# Use certificados

SANtricity 11.7

NetApp
February 13, 2025

# Índice

Use certificados . . . 1
Use certificados assinados pela CA para controladores . . . 1
Repor certificados de gestão . . . 4
Exibir informações de certificado importadas . . . 4
Importar certificados para controladores quando atua como clientes . . . 5
Ativar verificação de revogação de certificado . . . 6
Excluir certificados confiáveis . . . 6
Use certificados assinados pela CA para autenticação com um servidor de gerenciamento de chaves . . . 7
Exportar certificados do servidor de gerenciamento de chaves . . . 9

# Use certificados

## Use certificados assinados pela CA para controladores

Você pode obter certificados assinados pela CA para comunicações seguras entre os controladores e o navegador usado para acessar o System Manager.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Você deve saber o endereço IP ou os nomes DNS de cada controlador.

**Sobre esta tarefa**

O uso de certificados assinados pela CA é um procedimento de três etapas.

### Etapa 1: Conclua CSRs para os controladores

Primeiro, você deve gerar um arquivo de solicitação de assinatura de certificado (CSR) para cada controlador no storage de armazenamento.

**Sobre esta tarefa**

Esta tarefa descreve como gerar um ficheiro CSR a partir do System Manager. O CSR fornece informações sobre a sua organização e o endereço IP ou o nome DNS do controlador. Durante esta tarefa, um arquivo CSR é gerado se o storage array tiver um controlador e dois arquivos CSR se tiver dois controladores.

> Alternativamente, você pode gerar um arquivo CSR usando uma ferramenta como OpenSSL e pode pular para Passo 2: Envie os arquivos CSR.

**Passos**

1. Selecione **Definições › certificados**.
2. Na guia Gerenciamento de matrizes, selecione **Complete CSR**.

> Se você vir uma caixa de diálogo solicitando que você aceite um certificado autoassinado para o segundo controlador, clique em **aceitar certificado autoassinado** para continuar.

3. Insira as seguintes informações e clique em **Next**:
   - **Organização** — o nome completo e legal de sua empresa ou organização. Inclua sufixos, como Inc. Ou Corp.
   - * Unidade organizacional (opcional) * — a divisão da sua organização que está a lidar com o certificado.
   - **Cidade/localidade** — a cidade onde seu storage array ou negócio está localizado.
   - **Estado/região (opcional)** — o estado ou a região onde o storage ou a empresa está localizado.
   - **Código ISO do país** — o código ISO de dois dígitos do seu país (Organização Internacional para Padronização), como os EUA.

Alguns campos podem ser pré-preenchidos com as informações apropriadas, como o endereço IP do controlador. Não altere valores pré-preenchidos a menos que você tenha certeza de que eles estão incorretos. Por exemplo, se você ainda não concluiu um CSR, o endereço IP do controlador é definido como ""localhost". Neste caso, você deve alterar ""localhost"" para o nome DNS ou endereço IP do controlador.

4. Verifique ou insira as seguintes informações sobre o controlador A no storage array:
   - **Controller Um nome comum** — o endereço IP ou o nome DNS do controlador A é exibido por padrão. Certifique-se de que este endereço está correto; ele deve corresponder exatamente ao que você digita para acessar o System Manager no navegador. O nome DNS não pode começar com um curinga.
   - **Controller Um endereço IP alternativo** — se o nome comum for um endereço IP, você pode opcionalmente inserir quaisquer endereços IP adicionais ou aliases para o controlador A. para várias entradas, use um formato delimitado por vírgulas.
   - **Controller (controlador) De nomes DNS alternativos** — se o nome comum for um nome DNS, insira quaisquer nomes DNS adicionais para o controlador A. para várias entradas, use um formato delimitado por vírgulas. Se não houver nomes DNS alternativos, mas você inseriu um nome DNS no primeiro campo, copie esse nome aqui. O nome DNS não pode começar com um curinga. Se a matriz de armazenamento tiver apenas um controlador, o botão **Finish** estará disponível.

     Se a matriz de armazenamento tiver dois controladores, o botão **Next** estará disponível.

Não clique no link **Ignorar esta etapa** quando você estiver criando inicialmente uma solicitação CSR. Este link é fornecido em situações de recuperação de erros. Em casos raros, uma solicitação CSR pode falhar em um controlador, mas não no outro. Este link permite que você ignore a etapa para criar uma solicitação CSR no controlador A, se já estiver definida, e continue para a próxima etapa para recriar uma solicitação CSR no controlador B.

5. Se houver apenas um controlador, clique em **Finish**. Se houver dois controladores, clique em **Next** para inserir informações para o controlador B (o mesmo que acima) e, em seguida, clique em **Finish**.

