DuoによるセキュアなE-mail暗号化サービスSAML SSOの設定

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[設定](#)

[確認](#)

[一般的なエラー](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco Secure Email Encryption Service(CES)（以前のCisco Registered Envelope Service [CRES]）をDuo for Security Assertion Markup Language(SAML)シングルサインオン(SSO)と統合する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Email Encryption Service(SEES)管理ポータルへの管理アクセス。
- Duo Admin Panelへの管理アクセス。
- Microsoft Azureポータルへの管理アクセス。
- Duoユーザ登録のドキュメントの説明に従って、Duo Admin Panelでユーザを登録します。

使用するコンポーネント

このドキュメントの情報は、SAML 2.0に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。こ

のドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

Cisco Secure Email Encryption Service、Duo、およびMicrosoft Azure Active Directory間でSAML SSOを設定するには、次の手順を使用します。設定が完了すると、エンタープライズアプリケーションに割り当てられたユーザは、Duoを使用してCisco Secure Email Encryption Service(SEES)ポータルで認証を受けることができます。

ステップ 1：Duo Admin Panelにログインします。

ステップ 2Applicationsに移動します。

ステップ 3Protect an Applicationを選択します。

ステップ 4Generic SAML Service Providerを選択し、Protectをクリックします。

ステップ 5シングルサインオンURLをコピーします。

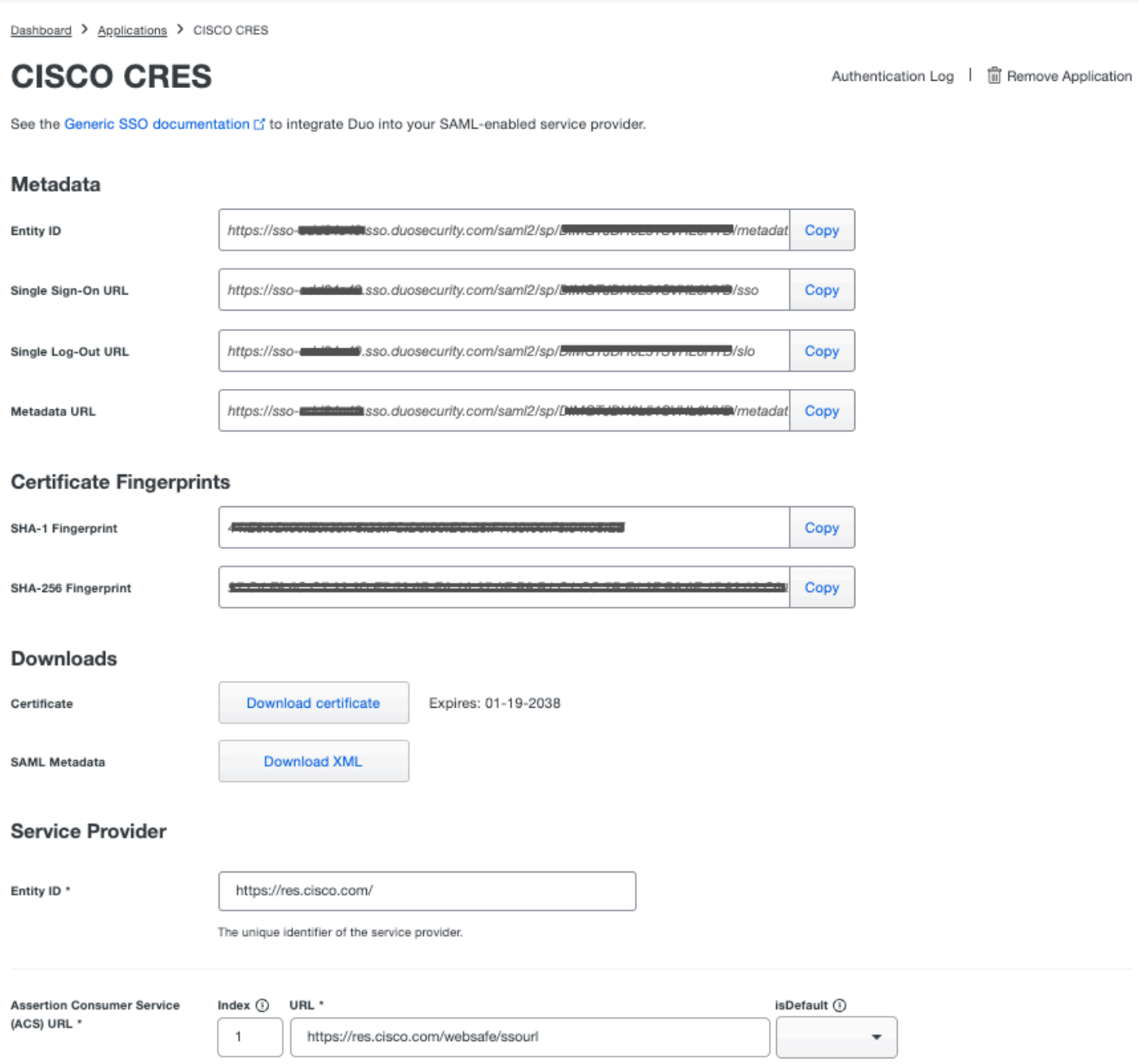
ステップ 6Download Certificateを選択します。

ステップ 7Download XMLを選択します。

ステップ 8Service Provider > Entity ID *で、Cisco Secure Email Encryption Service(SEES)エンティティIDを入力します。

ステップ 9Service Provider > Assertion Consumer Service (ACS) URL *で、Cisco Secure Email Encryption Service ACS URLを入力します。

