

# 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](#)

[A Cadeia de Certificados ISE está Correta, mas o Ponto de Extremidade Rejeita o Certificado 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.

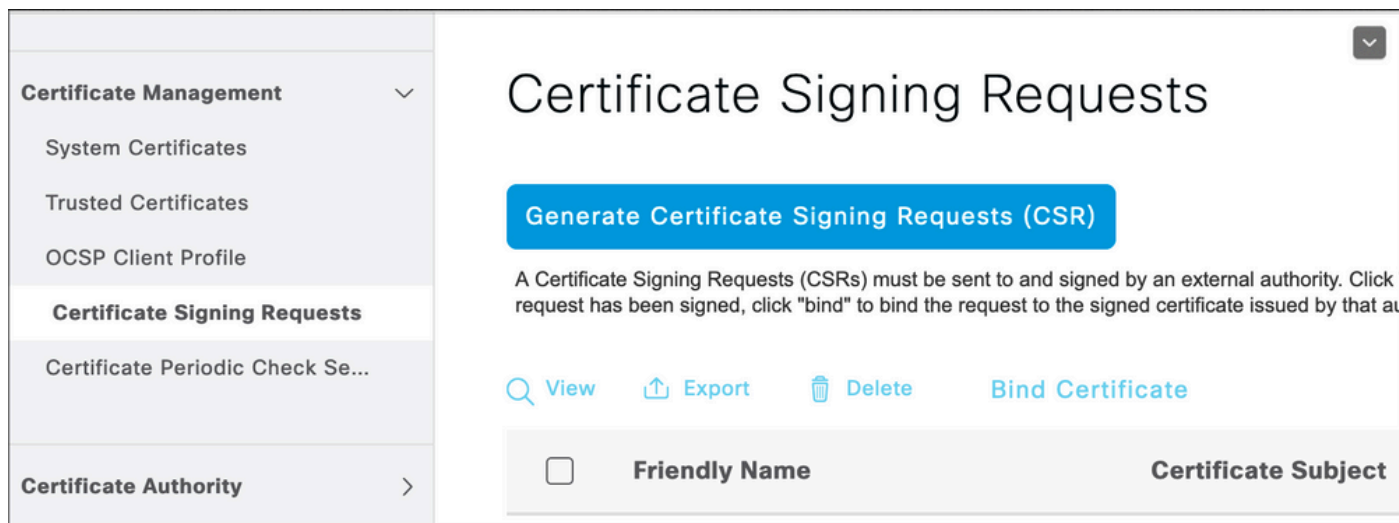
## Informações de Apoio

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).



The screenshot shows the 'Certificate Signing Requests' page in a management console. On the left is a navigation sidebar with categories: Certificate Management (expanded), Certificate Authority, and Certificate Periodic Check Se... Under Certificate Management, there are links for System Certificates, Trusted Certificates, OCSP Client Profile, Certificate Signing Requests (highlighted), and Certificate Periodic Check Se... Under Certificate Authority, there is a right-pointing arrow. The main content area has the title 'Certificate Signing Requests' and a prominent blue button labeled 'Generate Certificate Signing Requests (CSR)'. Below the button is a note: 'A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click 'request has been signed, click "bind" to bind the request to the signed certificate issued by that au...'. Below the note are four action buttons: 'View' (with a magnifying glass icon), 'Export' (with an upload icon), 'Delete' (with a trash icon), and 'Bind Certificate'. At the bottom, a table header is visible with columns 'Friendly Name' and 'Certificate Subject', and a checkbox on the left.


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 

 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 checked="" type="checkbox"/> abtomar30	abtomar30#Multi-Use

## Subject

Common Name (CN)  
\$FQDN\$ 

Organizational Unit (OU)  
Cisco TAC 

Organization (O)  
Cisco 

City (L)  
Bangalore



State (ST)  
Karnataka

Country (C)  
IN

Subject Alternative Name (SAN)

 IP Address  10.106.120.87   


\* Key type

RSA  

Exemplo de CSR curinga:

## 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  

## Subject

Common Name (CN)



Organizational Unit (OU)



Organization (O)



City (L)

State (ST)


Country (C)

Subject Alternative Name (SAN)



\* Key type




 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

exportado, esse arquivo deve ser enviado à autoridade de certificação para assinatura.

