# Instalar um certificado assinado por CA de terceiros no ISE

## Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configurar
Etapa 1. Gerar CSR (Certificate Signing Request, Solicitação de assinatura de certificado).
Etapa 2. Importar uma Nova Cadeia de Certificados.
Verificar
Troubleshooting
O requerente não confia no certificado de servidor local do ISE durante uma autenticação dot1x
<u>A Cadeia de Certificados ISE está Correta, mas o Ponto de Extremidade Rejeita o Certificado</u> ISEServer durante a Autenticação
Informações Relacionadas

## Introdução

Este documento descreve como instalar um certificado assinado por uma autoridade de certificação (CA) de terceiros no Cisco Identity Services Engine (ISE).

## Pré-requisitos

#### Requisitos

A Cisco recomenda que você tenha conhecimento da infraestrutura básica de chave pública.

#### **Componentes Utilizados**

As informações neste documento são baseadas no Cisco Identity Services Engine (ISE) Release 3.0. A mesma configuração se aplica às versões 2.X

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

Esse processo é o mesmo, independentemente da função do certificado final (autenticação EAP, Portal, Admin e pxGrid).

## Configurar

Etapa 1. Gerar CSR (Certificate Signing Request, Solicitação de assinatura de certificado).

Para gerar o CSR, navegue para Administration > Certificates > Certificate Signing Requests e clique em Generate Certificate Signing Requests (CSR).

Certificate Management System Certificates	~	Certi	ficate S	Sig	gning	Reque	ests
Trusted Certificates		Generat	e Certificate	Sign	ing Reque	sts (CSR)	
OCSP Client Profile		A Certificate	e Signing Requests	(CSR	(s) must be ser	nt to and signed	by an external authority. Click
Certificate Signing Requests		request has	been signed, click	"bind	to bind the red	quest to the sign	ed certificate issued by that au
Certificate Periodic Check Se		Q View	① Export	Ō	Delete	Bind Certif	ïcate
Certificate Authority	>		Friendly Nam	ie			Certificate Subject

- 1. Na seção Uso, selecione a função a ser usada no menu suspenso. Se o certificado for usado para várias funções, você poderá selecionar Multiuso. Depois que o certificado é gerado, as funções podem ser alteradas, se necessário.
- 2. Selecione o nó para o qual o certificado pode ser gerado.
- 3. Preencha as informações conforme necessário (Unidade organizacional, Organização, Cidade, Estado e País).
- Observação: no campo Nome comum (CN), o ISE preenche automaticamente o nó Nome de domínio totalmente qualificado (FQDN).

Caracteres curinga:

- Se o objetivo for gerar um certificado curinga, marque a caixa Permitir certificados curinga.
- 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 Validate Server Identity está desabilitado 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 (Nome alternativo do assunto).
- Observação: 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.

Exemplo de CSR de certificado de servidor individual:

#### Usage

Certificate(s) will be used for Multi-Use		~	4	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	0			
Node(s)				
Generate CSR's for these Nodes:				
Node	CSR Friendly Name			
✓ abtomar30	abtomar30#Multi-Use			
Subject				
Common Name (CN) \$FQDN\$		<b>(</b> )		
Organizational Unit (OU) Cisco TAC		(j)		
Organization (O) Cisco		<u>(</u> )		
City (L) Bangalore				
State (ST) Karnataka				
Country (C) IN				
Subject Alternative Name (SAN)				
IP Address	✓ 10.106.120.87		_	- + 0
* Key type				
RSA	× (j)			

Exemplo de CSR curinga:

