

在ISE中配置TLS/SSL證書

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[伺服器證書](#)

[ISE證書](#)

[系統憑證](#)

[受信任的證書儲存](#)

[基本任務](#)

[生成自簽名證書](#)

[續訂自簽名證書](#)

[安裝受信任的證書](#)

[安裝CA簽名的證書](#)

[備份證書和私鑰](#)

[疑難排解](#)

[檢查證書有效性](#)

[刪除證書](#)

[請求方不信任802.1x身份驗證上的ISE伺服器證書](#)

[ISE證書鏈正確，但終端在身份驗證期間拒絕ISE伺服器證書](#)

[常見問題](#)

[當ISE發出證書已存在的警告時，該怎麼做？](#)

[為什麼瀏覽器引發警告，指出來自ISE的門戶頁面由不受信任的伺服器顯示？](#)

[當由於無效證書導致升級失敗時，該怎麼做？](#)

[相關資訊](#)

簡介

本文檔介紹思科ISE中的TLS/SSL證書、ISE證書的種類和角色、如何執行常見任務和故障排除以及回答常見問題。

必要條件

需求

思科建議您瞭解以下主題：

1. 思科身分識別服務引擎(ISE)
2. 用於描述不同型別ISE和AAA部署的術語。
3. RADIUS協定和AAA基礎知識
4. SSL/TLS和x509證書
5. 公開金鑰基礎架構(PKI)基礎知識

採用元件

本文檔中的資訊基於Cisco ISE版本2.4 - 2.7軟體和硬體版本。它涵蓋從2.4版到2.7版的ISE，但是它必須與其他ISE 2.x軟體版本相似或相同，除非另有說明。

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。

伺服器證書

伺服器使用伺服器證書向客戶端呈現伺服器的身份以確保真實性，並為通訊提供安全通道。這些證書可以是自簽名（伺服器向自身頒發證書）或由證書頒發機構（組織內部或由知名供應商）頒發。

伺服器證書通常頒發給伺服器的主機名或FQDN（完全限定域名），或者它們也可以是萬用字元證書（*.domain.com）。發佈到的主機、域或子域通常在Common Name(CN)或Subject Alternative Name(SAN)欄位中提及。

萬用字元憑證是使用萬用字元標籤（以星號代替主機名）的SSL憑證，因此允許在一個組織中的多個主機之間共用相同的憑證。例如，萬用字元證書使用者名稱的CN或SAN值可能類似*.company.com 可用於保護此域的任何主機，例如 server1.com中， server2.com等等。

證書通常使用公鑰加密或非對稱加密。

- 公鑰：公鑰存在於其中一個欄位的證書中，並且在裝置嘗試與其通訊時由系統公開共用。
- 私鑰：私鑰對終端系統為私鑰，並與公鑰配對。用公鑰加密的資料只能用特定的配對私鑰解密，反之亦然。

ISE證書

Cisco ISE依靠公鑰基礎設施(PKI)提供與終端、使用者、管理員等的安全通訊，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數位證書傳輸用於加密和解密消息的公鑰，以及驗證使用者和裝置提供的其他證書的真實性。思科ISE通常使用兩種證書類別：

- 系統證書：這些是向客戶端標識思科ISE節點的伺服器證書。每個思科ISE節點都有自己的本地證書，每個證書與各自的私鑰一起儲存在節點上。
- 受信任的證書儲存證書：這些是證書頒發機構(CA)證書，用於驗證提供給ISE用於各種目的的證書。證書儲存中的這些證書在主管理節點上管理，並複製到分散式思科ISE部署中的所有其他節點。證書儲存還包含由ISE內部證書頒發機構為ISE節點生成的證書，該證書用於BYOD。