ステップ 10次の図に示すように、Settings > Nameで新しいアプリケーションの名前を入力し、Saveを選択します。



ステップ 11[Cisco Secure Email Encryption Service(SEES)管理ポータル]に移動します。

ステップ 12Accountsに移動して、Account Numberのハイパーリンクを選択します。

ステップ 13Detailsタブで、Authentication MethodをSAML 2.0に設定します。

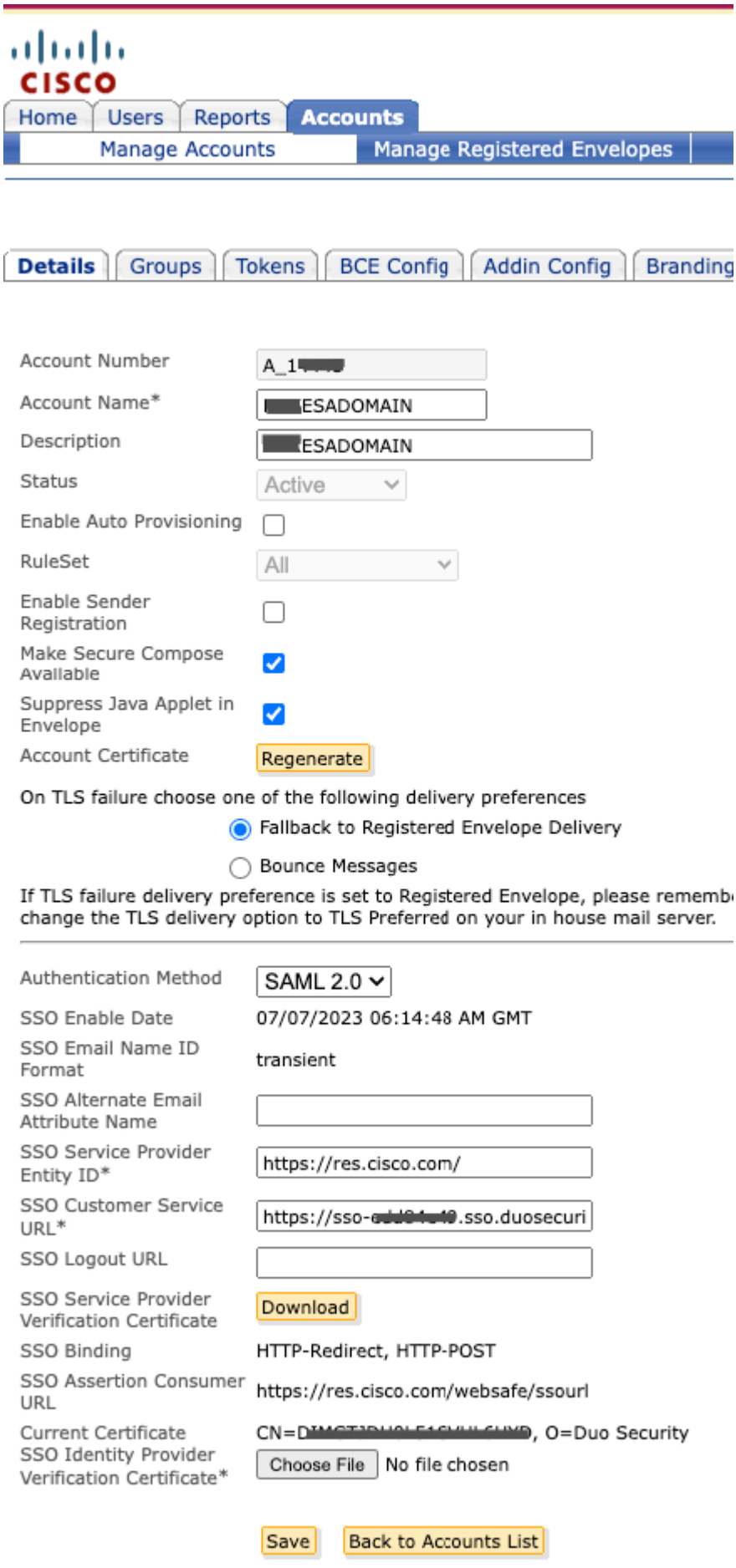
手順 14：SSO代替電子メール属性名は空白のままにします。

手順 15：SSOサービスプロバイダーエンティティIDに、[Cisco Secure Email Encryptionサービスエンティティ ID]を入力します。

ステップ 16：SSOカスタマーサービスのURLに、ステップ5でコピーしたURLを入力します。

ステップ 17：SSOログアウトURLは空白のままにします。

ステップ 18：図に示すように、Current Certificate SSO Identity Provider Verification Certificateで、Choose Fileをクリックし、ステップ6でダウンロードした証明書をアップロードします。



