使用Duo配置安全邮件加密服务SAML SSO

目录

简介

先决条件

- 要求
- 使用的组件

配置

验证

常见错误

相关信息

简介

本文档介绍如何将思科安全邮件加密服务（以前称为思科注册信封服务[CRES]）与Duo for Security Assertion Markup Language(SAML)单点登录(SSO)集成。

先决条件

要求

Cisco 建议您了解以下主题：

- 对Cisco Secure Email Encryption Service管理门户的管理访问权限。
- 对Duo Admin Panel具有管理权限。
- 对Microsoft Azure门户的管理访问权限。
- 按照Duo用户注册文档中的说明在Duo管理面板中注册用户。

使用的组件

本文档中的信息基于SAML 2.0。

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。

配置

若要在Cisco Secure Email Encryption Service、Duo和Microsoft Azure Active Directory之间配置SAML SSO，请使用此过程。配置完成后，分配给企业应用的用户可以通过Duo向Cisco安全邮件加密服务门户进行身份验证。

步骤1.登录到Duo Admin Panel。

步骤2.导航到Applications。

步骤3.选择保护应用。

步骤4.选择通用SAML服务提供商，然后单击保护。

步骤5.复制单点登录URL。

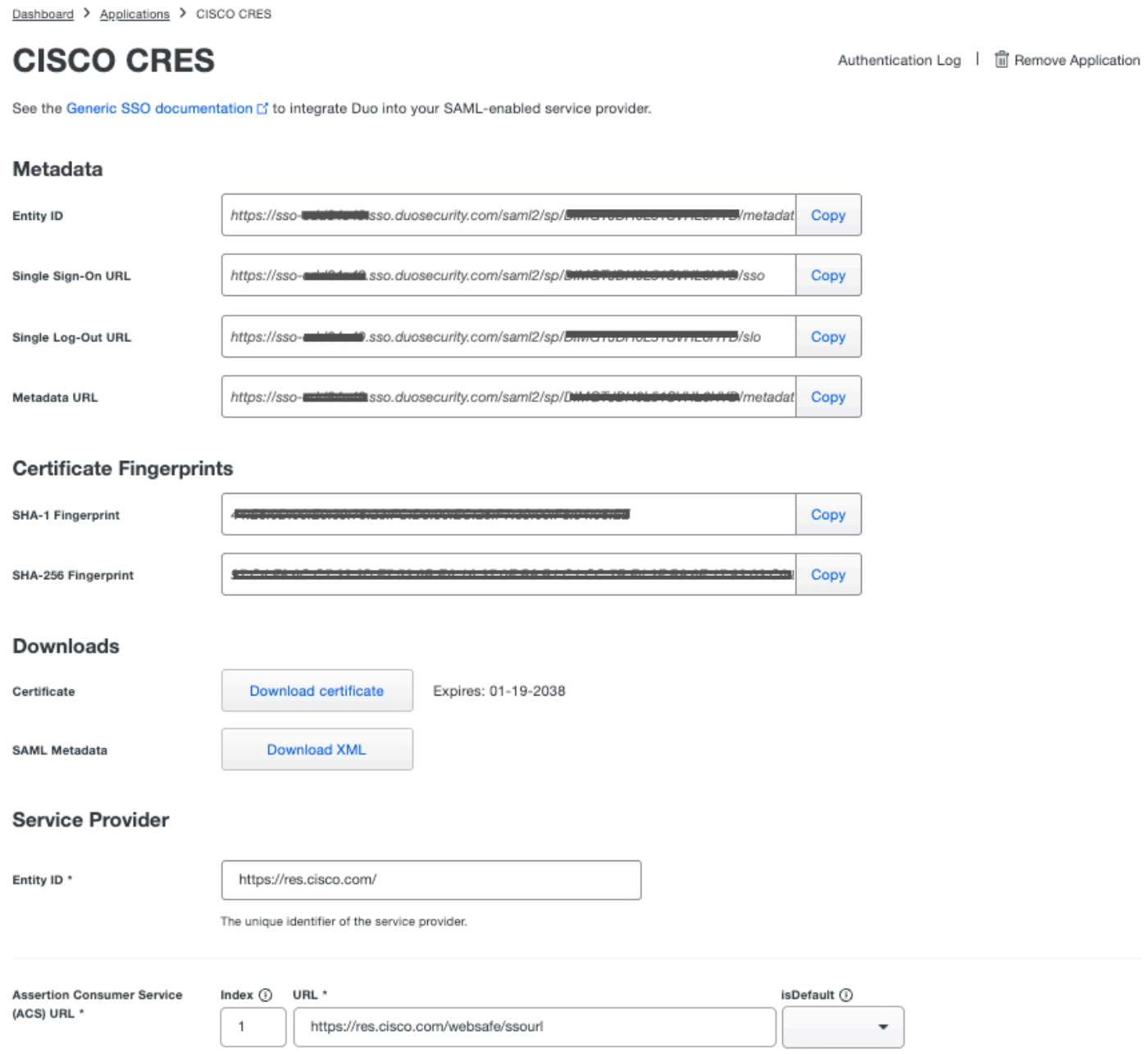
步骤6.选择下载证书。

步骤7.选择下载XML。

第8步：在服务提供商>实体ID *中，输入思科安全邮件加密服务实体ID。

第9步：在服务提供商>断言消费者服务(ACS)URL *中，输入思科安全邮件加密服务ACS URL。

步骤10.在设置>名称中，输入新应用程序的名称，然后选择保存，如图所示：



步骤11.登录到Cisco Secure Email Encryption Service管理门户。

步骤12.导航到Accounts，然后选择Account Number的超链接。

步骤13.在Details选项卡中，将Authentication Method设置为SAML 2.0。

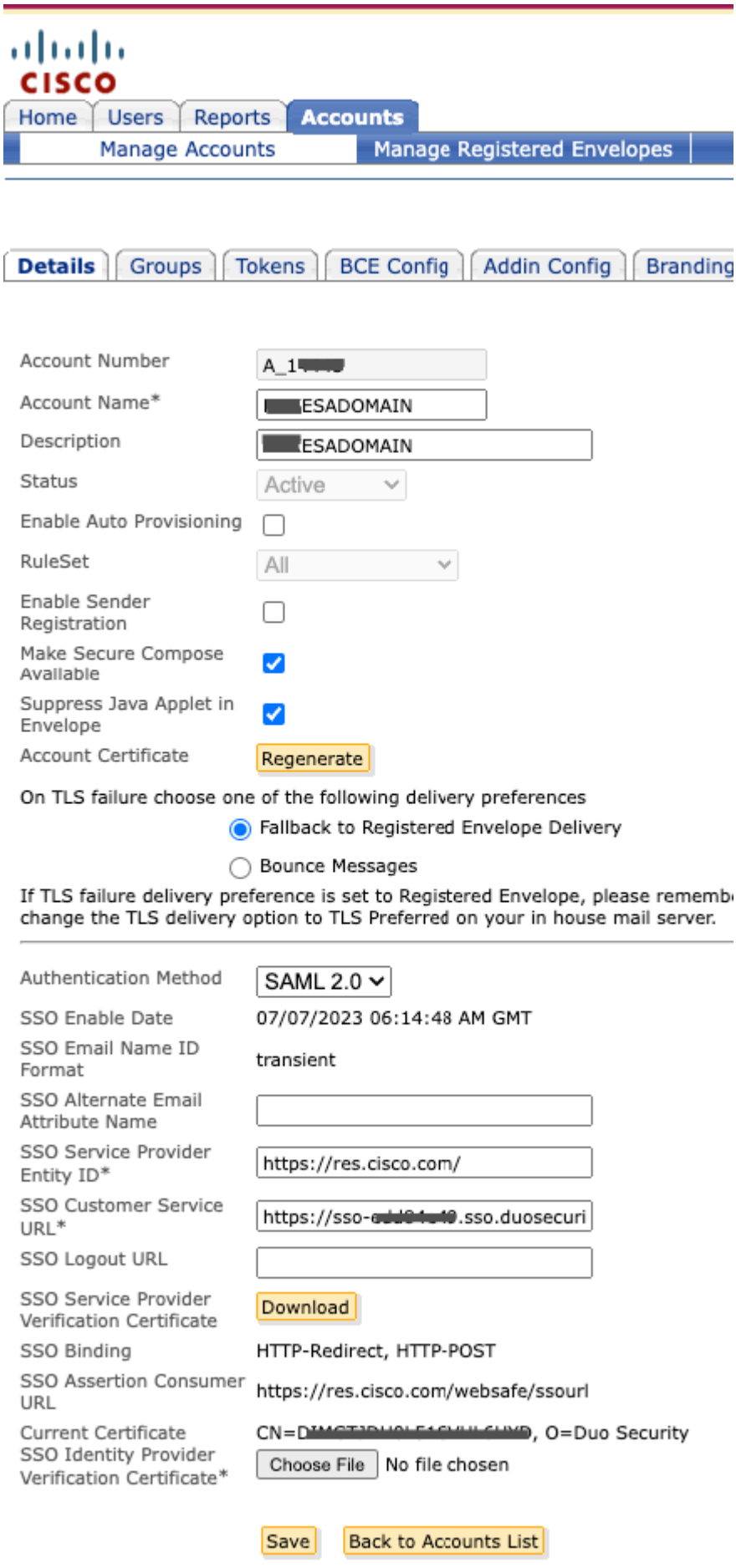
步骤14.将SSO Alternate Email Attribute Name留空。

