Intégrer le service Cisco Secure Email Encryption Service à Duo

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

Vérifier

Erreurs courantes

Introduction

Ce document décrit comment intégrer Cisco Secure Email Encryption Service, anciennement connu sous le nom de Cisco Registered Envelope Service (CRES), avec Duo.

Conditions préalables

Exigences

- Accès administrateur au portail CRES https://res.cisco.com/admin/
- Accès administrateur au portail Duo https://admin.duosecurity.com/
- Accès administrateur au portail Azure https://portal.azure.com/
- Les utilisateurs doivent être inscrits au panneau d'administration Duo, comme décrit dans https://duo.com/docs/enrolling-users

Composants utilisés

- 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

Étape 1. Connectez-vous au panneau d'administration Duo https://admin.duosecurity.com/

Étape 2. Accédez à Applications

Étape 3. Sélectionnez Protect Application

Étape 4. Sélectionner un fournisseur de services SAML générique et protéger

Étape 5. Copier l'URL d'authentification unique

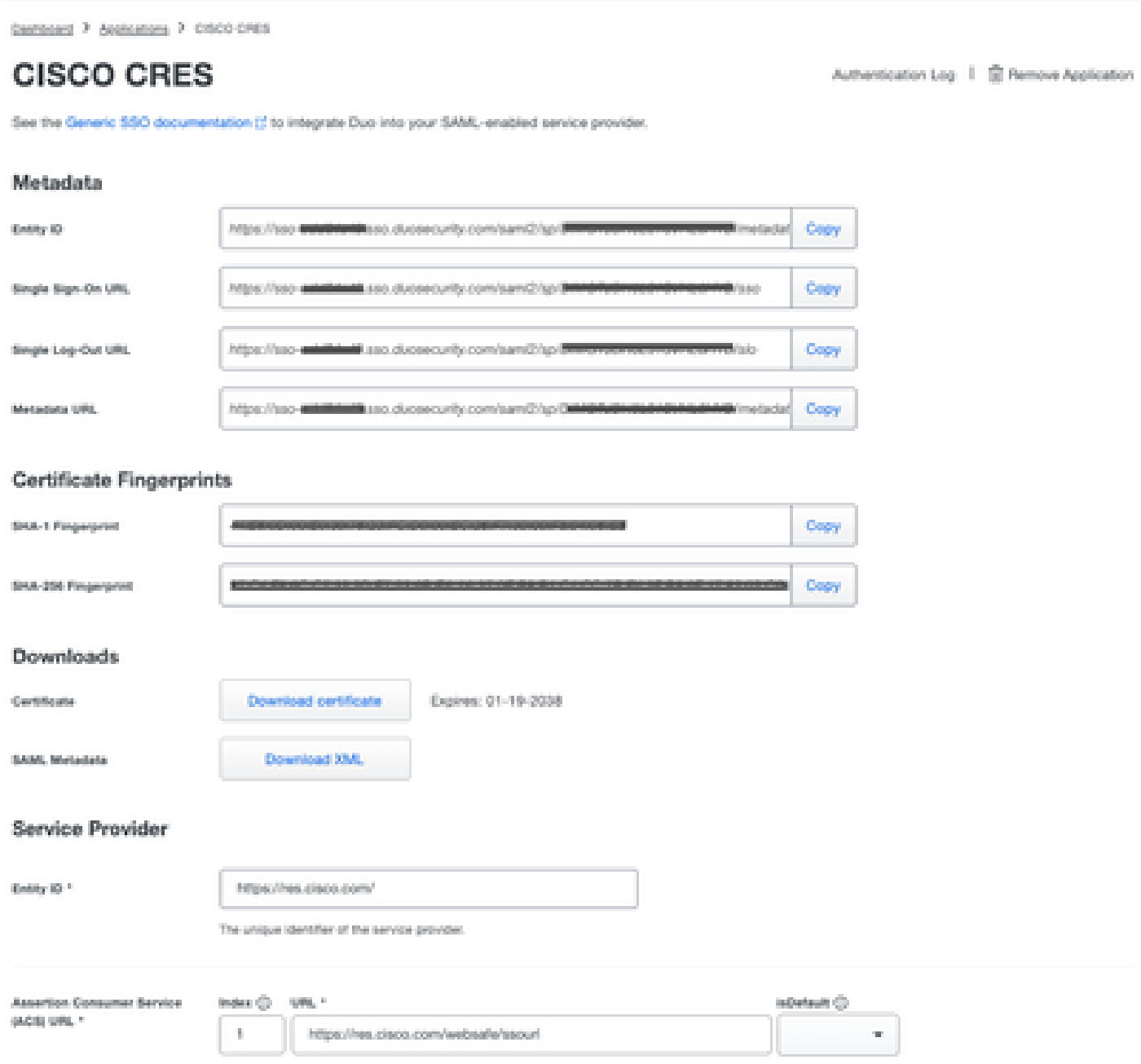
Étape 6. Sélectionnez Télécharger le certificat

Étape 7. Sélectionnez Télécharger XML

Étape 8. Sous Service Provider -> Entity ID *, tapez https://res.cisco.com/

Étape 9. Sous Service Provider -> Assertion Consumer Service (ACS) URL *, tapez https://res.cisco.com/websafe/ssourl

Étape 10. Faites défiler vers le bas jusqu'à ce que Settings -> Name tapez le titre de votre nouvelle application et sélectionnez Save, comme indiqué dans l'image :



Étape 11. Connectez-vous au portail CRES https://res.cisco.com/admin/

Étape 12. Accédez à l'onglet Comptes et sélectionnez le lien hypertexte de votre numéro de compte

Étape 13. Sous l'onglet Détails, sélectionnez Authentication Method -> SAML 2.0

Étape 14. Laissez le champ Nom de l'attribut de messagerie secondaire SSO vide

Étape 15. SSO Service Provider Entity ID type https://res.cisco.com/

Étape 16. SSO Customer Service URL collez l'URL copiée à l'étape 5

Étape 17. Laissez l'URL de déconnexion SSO vide

Étape 18. Certificat actuel Certificat de vérification du fournisseur d'identité SSO sélectionnez Choose File et utilisez le certificat téléchargé à l'étape 6, comme illustré dans l'image :

Home | Users | Reports | Accounts

Manage Accounts | Manage Registered Envelopes

Details | Groups | Tokens | BCE Config | Addin Config | Branding

Account Number	A_1[redacted]
Account Name*	[redacted]ESADOMAIN
Description	[redacted]ESADOMAIN
Status	Active
Enable Auto Provisioning	☐
RuleSet	All
Enable Sender Registration	☐
Make Secure Compose Available	☑
Suppress Java Applet in Envelope	☑
Account Certificate	Regenerate

On TLS failure choose one of the following delivery preferences

- ◉ Fallback to Registered Envelope Delivery
- ○ Bounce Messages

If TLS failure delivery preference is set to Registered Envelope, please remembe
change the TLS delivery option to TLS Preferred on your in house mail server.

Authentication Method	SAML 2.0
SSO Enable Date	07/07/2023 06:14:48 AM GMT
SSO Email Name ID Format	transient
SSO Alternate Email	

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.