

Configurar certificados TLS/SSL no ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Certificados de servidor](#)

[Certificados ISE](#)

[Certificados do sistema](#)

[Repositório de Certificados Confiáveis](#)

[Tarefas básicas](#)

[Gerar um certificado autoassinado](#)

[Renovar um certificado autoassinado](#)

[Instalar um Certificado Confiável](#)

[Instalar um certificado assinado pela CA](#)

[Fazer backup de certificados e chaves privadas](#)

[Troubleshoot](#)

[Verificar Validade do Certificado](#)

[Excluir um certificado](#)

[O requerente não confia no certificado do servidor ISE em uma autenticação 802.1x](#)

[A Cadeia de Certificados ISE está Correta, mas o Ponto de Extremidade Rejeita o Certificado de Servidor ISEs Durante a Autenticação](#)

[Perguntas mais freqüentes](#)

[O que fazer quando o ISE lança um aviso de que o certificado já existe?](#)

[Por que o navegador emite um aviso informando que a página do portal do ISE é apresentada por um servidor não confiável?](#)

[O que fazer quando uma atualização falhar devido a certificados inválidos?](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve os certificados TLS/SSL no Cisco ISE, os tipos e as funções dos certificados ISE, como executar tarefas e solucionar problemas comuns e respostas de perguntas frequentes.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

1. Cisco Identity Services Engine (ISE)
2. A terminologia usada para descrever diferentes tipos de implantações ISE e AAA.

3. Conceitos básicos de protocolo RADIUS e AAA
4. Certificados SSL/TLS e x509
5. Conceitos básicos de PKI (Public Key Infrastructure, infraestrutura de chave pública)

Componentes Utilizados

As informações neste documento são baseadas nas versões 2.4 a 2.7 de software e hardware do Cisco ISE. Ele abrange o ISE da versão 2.4 para a 2.7, no entanto, deve ser semelhante ou idêntico a outras versões do software ISE 2.x, a menos que declarado de outra forma.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Certificados de servidor

Os Certificados de Servidor são usados pelos servidores para apresentar a identidade do servidor aos clientes quanto à autenticidade e para fornecer um canal seguro de comunicação. Eles podem ser autoassinados (onde o servidor emite o certificado para si mesmo) ou emitidos por uma Autoridade de Certificação (interna a uma organização ou de um fornecedor conhecido).

Os certificados do servidor são normalmente emitidos para nomes de host ou FQDN (Fully Qualified Domain Name) do servidor, ou também podem ser um certificado curinga (*.domain.com). O(s) host(s), domínio ou subdomínio(s) para o(s) qual(is) ele é emitido normalmente é mencionado nos campos Nome comum (CN) ou Nome alternativo do assunto (SAN).

Os certificados curinga são certificados SSL que usam uma notação curinga (um asterisco no lugar do nome do host) e, portanto, permitem que o mesmo certificado seja compartilhado entre vários hosts em uma organização. Por exemplo, o valor CN ou SAN para um nome de assunto de certificados curinga pode ser semelhante a *.company.com e pode ser usado para proteger qualquer host desse domínio, como server1.com, server2.com, etc.

Os certificados normalmente usam criptografia de chave pública ou criptografia assimétrica.

- Chave pública: a chave pública está presente no certificado em um dos campos e é compartilhada publicamente por um sistema quando um dispositivo tenta se comunicar com ele.
- Chave Privada: A chave privada é privada para o sistema final e está emparelhada com a Chave Pública. Os dados criptografados por uma chave pública só podem ser descritos por uma chave privada do par específico e vice-versa.

Certificados ISE

O Cisco ISE conta com a infraestrutura de chave pública (PKI) para fornecer comunicação segura com endpoints, usuários, administradores e assim por diante, bem como entre nós do Cisco ISE

em uma implantação de vários nós. A PKI conta com certificados digitais x.509 para transferir chaves públicas para a criptografia e descryptografia de mensagens e para verificar a autenticidade de outros certificados apresentados por usuários e dispositivos. O Cisco ISE tem duas categorias de certificados normalmente usadas:

- **Certificados do sistema:** são certificados do servidor que identificam um nó do Cisco ISE para os clientes. Cada nó do Cisco ISE tem seus próprios certificados locais, cada um armazenado no nó junto com a respectiva chave privada.
- **Certificados de Repositório de Certificados Confiáveis:** estes são certificados de Autoridade de Certificação (CA) usados para validar os certificados apresentados ao ISE para várias finalidades. Esses certificados no armazenamento de certificados são gerenciados no nó de administração primária e replicados para todos os outros nós em uma implantação distribuída do Cisco ISE. O armazenamento de certificados também contém certificados gerados para os nós do ISE pela autoridade de certificação interna do ISE para BYOD.

