使用Microsoft O365配置电子邮件加密外接程序

目录

简介

本文档介绍如何通过Microsoft Office 365配置思科邮件加密服务加载项集中部署。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全电邮网关
- 思科安全邮件加密服务（以前称为思科注册信封服务）
- Microsoft O365套件(Exchange、Entra ID、Outlook)

使用的组件

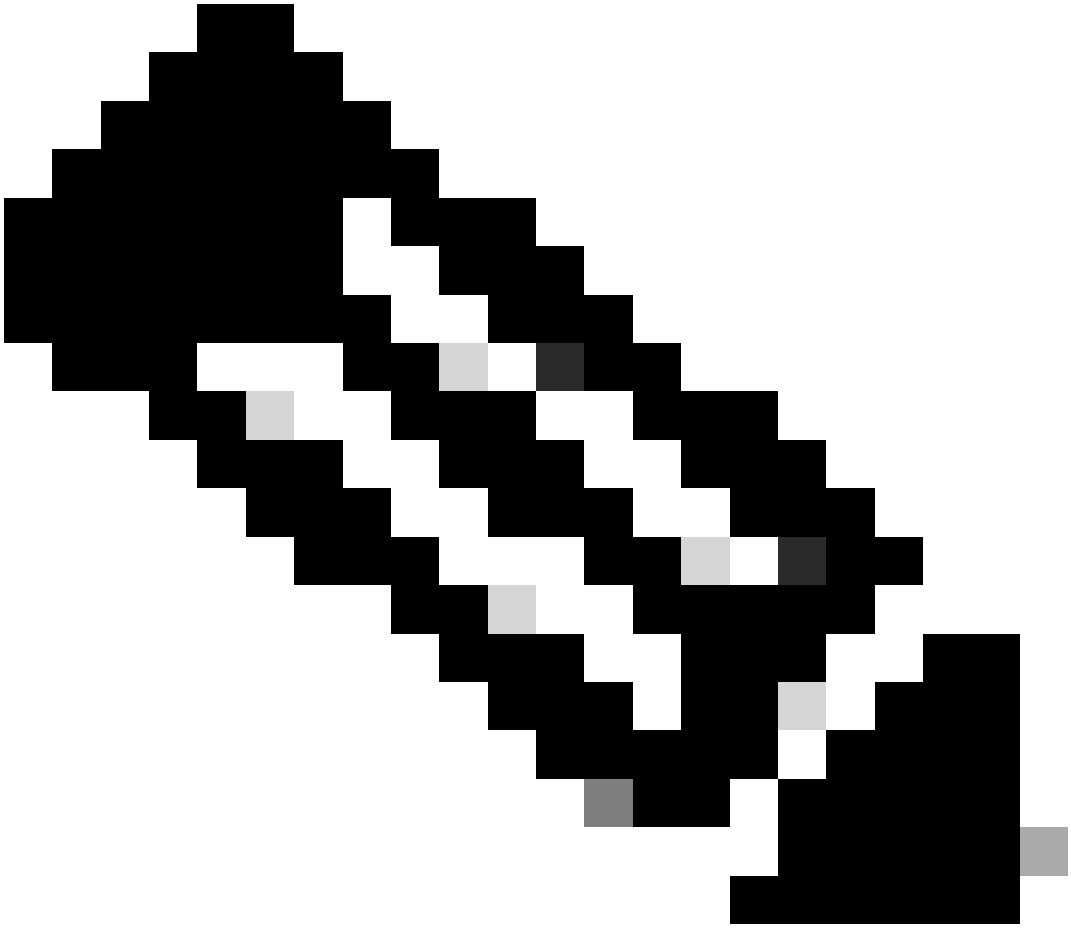
本文档中的信息基于以下软件和硬件版本：

- 思科电子邮件加密插件10.0.0
- Microsoft Exchange Online
- Microsoft Entra ID（以前称为Azure AD）
- Outlook for O365 (macOS、Windows)

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

Cisco Secure Email Encryption Service Add-in允许最终用户通过单击即可直接从Microsoft Outlook对邮件进行加密。此加载项可在Microsoft Outlook（适用于Windows和macOS）和Outlook Web App上部署。



注意：本文档非常适合计划使用外接程序Office 365/Microsoft 365订阅的所有最终用户，并且计划使用外接程序的所有最终用户都是已注册的Cisco安全邮件加密服务用户。

部署思科安全邮件加密服务加载项的最佳实践

- 测试阶段-将插件部署到某个部门或职能部门内一小群最终用户。评估结果，如果成功，则进入下一阶段。
- 试点阶段-将插件部署到来自不同部门和职能部门的更多最终用户。评估结果，如果成功，则进入下一阶段。

