

Konfigurieren von TLS/SSL-Zertifikaten in der ISE

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Serverzertifikate](#)

[ISE-Zertifikate](#)

[Systemzertifikate](#)

[Speicher für vertrauenswürdige Zertifikate](#)

[Grundlegende Aufgaben](#)

[Generieren eines selbstsignierten Zertifikats](#)

[Erneuern eines selbstsignierten Zertifikats](#)

[Installieren eines vertrauenswürdigen Zertifikats](#)

[Installieren eines von der Zertifizierungsstelle signierten Zertifikats](#)

[Sicherungszertifikate und private Schlüssel](#)

[Fehlerbehebung](#)

[Gültigkeit des Zertifikats überprüfen](#)

[Löschen eines Zertifikats](#)

[Der Supplicant vertraut dem ISE-Serverzertifikat bei einer 802.1x-Authentifizierung nicht.](#)

[ISE-Zertifikatkette ist korrekt, aber Endpunkt lehnt ISE-Serverzertifikat während der Authentifizierung ab](#)

[Häufig gestellte Fragen](#)

[Was zu tun ist, wenn die ISE eine Warnung ausgibt, dass das Zertifikat bereits vorhanden ist?](#)

[Warum gibt der Browser eine Warnung aus, dass die Portalseite der ISE von einem nicht vertrauenswürdigen Server dargestellt wird?](#)

[Was tun, wenn ein Upgrade aufgrund ungültiger Zertifikate fehlschlägt?](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt TLS/SSL-Zertifikate in der Cisco ISE, die Arten und Rollen von ISE-Zertifikaten, die Durchführung allgemeiner Aufgaben und die Fehlerbehebung sowie die Beantwortung häufig gestellter Fragen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

1. Cisco Identity Services Engine (ISE)

2. Die Terminologie, die zur Beschreibung verschiedener Arten von ISE- und AAA-Bereitstellungen verwendet wird.
3. RADIUS-Protokoll und AAA-Grundlagen
4. SSL/TLS- und x509-Zertifikate
5. PKI-Grundlagen (Public Key Infrastructure)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco ISE, Versionen 2.4 - 2.7, Software- und Hardwareversionen. Sie deckt ISE von Version 2.4 bis 2.7 ab, muss jedoch ähnlich oder identisch mit anderen ISE 2.x-Softwareversionen sein, sofern nichts anderes angegeben ist.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Serverzertifikate

Serverzertifikate werden von Servern verwendet, um den Clients die Identität des Servers für die Authentizität anzuzeigen und einen sicheren Kommunikationskanal bereitzustellen. Diese können selbst signiert sein (wenn der Server das Zertifikat selbst ausstellt) oder von einer Zertifizierungsstelle ausgestellt werden (entweder unternehmensintern oder von einem bekannten Anbieter).

Serverzertifikate werden in der Regel für Hostnamen oder FQDN (Fully Qualified Domain Name) des Servers ausgestellt oder können auch ein Platzhalterzertifikat sein (*.domain.com). Die Hosts, Domänen oder Subdomänen, für die sie ausgestellt werden, werden in der Regel in den Feldern "Common Name (CN)" (Gemeinsamer Name) oder "Subject Alternative Name (SAN)" (Alternativer Antragstellername) aufgeführt.

Platzhalterzertifikate sind SSL-Zertifikate, die die Platzhalternotation (ein Sternchen anstelle des Hostnamens) verwenden und somit die gemeinsame Nutzung desselben Zertifikats auf mehreren Hosts in einer Organisation ermöglichen. Beispiel: Der CN- oder SAN-Wert für ein Platzhalterzertifikat Der Antragstellername kann ähnlich aussehen wie *.company.com und zum Sichern aller Hosts dieser Domäne verwendet werden kann, z. B. server1.com, server2.com und so weiter.

Zertifikate verwenden normalerweise Public-Key-Verschlüsselung oder asymmetrische Verschlüsselung.

- Öffentlicher Schlüssel: Der öffentliche Schlüssel befindet sich im Zertifikat in einem der Felder und wird von einem System öffentlich freigegeben, wenn ein Gerät versucht, mit ihm zu kommunizieren.
- Privater Schlüssel: Der private Schlüssel ist für das Endsystem privat und wird mit dem öffentlichen Schlüssel gepaart. Durch einen öffentlichen Schlüssel verschlüsselte Daten können nur durch den jeweiligen gepaarten privaten Schlüssel entschlüsselt werden und umgekehrt.

ISE-Zertifikate

Die Cisco ISE bietet mit der Public Key Infrastructure (PKI) eine sichere Kommunikation mit Endgeräten, Benutzern, Administratoren usw. sowie zwischen Cisco ISE-Knoten in einer Bereitstellung mit mehreren Knoten. PKI verwendet digitale x.509-Zertifikate, um öffentliche Schlüssel für die Ver- und Entschlüsselung von Nachrichten zu übertragen und die Authentizität anderer Zertifikate zu überprüfen, die von Benutzern und Geräten präsentiert werden. Die Cisco ISE verwendet in der Regel zwei Zertifikatskategorien:

- **Systemzertifikate:** Dies sind Serverzertifikate, die einen Cisco ISE-Knoten für Clients identifizieren. Jeder Cisco ISE-Knoten verfügt über eigene lokale Zertifikate, die jeweils zusammen mit dem entsprechenden privaten Schlüssel auf dem Knoten gespeichert werden.
- **Zertifikate für vertrauenswürdige Zertifikatspeicher:** Dies sind Zertifikate der Zertifizierungsstelle (Certificate Authority, CA), mit denen die Zertifikate validiert werden, die der ISE für verschiedene Zwecke vorgelegt werden. Diese Zertifikate im Zertifikatspeicher werden auf dem primären Administrationsknoten verwaltet und auf alle anderen Knoten in einer verteilten Cisco ISE-Bereitstellung repliziert. Der Zertifikatspeicher enthält außerdem Zertifikate, die von der internen ISE-Zertifizierungsstelle für BYOD für die ISE-Knoten generiert werden.

