Gerar e adicionar certificados necessários para a instalação da Secure Endpoint Private Cloud 3.x em diante

Contents

Introduction

Este documento descreve o processo para gerar certificados que precisam ser carregados com cada instalação nova da Secure Console Private Cloud ou para renovar os serviços de certificado instalados.

Prerequisites

Requirements

As informações neste documento são baseadas nestas versões de software e hardware:

- Windows Server 2008
- CentOS 7/8
- Secure Console Virtual Private Cloud 3.0.2 (Posterior)
- OpenSSL 1.1.1

Componentes Utilizados

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Windows Server 2008 (a partir de)
- Instalação da nuvem privada do console seguro
- Infraestrutura de chave pública
- OpenSSL
- CLI do Linux

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.

Informações de Apoio

Com a introdução do Secure Console Private Cloud 3.X, os nomes de host e os pares de certificado/chave são necessários para todos os seguintes serviços:

- Portal de administração
- Autenticação (novo no Private Cloud 3.X)
- Console seguro
- Servidor de disposição
- Servidor de descarte - Protocolo estendido
- Serviço de atualização de disposição
- Firepower Management Center

Este documento é discutido como uma forma rápida de gerar e carregar os certificados necessários. Você pode ajustar cada um dos parâmetros, incluindo o algoritmo de hash, o tamanho da chave e outros, de acordo com a política da empresa, e o mecanismo de geração desses certificados pode não corresponder ao que está detalhado aqui.

> **Aviso**: o procedimento mencionado abaixo pode variar de acordo com a configuração do servidor de CA. Espera-se que o servidor de CA de sua escolha já esteja provisionado e a configuração do mesmo tenha sido concluída. A nota técnica a seguir descreve apenas um exemplo de geração de certificados e o Cisco TAC não está envolvido na solução de problemas relacionados à geração de certificados e/ou problemas do servidor de CA de qualquer tipo.

Criação de certificado

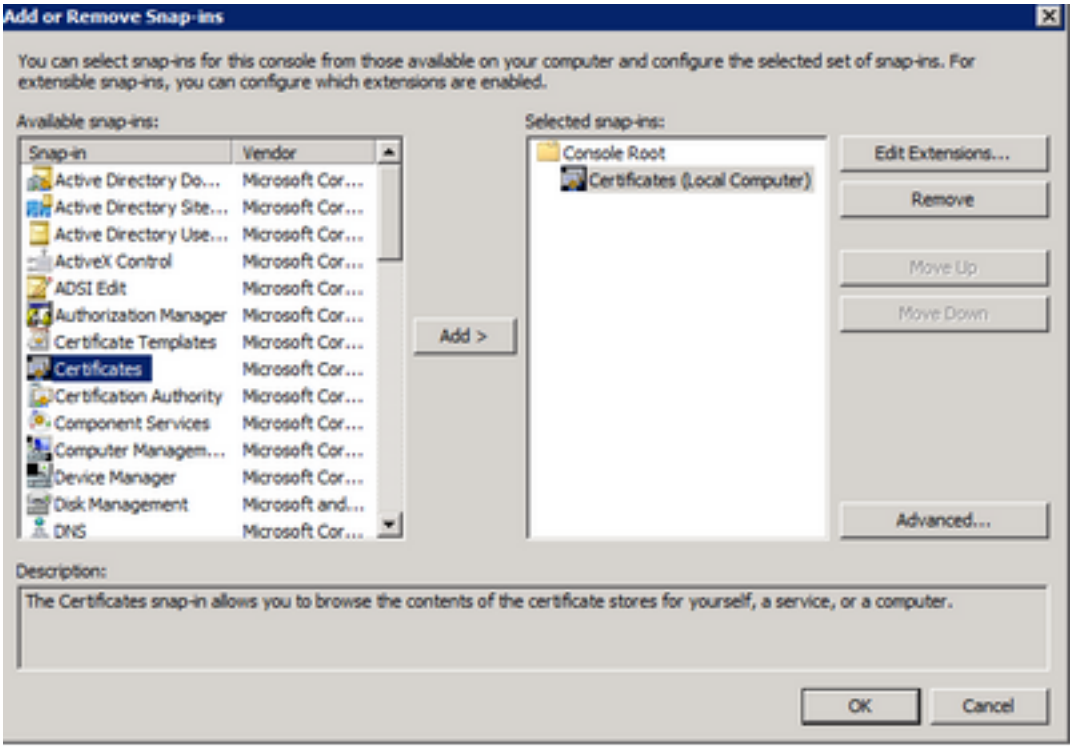
Gerar certificados no servidor Windows

Verifique se as funções a seguir estão instaladas e configuradas no Windows Server.

- Serviços de Certificados do Ative Diretory
- Autoridade de certificação
- Registro na Web de Autoridade de Certificação
- Respondente Online
- Serviço Web de Registro de Certificado
- Serviço Web de Diretiva de Registro de Certificado
- Serviços de Domínio Ative Diretory
- Servidores DNS
- Servidor Web (IIS)

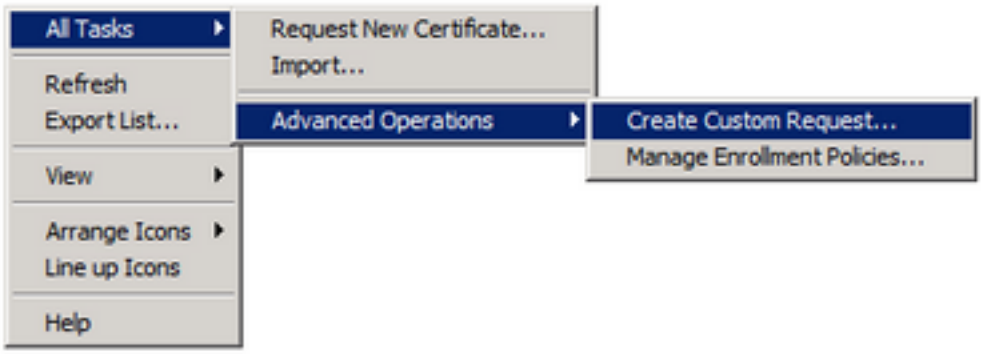
Gerar uma CSR (Certificate Signing Request, solicitação de assinatura de certificado)

Etapa 1. Navegue até o console MMC e adicione o snap-in Certificados para sua conta de computador como mostrado na imagem aqui.