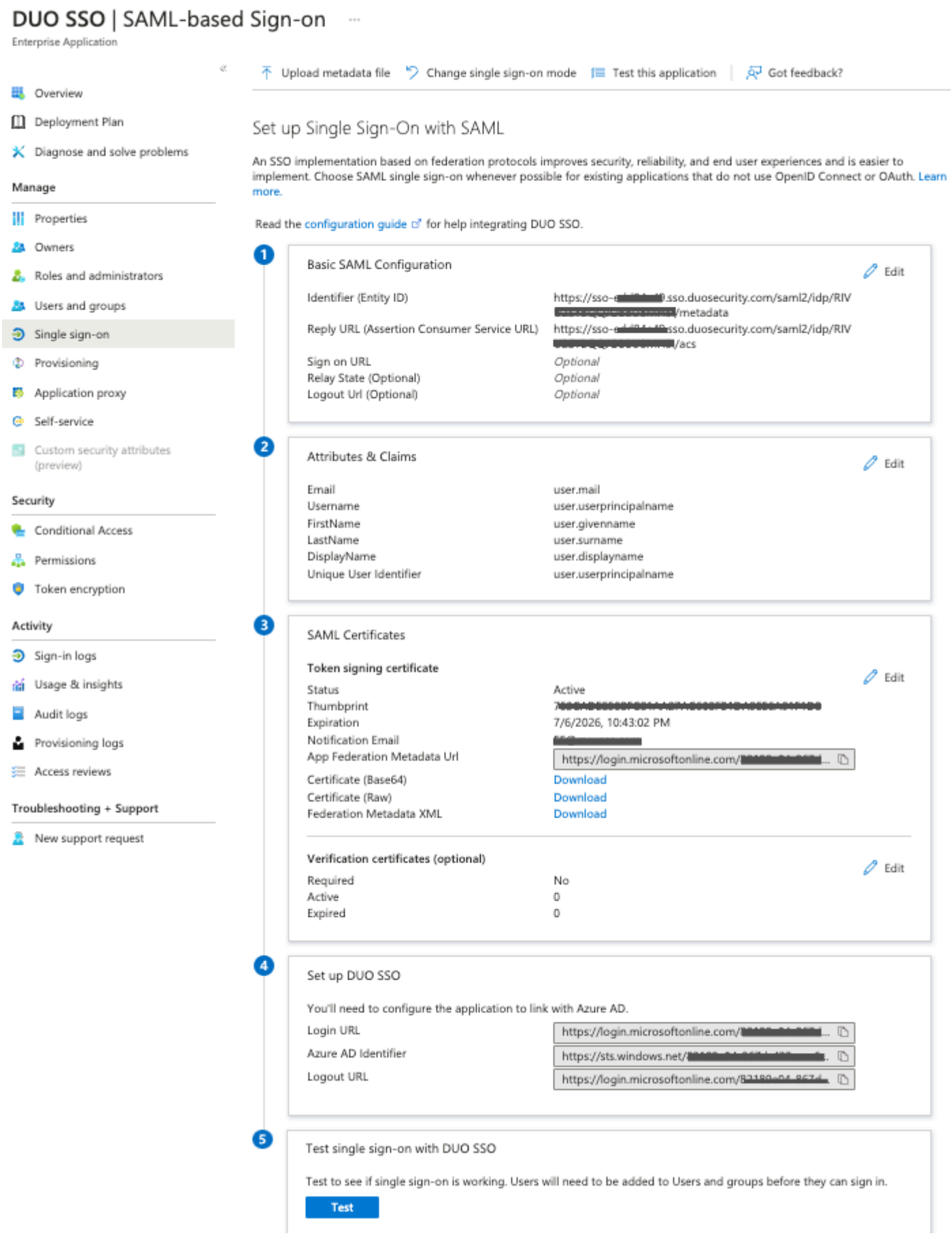
ステップ 19：Microsoft Azureポータルにログインします。

ステップ 20：Azure Active Directory > Enterprise Applications > New application > Create your own applicationの順に移動します。

ステップ 21：アプリケーション名を入力し、Integrate any other application you don't find in the gallery (Non-gallery)を選択し、Createをクリックします。

