

Configurazione dei certificati TLS/SSL in ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Certificati server](#)

[Certificati ISE](#)

[Certificati di sistema](#)

[Archivio certificati attendibili](#)

[Attività di base](#)

[Genera un certificato autofirmato](#)

[Rinnova un certificato autofirmato](#)

[Installare un certificato protetto](#)

[Installa un certificato firmato dalla CA](#)

[Certificati di backup e chiavi private](#)

[Risoluzione dei problemi](#)

[Verifica validità certificato](#)

[Eliminare un certificato](#)

[Il richiedente non considera attendibile il certificato del server ISE per un'autenticazione 802.1x](#)

[La catena di certificati ISE è corretta, ma l'endpoint rifiuta il certificato del server ISE durante l'autenticazione](#)

[Domande frequenti](#)

[Cosa fare quando ISE visualizza un avviso che il certificato esiste già?](#)

[Perché il browser visualizza un avviso che indica che la pagina del portale di ISE è stata presentata da un server non attendibile?](#)

[Cosa fare quando un aggiornamento non riesce a causa di certificati non validi?](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive i certificati TLS/SSL in Cisco ISE, i tipi e i ruoli dei certificati ISE, come eseguire le attività comuni e risolvere i problemi, e le risposte alle domande frequenti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

1. Cisco Identity Services Engine (ISE)
2. La terminologia utilizzata per descrivere i diversi tipi di implementazione di ISE e AAA.
3. Nozioni base sul protocollo RADIUS e sull'AAA

4. Certificati SSL/TLS e x509

5. Nozioni di base sull'infrastruttura a chiave pubblica (PKI)

Componenti usati

Il riferimento delle informazioni contenute in questo documento è la versione software e hardware di Cisco ISE 2007, release 2.4 - 2.7. Copre l'ISE dalla versione 2.4 alla versione 2.7; tuttavia, deve essere simile o identica ad altre versioni del software ISE 2.x, a meno che non sia specificato diversamente.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Certificati server

I certificati server vengono utilizzati dai server per presentare l'identità del server ai client ai fini dell'autenticità e per fornire un canale sicuro per la comunicazione. Questi possono essere autofirmati (quando il server rilascia il certificato a se stesso) o rilasciati da un'autorità di certificazione (interna a un'organizzazione o di un fornitore conosciuto).

I certificati server vengono in genere rilasciati ai nomi host o al nome di dominio completo (FQDN, Fully Qualified Domain Name) del server oppure possono essere anche certificati jolly (*.domain.com). Gli host, i domini o i sottodomini a cui vengono rilasciati sono in genere indicati nei campi Nome comune (CN) o Nome alternativo soggetto (SAN).

I certificati con caratteri jolly sono certificati SSL che utilizzano una notazione con caratteri jolly (un asterisco al posto del nome host) e consentono quindi di condividere lo stesso certificato tra più host di un'organizzazione. Ad esempio, il valore CN o SAN per un certificato con caratteri jolly Nome soggetto può essere simile a *.company.com e può essere utilizzato per proteggere qualsiasi host di questo dominio, ad esempio server1.com, server2.com e così via.

I certificati in genere utilizzano la crittografia a chiave pubblica o asimmetrica.

- Chiave pubblica: la chiave pubblica è presente nel certificato in uno dei campi ed è condivisa pubblicamente da un sistema quando un dispositivo tenta di comunicare con esso.
- Chiave privata: la chiave privata è privata del sistema finale e viene associata alla chiave pubblica. I dati crittografati con una chiave pubblica possono essere decrittografati solo dalla chiave privata associata specifica e viceversa.

Certificati ISE

Cisco ISE si basa sull'infrastruttura a chiave pubblica (PKI) per fornire comunicazioni sicure con endpoint, utenti, amministratori e così via, nonché tra i nodi Cisco ISE in un'implementazione

multinodo. La PKI si basa sui certificati digitali x.509 per trasferire le chiavi pubbliche per la crittografia e la decrittografia dei messaggi e per verificare l'autenticità di altri certificati presentati da utenti e dispositivi. Cisco ISE ha due categorie di certificati generalmente utilizzati:

- **Certificati di sistema:** si tratta di certificati server che identificano un nodo Cisco ISE per i client. Ogni nodo Cisco ISE ha i propri certificati locali, ciascuno dei quali è archiviato sul nodo insieme alla rispettiva chiave privata.
- **Archiviazione certificati protetti:** si tratta di certificati dell'Autorità di certificazione (CA) utilizzati per convalidare i certificati presentati all'ISE per vari scopi. Questi certificati nell'archivio certificati sono gestiti sul nodo Amministrazione primaria e vengono replicati su tutti gli altri nodi in un'implementazione Cisco ISE distribuita. L'archivio certificati contiene anche i certificati generati per i nodi ISE dall'autorità di certificazione interna di ISE destinata a BYOD.