- 生产阶段-将加载项部署到所有用户。

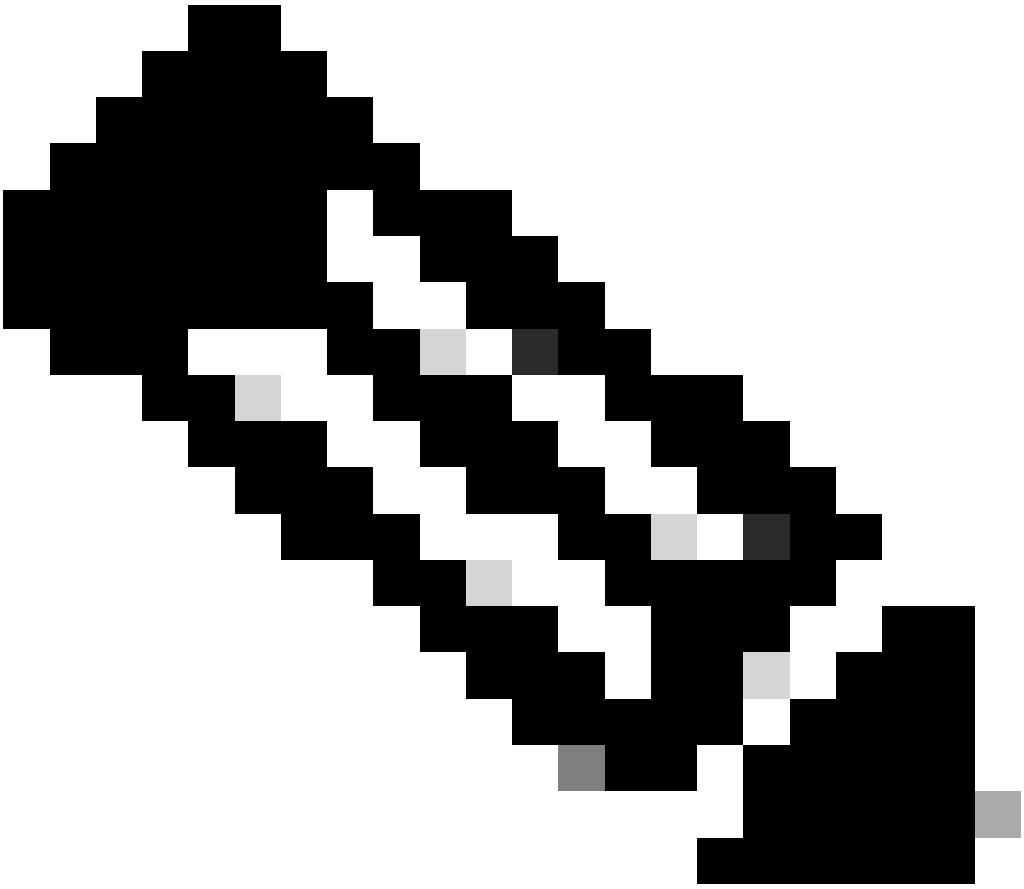
配置

思科安全邮件加密服务加载项应用注册

1. 至少以云应用管理员(Microsoft 365管理中心)的身份登录Microsoft 365管理中心。

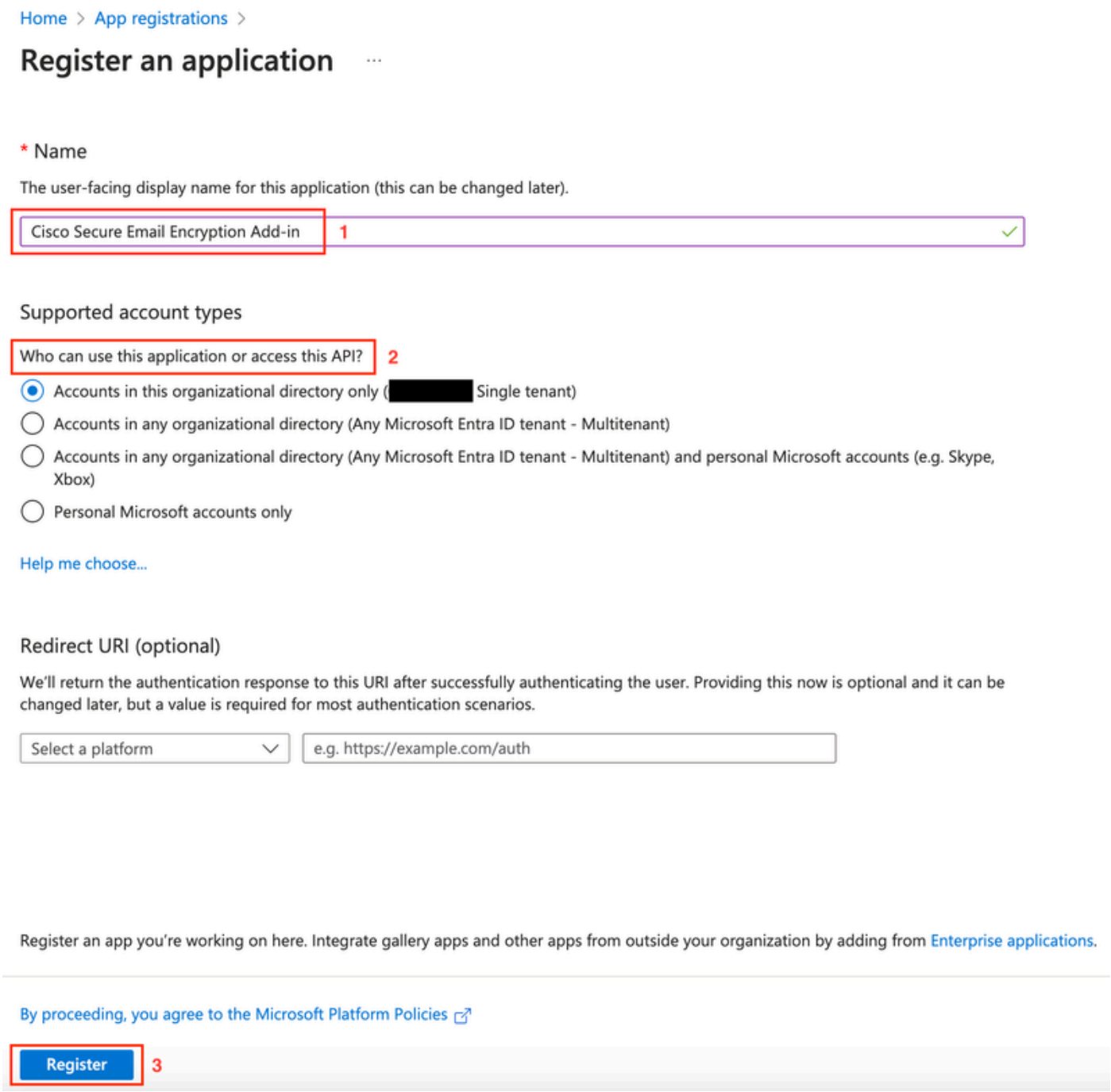
2. 在左侧菜单中，展开Admin Centers并单击Identity。

3. 定位至Identity > Applications > App registrations并选择 New registration.



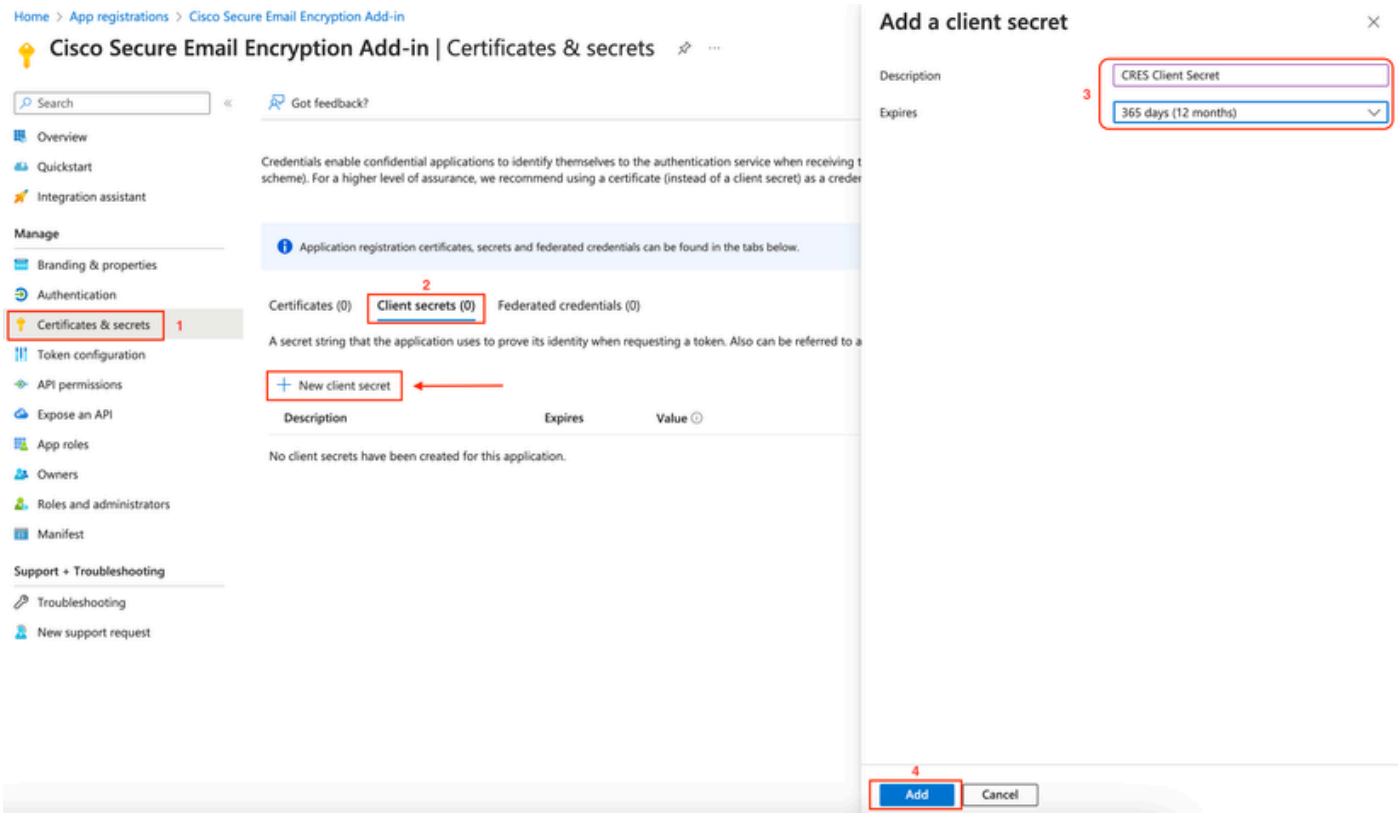
注意：如果您有权访问多个租户，请使用右上角菜单中的“设置”图标，从“目录+订阅”菜单切换到要在其中注册应用程序的租户。