Systemzertifikate

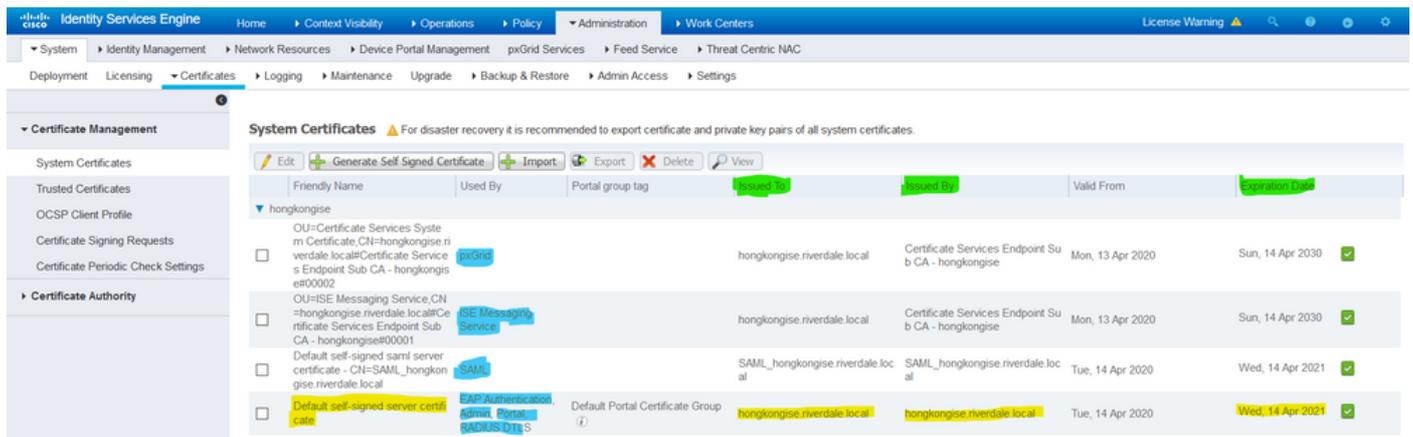
Systemzertifikate können für eine oder mehrere Rollen verwendet werden. Jede Rolle dient einem anderen Zweck und wird hier erläutert:

- **Admin:** Diese Funktion dient zum Schutz der gesamten Kommunikation über 443 (Admin-GUI) sowie für die Replikation und für alle hier nicht aufgeführten Ports/Verwendungen.
- **Portal:** Hiermit wird die HTTP-Kommunikation über Portale wie CWA-Portal (Centralized Web Authentication), Gast, BYOD, Client-Bereitstellung, Native Supplicant-Bereitstellungsportale usw. abgesichert. Jedes Portal muss einem Portal Group Tag (Standardportalgruppen-Tag) zugeordnet werden, der das Portal auf dem speziell gekennzeichneten Zertifikat anweist, verwendet zu werden. Über das Dropdown-Menü "Portal Group Tag" (Portalgruppen-Tag-Name) in den Bearbeitungsoptionen des Zertifikats können Sie ein neues Tag erstellen oder ein vorhandenes Tag auswählen.
- **EAP:** Diese Rolle gibt das Zertifikat an, das den Clients für die 802.1x-Authentifizierung bereitgestellt wird. Zertifikate werden mit fast allen möglichen EAP-Methoden wie EAP-TLS, PEAP, EAP-FAST usw. verwendet. Bei getunnelten EAP-Methoden wie PEAP und FAST wird Transport Layer Security (TLS) verwendet, um den Austausch von Anmeldeinformationen zu sichern. Die Client-Anmeldeinformationen werden erst nach Einrichtung dieses Tunnels an den Server gesendet, um einen sicheren Austausch zu gewährleisten.
- **RADIUS DTLS:** Diese Rolle gibt das Zertifikat an, das für eine DTLS-Verbindung (TLS-Verbindung über UDP) zur Verschlüsselung des RADIUS-Datenverkehrs zwischen einem Netzwerkzugriffgerät (NAD) und der ISE verwendet werden soll. Damit diese Funktion

genutzt werden kann, muss NAD DTLS-Verschlüsselung unterstützen.

- SAML: Das Serverzertifikat dient zur Sicherung der Kommunikation mit dem SAML Identity Provider (IdP). Ein für die SAML-Verwendung bestimmtes Zertifikat kann nicht für andere Dienste wie Admin, EAP-Authentifizierung usw. verwendet werden.
- ISE Messaging Service: Seit Version 2.6 verwendet die ISE ISE Messaging Service anstelle des älteren Syslog-Protokolls zur Protokollierung von Daten. Diese wird verwendet, um diese Kommunikation zu verschlüsseln.
- PxGrid: Dieses Zertifikat wird für PxGrid-Services auf der ISE verwendet.

Wenn die ISE installiert ist, generiert sie eine Default Self-Signed Server Certificate. Diese wird standardmäßig den DTLS-Formaten EAP-Authentifizierung, Admin, Portal und RADIUS zugewiesen. Es wird empfohlen, diese Rollen auf eine interne Zertifizierungsstelle oder ein bekanntes, von einer Zertifizierungsstelle signiertes Zertifikat zu verschieben.



Tipp: Es empfiehlt sich, sicherzustellen, dass sowohl der FQDN als auch die IP-Adressen des ISE-Servers dem SAN-Feld des ISE-Systemzertifikats hinzugefügt werden. Um sicherzustellen, dass die Zertifikatsauthentifizierung in der Cisco ISE nicht durch geringfügige Unterschiede bei den zertifikatbasierten Verifizierungsfunktionen beeinträchtigt wird, sollten Sie generell für alle in einem Netzwerk bereitgestellten Cisco ISE-Knoten Hostnamen in Kleinbuchstaben verwenden.

Hinweis: Das Format für ein ISE-Zertifikat muss Privacy Enhanced Mail (PEM) oder Distinguished Encoding Rules (DER) lauten.