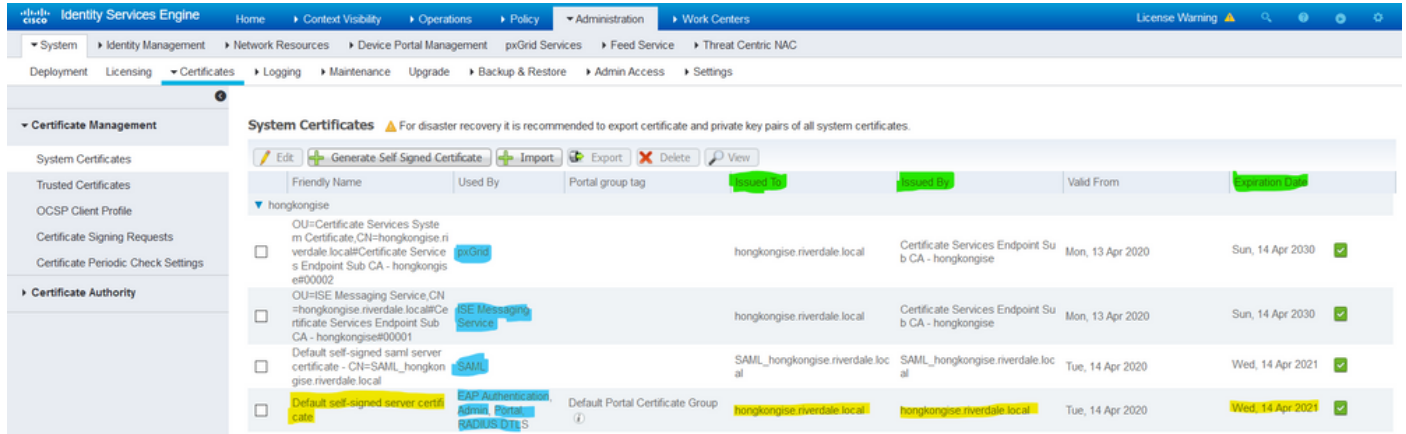
Certificati di sistema

I certificati di sistema possono essere utilizzati per uno o più ruoli. Ogni ruolo ha uno scopo diverso ed è spiegato di seguito:

- **Admin:** questa opzione viene utilizzata per proteggere tutte le comunicazioni oltre 443 (GUI di amministrazione), nonché per la replica e per qualsiasi porta/uso non elencato qui.
- **Portale:** viene utilizzato per proteggere la comunicazione HTTP tramite portali quali il portale CWA (Centralized Web Authentication), Guest, BYOD, provisioning client, portali Native Supplicant Provisioning e così via. È necessario mappare ogni portale a un tag del gruppo portale (l'impostazione predefinita è Tag predefinito del gruppo portale) che indica al portale di utilizzare il certificato con tag specifico. Il menu a discesa Nome tag gruppo portale nelle opzioni di modifica del certificato consente di creare un nuovo tag o di scegliere un tag esistente.
- **EAP:** ruolo che specifica il certificato presentato ai client per l'autenticazione 802.1x. I certificati vengono utilizzati con quasi tutti i metodi EAP possibili, ad esempio EAP-TLS, PEAP, EAP-FAST e così via. Con i metodi EAP con tunneling come PEAP e FAST, Transport Layer Security (TLS) viene utilizzato per proteggere lo scambio di credenziali. Le credenziali del client non vengono inviate al server fino a quando il tunnel non viene stabilito per garantire uno scambio sicuro.
- **DTLS RADIUS:** questo ruolo specifica il certificato da utilizzare per una connessione DTLS (connessione TLS su UDP) per crittografare il traffico RADIUS tra un dispositivo NAD (Network Access Device) e ISE. Per il corretto funzionamento di questa funzionalità, è necessario che sia supportata la crittografia DTLS.
- **SAML:** il certificato del server viene utilizzato per proteggere le comunicazioni con il provider di identità SAML (IdP). Un certificato designato per l'utilizzo SAML non può essere utilizzato per altri servizi, ad esempio l'amministrazione, l'autenticazione EAP e così via.
- **ISE Messaging Service:** a partire dalla versione 2.6, ISE utilizza ISE Messaging Service invece del protocollo Syslog legacy per la registrazione dei dati. Utilizzato per crittografare la comunicazione.
- **PxGrid:** questo certificato è utilizzato per i servizi PxGrid su ISE.

L'installazione di ISE genera `Default Self-Signed Server Certificate`. Questa opzione viene assegnata per le DTLS EAP Authentication, Admin, Portal e RADIUS per impostazione predefinita. È consigliabile

spostare questi ruoli in un'autorità di certificazione interna o in un certificato noto firmato dall'autorità di certificazione.