ステップ 22：Assign users and groupsを選択し、Cisco Secure Email Encryption Serviceへのアクセスを必要とするユーザを追加して、Assignをクリックします。

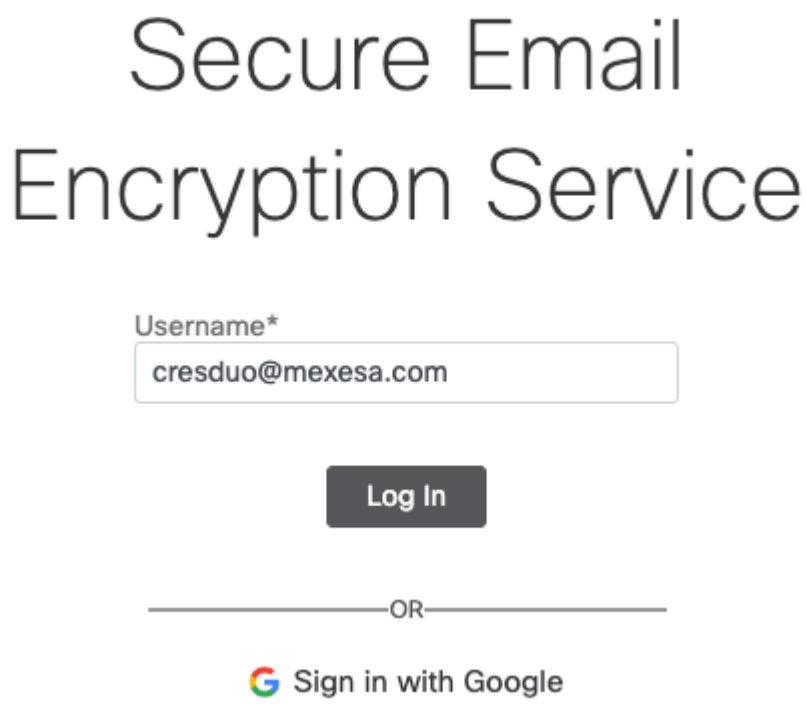
ステップ 23：図に示すように、Single sign-on > SAML > Upload metadata fileの順に選択し、ステップ7でダウンロードしたファイルを選択します。