4. 输入应用产品显示名称，选择可以使用该应用产品的帐户，然后单击Register。



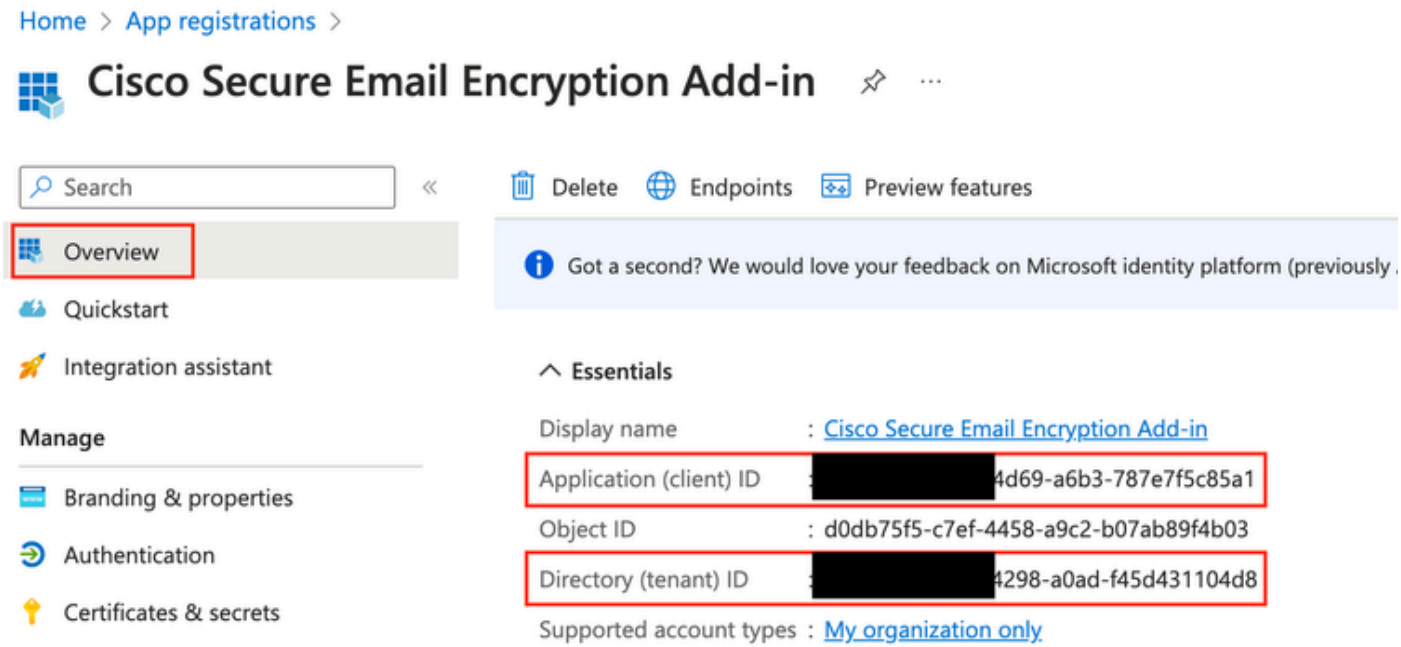
注册应用程序

5. 成功注册后，导航到Certificates & Secrets下的应用程序以配置客户端密钥。根据组织合规性选择到期日期。

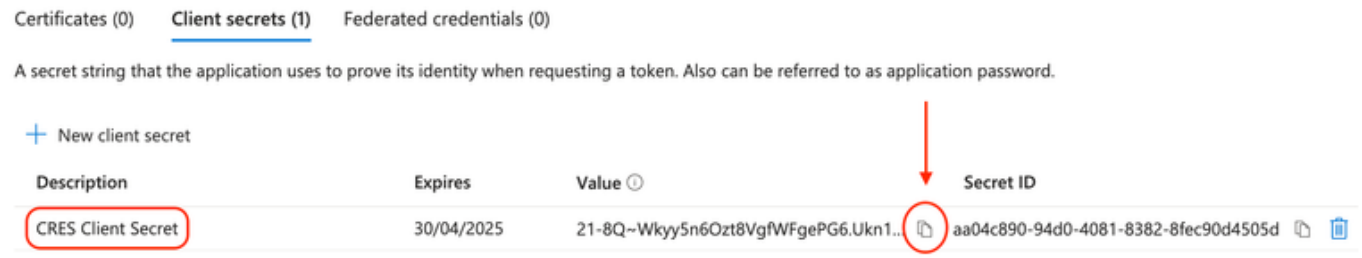


配置客户端密钥

6. 从已注册应用程序的“概述”页中，复制Application (client) ID 和Directory (tenant) ID。复制上一步中生成的证书和密钥(Certificates & Secrets)中的**Client Secret** 。