系統憑證

系統證書可用於一個或多個角色。每個角色都有不同的用途，如下所述：

- 管理：用於保護443上的所有通訊（管理GUI）、複製，以及此處未列出的任何埠/用途。
- 門戶：用於通過集中式Web身份驗證(CWA)門戶、訪客、BYOD、客戶端調配、本地請求方調配門戶等門戶保護HTTP通訊。每個門戶必須對映到入口組標籤（預設為預設入口組標籤），指示入口使用特定標籤的證書。證書的Edit選項中的Portal Group Tag name下拉選單允許您建立新標籤或選擇已存在的標籤。
- EAP：這是一個角色，它指定提供給客戶端用於802.1x身份驗證的證書。證書幾乎可與所有可能的EAP方法（如EAP-TLS、PEAP、EAP-FAST等）一起使用。使用隧道EAP方法（如PEAP和FAST），傳輸層安全(TLS)用於保護憑證交換。在建立此隧道以確保安全交換之前，不會將客戶端憑證傳送到伺服器。
- RADIUS DTLS：此角色指定用於DTLS連線（UDP上的TLS連線）的證書，以加密網路接入裝置(NAD)和ISE之間的RADIUS流量。NAD必須支援DTLS加密才能使用此功能。
- SAML：伺服器證書用於保護與SAML身份提供程式(IdP)之間的通訊。指定用於SAML的證書不能用於任何其他服務，如管理、EAP身份驗證等。
- ISE消息服務：自2.6起，ISE使用ISE消息服務而不是舊系統日誌協定來記錄資料。這用於加密此通訊。
- PxGrid：此證書用於ISE上的PxGrid服務。

安裝ISE時，它會生成 Default Self-Signed Server Certificate.預設情況下，此值分配給EAP身份驗證、管理員、門戶和RADIUS DTLS。建議將這些角色移動到內部CA或已知的CA簽名證書。

Friendly Name	Used By	Portal group tag	Valid From	Valid To
OU=Certificate Services System Certificate, CN=hongkongise riverdale local, Certificate Services Endpoint Sub CA - hongkongise#00002	pxGrid	hongkongise riverdale local	Mon, 13 Apr 2020	Sun, 14 Apr 2030
OU=ISE Messaging Service, CN=hongkongise riverdale local, Certificate Services Endpoint Sub CA - hongkongise#00001	ISE Messaging Service	hongkongise riverdale local	Mon, 13 Apr 2020	Sun, 14 Apr 2030
Default self-signed saml server certificate - CN=SAML_hongkongise riverdale local	SAML	SAML_hongkongise riverdale local	Tue, 14 Apr 2020	Wed, 14 Apr 2021
Default self-signed server certificate	Default Portal Certificate Group	hongkongise riverdale local	Tue, 14 Apr 2020	Wed, 14 Apr 2021

提示：最好確保ISE伺服器的FQDN和IP地址都新增到ISE系統證書的SAN欄位中。一般來說，為了確保思科ISE中的證書身份驗證不受證書驅動驗證功能細微差異的影響，請為網路中部署的所有思科ISE節點使用小寫主機名。

注意:ISE證書的格式必須是隱私增強郵件(PEM)或可分辨編碼規則(DER)。

受信任的證書儲存

證書頒發機構證書必須儲存在 Administration > System > Certificates > Certificate Store 他們必須擁有 Trust for client authentication 使用案例確保ISE使用這些證書來驗證終端、裝置或其他ISE節點提供的證書。

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Mon, 12 May 2025
Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00 ...	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mon, 14 May 2029
Cisco ECC Root CA	Enabled	Cisco Services	01	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Fri, 4 Apr 2053
Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root CA	Cisco Licensing Root CA	Thu, 30 May 2013	Sun, 30 May 2038
Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA ...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037
Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54 ...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2029
Cisco Root CA 2099	Enabled	Cisco Services	01 9A 33 58 78 CE ...	Cisco Root CA 2099	Cisco Root CA 2099	Tue, 9 Aug 2016	Sun, 9 Aug 2099
Cisco Root CA M1	Enabled	Cisco Services	2E D2 0E 73 47 D3...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 2033
Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037
Cisco RXC-R2	Enabled	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034
Default self-signed server certificate	Enabled	Endpoints Infrastructure	5E 95 93 55 00 00 ...	hongkongise.inverdale.local	hongkongise.inverdale.local	Tue, 14 Apr 2020	Wed, 14 Apr 2021
DigCert Global Root CA	Enabled	Cisco Services	08 3B E0 56 90 42 ...	DigCert Global Root CA	DigCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov 2031
DigCert root CA	Enabled	Endpoints Infrastructure	02 AC 5C 26 6A 0B...	DigCert High Assurance ...	DigCert High Assurance ...	Fri, 10 Nov 2006	Mon, 10 Nov 2031
DigCert SHA2 High Assurance Server CA	Enabled	Endpoints Infrastructure	04 E1 E7 A4 DC 5C...	DigCert SHA2 High Assu...	DigCert High Assurance ...	Tue, 22 Oct 2013	Sun, 22 Oct 2028
DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A3...	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 2021
HydrantID SSL ICA G2	Enabled	Cisco Services	75 17 16 77 83 D0 ...	HydrantID SSL ICA G2	QuoVadis Root CA 2	Tue, 17 Dec 2013	Sun, 17 Dec 2023
QuoVadis Root CA 2	Enabled	Cisco Services	05 09	QuoVadis Root CA 2	QuoVadis Root CA 2	Fri, 24 Nov 2006	Mon, 24 Nov 2031
Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5...	thawte Primary Root CA	thawte Primary Root CA	Fri, 17 Nov 2006	Wed, 16 Jul 2036
VerSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7D...	VerSign Class 3 Public Pr...	VerSign Class 3 Public Pr...	Wed, 8 Nov 2006	Wed, 16 Jul 2036
VerSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 03...	VerSign Class 3 Secure ...	VerSign Class 3 Public Pr...	Mon, 8 Feb 2010	Fri, 7 Feb 2020