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

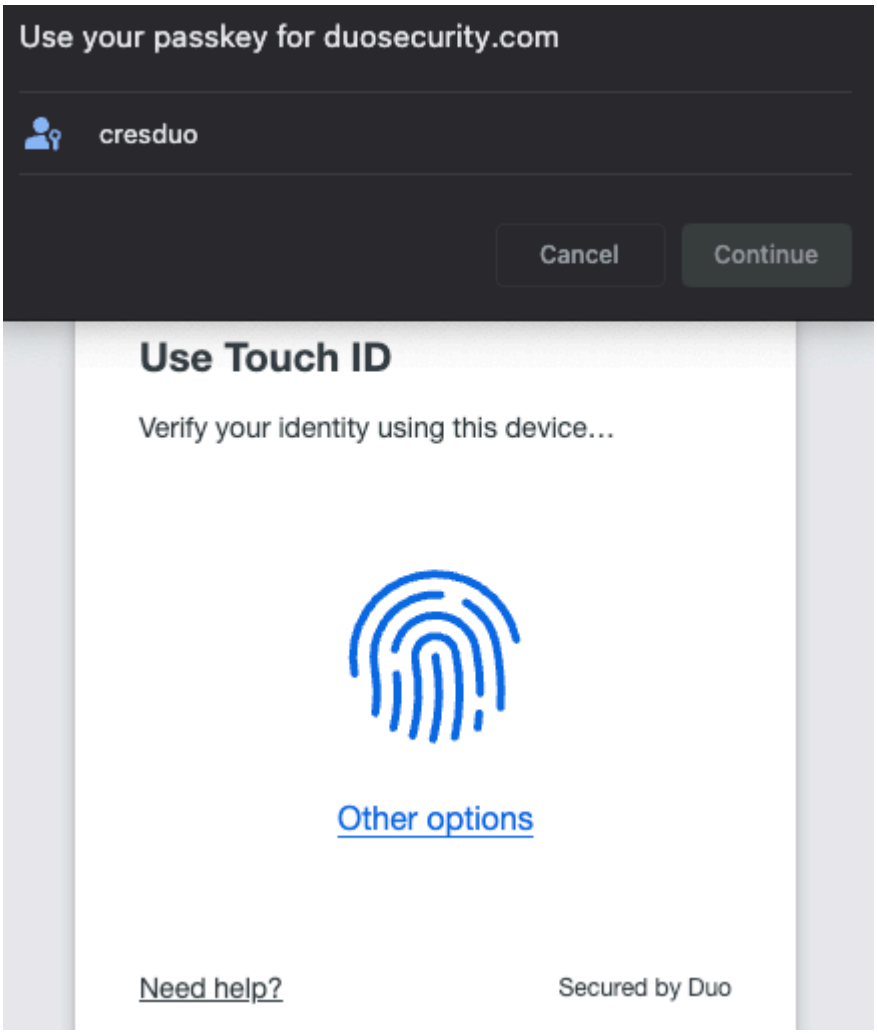
確認

割り当てられたユーザが認証のためにDuoにリダイレクトされ、認証が成功した後にCisco Secure Email Encryption Service(CEM)ポータルに戻ることを確認することで、SAML SSO設定が期待どおりに動作することを確認します。

