

ISE SAML證書

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[ISE中的SSL證書](#)

[ISE中的SAML證書](#)

[在ISE中續訂自簽名SAML證書](#)

[結論](#)

[相關資訊](#)

簡介

本檔案介紹思科身分識別服務引擎(ISE)中的安全宣告標籤語言(SAML)系統憑證。它涵蓋SAML證書的目的、如何執行續訂，最後回答常見問題。它涵蓋從2.4版到3.0版的ISE，但是，它應該與其他ISE 2.x和3.x軟體版本相似或相同，除非另有說明。

必要條件

需求

思科建議您瞭解以下主題：

1. Cisco ISE
2. 用於描述不同型別ISE和身份驗證、授權和記帳(AAA)部署的術語
3. RADIUS協定和AAA基礎知識
4. SAML協定
5. SSL/TLS和x509證書
6. 公開金鑰基礎架構(PKI)基礎知識

採用元件

本檔案中的資訊是根據思科身分識別服務引擎(ISE)版本2.4 - 3.0

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或設定可能造成的影響。

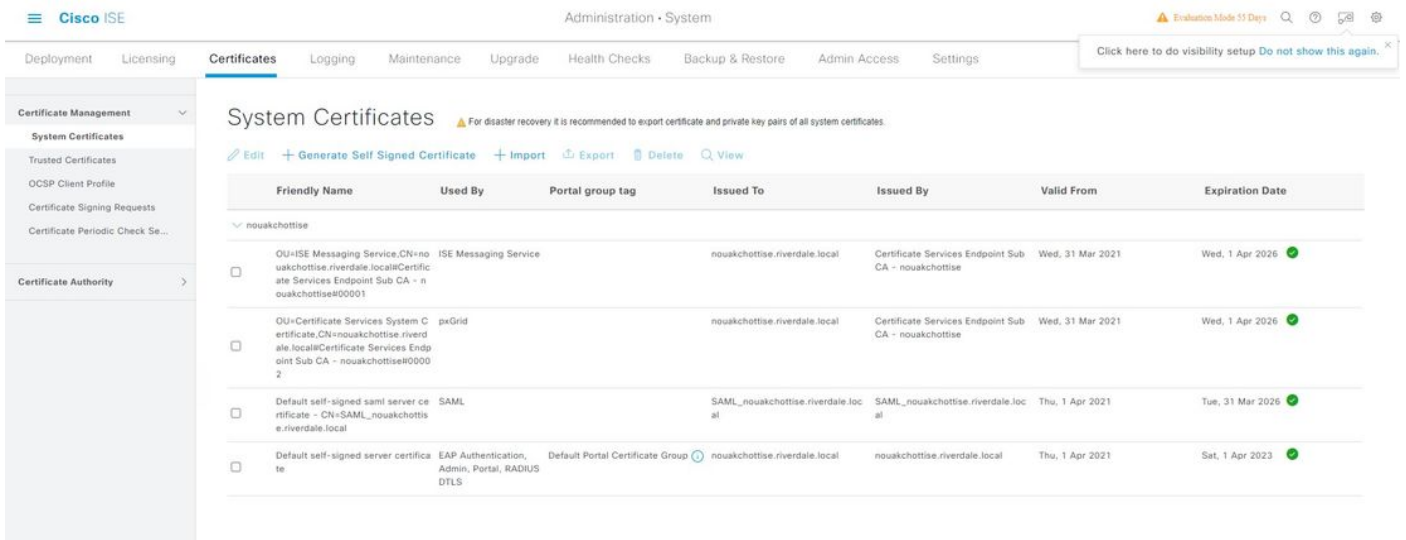
ISE中的SSL證書

安全套接字層(SSL)證書是標識個人、伺服器或任何其他數字實體，並將該實體與公鑰關聯的數字檔

案。自簽名證書由其建立者簽名。證書可以由外部證書頒發機構(CA) (通常是公司自己的CA伺服器或已知的CA供應商) 自簽名或數位簽章。CA簽署的數位證書被視為行業標準，比自簽署證書更安全。

Cisco ISE依靠PKI來提供與終端和管理員、ISE與其他伺服器/服務之間以及多節點部署中的Cisco ISE節點之間的安全通訊。PKI依靠X.509數位證書來傳輸用於加密和解密消息的公鑰，以及驗證代表使用者和裝置的其他證書的真實性。通過思科ISE管理門戶，您可以管理這些X.509證書。

在ISE中，系統證書是標識思科ISE節點到其他應用 (如終端、其他伺服器等) 的伺服器證書。每個思科ISE節點都有自己的系統證書與相應的私鑰一起儲存在節點上。每個系統證書都可以對映到「角色」，這些角色指示證書的用途，如下圖所示。



The screenshot shows the Cisco ISE Administration interface for System Certificates. The table lists four certificates with their friendly names, uses, portal group tags, issued to, issued by, valid from, and expiration dates.

