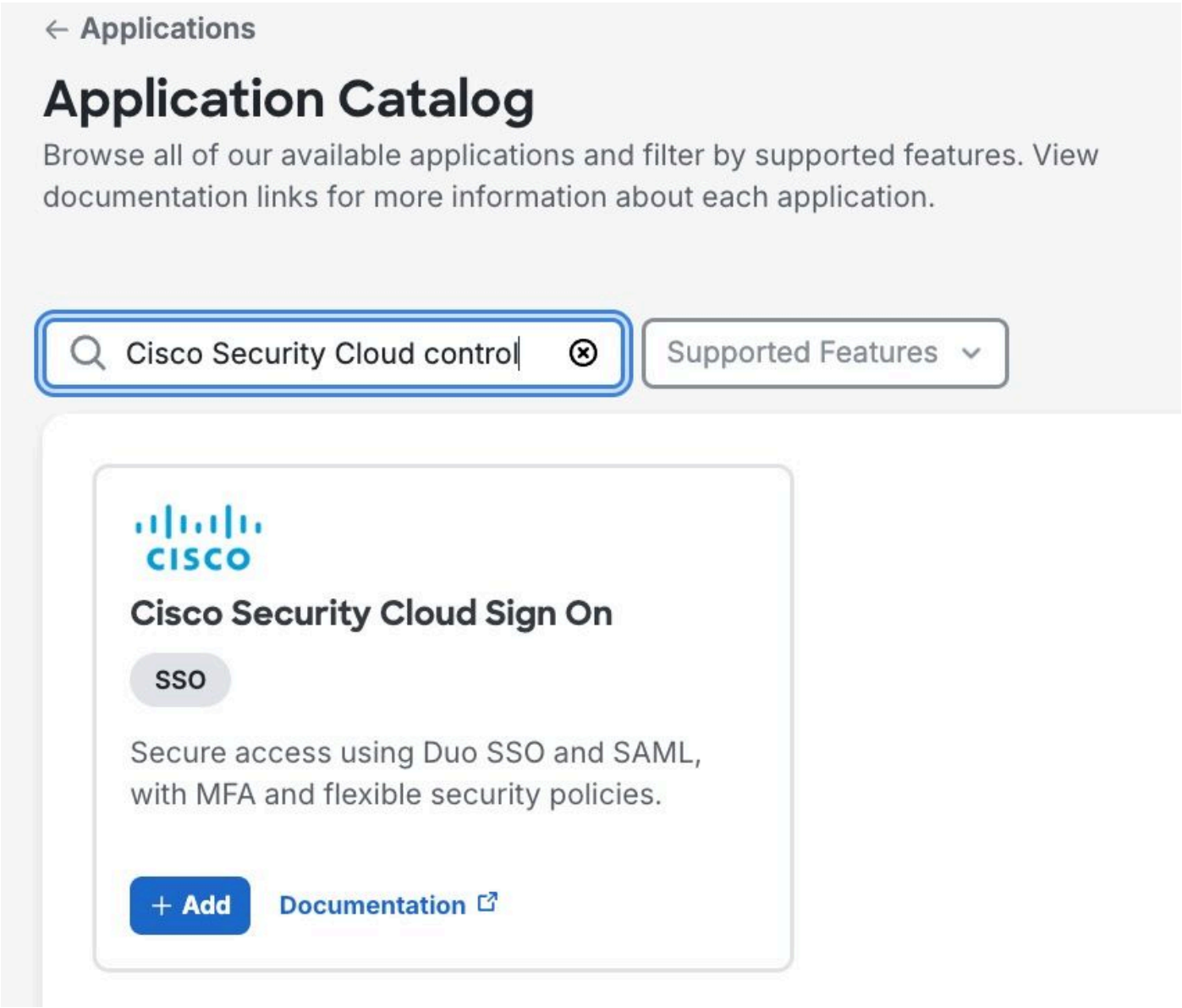
步骤3.创建相关数据，并在Cisco Duo配置过程中使用。
确保复制所有必需值和关联数据，并将它们存储在安全位置。
这些详细信息对于未来的集成步骤至关重要，因此请确保这些详细信息仅可供授权人员访问，并且根据贵组织的安全策略得到保护。