Speicher für vertrauenswürdige Zertifikate

Zertifizierungsstellen-Zertifikate müssen gespeichert werden unter Administration > System > Certificates > Certificate Store und sie müssen über Trust for client authentication use-case, um sicherzustellen, dass die ISE diese Zertifikate verwendet, um die von den Endpunkten, Geräten oder anderen ISE-Knoten vorgelegten Zertifikate zu validieren.

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

Grundlegende Aufgaben

Das Zertifikat hat ein Ablaufdatum und kann widerrufen oder zu einem späteren Zeitpunkt ersetzt werden. Wenn das ISE-Serverzertifikat abläuft, können schwerwiegende Probleme auftreten, es sei denn, sie werden durch ein neues gültiges Zertifikat ersetzt.

Hinweis: Wenn das für das Extensible Authentication Protocol (EAP) verwendete Zertifikat abläuft, können die Clientauthentifizierungen fehlschlagen, da der Client dem ISE-Zertifikat nicht mehr vertraut. Wenn ein Zertifikat für Portale abläuft, können Clients und Browser die Verbindung mit dem Portal ablehnen. Wenn das Benutzungszertifikat des Administrators abläuft, ist das Risiko noch größer, sodass sich der Administrator nicht mehr bei der ISE anmelden kann und die verteilte Bereitstellung nicht mehr wie gewünscht funktioniert.

Generieren eines selbstsignierten Zertifikats

Um neue selbstsignierte Zertifikate zu generieren, navigieren Sie zu Administration > System > Certificates > System Certificates. Klicken Sie auf 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

Diese Liste beschreibt die Felder auf der Seite "Selbstsigniertes Zertifikat generieren".

Richtlinien für die Verwendung von Feldnamen in den Einstellungen für selbstsignierte Zertifikate:

- Knoten auswählen: (Erforderlich) Der Knoten, für den das Systemzertifikat generiert werden muss.
- CN: (Erforderlich, wenn kein SAN angegeben ist) Standardmäßig ist der CN der FQDN des ISE-Knotens, für den das selbstsignierte Zertifikat generiert wird.
- Organisationseinheit (OU): Name der Organisationseinheit, z. B. Engineering.
- Organisation (O): Name der Organisation, z. B. Cisco.
- Stadt (L): (Nicht abkürzen) Name der Stadt, z. B. San Jose.
- Bundesstaat (ST): (Nicht abkürzen) Name des Bundesstaates, z. B. Kalifornien.
- Land (C): Ländername. Der zweistellige ISO-Ländercode wird benötigt. Zum Beispiel die USA.
- SAN: Eine IP-Adresse, ein DNS-Name oder ein URI (Uniform Resource Identifier), die bzw. der mit dem Zertifikat verknüpft ist.
- Schlüsseltyp: Geben Sie den Algorithmus an, der zum Erstellen des öffentlichen Schlüssels verwendet werden soll: RSA oder ECDSA.
- Schlüssellänge: Geben Sie die Bitgröße für den öffentlichen Schlüssel an. Diese Optionen stehen für RSA zur Verfügung: 512 1024 2048 4096 und diese Optionen sind für ECDSA verfügbar: 256 384.
- Digest zum Signieren mit: Wählen Sie einen der folgenden Hashalgorithmen: SHA-1 oder SHA-256.
- Zertifikatrichtlinien: Geben Sie die OID der Zertifikatrichtlinie oder die Liste der OIDs ein, denen das Zertifikat entsprechen muss. Trennen Sie die OIDs durch Kommas oder Leerzeichen.
- Ablaufdatum (TTL): Geben Sie die Anzahl der Tage an, nach denen das Zertifikat abläuft.
- Anzeigename: Geben Sie einen Anzeigenamen für das Zertifikat ein. Wenn kein Name angegeben wird, erstellt die Cisco ISE automatisch einen Namen im Format wo ist eine eindeutige fünfstellige Zahl.
- Platzhalterzertifikate zulassen: Aktivieren Sie dieses Kontrollkästchen, um ein selbstsigniertes Platzhalterzertifikat (ein Zertifikat, das ein Sternchen (*) in einer beliebigen CN im Betreff und/oder dem DNS-Namen im SAN enthält) zu generieren. Der dem SAN zugewiesene DNS-Name kann z. B. *.domain.com.
- Syntax: Wählen Sie den Dienst aus, für den dieses Systemzertifikat verwendet werden soll. Folgende Optionen sind verfügbar:
AdministratorEAP-AuthentifizierungRADIUS-DTLSpxGridSAMLPortal



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

OCSP 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

Hinweis: Öffentliche RSA- und ECDSA-Schlüssel können für dieselbe Sicherheitsstufe unterschiedliche Schlüssellängen haben. Wählen Sie 2048, wenn Sie ein von einer öffentlichen Zertifizierungsstelle signiertes Zertifikat erhalten möchten oder die Cisco ISE als ein FIPS-konformes Richtlinienmanagementsystem bereitstellen möchten.

Erneuern eines selbstsignierten Zertifikats

Um die vorhandenen selbstsignierten Zertifikate anzuzeigen, navigieren Sie zu Administration > System > Certificates > System Certificates in der ISE-Konsole. Jedes Zertifikat mit den Bezeichnungen "Issued To" (Ausgestellt von) und "Issued By" (Ausgestellt von), das im gleichen FQDN des ISE-Servers erwähnt wird, ist ein selbstsigniertes Zertifikat. Wählen Sie dieses Zertifikat aus, und klicken Sie auf **Edit**.