Certificate(s) will be used for Multi-Use     You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Perrats, EAP, and pxGrid).   Allow Wildcard Certificates <ul> <li> <li> </li></li></ul> Organizational Unit (CU) <li> <ul> <li> <li>Cisco</li> <li>Cisco <li>Cisco</li> <li>Cisco</li> <li></li></li></li></ul></li>	Usage			~
restrice. Rather, you doublin individual certificate specificality for each service (for example, one certificate specificate	Certificate(s) will be used for	Multi-Use	~	You can use a single certificate for multiple services, but doing so is not a recommended
example, one certificate each for Guest Portals, EAP, and pxGrid).  Subject  Common Name (CN)  Mycluster.mydomain.com  Organizational Unit (OU) Cisco TAC  Organization (O) Cisco  Oi Cisco  Oi State (ST) Karnataka  Country (C) IN  Subject Alternative Name (SAN)				practice. Rather, you should obtain individual certificates specifically for each service (for
Allow Wildcard Certificates				example, one certificate each for Guest Portals, EAP, and pxGrid).
Subject Common Name (CN) Mycluster.mydomain.com Organizational Unit (OU) Cisco TAC Organization (0) Cisco City (L) Bangalore State (ST) Karnataka Country (C) IN Subject Alternative Name (SAN) III III III III III IIII IIII IIIIIIII	Allow Wildcard Certificates 🔽	$\bigcirc$		
Common Name (CN) Mycluster.mydomain.com	Subject			
Mycluster.mydomain.com   Organizational Unit (OU)   Cisco TAC   Organization (O)   Cisco   Cisco   Cisco   State (ST)   Karnataka   Country (C)   IN   Subject Alternative Name (SAN)   Image: Product Alternative Name (SAN)	Common Name (CN)			
Organizational Uhit (OU)   Cisco TAC     Organization (0)   Cisco     City (L)   Bangalore     State (ST)   Karnataka     Country (C)   IN   Subject Alternative Name (SAN)        IP Address   V   10.106.120.87   Image: Imag	Mycluster.mydomain,com		(i) 	
Cisco TAC  Organization (0) Cisco  City (L) Bangalore  State (ST) Karnataka  Country (C) IN  Subject Alternative Name (SAN)        Image: Product Alternative Name (SAN) <tr< td=""><td>Organizational Unit (OU)</td><td></td><td></td><td></td></tr<>	Organizational Unit (OU)			
Organization (0)   Cisco     City (L)   Bangalore     State (ST)   Karnataka   Country (C)   IN   Subject Alternative Name (SAN)      Image:	Cisco TAC		_ 	
Cisco City (L) Bangalore State (ST) Karnataka Country (C) IN Subject Alternative Name (SAN)           Subject Alternative Name (SAN)           II           Subject Alternative Name (SAN)           II           Subject Alternative Name (SAN)           III           III           Subject Alternative Name (SAN)           III           III           Subject Alternative Name (SAN)           III           III           III           III           III           IIII           IIII           IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Organization (O)			
City (L) Bangalore	Cisco		<u>(</u> )	
State (ST) Karnataka Country (C) IN Subject Alternative Name (SAN) II       Address <ul> <li>10.106.120.87</li> <li>Imulaities</li> <li>Imulaities<td>City (L)</td><td></td><td></td><td></td></li></ul>	City (L)			
State (ST)   Karnataka	Bangalore			
Karnataka     Country (C)   IN     Subject Alternative Name (SAN)     IP Address   I DNS Name   * Mydomain.com     * Key type	State (ST)			
Country (C) IN Subject Alternative Name (SAN)          IP Address          IDNS Name          Model       *.mydomain.com	Karnataka			
Subject Alternative Name (SAN)     ii   IP Address   ·   10.106.120.87     ·   iii   DNS Name   ·   ·   ·   ·     ·	Country (C)			
Subject Alternative Name (SAN)          IP Address       ~       10.106.120.87       -       +         IDNS Name       ~       *.mydomain.com       -       +       ()         * Key type	IN			
Subject Alternative Name (SAN)          IP Address        10.106.120.87       Image: Comparing the state of the state o				
IP Address       ~       10.106.120.87       -       +         III       DNS Name       ~       *.mydomain.com       -       +       ()         * Key type	Subject Alternative Name (SAN)			
Image:	IP Address	✓ 10.106.120.87		- +
* Key type	DNS Name	✓ *.mydomain.com		- + 0
	* Key type			
RSA V (i)	RSA	~ (j		

Observação: cada endereço IP do(s) nó(s) de implantação pode ser adicionado ao campo SAN para evitar um aviso de certificado quando você acessa o servidor por meio do endereço IP.

Depois que o CSR é criado, o ISE exibe uma janela pop-up com a opção de exportá-lo. Depois de



Etapa 2. Importar uma Nova Cadeia de Certificados.