步骤4.打开Cisco Duo，导航到Applications部分，然后单击Add application。

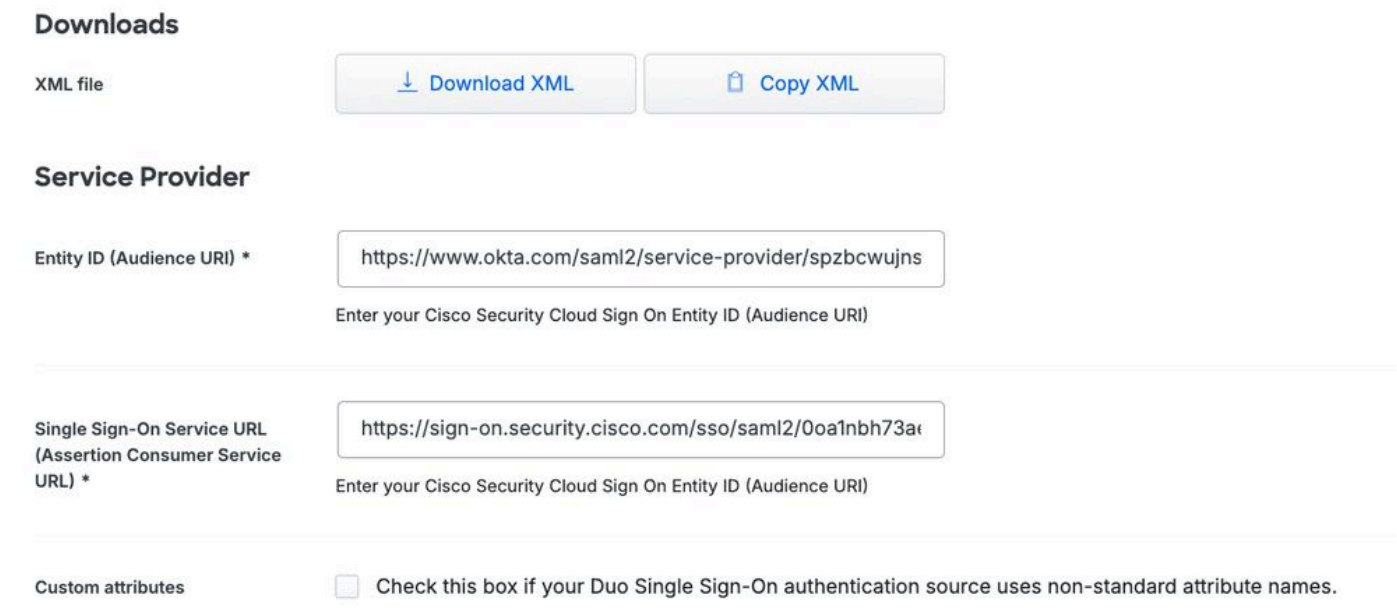


在菜单中，搜索Cisco Security Cloud，然后单击Add以开始集成。

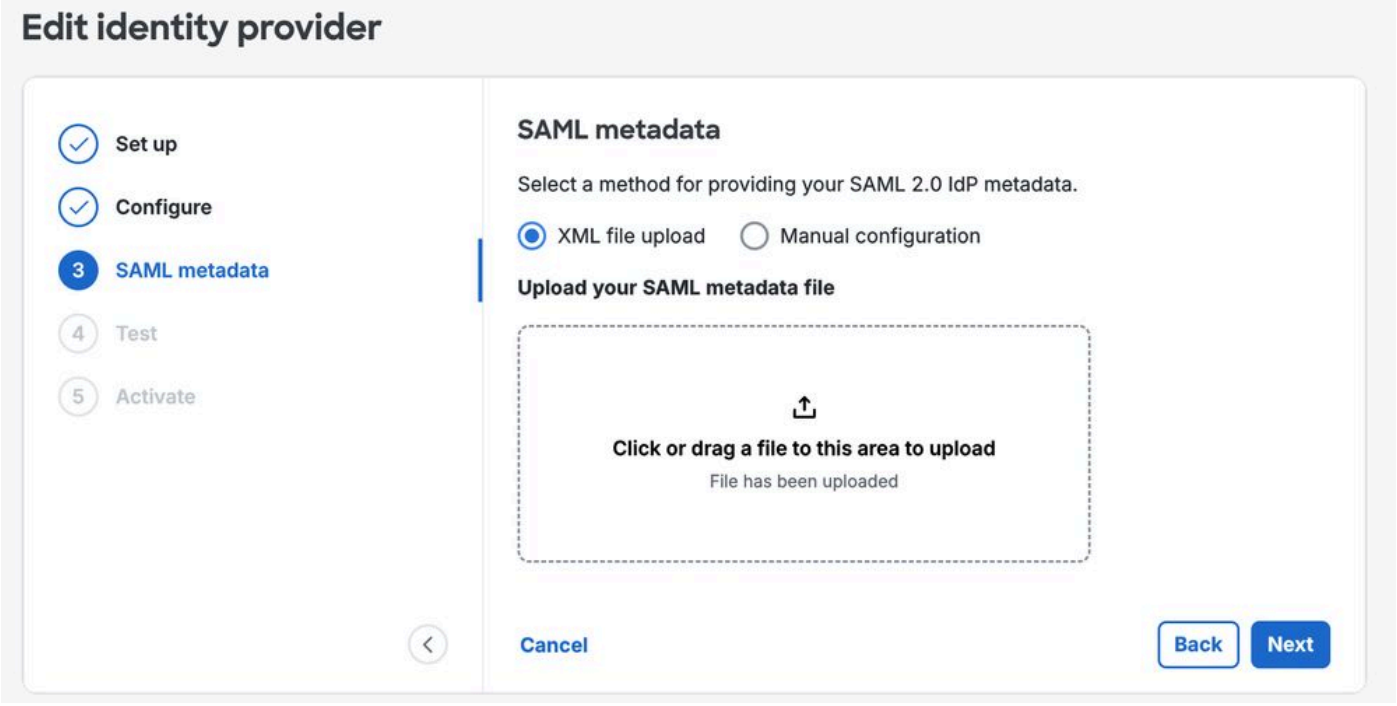


步骤5.在Cisco Duo应用程序中配置相关信息。

将实体ID和单点登录服务URL从Cisco SCC复制到Cisco Duo。



步骤6.下载XML并将文件上传到Cisco SCC。



注意：可从Cisco Duo控制台在应用中配置的其余参数必须根据您的特定要求进行调整。有关这些设置的详细说明，请参阅Cisco Duo官方文档。可配置参数的示例包括分配的应用程序名称、应用该策略的用户集，以及其他可以定制安全控制以满足组织需求的可定制选项。

