

Configuration des certificats TLS/SSL dans ISE

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Certificats de serveur](#)

[Certificats ISE](#)

[Certificats système](#)

[Magasin de certificats approuvés](#)

[Tâches de base](#)

[Générer un certificat auto-signé](#)

[Renouveler un certificat auto-signé](#)

[Installer un certificat sécurisé](#)

[Installer un certificat signé par une autorité de certification](#)

[Certificats de sauvegarde et clés privées](#)

[Dépannage](#)

[Vérifier la validité du certificat](#)

[Supprimer un certificat](#)

[Le demandeur n'approuve pas le certificat du serveur ISE sur une authentification 802.1x](#)

[La chaîne de certificats ISE est correcte, mais le terminal rejette le certificat du serveur ISE pendant l'authentification](#)

[Forum aux questions](#)

[Que faire lorsque ISE émet un avertissement indiquant que le certificat existe déjà ?](#)

[Pourquoi le navigateur émet-il un avertissement indiquant que la page du portail d'ISE est présentée par un serveur non approuvé ?](#)

[Que faire lorsqu'une mise à niveau échoue en raison de certificats non valides ?](#)

[Informations connexes](#)

Introduction

Ce document décrit les certificats TLS/SSL dans Cisco ISE, les types et les rôles des certificats ISE, comment effectuer des tâches et des dépannages courants et répond aux questions fréquentes.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

1. Cisco Identity Services Engine (ISE)
2. Terminologie utilisée pour décrire les différents types de déploiements ISE et AAA.

3. Protocole RADIUS et notions de base AAA
4. Certificats SSL/TLS et x509
5. Notions de base sur les infrastructures à clé publique (PKI)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles et matérielles de Cisco ISE, versions 2.4 à 2.7. Il couvre ISE de la version 2.4 à la version 2.7, mais il doit être similaire ou identique aux autres versions du logiciel ISE 2.x, sauf indication contraire.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Certificats de serveur

Les certificats de serveur sont utilisés par les serveurs pour présenter l'identité du serveur aux clients pour en assurer l'authenticité et pour fournir un canal sécurisé pour la communication. Ils peuvent être auto-signés (lorsque le serveur émet le certificat pour lui-même) ou émis par une autorité de certification (interne à une organisation ou provenant d'un fournisseur bien connu).

Les certificats de serveur sont généralement délivrés aux noms d'hôtes ou au nom de domaine complet (FQDN) du serveur, ou ils peuvent également être un certificat générique (*.domain.com). Le ou les hôtes, le domaine ou le ou les sous-domaines auxquels il est attribué sont généralement mentionnés dans les champs Common Name (CN) ou Subject Alternative Name (SAN).

Les certificats génériques sont des certificats SSL qui utilisent une notation générique (un astérisque à la place du nom d'hôte) et permettent ainsi de partager le même certificat entre plusieurs hôtes d'une organisation. Par exemple, la valeur CN ou SAN d'un certificat générique Nom de l'objet peut ressembler à *.company.com et peut être utilisé pour sécuriser tous les hôtes de ce domaine, tels que server1.com, server2.com, etc.

Les certificats utilisent généralement le chiffrement à clé publique ou le chiffrement asymétrique.

- **Public Key (Clé publique)** : la clé publique est présente dans le certificat dans l'un des champs et est partagée publiquement par un système lorsqu'un périphérique tente de communiquer avec lui.
- **Private Key (Clé privée)** : la clé privée est privée au système d'extrémité et est associée à la clé publique. Les données chiffrées par une clé publique ne peuvent être déchiffrées que par la clé privée spécifique appariée et vice versa.

Certificats ISE

Cisco ISE s'appuie sur l'infrastructure à clé publique (PKI) pour assurer une communication sécurisée avec les terminaux, les utilisateurs, les administrateurs, etc., ainsi qu'entre les nœuds

Cisco ISE dans un déploiement multinoeud. L'ICP s'appuie sur les certificats numériques x.509 pour transférer les clés publiques de chiffrement et de déchiffrement des messages et pour vérifier l'authenticité des autres certificats présentés par les utilisateurs et les périphériques. Cisco ISE comporte deux catégories de certificats généralement utilisées :