基本任務

證書已過期，可能會吊銷證書或要求證書在某個時間進行更換。如果ISE伺服器證書過期，除非用新的有效證書替換嚴重問題。

注意：如果用於可擴展身份驗證協定(EAP)的證書過期，客戶端身份驗證可能會失敗，因為客戶端不再信任ISE證書。如果用於門戶的證書過期，客戶端和瀏覽器可能會拒絕連線到門戶。如果管理員使用證書過期，風險更大，這將阻止管理員再登入到ISE，並且分散式部署可以停止運行，這是必須的。

生成自簽名證書

要生成新的自簽名證書，請導航至 Administration > System > Certificates > System Certificates. 按一下 Generate Self Signed Certificate.

System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs

Friendly Name	Used By	Portal group tag	Issued To
hongkongise			
OU=Certificate Services System Certificate,CN=hongkongise.inverdale.local#Certificate Services Endpoint Sub CA - hongkongise#00000?	pxGrid		hongkongise

此清單介紹了「生成自簽名證書」頁中的欄位。

自簽名證書設定欄位名稱使用指南：

- 選擇節點：(必需) 生成系統證書所需的節點。
- CN：(如果未指定SAN則必需) 預設情況下，CN是為其生成自簽名證書的ISE節點的FQDN。
- 組織單位(OU)：組織單位名稱，例如Engineering。
- 組織(O)：組織名稱，例如Cisco。
- 城市(L)：(請勿縮寫) 城市名稱，例如San Jose。
- 州(ST)：(請勿縮寫) 州名，例如California。
- 國家(C)：國家名稱。需要兩個字母的ISO國家/地區代碼。例如，美國。
- SAN：與證書關聯的IP地址、DNS名稱或統一資源識別符號(URI)。
- 金鑰型別：指定用於建立公鑰的演算法：RSA或ECDSA。
- 金鑰長度：指定公鑰的位大小。這些選項可用於RSA:512 1024 2048 4096，這些選項可用於ECDSA:256 384。
- 要使用的摘要：選擇以下雜湊演算法之一：SHA-1或SHA-256。
- Certificate Policies：輸入證書必須符合的證書策略OID或OID清單。使用逗號或空格分隔OID。
- Expiration TTL：指定證書到期的天數。
- 友好名稱：輸入證書的友好名稱。如果未指定名稱，思科ISE會自動建立格式的名稱 其中 是一個唯一的五位數。
- Allow Wildcard Certificates：選中此覈取方塊可生成自簽名的萬用字元證書(在主題中的任何CN和/或SAN中的DNS名稱中包含星號(*)的證書。例如，分配給SAN的DNS名稱可以是*.domain.com.
- 用法：選擇必須使用此系統證書的服務。可用選項包括：
AdminEAP身份驗證RADIUS DTLSpXGridSAML入口網站

The screenshot displays the 'Generate Self Signed Certificate' configuration page in the Cisco Identity Services Engine (ISE) interface. The page is organized into a sidebar on the left and a main configuration area on the right.

Navigation and Breadcrumbs:

- System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC
- Deployment > Licensing > Certificates > Logging > Maintenance > Upgrade > Backup & Restore > Admin Access > Settings

Left Sidebar (Certificate Management):

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings
- ▶ Certificate Authority

Main Configuration Area: Generate Self Signed Certificate

- * Select Node: hongkongise
- Subject**
 - Common Name (CN): SFQDNS
 - Organizational Unit (OU): Security
 - Organization (O): IT
 - City (L): Kolkata
 - State (ST): West Bengal
 - Country (C): IN
- Subject Alternative Name (SAN): IP Address, 10.127.196.248
- * Key type: RSA
- * Key Length: 2048
- * Digest to Sign With: SHA-256
- Certificate Policies: (Empty field)