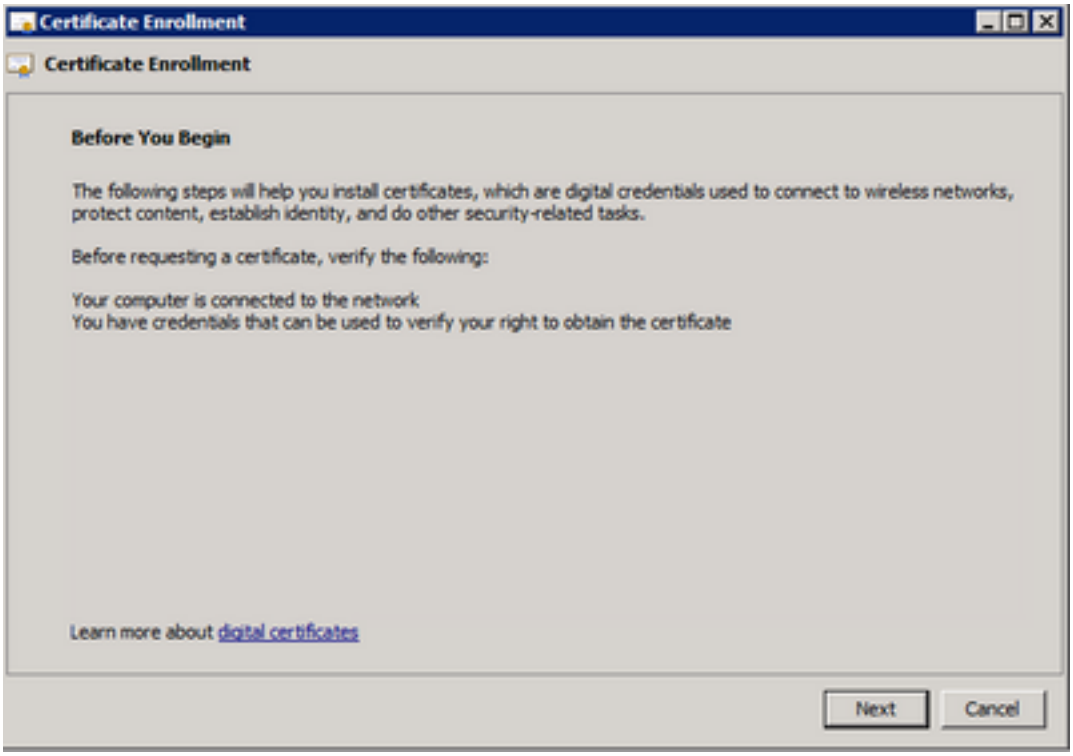


Etapa 2. Aprofunde **Certificados (Computador Local) > Pessoal > Certificados**.

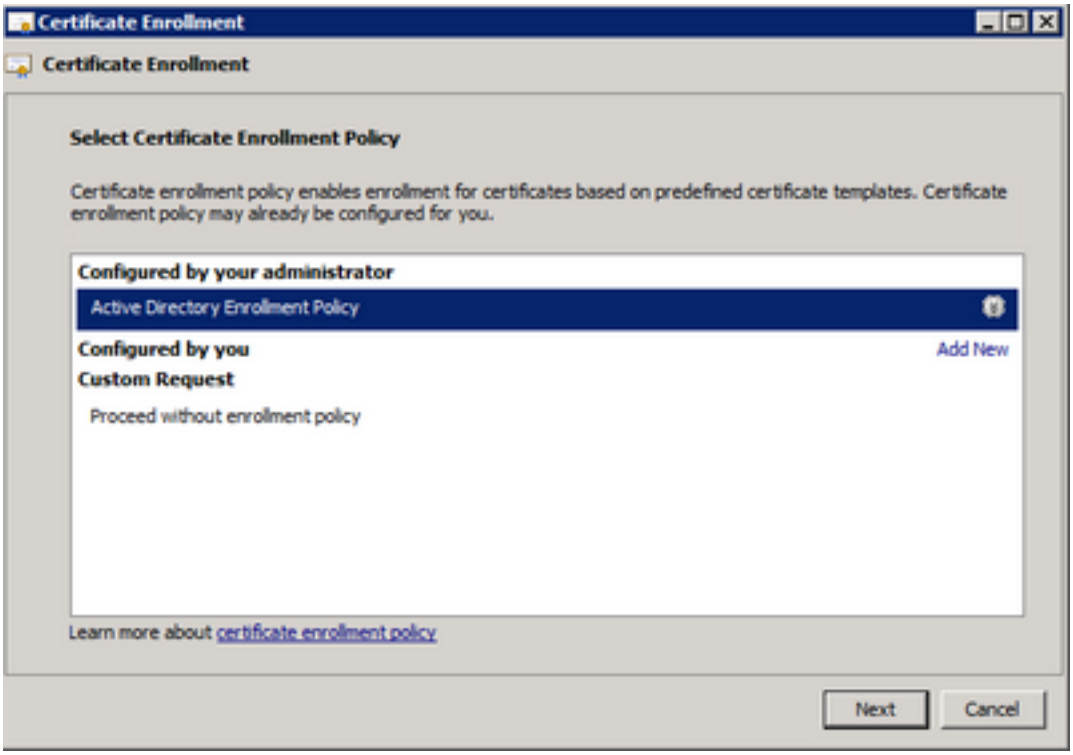
Etapa 3. Clique com o botão direito do mouse no espaço vazio e selecione **All Tasks > Advanced Operations > Create Custom Request.**



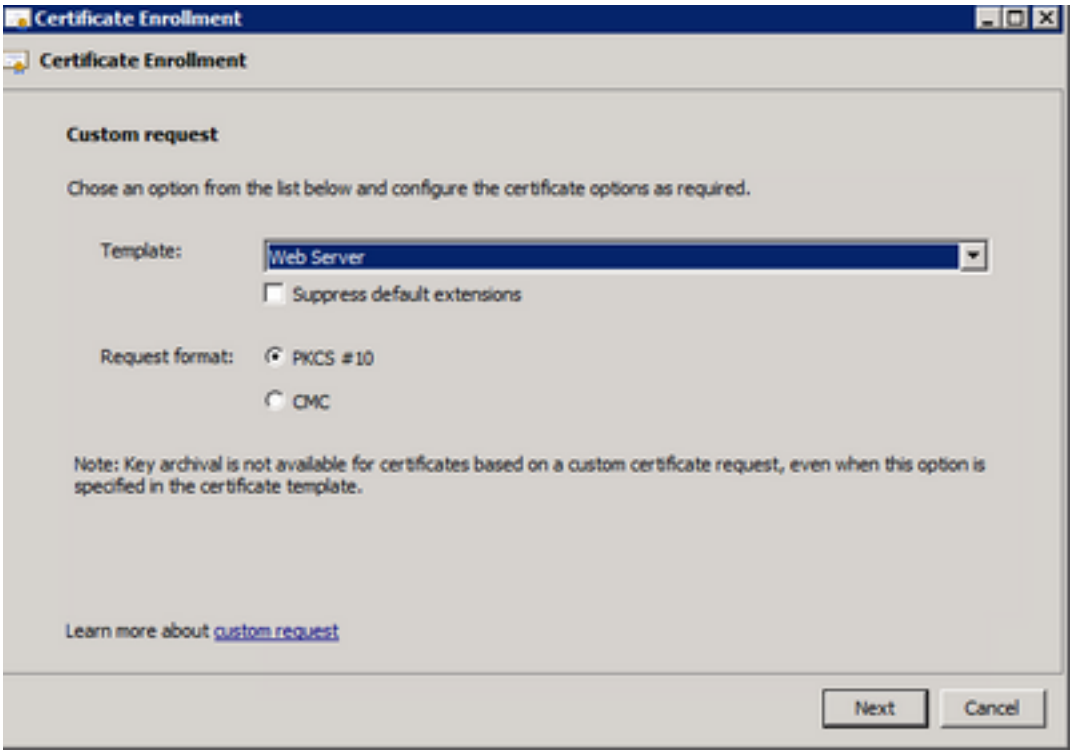
Etapa 4. Selecione **Próximo** na janela Inscrição.