第15步：在SSO服务提供商实体ID中，输入思科安全邮件加密服务实体ID。

第16步：在SSO客户服务URL中，输入在步骤5中复制的URL。

步骤17.将SSO注销URL留空。

第18步：在当前证书SSO身份提供程序验证证书中，点击选择文件，然后上传在步骤6中下载的证书，如图所示：



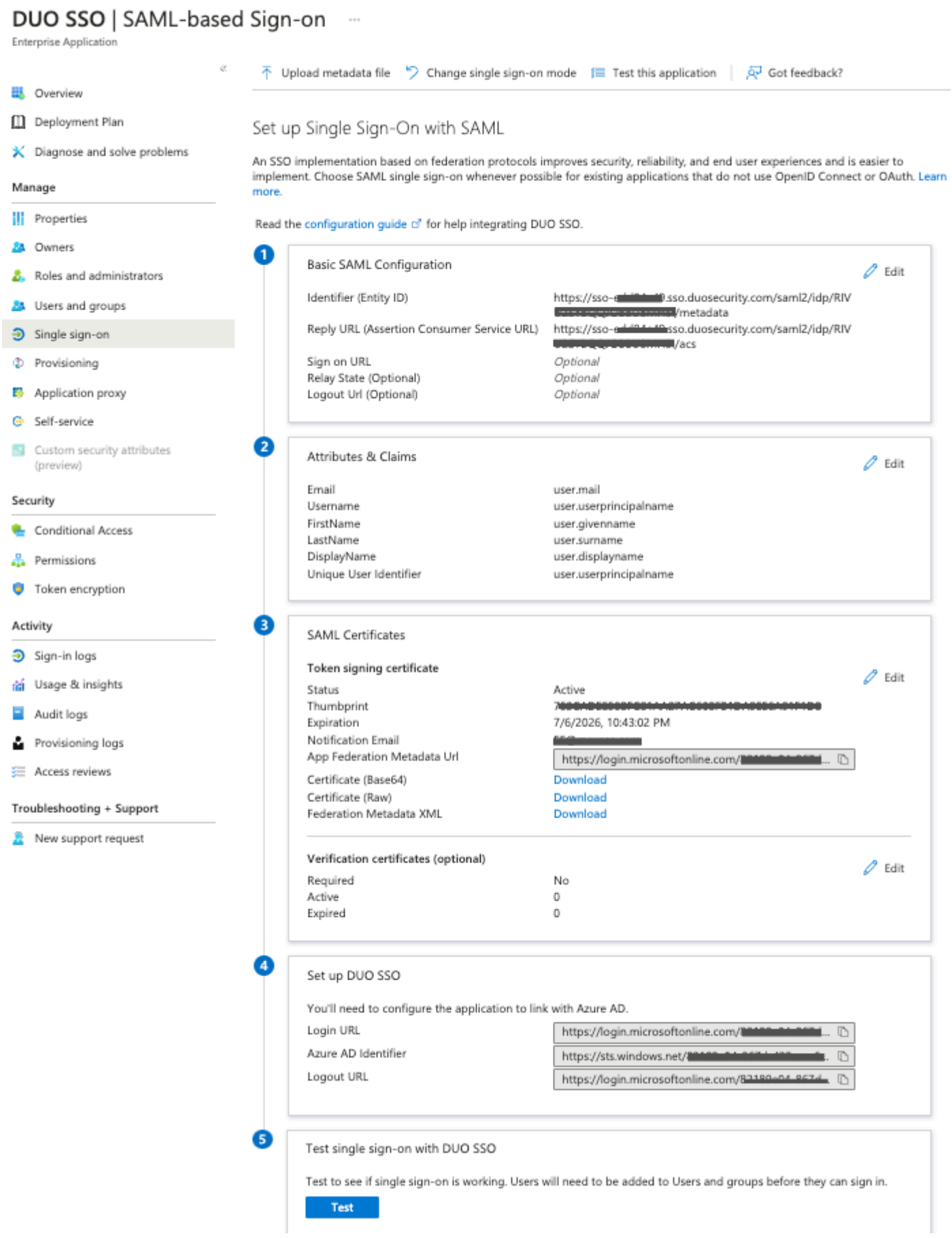
步骤19.登录到Microsoft Azure门户。

第20步：导航到Azure Active Directory >企业应用程序>新建应用程序>创建自己的应用程序。