注意：對於相同的安全級別，RSA和ECDSA公鑰可以具有不同的金鑰長度。如果目標是獲取公共CA簽名證書或將Cisco ISE部署為符合FIPS的策略管理系統，請選擇2048。

續訂自簽名證書

要檢視存在的自簽名證書，請導航至 Administration > System > Certificates > System Certificates 在ISE控制檯中。如果同一ISE伺服器FQDN中提到具有「Issued To」和「Issued By」的任何證書，則該證書為自簽名證書。選擇此證書，然後按一下 Edit。

在 Renew Self Signed Certificate，請檢視 Renewal Period 框中，並根據需要設定Expiration TTL。最後，按一下 Save。

安裝受信任的證書

從根CA、中間CA和/或需要受信任的主機獲取Base 64編碼證書。

1.登入到ISE節點並導航至 Administration > System > Certificate > Certificate Management > Trusted Certificates 然後按一下 Import如圖所示。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', and 'Policy'. Below it, a secondary navigation bar shows 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', and 'pxGrid Services'. The main navigation area includes 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', and 'Backup & Restore'. The left sidebar is expanded to 'Certificate Management', showing options like 'System Certificates', 'Trusted Certificates', 'OCSP Client Profile', 'Certificate Signing Requests', and 'Certificate Periodic Check Settings'. The main content area is titled 'Trusted Certificates' and features buttons for 'Edit', 'Import' (highlighted in yellow), 'Export', 'Delete', and 'View'. Below these buttons is a table with columns for 'Friendly Name' and 'Status'. The table lists several certificates: 'Baltimore CyberTrust Root' (checked), 'Cisco CA Manufacturing' (unchecked), 'Cisco ECC Root CA' (checked), and 'Cisco Licensing Root CA' (checked).

2.在下一頁上，上傳獲得的CA證書（順序與前面所述的相同）。給他們指派一個友好名稱和說明證書的用途，以便進行跟蹤。

根據使用需要，選中以下各項旁邊的框：

- 在ISE中信任身份驗證 — 這是當新的ISE節點將相同的受信任CA證書載入到其受信任的證書儲存時，新增新的ISE節點。
- Trust for client authentication and Syslog — 啟用此功能，以便使用證書對通過EAP和/或信任安全系統日誌伺服器連線到ISE的終端進行身份驗證。
- 信任思科服務的身份驗證 — 僅信任外部思科服務（如源服務）才需要信任。

3.最後，按一下 Submit.現在，證書必須在受信任的儲存中可見，並同步到所有輔助ISE節點（如果在部署中）。

The screenshot shows the Cisco Identity Services Engine (ISE) interface for importing a new certificate. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. Below it, a secondary navigation bar shows 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. The main navigation area includes 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Backup & Restore', 'Admin Access', and 'Settings'. The left sidebar is expanded to 'Certificate Management', showing options like 'System Certificates', 'Trusted Certificates', 'OCSP Client Profile', 'Certificate Signing Requests', and 'Certificate Periodic Check Settings'. The main content area is titled 'Import a new Certificate into the Certificate Store'. It features a 'Certificate File' field with a 'Browse...' button and the text 'CA certificate.cer'. Below this is a 'Friendly Name' field with the value 'Company CA certificate'. The 'Trusted For' section includes several checkboxes: 'Trust for authentication within ISE' (checked), 'Trust for client authentication and Syslog' (unchecked), 'Trust for authentication of Cisco Services' (unchecked), and 'Validate Certificate Extensions' (unchecked). At the bottom, there is a 'Description' field and 'Submit' and 'Cancel' buttons.

安裝CA簽名的證書

將根和中間CA證書新增到受信任的證書儲存中後，可以頒發證書簽名請求(CSR)，並且根據CSR簽名的證書可以繫結到ISE節點。

1.為此，請導航至 Administration > System > Certificates > Certificate Signing Requests 然後點選 **Generate Certificate Signing Requests (CSR)** 產生CSR。

2.在出現的頁面上的「用法」部分下，從下拉選單中選擇要使用的角色。

如果證書用於多個角色，請選擇「多用」。生成證書後，可以根據需要更改角色。在大多數情況下，證書可以設定為在「用於」(Used For)下拉選單中用於「多用途」(Multi-use)；這允許證書可用於所有ISE Web門戶。

3.選中ISE節點旁邊的框，選擇為其生成證書的節點。

4.如果目的是安裝/產生萬用字元憑證，請檢查 Allow Wildcard Certificates 框。

Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:

ISE Identity Certificates:

- Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- DTLS Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication
- SAML - SAML Signing Certificate
- ISE Messaging Service - This is not a signing request, but an ability to generate a brand new Messaging certificate.

