

Gerenciar certificados no RV34x Series Router

Objetivo

Um certificado digital certifica a propriedade de uma chave pública pelo assunto nomeado do certificado. Isso permite que as partes confiáveis dependam de assinaturas ou asserções feitas pela chave privada que corresponda à chave pública certificada. Um roteador pode gerar um certificado autoassinado, um certificado criado por um administrador de rede. Pode também enviar pedidos às Autoridades de Certificação (AC) para solicitarem um certificado de identidade digital. É importante ter certificados legítimos de aplicativos de terceiros.

Vamos falar sobre a obtenção de um certificado de uma autoridade de certificação (CA). Uma CA é usada para autenticação. Os certificados são adquiridos de qualquer número de sites de terceiros. É uma forma oficial de provar que seu site é seguro. Essencialmente, a AC é uma fonte confiável que verifica se você é uma empresa legítima e se pode ser confiável. Dependendo das suas necessidades, um certificado a um custo mínimo. Você recebe check-out do CA e, depois que ele verificar suas informações, ele emitirá o certificado para você. Este certificado pode ser baixado como um arquivo em seu computador. Você pode então ir para o roteador (ou servidor VPN) e carregá-lo lá.

O objetivo deste artigo é mostrar como gerar, exportar e importar e certificados no RV34x Series Router.

Dispositivos aplicáveis | Versão do software

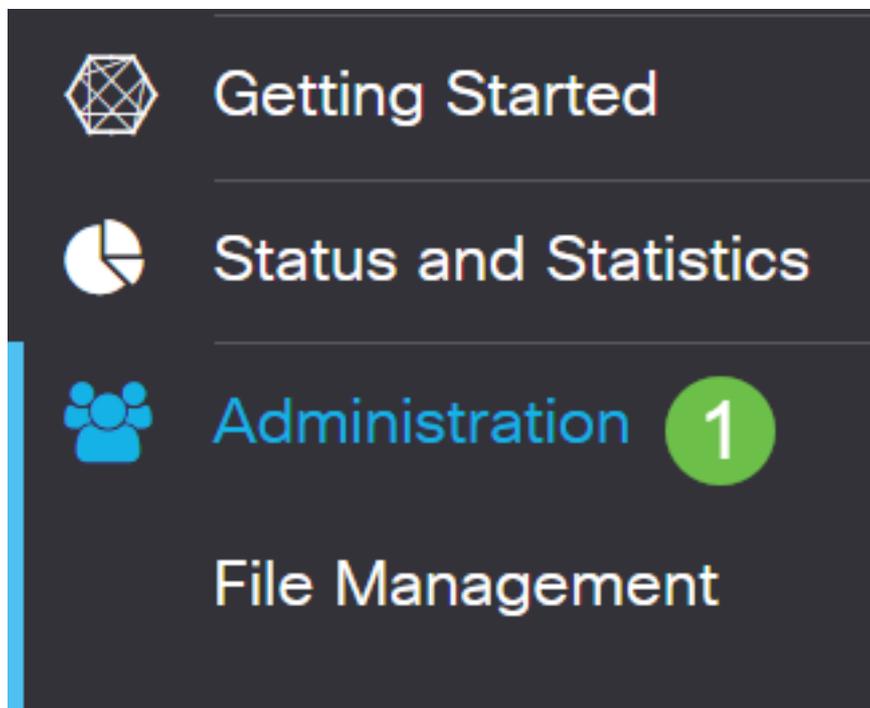
- Série RV34x | 1.0.03.20

Gerenciar certificados no roteador

Gerar CSR/certificado

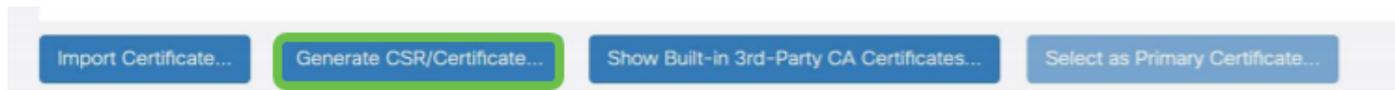
Passo 1

Faça login no utilitário baseado na Web do roteador e escolha **Administration > Certificate**.