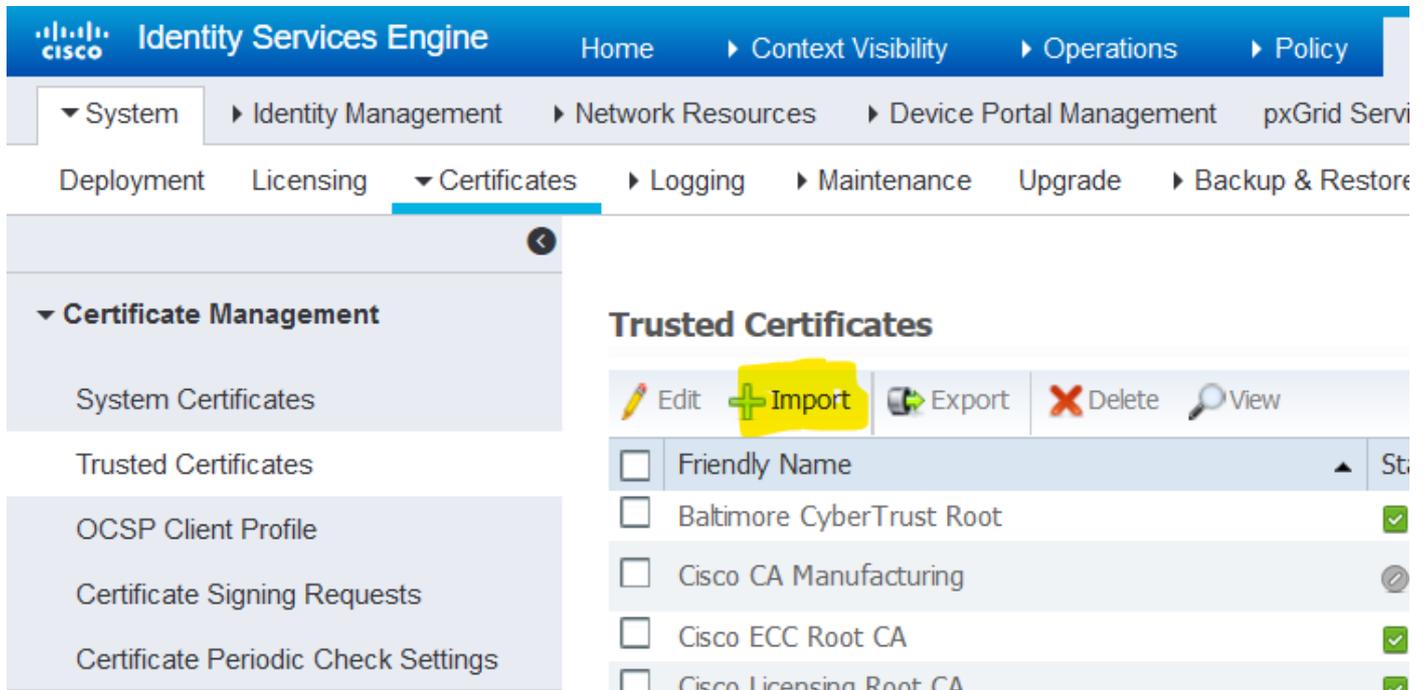
Unter **Renew Self Signed Certificate**, überprüfen Sie die **Renewal Period**, und legen Sie die Ablauf-TTL nach Bedarf fest. Klicken Sie abschließend auf **Save**.

Installieren eines vertrauenswürdigen Zertifikats

Rufen Sie das/die Base 64-codierte(n) Zertifikat/e von der Root-Zertifizierungsstelle (Root CA),

den Zwischen-Zertifizierungsstellen (Intermediate CA) und/oder den Hosts ab, die als vertrauenswürdig gelten sollen.

1. Melden Sie sich beim ISE-Knoten an, und navigieren Sie zu Administration > System > Certificate > Certificate Management > Trusted Certificates und klicke auf Import, wie in diesem Bild dargestellt.

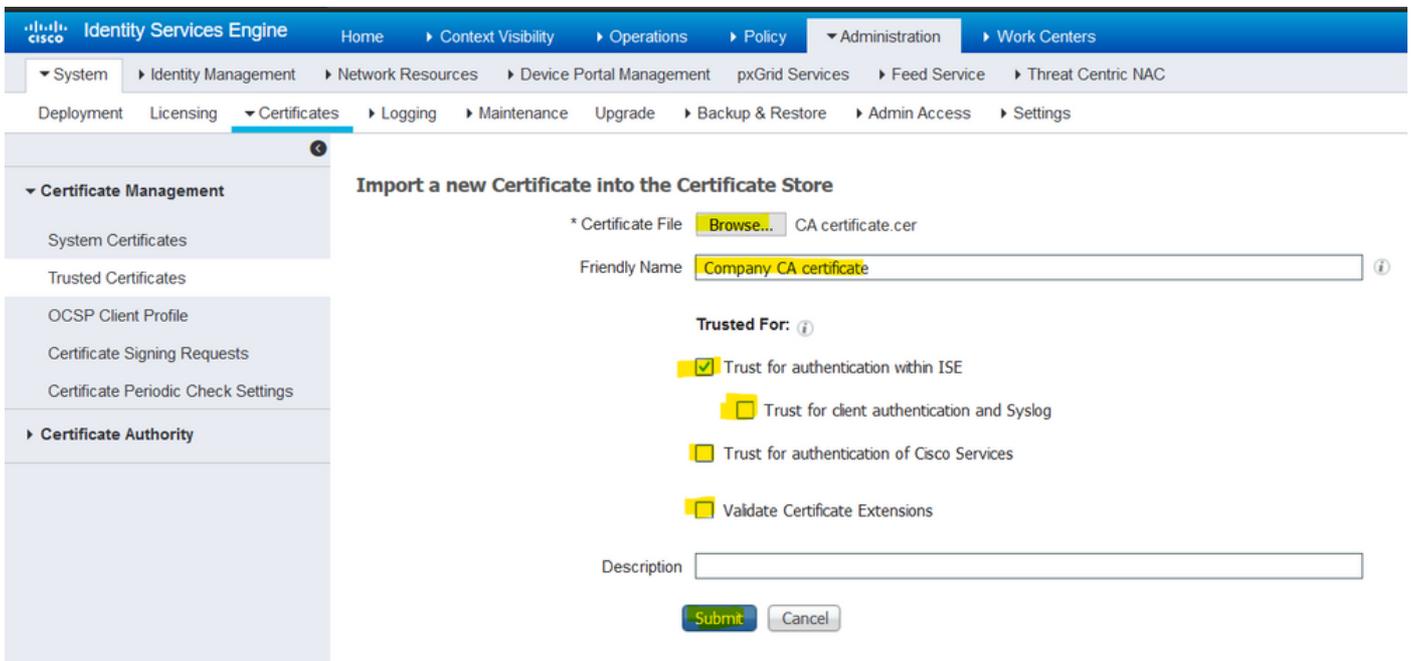


2. Laden Sie auf der nächsten Seite die erhaltenen Zertifizierungsstellenzertifikate hoch (in der gleichen Reihenfolge wie zuvor beschrieben). Weisen Sie ihnen einen Anzeigenamen und eine Beschreibung zu, in der erläutert wird, wofür das Zertifikat steht, damit sie es verfolgen können.