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for **Multi-Use** You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).


Allow Wildcard Certificates

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> hongkongise	hongkongise#Multi-Use

Usage

Certificate(s) will be used for Multi-Use  You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).

Allow Wildcard Certificates

Node(s)

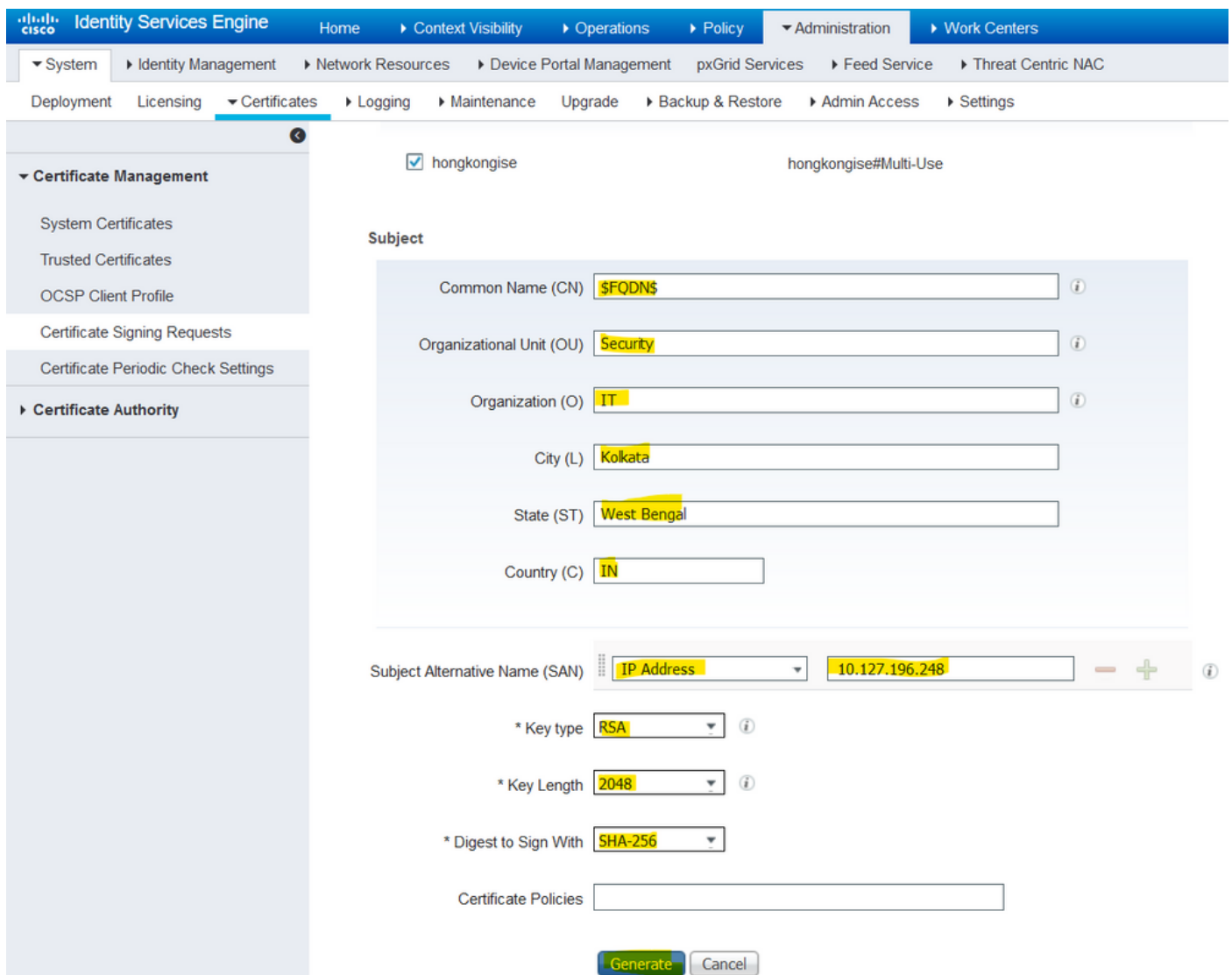
Generate CSR's for these Node

Node
<input type="checkbox"/> hongkongise
<input checked="" type="checkbox"/> hongkongise#Multi-Use