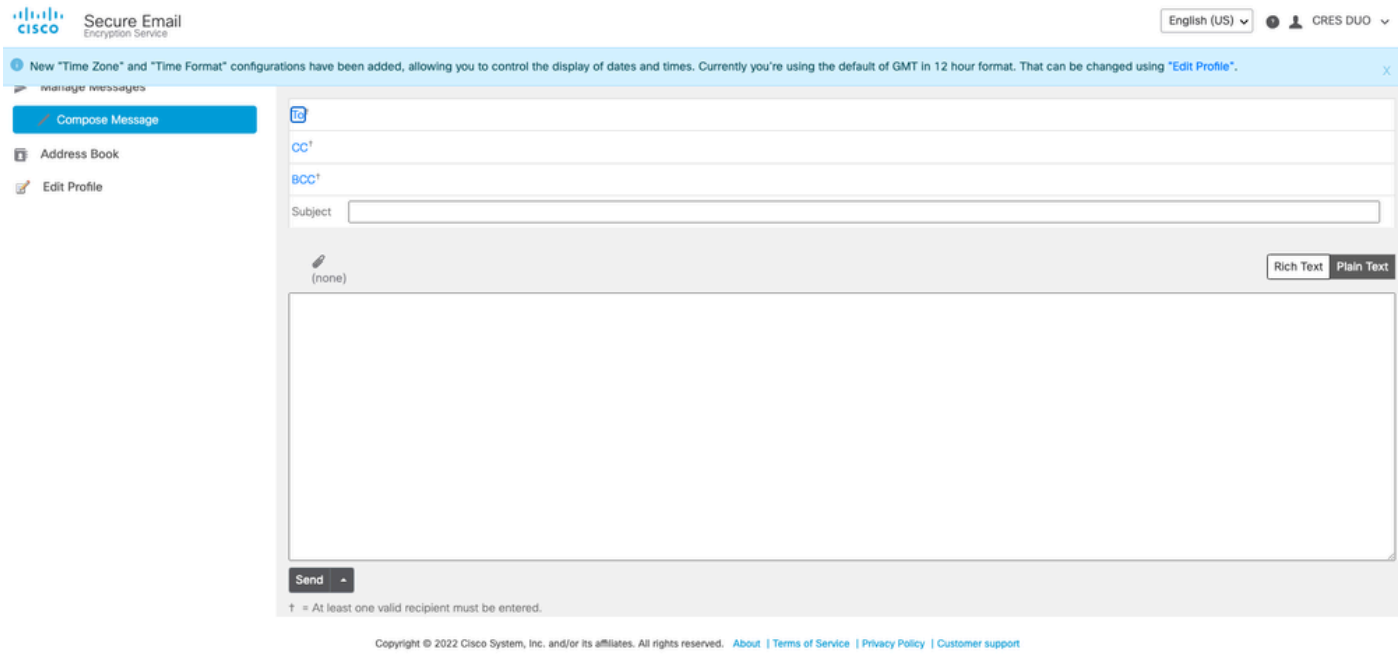
ステップ 1：図に示すように、Cisco Secure Email Encryption Service portalにログインします。