Certificados do sistema

Os certificados do sistema podem ser usados para uma ou mais funções. Cada função tem uma finalidade diferente e é explicada aqui:

- **Admin:** usado para proteger toda a comunicação em 443 (GUI Admin), bem como para replicação e para qualquer porta/uso não listado aqui.
- **Portal:** usado para proteger a comunicação HTTP nos portais como o Portal de Autenticação da Web Centralizada (CWA), Convidado, BYOD, provisionamento de clientes, portais de Provisionamento de solicitante nativo e assim por diante. Cada portal deve ser mapeado para uma tag de grupo de portal (o padrão é a tag de grupo de portal padrão) que instrui o portal sobre o certificado especificamente marcado a ser usado. O menu suspenso Nome da tag de grupo do portal nas opções Editar do certificado permite criar uma nova tag ou escolher uma existente.
- **EAP:** esta é uma função que especifica o certificado apresentado aos clientes para autenticação 802.1x. Os certificados são usados com quase todos os métodos EAP possíveis, como EAP-TLS, PEAP, EAP-FAST e assim por diante. Com métodos EAP em túnel, como PEAP e FAST, o Transport Layer Security (TLS) é usado para proteger a troca de credenciais. As credenciais do cliente não são enviadas ao servidor até que esse túnel seja estabelecido para garantir uma troca segura.
- **RADIUS DTLS:** essa função especifica o certificado a ser usado para uma conexão DTLS (conexão TLS sobre UDP) para criptografar o tráfego RADIUS entre um dispositivo de acesso à rede (NAD) e o ISE. O NAD deve ter capacidade de criptografia DTLS para que esse recurso funcione.
- **SAML:** o certificado do servidor é usado para proteger a comunicação com o Provedor de Identidade SAML (IdP). Um certificado designado para uso SAML não pode ser usado para nenhum outro serviço, como Admin, autenticação EAP e assim por diante.
- **Serviço de mensagens do ISE:** desde a versão 2.6, o ISE usa o serviço de mensagens do ISE em vez do protocolo Syslog legado para registrar dados. Isso é usado para criptografar essa comunicação.
- **PxGrid:** esse certificado é usado para serviços PxGrid no ISE.

Quando o ISE é instalado, ele gera um Default Self-Signed Server Certificate. Atribuído para Autenticação EAP, Admin, Portal e RADIUS DTLS por padrão. É recomendável mover essas funções para uma CA interna ou um certificado com assinatura CA bem conhecida.

System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

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

Dica: é uma boa prática garantir que os endereços FQDN e IP do servidor ISE sejam adicionados ao campo SAN do certificado do sistema ISE. Em geral, para garantir que a autenticação de certificado no Cisco ISE não seja afetada por diferenças mínimas nas funções de verificação controladas por certificado, use nomes de host em minúsculas para todos os nós do Cisco ISE implantados em uma rede.

Observação: o formato de um certificado ISE deve ser Privacy Enhanced Mail (PEM) ou Distinguished Encoding Rules (DER).

Repositório de Certificados Confiáveis

Os certificados da autoridade de certificação devem ser armazenados em Administration > System > Certificates > Certificate Store e eles devem ter a Trust for client authentication caso de uso para garantir que o ISE use esses certificados para validar os certificados apresentados pelos endpoints, dispositivos ou outros nós do 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 2000	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"/>	VeriSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7D...	VeriSign Class 3 Public Pr...	VeriSign Class 3 Public Pr...	Wed, 8 Nov 2006	Wed, 16 Jul 2036
<input type="checkbox"/>	VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 03...	VeriSign Class 3 Secure ...	VeriSign Class 3 Public Pr...	Mon, 8 Feb 2010	Fri, 7 Feb 2020

Tarefas básicas

O certificado tem uma data de expiração e pode ser revogado ou ter que ser substituído em algum momento. Se o certificado do servidor ISE expirar, problemas sérios podem surgir, a menos que sejam substituídos por um novo certificado válido.