Passo 2

Clique em **Gerar CSR/Certificado**. Você será direcionado para a página Gerar CSR/Certificado.



Etapa 3

Preencha as caixas com o seguinte:

- Escolha o tipo de certificado apropriado
 - Certificado de assinatura automática — Este é um certificado SSL (Secure Socket Layer) assinado por seu próprio criador. Este certificado é menos confiável, pois não pode ser cancelado se a chave privada for comprometida de alguma forma por um invasor.
 - Solicitação de assinatura certificada — esta é uma infraestrutura de chave pública (PKI) que é enviada à autoridade de certificação para solicitar um certificado de identidade digital. É mais segura do que autoassinada, já que a chave privada é mantida em segredo.
- Insira um nome para o certificado no campo *Nome do certificado* para identificar a solicitação. Este campo não pode estar em branco nem conter espaços e caracteres especiais.
- (Opcional) Na área Nome alternativo do assunto, clique em um botão de opção. As opções são:
 - Endereço IP — Insira um endereço IP (Internet Protocol [protocolo de Internet])
 - FQDN — Insira um nome de domínio totalmente qualificado (FQDN)
 - E-mail — insira um endereço de e-mail
- No campo *Nome alternativo do assunto*, insira o FQDN.
- Escolha um nome de país no qual sua organização está legalmente registrada na lista suspensa Nome do país.
- Insira um nome ou uma abreviação do estado, província, região ou território onde sua organização está localizada no campo *Estado ou Nome da Província(ST)*.
- Insira um nome da localidade ou cidade em que sua organização está registrada ou localizada no campo *Nome da localidade*.
- Insira um nome com o qual sua empresa está legalmente registrada. Se você estiver se inscrevendo como uma pequena empresa ou como proprietário exclusivo, insira o nome do solicitante de certificado no campo *Nome da organização*. Não é possível usar caracteres especiais.
- Informe um nome no campo *Nome da unidade da organização* para diferenciar divisões dentro de uma organização.
- Digite um nome no campo *Nome comum*. Esse nome deve ser o nome de domínio totalmente qualificado do site para o qual você usa o certificado.
- Insira o endereço de e-mail da pessoa que deseja gerar o certificado.
- Na lista suspensa Tamanho da criptografia de chave, escolha um comprimento de chave. As opções são 512, 1024 e 2048. Quanto maior o comprimento da chave, mais seguro o certificado.
- No campo *Duração válida*, insira o número de dias em que o certificado será válido. O padrão é 360.
- Clique em **Gerar**.

Certificate

2

Generate

Cancel

Generate CSR/Certificate

Type:	<input type="text" value="Self-Signing Certificate"/>
Certificate Name:	<input type="text" value="TestCACertificate"/>
Subject Alternative Name:	<input type="text" value="spprtfrms"/> <input type="radio"/> IP Address <input checked="" type="radio"/> FQDN <input type="radio"/> Email
Country Name(C):	<input type="text" value="US - United States"/>
State or Province Name(ST):	<input type="text" value="Wisconsin"/>
Locality Name(L):	<input type="text" value="Oconomowoc"/>
Organization Name(O):	<input type="text" value="Cisco"/>
Organization Unit Name(OU):	<input type="text" value="Cisco Business"/>
Common Name(CN):	<input type="text" value="cisco.com"/>
Email Address(E):	<input type="text" value="...@cisco.com"/>
Key Encryption Length:	<input type="text" value="2048"/>
Valid Duration:	<input type="text" value="360"/> days (Range: 1-10950, Default: 360)

1

Note: O certificado gerado agora deve aparecer na Tabela de certificados.

