Configuration du service de cryptage sécurisé des e-mails SAML SSO avec Duo

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

Vérifier

Erreurs courantes

Informations connexes

Introduction

Ce document décrit comment intégrer Cisco Secure Email Encryption Service (anciennement Cisco Registered Envelope Service [CRES]) à Duo pour la connexion unique SAML (Security Assertion Markup Language).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès administratif au portail d'administration du service Cisco Secure Email Encryption Service.
- Accès administratif au panneau d'administration Duo.
- Accès administratif au portail Microsoft Azure.
- Inscrivez les utilisateurs dans le panneau d'administration Duo comme décrit dans la documentation d'inscription des utilisateurs Duo.

Composants utilisés

Les informations contenues dans ce document sont basées sur SAML 2.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Utilisez cette procédure afin de configurer l'authentification unique SAML entre Cisco Secure Email Encryption Service, Duo et Microsoft Azure Active Directory. Une fois la configuration terminée, les utilisateurs affectés à l'application d'entreprise peuvent s'authentifier sur le portail Cisco Secure Email Encryption Service avec Duo.

Étape 1. Connectez-vous au panneau d'administration Duo.

Étape 2. Accédez à Applications.

Étape 3. Choisissez Protect an Application.

Étape 4. Choisissez Generic SAML Service Provider, puis cliquez sur Protect.

Étape 5. Copiez l'URL d'authentification unique.

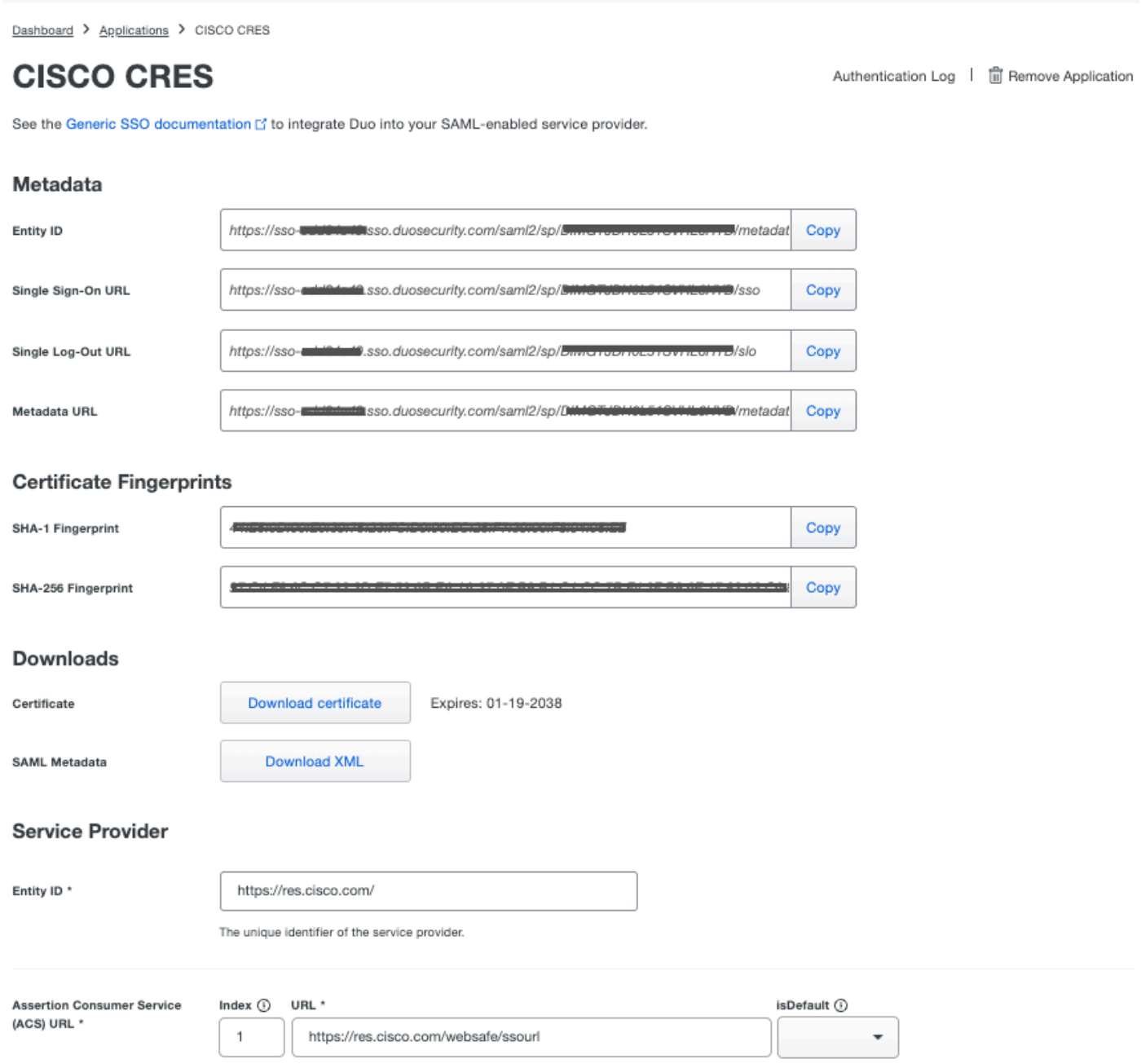
Étape 6. Choisissez Download Certificate.