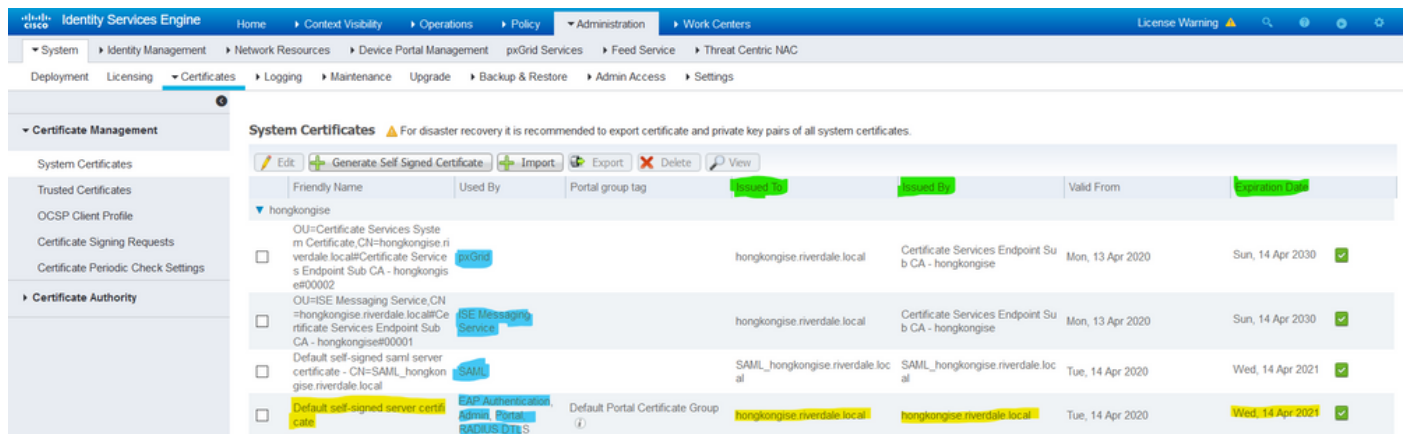
- Certificats système : il s'agit de certificats de serveur qui identifient un noeud Cisco ISE aux clients. Chaque noeud Cisco ISE possède ses propres certificats locaux, chacun d'entre eux étant stocké sur le noeud avec la clé privée correspondante.
- Certificats de magasin de certificats approuvés : il s'agit de certificats d'autorité de certification (CA) utilisés pour valider les certificats présentés à l'ISE à diverses fins. Ces certificats dans le magasin de certificats sont gérés sur le noeud d'administration principale et sont répliqués sur tous les autres noeuds dans un déploiement Cisco ISE distribué. Le magasin de certificats contient également des certificats qui sont générés pour les noeuds ISE par l'autorité de certification interne d'ISE destinée au BYOD.

Certificats système

Les certificats système peuvent être utilisés pour un ou plusieurs rôles. Chaque rôle sert un objectif différent et est expliqué ici :

- Admin : permet de sécuriser toutes les communications sur 443 (interface utilisateur graphique Admin), ainsi que la réplication, et pour tout port/utilisation non répertorié ici.
- Portal : permet de sécuriser la communication HTTP sur des portails tels que le portail CWA (Centralized Web Authentication), les portails Guest, BYOD, Client Provisioning, Native Supplicant Provisioning, etc. Chaque portail doit être mappé à une balise de groupe de portail (par défaut, il s'agit de la balise de groupe de portail par défaut) qui indique au portail le certificat spécifiquement balisé à utiliser. Le menu déroulant Nom de la balise du groupe de portails dans les options Modifier du certificat vous permet de créer une nouvelle balise ou de choisir une balise existante.
- EAP : il s'agit d'un rôle qui spécifie le certificat présenté aux clients pour l'authentification 802.1x. Les certificats sont utilisés avec presque toutes les méthodes EAP possibles telles que EAP-TLS, PEAP, EAP-FAST, etc. Avec les méthodes EAP par tunnel telles que PEAP et FAST, la sécurité de la couche transport (TLS) est utilisée pour sécuriser l'échange d'informations d'identification. Les informations d'identification du client ne sont envoyées au serveur qu'après l'établissement de ce tunnel afin de garantir un échange sécurisé.
- RADIUS DTLS : ce rôle spécifie le certificat à utiliser pour une connexion DTLS (connexion TLS sur UDP) pour chiffrer le trafic RADIUS entre un périphérique d'accès réseau (NAD) et l'ISE. NAD doit être compatible avec le cryptage DTLS pour que cette fonctionnalité fonctionne.
- SAML : le certificat du serveur est utilisé pour sécuriser la communication avec le fournisseur d'identité SAML (IdP). Un certificat désigné pour une utilisation SAML ne peut pas être utilisé pour un autre service tel que l'administration, l'authentification EAP, etc.
- Service de messagerie ISE : depuis la version 2.6, ISE utilise le service de messagerie ISE au lieu du protocole Syslog hérité pour consigner les données. Elle est utilisée pour chiffrer cette communication.
- PxGrid : ce certificat est utilisé pour les services PxGrid sur ISE.

Lorsqu'ISE est installé, il génère un Default Self-Signed Server Certificate. Il est attribué par défaut à l'authentification EAP, à l'administration, au portail et à RADIUS DTLS. Il est recommandé de déplacer ces rôles vers une autorité de certification interne ou vers un certificat signé par une autorité de certification connue.



Conseil : il est conseillé de s'assurer que les adresses FQDN et IP du serveur ISE sont ajoutées au champ SAN du certificat système ISE. En général, pour garantir que l'authentification des certificats dans Cisco ISE n'est pas affectée par des différences mineures dans les fonctions de vérification pilotées par certificat, utilisez des noms d'hôte en minuscules pour tous les noeuds Cisco ISE déployés dans un réseau.

Remarque : le format d'un certificat ISE doit être PEM (Privacy Enhanced Mail) ou DER (Distinguished Encoding Rules).

Magasin de certificats approuvés

Les certificats de l'autorité de certification doivent être stockés à Administration > System > Certificates > Certificate Store et ils doivent avoir la Trust for client authentication exemple d'utilisation pour garantir qu'ISE utilise ces certificats pour valider les certificats présentés par les terminaux, les périphériques ou d'autres noeuds ISE.