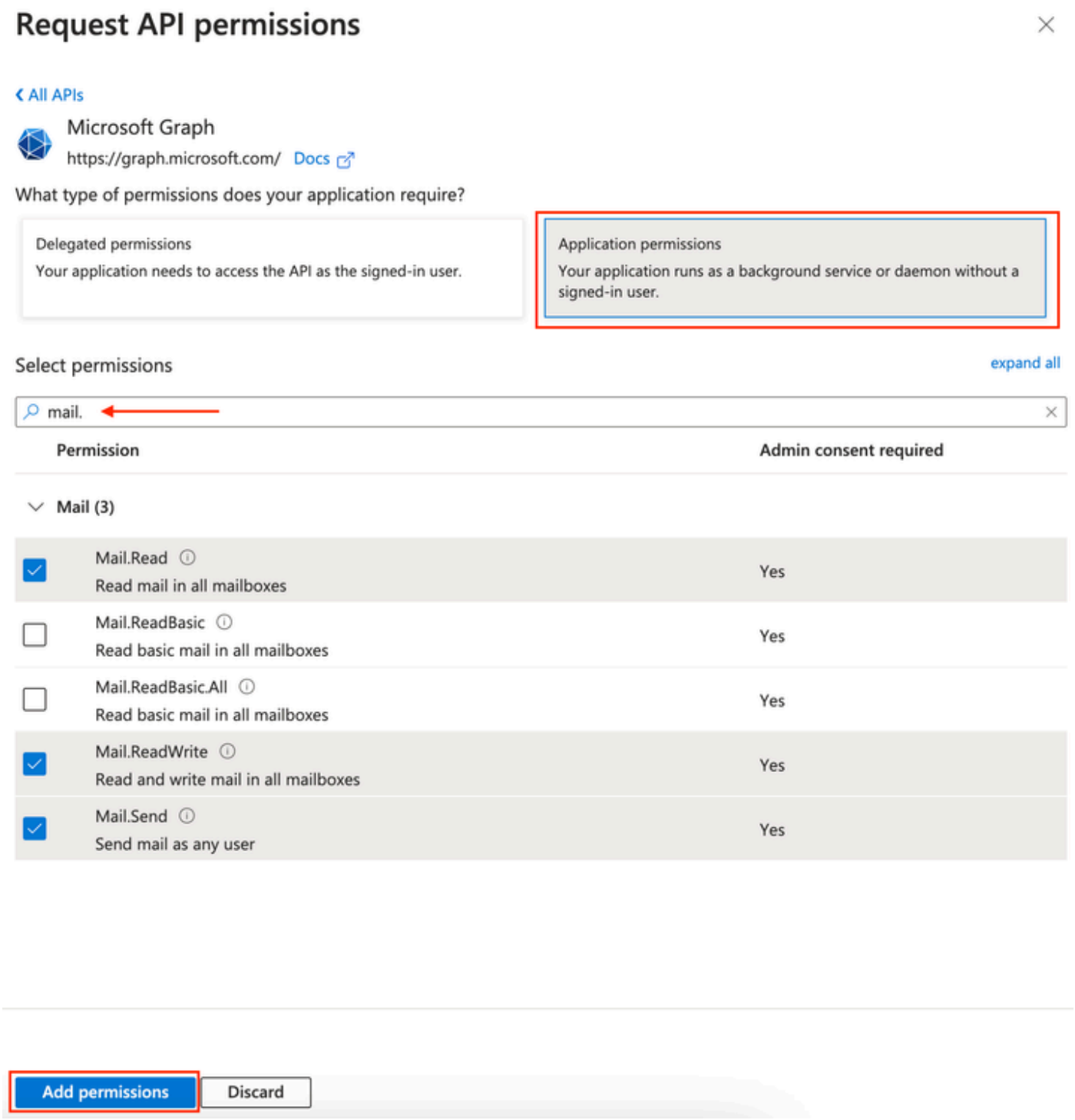
*Entra ID*应用概述



复制客户端密码

7. 定位至“**注册的**电子邮件加密应用程序” ，然后定位至API permissions。单击Add a permission并选择Microsoft Graph应用程序所需的权限：