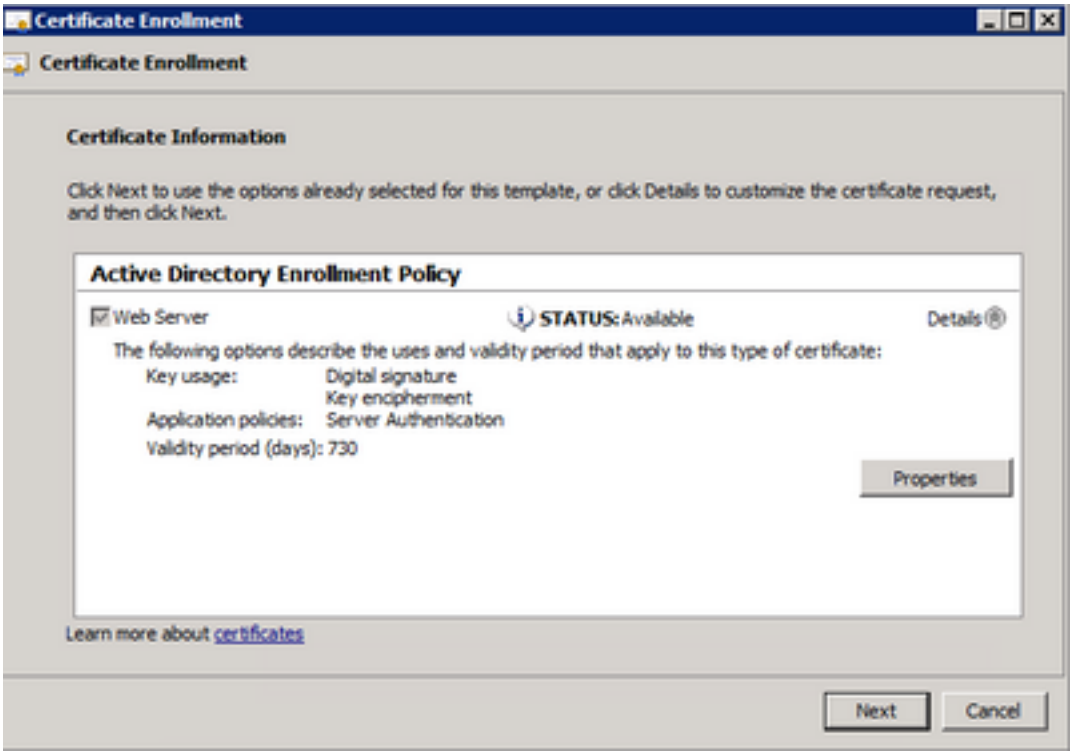
Etapa 5. Selecione sua política de registro de certificado e selecione **Avançar**.



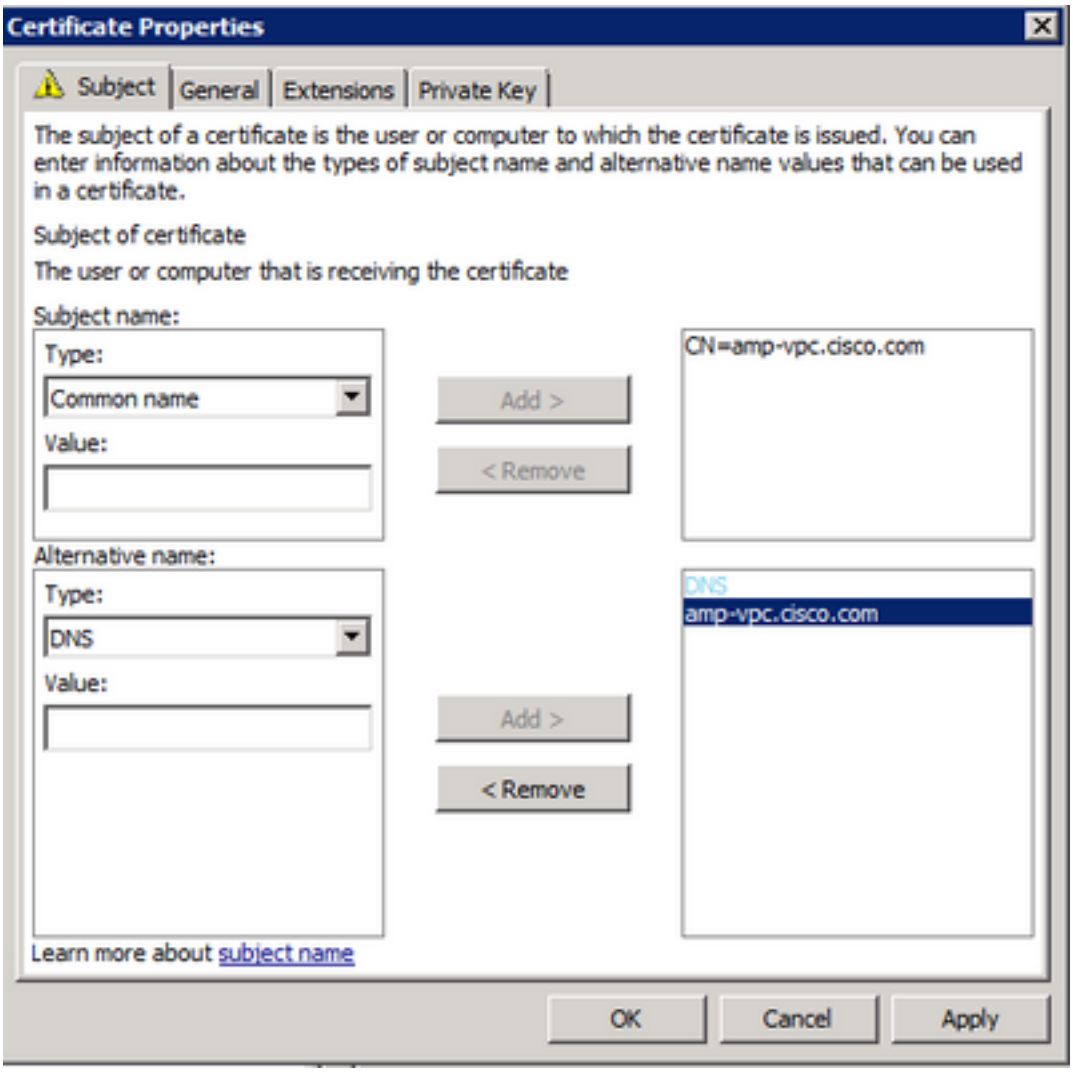
Etapa 6. Escolha o modelo como **Servidor Web** e selecione **Próximo**.