Étape 7. Choisissez Download XML.

Étape 8. Dans Service Provider > Entity ID *, saisissez l'ID d'entité Cisco Secure Email Encryption Service.

Étape 9. Dans Service Provider > Assertion Consumer Service (ACS) URL *, saisissez Cisco Secure Email Encryption Service ACS URL.

Étape 10. Dans Paramètres > Nom, entrez un nom pour la nouvelle application, puis choisissez Enregistrer, comme indiqué dans l'image :



Étape 11. Connectez-vous au portail d'administration du service Cisco Secure Email Encryption Service.

Étape 12. Accédez à Comptes, puis sélectionnez le lien hypertexte du numéro de compte.

Étape 13. Dans l'onglet Details, définissez Authentication Method sur SAML 2.0.

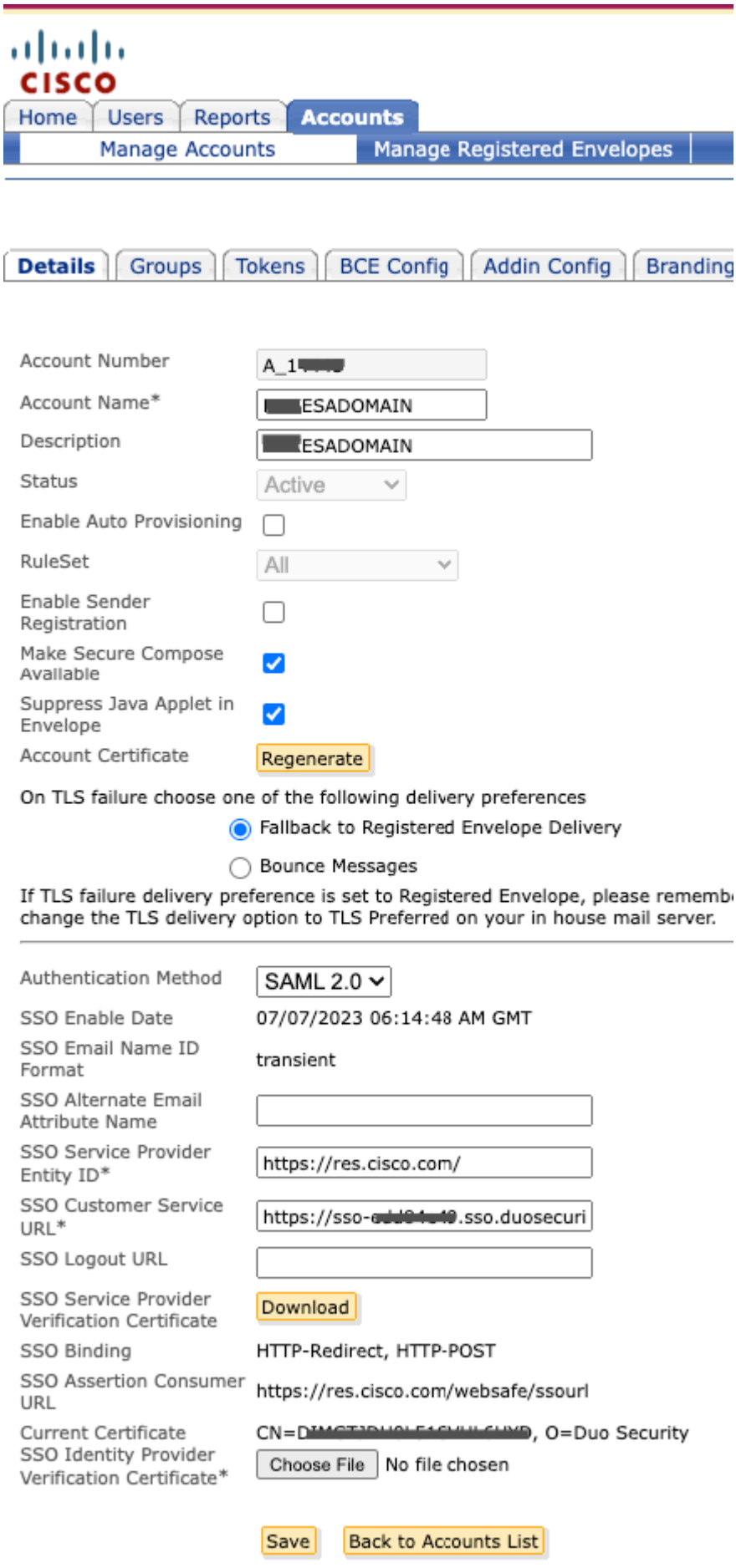
Étape 14. Laissez le champ Nom de l'attribut d'e-mail secondaire SSO vide.

Étape 15. Dans SSO Service Provider Entity ID, saisissez l'ID d'entité Cisco Secure Email Encryption Service.

Étape 16. Dans SSO Customer Service URL, entrez l'URL copiée à l'étape 5.

Étape 17. Laissez l'URL de déconnexion SSO vide.

Étape 18. Dans Certificat actuel Certificat de vérification du fournisseur d'identité SSO, cliquez sur Choisir un fichier, puis téléchargez le certificat téléchargé à l'étape 6., comme illustré dans l'image :



