

更新安全存取SAML VPN驗證憑證 (服務提供者憑證)

目錄

[簡介](#)

[背景資訊](#)

[必要條件](#)

[需求](#)

[思科安全訪問控制台](#)

[Microsoft Entra ID \(Microsoft Azure\)](#)

簡介

本檔案說明使用新的Secure Access Service Provider Certificate更新辨識提供者(IdP)憑證所需的步驟。

背景資訊

用於虛擬私人網路(VPN)驗證的思科安全存取安全宣告標籤語言(SAML)憑證即將過期，如果您目前的IdP用於驗證VPN使用者，則可以在使用者驗證此憑證時加以更新。

有關此過程的詳細資訊，請參閱[安全訪問通告](#)部分。



注意：預設情況下，大多數IdP不驗證此SAML證書，這不是要求，這意味著您的IdP中不需要執行任何進一步的操作。如果IdP確實驗證安全訪問證書，請繼續更新IdP配置中的安全訪問證書。

本文檔介紹確認配置的IdP是否執行證書驗證的步驟：Entra ID (Azure AD)、PingIdentity、Cisco DUO、OKTA。

必要條件

需求

- 訪問您的Cisco Secure Access Dashboard。
- 存取您的IdP儀表板。

思科安全訪問控制台

注意：請確保在執行啟用新安全訪問證書的下一個步驟之後，如果您的IdP正在進行此證書驗證，請使用新證書更新您的IdP；否則，遠端訪問使用者的VPN身份驗證可能會失敗。

如果您確認IdP正在進行此證書驗證，我們建議您在Secure Access中啟用新證書，並在非工作時間將其上傳到IdP。

在Secure Access Dashboard中，只需要轉到Secure > Certificates > SAML Authentication > Service Provider certificates，在「New」證書上按一下「Activate」。

點選Activate後，您就可以下載新的Secure Access證書，以便在IdP中導入（如果它正在進行證書驗證）。

	Serial number	Expiration date	
New	4001919680eb7bea75760c65dfcdc612	August 27, 2025 9:00:56 PM	Activate
Active	40018a952843fdce9813b8ae2d7b32e9	September 13, 2024 3:24:58 PM	Download

Microsoft Entra ID (Microsoft Azure)

預設情況下，Entra ID (Azure AD)不執行證書驗證。

Home > Enterprise applications | All applications > Secure Access - RA VPN Authentication (SAML SSO)

Secure Access - RA VPN Authentication (SAML SSO) | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

3 SAML Certificates

Token signing certificate

Status: Active [Edit]

Thumbprint: 0E8C78D0B0C8E705095496693737D4AAB14D38E4

Expiration: 5/21/2027, 12:24:06 PM

Notification Email

App Federation Metadata Url: <https://login.microsoftonline.com/71414a41-...>

Certificate (Base64): Download

Certificate (Raw): Download

Federation Metadata XML: Download

Verification certificates (optional) [Edit]

Required: No

如果IdP Entra ID的值「驗證證書（可選）」設定為「必需=是」，請點選「編輯」和「上傳證書」以上傳新的Secure Access SAML VPN證書。

Home > Enterprise applications | All applications > Secure Access - RA VPN Authentication (SAML SSO) | SAML SSO

Secure Access - RA VPN Authentication (SAML SSO) | SAML SSO

Enterprise Application

Overview | Deployment Plan | Diagnose and solve problems | Manage | Properties | Owners | Roles and administrators | Users and groups | **Single sign-on** | Provisioning

Upload metadata file | Change single sign-on mode

SAML Certificates

Token signing certificate

Status: Active
Thumbprint: 0E8C...
Expiration: 5/21/...