- Mail.Read
- **邮件。读写**
- Mail.Send
- User.Read.All



*Microsoft Graph*权限配置

7. 单击Grant Admin Consent for <tenant-name>，让应用程序代表组织访问权限。

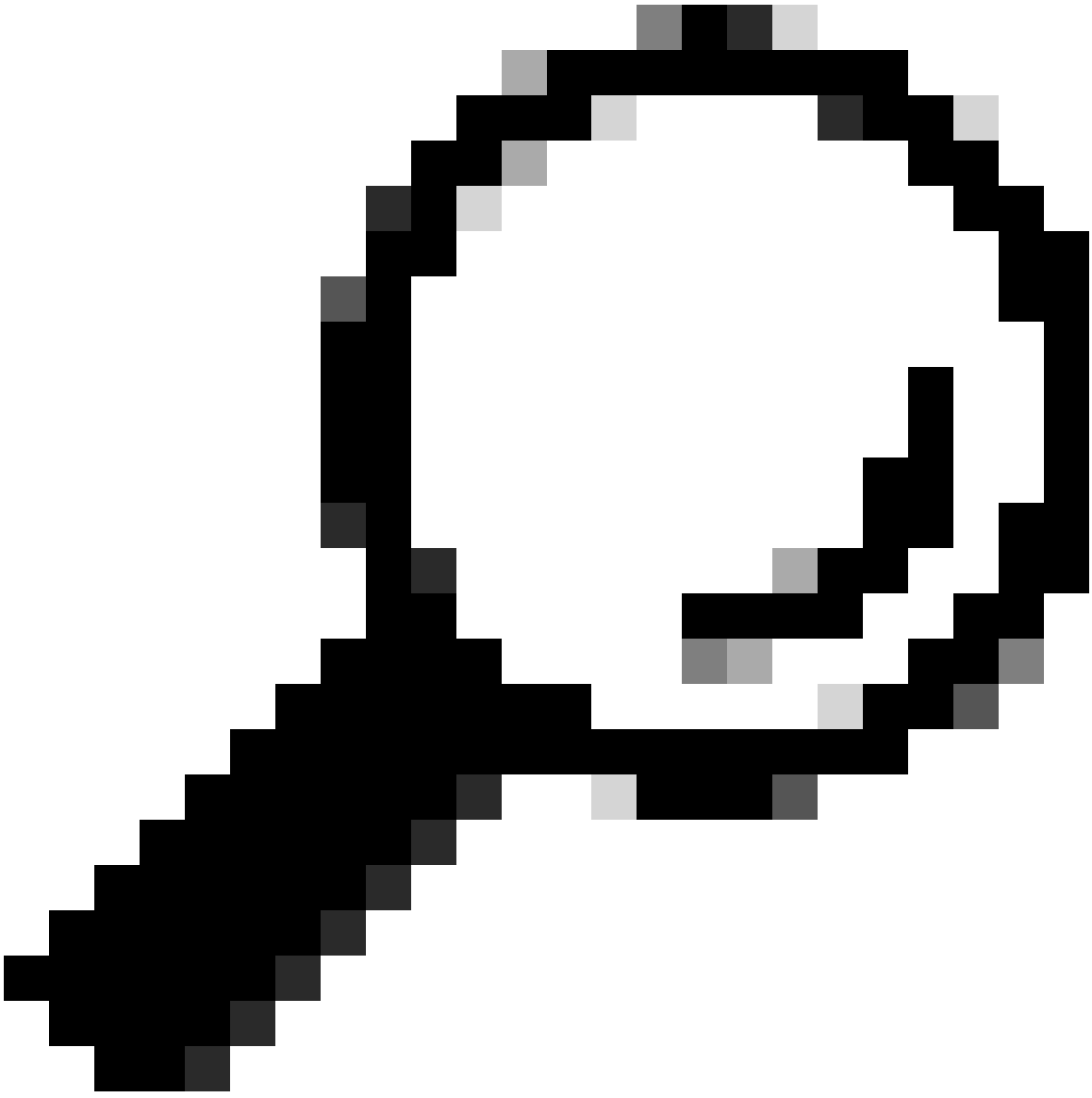
*Microsoft Graph API*权限

在思科安全邮件加密(CRES)管理员门户上配置域和加载项设置

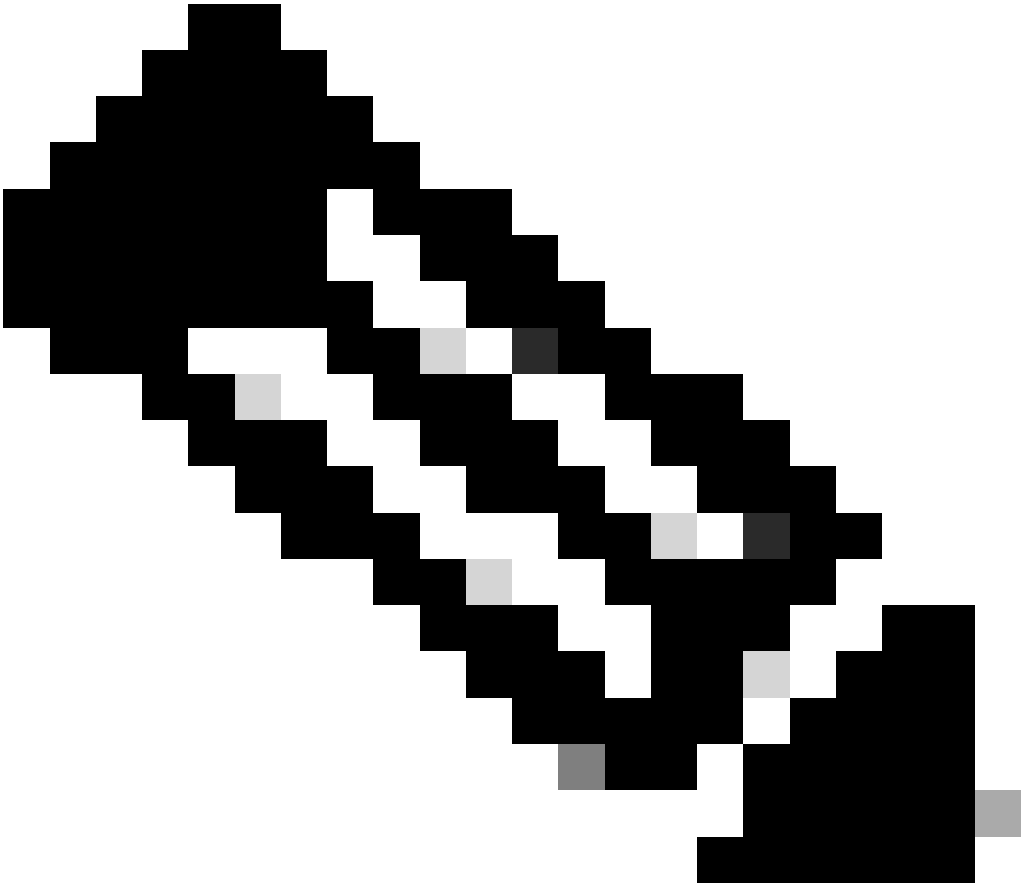
1. 以帐户管理员身份登录思科安全邮件加密服务(CRES)管理员门户。(安全邮件加密服务)

2. 定位至Accounts > Manage Accounts。点击分配给您组织的帐号，或您计划在其上配置邮件加密加载项的帐户。

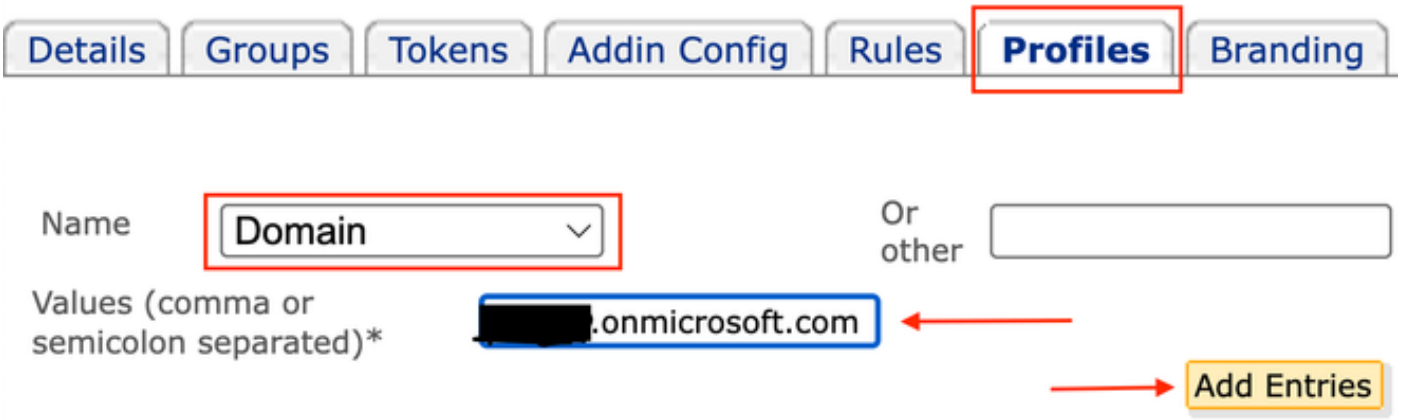
3. 导航至 Profiles，选择“**名称”类型**为“域”，然后在“值”下输入电子邮件域名。点击 **Add Entries** 并等待5到10秒。（在成功添加之前，请勿刷新浏览器页面或导航到其他页面）。



