Integration des Cisco Secure Email Encryption Service mit Duo

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Überprüfung Häufige Fehler

Einleitung

In diesem Dokument wird die Integration des Cisco Secure Email Encryption Service (CRES) in Duo beschrieben.

Voraussetzungen

Anforderungen

- Administratorzugriff auf das CRES-Portal https://res.cisco.com/admin/
- Administratorzugriff auf das Duo Portal https://admin.duosecurity.com/
- Administratorzugriff auf das Azure-Portal https://portal.azure.com/
- Benutzer müssen beim Duo-Admin-Panel angemeldet sein, wie in <u>https://duo.com/docs/enrolling-users</u> beschrieben.

Verwendete Komponenten

• SAML 2.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Schritt 1: Melden Sie sich bei der Duo-Administratorkonsole an https://admin.duosecurity.com/

Schritt 2: Navigieren zu Anwendungen

- Schritt 3: Anwendung schützen auswählen
- Schritt 4: Wählen Sie Generischer SAML-Dienstanbieter und Schützen
- Schritt 5: Kopieren der URL für die einmalige Anmeldung

Schritt 6: Zertifikat herunterladen auswählen

Schritt 7. XML herunterladen auswählen

Schritt 8: Geben Sie unter Service Provider -> Entity ID * https://res.cisco.com/ ein_

Schritt 9. Geben Sie unter Service Provider -> Assertion Consumer Service (ACS) URL * Folgendes ein: https://res.cisco.com/websafe/ssourl

Schritt 10. Scrollen Sie nach unten, bis **Einstellungen** -> **Name** den Titel Ihrer neuen Anwendung eingeben und **Speichern** auswählen, wie im Bild gezeigt:

Castocard > depications > 0	ISCO-DRES	
CISCO CRES	5	Authentication Log 🕆 Remove Application
See the Generic SSO docum	entation () to integrate Duo into your SAML-enabled service provider.	
Metadata		
Entity ID	https://soo	Copy
Single Sign-On URL	https://www.autologia.co.duceecurity.com/sam@/gr/ dmad/sdmaserder.co.ma /see	Copy
Single Log-Out URL	https://so-additional.aso.duosecurity.com/aam@/up/amorono.com/aam@/up/aao	Copy
Metadata URL	Attps://so-entities.co.duceecurity.com/sam@tp/Oentities.com/sam@tmetadat	Сору
Certificate Fingerpri	ints	
SHA-1 Fingerprint		Copy
SHA-256 Fingerprint		Copy
Downloads		
Gertificate	Download certificate Expines: 01-19-2038	
SAM, Metadata	Download XMs.	
Service Provider		
Entity ID 1	https://res.cisco.com/	
	The unique identifier of the service provider.	
Assertion Consumer Service	Index () UVEL*	O There
lycal ner .	1 https://res.ciaco.com/websafe/securi	•

Schritt 11. Melden Sie sich beim CRES-Portal an: https://res.cisco.com/admin/

Schritt 12: Navigieren Sie zur Registerkarte Accounts (Konten), und wählen Sie den Hyperlink für Ihre Kontonummer aus.

Schritt 13: Wählen Sie auf der Registerkarte Details die Option Authentication Method -> SAML 2.0 aus.

Schritt 14: Name des alternativen E-Mail-Attributs für SSO leer lassen

Schritt 15: SSO-Dienstanbieter-Element-ID Typ https://res.cisco.com/

Schritt 16: SSO-Kundenservice-URL: Fügen Sie die in Schritt 5 kopierte URL ein.

Schritt 17: URL für SSO-Abmeldung leer lassen

Schritt 18: Aktuelles Zertifikat SSO-Identitätsanbieter-Verifizierungszertifikat Wählen Sie Choose File aus, und verwenden Sie das in Schritt 6 heruntergeladene Zertifikat, wie im Bild gezeigt:

Home Users Repo	ACCOUNTS .
Manage Accou	nts Manage Registered Envelopes
Details Groups 1	lokens BCE Config Addin Config Brand
Account Number	A. 1999
Account Name*	EFSEDOMAIN
Description	Trisaponain
Status	Action
Enable Auto Provisioning	0
Rulefat	All V
Enable Sender	
Registration	0
Make Secure Compose Available	
Suppress Java Applet in	-
Envelope	
Envelope Account Certificate	Reponente
Envelope Account Certificate On TLS failure choose on	Reponents
Envelope Account Certificate On TLS failure choose on	Regenerate e of the following delivery preferences fallback to Registered Envelope Delivery
Envelope Account Certificate On TLS failure choose on	Regenerate e of the following delivery preferences falback to Registered Envelope Delivery bounce Messages
Envelope Account Certificate On TLS failure choose on Ut TLS failure delivery pro	Repenente e of the following delivery preferences e following delivery preferences following delivery preferences following delivery preferences set to Applicated Envelope, please remer
Envelope Account Certificate On TLS failure choose on UTLS failure delivery pro change the TLS delivery	Regenerate e of the following delivery preferences follback to Registered Envelope Delivery bounce Messages remons is set to Registered Envelope, please remer option to TLS Preferred on your in house mail serve
Envelope Account Certificate On TLS failure choose on If TLS failure delivery you change the TLS delivery Authentication Hethod	Regenerate er the following delivery preferences following delivery preferences following delivery house Messages forman is set to Registered Envelope, please reme poten to TLS Preferred on your in house mail serve (SAML 2.0 v)
Envelope Account Certificate On TLS failure choose on If TLS failure delivery you change the TLS delivery Authentication Method SSO Enable Date	Begenerate ef the following delivery preferences fatback is Rejatents (Envirigie Delivery bounce Messages therence is set to Replatent (Envirigie, please remer glatback 2.0 m) (SAML 2.0 m)
Envelope Account Certificate On TLS failure choose on U H TLS failure delivery or change the TLS delivery Authentication Method SSO Enable Date SSO Enable Date SSO Enable Date	ef the following delivery preferences e of the following delivery preferences fallback to Registered Envelope, please remer plotonce to Registered Envelope, please remer plotonce to TuS Preferred on your in house mail serve (SAML 2.0 v) 07/07/2023 06:141:48 AM GMT transient
Envelope Account: Cartificate On TLS failure choose on On TLS failure choose on On TLS failure delivery pri change the TLS delivery in Authentication Method SSO Email Name ID Format SSO Attante Email	Regenerate e of the following delivery preferences fallback to Registered Envelope Delivery bounce Messages fremence is set to Registered Envelope, please nemer sptien to TLS Preferred en your in house mail serve (SAML 2.0 ~) 0/107/2023 06:14:48 AM GMT transient
Envelope Account: Certificate On TLS failure choose on US TLS failure delivery por change the TLS delivery Authentication Method SSO Enable Date SSO Enable Date SSO Enable Name ID Format SSO Enable Rame	Begenerate ef the following delivery preferences fallback is Replatered Envelope Delivery bounce Messages therence is set to Replatered Envelope, please remer gotton to TLS Preferred on your in house mail serve SAML 2.0 Ory07/0223 06:14:48 AM GMT transient
Envelope Account Certificate On TLS failure choose on Certificate In TLS failure delivery on Center of the TLS delivery of Authentication Method SSO Enable Date SSO Enable Date SSO Enable Date SSO Enable Date SSO Enable Date SSO Enable Date SSO Astronate Email Astrolute Name SSO Service Provider Encep 30 ⁻⁴	Bagenerate ef the following delivery preferences fatback is Rejistent Envirigie Delivery bounce Mesages therence is set to Replatent Envirigie, please reme gisten to TLS Preferred in your in house mail serve BAML 2.0 * 07/07/2023 06:14:48 AM GMT themsient themsient
Envelope Account Certificate On TLS failure choose on Certificate ITLS failure delivery on Authentication Method SSO Enable Date SSO Enable Da	Bagenerate ef the following delivery preferences ef the following delivery preferences fallacia to Replatered Envelope, please reme plance Messages derence its set to Replatered Envelope, please reme SAML 2.0 * 07/07/2023 06:14:48 AM GMT transient
Envelope Account: Certificate On TLS failure choose on Certificate If TLS failure delivery pro- change the TLS delivery dhange the TLS delivery authentication Method SSO Enable Date SSO Enable Date SSO Enable Date SSO Account Provider Enable Name SSO Service Provider Enable 201 SSO Counter Service URL*	
Envelope Account: Certificate On TLS failure choose on Certificate (hange the TLS delivery of Authentication Method Sol Enable Date SSO Enable Date SSO Enable Date SSO Enable Date SSO Enable Date SSO Assences Enable SSO Assences Enable SSO Catationer Service URL SSO Costomer Service URL SSO Service Provider URL SSO Service Provider URL SSO Service Provider URL	Begenerate ef the following delivery preferences fallack to Registered Envelope Delivery bounce Messages fallack to Registered Envelope, please reme point to TLS Preferred on your in house mail serve (SAML 2.0 v) 07/07/2023 06:14:48 AM GMT transient (mps://res.does.com/ fmps://res.does.com/ (mps://res.does.com/ (mps://res.does.com/)
Envelope Account Certificate On TLS failure choose on U TLS failure choose on U TLS failure choose on U TLS failure cellerry on U TLS failure cellerry on U TLS failure choose on SSO Enable Date SSO Enable Date SSO Enable Date SSO Enable Date SSO Enable Date SSO Enable Choose TLS SSO Enable TLS SSO Enable TLS SSO Legout URL SSO Sancios Provider Werthcates Certificate SSO Banding	
Envelope Account Certificate On TLS failure choose on Certificate Of TLS failure choose on Certificate Of TLS failure choose of Of Certificate SSO Enable Date SSO Enable Date SSO Enable Date SSO Enable Date SSO Enable Date SSO Enable Service Format SSO Enable Service Format SSO Enable Provider Vertification Certificate SSO Bending SSO Assertson Consumer UR.	
Envelope Account Certificate On TLS failure choose on TLS failure choose on Certificate I TLS failure delivery on Authentication Method S50 Enable Date S50 En	Additional and a second s