Aktivieren Sie je nach Verwendungszweck die Kontrollkästchen neben:

- Für die Authentifizierung innerhalb der ISE als vertrauenswürdig einstufen - Mit dieser Option werden neue ISE-Knoten hinzugefügt, wenn dasselbe vertrauenswürdige Zertifizierungsstellenzertifikat in den Speicher für vertrauenswürdige Zertifikate geladen wurde.
- Trust for client authentication and Syslog (Für Client-Authentifizierung und Syslog vertrauen): Aktivieren Sie diese Option, um das Zertifikat für die Authentifizierung von Endpunkten zu verwenden, die mit EAP eine Verbindung zur ISE herstellen, und/oder um Secure Syslog-Servern zu vertrauen.
- Für die Authentifizierung von Cisco Services als vertrauenswürdig einstufen - Dies ist nur erforderlich, um externen Cisco Services wie einem Feed-Service als vertrauenswürdig einzustufen.

3. Klicken Sie abschließend auf Submit. Nun muss das Zertifikat im Trusted Store sichtbar sein und mit allen sekundären ISE-Knoten (falls in einer Bereitstellung) synchronisiert werden.



Installieren eines von der Zertifizierungsstelle signierten Zertifikats

Nachdem die Zertifikate der Stamm- und Zwischenzertifizierungsstelle(n) dem vertrauenswürdigen Zertifikatspeicher hinzugefügt wurden, kann eine Zertifikatssignierungsanforderung (Certificate Signing Request, CSR) ausgegeben und das auf der Grundlage der CSR signierte Zertifikat an den ISE-Knoten gebunden werden.

1. Navigieren Sie dazu zu Administration > System > Certificates > Certificate Signing Requests und klicke **Generate Certificate Signing Requests (CSR)** um eine CSR-Anfrage zu erstellen.

2. Wählen Sie auf der nächsten Seite im Abschnitt "Verwendung" aus dem Dropdown-Menü die Rolle, die verwendet werden soll.

Wenn das Zertifikat für mehrere Rollen verwendet wird, wählen Sie Mehrfachverwendung. Sobald das Zertifikat generiert wurde, können die Rollen bei Bedarf geändert werden. In den meisten Fällen kann das Zertifikat im Dropdown-Menü "Used For" (Verwendet für) so eingestellt werden, dass es für mehrere Verwendungen verwendet wird. Dadurch kann das Zertifikat für alle ISE-Webportale verwendet werden.

3. Aktivieren Sie das Kontrollkästchen neben den ISE-Knoten, um die Knoten auszuwählen, für die das Zertifikat generiert wird.

4. Wenn der Zweck darin besteht, ein Platzhalterzertifikat zu installieren/generieren, überprüfen Sie die **Allow Wildcard Certificates** Box.

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. Füllen Sie die Betreffdaten basierend auf den Angaben zum Gastgeber oder zur Organisation aus (Organisationseinheit, Organisation, Ort, Bundesland und Land).

6. Klicken Sie zum Abschließen auf **Generate**, und klicken Sie dann auf **Export** auf dem Pop-up-Fenster, das daraufhin angezeigt wird.

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

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) | | - + ⓘ

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

* Key type RSA

* Key Length 2048 ⓘ

* Digest to Sign With SHA-256

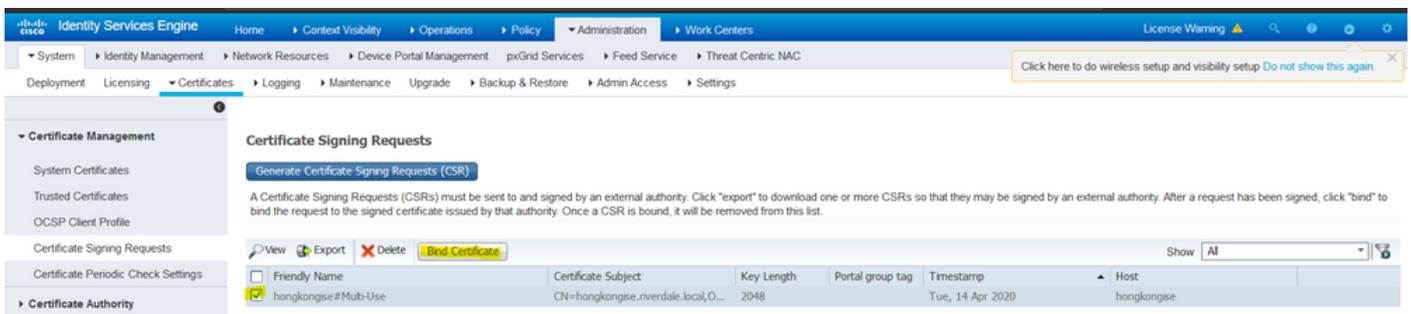
Dadurch wird die soeben erstellte Base-64-codierte Certificate Request-Anforderung heruntergeladen. Diese PEM-Datei muss zur Signatur an die Zertifizierungsstelle gesendet werden, und die resultierende signierte CER-Zertifikatsdatei (Base-64-codiert) wird abgerufen.

Hinweis: Im CN-Feld werden die Knoten automatisch von ISE mit FQDN ausgefüllt.