步骤21.输入应用程序名称，选择“集成未在库中找到的所有其他应用程序（非库）”，然后单击“创建”。

第22步：选择Assign users and groups，添加需要访问Cisco Secure Email Encryption Service的用户，然后单击Assign。

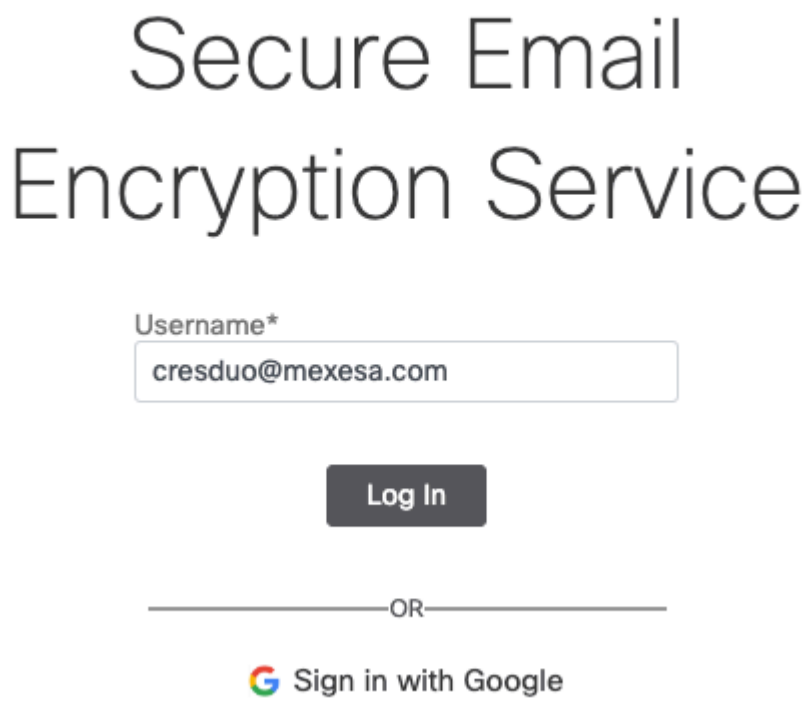
步骤23.选择单点登录> SAML >上传元数据文件，然后选择步骤7中下载的文件，如图所示：


