

# 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 is populated with 'https://res.cisco.com/' and the ACS URL field is populated with 'https://res.cisco.com/websafe/ssourl'. There are also 'Copy' buttons for each metadata and fingerprint field, and 'Download certificate' and 'Download XML' buttons in the Downloads section.

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:

Account Number: A\_123456  
 Account Name\*: ESADOMAIN  
 Description: ESADOMAIN  
 Status: Active  
 Enable Auto Provisioning:   
 RuleSet: All  
 Enable Sender Registration:   
 Make Secure Compose Available:   
 Suppress Java Applet in Envelope:   
 Account Certificate: Regenerate  
 On TLS failure choose one of the following delivery preferences:  
 Fallback to Registered Envelope Delivery  
 Bounce Messages  
 If TLS failure delivery preference is set to Registered Envelope, please remember to change the TLS delivery option to TLS Preferred on your in house mail server.  
 Authentication Method: SAML 2.0  
 SSO Enable Date: 03/03/2023 06:14:48 AM GMT  
 SSO Email Name ID Format: transient  
 SSO Alternate Email Attribute Name:  
 SSO Service Provider Entity ID\*: https://yes.cisco.com/  
 SSO Customer Service URL\*: https://ssc-~~xxxxxx~~ sso.duosecure.com  
 SSO Logout URL:  
 SSO Service Provider Verification Certificate: Download  
 SSO Binding: HTTP-Redirect, HTTP-POST  
 SSO Assertion Consumer URL: https://yes.cisco.com/webSAFE/ssourl  
 Current Certificate: CN=~~XXXXXXXXXXXXXXXXXXXX~~, O=Duo Security  
 SSO Identity Provider Verification Certificate\*: Choose File No file chosen  
 Save Back to Accounts List

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:

**DUO SSO | SAML-based Sign-on**

Overview | Deployment Plan | Diagnose and solve problems | Manage

Properties | Users and groups | Provisioning | Application proxy | Self service | Custom security attributes (optional) | Security | Conditional Access | Permissions | Token encryption | Activity | Sign-in logs | Usage & insights | Audit logs | Provisioning logs | Access reviews | Troubleshooting & Support | New support request

### Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, stability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more](#)

Read the [configuration guide](#) if you help integrating DUO SSO.

- Basic SAML Configuration**

Identifier (Entity ID)	<a href="https://res.*****.com/duosecurity.com/saml2/idp/REVISION/instadate">https://res.*****.com/duosecurity.com/saml2/idp/REVISION/instadate</a>
Reply URL (Assertion Consumer Service URL)	<a href="https://res.*****.com/duosecurity.com/saml2/idp/REVISION/instadate">https://res.*****.com/duosecurity.com/saml2/idp/REVISION/instadate</a>
Sign on URL	Optional
Relay State (Optional)	Optional
Logout URL (Optional)	Optional
- Attributes & Claims**

Email	user.mail
Username	user.username
FirstName	user.givenname
LastName	user.surname
DisplayName	user.displayName
Unique User Identifier	user.username
- SAML Certificates**

Token signing certificate	Active
Status	7/6/2024, 10:43:02 PM
Thumbprint	*****
Expiration	*****
Notification Email	*****
App Federation Metadata URL	<a href="https://login.microsoftonline.com/*****">https://login.microsoftonline.com/*****</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Hex)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

**Verification certificates (optional)**

Required	No
Active	0
Expired	0
- Set up DUO SSO**

You'll need to configure the application to link with Azure AD.

Login URL	<a href="https://login.microsoftonline.com/*****">https://login.microsoftonline.com/*****</a>
Azure AD Identifier	<a href="https://sts.windows.net/*****">https://sts.windows.net/*****</a>
Logout URL	<a href="https://login.microsoftonline.com/*****/wac/logout">https://login.microsoftonline.com/*****/wac/logout</a>
- Test single sign-on with DUO SSO**

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

[Test](#)