Hinweis: In ISE 1.3 und 1.4 mussten mindestens zwei CSRs ausgegeben werden, um pxGrid verwenden zu können. Einer ist pxGrid gewidmet, der andere für den Rest der Dienste. Seit Version 2.0 und höher läuft all dies auf einem CSR ab.

Hinweis: Wenn das Zertifikat für EAP-Authentifizierungen verwendet wird, darf sich das Symbol "*" nicht im Feld "Subject CN" (Betreff-CN) befinden, da Windows-Suppliants das Serverzertifikat ablehnen. Selbst wenn "Serveridentität überprüfen" auf dem Suppliant deaktiviert ist, kann der SSL-Handshake fehlschlagen, wenn sich "*" im CN-Feld befindet. Stattdessen kann im CN-Feld ein generischer FQDN verwendet werden. Anschließend wird der *.domain.com kann im Feld SAN DNS Name (SAN-DNS-Name) verwendet werden. Einige Zertifizierungsstellen (Certificate Authorities, CA) können den Platzhalter (*) in der CN des Zertifikats automatisch hinzufügen, selbst wenn er nicht im CSR vorhanden ist. In diesem Szenario ist eine spezielle Anforderung erforderlich, um diese Aktion zu verhindern.

7. Nachdem das Zertifikat von der Zertifizierungsstelle signiert wurde (die vom CSR generiert wurde, wie im Video gezeigt, [hier](#), wenn die Microsoft-Zertifizierungsstelle verwendet wird), wechseln Sie zurück zur ISE-GUI, und navigieren Sie zu **Administration > System > Certificates > Certificate Management > Certificate Signing Request**; Aktivieren Sie das Kontrollkästchen neben dem zuvor erstellten CSR, und klicken Sie auf die Schaltfläche **Bind Certificate**.



8. Als Nächstes laden Sie das signierte Zertifikat, das gerade empfangen wurde, und geben Sie ihm einen Anzeigenamen für ISE. Fahren Sie dann mit der Auswahl der Kästchen neben den verwendeten Zertifikaten (wie Admin- und EAP-Authentifizierung, Portal usw.) fort, und klicken Sie auf Submit, wie in diesem Bild gezeigt:

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)

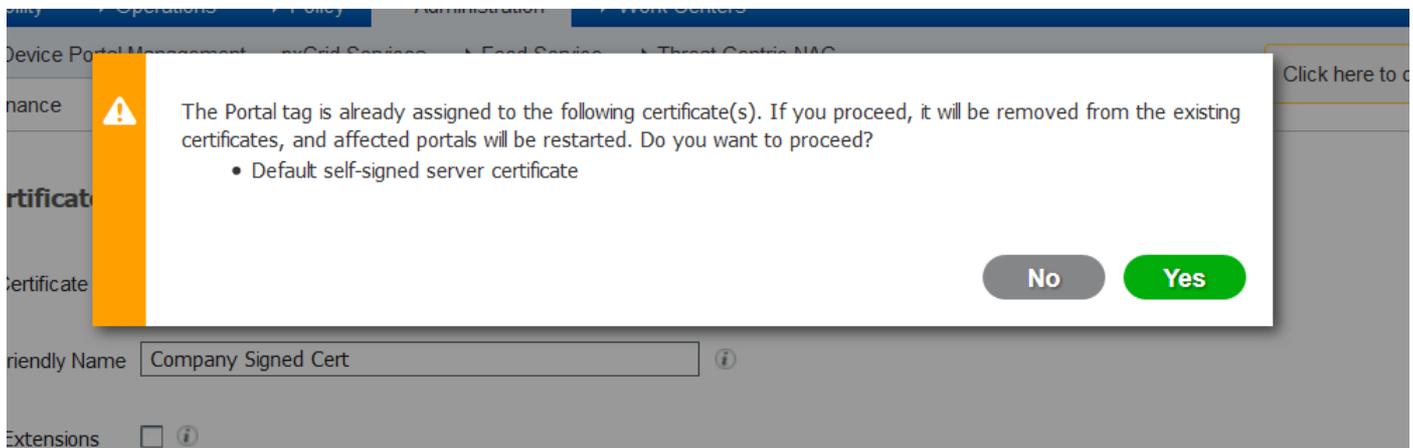
Wenn die Administratorrolle für dieses Zertifikat ausgewählt wurde, muss der ISE-Knoten seine Dienste neu starten. Je nach Version und zugewiesenen Ressourcen kann dies 10 bis 15 Minuten dauern. Um den Status der Anwendung zu überprüfen, öffnen Sie die ISE-Befehlszeile, und geben Sie `show application status ise aus`.

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

Friendly Name ⓘ



Wenn beim Zertifikatimport die Admin- oder Portalrolle ausgewählt wurde, kann überprüft werden, ob das neue Zertifikat vorhanden ist, wenn auf die Admin- oder Portalseiten im Browser zugegriffen wird. Wählen Sie das Sperrsymbol im Browser aus, und unter dem Zertifikat überprüft der Pfad, ob die gesamte Kette vorhanden ist und dem Computer vertraut. Der Browser muss dem neuen Admin- oder Portalzertifikat vertrauen, solange die Kette korrekt erstellt wurde und wenn der Browser der Zertifikatkette vertraut.

Hinweis: Um ein aktuelles CA-signiertes Systemzertifikat zu erneuern, generieren Sie einen neuen CSR, und binden Sie das signierte Zertifikat mit den gleichen Optionen an dieses. Da es möglich ist, ein neues Zertifikat auf der ISE zu installieren, bevor es aktiv ist, planen Sie, das neue Zertifikat zu installieren, bevor das alte Zertifikat abläuft. Diese Überlappungsperiode zwischen dem Ablaufdatum des alten Zertifikats und dem Startdatum des neuen Zertifikats gibt Zeit für die Erneuerung der Zertifikate und die Planung des Austauschs ohne oder mit nur geringer Ausfallzeit. Rufen Sie ein neues Zertifikat mit einem Startdatum ab, das vor dem Ablaufdatum des alten Zertifikats liegt. Der Zeitraum zwischen diesen beiden Daten ist das Änderungszeitfenster. Sobald das neue Zertifikat seinen gültigen Datumsbereich eingibt, aktivieren Sie die erforderlichen Protokolle (Admin/EAP/Portal). Denken Sie daran, dass bei aktivierter Admin-Nutzung ein Neustart des Diensts stattfindet.

