管理用户

从**设置**（齿轮图标）> **管理 (Administration)** 页面管理您的用户帐户。

Secure Email Threat Defense 使用思科 SecureX 登录 SSO 解决方案，以便进行用户身份验证管理。有关 SecureX 登录的信息，请参阅 https://cisco.com/go/securesignon。

注意：如果您是 Cisco SecureX Threat Response、Cisco Secure Malware Analytics（以前称为 Cisco Threat Grid）或 Cisco SecureEndpoint（以前称为 AMP）的客户，请务必使用现有的 SecureX 登录凭证进行登录。如果您不是现有用户，则必须创建一个新的 SecureX 登录帐户

虽然 SecureX 登录允许您使用其他类型的帐户进行登录，但我们建议您使用 SecureX 登录帐户，以便保持您的思科安全产品帐户的连接。

多帐户访问

您可以使用同一个 SecureX 登录帐户访问多个 Secure Email Threat Defense 实例。这样可以更轻松地跟踪每个实例，而无需注销并使用单独的 SecureX 登录帐户重新登录。

按照创建新用户，第 42 页中的步骤将用户添加到其他 Secure Email Threat Defense 实例。使用相同 SecureX 登录帐户的帐户将可从其“用户”(User) 菜单来访问。请注意，此访问权限仅限于同一地区（北美或欧洲）的 Secure Email Threat Defense 实例。

用户角色

基于角色的访问控制 (RBAC) 允许您在应用中为用户提供不同级别的控制或访问权限。Secure Email Threat Defense 可以在下表中描述的角色中创建用户。

表 1　　用户角色

角色	说明
super-admin	这些用户可以访问 Secure Email Threat Defense 中的所有功能。他们可以更改设置和策略，并对邮件进行重新分类和补救。
admin	这些用户具有超级管理员的所有功能，但不能创建、编辑或删除超级管理员或管理员用户。
analyst	这些用户可以使用搜索和见解功能。他们可以对邮件进行重新分类和补救，但不能从用户邮箱中删除邮件。他们无法更改帐户设置或策略，也无法创建新用户。
只读	这些用户可以使用搜索和见解功能。他们无法对邮件进行重新分类或补救，无法更改帐户设置或策略，也无法创建新用户。

注意：您无法编辑现有用户的角色。如果您想更改用户的角色，请删除现有用户，然后使用相同的邮件地址和所需角色来创建新用户。

创建新用户

完成以下步骤以创建新用户：

1. 选择**设置**（齿轮图标）> **管理 (Administration)** > **用户 (Users)**。
2. 点击**添加新用户**。
3. 输入用户的凭证，选择角色，然后点击**创建 (Create)**。

   注意：用户的邮箱地址*必须*与其 SecureX 登录帐户使用的邮箱地址相匹配。

用户收到主题为**欢迎使用 (Welcome to)思科安全邮件威胁防御** 的邮件。他们必须按照邮件中的说明来设置 SecureX 登录帐户（如果还没有）并登录。

删除用户

完成以下步骤以删除用户：

1. 选择**设置**（齿轮图标）> **管理 (Administration)** > **用户 (Users)**。
2. 点击用户名旁边的垃圾桶图标。
3. 在“确认删除”(Confirm Deletion) 对话框中点击**删除 (Delete)** 以完成操作。

一条状态消息将显示删除已完成。此操作会从Secure Email Threat Defense中删除用户的帐户，但不会删除其SecureX登录帐户。如果要从多个 Secure Email Threat Defense 实例中删除用户，则必须为每个实例完成这些步骤。

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。