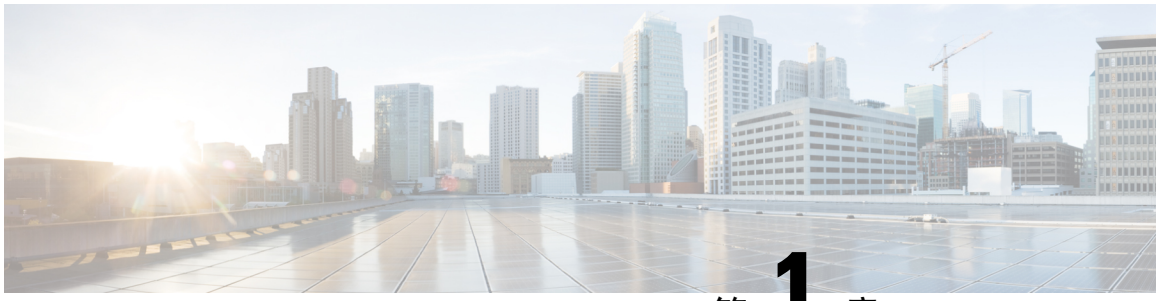
《思科 SecureX 登录快速入门指南》

首次发布日期: 2019 年 10 月 1 日

上次修改日期: 2021 年 8 月 11 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



第 1 章

欢迎

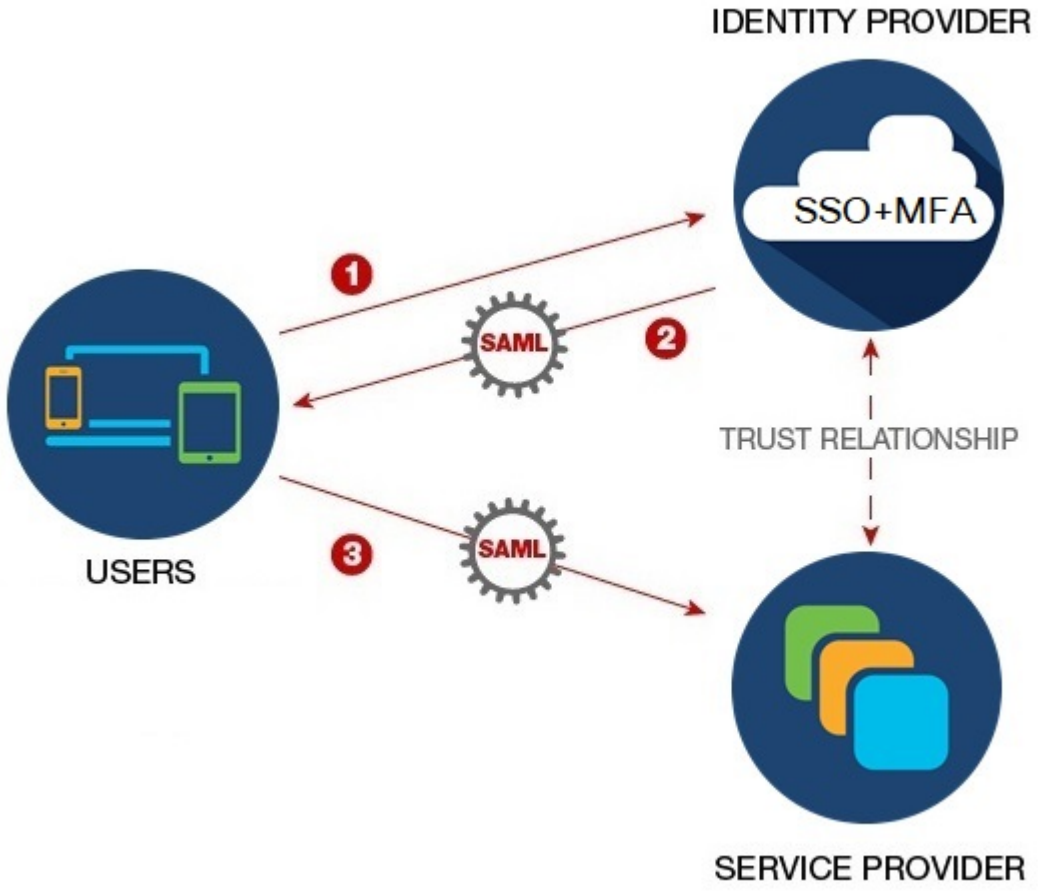
- 概述，第 1 页
- 工作原理，第 2 页

概述

通过思科 SecureX 登录，您可以从任何设备使用一组凭证来轻松访问所有思科安全产品。使用您的用户名和密码登录后，您的所有思科安全产品会在您的可自定义控制板中显示为应用。