Tipp: Es wird empfohlen, die firmeninterne Zertifizierungsstelle für Admin- und EAP-Zertifikate und ein öffentlich signiertes Zertifikat für Gast-/Sponsor-/Hotspot-/etc.-Portale zu verwenden. Wenn ein Benutzer oder Gast in das Netzwerk eintritt und das ISE-Portal ein privat signiertes Zertifikat für das Gastportal verwendet, erhält er Zertifikatfehler oder kann vom Browser blockiert werden. Um dies zu vermeiden, verwenden Sie ein öffentlich signiertes Zertifikat für die Portalnutzung, um ein besseres Benutzererlebnis zu gewährleisten. Darüber hinaus muss jede IP-Adresse des Bereitstellungsknotens/der Bereitstellungsknoten dem SAN-Feld hinzugefügt werden, um eine Zertifikatwarnung zu vermeiden, wenn auf den Server über die IP-Adresse zugegriffen wird.

Sicherungszertifikate und private Schlüssel

Es wird empfohlen, Folgendes zu exportieren:

1. Alle Systemzertifikate (von allen Knoten in der Bereitstellung) zusammen mit ihren privaten Schlüsseln (dies ist erforderlich, um sie neu zu installieren) an einem sicheren Ort. Notieren Sie sich die Zertifikatkonfiguration (für welchen Dienst das Zertifikat verwendet wurde).

2. Alle Zertifikate aus dem Speicher für vertrauenswürdige Zertifikate des primären Administrationsknotens. Notieren Sie sich die Zertifikatkonfiguration (für welchen Dienst das Zertifikat verwendet wurde).

3. Alle Zertifikate der Zertifizierungsstelle.

Hierzu

1. Navigieren Sie zu Administration > System > Certificates > Certificate Management > System Certificates. Wählen Sie das Zertifikat aus, und klicken Sie auf Export. Auswählen Export Certificates und das Optionsfeld Private Keys. Geben Sie das Passwort für den privaten Schlüssel ein, und bestätigen Sie das Passwort. Klicken Sie auf Export.
2. Navigieren Sie zu Administration > System > Certificates > Certificate Management > Trusted Certificates. Wählen Sie das Zertifikat aus, und klicken Sie auf Export. Klicken Sie auf Save File um das Zertifikat zu exportieren.
3. Navigieren Sie zu Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates. Wählen Sie das Zertifikat aus, und klicken Sie auf Export. Auswählen Export Certificates und das Optionsfeld Private Keys. Geben Sie das Kennwort für den privaten Schlüssel und die Kennwortbestätigung ein. Klicken Sie auf Export. Klicken Sie auf Save File um das Zertifikat zu exportieren.

Fehlerbehebung

Gültigkeit des Zertifikats überprüfen

Der Aktualisierungsvorgang schlägt fehl, wenn ein Zertifikat im Speicher für vertrauenswürdige Zertifikate oder Systemzertifikate der Cisco ISE abgelaufen ist. Überprüfen Sie die Gültigkeit im Feld Ablaufdatum der Fenster Vertrauenswürdige Zertifikate und Systemzertifikate (Administration > System > Certificates > Certificate Management), und erneuern Sie sie, falls erforderlich, vor dem Upgrade.

Überprüfen Sie außerdem die Gültigkeit der Zertifikate im Fenster "Zertifizierungsstellenzertifikate" im Feld "Ablaufdatum" (Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates), und erneuern Sie sie, falls erforderlich, vor dem Upgrade.

Löschen eines Zertifikats

Wenn ein Zertifikat in der ISE abgelaufen oder nicht verwendet wird, muss es entfernt werden. Stellen Sie vor dem Löschen sicher, dass die Zertifikate exportiert werden (ggf. mit ihren privaten Schlüsseln).

Um ein abgelaufenes Zertifikat zu löschen, navigieren Sie zu Administration > System > Certificates > Certificate Management. Klicken Sie auf System Certificates Store. Wählen Sie die abgelaufenen Zertifikate aus, und klicken Sie auf Delete.

Weitere Informationen zu vertrauenswürdigen Zertifikaten und Zertifikatsspeichern der Zertifizierungsstelle finden Sie auf der gleichen Seite.

Der Supplicant vertraut dem ISE-Serverzertifikat bei einer 802.1x-Authentifizierung

nicht.

Überprüfen Sie, ob die ISE die vollständige Zertifikatkette für den SSL-Handshake-Prozess sendet.

Bei EAP-Methoden, die ein Serverzertifikat erfordern (d. h. PEAP), und bei Auswahl von Serveridentität validieren in den Einstellungen des Client-Betriebssystems überprüft der Supplicant die Zertifikatkette mit den Zertifikaten, die er im lokalen Vertrauensspeicher als Teil des Authentifizierungsprozesses hat. Im Rahmen des SSL-Handshake-Prozesses stellt die ISE ihr Zertifikat sowie alle Root- und/oder Zwischenzertifikate in ihrer Kette vor. Der Supplicant ist nicht in der Lage, die Serveridentität zu validieren, wenn die Kette unvollständig ist oder diese Kette in seinem Trust Store fehlt.

Um zu überprüfen, ob die Zertifikatskette an den Client zurückgegeben wird, sollten Sie eine Paketerfassung von der ISE (Operations > Diagnostic Tools > General Tools > TCP Dump) oder Wireshark-Erfassung auf dem Endpunkt zum Zeitpunkt der Authentifizierung. Öffnen der Erfassung und Anwenden des Filters `ssl.handshake.certificates` in Wireshark und finde eine Herausforderung beim Zugriff.

Navigieren Sie nach der Auswahl zu `Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates`.

