

Integrate Cisco Secure Email Encryption Service with Duo

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Verify](#)

[Common Errors](#)

Introduction

This document describes how to integrate Cisco Secure Email Encryption Service, formerly known as Cisco Registered Envelope Service (CRES), with Duo.

Prerequisites

Requirements

- Admin access to CRES portal <https://res.cisco.com/admin/>
- Admin access to Duo portal <https://admin.duosecurity.com/>
- Admin access to Azure portal <https://portal.azure.com/>
- Users need to be enrolled in Duo Admin Panel as described in <https://duo.com/docs/enrolling-users>

Components Used

- SAML 2.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Step 1. Log in to Duo Admin Panel <https://admin.duosecurity.com/>

Step 2. Navigate to **Applications**

Step 3. Select **Protect Application**

Step 4. Select **Generic SAML Service Provider** and **Protect**

Step 5. Copy the **Single Sign-On URL**

Step 6. Select **Download Certificate**

Step 7. Select **Download XML**

Step 8. Under **Service Provider** -> **Entity ID** * type <https://res.cisco.com/>

Step 9. Under **Service Provider** -> **Assertion Consumer Service (ACS) URL**
* type <https://res.cisco.com/websafe/ssourl>

Step 10. Scroll down until you see **Settings** -> **Name** type the title of your new application and select **Save**, as shown in the image:

The screenshot shows the Cisco CRES configuration interface. At the top, it says 'CISCO CRES' and 'Authentication Log | Remove Application'. Below this, there is a link to 'Generic SSO documentation'. The main configuration area is divided into several sections:

- Metadata:** Contains four input fields for Entity ID, Single Sign-On URL, Single Log-Out URL, and Metadata URL, each with a 'Copy' button.
- Certificate Fingerprints:** Contains two input fields for SHA-1 Fingerprint and SHA-256 Fingerprint, each with a 'Copy' button.
- Downloads:** Contains two buttons: 'Download certificate' (with an expiration date of 01-19-2038) and 'Download XML'.
- Service Provider:** Contains an input field for 'Entity ID *' with the value 'https://res.cisco.com/' and a note: 'The unique identifier of the service provider.'
- Assertion Consumer Service (ACS) URL:** Contains a table with one row. The 'Index' is '1', the 'URL' is 'https://res.cisco.com/websafe/ssourl', and the 'isDefault' checkbox is checked.

Step 11. Log in to the CRES portal <https://res.cisco.com/admin/>

Step 12. Navigate to the **Accounts** tab and select the hyperlink for your **Account Number**

Step 13. Under the Details tab select **Authentication Method** -> **SAML 2.0**

Step 14. Leave **SSO Alternate Email Attribute Name** blank

Step 15. **SSO Service Provider Entity ID** type <https://res.cisco.com/>

Step 16. **SSO Customer Service URL** paste the URL you copied in Step 5

Step 17. Leave **SSO Logout URL** blank

Step 18. **Current Certificate SSO Identity Provider Verification Certificate** select **Choose File** and use the certificate downloaded in step 6, as shown in the image:

Account Number: A: [redacted]
 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-external.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/web/safe/ssourl
 Current Certificate: CN=CAMM...-Duo Security
 SSO Identity Provider Verification Certificate*: Choose File No file chosen
 Save Back to Accounts List