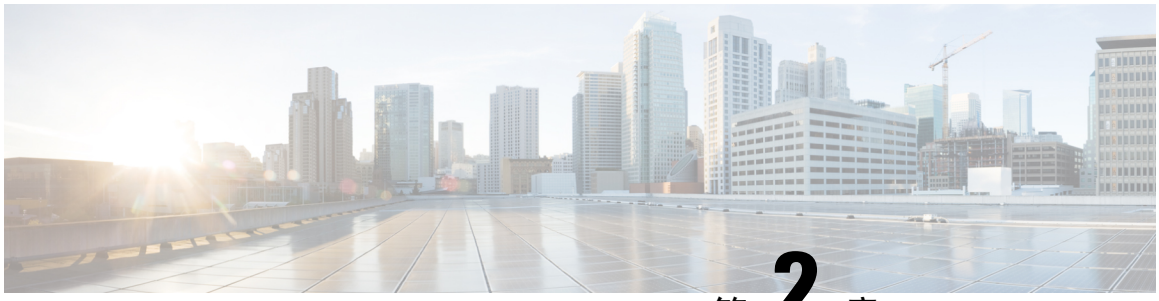
- 单击某个应用后您将自动登录，从而在思科安全产品中实现无缝工作流程。您不用再记住和处理多个密码。
- 与 Duo 的多因素身份验证 (MFA) 集成意味着自适应、分层和简化的身份验证。一个推送通知，单击一次，即时访问。

工作原理



安全断言标记语言 (SAML) 是一种基于 XML 的开放标准，用于在身份提供程序 (IdP) 和服务提供商 (SP) 之间交换身份验证和授权数据。SP 和 IdP 之间的交换会验证您的身份和权限。这使得您能够使用一组凭证登录不同的应用。管理每个用户的单点登录 (SSO) 比管理每个应用的单独登录要容易。

1. 用户登录 SSO IdP，即与 Duo 的 MFA 集成的思科 SecureX 登录。
2. IdP 和 SP 之间存在信任关系。IdP 可以将包含有关用户的受信任信息的 SAML 属性断言传递给 SP。
3. 当用户启动不同的应用时，SP 会向 IdP 请求用户授权和身份验证。由于到 IdP 的 SSO 已成功，因此用户现在可以访问所有不同的应用，而无需记住和输入更多凭证。



