

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 <https://duo.com/docs/enrolling-users> 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:

The screenshot shows the Cisco CRES configuration interface. It includes sections for Metadata (Entity ID, Single Sign-On URL, Single Log-Out URL, Metadata URL), Certificate Fingerprints (SHA-1, SHA-256), Downloads (Certificate, SAML Metadata), and Service Provider (Entity ID, Assertion Consumer Service (ACS) URL). The Entity ID field contains 'https://res.cisco.com/' and the ACS URL field contains 'https://res.cisco.com/websafe/ssourl'.

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:

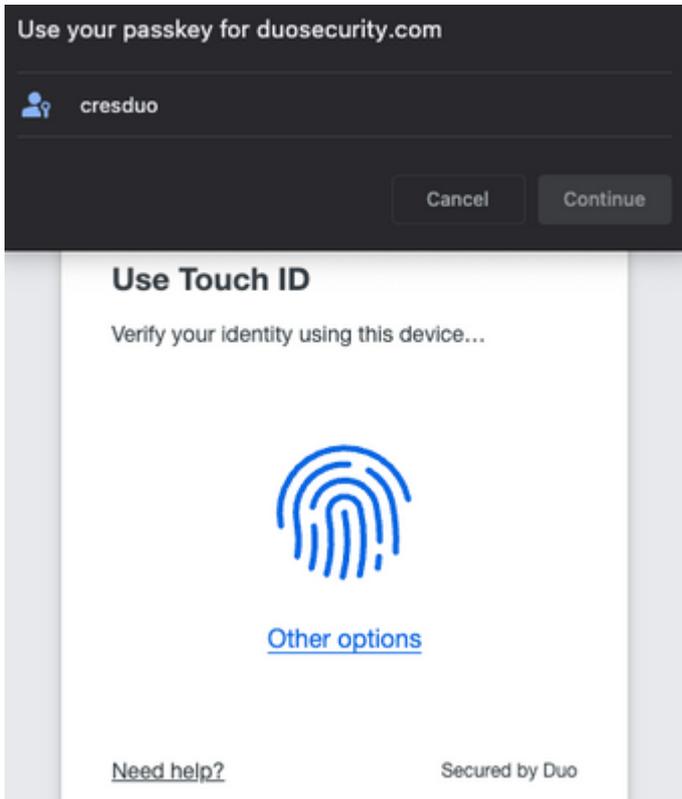
Schritt 19: Melden Sie sich beim Azure-Portal an <https://portal.azure.com/>