Observação: se o certificado usado para o EAP (Extensible Authentication Protocol) expirar, as autenticações dos clientes poderão falhar porque o cliente não confia mais no certificado ISE. Se um certificado usado para portais expirar, os clientes e navegadores poderão se recusar a se conectar ao portal. Se o certificado de uso Admin expirar, o risco é ainda maior, o que impede um administrador de fazer login no ISE mais e a implantação distribuída pode deixar de funcionar como deve.

Gerar um certificado autoassinado

Para gerar novos certificados autoassinados, navegue até Administration > System > Certificates > System Certificates. Clique no botão 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

Esta lista descreve os campos da página Gerar certificado autoassinado.

Diretrizes de Uso do Nome do Campo de Configurações de Certificado Autoassinado:

- Selecionar Nó: (Obrigatório) O nó para o qual é necessário gerar o certificado do sistema.
- CN: (obrigatório se SAN não for especificado) Por padrão, CN é o FQDN do nó ISE para o qual o certificado autoassinado é gerado.
- Unidade Organizacional (OU): nome da Unidade Organizacional, por exemplo, Engenharia.
- Organização (O): nome da organização, por exemplo, Cisco.
- Cidade (L): (Não abrevie) Nome da cidade, por exemplo, San Jose.
- Estado (ST): (Não abrevie) Nome do estado, por exemplo, Califórnia.
- País (C): Nome do país. O código ISO de país com duas letras é necessário. Por exemplo, os EUA.
- SAN: um endereço IP, nome DNS ou Uniform Resource Identifier (URI) associado ao certificado.
- Tipo de chave: especifique o algoritmo a ser usado para criar a chave pública: RSA ou ECDSA.
- Comprimento da Chave: Especifique o tamanho do bit para a chave pública. Essas opções estão disponíveis para RSA: 512 1024 2048 4096 e essas opções estão disponíveis para ECDSA: 256 384.
- Resumo com o qual assinar: escolha um destes algoritmos de hash: SHA-1 ou SHA-256.
- Políticas de Certificado: insira o OID da política de certificado ou a lista de OIDs que o certificado deve cumprir. Use vírgulas ou espaços para separar os OIDs.
- TTL de Expiração: Especifique o número de dias após os quais o certificado expira.
- Nome Amigável: Informe um nome amigável para o certificado. Se nenhum nome for especificado, o Cisco ISE cria automaticamente um nome no formato `where` é um número de cinco dígitos exclusivo.
- Permitir certificados curinga: marque esta caixa de seleção para gerar um certificado curinga autoassinado (um certificado que contenha um asterisco (*) em qualquer CN no assunto e/ou o nome DNS na SAN. Por exemplo, o nome DNS atribuído à SAN pode ser `*.domain.com`).
- Uso: Escolha o serviço para o qual este certificado do sistema deve ser usado. As opções disponíveis são:
AdminAutenticação EAPDTLS RADIUSpxGridSAMLPortal



▼ 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

Observação: as chaves públicas RSA e ECDSA podem ter comprimentos de chave diferentes para o mesmo nível de segurança. Escolha 2048 se a intenção for obter um certificado público assinado pela CA ou implantar o Cisco ISE como um sistema de gerenciamento de políticas compatível com FIPS.