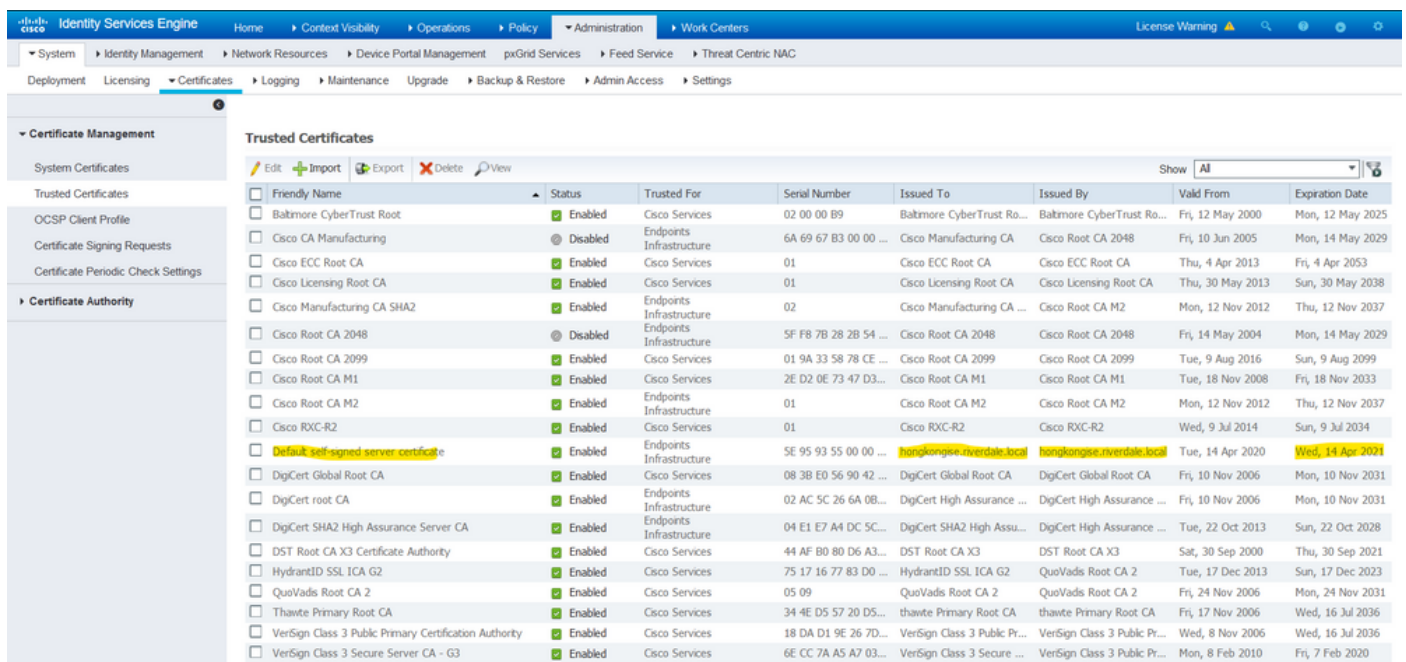


Suggerimento: è buona norma garantire che gli indirizzi IP e FQDN del server ISE siano aggiunti al campo SAN del certificato del sistema ISE. In generale, per garantire che l'autenticazione dei certificati in Cisco ISE non sia influenzata da differenze secondarie nelle funzioni di verifica basate sui certificati, usare nomi host in minuscolo per tutti i nodi Cisco ISE distribuiti in una rete.

Nota: il formato di un certificato ISE deve essere PEM (Privacy Enhanced Mail) o DER (Distinguished Encoding Rules).

Archivio certificati attendibili

I certificati dell'autorità di certificazione devono essere archiviati in Administration > System > Certificates > Certificate Store e devono avere la Trust for client authentication use-case per assicurarsi che ISE utilizzi questi certificati per convalidare i certificati presentati dagli endpoint, dai dispositivi o da altri nodi ISE.



Attività di base

Il certificato ha una data di scadenza e può essere revocato o sostituito. Se il certificato del server ISE scade, possono verificarsi gravi problemi se non vengono sostituiti con un nuovo certificato valido.

Nota: se il certificato utilizzato per il protocollo EAP (Extensible Authentication Protocol) scade, l'autenticazione dei client potrebbe non riuscire perché il client non considera più attendibile il certificato ISE. Se un certificato utilizzato per i portali scade, i client e i browser possono rifiutarsi di connettersi al portale. Se il certificato di utilizzo dell'amministratore scade, il rischio è ancora maggiore e questo impedisce a un amministratore di accedere all'ISE e la distribuzione distribuita può cessare di funzionare come deve.

Genera un certificato autofirmato

Per generare nuovi certificati autofirmati, passare a Administration > System > Certificates > System Certificates. Fare clic sul pulsante Generate Self Signed Certificate.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is Administration > System > Certificates > System Certificates. The 'Generate Self Signed Certificate' button is highlighted in yellow. The page displays a table of certificates with columns for Friendly Name, Used By, Portal group tag, and Issued To. A certificate entry is visible for 'hongkongise' with a friendly name 'OU=Certificate Services System Certificate, CN=hongkongise.riverdale.local#Certificate Services Endpoint Sub CA - hongkongise#0000?'.

Questo elenco descrive i campi della pagina Genera certificato autofirmato.

Linee guida per l'utilizzo del nome del campo Impostazioni certificato autofirmato:

- Seleziona nodo: (obbligatorio) il nodo per il quale è necessario generare il certificato di sistema.
- CN: (obbligatorio se SAN non è specificato) per impostazione predefinita, CN è il nome di dominio completo (FQDN) del nodo ISE per il quale viene generato il certificato autofirmato.
- Unità organizzativa: nome dell'unità organizzativa, ad esempio Ingegneria.
- Organizzazione (O): nome dell'organizzazione, ad esempio Cisco.
- Città (L): (Non abbreviare) Nome della città, ad esempio San Jose.
- Stato (ST): (non abbreviato) Nome dello stato, ad esempio California.
- Paese (C): nome del paese. È necessario il codice ISO a due lettere del paese. Per esempio, gli Stati Uniti.
- SAN: indirizzo IP, nome DNS o URI (Uniform Resource Identifier) associato al certificato.
- Tipo di chiave: specificare l'algoritmo da utilizzare per creare la chiave pubblica: RSA o ECDSA.

- Lunghezza chiave: specificare le dimensioni in bit per la chiave pubblica. Queste opzioni sono disponibili per RSA: 512 1024 2048 4096 e queste opzioni sono disponibili per ECDSA: 256 384.
- Digest con cui firmare: scegliere uno dei seguenti algoritmi hash: SHA-1 o SHA-256.
- Criteri certificati: immettere l'OID dei criteri dei certificati o l'elenco degli OID a cui il certificato deve conformarsi. Per separare gli OID, utilizzare virgole o spazi.
- TTL scadenza: specificare il numero di giorni dopo i quali il certificato scade.
- Nome descrittivo: immettere un nome descrittivo per il certificato. Se non si specifica alcun nome, Cisco ISE crea automaticamente un nome nel formato `XXXXX` dove `XXXXX` è un numero univoco di cinque cifre.
- Consenti certificati jolly: selezionare questa casella di controllo per generare un certificato jolly autofirmato (un certificato che contiene un asterisco (*) in qualsiasi CN nel soggetto e/o il nome DNS nella SAN. Ad esempio, il nome DNS assegnato alla SAN può essere `*.domain.com`).
- Utilizzo: scegliere il servizio per il quale deve essere utilizzato questo certificato di sistema. Le opzioni disponibili sono:

AdminAutenticazione EAPDTLS RADIUSpxGridSAMLPortale

The screenshot displays the 'Generate Self Signed Certificate' configuration page in the Cisco Identity Services Engine (ISE) Administration console. The interface includes a navigation menu on the left and a main configuration area on the right.

