Integrazione del servizio Cisco Secure Email Encryption con Duo

Sommario	
Introduzione	
<u>Prerequisiti</u>	
Requisiti	
Componenti usati	
Configurazione	
Verifica	
Errori comuni	

Introduzione

Questo documento descrive come integrare Cisco Secure Email Encryption Service, noto in precedenza come Cisco Registered Envelope Service (CRES), con Duo.

Prerequisiti

Requisiti

- Accesso amministrativo al portale CRES https://res.cisco.com/admin/
- Accesso amministrativo al portale Duo https://admin.duosecurity.com/
- Accesso amministrativo al portale di Azure https://portal.azure.com/
- Gli utenti devono essere registrati nel pannello di amministrazione Duo come descritto in <u>https://duo.com/docs/enrolling-users</u>

Componenti usati

• SAML 2.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Passaggio 1. Accedere a Duo Admin Panel https://admin.duosecurity.com/

Passaggio 2. Passa ad Applicazioni

Passaggio 3. Seleziona applicazione di protezione

Passaggio 4. Seleziona provider di servizi SAML generico e proteggi

Passaggio 5. Copia URL servizio Single Sign-on

Passaggio 6. Selezionare Scarica certificato

Passaggio 7. Selezionare Scarica XML

Passaggio 8. In Service Provider -> Entity ID * digitare https://res.cisco.com/

Passaggio 9. In Service Provider -> Assertion Consumer Service (ACS) URL * digitare <u>https://res.cisco.com/websafe/ssourl</u>

Passaggio 10. Scorrere verso il basso fino a visualizzare Settings-> Name (Impostazioni) e digitare il titolo della nuova applicazione e selezionare Save (Salva), come mostrato nell'immagine:

Cashooard > Applications > CISCO-CRES

CISCO CRES

See the Generic SSO documentation () to integrate Duo into your SAML-enabled service provider.

Metadata				
Entity ID	https://seo additionalities.co.ducescourity.com/sami2/spr3			
Single Sign-On URL	Mgrs://sec antidated.sec.dvcsecurity.com/sami2/gr/3m/01/c0-record/dvmean/v8/sec Copy			
Single Log-Out URL	https://wo-entitiendlaso.ducescurity.com/sami2/up.demonscretes-romeame/site			
Metaduta URL	https://wo-establisheditaso.duceecurity.com/samiC/up/Onicetation.com/samiC/up/SamiC/up/SamiC/up/SamiC/up/SamiC/up/SamiC/s			
Certificate Fingerprints				
SHA-1 Fingerprint	Ansangencipture and an an			
SHA-256 Pingerprint	Cray			
Downloads				
Certificate	Download certificate Expires: 01-19-2038			
SAMI, Mintadata	Download XML			
Service Provider				
Entity ID 1	https://res.sisco.com/			
	The unique identifier of the service provider.			
Assertion Consumer Service	Index () VML * Indexest ()			
OVCIE ONE .	Impo/hes.claco.com/websafe/securi			

Passaggio 11. Accedere al portale CRES https://res.cisco.com/admin/

Passaggio 12. Passare alla scheda Account e selezionare il collegamento ipertestuale per il numero di account

Passaggio 13. Nella scheda Dettagli selezionare Authentication Method -> SAML 2.0

Passaggio 14. Lasciare vuoto il campo Nome attributo e-mail alternativo SSO

Passaggio 15. Tipo di ID entità provider di servizi SSO https://res.cisco.com/

Passaggio 16. URL servizio clienti SSO incollare l'URL copiato nel passaggio 5

Passaggio 17. Lasciare vuoto l'URL di disconnessione SSO

Passaggio 18. Certificato corrente Certificato di verifica del provider di identità SSO selezionare

Authentication Log | 🕆 Remove Application

Choose File e utilizzare il certificato scaricato al punto 6, come mostrato nell'immagine:

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	

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).