Multi-Use
Admin
EAP Authentication
RADIUS DTLS
Portal
pxGrid
ISE Messaging Service
SAML
ISE Root CA
ISE Intermediate CA
Renew ISE OCSP Responder Certificates

5. 根據主機或組織（組織單位、組織、城市、州/省、國家）的詳細資訊，填寫主題資訊。

6. 為了完成此操作，請按一下 **Generate**，然後按一下 **Export** 在彈出視窗上。



Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

hongkongise hongkongise#Multi-Use

Subject

Common Name (CN)



Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Country (C)

Subject Alternative Name (SAN)  

* Key type

* Key Length

* Digest to Sign With

Certificate Policies

Generate Cancel

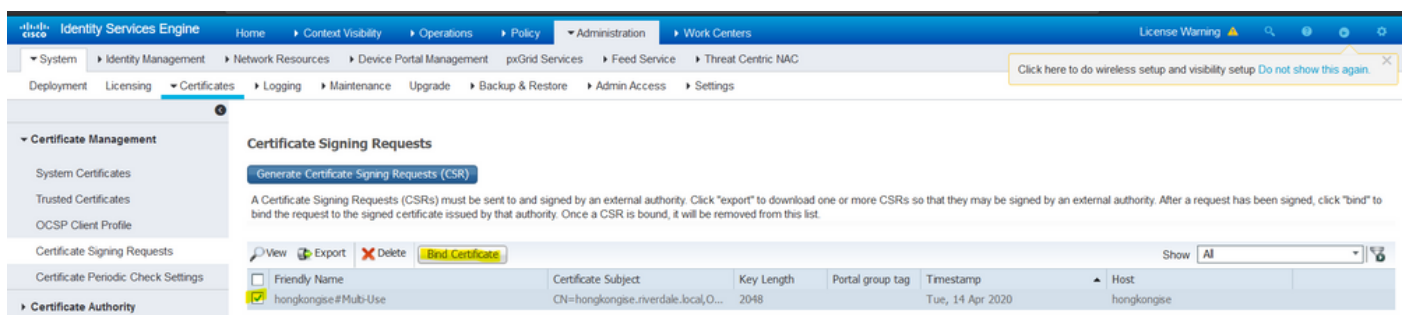
這會下載剛建立的Base-64編碼證書請求請求 — 必須將此PEM檔案傳送到CA進行簽名，並獲取生成的簽名證書CER檔案 (Base 64編碼)。

註：在CN欄位下，ISE自動填充節點FQDN。

註：在ISE 1.3和1.4中，至少需要發出兩個CSR才能使用pxGrid。一個專用於pxGrid，另一個專用於pxGrid的其他服務。自2.0及更新版本起，所有這一切都集中在一個CSR上。

注意：如果證書用於EAP身份驗證，則「*」符號不能在「主題CN」欄位中，因為Windows請求方拒絕伺服器證書。即使請求方禁用了Validate Server Identity，當「*」位於CN欄位中時，SSL握手也可能失敗。相反，可以在CN欄位中使用通用FQDN，然後 *.domain.com 可用於SAN DNS Name欄位。某些憑證授權單位(CA)可以在憑證的CN中自動新增萬用字元(*)，即使該萬用字元不存在於CSR中。在這種情況下，需要發出特殊請求來阻止此操作。

7.一旦證書由CA簽署(如影片所示從CSR生成，請返回到[ISE GUI](#)，然後導航到Administration > System > Certificates > Certificate Management > Certificate Signing Request；選中先前建立的CSR旁邊的框，然後按一下Bind Certificate按鈕。



8.接下來，上傳剛收到的簽名證書，並為其指定友好名稱ISE。然後根據證書的需要 (如管理員和EAP身份驗證、門戶等)，繼續選擇使用旁邊的框，然後按一下 Submit，如下圖所示：

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates
- OCSF Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings

Certificate Authority

Bind CA Signed Certificate

* Certificate File certnew(1).cer

Friendly Name ⓘ

Validate Certificate Extensions ⓘ

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
- Portal: Use for portal

* Portal group tag ⓘ

Portal(s) using this tag

BYOD Portal (default)	Blacklist Portal (default)
Certificate Provisioning Portal (default)	Client Provisioning Portal (default)
Hotspot Guest Portal (default)	MDM Portal (default)
My Devices Portal (default)	Self-Registered Guest Portal (default)
Sponsor Portal (default)	Sponsored Guest Portal (default)

如果已為此證書選擇管理員角色，則ISE節點必須重新啟動其服務。根據分配給虛擬機器的版本和資源，這可能需要10-15分鐘。要檢查應用程式的狀態，請開啟ISE命令列並發出 `show application status ise` 指令。

Warning: Enabling Admin role for this certificate will cause an application server restart on the selected node.