Schritt 19: Melden Sie sich beim Azure-Portal an https://portal.azure.com/

Schritt 20: Navigieren Sie zu Azure Active Directory -> Enterprise Applications -> Neue Anwendung -> Eigene Anwendung erstellen

Schritt 21: Benennen Sie Ihre Anwendung und wählen Sie Alle anderen Anwendungen integrieren, die Sie nicht in der Galerie finden (Nicht-Galerie) -> Erstellen

Schritt 22: Wählen Sie **Benutzer und Gruppen zuweisen aus**, fügen Sie die Benutzer hinzu, die Zugriff auf CRES erhalten sollen, und wählen Sie **Zuweisen** aus.

Schritt 23: Wählen Sie **Single sing-on** -> **SAML** -> **Upload metadaten-Datei**, und wählen Sie die Datei, die in Schritt 7 heruntergeladen wurde, wie im Bild gezeigt:



Überprüfung

Schritt 1: Melden Sie sich beim CRES-Portal https://res.cisco.com/websafe/ an, wie im Bild gezeigt:

Secure Email
Encryption Service
Username* cresduo@mexesa.com
Log In
OR
G Sign in with Google

Schritt 2: Verwenden Sie den Hauptschlüssel für DUO, wie im Bild gezeigt:



Schritt 3: Sobald Sie den richtigen Passkey festgelegt haben, können Sie sich erfolgreich beim CRES-Portal anmelden, wie in der Abbildung gezeigt:

CISCO Secure Email Encryption Service	
New "Time Zone" and "Time Format" configura Mallage messages	tions have been added, allowing you to control the display of dates and times. Currently you're using the default of GMT in 12 hour format. That
/ Compose Message	
Address Book	CC [†]
🧭 Edit Profile	BCC†
	Subject
	(none)
	f = At least one valid recipient must be entered.
	Consider © 2022 Clean System for and/or its affiliates All rights researed. About Literes of Sandes Drivery Delicy Outcomer support

Häufige Fehler

1. Wenn der Benutzer nicht unter **Benutzer und Gruppen** in der **Enterprise-Anwendung** zugewiesen ist, wird dieser Fehler angezeigt, wie im Bild gezeigt:



If you plan on getting help for this problem, enable flagging and try to reproduce the error within 20 minutes. Flagged events make diagnostics available and are raised to admin attention.

2. Wenn der Benutzer aus **Benutzern** im Duo-Administratorbereich entfernt wird, wird dieser Fehler angezeigt, wie in der Abbildung gezeigt:

cisco

Account disabled

Your Duo account is disabled and cannot access this application. Please contact your IT help desk.

Secured by Duo

3. Wenn der Benutzer nicht im Duo-Administratorbereich registriert ist, wird dieser Fehler angezeigt, wie in der Abbildung gezeigt:

Secure Email Encryption Service



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.