

Integre Cisco Secure Email Encryption Service con Duo

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificación](#)

[Errores comunes](#)

Introducción

Este documento describe cómo integrar Cisco Secure Email Encryption Service, anteriormente conocido como Cisco Registered Envelope Service (CRES), con Duo.

Prerequisites

Requirements

- Acceso de administrador al portal de CRES <https://res.cisco.com/admin/>
- Acceso de administrador al portal Duo <https://admin.duosecurity.com/>
- Acceso de administrador al portal de Azure <https://portal.azure.com/>
- Los usuarios deben estar inscritos en el panel de administración de Duo, como se describe en <https://duo.com/docs/enrolling-users>

Componentes Utilizados

- SAML 2.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Paso 1. Inicie sesión en Duo Admin Panel <https://admin.duosecurity.com/>

Paso 2. Vaya a **Aplicaciones**

Paso 3. Seleccione **Proteger aplicación**

Paso 4. Seleccione **Generic SAML Service Provider** y **Protect**

Paso 5. Copiar la **URL de inicio de sesión único**

Paso 6. Seleccione **Descargar certificado**

Paso 7. Seleccione **Descargar XML**

Paso 8. En **Service Provider** -> **Entity ID** * escriba <https://res.cisco.com/>

Paso 9. En **Service Provider** -> **Assertion Consumer Service (ACS) URL** * escriba <https://res.cisco.com/websafe/ssourl>

Paso 10. Desplácese hacia abajo hasta que vea **Settings** -> **Name** escriba el título de su nueva aplicación y seleccione **Save**, como se muestra en la imagen:

The screenshot shows the Cisco CRES configuration interface. At the top, there is a breadcrumb trail: Dashboard > Applications > CISCO CRES. The main heading is 'CISCO CRES' with a sub-heading 'Authentication Log' and a 'Remove Application' button. Below this, there is a link to 'Generic SSO documentation' for integrating Duo into a SAML-enabled service provider.

The 'Metadata' section contains four input fields, each with a 'Copy' button:

- Entity ID: <https://sso.██████████.sso.duosecurity.com/saml2/sp/██████████-metadata>
- Single Sign-On URL: <https://sso.██████████.sso.duosecurity.com/saml2/sp/██████████-sso>
- Single Log-Out URL: <https://sso.██████████.sso.duosecurity.com/saml2/sp/██████████-slo>
- Metadata URL: <https://sso.██████████.sso.duosecurity.com/saml2/sp/██████████-metadata>

The 'Certificate Fingerprints' section contains two input fields, each with a 'Copy' button:

- SHA-1 Fingerprint: [Redacted]
- SHA-256 Fingerprint: [Redacted]

The 'Downloads' section contains two buttons:

- Download certificate: Expires: 01-19-2038
- Download XML

The 'Service Provider' section contains an input field for 'Entity ID *' with the value 'https://res.cisco.com/' and a note: 'The unique identifier of the service provider.'

The 'Assertion Consumer Service (ACS) URL' section contains an input field with the value 'https://res.cisco.com/websafe/ssourl' and a dropdown menu set to 'Default'.

Paso 11. Inicie sesión en el portal de CRES <https://res.cisco.com/admin/>

Paso 12. Navegue hasta la pestaña **Cuentas** y seleccione el hipervínculo para su **Número de cuenta**

Paso 13. En la ficha Detalles, seleccione **Método de autenticación** -> **SAML 2.0**

Paso 14. Deje en blanco **SSO Nombre de atributo de correo electrónico alternativo**

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

Paso 16. **SSO Customer Service URL** pegue la URL que copió en el paso 5

Paso 17. Deje en blanco **SSO Logout URL**

Paso 18. **Certificado actual Certificado de verificación del proveedor de identidad SSO** seleccione **Choose File** y utilice el certificado descargado en el paso 6, como se muestra en la imagen:

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://yes-cisco.com/ssp_duosecure/
 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/issourl
 Current Certificate: CN=ESADOMAIN, O=Duo Security
 SSO Identity Provider Verification Certificate*: Choose File No file chosen
 Save Back to Accounts List