A Autoridade de Certificação retorna o certificado de servidor assinado junto com a cadeia completa de certificados (Raiz/Intermediário). Depois de recebido, siga estas etapas para importar os certificados para o servidor ISE:

- 1. Para importar qualquer certificado raiz e (ou) intermediário fornecido pela CA, navegue para Administração > Certificados > Certificados de Confiabilidade.
- 2. Clique em Importar e escolha o certificado Raiz e/ou Intermediário e marque as caixas de seleção relevantes conforme foram aplicadas ao envio.
- 3. Para importar o certificado do servidor, navegue para Administração > Certificados > Solicitações de assinatura de certificado.
- 4. Selecione o CSR criado anteriormente e clique em Bind Certificate.
- 5. Selecione o novo local do certificado e o ISE vinculará o certificado à chave privada criada e armazenada no banco de dados.

Observação: se a função de administrador tiver sido selecionada para esse certificado, os serviços do servidor ISE específicos serão reiniciados.

A Cuidado: Se o certificado importado for para o Nó de Administração Primário da implantação e se a função Admin estiver selecionada, os serviços em todos os nós serão reiniciados um A após o outro. Isso é esperado e um tempo de inatividade é recomendado para executar essa atividade.

## Verificar

Se a função de administrador foi selecionada durante a importação do certificado, você pode verificar se o novo certificado está no lugar carregando a página de admin no navegador. O navegador deve confiar no novo certificado de administrador, desde que a cadeia tenha sido criada corretamente e a cadeia de certificados seja confiável para o navegador.

Certificate	
General Details Certification Path Certification path abtomar-WIN-231PNBS4IPH-CA abtomar30.abtomar.local	cisco
	Identity Services Engine
	Intuitive network security
	Username
View Certificate Certificate status: This certificate is OK.	Password
	Login
ОК	English   日本語
	Problems logging in?
2020 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are register	ered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S and certain other countries. Cisco Systems, Inc. and notices

Para verificação adicional, selecione o símbolo de bloqueio no navegador e, no caminho do certificado, verifique se a cadeia completa está presente e é confiável para a máquina. Este não é um indicador direto de que a cadeia completa foi passada corretamente pelo servidor, mas um indicador de que o navegador pode confiar no certificado do servidor com base em seu repositório

## Troubleshooting

de confiança local.

O requerente não confia no certificado de servidor local do ISE durante uma

#### autenticação dot1x

Verifique se o ISE está passando a cadeia completa de certificados durante o processo de handshake SSL.

Ao usar métodos EAP que exigem um certificado de servidor (ou seja, PEAP) e Validar Identidade do Servidor estiver selecionado, o requerente valida a cadeia de certificados usando os certificados que tem 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. Para verificar se a cadeia de certificados é passada de volta para o cliente, você pode executar as próximas etapas:

- 1. Para obter uma captura do ISE (TCPDump) durante a autenticação, navegue para Operations > Diagnostic Tools > General Tools > TCP Dump.
- 2. Baixe/abra a captura e aplique o filtro ssl.handshake.certificates no Wireshark e encontre um desafio de acesso.
- Depois de selecionado, navegue para Expandir Protocolo Radius > Pares de valores de atributo > Último segmento de mensagem EAP > Protocolo de autenticação extensível > Secure Sockets Layer > Certificado > Certificados.

Cadeia de certificados na captura.