Navigation Menu:

- 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 Panel: 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:
- Subject**
 - Common Name (CN):
 - Organizational Unit (OU):
 - Organization (O):
 - City (L):
 - State (ST):
 - Country (C):
- Subject Alternative Name (SAN):
 - IP Address:
- * Key type:
- * Key Length:
- * Digest to Sign With:
- Certificate Policies:

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

Certificate Management

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

Certificate Authority

Subject Alternative Name (SAN)

* Key type

* Key Length

* Digest to Sign With

Certificate Policies

* Expiration TTL

Friendly Name

Allow Wildcard Certificates

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
- SAML: Use certificate for SAML Signing
- Portal: Use for portal

Nota: le chiavi pubbliche RSA ed ECDSA possono avere lunghezze di chiave diverse per lo stesso livello di protezione. Scegliere 2048 se si desidera ottenere un certificato pubblico firmato da un'autorità di certificazione o distribuire Cisco ISE come sistema di gestione dei criteri conforme a FIPS.

Rinnova un certificato autofirmato

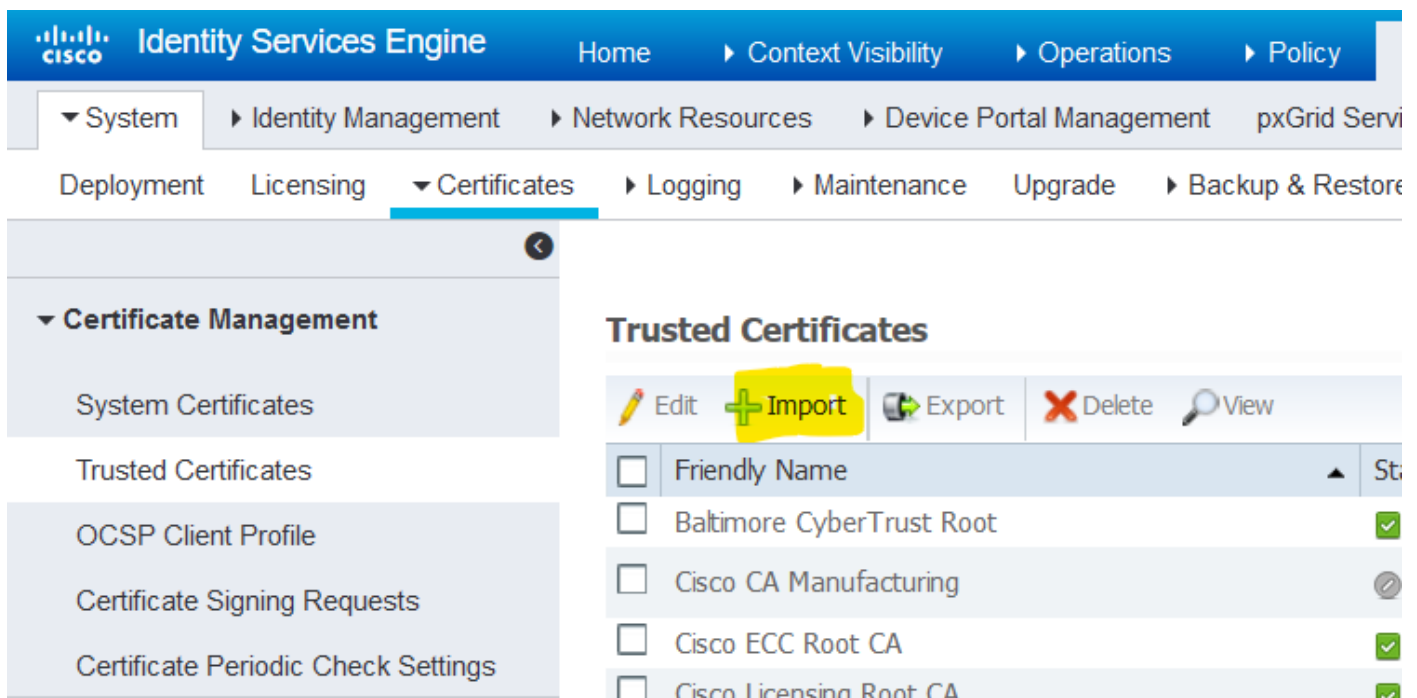
Per visualizzare i certificati autofirmati esistenti, passare a Administration > System > Certificates > System Certificates nella console ISE. Qualsiasi certificato con le diciture 'Rilasciato a' e 'Rilasciato da' se menzionato nello stesso FQDN del server ISE, è un certificato autofirmato. Scegliere questo certificato e fare clic su **Edit**.

Inferiore **Renew Self Signed Certificate**, controllare la **Renewal Period** e impostare il valore TTL di scadenza in base alle esigenze. Infine, fare clic su **Save**.

Installare un certificato protetto

Ottenere i certificati con codifica Base 64 dalla CA radice, dalle CA intermedie e/o dagli host che devono essere considerati attendibili.

1. Accedere al nodo ISE e selezionare Administration > System > Certificate > Certificate Management > Trusted Certificates e fare clic su Import, come mostrato nell'immagine.