第 2 章

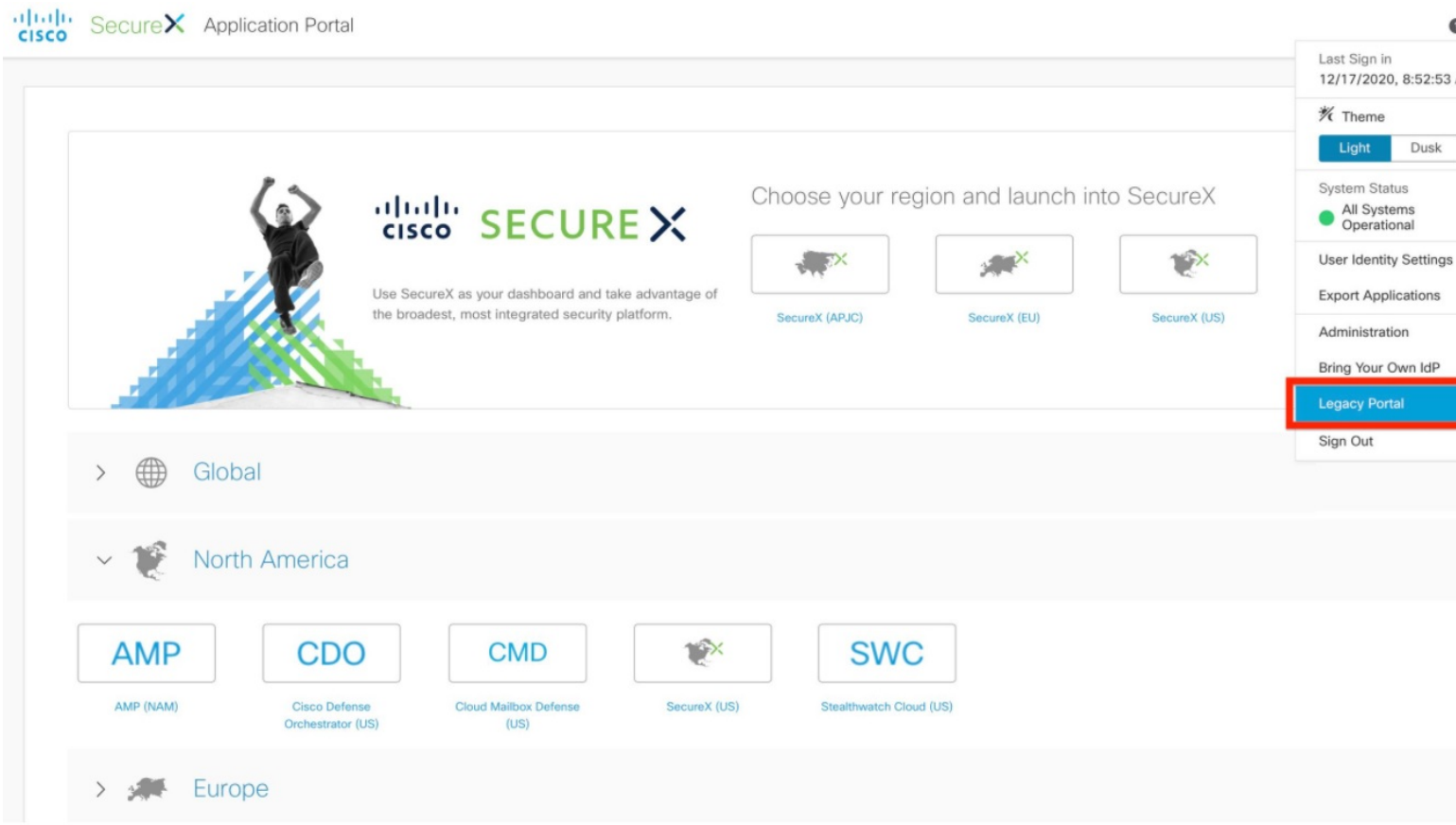
最新产品

- 新门户网站， 第 3 页
- Cisco SecureX， 第 4 页
- Microsoft Azure， 第 4 页
- Cisco.com， 第 5 页
- URL 变更， 第 6 页

新门户网站

思科 SecureX 登录的外观和可用性在其新门户中得到了改进。选择您所在的地区，然后从增强型门户启动 SecureX 或任何其他思科安全产品。要返回旧门户，请从右上角的用户配置文件菜单中选择**传统门户 (Legacy Portal)**。

图 *1:*



Cisco SecureX

使用思科 Secure 登录登录到思科 SecureX

现在，您可以使用您的思科安全登录帐户登录思科 SecureX。此后，思科 Secure 登录会被称为思科 SecureX 登录。

Microsoft Azure

使用您的 Microsoft Azure 帐户登录 Cisco Secure Sign-On

现在，您可以使用您的 Microsoft Azure 帐户登录 Cisco Secure Sign-On。

- 谁可以使用此方法？

  使用 Microsoft Azure 作为组织的身份提供程序 (IdP) 的客户。

- 如何启用此方法？

根据客户的 Microsoft Azure 配置，它能为组织透明地工作。否则，一旦第一个用户尝试访问，管理员就需要在 Azure 门户中批准访问。有关配置详细信息，请转到 Microsoft Docs 网站并查看其 Azure 文档中有关以下主题的信息：

- 将用户或组分配给企业应用
- 向应用授予租户范围的管理员同意
- 配置管理员同意工作流程

- 这是否会从客户的 Microsoft Azure Active Directory (AD) 配置文件中提取用户身份属性？

  是的，它会提取名字、姓氏、显示名称、标题、移动电话和组织。

- 这是否会提取 Azure 组信息并允许由 Cisco Secure Sign-On 保护的应用识别和使用？

  不会，组分配和角色权限由每个思科应用单独处理。

- 这是否会改变我访问使用 Cisco Secure Sign-On 的应用的方式？

  不会，只要您使用相同的用户名，就可以像以前一样映射到应用中；它只会更改您的身份验证方式。

- 我能否同时保留并使用这两个帐户？

  两者答案均为是。

- 这对使用 @cisco.com 用户名的思科员工有什么影响？

  思科还没有为 @cisco.com 帐户启用 Microsoft 登录，因此，如果您尝试使用此方法登录，则会收到一条失败消息。

- 如果使用**使用 Microsoft 登录 (Sign in with Microsoft)** 选项，但没有 Cisco Secure Sign-On 帐户会怎样？

  这将为您透明地工作并允许您直接登录，而无需创建单独的帐户。

Cisco.com

使用您的 Cisco.com 帐户登录 Cisco Secure Sign-On

现在，您可以使用自己的 cisco.com 帐户登录 Cisco Secure Sign-On。

- 这与我的 Cisco Secure Sign-On 帐户有何不同？

  这是您的标准 cisco.com 帐户（以前称为 CCO），用于访问支持、下载软件等。

- 这是否会改变我访问使用 Cisco Secure Sign-On 的应用的方式？

  不会，只要您使用相同的用户名，就可以像以前一样映射到应用中；它只会更改您的身份验证方式。

- 我能否同时保留并使用这两个帐户？

两者答案均为是。

- 这对使用 @cisco.com 用户名的思科员工有什么影响？

  鼓励思科员工使用**使用 Cisco.com 登录 (Sign in with Cisco.com)** 选项，以便我们可以在指标中将他们识别为员工，同时确保他们仅收到一个 MFA 提示。