思科ETD的思科双核中的策略配置

在此阶段，所有组件均已连接，下一步是在Cisco ETD控制台中配置适用于管理员身份验证过程的策略。

在本示例中，重点特别放在基于IP地址的访问控制上。但是，Cisco Duo提供许多其他访问控制选项。

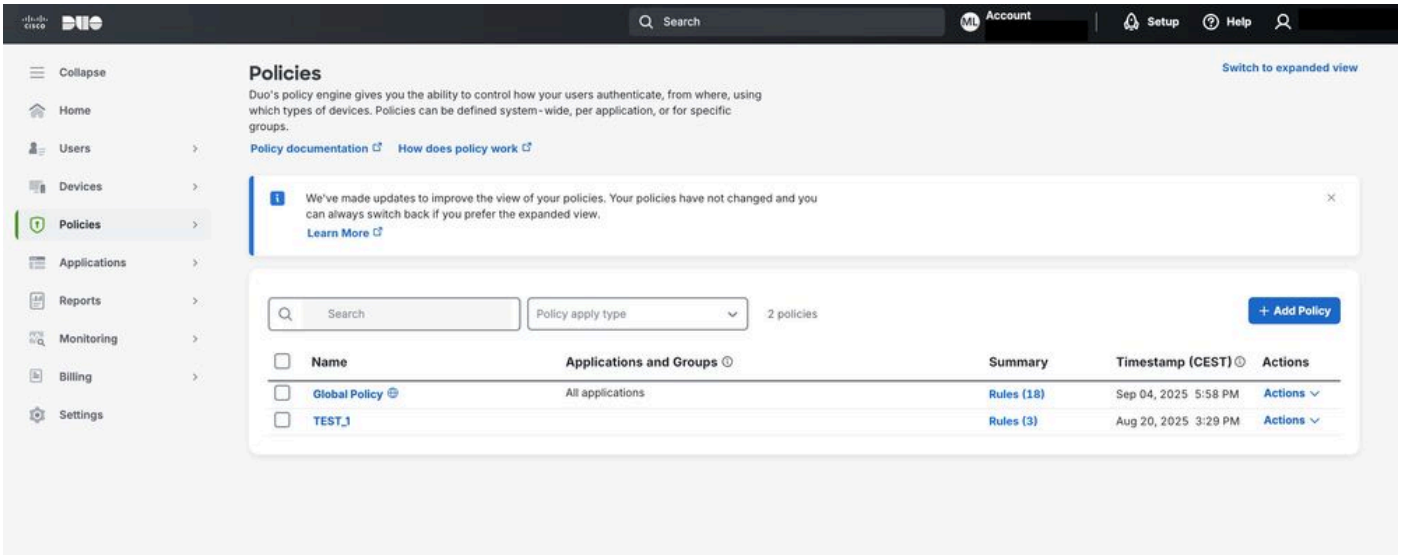
可以创建新的策略并分配给应用，从而实施所需的身份验证规则和对管理员登录的安全限制。