Renovar um certificado autoassinado

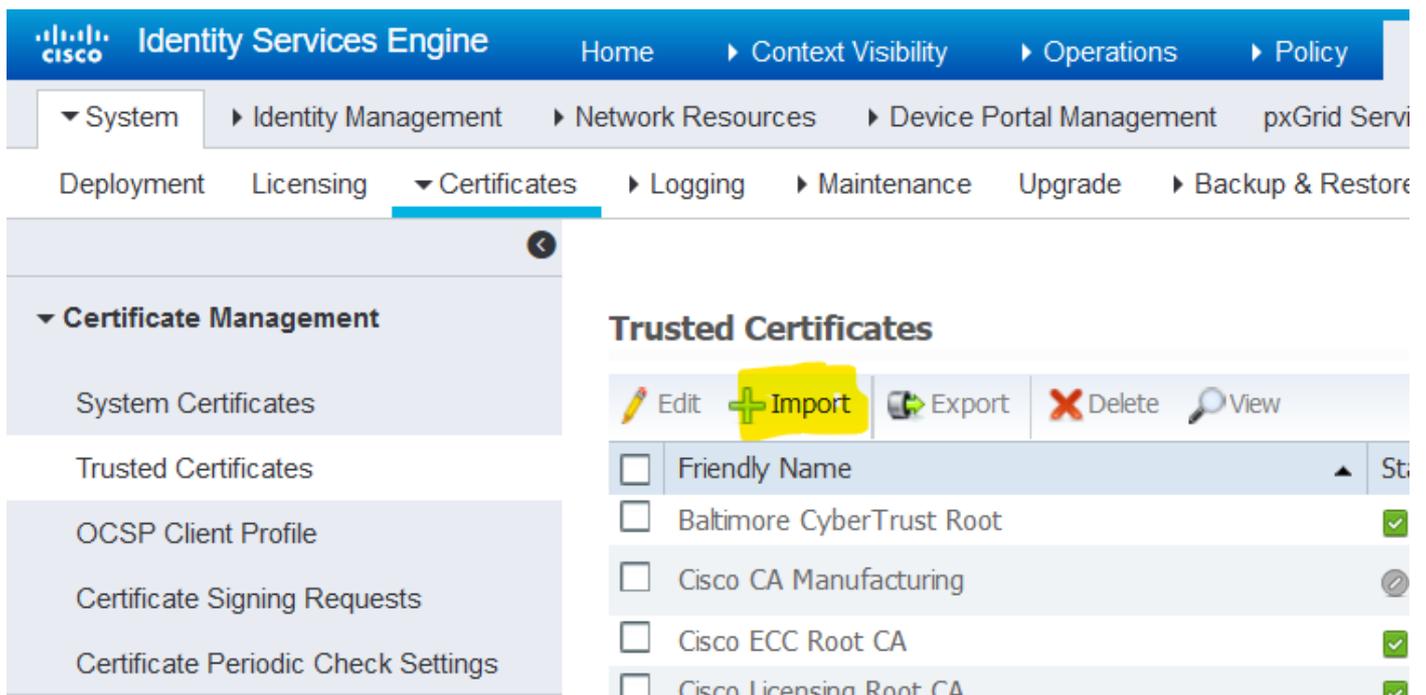
Para exibir os certificados autoassinados existentes, navegue até Administration > System > Certificates > System Certificates no console do ISE. Qualquer certificado com 'Emitido para' e 'Emitido por', se mencionado no mesmo FQDN do servidor do ISE, é um certificado autoassinado. Escolha este certificado e clique em Edit.

Sob Renew Self Signed Certificate, verifique a Renewal Period e defina o TTL de vencimento conforme necessário. Finalmente, clique em Save.

Instalar um Certificado Confiável

Obtenha o(s) certificado(s) codificado(s) Base 64 da CA raiz, CA(s) intermediária(s) e/ou dos hosts que devem ser confiáveis.

1. Faça login no nó do ISE e navegue até Administration > System > Certificate > Certificate Management > Trusted Certificates e clique em Import, como mostrado nesta imagem.



2. Na página seguinte, carregue o(s) certificado(s) de CA obtido(s) (na mesma ordem descrita anteriormente). Atribua a eles um nome amigável e uma descrição que explique para que serve o certificado para manter o controle.

Conforme as necessidades de uso, marque as caixas ao lado de:

- Confiança para autenticação no ISE - Adiciona novos nós do ISE quando eles têm o mesmo certificado CA confiável carregado no armazenamento de certificados confiáveis.
- Trust for client authentication and Syslog - Habilite esta opção para usar o certificado para autenticar pontos de extremidade que se conectam ao ISE com EAP e/ou confiar em servidores Syslog seguros.
- Confiança para autenticação dos serviços Cisco - Isso é necessário apenas para confiar em serviços Cisco externos, como um serviço de feed.

3. Finalmente, clique em Submit. Agora o certificado deve estar visível no Repositório Confiável e ser sincronizado com todos os nós ISE secundários (se estiver em uma implantação).

Identity Services Engine Administration Work Centers

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

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

▼ Certificate Management

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

▶ Certificate Authority

Import a new Certificate into the Certificate Store

* Certificate File CA certificate.cer

Friendly Name ⓘ

Trusted For: ⓘ

- Trust for authentication within ISE
- Trust for client authentication and Syslog
- Trust for authentication of Cisco Services
- Validate Certificate Extensions

Description

Instalar um certificado assinado pela CA

Depois que os certificados de CAs raiz e intermediária forem adicionados ao Repositório de certificados confiáveis, uma CSR (Certificate Signing Request, Solicitação de assinatura de certificado) poderá ser emitida e o certificado assinado com base na CSR poderá ser associado ao nó do ISE.

