# Intégrer le service Cisco Secure Email Encryption Service à Duo

# Table des matières

troduction	
onditions préalables	
Exigences	
Composants utilisés	
onfigurer	
<u>érifier</u>	
rreurs 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 <u>https://res.cisco.com/admin/</u>
- Accès administrateur au portail Duo <a href="https://admin.duosecurity.com/">https://admin.duosecurity.com/</a>
- Accès administrateur au portail Azure <a href="https://portal.azure.com/">https://portal.azure.com/</a>
- Les utilisateurs doivent être inscrits au panneau d'administration Duo, comme décrit dans <u>https://duo.com/docs/enrolling-users</u>

### 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 <u>https://res.cisco.com/websafe/ssourl</u>

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 :

Castocard > Accelerators > Crico cres						
CISCO CRES		Authentication Log   🗍 Remove Application				
See the Generic SSO documentation (2 to integrate Duo into your SAML-enabled service provider.						
Metadata						
Entity ID	https://sec.exel.exel.exel.exel.exel.exel.exel.ex	Ceary				
Single Sign-On URL	Mige://pso-entroletable.soo.ducoecumity.com/sam/2/tgr/@microsof.com/sam	Ceary				
Single Log-Out URL	https://sac-minimiz.asc.duceecunty.com/sam@hp/amorecomecanonecome/sab	Copy				
Metaduta URL	https://sec-entropy.com/sami2/sp/0-entropy.com/sami2/sp	Copy				
Certificate Fingerprin	Certificate Fingerprints					
SHA-1 Fingerprint		Copy				
SHA-204 Fingerprint		Copy				
Downloads						
Certificate	Download certificate Expires: 01-19-2008					
SAM, Metadata	Download XML					
Service Provider						
Entity ID 1	https://ws.cisco.com/					
	The unique identifier of the service provider.					
Assertion Consumer Bervice (ACII) URL *	Index © 10%, * Ind 1   https://ws.cisco.com/websafe/securi	eteett ()				

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 :

alada	
CISCO	
Home Users Reports	Accounts
Manage Accounts	Manage Registered Envelopes

Details Groups	Tokens	608	Config	Addin Config	Branding
Account Number	A.198				
Account Name*	-	моом	AIN		
Description	i i i i	ADOM	AIN		
Status	Active		v		
Enable Auto Provisionin	9 🖸				
RuleSet	All		v		
Enable Sender Registration	0				
Make Secure Compose Available					
Suppress Java Applet in Envelope					
Account Certificate	Repon	eriste			
and the second s				a server dimension of the server	

On TLS failure choose one of the following delivery preferences

Falback to Registered Envelope Delivery

Bounce Messages

If TLS failure delivery preference is set to Registered Envelope, please remembchange 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.