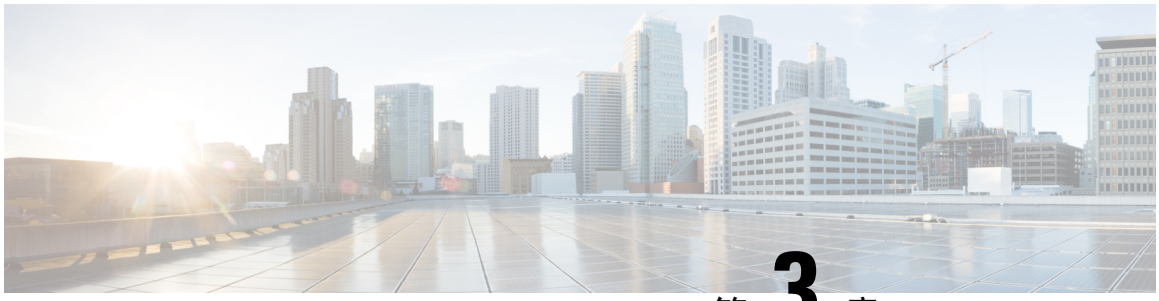
- 如果使用**使用 Cisco.com 登录 (Sign in with Cisco.com)** 选项，但没有 Cisco Secure Sign-On 帐户会怎样？

  这将为您透明地工作并允许您直接登录，而无需创建单独的帐户。

URL 变更

URL 变更

2020 年 3 月 24 日，Cisco Secure Sign-On 域从 security.cisco.com 移至 sign-on.security.cisco.com，以满足思科 SecureX 的需要。更新您的书签和密码管理器（例如 LastPass、1Password 或 DashLane）以引用新 URL。



第 3 章

操作步骤

- 使用入门，第 7 页

使用入门

开始之前

对于支持的产品，请参阅迁移和选择指南，以便了解产品特定的详细信息。

步骤 1 访问 https://sign-on.security.cisco.com。

步骤 2 如果您有 SecureX 登录帐户：

a) 输入您的用户名。如果您之前已在使用的网络浏览器上成功完成登录，则系统会自动显示您的安全映像。此功能需要使用浏览器 Cookie。

注意　如果您之前已在当前网络浏览器上成功登录并且未清除 Cookie，倘若在输入用户名时安全映像未显示，那么请不要输入密码。如果未显示安全映像，请关闭网络浏览器，然后确认您使用了正确的 Web 地址登录。然后，打开新的网络浏览器窗口，手动输入 Web 地址并输入用户名。如果您的安全映像仍未显示，请联系您的产品支持团队。

b) 单击**下一步 (Next)** 并输入您的密码。
c) 单击**登录 (Sign In)**。如果您看到**无法登录 (Unable to sign in)** 错误消息，则您的用户名和密码与为您的配置文件指定的用户名和密码不匹配，或者您没有访问权限。请联系您的产品支持团队。
d) 在 Duo MFA 提示符后，将通知推送到您的注册设备，然后单击该设备上的审批进行身份验证。

步骤 3 或者，您可以选择使用备用帐户继续：

- Cisco.com - 如果您是思科员工或客户，并且 Cisco.com 帐户仅供您使用。
- Microsoft Azure - 如果您的公司在 Microsoft Azure Active Directory 中维护员工帐户。

步骤 4 如果您没有 SecureX 登录帐户：

a) 单击**创建 SecureX 登录 (Create a SecureX Sign-On)**。

b) 填写表单，然后单击**注册 (Register)**。

c) 在思科中查找无需答复的“激活帐户”邮件，然后单击**激活帐户 (Activate Account)**。

d) 通过配置 Duo Security 来设置 MFA。双因素身份验证（一种 MFA）通过使用辅助设备对您进行身份验证，从而增强帐户的安全性。这样可以防止除您之外的任何人访问您的帐户，即使他们知道您的密码也无法访问。

e) 选择设备并按照提示注册设备。有关更多信息，请参阅《Duo MFA 和设备注册指南》。如果您的设备上已经有 Duo 应用，您将收到此帐户的激活代码。Duo 支持一个设备上的多个帐户。

f) 为了提高安全性，我们建议您至少注册两个不同的设备。单击**+ 添加其他设备 (+Add another device)**，然后按照提示注册其他设备。有关更多信息，请参阅《Duo MFA 和设备管理指南》。

g) 将设备与帐户配对后，单击**完成 (Finish)**。或者，现有的 MFA Google 身份验证器用户可以通过单击**设置 (Setup)** 来设置 Google 身份验证器并按照提示将其添加到此处作为备份因素。