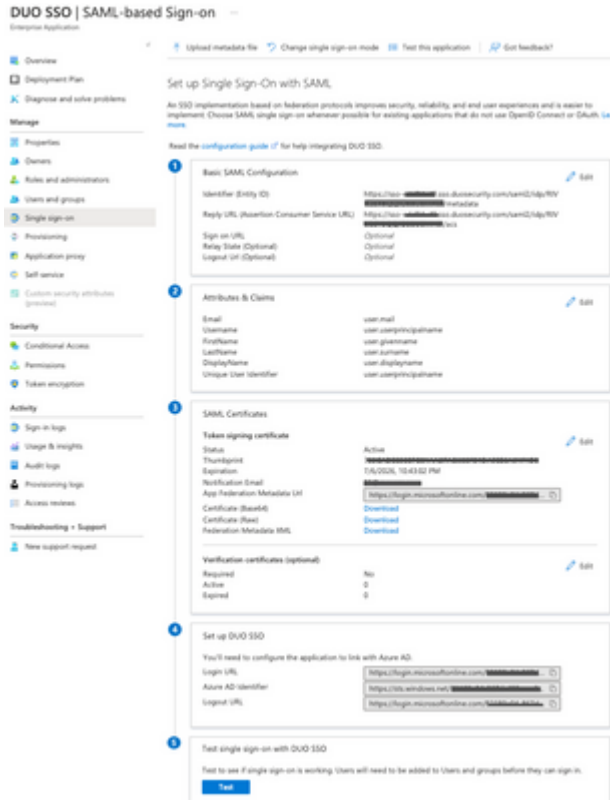
Paso 19. Inicie sesión en el portal de Azure <https://portal.azure.com/>

Paso 20. Vaya a **Azure Active Directory** -> **Enterprise Applications** -> **New application** -> **Create your own application** (Azure Active Directory-> Aplicaciones empresariales -> Nueva aplicación)

Paso 21. Asigne un nombre a la aplicación y seleccione **Integrar cualquier otra aplicación que no encuentre en la galería** (No galería) -> **Crear**

Paso 22. Seleccione **Assign users and groups** y agregue los usuarios que desea tener acceso a CRES y seleccione **Assign** .

Paso 23. Seleccione **Single Sign-on** -> **SAML** -> **Upload metadata file**, y seleccione el archivo descargado en el paso 7, como se muestra en la imagen:



Verificación

Paso 1. Inicie sesión en el portal de CRES <https://res.cisco.com/websafe/>, como se muestra en la imagen:

Secure Email Encryption Service

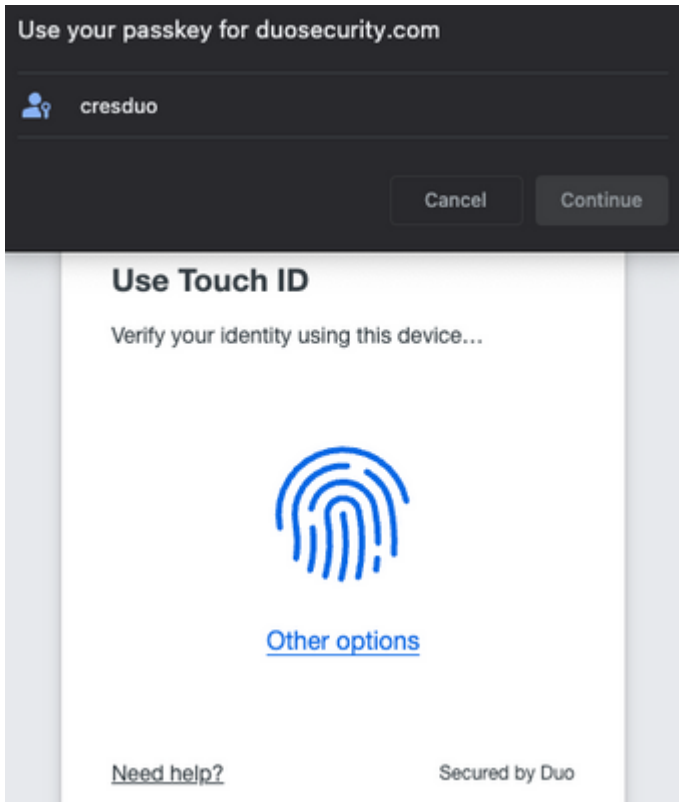
Username*
cresduo@mexesa.com

Log In

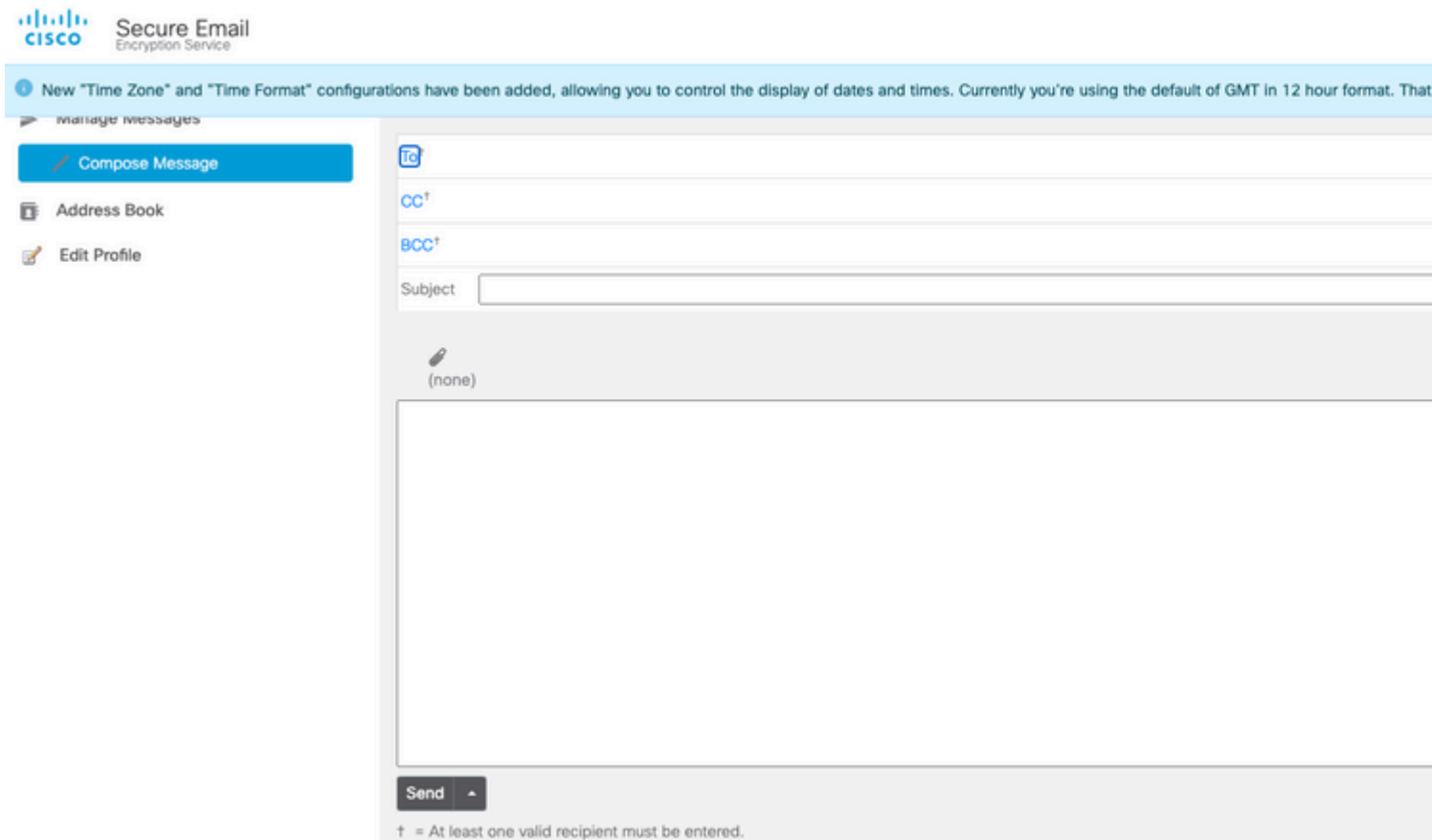
OR

Sign in with Google

Paso 2. Utilice la clave de paso para DUO, como se muestra en la imagen:



Paso 3. Una vez que haya establecido la clave de paso adecuada, podrá iniciar sesión correctamente en el portal de CRES, como se muestra en la imagen:



Errores comunes

1. Si el usuario no está asignado en **Usuarios y grupos** en la **aplicación de empresa**, se obtiene este error, como se muestra en la imagen:



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 '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: 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 '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. Si el usuario se elimina de **Usuarios** en el Duo Admin Panel, obtiene este error, como se muestra en la imagen:



Account disabled

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

Secured by Duo

3. Si el usuario no está inscrito en el panel de administración Duo, obtendrá este error, como se muestra en la imagen:


Secure Email Encryption Service

Username*

 You entered an incorrect email address.

Log In

OR

 Sign in with Google

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).