---



Successfully generated CSR(s) 

Certificate Signing request(s) generated:

abtomar30.abtomar.local#Multi-Use

Click Export to download CSR(s) or OK to return to list of CSR(s) screen

OK

Export


---

## 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.

---

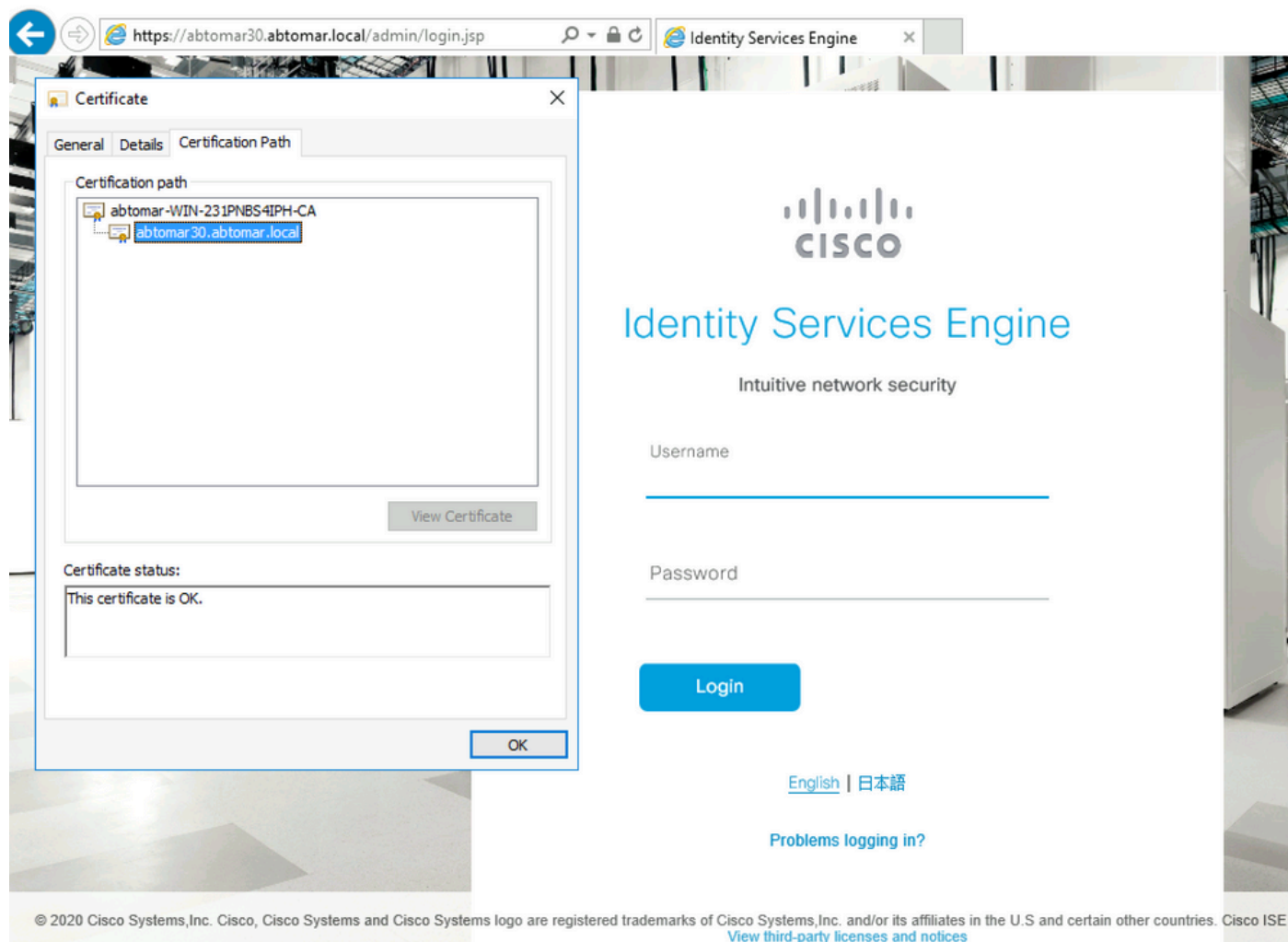
 Cuidado: Se o certificado importado for para o Nó de Administração Primário da implantação e se a função Admin estiver selecionada, os serviços em todos os nós serão reiniciados um