提示：重复相同的步骤以添加要在您的组织中使用邮件加密服务的其他邮件域。



注意：请与思科技术支持中心联系，以获取在CRES管理员门户上添加的邮件域。

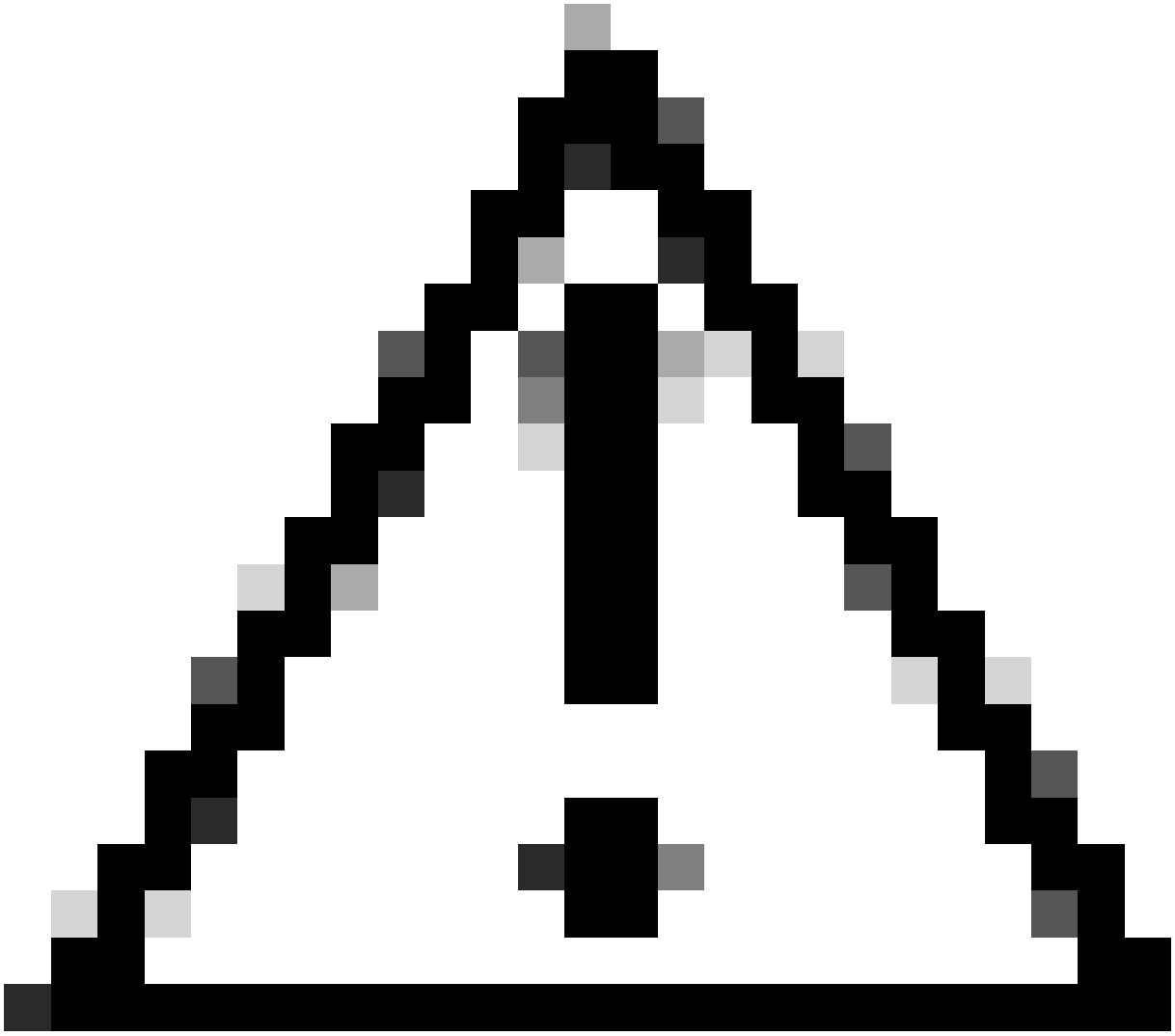


*CRES*管理员门户配置文件

4. 定位至“选Add-in Config 项卡”。

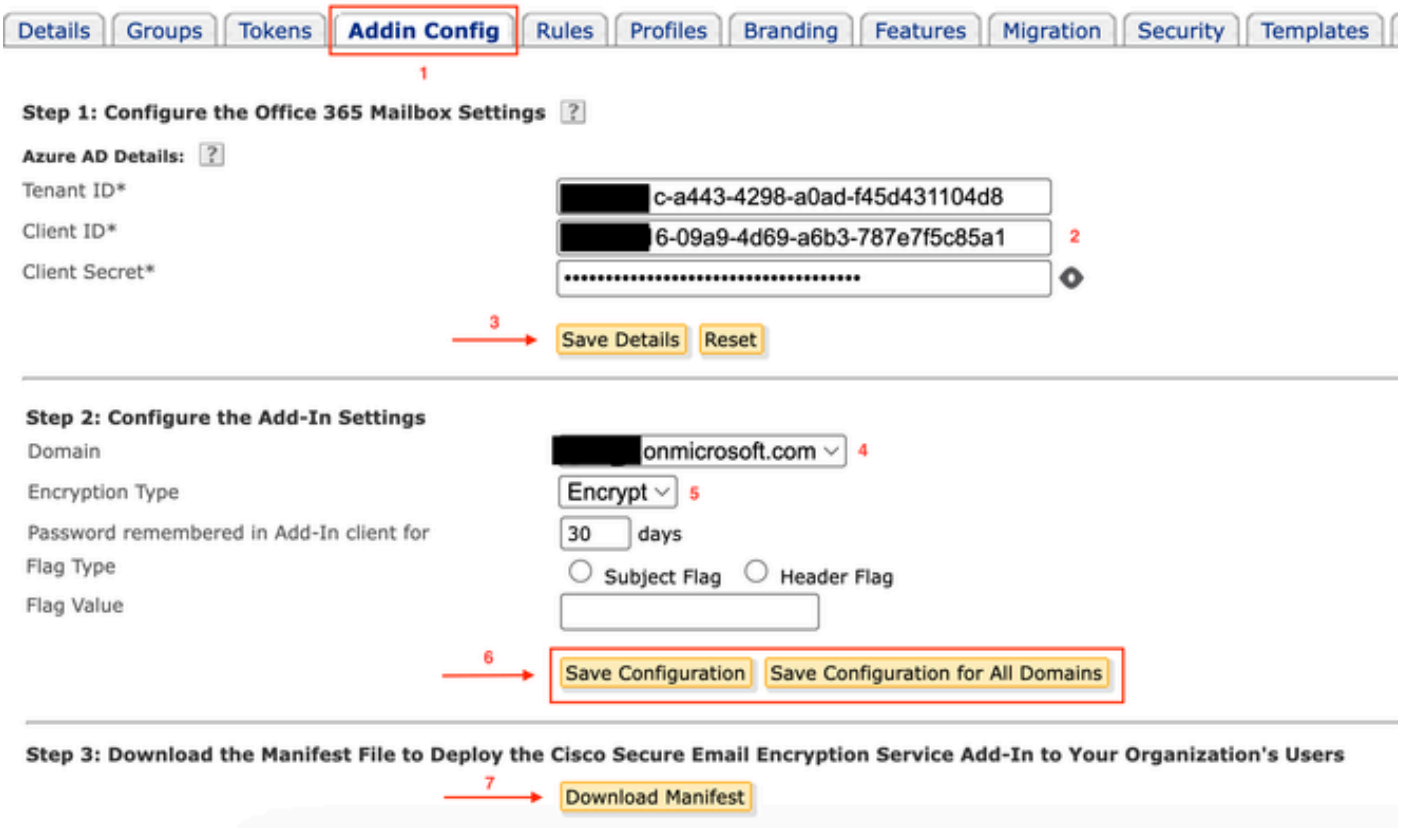
第1步：在Azure AD Details下输入从Entra ID获取的租户、客户端ID和密钥。单击。Save Details