Note: Make sure required Certificate Chain is imported under Trusted Certificates

* Certificate

Friendly Name ⓘ

Warning: The Portal tag is already assigned to the following certificate(s). If you proceed, it will be removed from the existing certificates, and affected portals will be restarted. Do you want to proceed?

- Default self-signed server certificate

Friendly Name ⓘ

Extensions ⓘ

如果在證書匯入時選擇了admin或portal角色，則可以在訪問瀏覽器中的管理員或門戶頁面時驗證新證書是否就位。在瀏覽器中選擇鎖定符號，在證書下，路徑會驗證整個鏈是否存在，以及電腦是否信任該鏈。瀏覽器必須信任新的管理員或門戶證書，只要該證書鏈構建正確，且瀏覽器信任該證書鏈。

注意：若要續訂當前由CA簽署的系統憑證，請產生新的CSR，並使用相同的選項將簽署的憑證繫結到該憑證。由於可以在ISE啟用之前安裝新證書，因此計畫在新證書過期之前安裝新證書。舊證書到期日期與新證書開始日期之間的這段重疊期為續訂證書和計畫交換提供了時間，幾乎不需要停機。請取得開始日期早於舊憑證到期日期的新憑證。這兩個日期之間的時間間隔即為變更期間。新證書進入其有效日期範圍後，啟用所需的協定(Admin/EAP/Portal)。請記住，如果啟用Admin用法，服務將重新啟動。

提示：建議對管理員和EAP證書使用公司內部CA，對訪客/發起人/熱點/等門戶使用公開簽名的證書。原因在於，如果使用者或訪客進入網路且ISE門戶使用訪客門戶的私密簽名證書，他們將會收到證書錯誤或者其瀏覽器可能會阻止他們進入門戶頁面。要避免所有這些情況，請使用公共簽名證書供門戶使用，以確保更好的使用者體驗。此外，必須將每個部署節點的IP地址新增到SAN欄位，以避免通過IP地址訪問伺服器時出現證書警告。

備份證書和私鑰

建議匯出：

- 1.所有系統證書（來自部署中的所有節點）及其私鑰（重新安裝這些證書需要私鑰）都傳送到安全位置。請記下證書配置（證書用於何種服務）。
- 2.來自主管理節點的受信任證書儲存的所有證書。請記下證書配置（證書用於何種服務）。
- 3.所有證書頒發機構證書。

為了做到這一點，

1. 導航至 Administration > System > Certificates > Certificate Management > System Certificates. 選擇證書並按一下 Export. 選擇 Export Certificates 和私鑰單選按鈕。輸入私鑰密碼並確認密碼。按一下 Export.
2. 導航至 Administration > System > Certificates > Certificate Management > Trusted Certificates. 選擇證書並按一下 Export. 按一下 Save File 匯出證書。
3. 導航至 Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates. 選擇證書並按一下 Export. 選擇 Export Certificates 和私鑰單選按鈕。輸入私鑰密碼和確認密碼。按一下 Export. 按一下 Save File 匯出證書。

疑難排解

檢查證書有效性

如果思科ISE受信任證書或系統證書儲存中的任何證書已過期，升級過程將失敗。確保檢查「受信任的證書」和「系統證書」視窗的「到期日期」欄位中的有效性(Administration > System > Certificates > Certificate Management)，如有必要，請在升級之前續訂它們。

此外，在CA Certificates視窗中檢查證書的Expiration Date欄位的有效性(Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates)，如有必要，請在升級之前續訂它們。

刪除證書

如果ISE中的證書已過期或未使用，則需要將其刪除。確保在刪除之前匯出證書（如果適用，請使用其私鑰）。

若要刪除過期的證書，請導航至 Administration > System > Certificates > Certificate Management.按一下 System Certificates Store.選擇過期證書並按一下 Delete.有關受信任證書和證書頒發機構證書儲存的資訊，請參閱相同內容。

請求方不信任802.1x身份驗證上的ISE伺服器證書

驗證ISE是否為SSL握手進程傳送完整證書鏈。

在客戶端OS設定中選擇了需要伺服器證書（即PEAP）和驗證伺服器標識的EAP方法，作為身份驗證過程的一部分，請求方使用本地信任儲存中的證書來驗證證書鏈。作為SSL握手流程的一部分，ISE會呈現其證書以及鏈中存在的任何根證書和/或中間證書。如果鏈不完整或其信任儲存中缺少此鏈，則請求方無法驗證伺服器身份。

為了驗證證書鏈是否傳遞回客戶端，請從ISE捕獲資料包(Operations > Diagnostic Tools > General Tools > TCP Dump)或Wireshark捕獲。開啟捕獲並應用篩選器 ssl.handshake.certificates 查詢訪問質詢。

選擇後，導航至 Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates.