h) 选择一个“忘记密码”问答。

i) 添加用于重置密码或使用 SMS 解锁帐户的电话号码：在您无权访问邮件帐户并且需要发送恢复代码的文本消息时非常有用。

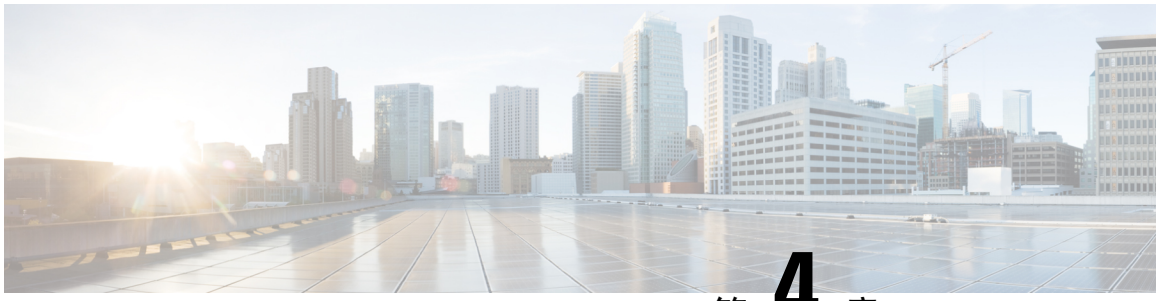
j) 选择安全图像。

k) 单击**创建我的帐户 (Create my account)**。

下一步做什么

欢迎使用 SecureX 登录应用门户：

- 选择您所在的地区并启动 SecureX。
- 单击任意磁贴以启动该应用，并且无需密码。
- 要将应用从此处导出到 SSO 门户，请从右上角的用户配置文件菜单中选择**导出应用 (Export Applications)**。
- 要返回旧门户，请从右上角的用户配置文件菜单中选择**传统门户 (Legacy Portal)**。



第 4 章

支持的产品

- 支持的产品 ， 第 13 页

支持的产品

产品	说明	想要此产品？	支持
思科 Cloudlock	思科 Cloudlock 是一个基于 API 的云访问安全代理 (CASB)，有助于加速安全使用云。通过保护您的身份、数据和应用，Cloudlock 可抵御帐户入侵、漏洞和云应用生态系统风险。Cloudlock 以 API 为驱动的方法提供了一种简单且开放的方式，以实现健康的云采用并管理您的云应用生态系统中的风险。请参阅思科 Umbrella + Cloudlock 解决方案简介。	请求报价	选择加入指南 查看文档 邮件支持
思科防御协调器	Cisco Defense Orchestrator (CDO) 是基于云的应用，可帮助对思科安全产品实现一致的策略管理。这款基于云的应用能够以简驭繁，让您轻松抵御最新的网络威胁，节省您的宝贵时间。	免费试用 CDO	迁移指南 查看文档 提交支持案例 邮件支持

支持的产品

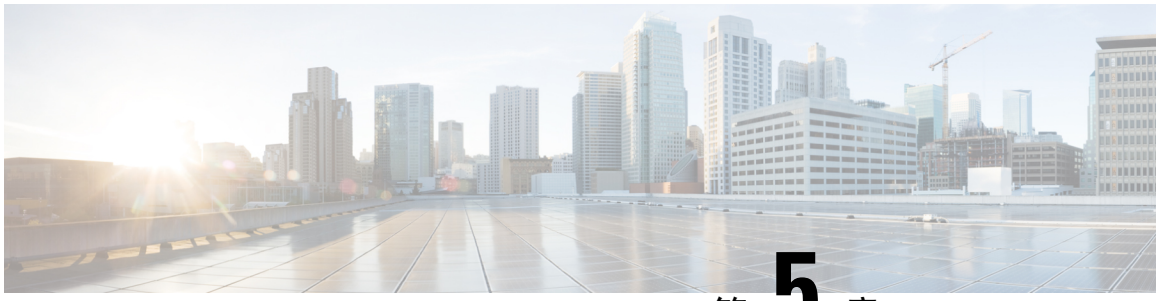
产品	说明	想要此产品？	支持
思科 Meraki	思科 Meraki 拥有行业最大规模的智能管理平台网络解决方案。思科 Meraki 云服务助力全球数以万计的网络并连接数百万台设备。从企业到医院、银行和零售商，思科 Meraki 云网络平台赢得了成千上万 IT 专业人员的信任。	免费试用思科 Meraki	选择加入指南 查看文档 提交支持案例
Cisco Secure Cloud Analytics（以前称为 Stealthwatch Cloud）	Cisco Secure Cloud Analytics 可提高从办公室到公共云的分布式网络的安全性和事件响应。实时检测威胁。减少误报。获取可行的安全情报，以便让您的安全团队更加高效。	免费试用 Cisco Secure Cloud Analytics	迁移指南 查看文档 提交支持案例 邮件支持
Cisco Secure Email Cloud Gateway	思科安全邮件云网关使用户能够安全地进行通信，并通过多层次的安全防御方法帮助组织抵御商业邮件攻击 (BEC)、勒索软件、高级恶意软件、网络钓鱼、垃圾邮件和数据丢失。它还包括高级威胁防护功能，可以更快地检测、阻止威胁并进行补救；防止数据丢失；并通过端到端加密在传输过程中保护重要信息。	免费试用安全邮件云网关	查看文档 提交支持案例