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

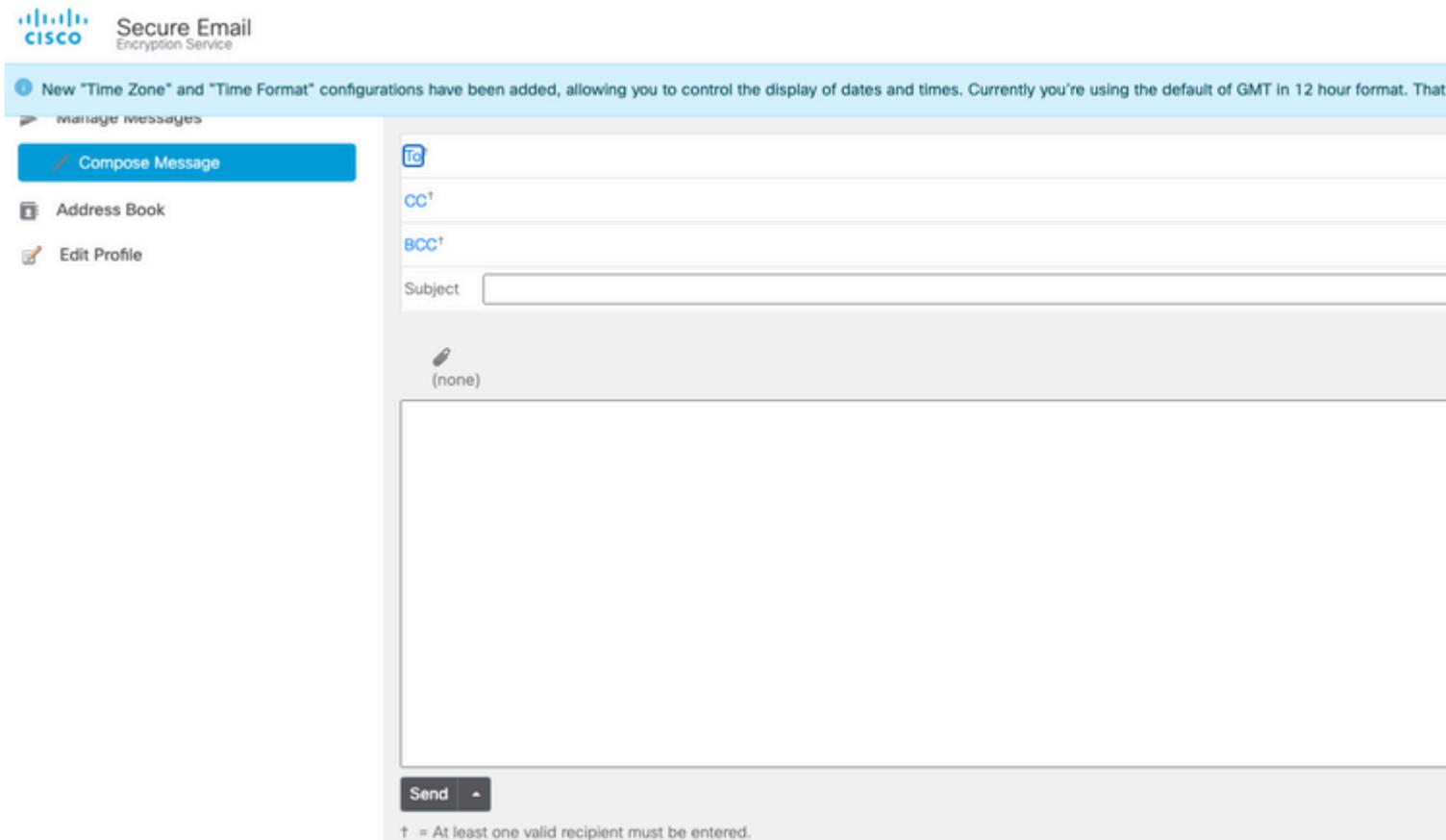
Schritt 21: Benennen Sie Ihre Anwendung und wählen Sie **Alle anderen Anwendungen integrieren, die Sie nicht in der Galerie finden (Nicht-Galerie)** -> **Erstellen**

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 sign-on** -> **SAML** -> **Upload metadaten-Datei**, und wählen Sie die Datei, die in Schritt 7 heruntergeladen wurde, 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:



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:



DUO SSO

Sorry, but we're having trouble signing you in.

AADSTS50105: Your administrator has configured the application DUO SSO ('7a868b56-764f-4071-96f6-f9608c0ead2e') to block users unless they are specifically granted ('assigned') access to the application. The signed in user 'creduo@mexesa.com' is blocked because they are not a direct member of a group with access, nor had access directly assigned by an administrator. Please contact your administrator to assign access to this application.

Troubleshooting details

If you contact your administrator, send this info to them.

[Copy info to clipboard](#)

Request id: 0e51cd84-ee3-4923-3d33-21747760500

Correlation id: d6f9d134-0823-4cce-a906-a3a4a942f911

Timestamp: 2023-07-12T03:54:13Z

Message: AADSTS50105: Your administrator has configured the application DUO SSO ('7a868b56-764f-4071-96f6-f9608c0ead2e') to block users unless they are specifically granted ('assigned') access to the application. The signed in user 'creduo@mexesa.com' is blocked because they are not a direct member of a group with access, nor had access directly assigned by an administrator. Please contact your administrator to assign access to this application.

Flag sign-in errors for review: [Enable flagging](#)

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:



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

Username*

 You entered an incorrect email address.

Log In

OR

 Sign in with Google

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.