Passo 7. Se o seu modelo de "Servidor Web" tiver sido configurado corretamente e estiver disponível para inscrição, o status Disponível será exibido. Selecione **Details** para expandir Properties.

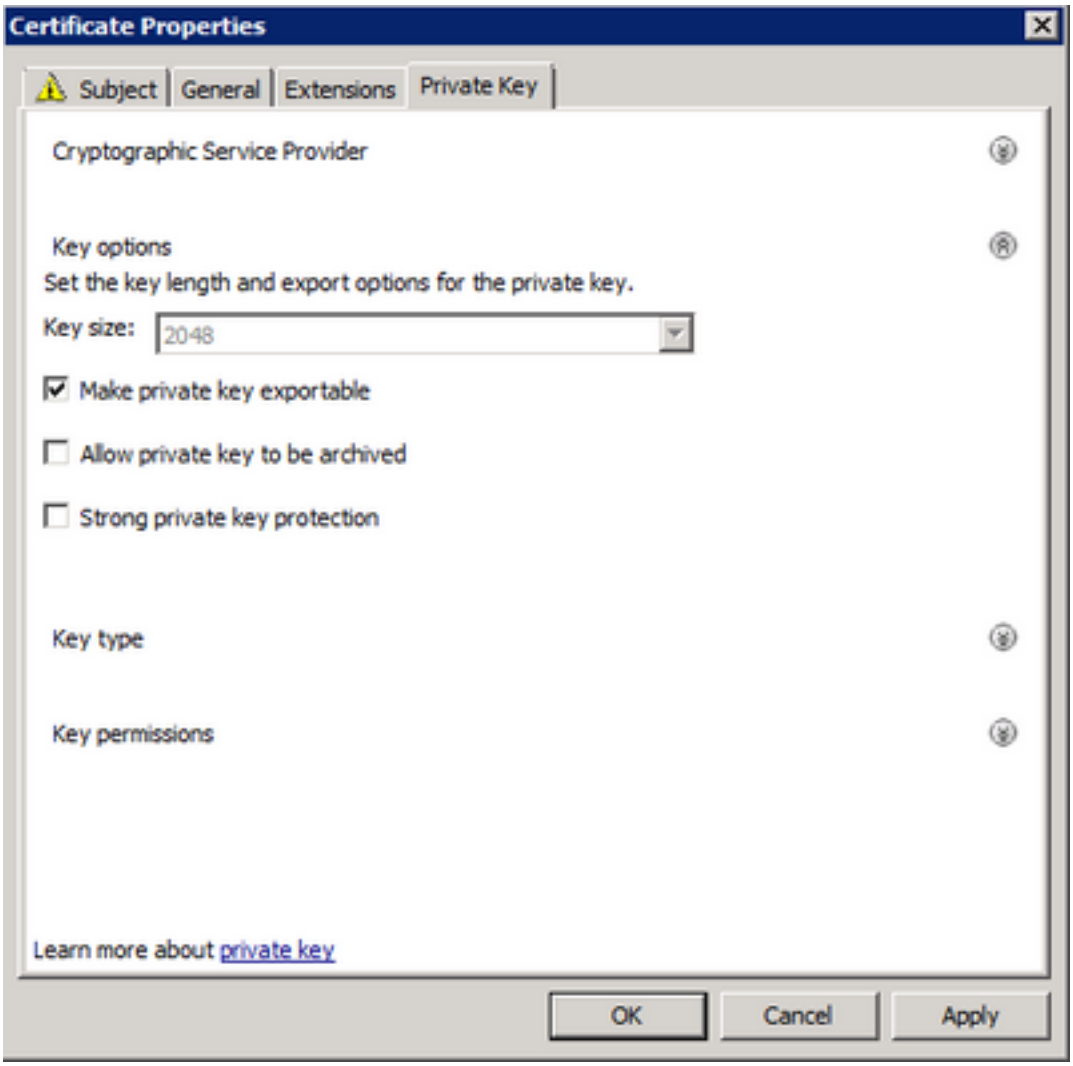


Etapa 8. No mínimo, adicione os atributos CN e DNS. O restante dos atributos pode ser adicionado de acordo com seus requisitos de segurança.



Etapa 9. Como opção, forneça um Nome Amigável na guia **Geral**.

Etapa 10. Selecione na guia **Private** Key e verifique se você está habilitando a opção **Make private key exportable na seção** Key Options**.**

