

Cisco Secure E-mail encryptie-service integreren met Duo

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Verifiëren](#)

[Veelvoorkomende fouten](#)

Inleiding

Dit document beschrijft hoe u de Cisco Secure Email Encryption Service (CRES), voorheen bekend als Cisco Registered Envelope Service, met Duo kunt integreren.

Voorwaarden

Vereisten

- Admin-toegang tot CRES-portal <https://res.cisco.com/admin/>
- Admin-toegang tot Duo-portal <https://admin.duosecurity.com/>
- Admin-toegang tot Azure-portal <https://portal.azure.com/>
- Gebruikers moeten worden aangemeld bij het Duo Admin Panel zoals beschreven in <https://duo.com/docs/enrolling-users>

Gebruikte componenten

- SAML 2.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Stap 1. Log in op het Duo Admin Panel <https://admin.duosecurity.com/>

Stap 2. Naar **toepassingen** navigeren

Stap 3. Selecteer **Protect Application**

Stap 4. Selecteer **Generieke SAML-serviceprovider** en **bescherm**

Stap 5. De **URL voor eenmalige aanmelding** kopiëren

Stap 6. Selecteer **Downloadcertificaat**

Stap 7. Selecteer **Download XML**

Stap 8. Onder **Serviceprovider** -> **Identiteitskaart van entiteit** * type <https://res.cisco.com/>

Stap 9. **URL voor** onder **Serviceprovider** -> **Assertion Consumer Service (ACS)** * type <https://res.cisco.com/websafe/ssourl>

Stap 10. Blader naar beneden totdat u **Instellingen** ziet -> **Naam** typt de titel van uw nieuwe toepassing en selecteer **Opslaan**, zoals in de afbeelding:

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

- Metadata:** Contains four input fields with 'Copy' buttons: Entity ID, Single Sign-On URL, Single Log-Out URL, and Metadata URL. All fields contain a long, complex URL.
- Certificate Fingerprints:** Contains two input fields with 'Copy' buttons: SHA-1 Fingerprint and SHA-256 Fingerprint. Both fields contain long hexadecimal strings.
- Downloads:** Contains two buttons: 'Download certificate' (with 'Expires: 01-19-2038' next to it) and 'Download XML'.
- Service Provider:** Contains an 'Entity ID' input field with the value 'https://res.cisco.com/' and a note: 'The unique identifier of the service provider.'
- Assertion Consumer Service (ACS) URL:** Contains an 'Index' dropdown set to '1', an 'URL' input field with the value 'https://res.cisco.com/websafe/ssourl', and an 'isDefault' dropdown set to 'Default'.

Stap 11. Meld u aan bij het CRES-portaal <https://res.cisco.com/admin/>

Stap 12. Navigeer naar het tabblad **Accounts** en selecteer de hyperlink voor uw **accountnummer**

Stap 13. Selecteer onder het tabblad Details de optie **Verificatiemethode** -> **SAML 2.0**

Stap 14. Laat **SSO Alternate Email Attribute Naam** leeg

Stap 15. ID-type **entiteit-id voor SSO-serviceproviders** <https://res.cisco.com/>

Stap 16. De **klantenservice-URL** van SSO plakt de URL die u in Stap 5 hebt gekopieerd

Stap 17. **URL-lege aanmelding voor SSO** laten

Stap 18. **Huidig certificaat van de SSO Identity Provider Verification Certificate** Selecteer **Bestand kiezen** en gebruik het certificaat dat is gedownload in stap 6, zoals in de afbeelding:

Account Number: A_10000
 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 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/web/safe/ssourl
 Current Certificate: CN=~~XXXXXXXXXXXXXXXXXXXX~~, O=Duo Security
 SSO Identity Provider Verification Certificate*: Choose File No file chosen
 Save Back to Accounts List

Stap 19. Log in op Azure portal <https://portal.azure.com/>

Stap 20. Navigeren naar **Azure Active Directory** -> **Enterprise-toepassingen** -> **Nieuwe toepassing** -> **Uw eigen toepassing maken**

Stap 21. Geef uw toepassing een naam en selecteer **Integreren een andere toepassing die u niet in de galerij vindt (Non-gallery)** -> **Creëer**

Stap 22. Selecteer **Gebruikers en groepen toewijzen** en voeg de gebruikers toe die u toegang tot kernen wilt hebben en selecteer **Toewijzen**

Stap 23. Selecteer **Single sing-on** -> **SAML** -> **Upload metadata bestand**, en selecteer het bestand dat gedownload is in stap 7, zoals in de afbeelding:

DUO SSO | SAML-based Sign-on

Updated metadata file | Change single sign-on mode | Test this application | Get feedback!