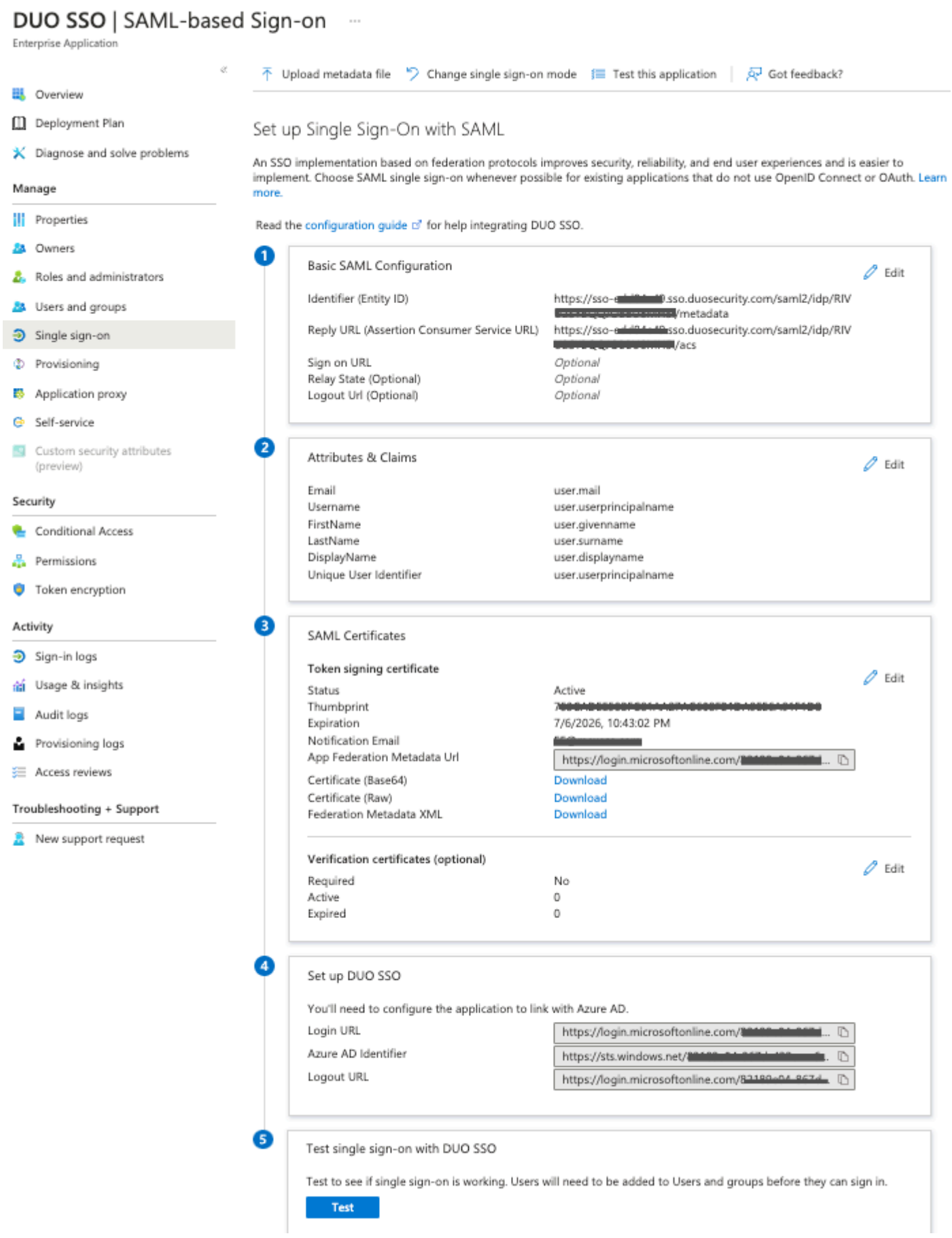
Étape 19. Connectez-vous au portail Microsoft Azure.

Étape 20. Accédez à Azure Active Directory > Applications d'entreprise > Nouvelle application > Créer votre propre application.

Étape 21. Entrez un nom d'application, choisissez Intégrer toute autre application que vous ne trouvez pas dans la galerie (hors galerie), puis cliquez sur Créer.

Étape 22. Choisissez Assign users and groups, ajoutez les utilisateurs qui ont besoin d'un accès au service Cisco Secure Email Encryption Service, puis cliquez sur Assign.