---

⚠ 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.



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 de confiança local.

## Troubleshooting

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

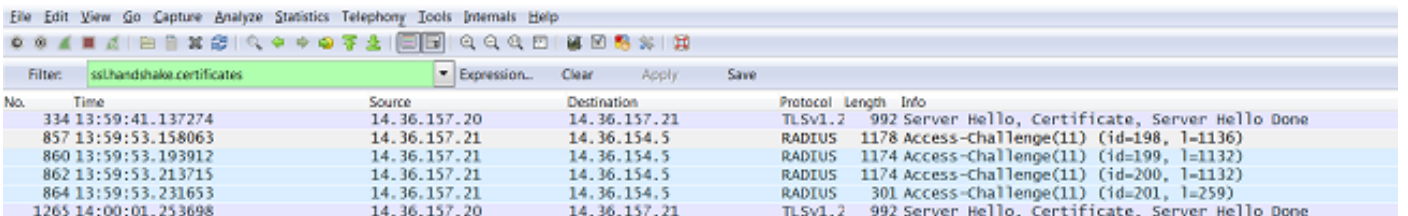
## autenticação dot1x

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

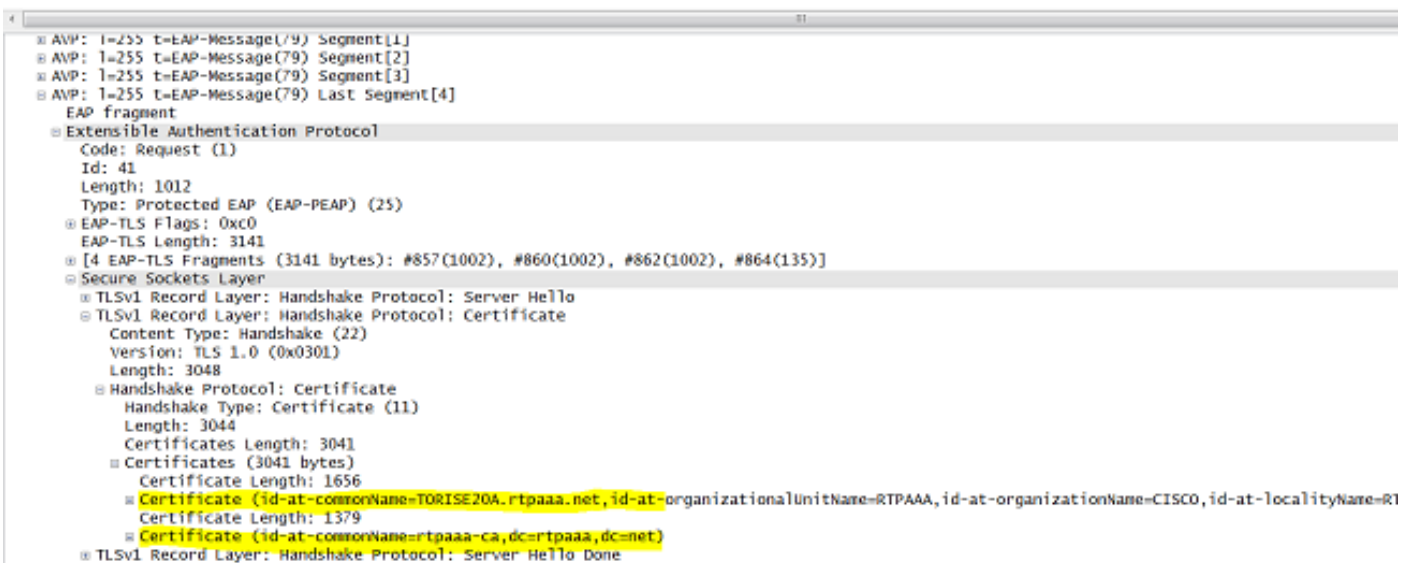
Ao usar métodos EAP que exigem um certificado de servidor (ou seja, PEAP) e Validar Identidade do Servidor estiver selecionado, o requerente valida a cadeia de certificados usando os certificados que tem em seu armazenamento confiável local como parte do processo de autenticação. Como parte do processo 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.
3. 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.