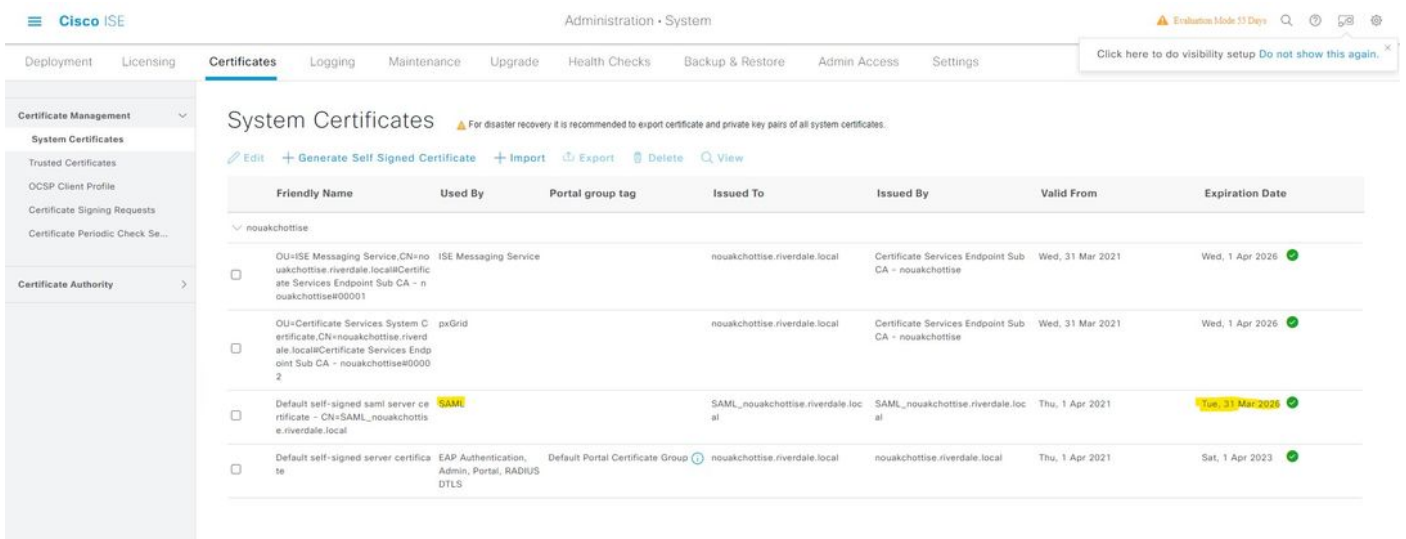
Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
OU=ISE Messaging Service,CN=no-uakchottise.riverdale.local Certificate Services Endpoint Sub CA - nouakchottise#00001	ISE Messaging Service		nouakchottise.riverdale.local	Certificate Services Endpoint Sub CA - nouakchottise	Wed, 31 Mar 2021	Wed, 1 Apr 2026
OU=Certificate Services System Certificate,CN=nouakchottise.riverdale.local Certificate Services Endpoint Sub CA - nouakchottise#00002	pxGrid		nouakchottise.riverdale.local	Certificate Services Endpoint Sub CA - nouakchottise	Wed, 31 Mar 2021	Wed, 1 Apr 2026
Default self-signed saml server certificate - CN=SAML_nouakchottise.riverdale.local	SAML		SAML_nouakchottise.riverdale.local	SAML_nouakchottise.riverdale.local	Thu, 1 Apr 2021	Tue, 31 Mar 2026
Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group	nouakchottise.riverdale.local	nouakchottise.riverdale.local	Thu, 1 Apr 2021	Sat, 1 Apr 2023