DUO SSO | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Got feedback?
Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes (preview)
Security
Conditional Access
Permissions
Token encryption
Activity
Sign-in logs
Usage & insights
Audit logs
Provisioning logs
Access reviews
Troubleshooting + Support
New support request
Set up Single Sign-On with SAML
An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.
Read the configuration guide for help integrating DUO SSO.
1
Basic SAML Configuration
Edit
Identifier (Entity ID)
https://sso-[redacted].sso.duosecurity.com/saml2/idp/RIV[redacted]/metadata
Reply URL (Assertion Consumer Service URL)
https://sso-[redacted].sso.duosecurity.com/saml2/idp/RIV[redacted]/acs
Sign on URL
Optional
Relay State (Optional)
Optional
Logout Url (Optional)
Optional
2
Attributes & Claims
Edit
Email
user.mail
Username
user.userprincipalname
FirstName
user.givenname
LastName
user.surname
DisplayName
user.displayname
Unique User Identifier
user.userprincipalname
3
SAML Certificates
Token signing certificate
Edit
Status
Active
Thumbprint
[redacted]
Expiration
7/6/2026, 10:43:02 PM
Notification Email
[redacted]
App Federation Metadata Url
https://login.microsoftonline.com/[redacted]...
Certificate (Base64)
Download
Certificate (Raw)
Download
Federation Metadata XML
Download
Verification certificates (optional)
Edit
Required
No
Active
0
Expired
0
4
Set up DUO SSO
You'll need to configure the application to link with Azure AD.
Login URL
https://login.microsoftonline.com/[redacted]...
Azure AD Identifier
https://sts.windows.net/[redacted]...
Logout URL
https://login.microsoftonline.com/[redacted]...
5
Test single sign-on with DUO SSO
Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.
Test