No.	Time	Source	Destination	Protocol	Length	Info
334	13:59:41.137274	14.36.157.20	14.36.157.21	TLSv1.2	992	Server Hello, Certificate, Server Hello Done
857	13:59:53.158063	14.36.157.21	14.36.154.5	RADIUS	1178	Access-Challenge(11) (id=198, l=1136)
860	13:59:53.193912	14.36.157.21	14.36.154.5	RADIUS	1174	Access-Challenge(11) (id=199, l=1132)
862	13:59:53.213715	14.36.157.21	14.36.154.5	RADIUS	1174	Access-Challenge(11) (id=200, l=1132)
864	13:59:53.231653	14.36.157.21	14.36.154.5	RADIUS	301	Access-Challenge(11) (id=201, l=259)
1265	14:00:01.253698	14.36.157.20	14.36.157.21	TLSv1.2	992	Server Hello, Certificate, Server Hello Done



```

AVP: l=255 t=EAP-Message(79) Segment[1]
AVP: l=255 t=EAP-Message(79) Segment[2]
AVP: l=255 t=EAP-Message(79) Segment[3]
AVP: l=255 t=EAP-Message(79) Last Segment[4]
EAP fragment
  Extensible Authentication Protocol
    Code: Request (1)
    Id: 41
    Length: 1012
    Type: Protected EAP (EAP-PEAP) (25)
    EAP-TLS Flags: 0xc0
    EAP-TLS Length: 3141
    [4 EAP-TLS Fragments (3141 bytes): #857(1002), #860(1002), #862(1002), #864(135)]
    Secure Sockets Layer
      TLSv1 Record Layer: Handshake Protocol: Server Hello
      TLSv1 Record Layer: Handshake Protocol: Certificate
        Content Type: Handshake (22)
        Version: TLS 1.0 (0x0301)
        Length: 3048
        Handshake Protocol: Certificate
          Handshake Type: Certificate (11)
          Length: 3044
          Certificates Length: 3041
          Certificates (3041 bytes)
            Certificate Length: 1656
            Certificate (id-at-commonName=TORISE204.rtpaaa.net,id-at-organizationalUnitName=RTPAAA,id-at-organizationName=CISCO,id-at-localityName=R1)
              Certificate Length: 1379
            Certificate (id-at-commonName=rtpaaa-ca,dc=rtpaaa,dc=net)
      TLSv1 Record Layer: Handshake Protocol: Server Hello Done