System Certificates	Trusted Certificates	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
<input type="checkbox"/>	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Mon, 12 May 2025
<input type="checkbox"/>	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
<input type="checkbox"/>	Cisco ECC Root CA	Enabled	Cisco Services	01	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Fri, 4 Apr 2053
<input type="checkbox"/>	Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root CA	Cisco Licensing Root CA	Thu, 30 May 2013	Sun, 30 May 2038
<input type="checkbox"/>	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA ...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037
<input type="checkbox"/>	Cisco RXC-R2	Enabled	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034
<input type="checkbox"/>	Default self-signed server certificate	Enabled	Endpoints Infrastructure	5E 95 93 55 00 00 ...	hongkongise.verdale.local	hongkongise.verdale.local	Tue, 14 Apr 2020	Wed, 14 Apr 2021
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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 2006	Thu, 30 Sep 2021
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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

Tâches de base

Le certificat a une date d'expiration et peut être révoqué ou être remplacé à un moment donné. Si le certificat du serveur ISE expire, des problèmes graves peuvent survenir, sauf s'ils sont remplacés par un nouveau certificat valide.

Remarque : si le certificat utilisé pour le protocole EAP (Extensible Authentication Protocol) expire, les authentifications des clients peuvent échouer car le client ne fait plus confiance au certificat ISE. Si un certificat utilisé pour les portails expire, les clients et les navigateurs peuvent refuser de se connecter au portail. Si le certificat d'utilisation Admin expire, le risque est encore plus grand, ce qui empêche un administrateur de se connecter à l'ISE et le déploiement distribué peut cesser de fonctionner comme il le doit.

Générer un certificat auto-signé

Pour générer de nouveaux certificats auto-signés, accédez à Administration > System > Certificates > System Certificates. Cliquez sur le bouton 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
<input type="checkbox"/> hongkongise OU=Certificate Services System Certificate,CN=hongkongise.verdale.local#Certificate Services Endpoint Sub CA - hongkongise#000002	pxGrid		hongkongise

Cette liste décrit les champs de la page Générer un certificat auto-signé.

Paramètres du certificat auto-signé Nom du champ Instructions d'utilisation :

- Select Node : (Obligatoire) noeud pour lequel il est nécessaire de générer le certificat système.
- CN : (obligatoire si SAN n'est pas spécifié) Par défaut, le CN est le nom de domaine complet du noeud ISE pour lequel le certificat auto-signé est généré.
- Unité organisationnelle (OU) : nom de l'unité organisationnelle, par exemple, Ingénierie.
- Organisation (O) : nom de l'organisation, par exemple, Cisco.
- Ville (L) : (Ne pas abréger) Nom de la ville, par exemple, San Jose.
- État (ST) : (Ne pas abréger) nom de l'État, par exemple, Californie.
- Pays (C) : nom du pays. Le code pays ISO à deux lettres est nécessaire. Par exemple, les États-Unis.
- SAN : adresse IP, nom DNS ou URI (Uniform Resource Identifier) associé au certificat.
- Key Type : spécifiez l'algorithme à utiliser pour créer la clé publique : RSA ou ECDSA.
- Key Length : spécifiez la taille de bit de la clé publique. Ces options sont disponibles pour RSA : 512 1024 2048 4096 et ces options sont disponibles pour ECDSA : 256 384.
- Digest to Sign With : choisissez l'un de ces algorithmes de hachage : SHA-1 ou SHA-256.
- Certificate Policies : saisissez l'OID de la stratégie de certificat ou la liste des OID auxquels le certificat doit se conformer. Utilisez des virgules ou des espaces pour séparer les OID.
- Expiration TTL : spécifiez le nombre de jours après lesquels le certificat expire.
- Friendly Name : saisissez un nom convivial pour le certificat. Si aucun nom n'est spécifié, Cisco ISE crée automatiquement un nom au format `where` est un numéro unique à cinq chiffres.
- Allow Wildcard Certificates : cochez cette case afin de générer un certificat générique auto-signé (un certificat qui contient un astérisque (*) dans n'importe quel CN dans l'objet et/ou le nom DNS dans le SAN. Par exemple, le nom DNS attribué au SAN peut être `*.domain.com`).
- Utilisation : sélectionnez le service pour lequel ce certificat système doit être utilisé. Les options disponibles sont les suivantes :
AdminAuthentification EAPRADIUS DTLSpxGridSAMLPortail



Certificate Management

System Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Settings

Certificate Authority

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) - +

* 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) IP Address 10.127.196.248

* Key type RSA

* Key Length 2048

* Digest to Sign With SHA-256

Certificate Policies

* Expiration TTL 10 years

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

Submit Cancel

Remarque : les clés publiques RSA et ECDSA peuvent avoir des longueurs de clé différentes pour le même niveau de sécurité. Choisissez 2048 si l'intention est d'obtenir un certificat public signé par une autorité de certification ou de déployer Cisco ISE en tant que système de gestion des politiques conforme à la norme FIPS.