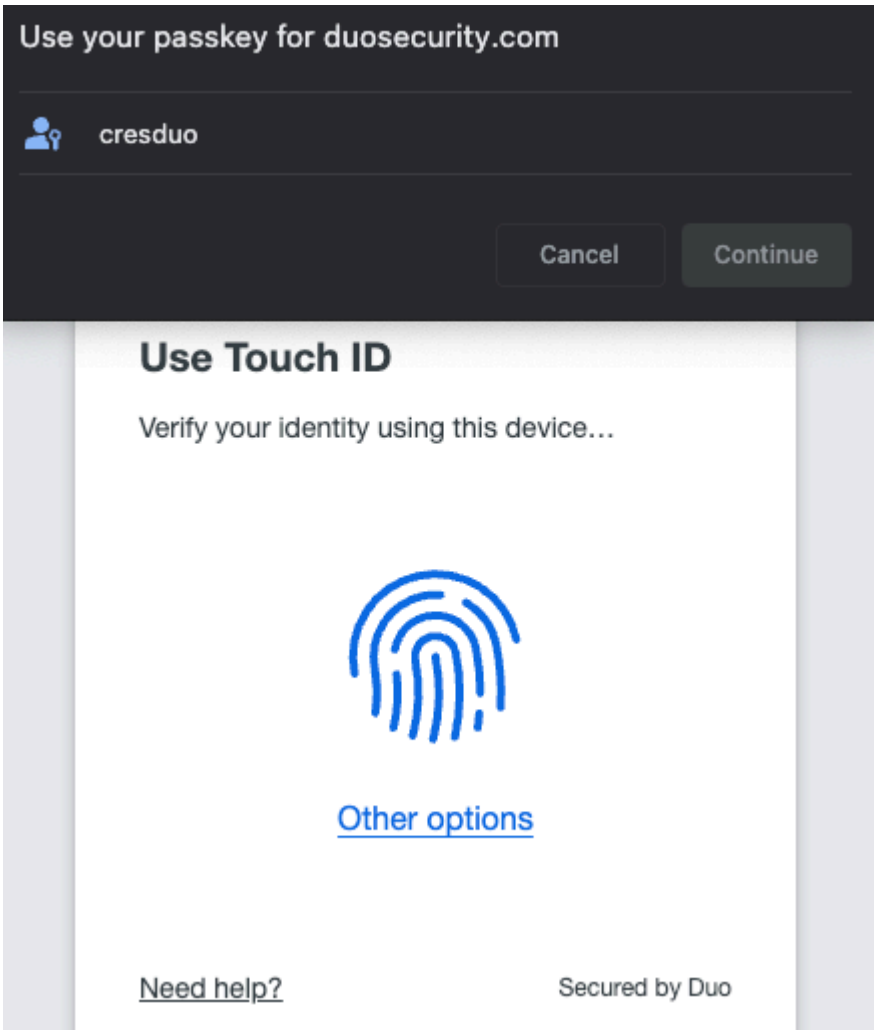
验证

通过确认已分配用户重定向到Duo进行身份验证，然后在身份验证成功后返回到Cisco安全邮件加密服务门户，验证SAML SSO配置是否按预期工作。

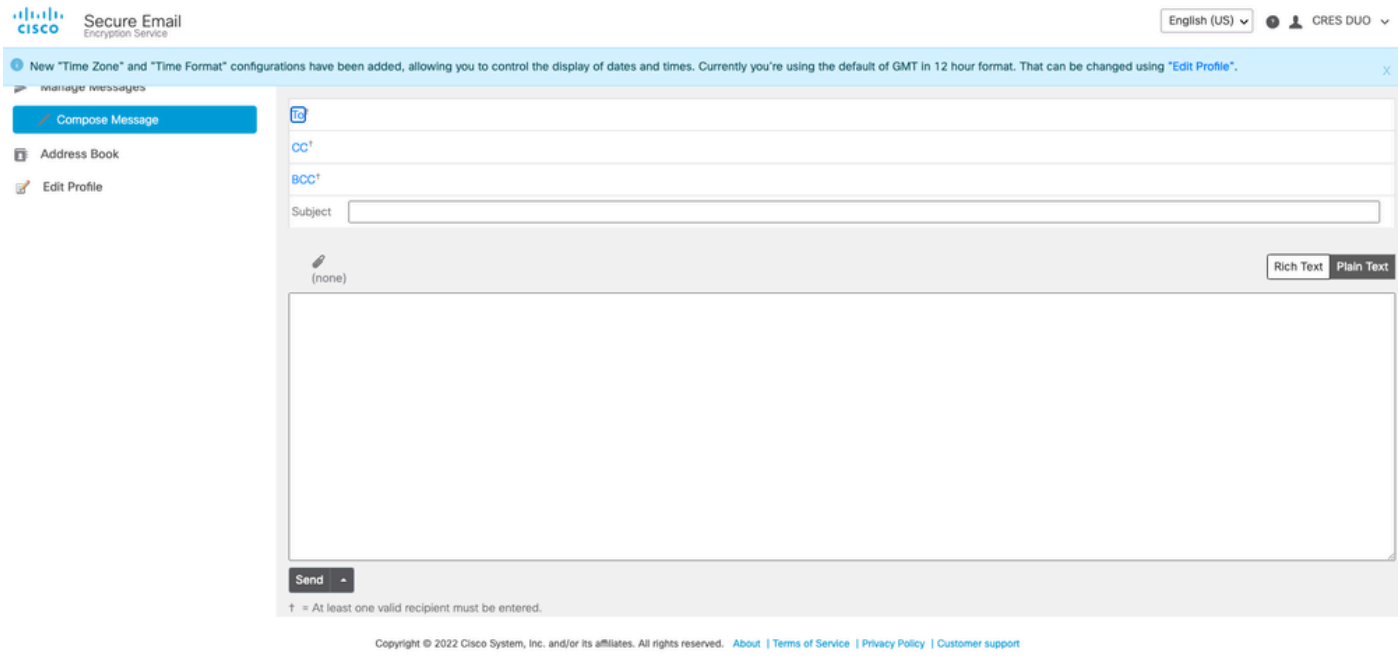
步骤1.登录到Cisco Secure Email Encryption Service门户，如图所示：