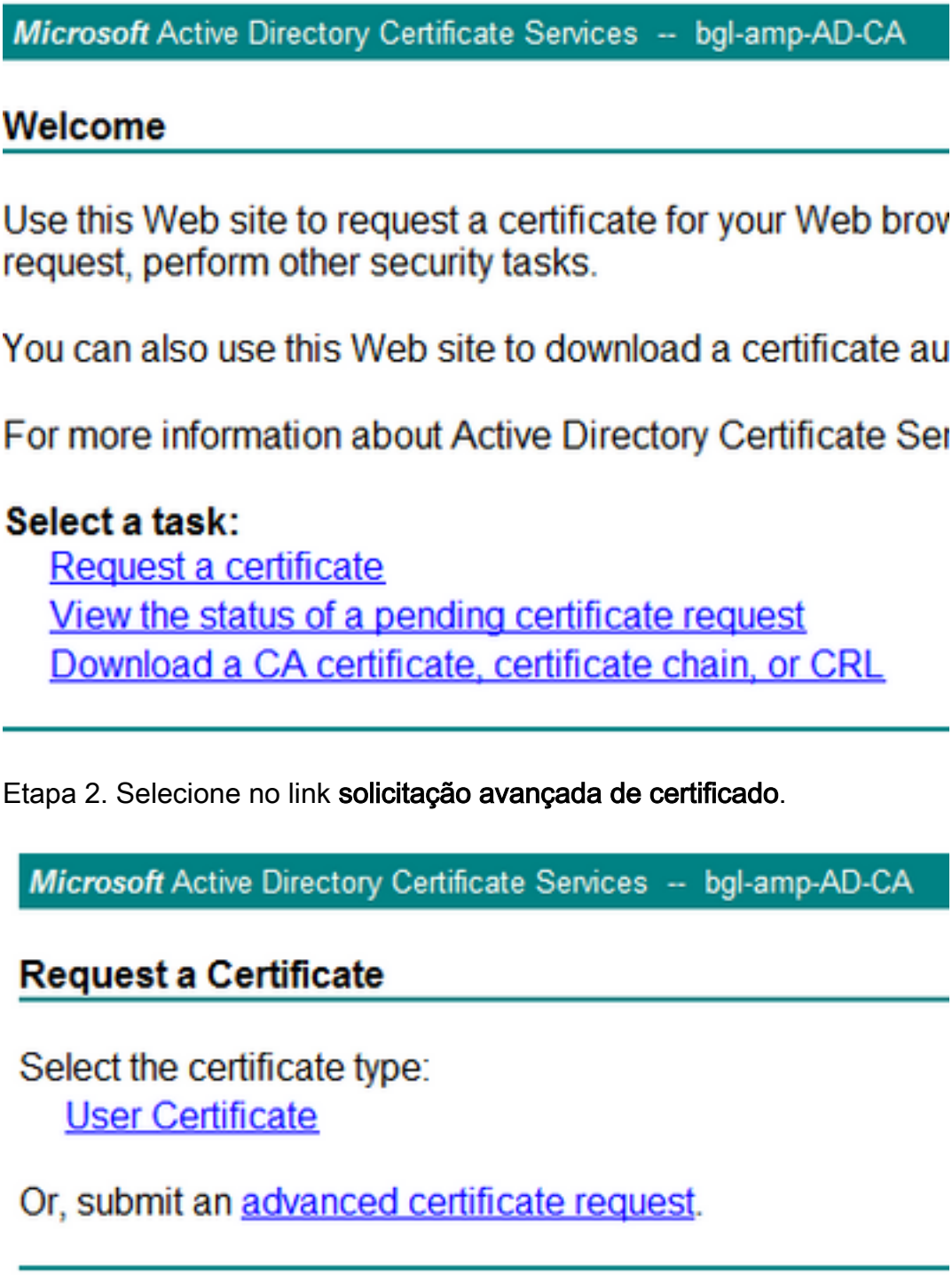


Etapa 11. Por fim, selecione **OK**. Isso deve levá-lo à caixa de diálogo Inscrição de certificado, na qual você pode selecionar **Próximo**.

Etapa 12. Navegue até um local para salvar o arquivo .req que é enviado ao servidor de CA para assinatura.

Enviando o CSR para a CA e gerando o certificado

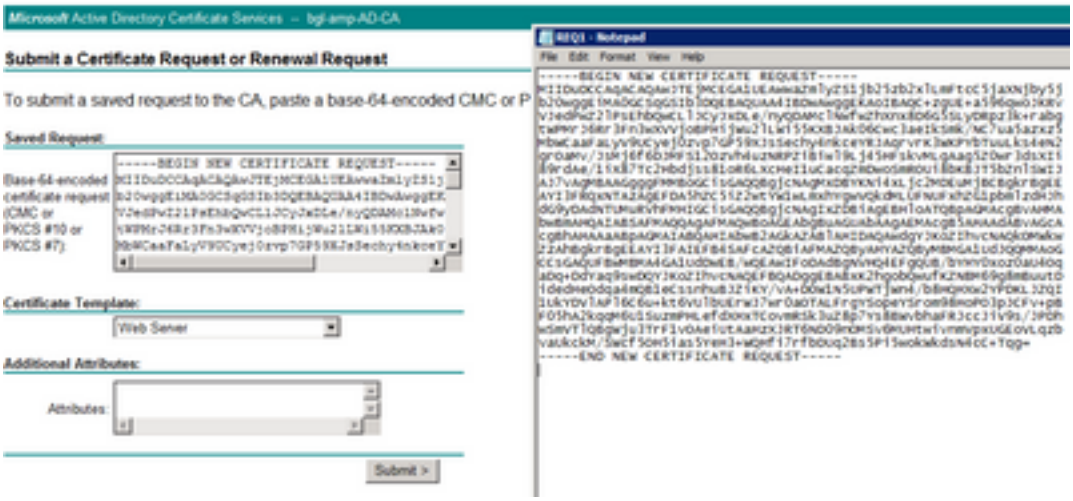
Etapa 1. Navegue até a página da Web Serviços de Certificados do MS AD conforme abaixo e selecione **Solicitar um Certificado**.



Etapa 2. Selecione no link **solicitação avançada de certificado**.

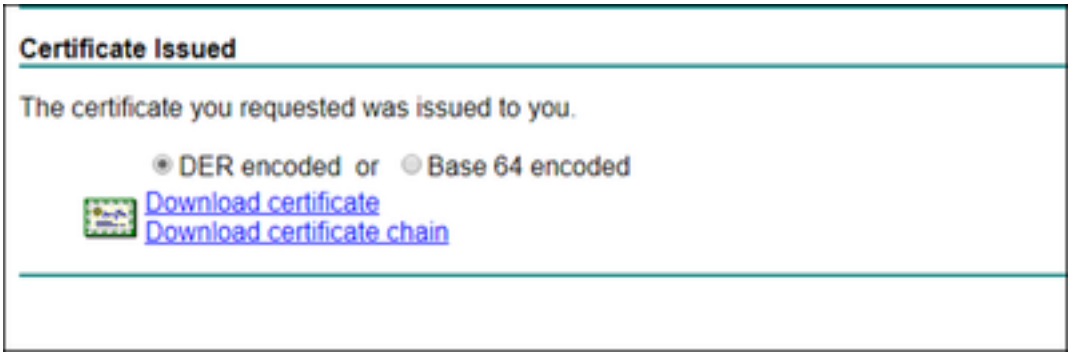
Etapa 3. Selecione on **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file (Enviar uma solicitação de certificado usando um arquivo de #7 PKCS codificado na base 64) ou envie uma solicitação de renovação usando um arquivo de PKCS codificado na base 64**.

Etapa 4. Abra o conteúdo do arquivo .req (CSR) salvo anteriormente no Bloco de Notas. Copie o conteúdo e cole-o aqui. Verifique se o Modelo de Certificado está selecionado como **Servidor Web**



Etapa 5. Por fim, selecione **Enviar**.

Etapa 6. Neste ponto, você deve ser capaz de **baixar** o certificado, como mostrado na imagem.



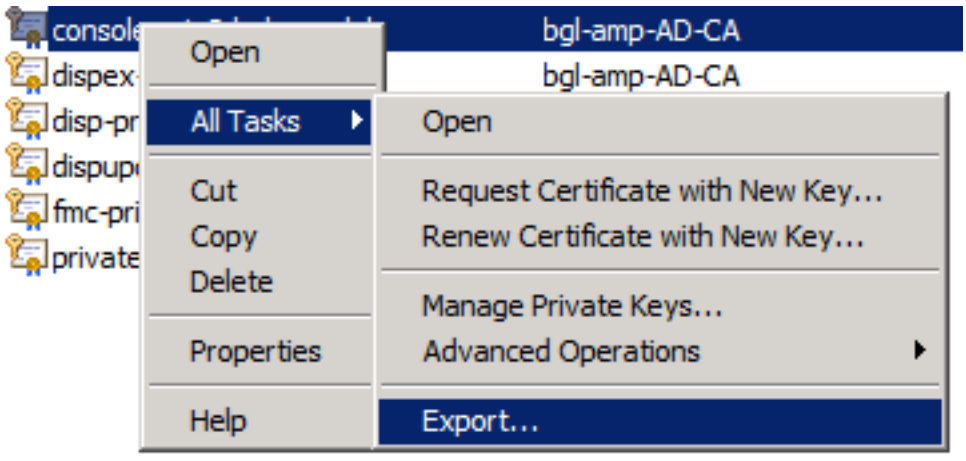
Exportando a chave privada e convertendo para o formato PEM

Etapa 1. Instale o certificado no Repositório de Certificados abrindo o arquivo .cer e selecione **Instalar Certificado**.