```

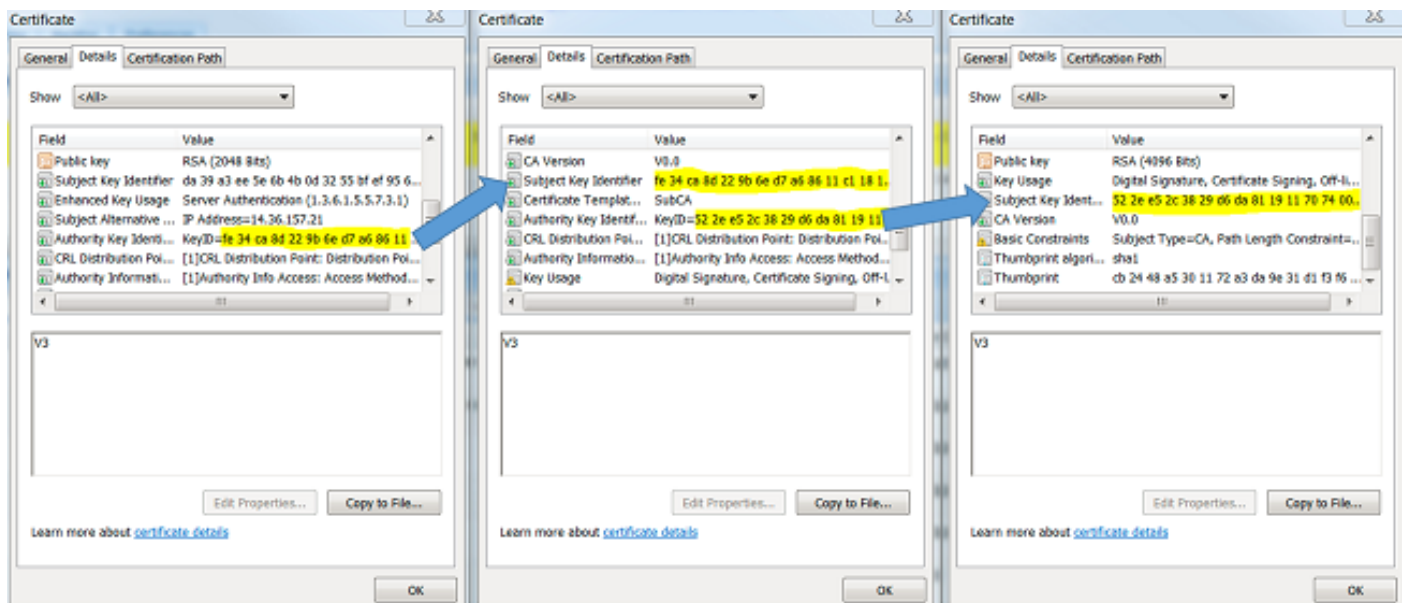
Se a cadeia estiver incompleta, navegue para Administração do ISE > Certificados > Certificados



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.