支持的产品

产品	说明	想要此产品？	支持
思科安全邮件云邮箱（以前称为云邮箱防御）	思科安全邮件云邮箱是面向 Microsoft 365 的集成式云原生安全解决方案，主要特点包括：部署轻松；可简化攻击补救；具有卓越的可视性；可提供由 Cisco Talos 支持的一流防护。利用成熟的思科安全邮件技术，云邮箱通过阻止勒索软件、BEC、网络钓鱼、欺骗和垃圾邮件等高级邮件威胁来解决 Microsoft 365 安全方面的漏洞。	免费试用云邮箱	用户指南 常见问题 邮件支持
思科安全终端（以前称为“面向终端的高级恶意软件保护”）	思科安全终端将全球威胁智能、先进的沙盒技术，以及实时恶意软件拦截功能集于一身，防止各种漏洞。但仅仅依赖防御是不够的，所以思科安全终端还会持续分析整个扩展网络中的文件活动，使您可以快速检测、遏制和删除高级恶意软件。	免费试用 Cisco Secure Endpoint	选择加入指南 查看文档 提交支持案例
Cisco Secure Malware Analytics（以前称为 Threat Grid）	Cisco Secure Malware Analytics 将高级沙盒与威胁智能整合到一个统一的解决方案中，保护组织免受恶意软件的影响。借助情景丰富的强大恶意软件知识库，您可以了解恶意软件正在执行或尝试执行的操作，它会造成多大的威胁，以及如何抵御它。	免费试用 Cisco Secure Malware Analytics	选择加入指南（需要登录） 提交支持案例

支持的产品

产品	说明	想要此产品？	支持
Cisco SecureX	思科 SecureX 是一个简化的平台体验。将思科的集成安全产品组合连接到您现有的基础设施，以便提供可统一可视性、实现自动化并增强网络、终端、云和应用安全性的一致体验。	免费试用 SecureX	登录指南 查看文档 提交支持案例
Cisco Umbrella	Cisco Umbrella 有助于确保互联网的访问，同时控制整个网络、分支机构和漫游用户的云应用使用。它是一个云安全平台，可在几分钟内轻松部署，同时提供深度检查和控制，以支持合规性并阻止威胁。	免费试用 Cisco Umbrella	选择加入指南 查看文档 提交支持案例



第 5 章

常见问题解答

- 常见问题解答，第 17 页

常见问题解答

我目前在使用 OneLogin。我要怎样才能迁移到思科 SecureX 登录？

转至思科 SecureX 登录 (Cisco SecureX Sign-On) 页面，然后单击**创建 SecureX 登录 (Create a SecureX Sign-On)** 开始自注册过程。

帐户激活邮件在多长时间内有效？

您的帐户激活邮件自发送后的 7 天内有效。

如何更改安全映像？

要更改安全映像，请登录并单击顶部菜单中的用户名，然后选择**设置 (Settings)**。在**安全映像 (Security Image)** 部分中，单击**编辑 (Edit)**。选择新的安全映像，然后单击**保存 (Save)**。

如何更改帐户密码？

要更改帐户密码，请登录并单击顶部菜单中的用户名，然后选择**设置 (Settings)**。在**更改密码 (Change Password)** 部分中，单击**编辑 (Edit)**。输入当前密码和新密码，单击**更改密码 (Change Password)**，然后单击**保存 (Save)**。

如何更改“忘记密码”问题？

要更改“忘记密码”问题，请登录并单击顶部菜单中的用户名，然后选择**设置 (Settings)**。在**忘记密码 (Forgotten Password)** 问题部分中，单击**编辑 (Edit)**。选择一个新问题并输入答案，然后单击**保存 (Save)**。

目前，我正在对 MFA 使用 Google 身份验证器。我的 ID 是否会迁移？

不会，您的 Google 身份验证器 MFA 不会迁移。所有思科 SecureX 登录帐户都必须使用 Duo 的 MFA，因为它允许调用和文本到硬件和软件解决方案。如果您希望继续使用 Google 身份验证器，则可以将