ISE 3.0系統證書

本文檔的範圍僅適用於SAML證書。有關ISE中的其他證書以及有關ISE中的SSL證書的更多資訊，請參閱本文文檔：[ISE中的TLS/SSL證書 — 思科](#)

ISE中的SAML證書

ISE中的SAML證書通過查詢使用欄位下具有SAML條目的系統證書來確定。此證書將用於與SAML身份提供程式(IdP)通訊，如驗證正在從正確的IdP接收SAML響應，以及確保與IdP的通訊安全。請注意，指定用於SAML使用的證書不能用於任何其他服務，如管理、EAP身份驗證等。



The screenshot shows the same Cisco ISE Administration interface for System Certificates. The SAML certificate row is highlighted in yellow, indicating it is the certificate used for SAML.

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
OU=ISE Messaging Service,CN=no-uakchottise.riverdale.local Certificate Services Endpoint Sub CA - nouakchottise#00001	ISE Messaging Service		nouakchottise.riverdale.local	Certificate Services Endpoint Sub CA - nouakchottise	Wed, 31 Mar 2021	Wed, 1 Apr 2026
OU=Certificate Services System Certificate,CN=nouakchottise.riverdale.local Certificate Services Endpoint Sub CA - nouakchottise#00002	pxGrid		nouakchottise.riverdale.local	Certificate Services Endpoint Sub CA - nouakchottise	Wed, 31 Mar 2021	Wed, 1 Apr 2026
Default self-signed saml server certificate - CN=SAML_nouakchottise.riverdale.local	SAML		SAML_nouakchottise.riverdale.local	SAML_nouakchottise.riverdale.local	Thu, 1 Apr 2021	Tue, 31 Mar 2026
Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group	nouakchottise.riverdale.local	nouakchottise.riverdale.local	Thu, 1 Apr 2021	Sat, 1 Apr 2023

ISE首次安裝自簽名的SAML伺服器證書具有以下屬性：

金鑰大小：2048

有效性：一年

金鑰用法：數位簽章（簽名）

擴展金鑰用法：TLS Web伺服器身份驗證(1.3.6.1.5.5.7.3.1)

The screenshot shows the Cisco ISE Administration console. The left sidebar is expanded to 'Certificate Management' > 'System Certificates' > 'Trusted Certificates'. The main content area displays the details for a certificate with the Issuer 'SAML_nouakchottise.riverdale.local'. The details include:

- * Friendly Name: Default self-signed saml server certificate - CN=SAML_nouakchottise.riverdale.local
- Description:
- Subject: CN=SAML_nouakchottise.riverdale.local
- Subject Alternative Name (SAN): DNS Name: nouakchottise.riverdale.local
- Issuer: SAML_nouakchottise.riverdale.local
- Valid From: Thu, 1 Apr 2021 21:56:23 UTC
- Valid To (Expiration): Tue, 31 Mar 2026 21:56:23 UTC
- Serial Number: 60 66 41 87 00 00 00 00 51 F3 02 84 54 6F 0B 27
- Signature Algorithm: SHA384WITHRSA
- Key Length: 4096
- Certificate Policies:

Usage options are listed at the bottom:

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADIUS server

附註：建議不要將包含2.5.29.37.0值的證書用於「擴展金鑰用法」屬性中的「任何目的」對象識別符號。如果在「擴展金鑰用法」屬性中使用的「任意用途」對象識別符號包含值2.5.29.37.0的證書，則該證書將被視為無效，並顯示以下錯誤消息："source=local；type=fatal；message="unsupported certificate"。"

ISE管理員需要在到期之前續訂此自簽名SAML證書，即使SAML功能未主動使用。

在ISE中續訂自簽名SAML證書

使用者面臨的一個常見問題是，他們的SAML證書最終將過期，ISE會使用以下消息提醒他們：

Alarm Name :

Certificate Expiration

Details :

Trust certificate 'Default self-signed server certificate' will expire in 60 days :

Server=Kolkata-ISE-001

Description :

This certificate will expire soon. When it expires, ISE may fail when attempting to establish secure communications with clients. Inter-node communication may also be affected

Severity :

Warning

Suggested Actions :

Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use ISE to extend the expiration date. You can just delete the certificate if it is no longer used.