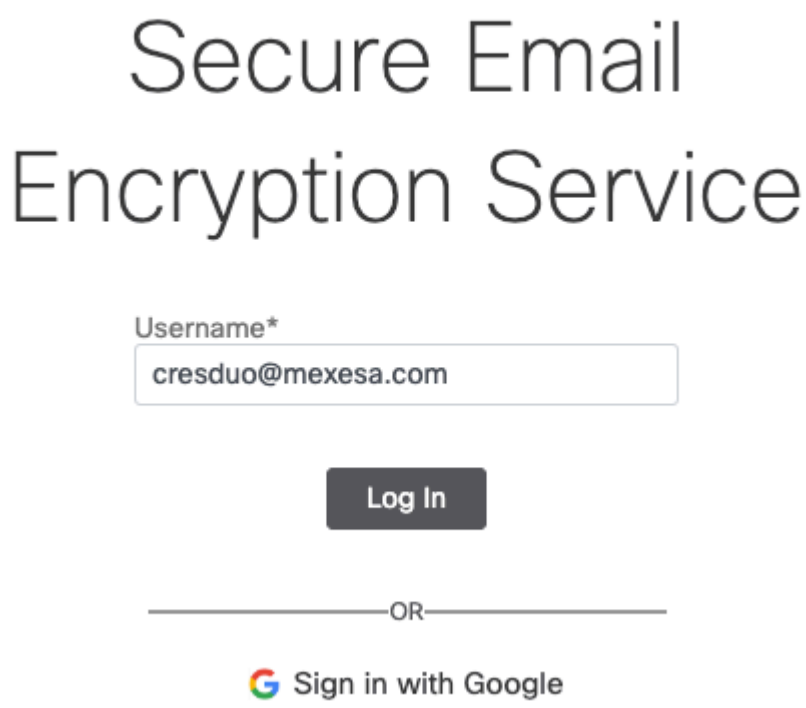
Étape 23. Choisissez Single sign-on > SAML > Upload metadata file, puis choisissez le fichier téléchargé à l'étape 7., comme illustré dans l'image :


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

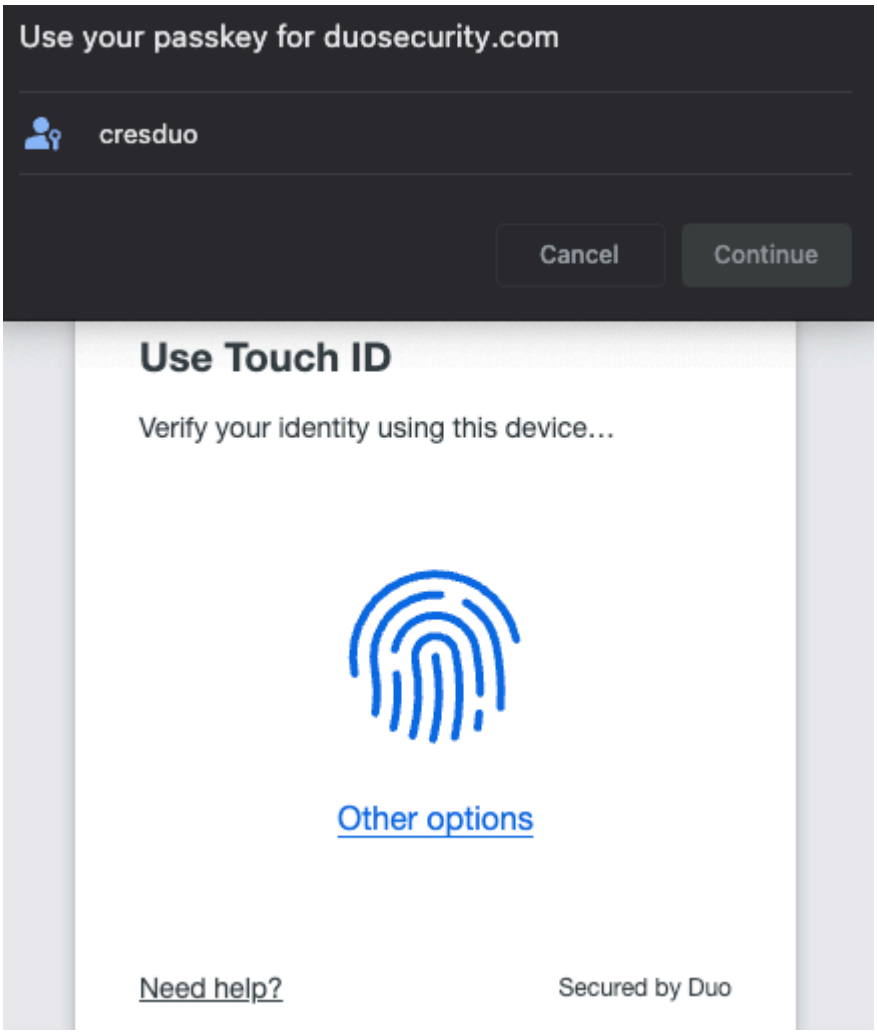
Vérifier

Vérifiez que la configuration de l'authentification unique SAML fonctionne comme prévu en confirmant qu'un utilisateur affecté est redirigé vers Duo pour l'authentification, puis renvoyé au portail Cisco Secure Email Encryption Service après une authentification réussie.