The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', and 'Policy'. Below this, a secondary navigation bar shows 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', and 'pxGrid Services'. The 'System' menu is expanded, showing 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', and 'Backup & Restore'. The 'Certificates' menu is further expanded, showing 'Certificate Management', 'System Certificates', 'Trusted Certificates', 'OCSP Client Profile', 'Certificate Signing Requests', and 'Certificate Periodic Check Settings'. The 'Trusted Certificates' page is displayed, featuring a toolbar with 'Edit', 'Import' (highlighted in yellow), 'Export', 'Delete', and 'View' buttons. Below the toolbar is a table of trusted certificates:

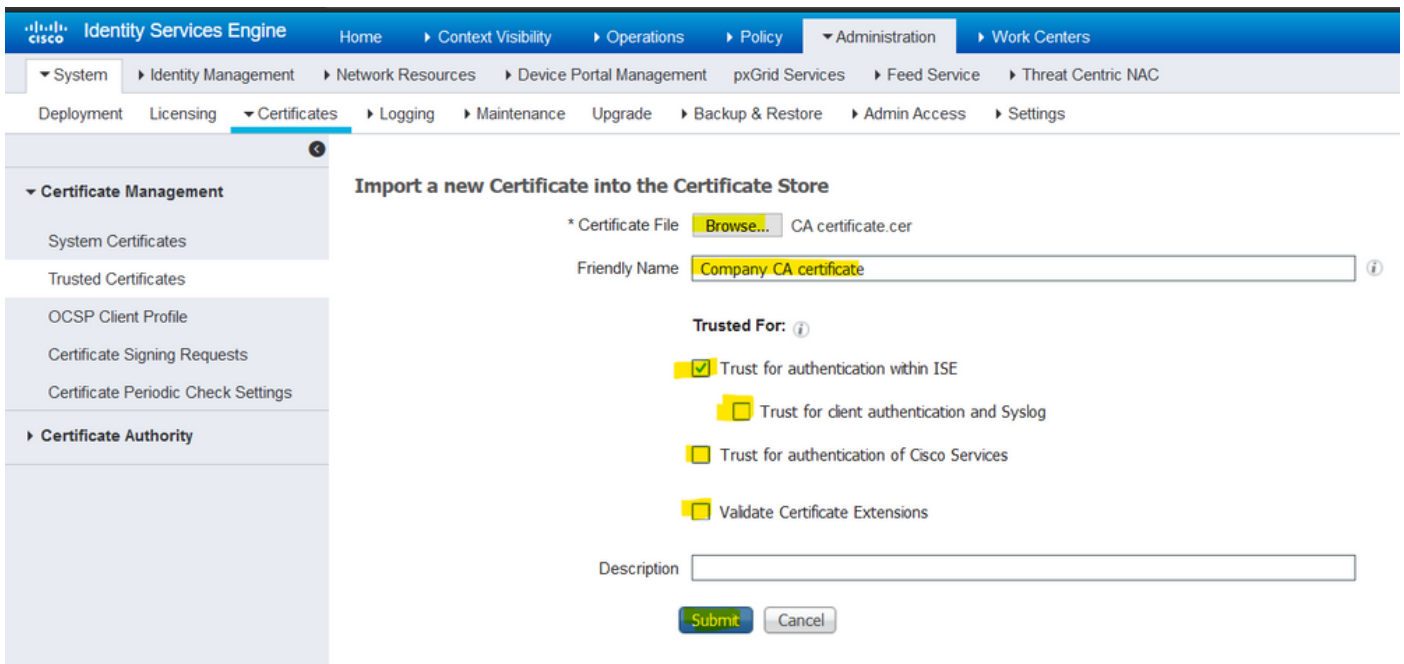
<input type="checkbox"/>	Friendly Name	Status
<input type="checkbox"/>	Baltimore CyberTrust Root	✓
<input type="checkbox"/>	Cisco CA Manufacturing	⊘
<input type="checkbox"/>	Cisco ECC Root CA	✓
<input type="checkbox"/>	Cisco Licensing Root CA	✓

2. Nella pagina successiva, caricare i certificati CA ottenuti (nello stesso ordine descritto in precedenza). Assegnare loro un nome descrittivo e una descrizione che spieghi a cosa serve il certificato per tenerne traccia.

In base alle esigenze, selezionare le caselle accanto a:

- Attendibilità per l'autenticazione in ISE - Consente di aggiungere nuovi nodi ISE in cui lo stesso certificato CA attendibile è stato caricato nell'archivio certificati attendibili.
- Trust for client authentication and Syslog: selezionare questa opzione per utilizzare il certificato per autenticare gli endpoint che si connettono ad ISE con i server EAP e/o Secure Syslog.
- Attendibilità per l'autenticazione dei servizi Cisco - Necessario solo per considerare attendibili i servizi Cisco esterni, ad esempio un servizio feed.

3. Infine, fare clic su Submit. A questo punto, il certificato deve essere visibile nell'archivio attendibile ed essere sincronizzato con tutti i nodi ISE secondari (se presenti in una distribuzione).



Installa un certificato firmato dalla CA

Dopo aver aggiunto i certificati CA radice e intermedia all'archivio certificati attendibili, è possibile emettere una richiesta di firma del certificato (CSR) e associare il certificato firmato in base al CSR al nodo ISE.

1. A tale scopo, passare a **Administration > System > Certificates > Certificate Signing Requests** e fai clic su **Generate Certificate Signing Requests (CSR)** per generare un CSR.
 2. Nella pagina visualizzata, nella sezione **Uso**, scegliere il ruolo da utilizzare dal menu a discesa.
- Se il certificato viene utilizzato per più ruoli, scegliere **Multiuso**. Una volta generato il certificato, i ruoli possono essere modificati, se necessario. Nella maggior parte dei casi, il certificato può essere impostato per l'utilizzo multiuso nell'elenco a discesa **Utilizzato per**; in questo modo il certificato può essere utilizzato per tutti i portali Web ISE.
3. Selezionare la casella accanto al nodo o ai nodi ISE per scegliere il nodo o i nodi per i quali il certificato è generato.
 4. Se lo scopo è installare/generare un certificato con caratteri jolly, controllare la **Allow Wildcard Certificates** casella.