## Überprüfung


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

# Secure Email Encryption Service

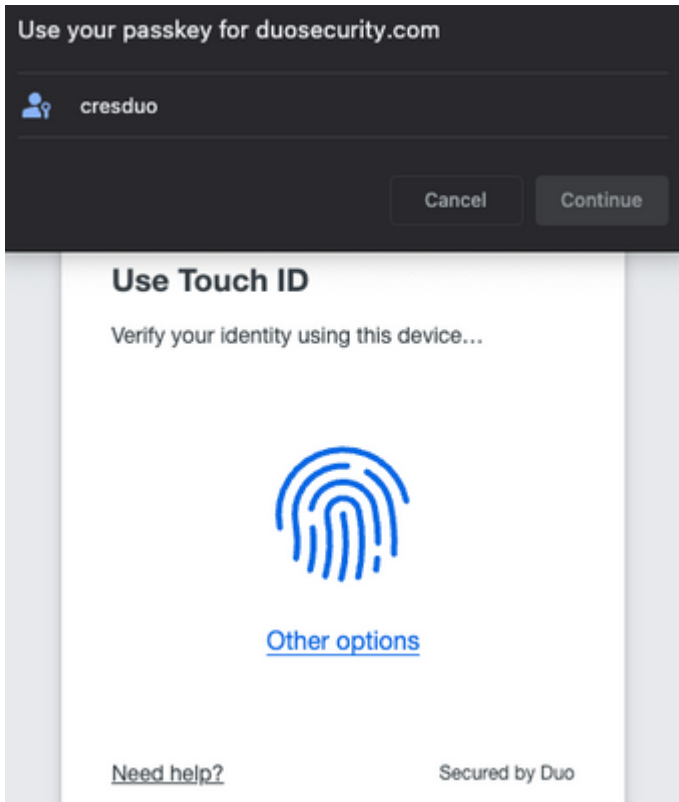
Username\*

**Log In**

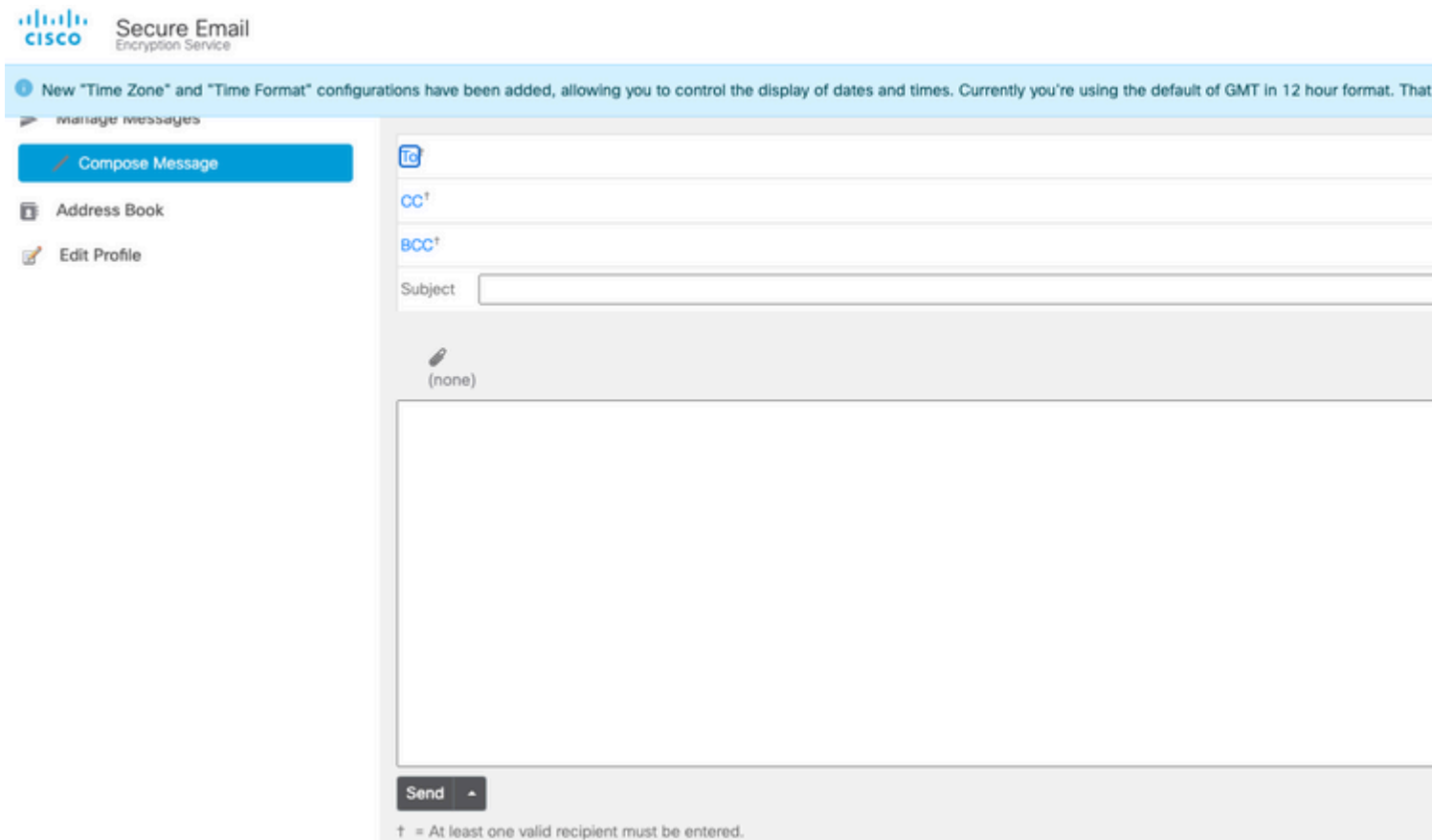
OR

 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:



## 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-f9808c0ead2e') to block users unless they are specifically granted ('assigned') access to the application. The signed in user 'cred Duo@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:** d8f9d134-0823-4cce-a906-a3a4a942f911

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

**Message:** AADSTS50105: Your administrator has configured the application DUO SSO ('7a868b56-764f-4071-96f6-f9808c0ead2e') to block users unless they are specifically granted ('assigned') access to the application. The signed in user 'cred Duo@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.