Overview

- Deployment Plan
- Diagnose and solve problems
- Manage**
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on
 - 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, reliability, 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)	https://res- [redacted] .res.duosecurity.com/saml2/idp/REX
Reply URL (Assertion Consumer Service URL)	https://res- [redacted] .res.duosecurity.com/saml2/idp/REX
Sign on URL	Optional
Relay State (Optional)	Optional
Logout URL (Optional)	Optional
- Attributes & Claims**

Email	user.mail
Username	user.username@pathname
FirstName	user.firstname
LastName	user.lastname
DisplayName	user.displayName
Unique User Identifier	user.username@pathname
- SAML Certificates**

Token signing certificate	Active
Status	7/16/2024, 10:43:02 PM
Thumbprint	[redacted]
Expiration	[redacted]
Notification Email	[redacted]
App Federation Metadata URL	https://login.microsoftonline.com/...
Certificate (Base64)	Download
Certificate (Hex)	Download
Federation Metadata XML	Download

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	https://login.microsoftonline.com/...
Azure AD identifier	https://res.windows.net/...
Logout URL	https://login.microsoftonline.com/...
- 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](#)

Verifiëren

Stap 1. Log in op de CRES-portal <https://res.cisco.com/websafe/>, zoals in de afbeelding:

Secure Email Encryption Service

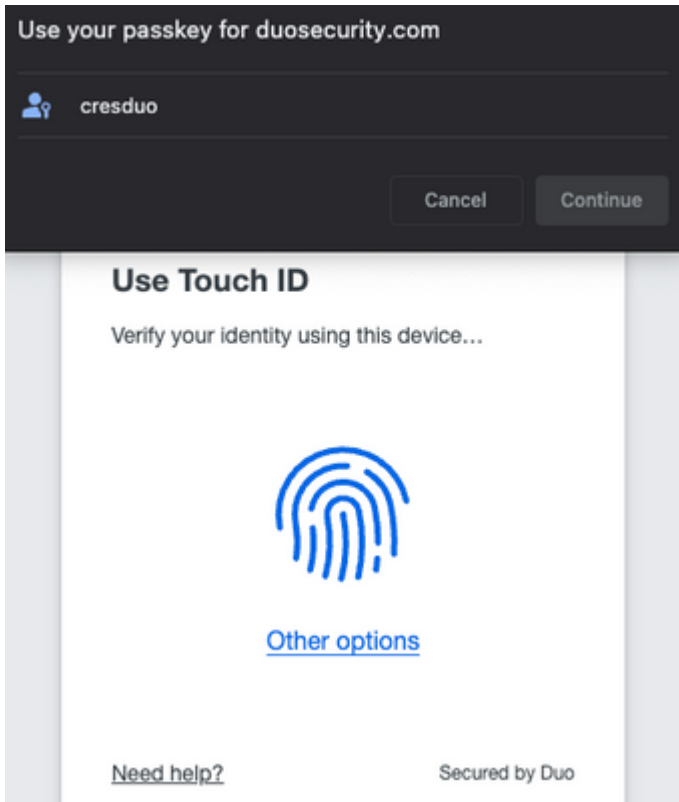
Username*

Log In

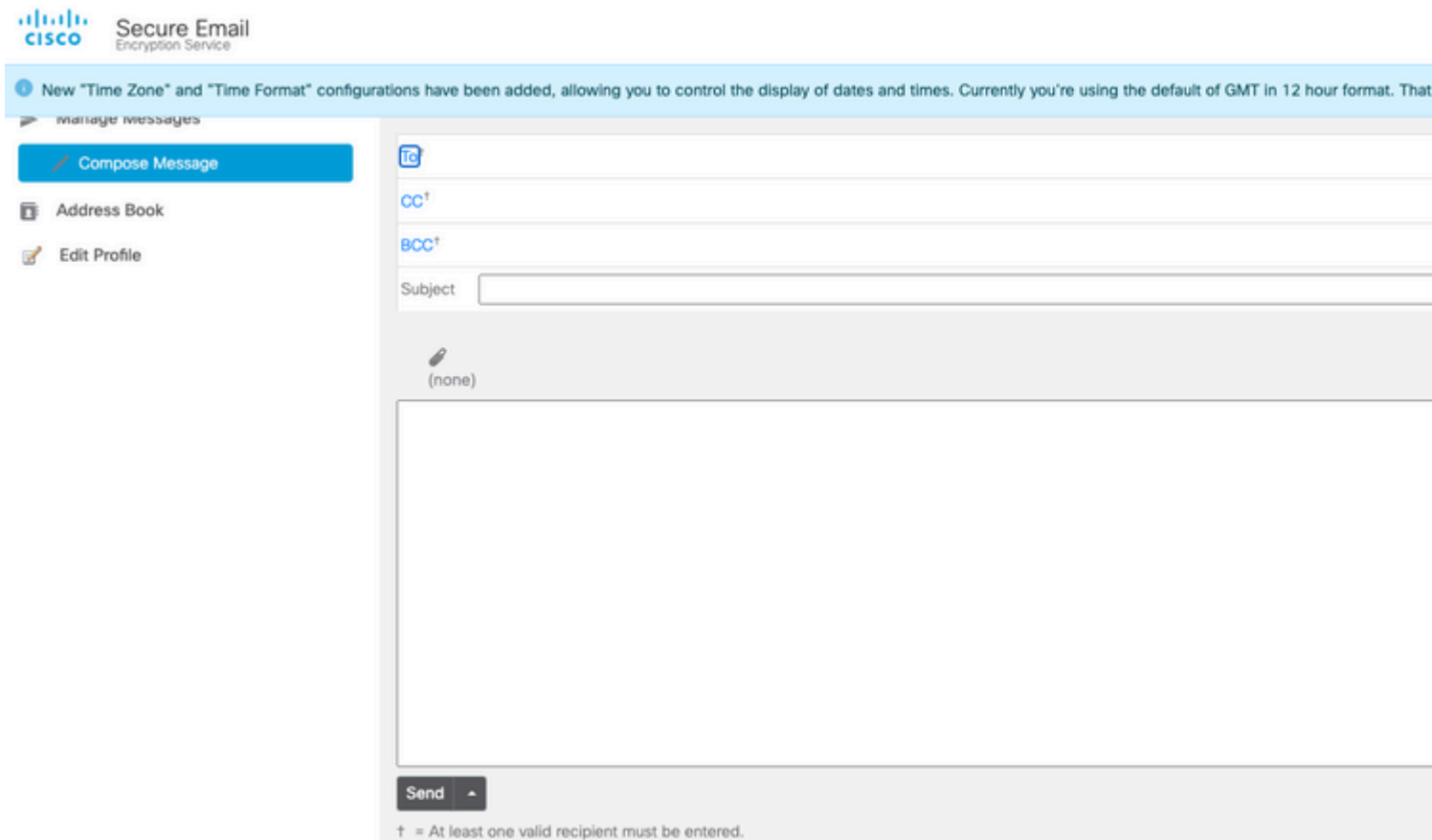
OR

 Sign in with Google

Stap 2. Gebruik de sleutel voor DUO, zoals in de afbeelding:



Stap 3. Zodra u de juiste sleutel hebt ingesteld, kunt u zich met succes aanmelden bij het CRES-portal, zoals wordt aangegeven in de afbeelding:



Veelvoorkomende fouten

1. Als de gebruiker niet is toegewezen onder **Gebruikers en groepen** in de **Enterprise Application**, krijgt u deze fout, zoals in de afbeelding:



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-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 '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. Als de gebruiker wordt verwijderd van **gebruikers** in het Duo Admin-paneel, krijgt u deze fout, zoals in de afbeelding:



Account disabled

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

Secured by Duo

3. Als de gebruiker niet is ingeschreven in het Duo Admin-paneel, krijgt u deze fout, zoals in de afbeelding:


Secure Email Encryption Service

Username*

 You entered an incorrect email address.

Log In

OR

 Sign in with Google

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.