

將思科安全電子郵件加密服務與Duo整合

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[驗證](#)

[常見錯誤](#)

簡介

本檔案介紹如何將思科安全電子郵件加密服務(以前稱為思科註冊信封服務(CRES))與Duo整合。

必要條件

需求

- 管理員訪問CRES門戶<https://res.cisco.com/admin/>
- 管理員訪問Duo門戶<https://admin.duosecurity.com/>
- 管理員訪問Azure門戶<https://portal.azure.com/>
- 使用者需要註冊到Duo Admin Panel，如<https://duo.com/docs/enrolling-users>中所述

採用元件

- SAML 2.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設)的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

步驟 1. 登入到Duo Admin Panel <https://admin.duosecurity.com/>

步驟 2. 導航至應用程式

步驟 3. 選擇保護應用程式

步驟 4. 選擇通用SAML服務提供程式並保護

步驟 5. 複製單一登入URL

步驟 6.選擇Download Certificate

步驟 7.選擇下載XML

步驟 8.在Service Provider -> Entity ID * 下，鍵入<https://res.cisco.com/>

步驟 9.在Service Provider -> Assertion Consumer Service(ACS)URL * 下鍵入
<https://res.cisco.com/websafe/ssourl>

步驟 10.向下滾動，直到看到Settings-> Name鍵入新應用程式的標題，然後選擇Save，如下圖所示：

The screenshot shows the configuration page for Cisco CRES. At the top, there is a breadcrumb trail: "Applications > Applications > 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" to integrate Duo into a SAML-enabled service provider.

The "Metadata" section contains four rows, each with a text input field and a "Copy" button:

- Entity ID: <https://sso-XXXXXXXXXX.sso.duosecurity.com/saml2/http://XXXXXXXXXX.sso>
- Single Sign-On URL: <https://sso-XXXXXXXXXX.sso.duosecurity.com/saml2/http://XXXXXXXXXX.sso>
- Single Log-Out URL: <https://sso-XXXXXXXXXX.sso.duosecurity.com/saml2/http://XXXXXXXXXX.sso>
- Metadata URL: <https://sso-XXXXXXXXXX.sso.duosecurity.com/saml2/http://XXXXXXXXXX.sso>

The "Certificate Fingerprints" section contains two rows, each with a text input field and a "Copy" button:

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

The "Downloads" section contains two rows, each with a "Download" button and an expiration date:

- Certificate: "Download certificate" button, Expires: 01-19-2038
- SAML Metadata: "Download XML" button

The "Service Provider" section contains one row with a text input field and a label:

- Entity ID *: The unique identifier of the service provider.

At the bottom, there is a section for "Assertion Consumer Service (ACS) URL *". It has a "Index" dropdown set to "1", a "URL" input field containing <https://res.cisco.com/websafe/ssourl>, and an "isDefault" dropdown set to "1".

步驟 11.登入到CRES門戶<https://res.cisco.com/admin/>

步驟 12.導航到Accounts頁籤，然後選擇您的Account Number的超連結

步驟 13.在Details頁籤下，選擇Authentication Method -> SAML 2.0

步驟 14.將SSO備用電子郵件屬性名稱留空

步驟 15.SSO服務提供程式實體ID型別<https://res.cisco.com/>

步驟 16.SSO客戶服務URL貼上您在步驟5中複製的URL

步驟 17.將SSO註銷URL留空

步驟 18. 當前證書SSO身份提供程式驗證證書 選擇Choose File，然後使用步驟6下載的憑證，如下圖所示：

[Home](#)[Users](#)[Reports](#)[Accounts](#)[Manage Accounts](#)[Manage Registered Envelopes](#)[Details](#)[Groups](#)[Tokens](#)[SCE Config](#)[Admin Config](#)[Branding](#)

Account Number

A_123456

Account Name*

[REDACTED]@DOMAIN

Description

[REDACTED]@DOMAIN

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

03/03/2025 06:24:48 AM GMT

SSO Email Name ID Format

transient

SSO Alternate Email

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。