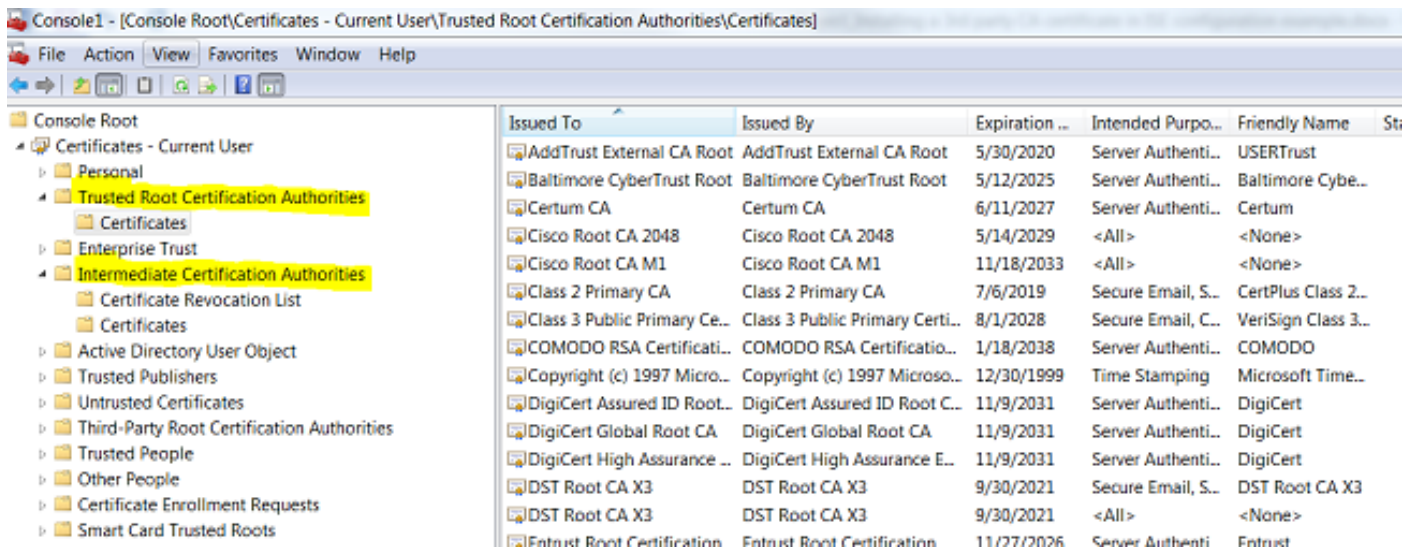


A Cadeia de Certificados ISE está Correta, mas o Ponto de Extremidade Rejeita o Certificado do Servidor ISE durante a Autenticação

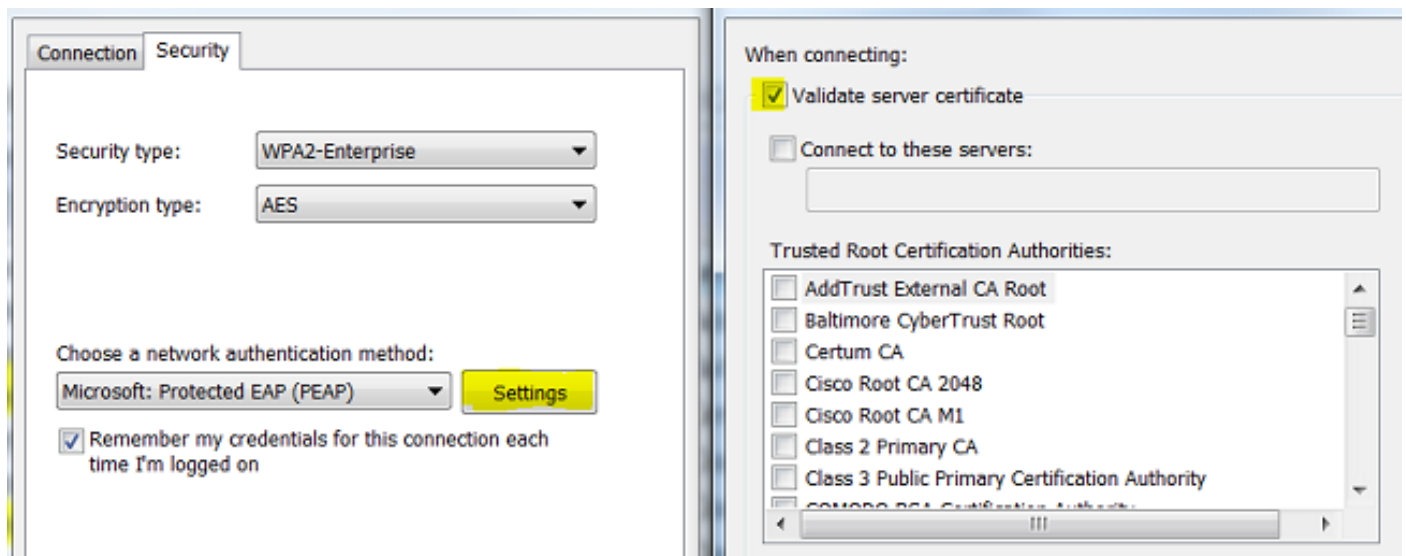
Se o ISE estiver apresentando sua cadeia completa de certificados durante o handshake SSL e o requerente ainda estiver rejeitando a cadeia de certificados; a próxima etapa é verificar se os certificados Raiz e/ou Intermediário estão no Local Trust Store do cliente.

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.



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.



## 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.