Renouveler un certificat auto-signé

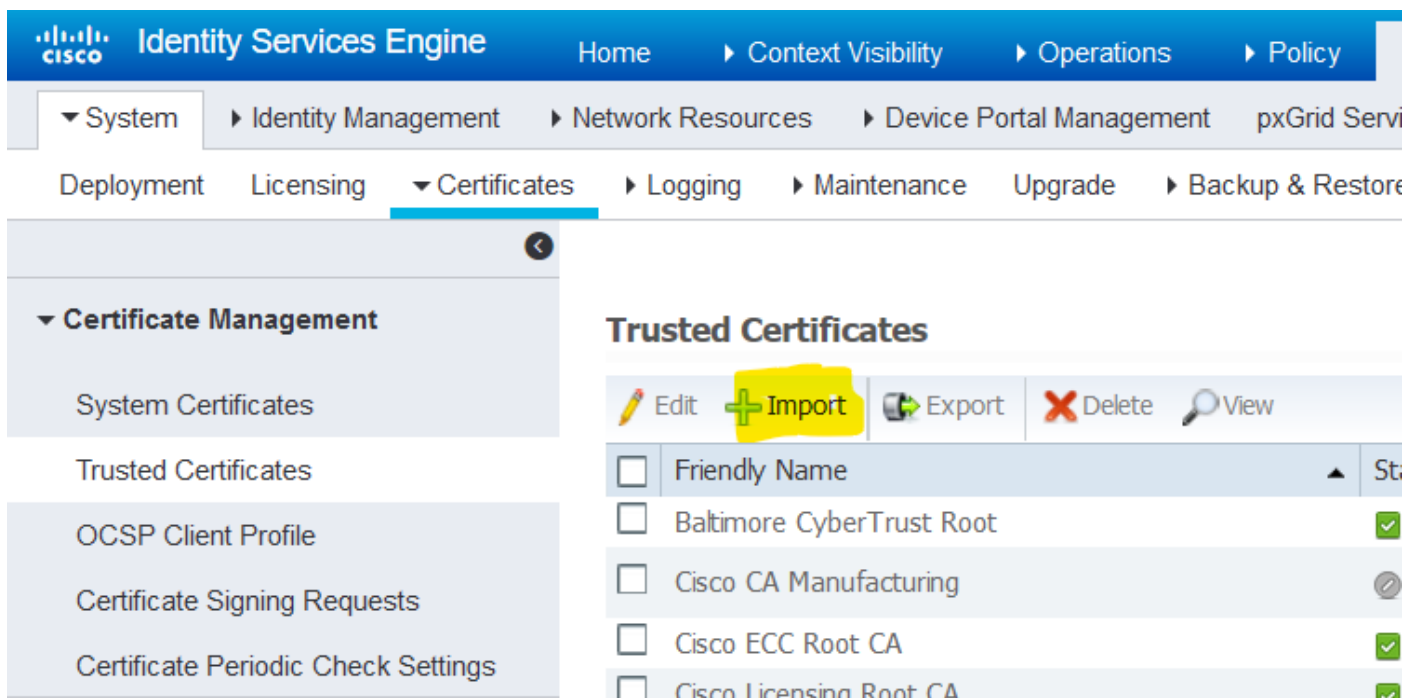
Pour afficher les certificats auto-signés existants, accédez à Administration > System > Certificates > System Certificates dans la console ISE. Tout certificat avec les valeurs « Issued To » et « Issued By » s'il est mentionné dans le même nom de domaine complet du serveur ISE, il s'agit d'un certificat auto-signé. Sélectionnez ce certificat, puis cliquez sur **Edit**.

Sous **Renew Self Signed Certificate**, cochez la case **Renewal Period** et définissez la durée de vie d'expiration, le cas échéant. Enfin, cliquez sur **Save**.

Installer un certificat sécurisé

Obtenez le ou les certificats codés en Base 64 auprès de l'autorité de certification racine, des autorités de certification intermédiaires et/ou des hôtes devant être approuvés.

1. Connectez-vous au noeud ISE et accédez à Administration > System > Certificate > Certificate Management > Trusted Certificates et cliquez sur Import, comme le montre cette image.