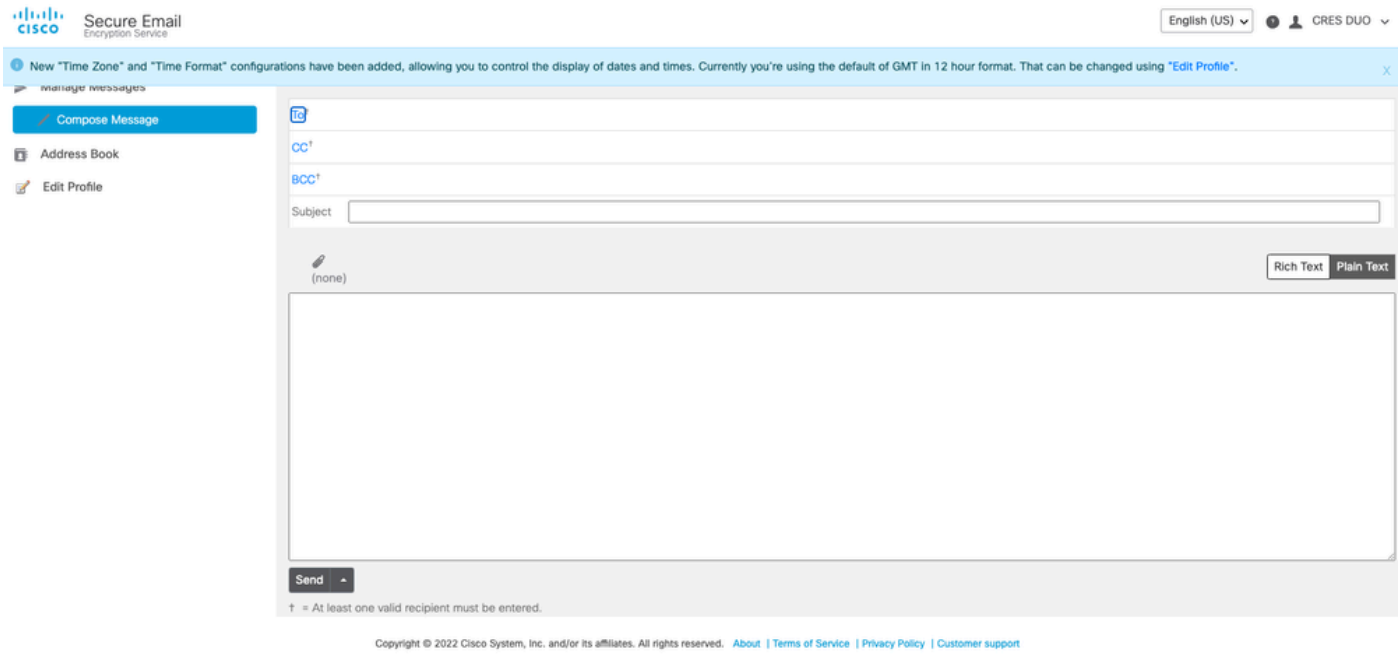
Étape 1. Connectez-vous au portail Cisco Secure Email Encryption Service, comme illustré dans l'image :



Étape 2. Effectuez l'authentification par clé d'accès Duo, comme illustré dans l'image :