1. Para fazer isso, navegue até **Administration > System > Certificates > Certificate Signing Requests** e clique em **Generate Certificate Signing Requests (CSR)** para gerar um CSR.

2. Na página que aparece, na seção **Uso**, escolha a atribuição a ser usada no menu drop-down.

Se o certificado for usado para várias funções, escolha **Multiuso**. Depois que o certificado é gerado, as funções podem ser alteradas, se necessário. Na maioria dos casos, o certificado pode ser definido para ser usado para multiuso no menu suspenso **Usado para**; isso permite que o certificado seja utilizável para todos os portais da Web do ISE.

3. Marque a caixa ao lado do(s) nó(s) do ISE para escolher o(s) nó(s) para o(s) qual(is) o certificado é gerado.

4. Se o objetivo for instalar/gerar um certificado curinga, verifique a **Allow Wildcard Certificates** caixa de diálogo.

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. Preencha as informações sobre o assunto com base nos detalhes sobre o host ou a organização (Unidade Organizacional, Organização, Cidade, Estado e País).

6. Para finalizar isso, clique em **Generate** e clique em **Export** no pop-up que aparece.

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) ⓘ

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

* Key type RSA

* Key Length 2048 ⓘ

* Digest to Sign With SHA-256

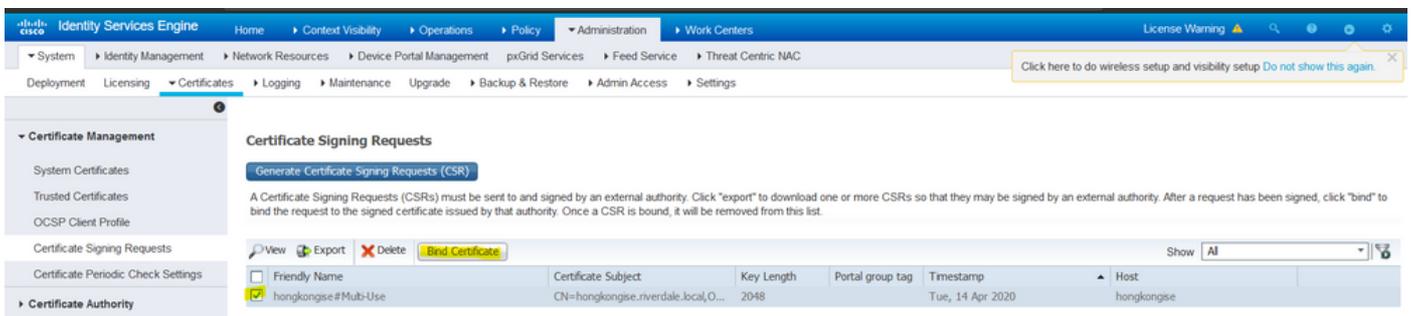
Isso faz o download da solicitação de certificado codificada na Base 64 que acabou de ser criada - esse arquivo PEM deve ser enviado à CA para assinatura e obtém o arquivo CER de certificado assinado resultante (codificado na Base 64).

Observação: no campo CN, o ISE preenche automaticamente o FQDN dos nós.

Observação: no ISE 1.3 e 1.4, era necessário emitir dois CSRs pelo menos para usar o pxGrid. Um é dedicado ao pxGrid e o outro, para o restante dos serviços. Desde o 2.0 e posterior, tudo isso está em um CSR.

Observação: se o certificado for usado para autenticações EAP, o símbolo '*' não deverá estar no campo CN do assunto, pois os solicitantes do Windows rejeitam o certificado do servidor. Mesmo quando a opção Validar identidade do servidor está desativada no solicitante, o handshake SSL pode falhar quando o '*' está no campo CN. Em vez disso, um FQDN genérico pode ser usado no campo CN e, em seguida, o *.domain.com pode ser usado no campo Nome DNS da SAN. Algumas Autoridades de Certificação (CA) podem adicionar o curinga (*) ao CN do certificado automaticamente, mesmo que ele não esteja presente no CSR. Neste cenário, uma solicitação especial deve ser feita para evitar essa ação.