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

Certificate Management

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

Certificate Authority

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  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 type="checkbox"/> hongkongise	hongkongise#Multi-Use

Usage

Certificate(s) will be used for  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 type="checkbox"/> hongkongise	hongkongise#Multi-Use

5. Compilare le informazioni sull'oggetto in base ai dettagli relativi all'host o all'organizzazione (unità organizzativa, organizzazione, città, stato e paese).

6. Per terminare, fai clic su **Generate** e quindi fare clic su **Export** sul popup che viene fuori.

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

Certificate Management

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

Certificate Authority

hongkongise hongkongise#Multi-Use

Subject

Common Name (CN) \$FQDN\$

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

Generate Cancel

Country (C) IN

Subject Alternative Name (SAN) [Dropdown]

- DNS Name
- IP Address
- Uniform Resource Identifier
- Directory Name

* Key type RSA

* Key Length 2048

* Digest to Sign With SHA-256

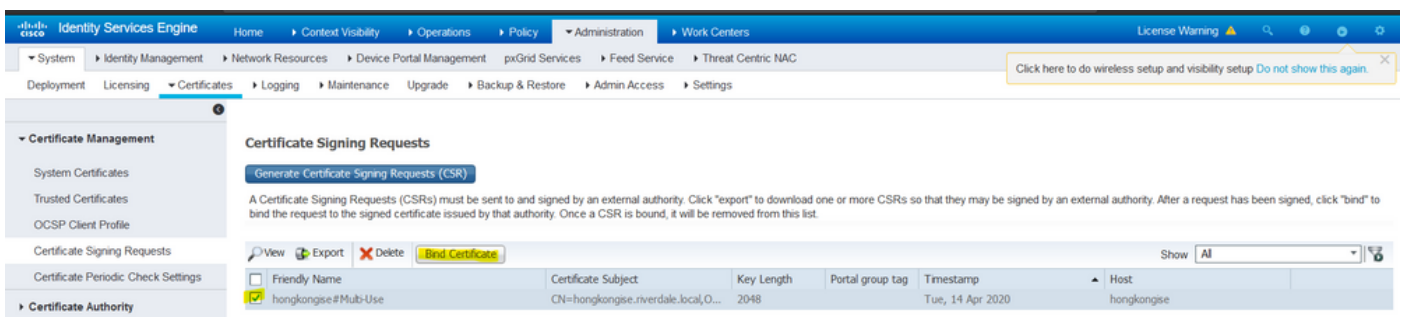
In questo modo viene scaricata la richiesta di certificato con codifica Base 64 appena creata. Questo file PEM deve essere inviato alla CA per la firma e ottenere il file CER del certificato firmato risultante (con codifica Base 64).

Nota: sotto il campo CN, ISE compila automaticamente l'FQDN dei nodi.

Nota: in ISE 1.3 e 1.4, era necessario emettere due CSR almeno per utilizzare pxGrid. Una è dedicata a pxGrid e l'altra al resto dei servizi. Dalla versione 2.0 in poi, tutto questo è su un unico CSR.

Nota: se il certificato viene utilizzato per le autenticazioni EAP, il simbolo '*' non deve trovarsi nel campo CN soggetto in quanto i supplicant Windows rifiutano il certificato server. Anche se Convalida identità server è disabilitato sul supplicant, l'handshake SSL può non riuscire quando '*' è nel campo CN. È invece possibile utilizzare un FQDN generico nel campo CN e quindi *.domain.com può essere utilizzato nel campo Nome DNS SAN. Alcune Autorità di certificazione (CA) possono aggiungere automaticamente il carattere jolly (*) nel CN del certificato anche se non è presente nel CSR. In questo scenario, è necessario inviare una richiesta speciale per impedire questa azione.

7. Una volta che il certificato è stato firmato dalla CA (generata dal CSR come mostrato nel video, [qui](#) se si usa Microsoft CA), tornare alla GUI di ISE e selezionare **Amministrazione > Sistema > Certificati > Gestione certificati > Richiesta di firma certificato**; selezionare la casella accanto al CSR creato in precedenza e fare clic sul pulsante **Associa certificato**.



8. Caricare quindi il certificato firmato appena ricevuto e assegnargli un nome descrittivo per ISE. Scegliere quindi le caselle accanto a Usi in base alle esigenze del certificato (come autenticazione Admin e EAP, Portal e così via) e fare clic su **Submit**, come mostrato nell'immagine:

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

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)

Se per questo certificato è stato scelto il ruolo di amministratore, il nodo ISE deve riavviare i servizi. In base alla versione e alle risorse allocate alla VM, questa operazione può richiedere 10-15 minuti. Per controllare lo stato dell'applicazione, aprire la riga di comando di ISE e usare il comando `show application status ise`