ステップ 2図に示すように、Duoパスキー認証を完了します。



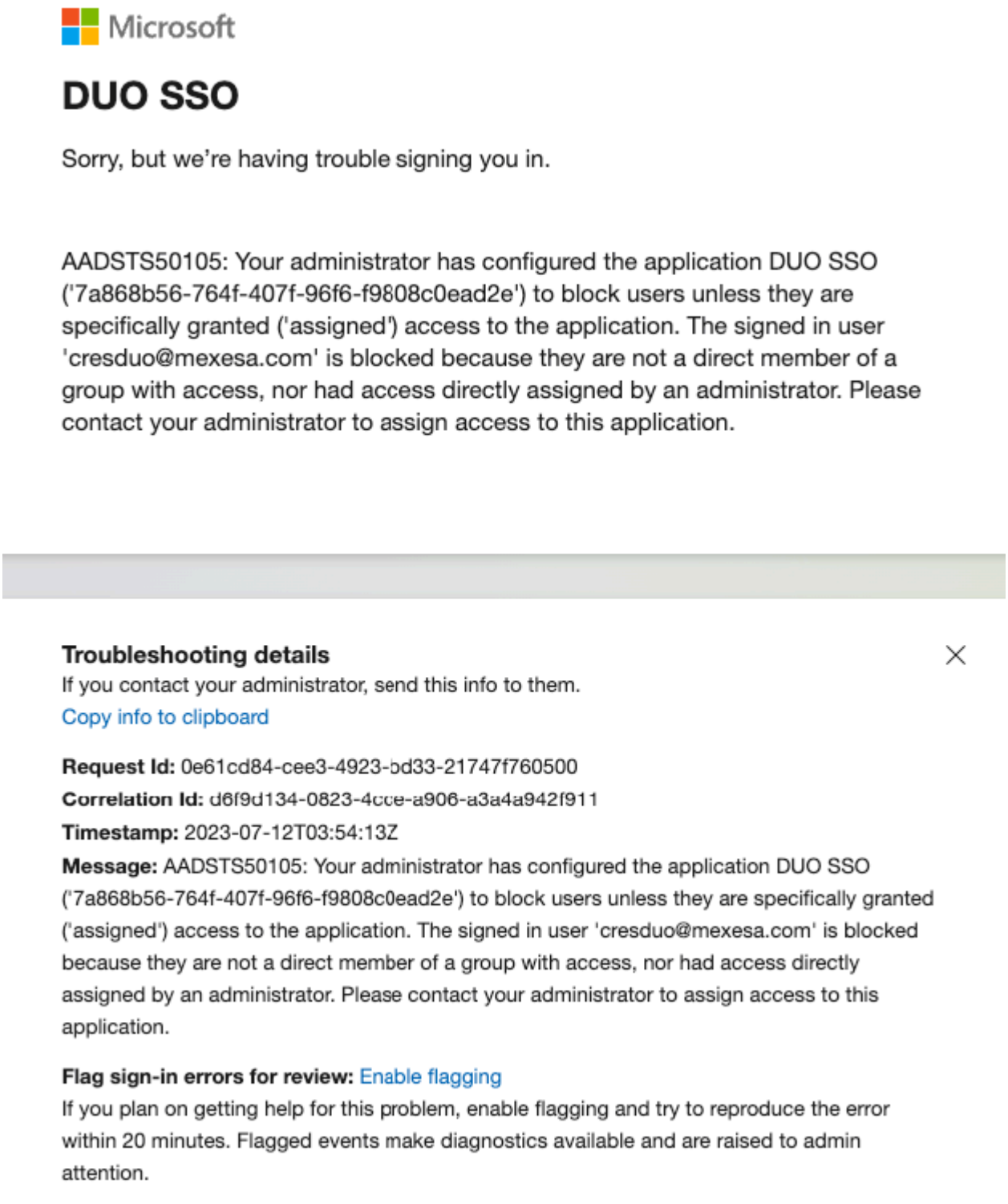
ステップ 3正しいパスキーを入力したら、次の図に示すように、ユーザがCisco Secure Email Encryption Service(CES)ポータルに正常にログインできることを確認します。