第2步：选择域、加密类型，然后点击Save Configuration。使用Save Configuration对所有域应用相同的设置到所有添加的域。



注意：如果没有同时完成第1步和第2步，请勿导航到其他页面。如果第2步未同时完成，则不会保存Azure AD详细信息。

第3步：点击Download Manifest。

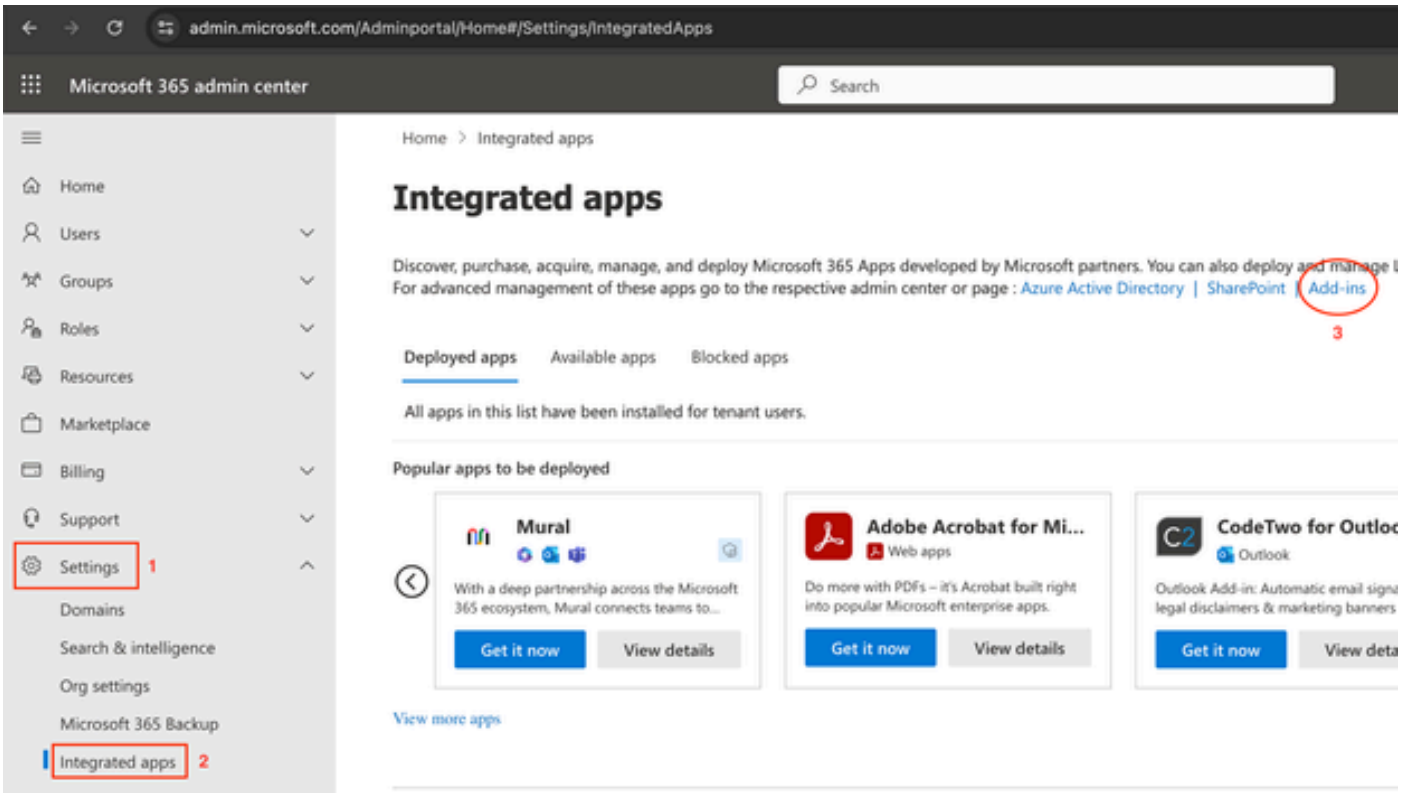


*CRES*管理员门户添加配置

将清单文件上载到Microsoft 365以部署邮件加密服务加载项

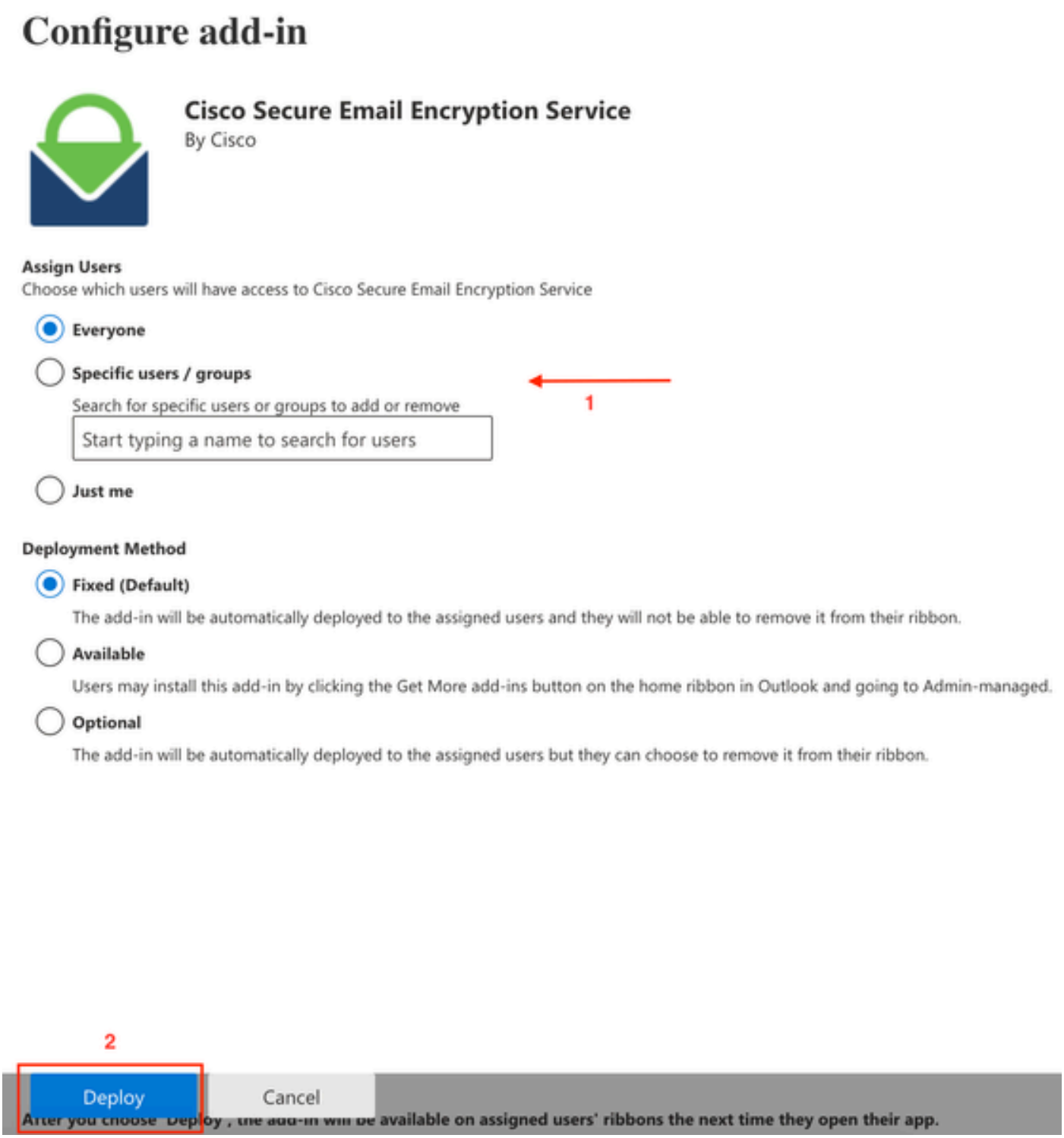
1. 以管理员身份登录到Microsoft 365管理中心。(Microsoft 365管理中心)。

2. 导航至Settings > Integrated apps 并单击"**加载项**" 。



3. 单击Deploy Add-in并选择Upload Custom Apps。选择I have the manifest file (.xml) on this device并上传从上一步的Cisco Email Encryption Service Admin Portal下载的文件。单击。Upload