有关Cisco Duo中所有可用控件和配置选项的更多详细信息，请参阅官方Cisco Duo文档。

此资源提供有关设置、自定义和最佳实践的全面指导，以帮助优化安全策略。

通过导航到Cisco Duo中的Policies部分，可以创建策略，并通过Cisco Duo将其分配给Cisco ETD连接。

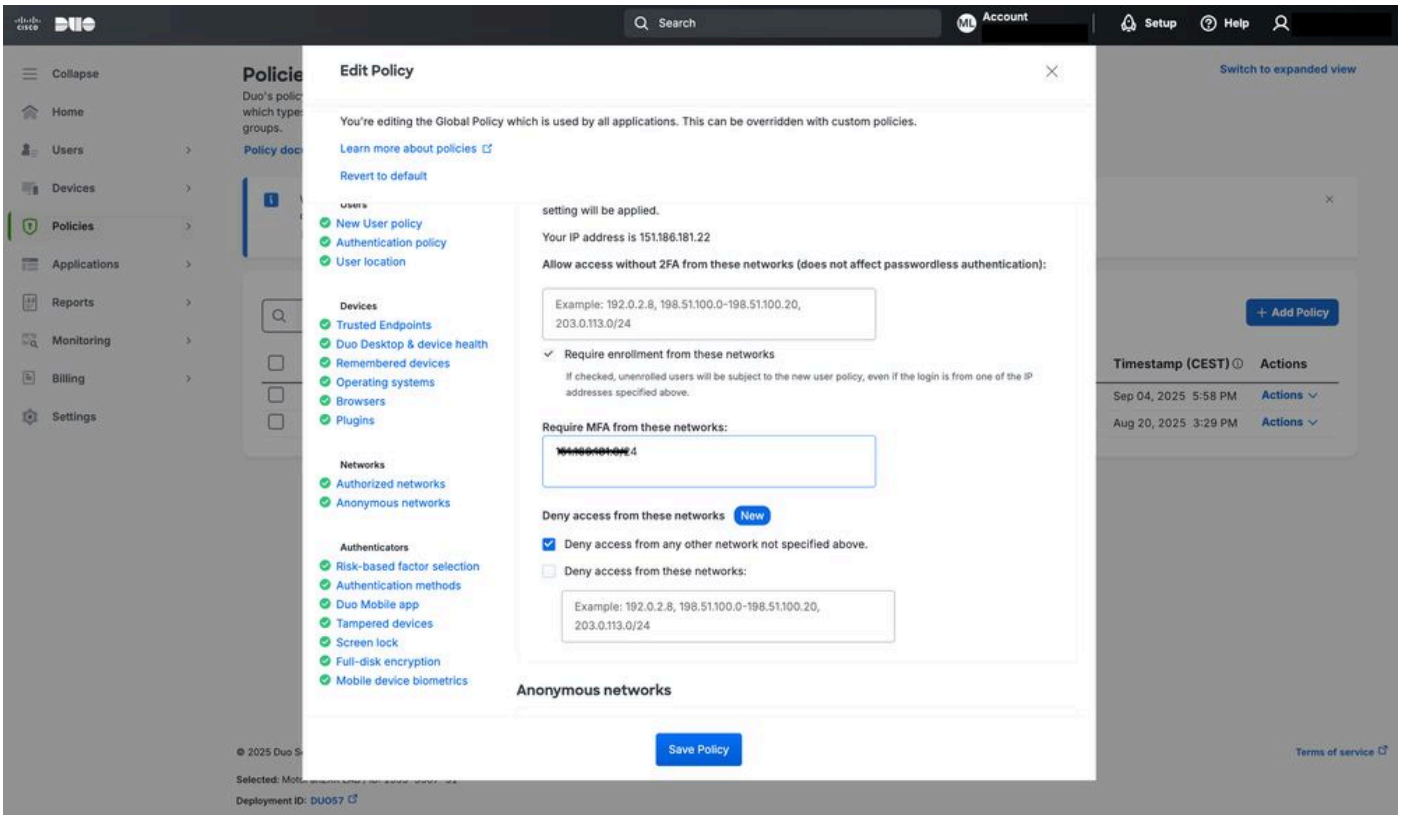