其添加为帐户的备份因素。在帐户激活期间，使用 Duo（主要）来设置 MFA。然后，使用 Google 身份验证器（备份）来设置您的其他 MFA。

我能否将组织的 Duo 策略和设置用于 Duo MFA？

还没有。我们将添加“自带”功能，让您能够将 Duo MFA 指向您组织的 Duo 策略和设置。

如果我忘记了密码该怎么办？

在思科 SecureX 登录 (Cisco SecureX Sign-On) 页面上，单击**需要帮助登录？(Need help signing in?)** 和**忘记密码？(Forgot Password?)**。您可以通过三个选项来重置密码（按照偏好的顺序）：

- 单击**通过 Duo 重置 (Reset via Duo)**，通过身份验证来验证您的身份，然后输入新密码。
- 输入您添加到帐户设置的手机号码，然后单击**通过短信重置 (Reset via SMS)**。查看短信并按照提示操作。
- 输入您的邮件或用户名，然后单击**通过邮件重置 (Reset via Email)**。查看邮件并按照提示操作。

如果您无法使用这些方法，请联系您的支持的产品团队。

我的密码是否安全？

是，我们提供严格的安全措施和控制措施来保护您的信息。这些控制会在我们的 SOC2 报告中进行审核和证明。

我的用户名和密码存储在哪里？如何存储？

正如我们使用强加密来保护您的数据一样，我们也会为您的用户名和密码凭证使用强（256 位 AES）加密。

如果我丢失了用于验证 Duo 身份的手机该怎么办？

如果您丢失了手机并且仍然可以使用自己的用户名和密码进行登录，请单击 Duo 验证页面上的**设置 (Settings)**。选择**添加新设备 (Add a new device)** 并按照提示注册新电话。有关详细信息，请参阅 Duo 添加新设备指南。

为什么我必须为某些应用输入密码，而其他一些应用则不用？

通过思科 SecureX 登录，您可以通过一个统一的控制面板来访问您的应用。通过使用安全断言标记语言 (SAML) 的单点登录 (SSO) 技术来提供对这些应用的访问权限。借助 SAML，思科 SecureX 登录会自动通过令牌来传递访问权限，因此，当应用需要更新时，您无需手动进行更改。

如何更改现有应用的用户名和密码？

要更改现有密码，请将鼠标指针悬停在应用的磁贴上。磁贴的右上角有一个齿轮图标。单击齿轮图标以打开设置，然后提供您的当前用户名和密码进行身份验证。通过验证后，您就能够输入新密码。

管理员能否看到我的登录信息？

管理员可以看到您的用户名，但他们无权访问您的密码。

如果我被帐户锁定该怎么办？

如果您的帐户已锁定，请单击**需要帮助登录？(Need help signing in?)** 和思科 SecureX 登录 (Cisco SecureX Sign-On) 页面上的**解锁帐户 (Unlock Account)**。如果您无法使用这些方法，请联系您的支持的产品团队。

为什么有时我看不到安全映像？

安全映像是您登录时设置的一个 Cookie。如果浏览器中的 Cookie 已被清除，那么您下次登录时可能就看不到安全映像。

为什么我的会话到期了，但某些应用仍处于打开状态？

虽然您可能已退出思科 SecureX 登录会话，但思科 SecureX 登录不会将您从应用注销。

如果思科 SecureX 登录失败会怎样？

思科 SecureX 登录建立在“永远在线”架构上。如果服务关闭，您将无法使用单点登录登录和访问您的应用。但是，您仍然可以通过直接链接来访问某些应用。如果您无法访问思科 SecureX 登录并想了解是否是因为服务中断，请联系您的支持的产品团队。

如何删除现有的思科 SecureX 登录帐户？

虽然产品管理员可以通过删除帐户来删除对其单个产品应用的访问权限，但您必须通过支持的产品与思科 TAC 联系，让思科 SecureX 登录工程团队为您删除帐户。

如何返回旧的 SecureX 登录门户？

从右上角的用户配置文件菜单中选择**传统门户 (Legacy Portal)**。

我的组织已使用 IdP 进行单点登录。如何将其与 SecureX 登录集成？

您可以“自带 IdP”并将其与 SecureX 登录集成，以便访问思科安全应用，而无需手动重新创建所有用户帐户。有关详细信息，请参阅《思科 SecureX 登录第三方 IdP 集成指南》。