7. Depois que o certificado tiver sido assinado pela CA (que foi gerada a partir do CSR como mostrado no vídeo, [aqui](#) se a CA da Microsoft for usada), volte para a GUI do ISE e navegue para **Administração > Sistema > Certificados > Gerenciamento de Certificados > Solicitação de Assinatura de Certificado**; Marque a caixa ao lado do CSR criado anteriormente e clique no botão **Vincular Certificado**.



8. Em seguida, carregue o certificado assinado que acabou de ser recebido e atribua a ele um nome amigável para o ISE. Em seguida, prossiga para escolher as caixas ao lado dos usos de acordo com a necessidade do certificado (como Admin e autenticação EAP, Portal e assim por diante) e clique em Submit, como mostrado nesta imagem:

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)

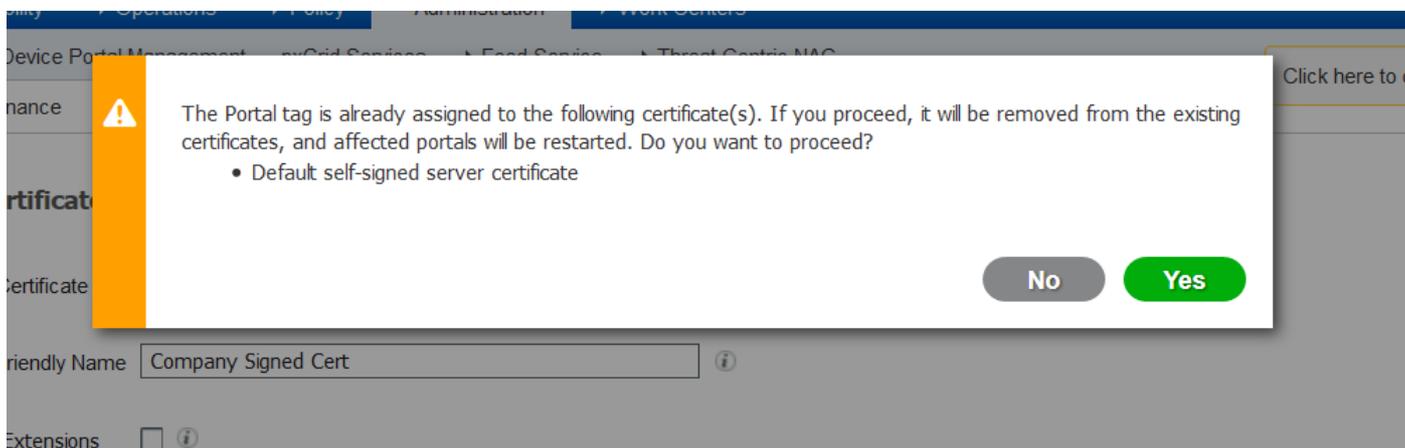
Se a função Admin tiver sido escolhida para esse certificado, o nó ISE deverá reiniciar seus serviços. Com base na versão e nos recursos alocados para a VM, isso pode levar de 10 a 15 minutos. Para verificar o status do aplicativo, abra a linha de comando do ISE e execute o comando `show application status ise` comando.

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 ⓘ



Se a função de administrador ou portal tiver sido escolhida na importação do certificado, poderá ser verificado se o novo certificado está em vigor quando as páginas de administrador ou portal no navegador forem acessadas. Escolha o símbolo de bloqueio no navegador e, sob o certificado, o caminho verifica se a cadeia completa está presente e é confiável para a máquina. O navegador deve confiar no novo certificado de administrador ou portal, desde que a cadeia tenha sido criada corretamente e a cadeia de certificados seja confiável pelo navegador.

Observação: para renovar um certificado de sistema atual assinado pela CA, gere um CSR novo e vincule o certificado assinado a ele com as mesmas opções. Como é possível instalar um novo certificado no ISE antes de ele estar ativo, planeje instalar o novo certificado antes que o certificado antigo expire. Esse período de sobreposição entre a data de expiração do certificado antigo e a data de início do novo certificado dá tempo para renovar certificados e planejar sua troca com pouco ou nenhum tempo de inatividade. Obtenha um novo certificado com uma data de início anterior à data de validade do certificado antigo. O período entre essas duas datas é a janela de alteração. Quando o novo certificado entrar no intervalo de datas válido, ative os protocolos necessários (Admin/EAP/Portal). Lembre-se de que, se o uso de Admin estiver habilitado, haverá uma reinicialização do serviço.