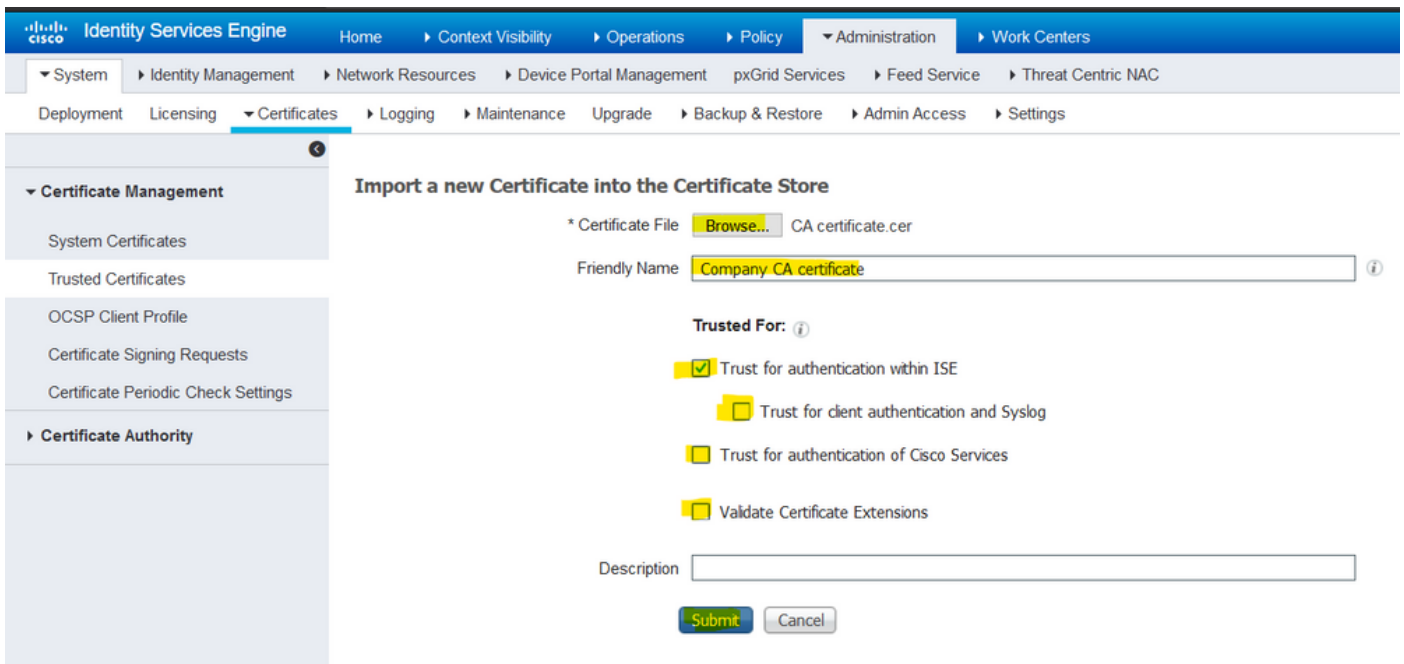


2. Sur la page suivante, téléchargez le ou les certificats d'autorité de certification obtenus (dans le même ordre que celui décrit précédemment). Attribuez-leur un nom convivial et une description qui explique à quoi sert le certificat afin d'en assurer le suivi.

En fonction des besoins d'utilisation, cochez les cases en regard de :

- Approbation de l'authentification au sein d'ISE : cette option permet d'ajouter de nouveaux noeuds ISE lorsque le même certificat d'autorité de certification approuvée est chargé dans leur magasin de certificats approuvés.
- Trust for client authentication and Syslog : activez cette option afin d'utiliser le certificat pour authentifier les terminaux qui se connectent à ISE avec des serveurs EAP et/ou Secure Syslog.
- Confiance pour l'authentification des services Cisco : cette option est nécessaire uniquement pour faire confiance aux services Cisco externes, tels qu'un service de flux.

3. Enfin, cliquez sur Submit. À présent, le certificat doit être visible dans le magasin approuvé et synchronisé avec tous les noeuds ISE secondaires (s'il est dans un déploiement).



Installer un certificat signé par une autorité de certification

Une fois les certificats d'autorité de certification racine et intermédiaire ajoutés au magasin de certificats de confiance, une demande de signature de certificat (CSR) peut être émise et le certificat signé sur la base de la demande de signature de certificat peut être lié au nœud ISE.

1. Pour ce faire, accédez à Administration > System > Certificates > Certificate Signing Requests et cliquez sur **Generate Certificate Signing Requests (CSR)** pour générer un CSR.

2. Sur la page qui s'affiche, sous la section Utilisation, choisissez le rôle à utiliser dans le menu déroulant.

Si le certificat est utilisé pour plusieurs rôles, sélectionnez Multi-Use. Une fois le certificat généré, les rôles peuvent être modifiés si nécessaire. Dans la plupart des cas, le certificat peut être défini pour être utilisé pour plusieurs utilisations dans la liste déroulante Utilisé pour ; cela permet au certificat d'être utilisable pour tous les portails Web ISE.

3. Cochez la case en regard du ou des nœuds ISE pour choisir le ou les nœuds pour lesquels le certificat est généré.

4. Si l'objectif est d'installer/de générer un certificat générique, vérifiez la **Allow Wildcard Certificates**, sélectionnez une option.

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. Complétez les informations sur le sujet en fonction des détails sur l'hôte ou l'organisation (Unité organisationnelle, Organisation, Ville, État et Pays).

6. Afin de terminer ceci, cliquez sur **Generate**, puis cliquez sur **Export** dans la fenêtre contextuelle qui s'affiche.

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

La demande de certificat codée en base 64 qui vient d'être créée est téléchargée. Ce fichier PEM doit être envoyé à l'autorité de certification pour signature et obtenir le fichier CER de certificat signé résultant (codé en base 64).

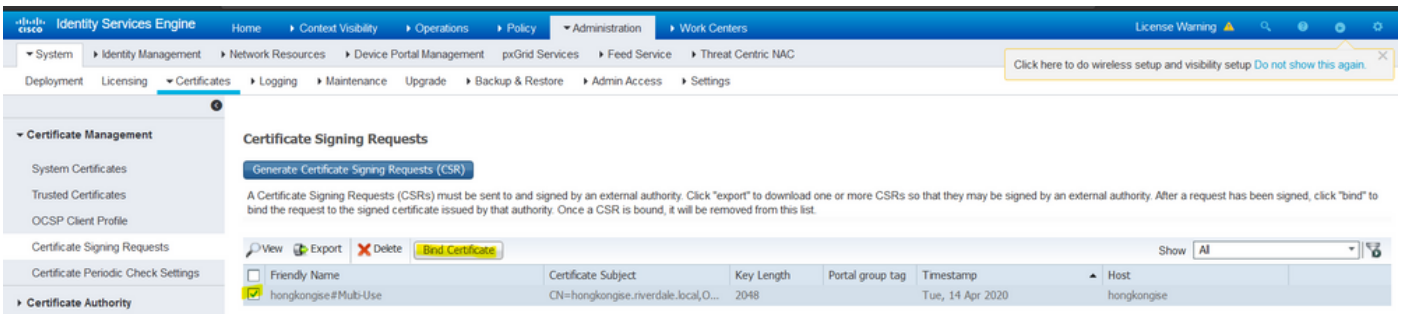
Remarque : sous le champ CN, ISE renseigne automatiquement le nom de domaine complet des noeuds.