Etapa 2. Navegue até o snap-in do MMC que foi selecionado anteriormente.

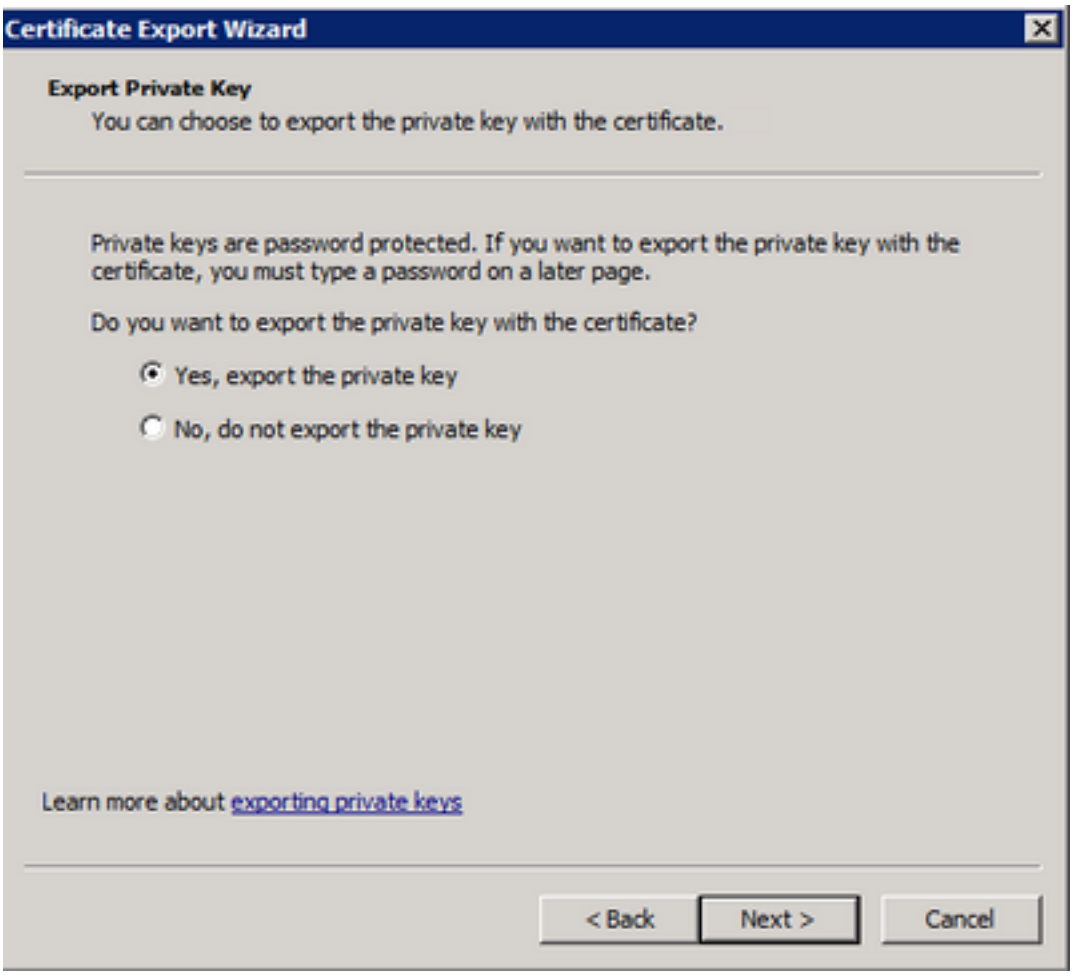
Etapa 3. Navegue até o armazenamento onde o certificado foi instalado.

Etapa 4. Clique com o botão direito do mouse no certificado correto, selecione **All Tasks > Export**.



Etapa 5. No Assistente para Exportação de Certificados, confirme a exportação da chave privada,

conforme mostrado na imagem.



Etapa 6. Insira uma senha e selecione **Avançar** para salvar a chave privada no disco.

Passo 7. Isso salva a chave privada no formato .PFX. No entanto, ela precisa ser convertida no formato .PEM para usá-la com a Nuvem Privada de Ponto de Extremidade Seguro.

Etapa 8. Instalar bibliotecas OpenSSL.

Etapa 9. Abra uma janela do prompt de comando e mude para o diretório onde você instalou o OpenSSL.

Etapa 10. Execute o seguinte comando para extrair a chave privada e salvá-la em um novo arquivo: (Se o seu arquivo PFX não estiver no mesmo caminho em que a biblioteca OpenSSL está armazenada, você terá que especificar o caminho exato junto com o nome do arquivo)

```
openssl pkcs12 -in yourpfxfile.pfx -nocerts -out privatekey.pem -nodes
```

Etapa 11. Agora, execute o seguinte comando para também extrair o certificado público e salvá-lo em um novo arquivo:

```
openssl pkcs12 -in yourpfxfile.pfx -nokeys -out publiccert.pem -nodes
```

Gerar Certificado no Servidor Linux (Verificação SSL estrita DESABILITADA)

Observação: a verificação TLS rigorosa verifica se o certificado atende aos requisitos TLS da Apple. Consulte o Guia do administrador para obter mais informações.

Verifique se o servidor Linux para o qual você está tentando gerar os certificados necessários tem as bibliotecas OpenSSL 1.1.1 instaladas. Verificando se este e o procedimento listado abaixo podem variar da distribuição Linux que você está executando. Esta parte foi documentada, como feito em um servidor CentOS 8.4.

Gerar RootCA com assinatura automática

Etapa 1. Gere a chave privada para o certificado de CA raiz.