Notification Email: [redacted]
App Federation Metadata Url: http://[redacted]
Certificate (Base64): [redacted]
Certificate (Raw): [redacted]
Federation Metadata XML: [redacted]

Verification certificates (optional)

Required	Active
Yes	1

Verification certificates

Requiring verification certificates will impact certain admin and end-user experiences, such as the Single sign-on testing feature, My Apps and M365 app launcher experiences. [Learn more](#)

Verification certificates are used to verify requests coming from this application to Microsoft Entra ID. [Learn more](#)

Require verification certificates

Allow requests signed with RSA-SHA1

Upload certificate

Thumbprint	Key Id	Start date	Expiration date
362A5200CB4EBC282403FA2...	e5468291-e750-44c...	8/27/2024, 4:22 PM	8/27/2025, 4:21 PM

PingIdentity

預設情況下，PingIdentity不執行證書驗證。

Getting Started | Overview | Monitoring | Directory | Applications | **Applications** | Application Catalog | Resources | Application Portal

Applications

Search

4 Applications by Application Name

SAML Secure Access

SAML Secure Access

Overview | **Configuration**

Subject NameId Format: *Not Specified*

Assertion Validity Duration: 300 seconds

Target Application URL: *Not Specified*

Enforce Signed AuthnRequest: *Disabled*

如果IdP Pingidentity中的值Enforce Signed AuthnRequest設定為「Enabled」，請點選Edit並上傳新的Secure Access SAML VPN證書。

Cisco DUO

預設情況下，Cisco DUO正在進行簽名請求驗證，但是，除非啟用了斷言加密，否則不需要對DUO本身執行操作。

對於簽名請求，DUO可以使用管理員提供的後設資料實體ID連結下載新證書。

簽署回應與宣告動作

Signing options *

- Sign response
- Sign assertion

Choose at least one option for signing the SAML response.

實體辨識碼設定

此步驟中無需任何操作，DUO可以從實體ID連結中提取新證書：https://<entry-id>.vpn.sse.cisco.com/saml/sp/metadata/<profile_name>。

Service Provider

Metadata Discovery

None (manual input)

Entity ID *

https://[redacted].sse.cisco.com/saml/sp/metadata/[redacted]

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *

https://[redacted].sse.cisco.com/+CSCOE+/saml/sp/acs?tgn

[+ Add an ACS URL](#)

The service provider endpoint that receives and processes SAML assertions.

宣告加密

如果在IdP Cisco DUO中的值「Assertion encryption」標籤「Encrypt the SAML Assertion」，請按一下「選擇檔案」並上傳新的安全訪問SAML VPN證書。

[Dashboard](#) > [Applications](#) > [Generic SAML Service Provider - Single Sign-On](#)

Generic SAML Service Provider - Single Sign-On

Assertion encryption

Encrypt the SAML assertion

Generic SAML Service Provider - Single Sign-On

Assertion encryption

Encrypt the SAML assertion

Existing Certificate *

VPN Service Provider.cer

歐克塔

OKTA預設不執行證書驗證。「General > SAML Settings (常規 > SAML設定)」下沒有顯示「Signature Certificate (簽名證書)」的選項。

← Back to Applications



Secure Access - VPN

Active ▾



[View Logs](#) [Monitor Imports](#)

GENERAL

Single Sign On URL

Recipient URL

Destination URL

Audience Restriction

Default Relay State

Name ID Format

EmailAddress

Response

Signed

Assertion Signature

Signed

Signature Algorithm

RSA_SHA256

Digest Algorithm

SHA256

Assertion Encryption

Unencrypted

SAML Single Logout

Disabled

如果在IdP OKTA中「General」>「SAML Settings」下有一個值，表示「Signature Certificate Assertion encryption」，則表示OKTA正在執行證書驗證。點選「編輯SAML設定」，點選「簽名證書」，然後上傳新的安全訪問SAML VPN證書。

← Back to Applications



Secure Access - VPN

Active ▾



[View Logs](#) [Monitor Imports](#)

Signature Certificate ⓘ



VPN Service Provider.cer X

Uploaded by Josue Brenes on September 5, 2024 at 11:25:06 AM CST

CN=HydrantID Server CA O1,OU=HydrantID Trusted Certificate Service,O=IdenTrust,C=US
Valid from August 27, 2024 at 4:22:25 PM CST to August 27, 2025 at 4:21:25 PM CST

Certificate expires in 356 days

Enable Single Logout ⓘ

Allow application to initiate Single Logout

Signed Requests ⓘ

Validate SAML requests with signature certificates.

相關資訊

- [Secure Access 幫助中心 \(使用手冊\)](#)
- [技術支援與文件 - Cisco Systems](#)
- [安全存取社群頁面](#)
- [用於VPN的新安全訪問SAML身份驗證證書](#)

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）。