Remarque : dans ISE 1.3 et 1.4, il était nécessaire d'émettre deux CSR au moins pour utiliser pxGrid. L'un est dédié à pxGrid et l'autre, au reste des services. Depuis la version 2.0

et les versions ultérieures, tout cela repose sur un seul CSR.

Remarque : si le certificat est utilisé pour les authentifications EAP, le symbole « * » ne doit pas figurer dans le champ Objet CN, car les demandeurs Windows rejettent le certificat du serveur. Même lorsque la fonction Valider l'identité du serveur est désactivée sur le demandeur, la connexion SSL peut échouer lorsque le signe * est dans le champ CN. À la place, un nom de domaine complet générique peut être utilisé dans le champ CN, puis *.domain.com peut être utilisé dans le champ SAN DNS Name. Certaines autorités de certification (AC) peuvent ajouter automatiquement le caractère générique (*) dans le CN du certificat même s'il n'est pas présent dans le CSR. Dans ce scénario, une demande spéciale doit être émise pour empêcher cette action.

7. Une fois que le certificat a été signé par l'autorité de certification (qui a été généré à partir du CSR, comme indiqué dans la vidéo, [ici](#) si l'autorité de certification Microsoft est utilisée), revenez à l'interface utilisateur graphique d'ISE, et naviguez vers **Administration > Système > Certificats > Gestion des certificats > Demande de signature de certificat** ; Cochez la case en regard du CSR précédemment créé, et cliquez sur le bouton **Lier certificat**.



8. Ensuite, téléchargez le certificat signé qui vient d'être reçu et donnez-lui un nom convivial pour ISE. Ensuite, sélectionnez les cases en regard des utilisations en fonction des besoins pour le certificat (comme Admin et authentification EAP, Portal, etc.) et cliquez sur Submit, comme le montre cette image :

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)

Si le rôle Admin a été choisi pour ce certificat, le noeud ISE doit redémarrer ses services. En fonction de la version et des ressources allouées à la machine virtuelle, cette opération peut prendre de 10 à 15 minutes. Afin de vérifier l'état de l'application, ouvrez la ligne de commande ISE et émettez le `show application status ise erasecat4000_flash:`.

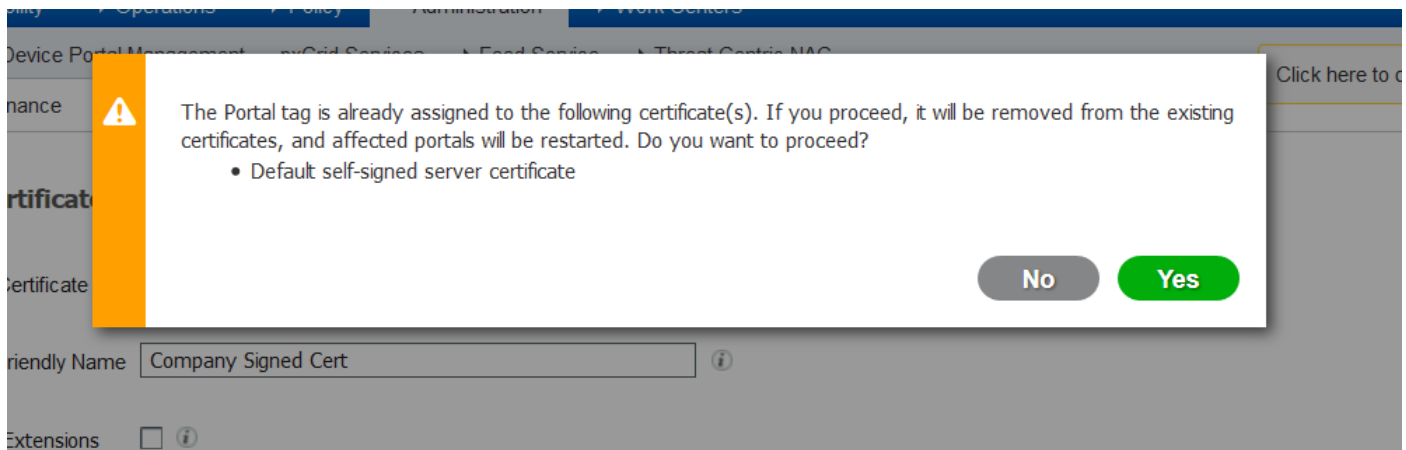
Warning dialog box:

! 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 ⓘ



Si le rôle admin ou portail a été choisi lors de l'importation du certificat, vous pouvez vérifier que le nouveau certificat est en place lors de l'accès aux pages admin ou portail du navigateur. Choisissez le symbole de verrouillage dans le navigateur et sous le certificat, le chemin vérifie que la chaîne complète est présente et approuvée par la machine. Le navigateur doit faire confiance au nouveau certificat d'administration ou de portail tant que la chaîne a été créée correctement et si la chaîne de certificats est approuvée par le navigateur.