此策略可以根据访问要求按用户或组应用。



思科双核

在本示例中，如图所示，源IP访问控制通过配置Authorized Networks部分启用。

此配置仅允许从指定的受信任IP范围进行访问，从而增强思科ETD的安全性。



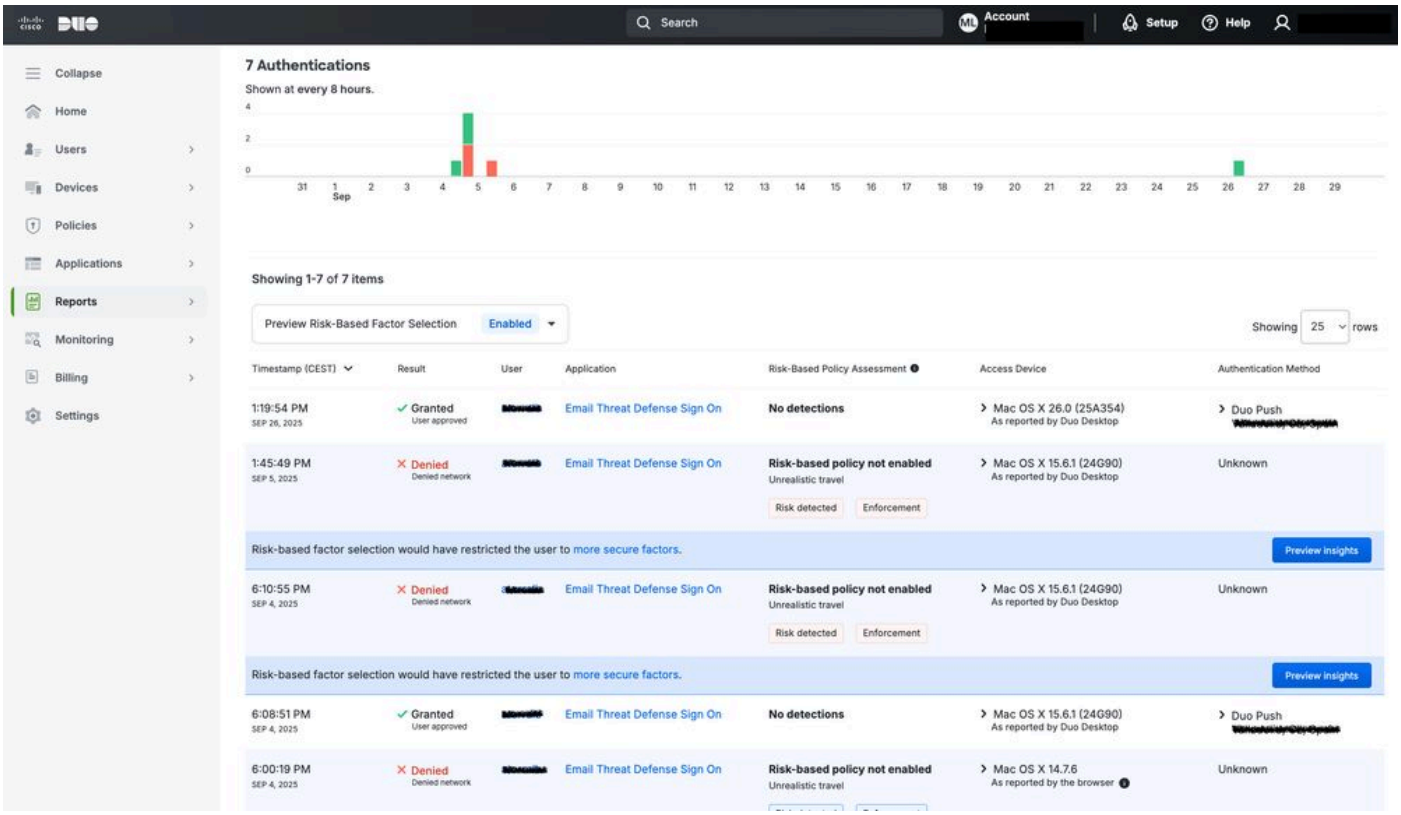