對於自簽名的伺服器證書，可以續訂證書，只需勾選續訂週期即可，還可以保留5-10年，如下圖所示。

The screenshot shows the 'System Certificates' page in Cisco ISE Administration. The page title is 'System Certificates' with a warning icon and text: 'For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.' Below the title are action buttons: 'Edit', '+ Generate Self Signed Certificate', '+ Import', 'Export', 'Delete', and 'View'. A table lists certificates with columns: 'Friendly Name', 'Used By', 'Portal group tag', 'Issued To', 'Issued By', 'Valid From', and 'Expiration Date'. The table contains four entries, with the third entry 'Default self-signed saml server certificate' highlighted in yellow.

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
OU=ISE Messaging Service,CN=noakchottise.riverdale.local,Certificate Services Endpoint Sub CA - noakchottise#00001	ISE Messaging Service		noakchottise.riverdale.local	Certificate Services Endpoint Sub CA - noakchottise	Wed, 31 Mar 2021	Wed, 1 Apr 2026
OU=Certificate Services System Certificate,CN=noakchottise.riverdale.local,Certificate Services Endpoint Sub CA - noakchottise#00002	pxGrid		noakchottise.riverdale.local	Certificate Services Endpoint Sub CA - noakchottise	Wed, 31 Mar 2021	Wed, 1 Apr 2026
Default self-signed saml server certificate - CN=SAML_noakchottise.riverdale.local	SAML		SAML_noakchottise.riverdale.local	SAML_noakchottise.riverdale.local	Thu, 1 Apr 2021	Tue, 31 Mar 2026
Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group	noakchottise.riverdale.local	noakchottise.riverdale.local	Thu, 1 Apr 2021	Sat, 1 Apr 2023

The screenshot shows the details page for a certificate in Cisco ISE Administration. The page title is 'ISSUER'. The 'Friendly Name' is 'Default self-signed saml server certificate - CN=SAML_noakchottise.riverdale.local'. The 'Subject' is 'CN=SAML_noakchottise.riverdale.local'. The 'Valid From' is 'Thu, 1 Apr 2021 21:56:23 UTC' and the 'Valid To (Expiration)' is 'Tue, 31 Mar 2026 21:56:23 UTC'. The 'Serial Number' is '60 66 41 87 00 00 00 51 F3 02 84 54 6F 0B 27'. The 'Signature Algorithm' is 'SHA384WITHRSA' and the 'Key Length' is '4096'. The 'Usage' section is checked for 'Admin: Use certificate to authenticate the ISE Admin Portal', 'EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling', and 'RADIUS DTLS: Use certificate for the RADIUS server'.

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore A

Subject Alternative Name (SAN) DNS Name: nouakchottise.riverdale.local

Issuer	SAML_nouakchottise.riverdale.local
Valid From	Thu, 1 Apr 2021 21:56:23 UTC
Valid To (Expiration)	Tue, 31 Mar 2026 21:56:23 UTC
Serial Number	60 66 41 87 00 00 00 00 51 F3 02 84 54 6F 0B 27
Signature Algorithm	SHA384WITHRSA
Key Length	4096
Certificate Policies	

Certificate Management ▾

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Se...

Certificate Authority >

Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- ISE Messaging Service: Use certificate for the ISE Messaging Service
- SAML: Use certificate for SAML Signing
- Portal: Use for portal

Renew Self Signed Certificate

Renewal Period

* Expiration TTL 10 years

Save **Reset**

事實上，ISE部署節點未使用的所有自簽名證書都可以續訂10年；這可確保不會收到您未使用的服務證書的任何過期通知。10年是ISE自簽名證書允許的最大壽命，通常應該足夠長。更新ISE上的任何系統證書不會觸發服務重新啟動，只要它不是指定為「管理」使用。

結論

對於未使用的任何過期ISE系統證書（自簽名和CA簽名），可以將其替換、刪除或續訂，建議在執行ISE升級之前不要在ISE上保留任何過期證書（系統或受信任）。

相關資訊

- ISE 3.0管理證書：[思科身份服務引擎管理員指南3.0版 — 基本設定\[思科身份服務引擎\] — 思科](#)
- ISE中的SSL證書：[ISE中的TLS/SSL證書 — 思科](#)
- [技術支援與文件 - Cisco Systems](#)