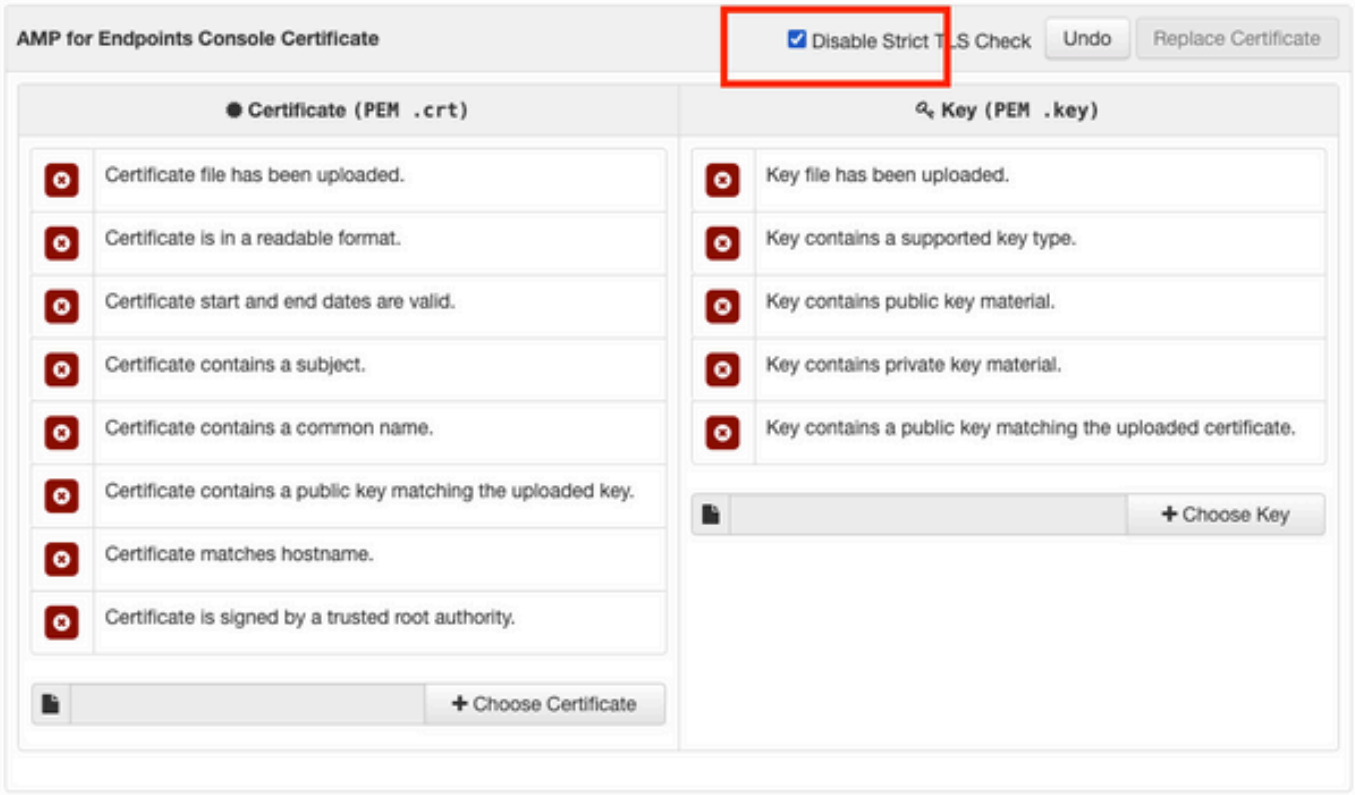
```
openssl genrsa -out
```

Etapa 2. Gerar o certificado CA.

```
openssl req \
-subj '/CN=
-addext "extendedKeyUsage = serverAuth, clientAuth" \
-outform pem -out
-key
-days "1000"
```

Gerar um certificado para cada serviço

Crie o certificado para o serviço de Autenticação, Console, Disposição, Disposição estendida, Servidor de atualização, Firepower Management Center (FMC) de acordo com a entrada de nome DNS. Você precisa repetir o processo de geração de certificado abaixo para cada serviço (Autenticação, Console etc.).



Gerar chave privada

```
openssl genrsa -out
```

Substitua <YourServiceName.key> pelo novo nome de arquivo KEY a ser criado como Auth-Cert.key

Gerar CSR

```
openssl req -new \
-subj '/CN=
-key
```

Substitua o <YourServiceName.key> com o arquivo de certificado KEY atual (ou novo) como Auth-Cert.key

Substitua <YourServiceName.csr> pelo nome de arquivo CSR a ser criado, como Auth-Cert.crt

Gerar certificado

```
openssl x509 -req \
-in
-CAkey
-days 397 -sha256
```

Substitua <YourServiceName.csr> por um CSR de certificado real (ou novo), como Auth-Cert.csr

Substitua <YourRootCAName.pem> por um nome de arquivo PEM real (ou novo) como RootCAName.pem

Substitua <YourServiceName.key> pelo arquivo de certificado KEY atual (ou novo), como Auth-Cert.key

Substitua <YourServiceName.crt> pelo nome de arquivo a ser criado, como Auth-Cert.crt

Gerar Certificado no Servidor Linux (Verificação SSL estrita HABILITADA)

> **Observação**: a verificação TLS rigorosa verifica se o certificado atende aos requisitos TLS da Apple. Consulte o Guia do administrador para obter mais informações.

Gerar RootCA com assinatura automática

Etapa 1. Gere a chave privada para o certificado de CA raiz.