Cisco Duo策略配置

结论

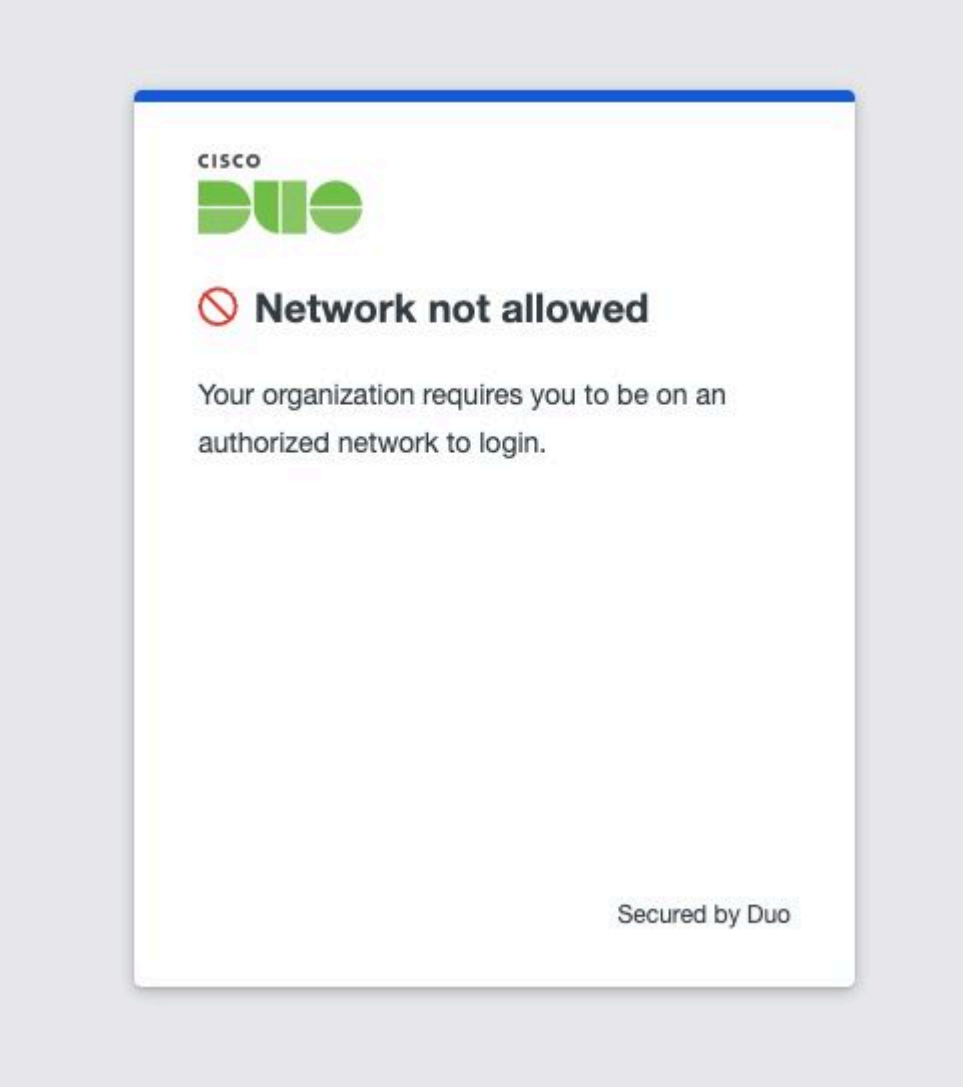
Cisco ETD提供灵活的选项，以便通过MFA和与身份提供商的集成保护管理员访问。
通过将Cisco SCC与Cisco Duo相结合，组织可以实施更强大的身份验证策略，降低未经授权访问的风险，并遵循行业最佳实践，实现安全的云服务管理。