next visibility Operations Policy Administration Work Centers

es Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Maintenance

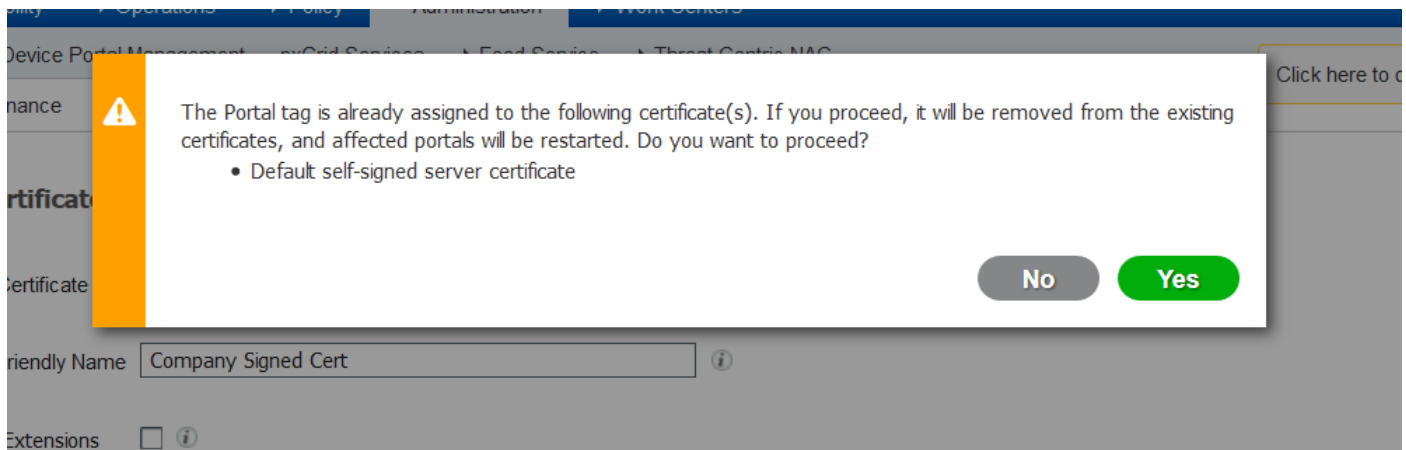
Bind CA Signed Certificate

* Certificate

Friendly Name ⓘ

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



Se durante l'importazione del certificato è stato scelto il ruolo di amministratore o di portale, è possibile verificare che il nuovo certificato sia presente quando si accede alle pagine di amministrazione o del portale nel browser. Scegliere il simbolo di blocco nel browser e sotto il certificato, il percorso verifica che l'intera catena sia presente e considerata attendibile dal computer. Il browser deve considerare attendibile il nuovo certificato dell'amministratore o del portale se la catena è stata creata correttamente e se è considerata attendibile dal browser.

Nota: per rinnovare un certificato di sistema attualmente firmato dalla CA, generare un nuovo CSR e associarvi il certificato firmato con le stesse opzioni. Poiché è possibile installare un nuovo certificato sull'ISE prima che sia attivo, pianificare l'installazione del nuovo certificato prima della scadenza di quello precedente. Questo periodo di sovrapposizione tra la vecchia data di scadenza del certificato e la nuova data di inizio del certificato consente di rinnovare i certificati e pianificare lo scambio con un tempo di inattività minimo o nullo. Richiedere un nuovo certificato con una data di inizio antecedente alla data di scadenza del vecchio certificato. La differenza tra le due date viene chiamato intervallo di modifica. Quando il nuovo certificato entra nell'intervallo di date valido, abilitare i protocolli necessari (Admin/EAP/Portal). Tenere presente che se l'utilizzo di Admin è abilitato, è necessario riavviare il servizio.

Suggerimento: si consiglia di utilizzare l'autorità di certificazione interna della società per i certificati di amministrazione ed EAP e un certificato firmato pubblicamente per i portali Guest/Sponsor/Hotspot/etc. Il motivo è che se un utente o un guest accede alla rete e il portale ISE utilizza un certificato firmato privatamente per il portale guest, vengono restituiti errori di certificato o il browser potrebbe bloccarli dalla pagina del portale. Per evitare tutto ciò, utilizzare un certificato firmato pubblicamente per l'utilizzo del portale per garantire una migliore esperienza utente. Inoltre, ogni nodo di distribuzione deve essere aggiunto al campo SAN per evitare che venga visualizzato un avviso di certificato quando si accede al server tramite l'indirizzo IP.

Certificati di backup e chiavi private

Si consiglia di esportare:

1. Tutti i certificati di sistema (provenienti da tutti i nodi della distribuzione) insieme alle relative chiavi private (necessarie per reinstallarli) in una posizione sicura. Prendere nota della configurazione del certificato (per quale servizio è stato utilizzato il certificato).

2. Tutti i certificati dell'archivio dei certificati protetti del nodo di amministrazione principale. Prendere nota della configurazione del certificato (per quale servizio è stato utilizzato il certificato).
3. Tutti i certificati dell'autorità di certificazione.

A tal fine,

1. Passa a Administration > System > Certificates > Certificate Management > System Certificates. Scegliere il certificato e fare clic su Export. Scegli Export Certificates e il pulsante di opzione Chiavi private. Immettere la password della chiave privata e confermare la password. Clic Export.
2. Passa a Administration > System > Certificates > Certificate Management > Trusted Certificates. Scegliere il certificato e fare clic su Export. Clic Save File per esportare il certificato.
3. Passa a Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates. Scegliere il certificato e fare clic su Export. Scegli Export Certificates e il pulsante di opzione Chiavi private. Immettere la password della chiave privata e la password di conferma. Clic Export. Clic Save File per esportare il certificato.

Risoluzione dei problemi

Verifica validità certificato

Il processo di aggiornamento non riesce se un certificato presente nell'archivio dei certificati protetti di Cisco ISE o dei certificati di sistema è scaduto. Verificare la validità nel campo Data scadenza delle finestre Certificati attendibili e Certificati di sistema (Administration > System > Certificates > Certificate Management) e, se necessario, rinnovarli prima dell'aggiornamento.

Verificare inoltre la validità nel campo Data scadenza dei certificati nella finestra Certificati CA (Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates) e, se necessario, rinnovarli prima dell'aggiornamento.

Eliminare un certificato

Se un certificato nell'ISE è scaduto o inutilizzato, deve essere rimosso. Assicurarsi di esportare i certificati (con le relative chiavi private, se applicabile) prima dell'eliminazione.

Per eliminare un certificato scaduto, passare a Administration > System > Certificates > Certificate Management. Fare clic sul pulsante System Certificates Store. Scegliere i certificati scaduti e fare clic su Delete. Fare riferimento alla stessa procedura per gli archivi certificati attendibili e certificati dell'Autorità di certificazione.

