# Cisco Secure Email Encryption ServiceとDuoの 統合

为容	
<u> </u>	
前提条件	
<u>要件</u>	
<u>使用するコンポーネント</u>	
<u>設定</u>	
<u>確認</u>	
<u>一般的なエラー</u>	

### はじめに

このドキュメントでは、Cisco Secure Email Encryption Service(CES)(旧称Cisco Registered Envelope Service(CRES))をDuoと統合する方法について説明します。

# 前提条件

#### 要件

- CRESポータル<u>https://res.cisco.com/admin/</u>への管理者アクセス
- Duoポータル<u>https://admin.duosecurity.com/</u>への管理者アクセス
- Azureポータル<u>https://portal.azure.com/</u>への管理者アクセス
- <u>https://duo.com/docs/enrolling-users</u>に記載されているように、ユーザはDuo Admin Panelに 登録する必要があります。

#### 使用するコンポーネント

• SAML 2.0

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ました。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

ステップ1: Duo Admin Panel <u>https://admin.duosecurity.com/</u>にログインします

ステップ2: Applicationsに移動します。

ステップ3: Protect Applicationの選択

ステップ4: Generic SAML Service ProviderとProtectを選択します

ステップ5:シングルサインオンURLのコピー

手順 6: Download Certificateを選択します

手順7: Download XMLを選択します

ステップ 8: Service Provider -> Entity ID \* の下に、https://res.cisco.com/と入力します。

ステップ 9: Service Provider -> Assertion Consumer Service (ACS) URL \*で、 https://res.cisco.com/websafe/ssourlと入力します。

ステップ 10 : Settings -> Nameが表示されるまでスクロールダウンして、新しいアプリケーショ ンのタイトルを入力し、次の図に示すようにSaveを選択します。

Castocard > desications > Citic	to cres			
CISCO CRES		Authentication Log 1 🖹 Remove Application		
See the Generic SSO document	ation [] to integrate Duo into your SAML-enabled service provider.			
Metadata				
Entity ID	https://soc.extended.soc.ducescurity.com/sam@/god	Ceary		
Single Sign-On URL	https://soc.extended.soc.ducescurity.com/sam@/gc@meditud=modescurity/soc	Copy		
Single Log-Out URL	https://wo-entrol.com/sam2/sp/encoreaneaneaneaneaneaneaneaneaneaneaneaneane	Copy		
Metadata URL	https://www.analytics.com/sam@/sp/0	Copy		
Certificate Fingerprint	5			
SHA-1 Fingerprint		Copy		
SHA-256 Fingerprint		Copy		
Downloads				
Certificate	Download certificate Expines: 01-19-2038			
SAM, Metadata	Download XML			
Service Provider				
Entity ID 1	Https://ws.cisco.com/			
	The unique identifier of the service provider.			
Assertion Consumer Service (ACII) URL *	Index () VML* Index () VML* Index () VML* () V	etwate (b)		

ステップ 11CRESポータル<u>https://res.cisco.com/admin/</u>にログインします。

ステップ 12Accountsタブに移動し、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 -> SAML 2.0の順に選択します。

ステップ14:SSO代替電子メール属性名は空白のままにします

ステップ 15: SSOサービスプロバイダーエンティティIDタイプ<u>https://res.cisco.com/</u>

ステップ16:SSOカスタマーサービスURLステップ5でコピーしたURLを貼り付けます

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 : 現在の証明書SSO IDプロバイダー検証証明書 Choose Fileを選択し、次の図に示 すように、ステップ6でダウンロードした証明書を使用します。

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	

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。