ile <u>E</u> di	View Go Capture Analyze Stat	istics Telephony Iools Internals He	ip.				
2 00 /	(■ <u>∦ </u> ⊟∃¥₿ ९♦।	•• <b>*</b> 2	🕷 🗹 🥵 🛠	Ħ			
Filter	ssLhandshake.certificates	<ul> <li>Expression</li> </ul>	Clear Appl	/ Save			
a	Time	Source	Destination	Protocol I	ength Info		
33	13:59:41.137274	14.36.157.20	14.36.157.2	1 TLSV1.2	992 Server	<ul> <li>Hello, Certificate, Server Hello Don</li> </ul>	16
85	13:59:53.158063	14.36.157.21	14.36.154.5	RADIUS	1178 Access	-Challenge(11) (id=198, 1=1136)	
86	13:59:53.193912	14.36.157.21	14.36.154.5	RADIUS	1174 Access	-Challenge(11) (1d=199, 1=1132)	
86.	13:59:53.213/15	14.36.157.21	14.36.154.5	RADIUS	1174 Access	-Challenge(11) (id=200, 1=1132)	
86	13:59:53.231653	14.36.157.21	14.36.154.5	RADIUS	301 Access	-Challenge(11) (1d=201, 1=259)	
126	14:00:01.253698	14.36.157.20	14.36.157.2	1 TLSV1.2	992 Server	Hello, Certificate, Server Hello Don	10
				11			
- A1	U: I=/SS t=FAR-Marragal/W	) Secment[]]					
0.4	P: 1-255 t-EAD-Message(79) P: 1-255 t-EAD-Message(79)	Segment[2]					
- A1	P: 1=255 t=EAP-Message(79 0: 1=255 t=EAP-Message(79)	Segment[3]					
E AV	P: 1=255 T=FAP-Message(79	) Last Segment[4]					
	EAP fragment	/ case segmence(+)					
8	Extensible Authentication	Protocol					
	Code: Request (1)						
	Id: 41						
	Length: 1012						
	Type: Protected EAP (EAP	-PEAP) (25)					
	EAP-TLS Flags: 0xc0						
	EAP-TLS Length: 3141						
	8 [4 EAP-TLS Fragments (31)	41 bytes): #857(1002), #860	(1002), #862(	1002), #864(135)]			
	Secure Sockets Layer						
	III TLSv1 Record Layer: Har	ndshake Protocol: Server He	110				
	□ TLSv1 Record Layer: Har	ndshake Protocol: Certifica	te				
	Content Type: Handsha	ke (22)					
	Version: TLS 1.0 (0x0	(301)					
	Length: 3048						
	B Handshake Protocol: C	ertificate					
	Handshake Type: Cer	tificate (11)					
	Length: 3044						
	Certificates Length	: 3041					
	Certificates (3041)	bytes)					
	Certificate Length	1656					
	Certificate (id-at)	-commonName=TORISE20A.rtpa	aa.net,id-at-o	rganizationalUnitNa	me=RTPAAA,id	i-at-organizationName=CISCO,id-at-loca	alityNam
	CONTRESSOR & CONTR	1370					
	Certificate Lengtr	11 1.57.5					
	# Certificate (id-at	-commonWame=rtpaaa-ca,dc=r	tpaaa,dc=net)				
	# Certificate (id-at # TLSv1 Record Layer: Har	-commonName=rtpaaa-ca,dc=r hdshake Protocol: Server He	tpaaa,dc=net) 11o Done				

Se a cadeia estiver incompleta, navegue para Administração do ISE > Certificados > Certificados

de Confiabilidade e verifique se os certificados Raiz e (ou) Intermediário estão presentes. Se a cadeia de certificados for aprovada com êxito, a própria cadeia deve ser verificada como válida usando o método descrito aqui.

Abra cada certificado (servidor, intermediário e raiz) e verifique a cadeia de confiança fazendo a correspondência do identificador da chave do assunto (SKI) de cada certificado com o identificador da chave da autoridade (AKI) do próximo certificado na cadeia.

Exemplo de uma cadeia de certificados.

Certificate 25	Certificate 24	S Certificate 26
General Details Certification Path	General Details Certification Path	General Details Certification Path
Show <all></all>	Show <all></all>	Show <all></all>
Field Value ^	Field Value *	Field Value ^
Public key RSA (2048 Bits)	CA Version V0.0	Public key RSA (4096 Bits)
Subject Key Identifier da 39 a3 ee 5e 6b 4b 0d 32 55 bf ef 95 6	Subject Key Identifier fe 34 ca 8d 22 9b 6e d7 as 86 11 cl 18 1.	Key Usage Digital Signature, Certificate Signing, Off-II
Enhanced Key Usage Server Authentication (1.3.6.1.5.5.7.3.1)	Tertificate Templat SubCA	Subject Key Ment 52 2e e5 2c 38 29 66 da 81 19 11 70 74 60
Subject Alternative P Address=14.39.157.21	CDI Distribution Sol 11/CDI Distribution Doint: Distribution Doi	Real Constraints Subject Types CA. Bath Leasth Constraints
CRI Distribution Pol. [11CRI Distribution Spint: Distribution Pol.	Authority Informatio	Thurshorint algority, that
Authority Informati [1]Authority Info Access: Access Method	Key Usage Digital Signature, Certificate Signing, Off-L -	Thumborint cb 24 48 a5 30 11 72 a3 da 9e 31 d1 f3 f6
		4 11
V3	V3	V3
Edit Properties Copy to File	Edit Properties Copy to File	Edit Properties Copy to File Learn more about <u>contificate details</u>
OK	06	ОК