Ist die Kette unvollständig, navigieren Sie zur ISE `Administration > Certificates > Trusted Certificates` und überprüfen, ob die Stammzertifikate und/oder Zwischenzertifikate vorhanden sind. Wenn die Zertifikatskette erfolgreich bestanden wurde, muss die Kette selbst mit der hier beschriebenen Methode auf ihre Gültigkeit überprüft werden.

Öffnen Sie jedes Zertifikat (Server, Intermediate und Root), und überprüfen Sie die Vertrauenskette, damit die Subject Key Identifier (SKI) jedes Zertifikats mit der Authority Key Identifier (AKI) des nächsten Zertifikats in der Kette übereinstimmt.

ISE-Zertifikatkette ist korrekt, aber Endpunkt lehnt ISE-Serverzertifikat während der Authentifizierung ab

Wenn die ISE ihre vollständige Zertifikatkette für den SSL-Handshake darstellt und der Supplicant die Zertifikatkette immer noch zurückgewiesen hat, besteht der nächste Schritt darin, zu überprüfen, ob die Root- und/oder Intermediate-Zertifikate im lokalen Vertrauensspeicher des Clients vorhanden sind.

Um dies auf einem Windows-Gerät zu überprüfen, starten Sie `mmc.exe` (Microsoft Management Console), navigieren Sie zu `File > Add-Remove Snap-in`. Wählen Sie in der Spalte "Verfügbare Snap-Ins" `Certificates` und klicke auf `Add`. Wählen Sie eine `My user account` Oder `Computer account` auf Basis des verwendeten Authentifizierungstyps (Benutzer oder Computer), und klicken Sie dann auf `OK`.

Wählen Sie in der Konsolenansicht Vertrauenswürdige Stammzertifizierungsstellen und Zwischenzertifizierungsstellen aus, um das Vorhandensein von Stammzertifizierungsstellen und Zwischenzertifizierungsstellen im lokalen Vertrauensspeicher zu überprüfen.

Um auf einfache Weise zu überprüfen, ob es sich um ein Problem mit der Serveridentitätsprüfung handelt, deaktivieren Sie die Option Serverzertifikat validieren in der Konfiguration des Komponentenprofils, und testen Sie es erneut.

Häufig gestellte Fragen

Was zu tun ist, wenn die ISE eine Warnung ausgibt, dass das Zertifikat bereits vorhanden ist?

Diese Meldung bedeutet, dass ISE ein Systemzertifikat mit exakt demselben OU-Parameter erkannt hat und ein Duplikat des Zertifikats versucht wurde, es zu installieren. Da ein doppeltes Systemzertifikat nicht unterstützt wird, wird empfohlen, einen der Werte für Stadt/Bundesland/Abteilung auf einen etwas anderen Wert zu ändern, um sicherzustellen, dass das neue Zertifikat anders ist.

Warum gibt der Browser eine Warnung aus, dass die Portalseite der ISE von einem nicht vertrauenswürdigen Server dargestellt wird?

Dies geschieht, wenn der Browser dem Identitätszertifikat des Servers nicht vertraut.

Stellen Sie zunächst sicher, dass das im Browser sichtbare Portalzertifikat den Erwartungen entspricht und auf der ISE für das Portal konfiguriert wurde.

Stellen Sie zweitens sicher, dass Sie über FQDN auf das Portal zugreifen: Stellen Sie bei der verwendeten IP-Adresse sicher, dass sich sowohl der FQDN als auch die IP-Adresse im SAN- und/oder CN-Feld des Zertifikats befinden.

Stellen Sie abschließend sicher, dass die Zertifikatkette des Portals (ISE-Portal, zwischengeschaltete Zertifizierungsstelle(n), Stammzertifizierungsstelle(n)) in das bzw. von der Client-Betriebssystem-/Browser-Software importiert wird bzw. diesem vertraut.

Hinweis: Einige neuere Versionen von iOS-, Android-OS- und Chrome/Firefox-Browsern haben strenge Sicherheitsanforderungen an das Zertifikat. Selbst wenn diese Punkte erfüllt sind, können sie die Verbindung ablehnen, wenn die Portal- und Intermediate-CAs weniger als SHA-256 sind.

Was tun, wenn ein Upgrade aufgrund ungültiger Zertifikate fehlschlägt?

Der Aktualisierungsvorgang schlägt fehl, wenn ein Zertifikat im Speicher für vertrauenswürdige Zertifikate oder Systemzertifikate der Cisco ISE abgelaufen ist. Überprüfen Sie die Gültigkeit im Feld Ablaufdatum der Fenster Vertrauenswürdige Zertifikate und Systemzertifikate (Administration > System > Certificates > Certificate Management), und erneuern Sie sie, falls erforderlich, vor dem Upgrade.

Überprüfen Sie außerdem die Gültigkeit der Zertifikate im Fenster "Zertifizierungsstellenzertifikate" im Feld "Ablaufdatum" (Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates), und erneuern Sie sie, falls erforderlich, vor dem Upgrade.

Stellen Sie vor dem ISE-Upgrade sicher, dass die interne Zertifizierungsstellen-Zertifikatskette gültig ist.

Navigieren Sie zu Administration > System > Certificates > Certificate Authority Certificates. Wählen Sie für jeden Knoten in der Bereitstellung in der Spalte Anzeigename das Zertifikat mit der untergeordneten Zertifizierungsstelle für Zertifikatdienste aus. Klicken Sie auf View und überprüfen Sie, ob der Zertifikatsstatus eine gute Nachricht ist und angezeigt wird.

Wenn eine Zertifikatskette unterbrochen ist, stellen Sie sicher, dass das Problem behoben ist, bevor das Cisco ISE-Upgrade beginnt. Um das Problem zu beheben, navigieren Sie zu **Administration > System > Certificates > Certificate Management > Certificate Signing Requests** und generieren Sie eine für die ISE Root CA-Option.

Zugehörige Informationen

- [ISE 2.7 Verwalten von Zertifikaten und Zertifikatspeichereinstellungen](#)
- [Digitale Zertifikate in ISE implementieren](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.