除MFA外，管理员还可以利用Cisco Duo的基于策略的控制，以便根据特定条件（如源IP地址）限制访问。例如，如下图所示，系统会自动阻止从授权范围之外的IP地址进行的访问尝试。这样可以确保仅允许来自受信任网络的请求，从而增加一层额外的保护来防止潜在攻击。

通过结合MFA实施基于IP的访问控制，组织可以实现深度防御方法，将身份验证和网络位置验证相结合，以保护云中的关键管理接口。


Search
Account
Setup
Help
Collapse
Home
Users
Devices
Policies
Applications
Reports
Monitoring
Billing
Settings
7 Authentications
Shown at every 8 hours.
Showing 1-7 of 7 items
Preview Risk-Based Factor Selection
Enabled
Showing 25 rows
Timestamp (CEST)
Result
User
Application
Risk-Based Policy Assessment
Access Device
Authentication Method
1:19:54 PM
SEP 26, 2025
Granted
User approved
Email Threat Defense Sign On
No detections
Mac OS X 26.0 (25A354)
As reported by Duo Desktop
Duo Push
1:45:49 PM
SEP 5, 2025
Denied
Denied network
Email Threat Defense Sign On
Risk-based policy not enabled
Unrealistic travel
Risk detected
Enforcement
Mac OS X 15.6.1 (24G90)
As reported by Duo Desktop
Unknown
Risk-based factor selection would have restricted the user to more secure factors.
Preview insights
6:10:55 PM
SEP 4, 2025
Denied
Denied network
Email Threat Defense Sign On
Risk-based policy not enabled
Unrealistic travel
Risk detected
Enforcement
Mac OS X 15.6.1 (24G90)
As reported by Duo Desktop
Unknown
Risk-based factor selection would have restricted the user to more secure factors.
Preview insights
6:08:51 PM
SEP 4, 2025
Granted
User approved
Email Threat Defense Sign On
No detections
Mac OS X 15.6.1 (24G90)
As reported by Duo Desktop
Duo Push
6:00:19 PM
SEP 4, 2025
Denied
Denied network
Email Threat Defense Sign On
Risk-based policy not enabled
Unrealistic travel
Mac OS X 14.7.6
As reported by the browser
Unknown

Cisco Duo报告



网络控制结果

警告：需要了解的是，此更改会影响使用相同身份验证域的所有应用；不只是ETD，还包括其他依赖相同身份验证过程的产品，例如对思科安全访问控制台的访问。

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）。