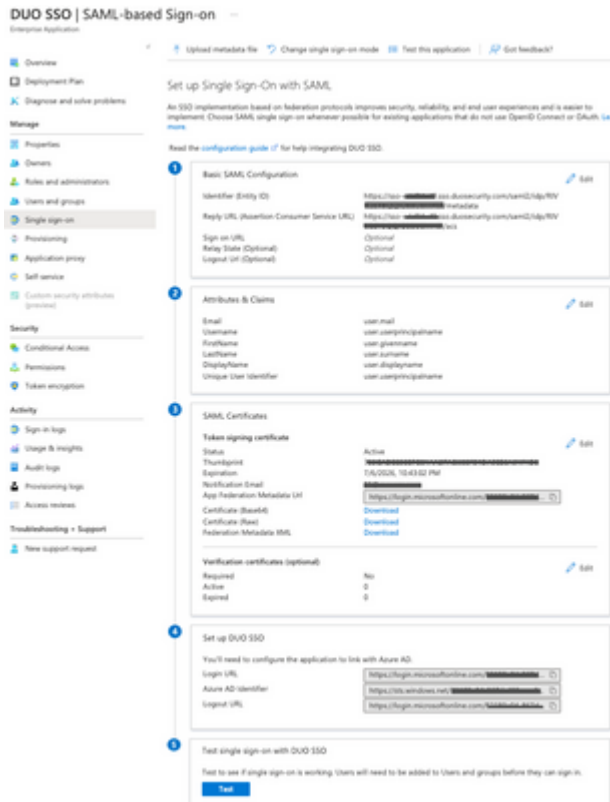
Step 19. Log in to Azure portal <https://portal.azure.com/>

Step 20. Navigate to **Azure Active Directory -> Enterprise Applications -> New application -> Create your own application**

Step 21. Name your application and select **Integrate any other application you don't find in the gallery (Non-gallery) -> Create**

Step 22. Select **Assign users and groups** and add the users you want to have access to CRES and select **Assign**

Step 23. Select **Single sign-on -> SAML -> Upload metadata file**, and select the file downloaded in step 7, as shown in the image:



Verify

Step 1. Log in to the CRES portal <https://res.cisco.com/websafe/>, as shown in the image:

Secure Email Encryption Service

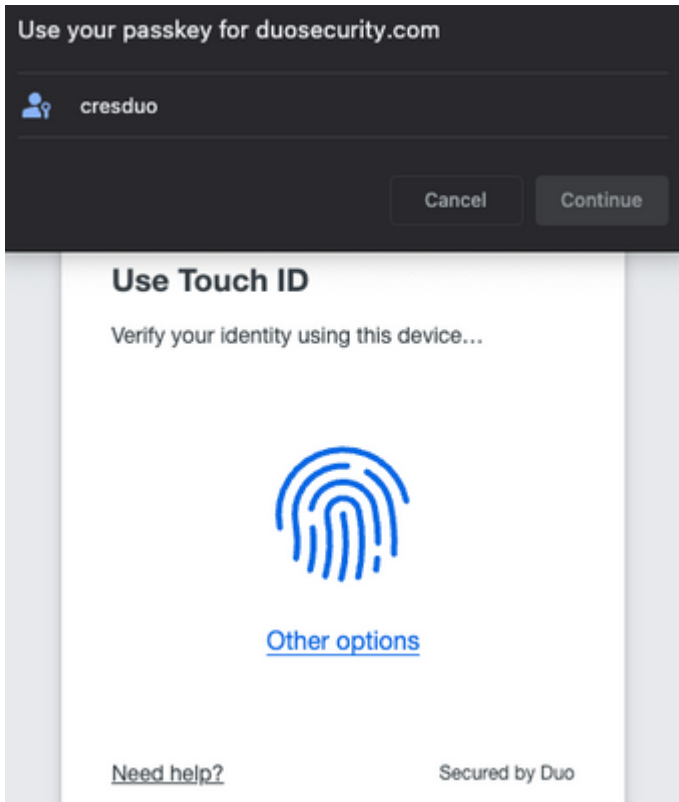
Username*
cresduo@mexesa.com

Log In

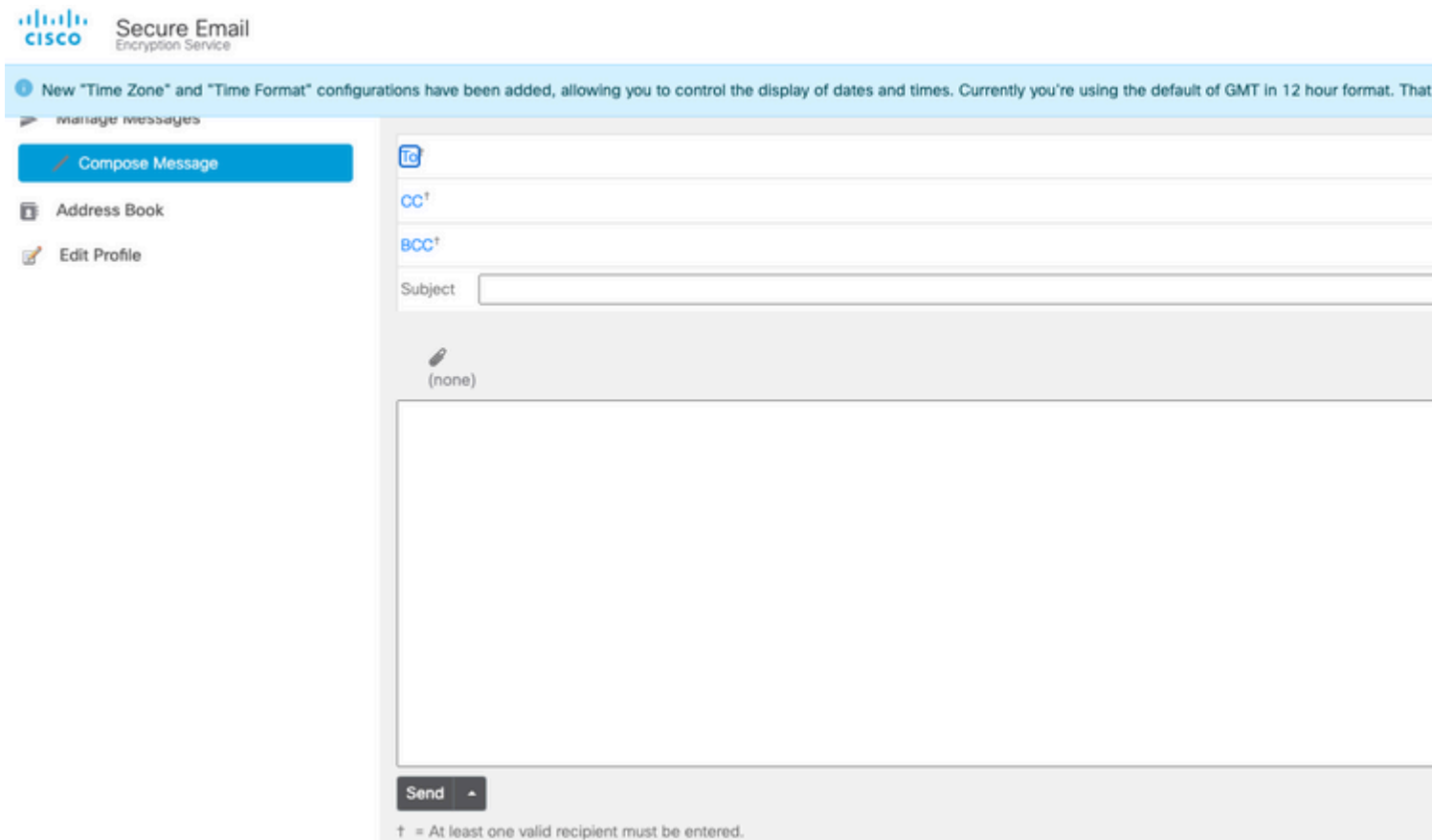
OR

 Sign in with Google

Step 2. Use the passkey for DUO, as shown in the image:



Step 3. Once you set the proper passkey, you will be able to login successfully into the CRES portal, as shown in the image:



Common Errors

1. If the user is not assigned under **Users and Groups** in the **Enterprise Application**, you get this error, as shown in the image:



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-cee3-4923-3d33-21747760500

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. If the User is removed from **Users** in the Duo Admin Panel, you get this error, as shown in the image:



Account disabled

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

Secured by Duo

3. If the User is not enrolled in the Duo Admin Panel, you get this error, as shown in the image:


Secure Email Encryption Service

Username*

 You entered an incorrect email address.

Log In

OR

 Sign in with Google