Il richiedente non considera attendibile il certificato del server ISE per un'autenticazione 802.1x

Verificare se ISE invia l'intera catena di certificati per il processo di handshake SSL.

Se nelle impostazioni del sistema operativo del client sono selezionati i metodi EAP che richiedono un certificato server (PEAP) e Convalida identità server, il richiedente convalida la catena di certificati con i certificati presenti nel proprio archivio attendibilità locale come parte del

processo di autenticazione. Nell'ambito del processo di handshake SSL, ISE presenta il proprio certificato e tutti i certificati radice e/o intermedi presenti nella propria catena. Il supplicant non è in grado di convalidare l'identità del server se la catena è incompleta o se manca nel relativo archivio di attendibilità.

Per verificare che la catena di certificati venga restituita al client, acquisire un pacchetto da ISE (Operations > Diagnostic Tools > General Tools > TCP Dump) o Wireshark sull'endpoint al momento dell'autenticazione. Aprire l'acquisizione e applicare il filtro `ssl.handshake.certificates` in Wireshark e trovare una sfida di accesso.

Una volta scelto, passare a `Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates`.

Se la catena è incompleta, passare ad ISE `Administration > Certificates > Trusted Certificates` e verificare che i certificati radice e/o intermedio siano presenti. Se la catena di certificati viene passata correttamente, è necessario verificarne la validità con il metodo qui descritto.

Aprire ogni certificato (server, intermedio e radice) e verificare che la catena di attendibilità corrisponda all'identificatore della chiave del soggetto (SKI, Subject Key Identifier) di ogni certificato all'identificatore della chiave dell'autorità (AKI, Authority Key Identifier) del certificato successivo nella catena.

La catena di certificati ISE è corretta, ma l'endpoint rifiuta il certificato del server ISE durante l'autenticazione

Se ISE presenta l'intera catena di certificati per l'handshake SSL e il richiedente ha ancora rifiutato la catena di certificati, il passaggio successivo consiste nel verificare che i certificati radice e/o intermedi si trovino nell'archivio di attendibilità locale del client.

Per verificare questa condizione da un dispositivo Windows, avviare `mmc.exe` (Microsoft Management Console), passare a `File > Add-Remove Snap-in`. Nella colonna snap-in disponibili scegliere `Certificates` e fare clic su `Add`. Scegliere una delle opzioni `My user account` o `Computer account` in base al tipo di autenticazione in uso (Utente o Computer) e quindi fare clic su `OK`.

Nella visualizzazione della console scegliere Autorità di certificazione radice attendibili e Autorità di certificazione intermedie per verificare la presenza di certificati radice e intermedi nell'archivio attendibile locale.

Per verificare in modo semplice se si tratta di un problema di controllo dell'identità del server, deselezionare `Convalida certificato server` nella configurazione del profilo del supplicant e testarlo di nuovo.

Domande frequenti

Cosa fare quando ISE visualizza un avviso che informa che il certificato esiste già?

Questo messaggio indica che ISE ha rilevato un certificato di sistema con lo stesso identico parametro dell'unità organizzativa ed è stato tentato l'installazione di un certificato duplicato. Poiché i certificati di sistema duplicati non sono supportati, si consiglia di modificare i valori di `Città/Stato/Rep.` su un valore leggermente diverso per garantire che il nuovo certificato sia diverso.

Perché il browser visualizza un avviso che indica che la pagina del portale di ISE è stata presentata da un server non attendibile?

Questo si verifica quando il browser non considera attendibile il certificato di identità del server.

In primo luogo, accertarsi che il certificato del portale visibile sul browser sia quello previsto e che sia stato configurato sull'ISE per il portale.

In secondo luogo, garantire l'accesso al portale tramite FQDN: nel caso in cui l'indirizzo IP sia in uso, verificare che l'FQDN e l'indirizzo IP siano presenti nei campi SAN e/o CN del certificato.

Infine, accertarsi che la catena di certificati del portale (portale ISE, CA intermedie, certificati CA radice) sia importata/considerata attendibile dal sistema operativo del client o dal browser.

Nota: alcune versioni più recenti di iOS, Android OS e Chrome/Firefox browser hanno rigorose aspettative di sicurezza del certificato. Anche se questi punti sono soddisfatti, possono rifiutarsi di connettersi se le CA del portale e intermedie sono inferiori a SHA-256.

Cosa fare quando un aggiornamento non riesce a causa di certificati non validi?

Il processo di aggiornamento non riesce se un certificato presente nell'archivio dei certificati protetti di Cisco ISE o dei certificati di sistema è scaduto. Verificare la validità nel campo Data scadenza delle finestre Certificati attendibili e Certificati di sistema (Administration > System > Certificates > Certificate Management) e, se necessario, rinnovarli prima dell'aggiornamento.

Verificare inoltre la validità nel campo Data scadenza dei certificati nella finestra Certificati CA (Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates) e, se necessario, rinnovarli prima dell'aggiornamento.

Prima dell'aggiornamento ISE, verificare che la catena di certificati della CA interna sia valida.

Passa a Administration > System > Certificates > Certificate Authority Certificates. Per ogni nodo della distribuzione scegliere il certificato con la CA secondaria dell'endpoint di Servizi certificati nella colonna Nome descrittivo. Clic **View** e verificare se lo stato del certificato è un messaggio valido e visibile.

Se si verifica un'interruzione nella catena di certificati, accertarsi di risolvere il problema prima di avviare il processo di aggiornamento di Cisco ISE. Per risolvere il problema, passare a Administration > System > Certificates > Certificate Management > Certificate Signing Request e generarne uno per l'opzione ISE Root CA.

Informazioni correlate

- [ISE 2.7 Gestire le impostazioni di Certificati e Archivio certificati](#)
- [Implementazione dei certificati digitali in ISE](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).