4. 在下一步中，分配需要访问思科安全邮件加密服务的用户。对于分阶段部署，请选择Specifc Users/groups并点击Deploy。

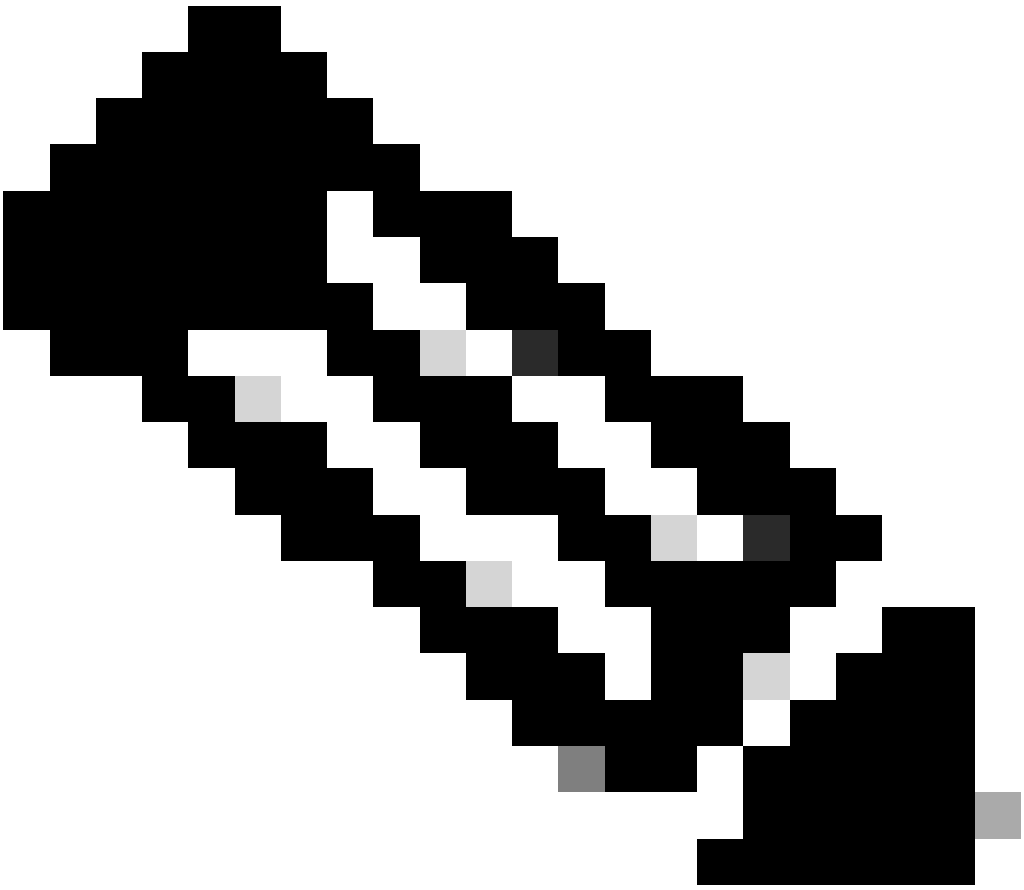


5. 加载项成功部署后，可能需要长达12小时才能显示在最终用户功能区（Outlook客户端）上。

验证

使用本部分可确认配置能否正常运行。

1. 启动Outlook for Office 365/Microsoft 365或Outlook Web App，撰写要加密的邮件，并向其中至少添加一个有效收件人。



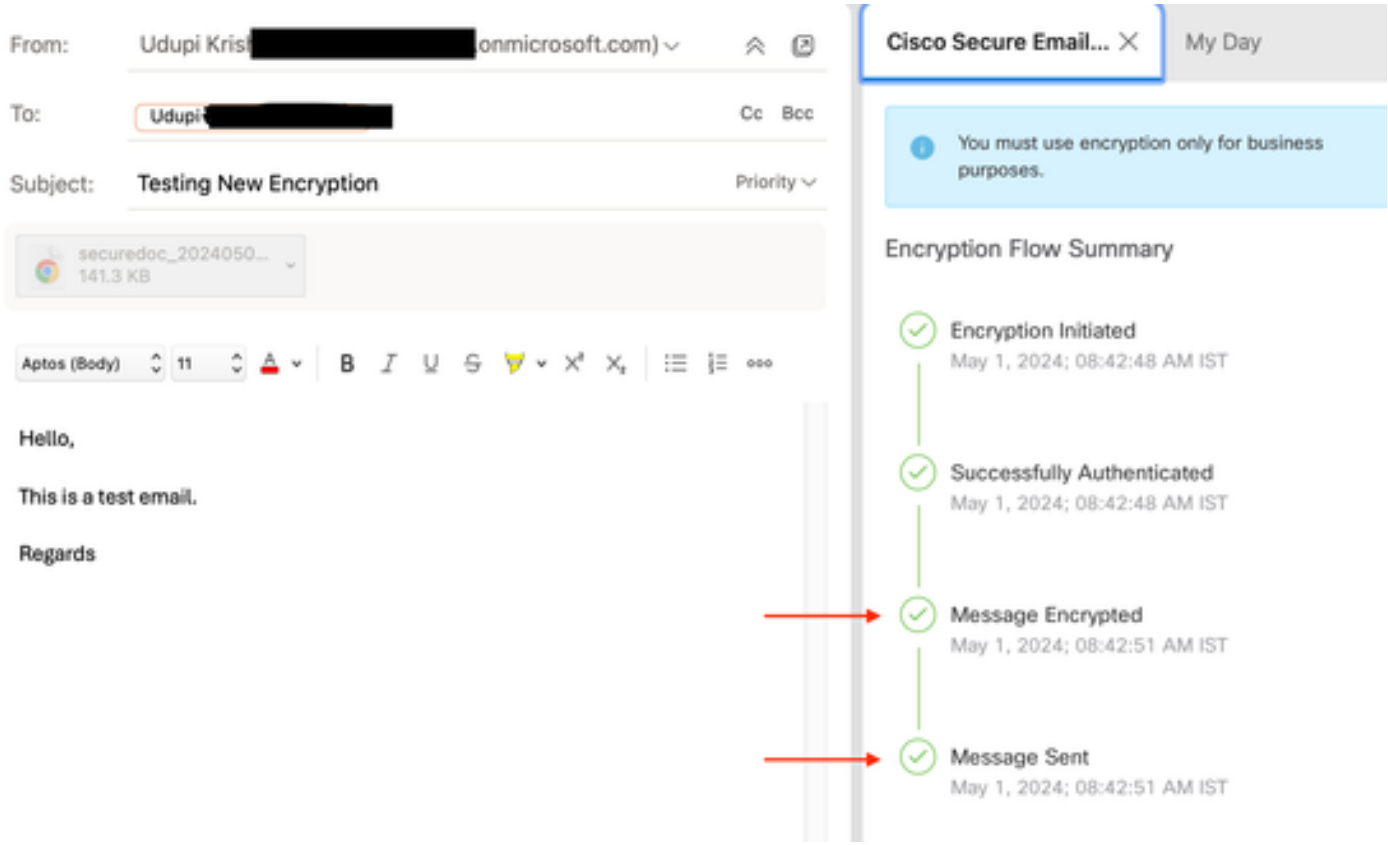
注意：如果“加密类型”(Encryption Type)（由管理员设置）为“加密”(Encrypt)，请确保已完成消息并添加了有效收件人，然后再继续下一步。第3步之后，消息将被加密并立即发送。

---

2. 打开/单击Cisco Secure Email Encryption Service插件。

- 在Outlook Web App中，单击省略号图标（位于“发送”和“丢弃”按钮附近），然后单击Cisco Secure Email Encryption Service。
- 在Outlook for Windows或MacOS上，从功能区或工具栏中单击**加密**。
- 如果您使用的是Outlook for MacOS版本16.42或更高版本，并且使用的是新的Outlook界面，请从工具栏中单击Cisco Secure Email Encryption Service。

3. 输入您的凭证并单击Sign in。(仅当加密类型是Flag时，才单击Send)。



*Microsoft Outlook*加密状态

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 思科安全邮件加密服务帐户管理员用户指南

    - 思科安全邮件加密服务插件用户指南
- Microsoft Entra应用程序注册指南
- 思科技术支持和下载

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）。