Dica: é recomendável usar a CA interna da empresa para certificados Admin e EAP e um certificado assinado publicamente para portais de convidado/patrocinador/hotspot/etc. O motivo é que, se um usuário ou convidado entra na rede e o portal do ISE usa um certificado assinado de forma privada para o Portal do convidado, ele obtém erros de certificado ou potencialmente faz com que seu navegador os bloqueie na página do portal. Para evitar tudo isso, use um certificado assinado publicamente para o uso do portal para garantir uma melhor experiência do usuário. Além disso, cada endereço IP do(s) nó(s) de implantação deve ser adicionado ao campo SAN para evitar um aviso de certificado quando o servidor é acessado por meio do endereço IP.

Fazer backup de certificados e chaves privadas

Recomenda-se exportar:

1. Todos os certificados do sistema (de todos os nós na implantação) junto com suas chaves privadas (isso é necessário para reinstalá-los) em um local seguro. Anote a configuração do certificado (para que serviço o certificado foi usado).

2. Todos os certificados do Repositório de Certificados de Confiabilidade do Nó de Administração Primário. Anote a configuração do certificado (para que serviço o certificado foi usado).
3. Todos os certificados da autoridade de certificação.

Para isso,

1. Navegue até Administration > System > Certificates > Certificate Management > System Certificates. Escolha o certificado e clique em Export. Escolher Export Certificates e as teclas privadas. Insira a senha da chave privada e confirme a senha. Clique em Export.
2. Navegue até Administration > System > Certificates > Certificate Management > Trusted Certificates. Escolha o certificado e clique em Export. Clique em Save File para exportar o certificado.
3. Navegue até Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates. Escolha o certificado e clique em Export. Escolher Export Certificates e as teclas privadas. Insira a senha da chave privada e confirme a senha. Clique em Export. Clique em Save File para exportar o certificado.

Troubleshoot

Verificar Validade do Certificado

O processo de atualização falhará se algum certificado no armazenamento de Certificados de Confiabilidade do Cisco ISE ou de Certificados de Sistema tiver expirado. Certifique-se de verificar a validade no campo Data de vencimento das janelas Certificados de Confiabilidade e Certificados de Sistema (Administration > System > Certificates > Certificate Management) e renove-os, se necessário, antes da atualização.

Além disso, verifique a validade no campo Data de vencimento dos certificados na janela Certificados de CA (Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates) e renove-os, se necessário, antes da atualização.

Excluir um certificado

Caso um certificado do ISE esteja expirado ou não seja usado, ele precisará ser removido. Verifique se os certificados foram exportados (com suas chaves privadas, se aplicável) antes da exclusão.

Para excluir um certificado expirado, navegue até Administration > System > Certificates > Certificate Management. Clique no botão System Certificates Store. Escolha o(s) certificado(s) expirado(s) e clique em Delete.

Consulte o mesmo para armazenamentos de Certificados de Confiabilidade e Certificados de Autoridade de Certificação.

O requerente não confia no certificado do servidor ISE em uma autenticação 802.1x

Verifique se o ISE envia a cadeia completa de certificados para o processo de handshake SSL.

Com os métodos EAP que exigem um certificado de servidor (ou seja, PEAP) e a opção Validar Identidade do Servidor é selecionada nas configurações do SO cliente, o solicitante valida a

cadeia de certificados com os certificados que possui em seu armazenamento confiável local como parte do processo de autenticação. Como parte do processo de handshake SSL, o ISE apresenta seu certificado e também todos os certificados raiz e/ou intermediários presentes em sua cadeia. O solicitante não poderá validar a identidade do servidor se a cadeia estiver incompleta ou se não tiver essa cadeia em seu repositório de confiança.

Para verificar se a cadeia de certificados é passada de volta para o cliente, faça uma captura de pacote do ISE (Operations > Diagnostic Tools > General Tools > TCP Dump) ou captura Wireshark no endpoint no momento da autenticação. Abra a captura e aplique o filtro `ssl.handshake.certificates` no Wireshark e encontrar um desafio de acesso.

Depois de escolhido, navegue até `Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates`.

Se a cadeia estiver incompleta, navegue até o ISE `Administration > Certificates > Trusted Certificates` e verifique se os certificados Raiz e/ou Intermediário estão presentes. Se a cadeia de certificados for aprovada com êxito, a própria cadeia deverá ser verificada como válida com o método descrito aqui.