步骤2.完成Duo密钥身份验证，如图所示：



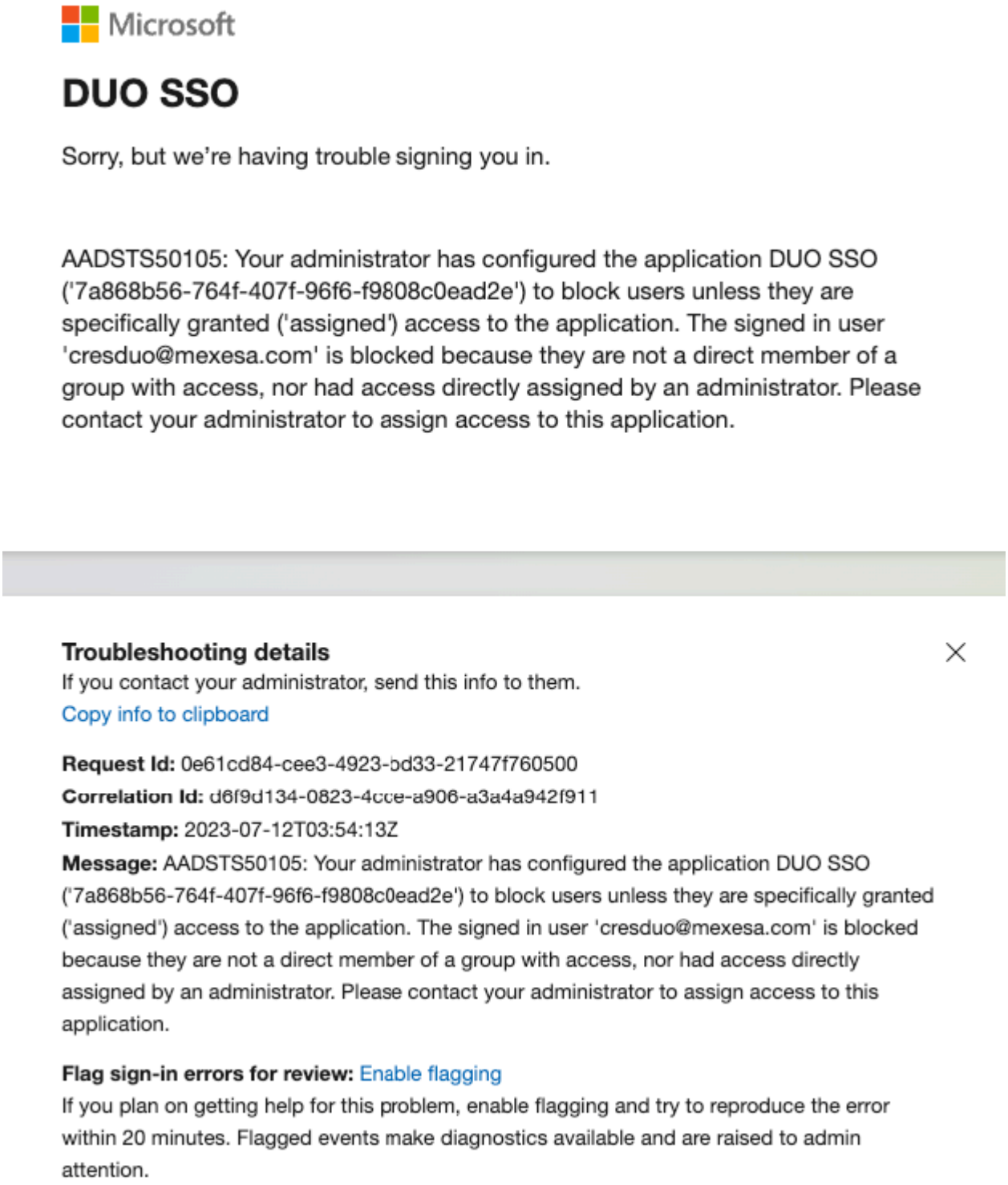
步骤3.输入正确的密钥后，确认用户可以成功登录思科安全邮件加密服务门户，如图所示：