其他资源？

有关其他信息，请参阅这些资源：

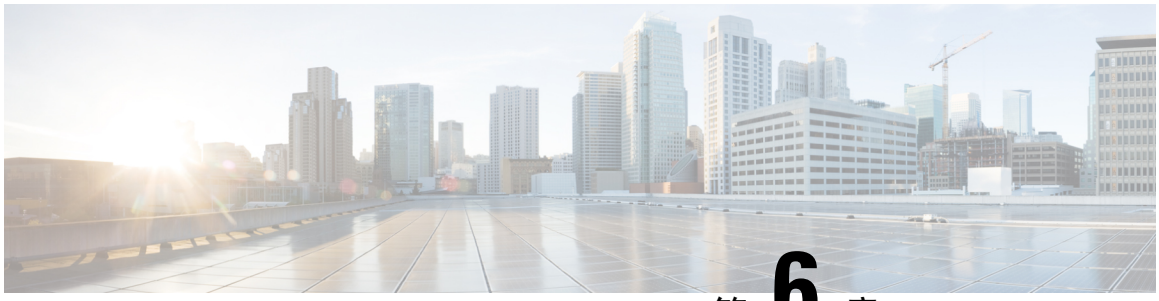
- 思科 SecureX 登录产品页面
- 思科 SecureX 登录隐私数据表

常见问题解答

第 I 部分

附录

- 导出应用， 第 23 页



第 6 章

导出应用

- 概述， 第 23 页
- 导出应用到 Duo Access Gateway， 第 23 页
- 将应用导出到 Microsoft Azure， 第 24 页

概述

“导出应用”(Export Applications) 页面（可从控制板页面上的用户配置文件菜单访问）列出了您可以从 SecureX 登录访问的思科安全产品应用。每个应用旁边的链接包括：

- 将应用的名称复制到剪贴板
- 将应用的 URL 复制到剪贴板
- 将应用的徽标下载到您的计算机

您可以从此处将思科安全产品应用导出到您的单点登录 (SSO) 应用门户：一个登录页面，提供您可以通过单次通用登录访问的一组应用。常见的 SSO 应用包括 Duo Access Gateway、Microsoft Azure 和 Okta SSO，它们允许您登录一次，然后就能使用相同的用户身份和凭证访问您的应用。使用“导出应用”(Export Applications) 页面上的链接及其中的信息在 SSO 应用中添加和配置应用。本章通过两个示例来介绍一般流程。

导出应用到 Duo Access Gateway

按照以下步骤在 Duo Access Gateway 启动器中向思科安全产品应用添加书签。

开始之前

- 您必须有权访问思科 SecureX 登录中的应用。
- 您必须在 Duo Access Gateway 中拥有管理员权限。
- 设置并启用 Duo Access Gateway 启动程序： https://guide.duo.com/dag-launcher

步骤 1 在 Duo Access Gateway 管理控制台中，单击**启动器 (Launcher)**。

步骤 2 单击**书签 (Bookmarks)**。

步骤 3 单击**添加书签 (Add a Bookmark)**。

步骤 4 输入应用的**名称 (Name)**（从“导出应用”(Export Applications) 页面上的应用**复制名称**）。

步骤 5 输入您的用户将用于访问应用的 **URL**（从“导出应用”(Export Applications) 页面上的应用**复制 URL**）。

步骤 6 （可选）上传应用的**徽标**图像（从“导出应用”(Export Applications) 页面上的应用**下载徽标**）。

步骤 7 默认情况下，新书签会向所有用户显示。您可以使用 Duo 组 (Duo groups) 来控制哪些用户可以看到书签。选中**仅允许来自特定组中的用户的访问权限 (Only allow access from users in certain groups)** 或**显示仅向特定用户组显示此书签 (Show this bookmark to only certain groups of users)** 复选框，并开始在组选择字段中键入以检索 Duo 组列表。单击包含要在启动器中查看新书签的用户的每个组。

步骤 8 单击**添加 (Add)** 或**保存 (Save)**。

将应用导出到 Microsoft Azure

请按照以下步骤将思科安全产品应用添加到 Microsoft Azure 门户。

开始之前

- 您必须有权访问思科 SecureX 登录中的应用。
- 您必须在 Microsoft Azure 中具有超级管理员权限。

步骤 1 通过超级管理员权限登录 https://portal.azure.com。

步骤 2 单击 **Azure Active Directory**。

步骤 3 在左侧菜单中，选择**企业应用 (Enterprise applications)**。

步骤 4 单击**新建应用 (New application)** → **非图库应用 (Non-gallery application)**。

步骤 5 输入应用的**名称 (Name)**（从“导出应用”(Export Applications) 页面上的应用**复制名称**）。

步骤 6 （可选）上传应用的徽标图像（从“导出应用”(Export Applications) 页面上的应用**下载徽标**）。

步骤 7 单击**设置单点登录 (Set up single sign on)**。

步骤 8 选择**已链接 (Linked)**。

步骤 9 将**登录 URL (Sign on URL)** 设置为用于访问应用的URL（从“导出应用”(Export Applications) 页面上的应用**复制 URL**），然后单击**保存 (Save)**。

步骤 10 在应用的左侧菜单中，单击**用户和组 (Users and groups)**。

步骤 11 分配用户或组到应用。只有分配的用户在访问 https://myapplications.microsoft.com 时才会看到应用。