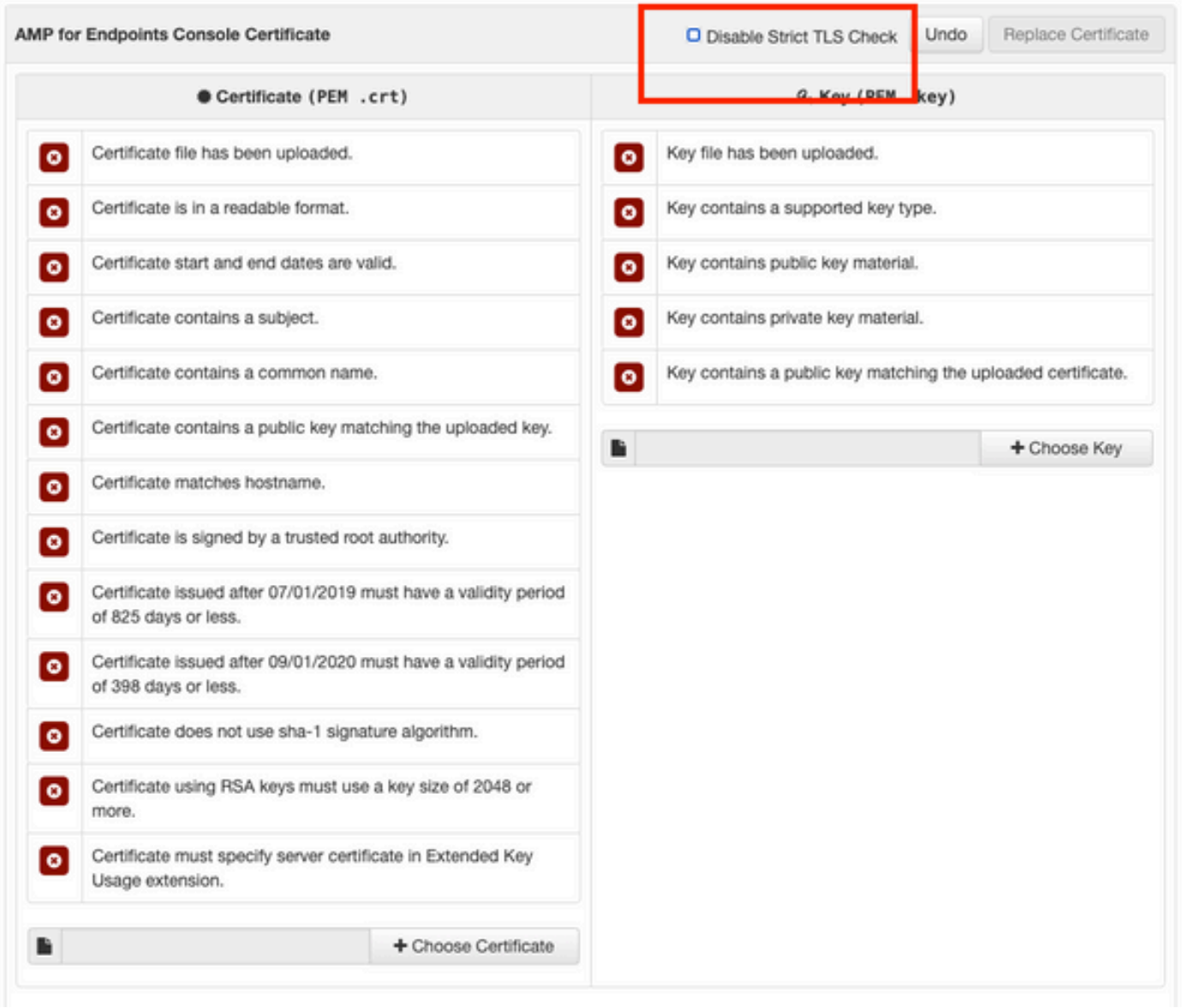
```
openssl genrsa -out
```

Etapa 2. Gerar o certificado CA.

```
openssl req \
-subj '/CN=
-outform pem -out
-key
-days "1000"
```

Gerar um certificado para cada serviço

Crie o certificado para o serviço de Autenticação, Console, Disposição, Disposição estendida, Servidor de atualização, Firepower Management Center (FMC) de acordo com a entrada de nome DNS. Você precisa repetir o processo de geração de certificado abaixo para cada serviço (Autenticação, Console etc.).



Crie um arquivo de Configuração de Extensões e salve-o (extensions.cnf)

```
[v3_ca]
basicConstraints = CA:FALSE
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = critical, serverAuth, clientAuth
```

Gerar chave privada

```
openssl genrsa -out
```

Substitua <YourServiceName.key> por um novo nome de arquivo KEY a ser criado como Auth-Cert.key

Gerar CSR

```
openssl req -new \
-key
-subj '/CN=
-out
```

Substitua o <YourServiceName.key> com a CHAVE de certificado atual (ou nova), como Auth-Cert.key

Substitua <YourServiceName.csr> pelo CSR de certificado atual (ou novo), como Auth-Cert.csr

Gerar certificado

```
openssl x509 -req -in
-CA
-CAcreateserial -out
-extensions v3_ca -extfile extensions.cnf \
-days 397 -sha256
```

Substitua <YourServiceName.csr> pelo CSR de certificado atual (ou novo), como Auth-Cert.csr

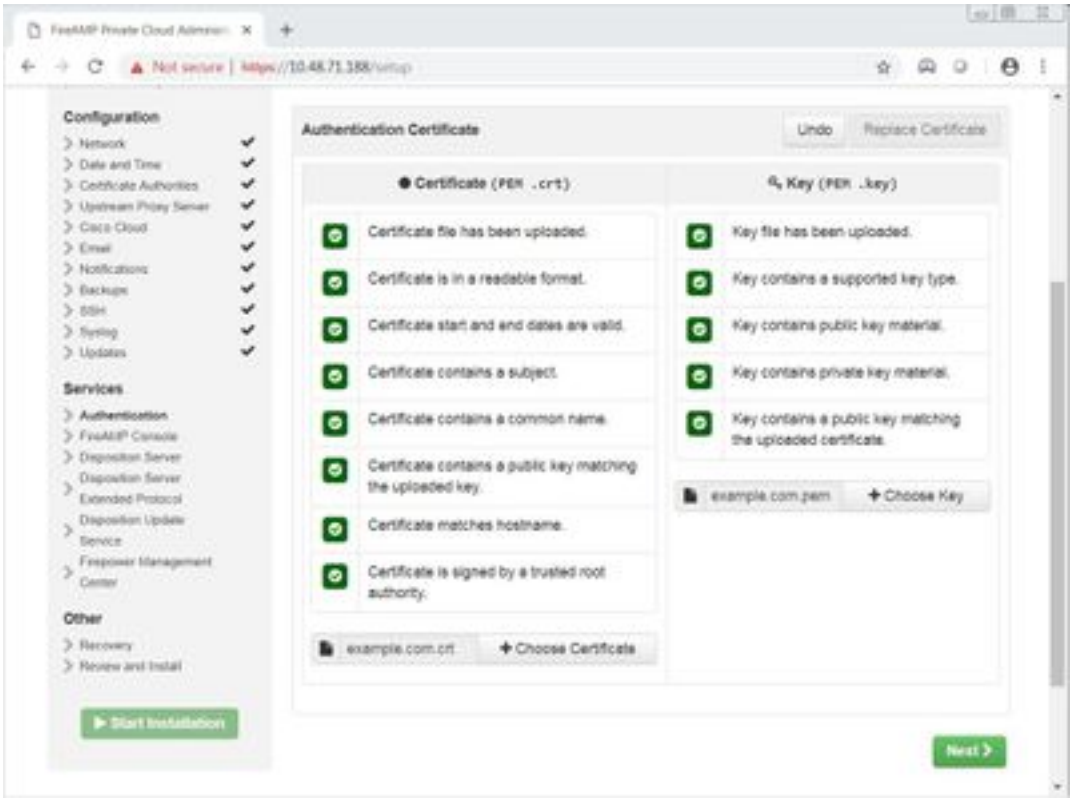
Substitua <YourRootCAName.pem> pelo nome de arquivo PEM atual (ou novo) como RootCAName.pem

Substitua <YourServiceName.key> pelo arquivo de certificado KEY atual (ou novo), como Auth-Cert.key

Substitua <YourServiceName.crt> pelo nome de arquivo a ser criado, como Auth-Cert.crt

Adicionando os certificados à nuvem privada do console seguro

Etapa 1. Quando os certificados forem gerados a partir de qualquer um dos métodos acima, carregue o certificado correspondente para cada um dos serviços. Se eles foram gerados corretamente, todas as marcas de seleção são ativadas conforme ilustrado na imagem aqui.



Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

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.