Remarque : pour renouveler un certificat système signé par une autorité de certification, générez un nouveau CSR et liez-lui le certificat signé avec les mêmes options. Puisqu'il est possible d'installer un nouveau certificat sur l'ISE avant qu'il ne soit actif, prévoyez d'installer le nouveau certificat avant que l'ancien n'expire. Cette période de chevauchement entre l'ancienne date d'expiration du certificat et la nouvelle date de début du certificat donne le temps de renouveler les certificats et de planifier leur remplacement avec peu ou pas de temps d'arrêt. Obtenez un nouveau certificat dont la date de début précède la date d'expiration de l'ancien certificat. La période comprise entre ces deux dates représente la fenêtre de modification. Une fois que le nouveau certificat entre sa plage de dates valide, activez les protocoles requis (Admin/EAP/Portal). N'oubliez pas que si l'utilisation Admin est activée, le service redémarre.

Conseil : il est recommandé d'utiliser l'autorité de certification interne de la société pour les certificats Admin et EAP, ainsi qu'un certificat signé publiquement pour les portails Guest/Sponsor/Hotspot/etc. La raison en est que si un utilisateur ou un invité arrive sur le réseau et que le portail ISE utilise un certificat signé de manière privée pour le portail invité, il obtient des erreurs de certificat ou peut-être que son navigateur les bloque à partir de la page du portail. Pour éviter tout cela, utilisez un certificat signé publiquement pour l'utilisation du portail afin d'assurer une meilleure expérience utilisateur. En outre, chaque adresse IP de noeud de déploiement doit être ajoutée au champ SAN pour éviter un avertissement de certificat lorsque l'accès au serveur s'effectue via l'adresse IP.

Certificats de sauvegarde et clés privées

Il est recommandé d'exporter :

1. Tous les certificats système (de tous les noeuds du déploiement) ainsi que leurs clés privées (nécessaires pour les réinstaller) vers un emplacement sécurisé. Notez la configuration du certificat (le service pour lequel le certificat a été utilisé).

2. Tous les certificats du magasin de certificats approuvés du noeud d'administration principal. Notez la configuration du certificat (le service pour lequel le certificat a été utilisé).

3. Tous les certificats d'autorité de certification.

Pour ce faire,

1. Naviguez jusqu'à Administration > System > Certificates > Certificate Management > System Certificates. Sélectionnez le certificat et cliquez sur Export. Choisir Export Certificates et les clés privées. Saisissez le mot de passe de la clé privée et confirmez le mot de passe. Cliquez Export.
2. Naviguez jusqu'à Administration > System > Certificates > Certificate Management > Trusted Certificates. Sélectionnez le certificat et cliquez sur Export. Cliquez Save File pour exporter le certificat.
3. Naviguez jusqu'à Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates. Sélectionnez le certificat et cliquez sur Export. Choisir Export Certificates et les clés privées. Saisissez le mot de passe de la clé privée et confirmez le mot de passe. Cliquez Export. Cliquez Save File pour exporter le certificat.

Dépannage

Vérifier la validité du certificat

Le processus de mise à niveau échoue si un certificat du magasin de certificats de confiance Cisco ISE ou de certificats système a expiré. Assurez-vous de vérifier la validité dans le champ Date d'expiration des fenêtres Certificats approuvés et Certificats système (Administration > System > Certificates > Certificate Management), et les renouveler, si nécessaire, avant la mise à niveau.

Vérifiez également la validité dans le champ Date d'expiration des certificats de la fenêtre Certificats de l'autorité de certification (Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates), et les renouveler, si nécessaire, avant la mise à niveau.

Supprimer un certificat

Si un certificat de l'ISE a expiré ou n'est pas utilisé, il doit être supprimé. Veillez à ce que les certificats soient exportés (avec leurs clés privées, le cas échéant) avant la suppression.

Afin de supprimer un certificat expiré, accédez à Administration > System > Certificates > Certificate Management. Cliquez sur le bouton System Certificates Store. Sélectionnez le ou les certificats expirés et cliquez sur Delete.

Référez-vous à la même section pour les magasins Certificats de confiance et Certificats d'autorité de certification.

Le demandeur n'approuve pas le certificat du serveur ISE sur une authentification 802.1x

Vérifiez si ISE envoie la chaîne de certificats complète pour le processus de connexion SSL.

Avec les méthodes EAP qui nécessitent un certificat de serveur (c'est-à-dire, PEAP) et que l'option Valider l'identité du serveur est sélectionnée dans les paramètres du système

d'exploitation client, le demandeur valide la chaîne de certificats avec les certificats qu'il possède dans son magasin de confiance local dans le cadre du processus d'authentification. Dans le cadre du processus d'échange SSL, ISE présente son certificat ainsi que tous les certificats racine et/ou intermédiaires présents dans sa chaîne. Le demandeur ne peut pas valider l'identité du serveur si la chaîne est incomplète ou si cette chaîne est absente de son magasin approuvé.