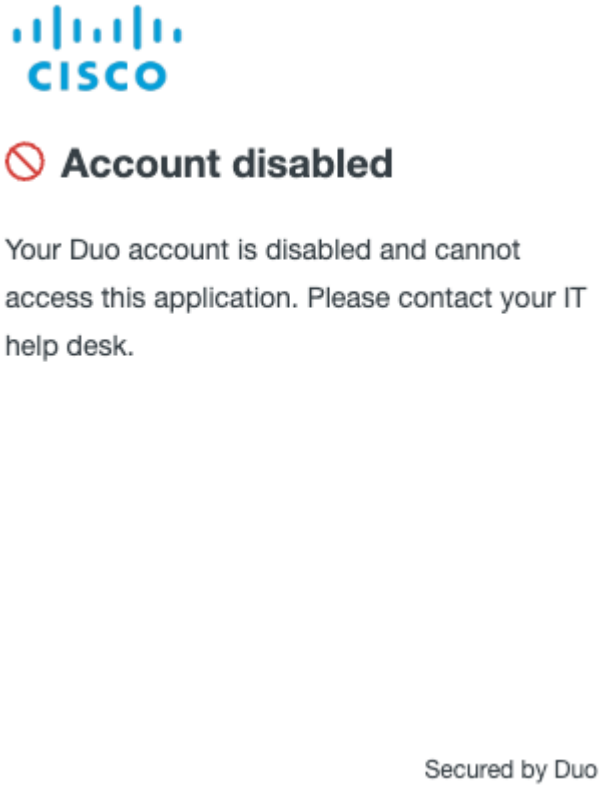
一般的なエラー

Cisco Secure Email Encryption ServiceへのSAML SSOが正常に完了しない場合は、これらの一般的なエラーを確認してください。

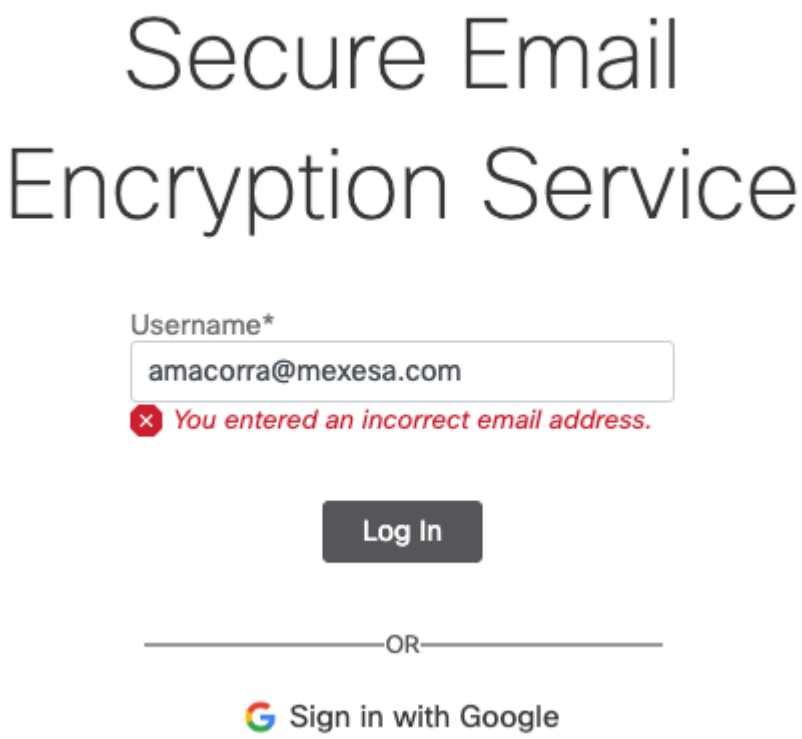
1. ユーザがエンタープライズアプリケーションのユーザとグループの下に割り当てられていない場合、次の図に示すようにエラーが表示されます。



2. ユーザがDuo Admin PanelのUsersから削除されると、次の図に示すようにエラーが表示されます。



3. ユーザがDuo Admin Panelに登録されていない場合、次の図に示すようにエラーが表示されます。



関連情報

設定の詳細と製品ドキュメントについては、次のリソースを参照してください。

- Cisco Secure Email Encryption Service管理ポータル
- Duo管理パネル
- Microsoft Azureポータル
- Duoユーザー登録ドキュメント
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。