## A Cadeia de Certificados ISE está Correta, mas o Ponto de Extremidade Rejeita o Certificado do Servidor ISE durante a Autenticação

Se o ISE estiver apresentando sua cadeia completa de certificados durante o handshake SSL e o requerente ainda estiver rejeitando a cadeia de certificados; a próxima etapa é verificar se os certificados Raiz e/ou Intermediário estão no Local Trust Store do cliente.

Para verificar isso a partir de um dispositivo do Windows, navegue para mmc.exe Arquivo > Add-Remove Snap-in. Na coluna Snap-ins disponíveis, selecione Certificados e clique em Adicionar. Selecione Minha conta de usuário ou conta do computador, dependendo do tipo de autenticação em uso (Usuário ou Computador) e clique em OK.

Na exibição do console, selecione Autoridades de Certificação Raiz Confiáveis e Autoridades de Certificação Intermediárias para verificar a presença de Certificado Raiz e Intermediário no armazenamento confiável local.

🖕 Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

File Action View Favorites Window Help						
	A					
Console Root	Issued To	Issued By	Expiration	Intended Purpo	Friendly Name S	t
A 🖓 Certificates - Current User	AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenti	USERTrust	
Personal	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenti	Baltimore Cybe	
Trusted Root Certification Authorities	Certum CA	Certum CA	6/11/2027	Server Authenti	Certum	
Certificates	GCisco Root CA 2048	Cisco Root CA 2048	5/14/2029	<all></all>	<none></none>	
Interprise Trust     Intermediate Certification Authorities	Gisco Root CA M1	Cisco Root CA M1	11/18/2033	<all></all>	<none></none>	
Certificate Revocation List	Class 2 Primary CA	Class 2 Primary CA	7/6/2019	Secure Email, S	CertPlus Class 2	
Certificates	Class 3 Public Primary Ce	Class 3 Public Primary Certi	8/1/2028	Secure Email, C	VeriSign Class 3	
Active Directory User Object	COMODO RSA Certificati	COMODO RSA Certificatio	1/18/2038	Server Authenti	COMODO	
Trusted Publishers	Copyright (c) 1997 Micro	Copyright (c) 1997 Microso	12/30/1999	Time Stamping	Microsoft Time	
Untrusted Certificates	DigiCert Assured ID Root	DigiCert Assured ID Root C	11/9/2031	Server Authenti	DigiCert	
Dirac Interview Party Root Certification Authorities	DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenti	DigiCert	
Trusted People	DigiCert High Assurance	DigiCert High Assurance E.,	11/9/2031	Server Authenti	DigiCert	
Display the second s	DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, S	DST Root CA X3	
Certificate Enrollment Requests	DST Root CA X3	DST Root CA X3	9/30/2021	<all></all>	<none></none>	
Smart Card Trusted Roots	Entrust Root Certification	Entrust Root Certification	11/27/2026	Server Authenti	Entrust	

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.

Connection Security	When connecting:
Security type: WPA2-Enterprise   Encryption type: AES	Connect to these servers:
	Trusted Root Certification Authorities:  AddTrust External CA Root Baltimore CyberTrust Root
Choose a network authentication method: Microsoft: Protected EAP (PEAP) Settings Remember my credentials for this connection each time I'm logged on	Certum CA Cisco Root CA 2048 Cisco Root CA M1 Class 2 Primary CA
une in ogged on	Class 3 Public Primary Certification Authority

## Informações Relacionadas

- Guia do Administrador do Cisco Identity Services Engine, Versão 3.0
- Suporte técnico e downloads da Cisco

#### 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.