Abra cada certificado (servidor, intermediário e raiz) e verifique a cadeia de confiança para corresponder ao identificador da chave do assunto (SKI) de cada certificado ao identificador da chave da autoridade (AKI) do próximo certificado na cadeia.

A Cadeia de Certificados ISE está Correta, mas o Ponto de Extremidade Rejeita o Certificado de Servidor ISEs Durante a Autenticação

Se o ISE apresentar sua cadeia completa de certificados para o handshake SSL e o requerente ainda tiver rejeitado a cadeia de certificados, a próxima etapa é verificar se os certificados Raiz e/ou Intermediários estão no Local Trust Store dos clientes.

Para verificar isso de um dispositivo Windows, inicie o `mmc.exe` (Console de Gerenciamento Microsoft), navegue até `File > Add-Remove Snap-in`. Na coluna snap-ins disponíveis, escolha `Certificates` e clique em `Add`. Escolha `My user account or Computer account` com base no tipo de autenticação em uso (Usuário ou Máquina) e clique em `OK`.

Na exibição do console, escolha `Autoridades de Certificação Raiz Confiáveis` e `Autoridades de Certificação Intermediárias` para verificar a presença de certificados Raiz e Intermediários no armazenamento confiável local.

Uma maneira fácil de verificar se este é um problema de verificação de identidade do servidor, desmarque `Validar certificado do servidor` na configuração do perfil do solicitante e teste-o novamente.

Perguntas mais frequentes

O que fazer quando o ISE emitir um aviso de que o certificado já existe?

Esta mensagem significa que o ISE detectou um Certificado do Sistema com exatamente o mesmo parâmetro de OU, e um certificado duplicado tentou ser instalado. Como não há suporte para a duplicação do certificado do sistema, é aconselhável simplesmente alterar qualquer um

dos valores de Cidade/Estado/Departamento para um valor ligeiramente diferente para garantir que o novo certificado seja diferente.

Por que o navegador emite um aviso informando que a página do portal do ISE é apresentada por um servidor não confiável?

Isso acontece quando o navegador não confia no certificado de identidade do servidor.

Primeiro, verifique se o certificado do portal visível no navegador é o esperado e se foi configurado no ISE para o portal.

Segundo, garanta acesso ao portal via FQDN - no caso do endereço IP em uso, garanta que o FQDN e o endereço IP estejam nos campos SAN e/ou CN do certificado.

Por fim, certifique-se de que a cadeia de certificados do portal (portal ISE, CA(s) intermediária(s), certificados de CA raiz) seja importada no/confiável pelo software do navegador/SO cliente.

Observação: algumas versões mais recentes do iOS, SOs Android e navegadores Chrome/Firefox têm expectativas de segurança rígidas do certificado. Mesmo se esses pontos forem atendidos, eles poderão se recusar a se conectar se o Portal e as CAs Intermediárias forem menores que SHA-256.

O que fazer quando uma atualização falhar devido a certificados inválidos?

O processo de atualização falhará se algum certificado no armazenamento de Certificados de Confiabilidade do Cisco ISE ou de Certificados de Sistema tiver expirado. Certifique-se de verificar a validade no campo Data de vencimento das janelas Certificados de Confiabilidade e Certificados de Sistema (Administration > System > Certificates > Certificate Management) e renove-os, se necessário, antes da atualização.

Além disso, verifique a validade no campo Data de vencimento dos certificados na janela Certificados de CA (Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates) e renove-os, se necessário, antes da atualização.

Antes da atualização do ISE, verifique se a cadeia de certificados internos da CA é válida.

Navegue até Administration > System > Certificates > Certificate Authority Certificates. Para cada nó na implantação, escolha o certificado com a Sub CA do ponto final dos serviços de certificado na coluna Nome amigável. Clique em View e verifique se o Status do certificado é uma boa mensagem e está visível.

Se alguma cadeia de certificados estiver quebrada, corrija o problema antes do início do processo de atualização do Cisco ISE. Para corrigir o problema, navegue até Administration > System > Certificates > Certificate Management > Certificate Signing Requests e gere um para a opção CA raiz do ISE.

Informações Relacionadas

- [Configurações de Gerenciar Certificados e Repositório de Certificados do ISE 2.7](#)
- [Implemente certificados digitais no ISE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.