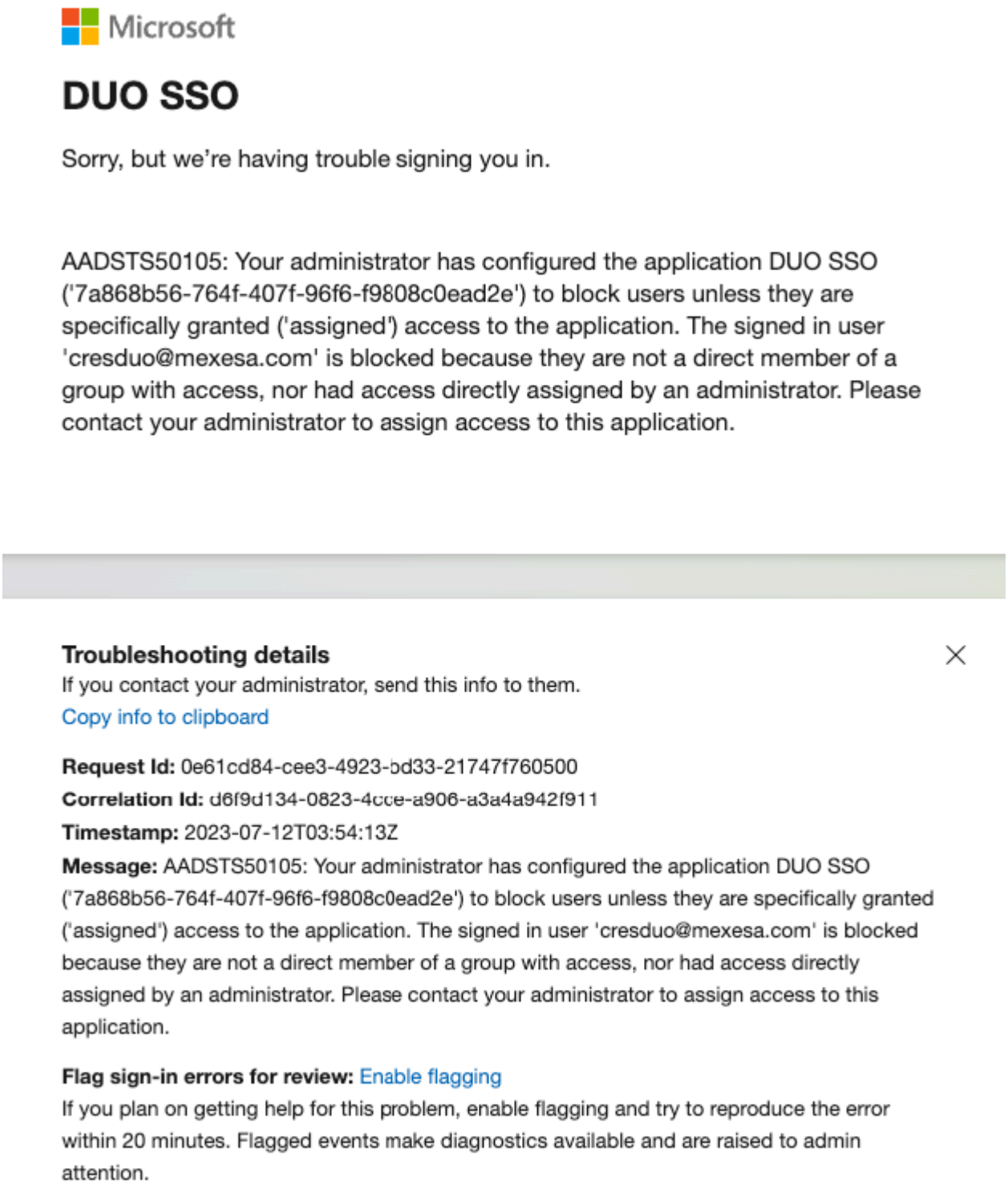
Étape 3. Une fois la clé d'accès saisie, vérifiez que l'utilisateur peut se connecter au portail Cisco Secure Email Encryption Service avec succès, comme indiqué dans l'image :