如果鏈不完整，請導航到ISE Administration > Certificates > Trusted Certificates 並驗證是否存在根和/或中間證書。如果憑證鏈結成功通過，則憑證鏈結本身必須透過此處概述的方法驗證為有效。

開啟每個證書（伺服器、中間和根）並驗證信任鏈，將每個證書的主題金鑰識別符號(SKI)與鏈中下一個證書的頒發機構金鑰識別符號(AKI)匹配。

ISE證書鏈正確，但終端在身份驗證期間拒絕ISE伺服器證書

如果ISE為SSL握手顯示其完整證書鏈且請求方仍拒絕證書鏈；下一步是驗證根證書和/或中間證書是否在客戶端本地信任儲存中。

若要從Windows裝置驗證這一點，請啟動 mmc.exe(Microsoft Management Console)，導航到 File > Add-Remove Snap-in.從可用管理單元列中選擇 Certificates 然後按一下 Add.選擇任一 My user account 或 Computer account 根據使用的身份驗證型別（使用者或電腦），然後按一下 OK.

在控制檯檢視中，選擇受信任的根證書頒發機構和中間證書頒發機構以驗證本地信任儲存中是否存在根證書和中間證書。

驗證這是伺服器身份檢查問題的一種簡單方法，取消選中Suppllicant客戶端配置檔案配置下的 Validate Server Certificate，然後再次對其進行測試。

常見問題

當ISE發出證書已存在的警告時，該怎麼做？

此消息表示ISE檢測到具有完全相同OU引數的系統證書，並且嘗試安裝重複的證書。由於不支援重複的系統證書，因此建議將任何城市/州/省(City/State/Dept.)值更改為稍有不同的值，以確保新證書不同。

為什麼瀏覽器引發警告，指出來自ISE的門戶頁面由不受信任的伺服器顯示？

當瀏覽器不信任伺服器的身份證書時，會發生這種情況。

首先，確保瀏覽器上顯示的門戶證書符合預期，並且已在ISE上為門戶配置。

第二，確保通過FQDN訪問門戶 — 在使用中的IP地址的情況下，確保FQDN和IP地址都位於證書的SAN和/或CN欄位中。

最後，確保門戶證書鏈 (ISE門戶、中間CA、根CA證書) 在客戶端OS/瀏覽器軟體上匯入/受信任。

註:iOS、Android OS和Chrome/Firefox瀏覽器的某些較新版本對證書有嚴格的安全期望。即使滿足這些點，如果入口和中間CA小於SHA-256，它們也可以拒絕連線。

當由於無效證書導致升級失敗時，該怎麼做？

如果思科ISE受信任證書或系統證書儲存中的任何證書已過期，升級過程將失敗。確保檢查「受信任的證書」和「系統證書」視窗的「到期日期」欄位中的有效性(Administration > System > Certificates > Certificate Management)，如有必要，請在升級之前續訂它們。

此外，在CA Certificates視窗中檢查證書的Expiration Date欄位的有效性(Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates)，如有必要，請在升級之前續訂它們。

在ISE升級之前，請確保內部CA證書鏈有效。

導航至 Administration > System > Certificates > Certificate Authority Certificates。對於部署中的每個節點，在Friendly Name (友好名稱) 列中選擇具有Certificate Services Endpoint Sub CA的證書。按一下 View 並檢查「Certificate Status (證書狀態)」是否為正常消息且是否可見。

如果任何證書鏈中斷，請確保在Cisco ISE升級過程開始之前解決此問題。要解決此問題，請導航至 Administration > System > Certificates > Certificate Management > Certificate Signing Requests，並為ISE根CA選項生成一個。

相關資訊

- [ISE 2.7管理證書和證書儲存設定](#)
- [在ISE中實施數位證書](#)
- [技術支援與文件 - Cisco Systems](#)

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）。