Certificate Table

<input type="checkbox"/>	Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
<input type="checkbox"/>	1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
<input type="checkbox"/>	2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
<input type="checkbox"/>	3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
<input type="checkbox"/>	4	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT		

Agora você deve ter criado com êxito um certificado no roteador RV345P.

Exportar um certificado

Passo 1

Na Tabela de certificados, marque a caixa de seleção do certificado que deseja exportar e clique no ícone **exportar**.

Certificate Table

<input type="checkbox"/>	Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
<input type="checkbox"/>	1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
<input type="checkbox"/>	2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
<input type="checkbox"/>	3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
<input checked="" type="checkbox"/>	4	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT		

1 2

Passo 2

- Clique em um formato para exportar o certificado. As opções são:
 - PKCS #12 — Public Key Cryptography Standards (PKCS) #12 é um certificado exportado que vem em uma extensão .p12. Será necessária uma senha para criptografar o arquivo para protegê-lo à medida que for exportado, importado e excluído.

- PEM — O Privacy Enhanced Mail (PEM) é frequentemente usado para servidores Web para que eles possam ser facilmente traduzidos em dados legíveis usando um editor de texto simples, como o notepad.
- Se você escolheu PEM, clique em **Exportar**.
- Digite uma senha para proteger o arquivo a ser exportado no campo *Digitar senha*.
- Digite novamente a senha no campo *Confirmar senha*.
- Na área Selecionar destino, o PC foi escolhido e é a única opção disponível no momento.
- Clique em **Exportar**.

Export Certificate ✕

1

Export as PKCS#12 format

Enter Password

.....

2

Confirm Password

.....

Export as PEM format

Select Destination to Export:

PC

3

4

Export

Cancel

Etapa 3

Uma mensagem indicando o sucesso do download será exibida abaixo do botão Download. Um arquivo começará a ser baixado em seu navegador. Click **OK**.



Success



Ok

Você deve ter exportado com êxito um certificado no Rv34x Series Router.

Importar um certificado

Passo 1

Clique em **Importar certificado...**

Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
4	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT		

Buttons: **Import Certificate...** (highlighted), Generate CSR/Certificate..., Show Built-in 3rd-Party CA Certificates..., Select as Primary Certificate...

Passo 2

- Escolha o tipo de certificado a importar na lista suspensa. As opções são:
 - Certificado local — Um certificado gerado no roteador.
 - Certificado CA — Um certificado certificado certificado por uma autoridade de terceiros confiável que confirmou a exatidão das informações contidas no certificado.
 - Arquivo codificado PKCS #12 — PKCS #12 é um formato de armazenamento de um certificado de servidor.
- Digite um nome para o certificado no campo *Nome do certificado*.
- Se PKCS #12 foi escolhido, digite uma senha para o arquivo no campo *Import Password (Importar senha)*. Caso contrário, vá para o passo 3.
- Clique em uma origem para importar o certificado. As opções são:
 - Importar do PC
 - Importar de USB
- Se o roteador não detectar uma unidade USB, a opção Import from USB (Importar de USB) ficará acinzentada.
- Se você escolheu Importar de USB e seu USB não está sendo reconhecido pelo roteador, clique em Atualizar.
- Clique no botão Escolher arquivo e escolha o arquivo apropriado.
- Clique em **Fazer upload**.

Certificate

3 Upload Cancel

Import Certificate

Type: PKCS#12 encoded file

Certificate Name: cisco 1

Import Password:

Upload certificate file

Import From PC

2 Browse... TestCACertificate

Import From USB

Depois de obter êxito, você será automaticamente levado para a página principal Certificado. A tabela de certificados será preenchida com o certificado importado recentemente.

Certificate Table

^

<input type="checkbox"/>	Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
<input type="checkbox"/>	1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
<input type="checkbox"/>	2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
<input type="checkbox"/>	3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
<input type="checkbox"/>	4	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT		

Você deve ter importado com êxito um certificado no RV34x Series Router.