Afin de vérifier que la chaîne de certificats est renvoyée au client, effectuez une capture de paquets à partir d'ISE (Operations > Diagnostic Tools > General Tools > TCP Dump) ou une capture Wireshark sur le terminal au moment de l'authentification. Ouvrez la capture et appliquez le filtre `ssl.handshake.certificates` dans Wireshark et recherchez un défi d'accès.

Une fois sélectionné, accédez à `Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates`.

Si la chaîne est incomplète, accédez à ISE `Administration > Certificates > Trusted Certificates` et vérifiez que les certificats racine et/ou intermédiaire sont présents. Si la chaîne de certificats est passée avec succès, la chaîne elle-même doit être vérifiée comme étant valide selon la méthode décrite ici.

Ouvrez chaque certificat (serveur, intermédiaire et racine) et vérifiez la chaîne de confiance pour faire correspondre l'identificateur de clé de sujet (SKI) de chaque certificat à l'identificateur de clé d'autorité (AKI) du certificat suivant dans la chaîne.

La chaîne de certificats ISE est correcte, mais le terminal rejette le certificat du serveur ISE pendant l'authentification

Si ISE présente sa chaîne de certificats complète pour la connexion SSL et que le demandeur a toujours rejeté la chaîne de certificats, l'étape suivante consiste à vérifier que les certificats racine et/ou intermédiaire se trouvent dans le magasin local d'approbations des clients.

Afin de vérifier cela à partir d'un périphérique Windows, lancez `mmc.exe` (Microsoft Management Console), accédez à `File > Add-Remove Snap-in`. Dans la colonne Composants logiciels enfichables disponibles, sélectionnez `Certificates` et cliquez sur `Add`. Choisissez : `My user account` OU `Computer account` en fonction du type d'authentification utilisé (Utilisateur ou Ordinateur), puis cliquez sur `OK`.

Dans la vue de la console, sélectionnez `Autorités de certification racines de confiance` et `Autorités de certification intermédiaires` pour vérifier la présence de certificats racines et intermédiaires dans le magasin d'approbations local.

Pour vérifier facilement qu'il s'agit d'un problème lié à la vérification de l'identité du serveur, désactivez la case à cocher `Valider le certificat du serveur` dans la configuration du profil du demandeur et testez-la à nouveau.

Forum aux questions

Que faire lorsque ISE émet un avertissement indiquant que le certificat existe déjà ?

Ce message signifie qu'ISE a détecté un certificat système avec le même paramètre d'unité d'organisation et qu'un certificat dupliqué a été tenté d'installer. Étant donné que le certificat système en double n'est pas pris en charge, il est conseillé de modifier simplement n'importe laquelle des valeurs `Ville/État/Service` à une valeur légèrement différente pour s'assurer que le

nouveau certificat est différent.

Pourquoi le navigateur émet-il un avertissement indiquant que la page du portail d'ISE est présentée par un serveur non approuvé ?

Cela se produit lorsque le navigateur n'approuve pas le certificat d'identité du serveur.

Tout d'abord, assurez-vous que le certificat de portail visible sur le navigateur correspond à ce qui était attendu et avait été configuré sur ISE pour le portail.

Ensuite, assurez-vous d'accéder au portail via le nom de domaine complet (FQDN). Dans le cas de l'adresse IP utilisée, assurez-vous que le nom de domaine complet (FQDN) et l'adresse IP figurent dans les champs SAN et/ou CN du certificat.

Enfin, assurez-vous que la chaîne de certificats du portail (portail ISE, CA intermédiaire, certificats CA racine) est importée sur/approuvée par le système d'exploitation/navigateur client.

Remarque : certaines versions ultérieures d'iOS, d'Android et de Chrome/Firefox ont des attentes strictes en matière de sécurité du certificat. Même si ces points sont respectés, ils peuvent refuser de se connecter si les autorités de certification Portal et Intermediate sont inférieures à SHA-256.

Que faire lorsqu'une mise à niveau échoue en raison de certificats non valides ?

Le processus de mise à niveau échoue si un certificat du magasin de certificats de confiance Cisco ISE ou de certificats système a expiré. Assurez-vous de vérifier la validité dans le champ Date d'expiration des fenêtres Certificats approuvés et Certificats système (Administration > System > Certificates > Certificate Management), et les renouveler, si nécessaire, avant la mise à niveau.

Vérifiez également la validité dans le champ Date d'expiration des certificats de la fenêtre Certificats de l'autorité de certification (Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates), et les renouveler, si nécessaire, avant la mise à niveau.

Avant la mise à niveau ISE, assurez-vous que la chaîne de certificats CA interne est valide.

Naviguez jusqu'à Administration > System > Certificates > Certificate Authority Certificates. Pour chaque noeud du déploiement, sélectionnez le certificat avec l'autorité de certification secondaire du point de terminaison des services de certificats dans la colonne Nom convivial. Cliquez sur View et vérifiez si l'état du certificat est un bon message et s'il est visible.

Si une chaîne de certificats est rompue, assurez-vous de résoudre le problème avant le début du processus de mise à niveau de Cisco ISE. Pour résoudre le problème, accédez à Administration > System > Certificates > Certificate Management > Certificate Signing Request et générez-en une pour l'option d'autorité de certification racine ISE.

Informations connexes

- [ISE 2.7 Gestion des certificats et paramètres du magasin de certificats](#)
- [Implémenter des certificats numériques dans ISE](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.