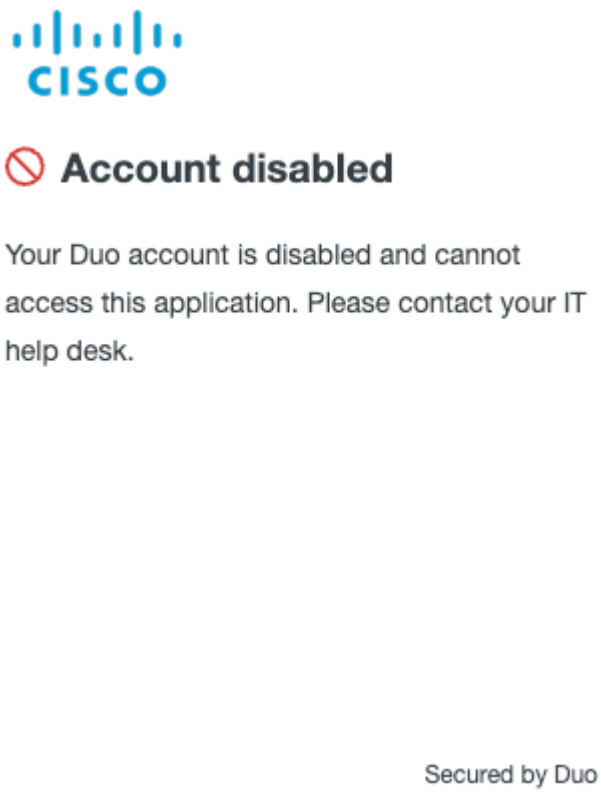
常见错误

如果SAML SSO未成功完成至思科安全邮件加密服务，请查看这些常见错误。

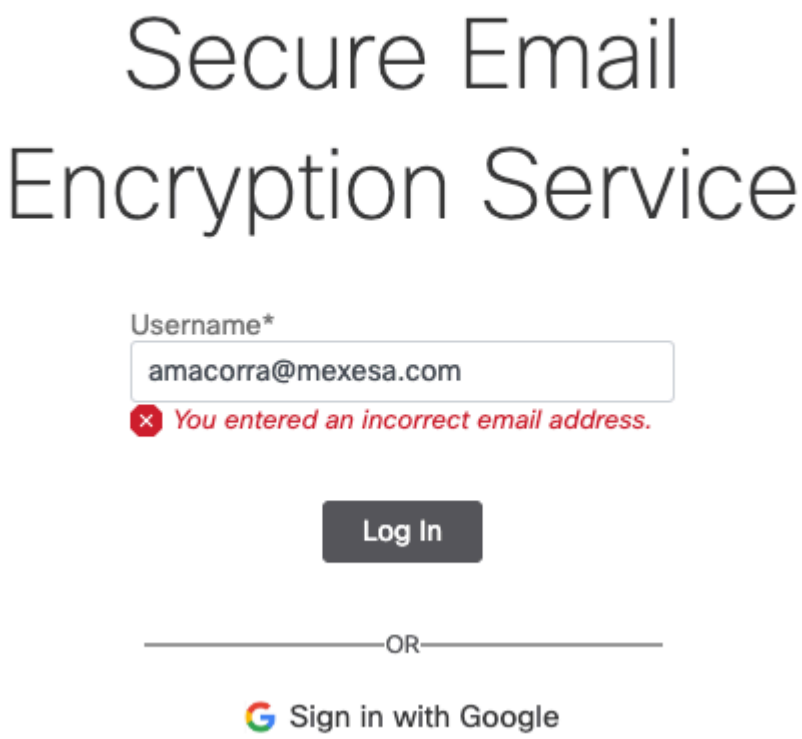
1.如果在企业应用产品中的用户和组下未分配用户，则会出现此错误，如图所示：



2.如果用户从Duo Admin Panel中的Users中删除，则会出现此错误，如图所示：



3.如果用户未在Duo Admin Panel中注册，则会出现此错误，如图所示：



相关信息

有关其他配置详细信息和产品文档，请参阅以下资源：

- 思科安全邮件加密服务管理门户
- 双管理面板
- Microsoft Azure门户
- Duo用户注册文档
- 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）。