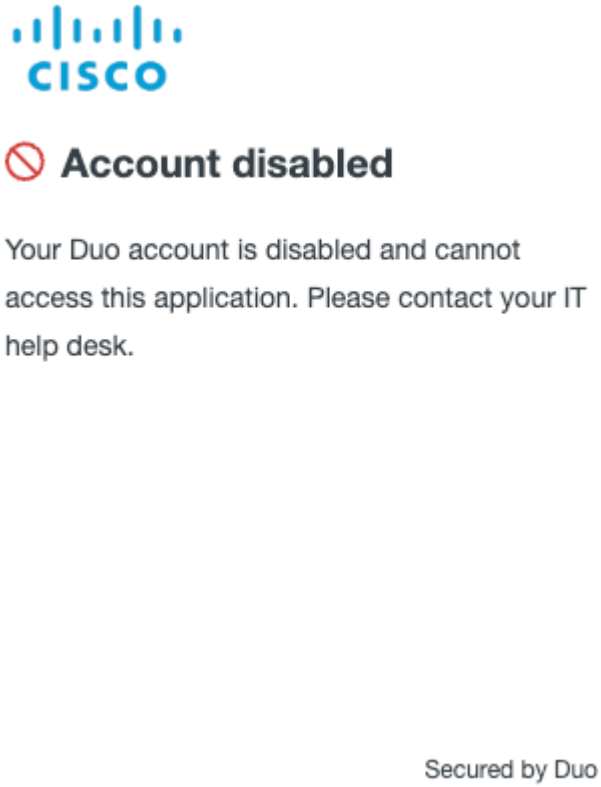
Erreurs courantes

Vérifiez ces erreurs courantes si l'authentification unique SAML au service de chiffrement sécurisé de la messagerie Cisco ne se termine pas correctement.

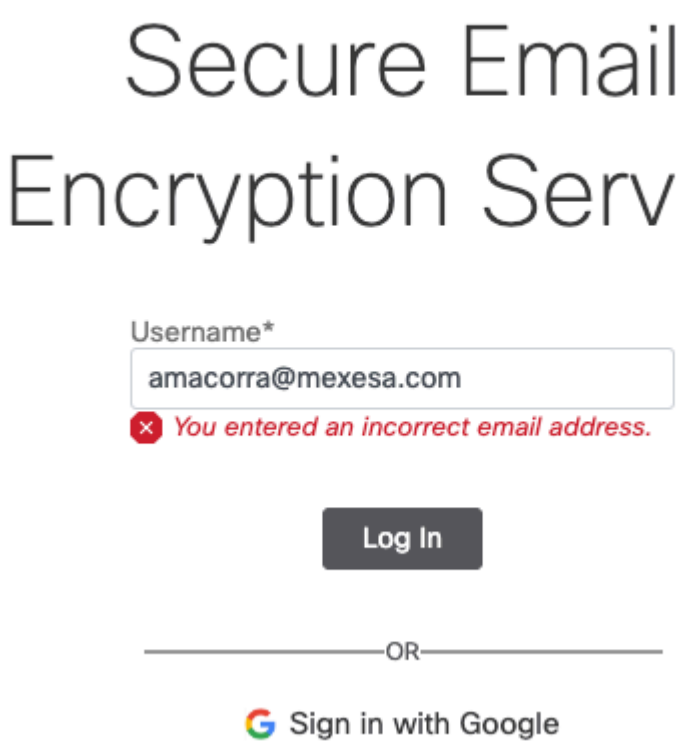
1. Si l'utilisateur n'est pas affecté sous Utilisateurs et groupes dans l'application d'entreprise, cette erreur apparaît, comme illustré dans l'image :



2. Si l'utilisateur est supprimé de Users dans le panneau d'administration Duo, cette erreur s'affiche, comme illustré dans l'image :



3. Si l'utilisateur n'est pas inscrit dans le panneau d'administration Duo, cette erreur apparaît, comme illustré dans l'image :



Informations connexes

Reportez-vous aux ressources suivantes pour obtenir des détails supplémentaires sur la configuration et la documentation produit :

- Portail d'administration de Cisco Secure Email Encryption Service
- Panneau d'administration Duo
- Portail Microsoft Azure
- Documentation d'inscription utilisateur Duo
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.