   Para um único controlador, um ficheiro CSR é transferido para o seu sistema local. Para controladores duplos, são transferidos dois ficheiros CSR. A localização da pasta do download depende do seu navegador.

6. Vá para Passo 2: Envie os arquivos CSR.

## Passo 2: Envie os arquivos CSR

Depois de criar os arquivos de solicitação de assinatura de certificado (CSR), envie os arquivos para uma autoridade de certificação (CA). Os sistemas e-Series exigem o formato PEM (codificação ASCII Base64) para certificados assinados, que inclui os seguintes tipos de arquivo: pem, .crt, .cer ou .key.

**Passos**

1. Localize os ficheiros CSR transferidos.
2. Envie os arquivos CSR para uma CA (por exemplo, VeriSign ou DigiCert) e solicite certificados assinados no formato PEM.

**Depois de enviar um arquivo CSR para a CA, NÃO regenere outro arquivo CSR.** Sempre que você gera um CSR, o sistema cria um par de chaves privadas e públicas. A chave pública faz parte da CSR, enquanto a chave privada é mantida no keystore do sistema. Quando você recebe os certificados assinados e os importa, o sistema garante que as chaves privadas e públicas sejam o par original. Se as chaves não corresponderem, os certificados assinados não funcionarão e você deverá solicitar novos certificados à CA.

3. Quando a CA retornar os certificados assinados, vá para Etapa 3: Importar certificados assinados para controladores.

## Etapa 3: Importar certificados assinados para controladores

Depois de receber certificados assinados da Autoridade de Certificação (CA), importe os arquivos para os controladores.

**Antes de começar**

- A CA retornou arquivos de certificado assinados. Esses arquivos incluem o certificado raiz, um ou mais certificados intermediários e os certificados do servidor.
- Se a CA forneceu um arquivo de certificado encadeado (por exemplo, um arquivo .p7b), você deve descompactar o arquivo encadeado em arquivos individuais: O certificado raiz, um ou mais certificados intermediários e os certificados de servidor que identificam os controladores. Você pode usar o utilitário Windows `certmgr` para descompactar os arquivos (clique com o botão direito do Mouse e selecione **todas as tarefas › Exportar**). A codificação base-64 é recomendada. Quando as exportações estiverem concluídas, um arquivo CER é exibido para cada arquivo de certificado na cadeia.
- Você copiou os arquivos de certificado para o sistema host onde você acessa o System Manager.

**Passos**

1. Selecione o **Configurações › certificados**
2. Na guia Gerenciamento de matrizes, selecione **Importar**.

   Abre-se uma caixa de diálogo para importar o(s) ficheiro(s) de certificado.

3. Clique nos botões **Browse** para selecionar primeiro os arquivos de certificado raiz e intermediário e, em seguida, selecione cada certificado de servidor para os controladores. Os arquivos raiz e intermediário são os mesmos para ambos os controladores. Apenas os certificados de servidor são exclusivos para cada controlador. Se você gerou o CSR a partir de uma ferramenta externa, você também deve importar o arquivo de chave privada que foi criado juntamente com o CSR.

   Os nomes dos arquivos são exibidos na caixa de diálogo.

4. Clique em **Importar**.

   Os arquivos são carregados e validados.

**Resultado**

A sessão é terminada automaticamente. Você deve fazer login novamente para que os certificados entrem em vigor. Quando você faz login novamente, os novos certificados assinados pela CA são usados para sua sessão.

# Repor certificados de gestão

Você pode reverter os certificados nos controladores de usar certificados assinados pela CA de volta para os certificados autoassinados definidos de fábrica.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Os certificados assinados pela CA devem ser importados anteriormente.

**Sobre esta tarefa**

A função Redefinir exclui os arquivos de certificado assinados pela CA atuais de cada controlador. Em seguida, os controladores reverterão para o uso de certificados autoassinados.

**Passos**

1. Selecione **Definições › certificados**.
2. Na guia Gerenciamento de matrizes, selecione **Redefinir**.

   Uma caixa de diálogo confirmar certificados de Gerenciamento é aberta.

3. Digite `reset` o campo e clique em **Reset**.

   Após a atualização do navegador, o navegador pode bloquear o acesso ao site de destino e informar que o site está usando HTTP Strict Transport Security. Essa condição surge quando você volta para certificados autoassinados. Para limpar a condição que está bloqueando o acesso ao destino, você deve limpar os dados de navegação do navegador.

**Resultados**

Os controladores revertem para o uso de certificados autoassinados. Como resultado, o sistema solicita aos usuários que aceitem manualmente o certificado autoassinado para suas sessões.

# Exibir informações de certificado importadas

Na página certificados, você pode exibir o tipo de certificado, a autoridade emissora e o intervalo de datas válido de certificados para o storage array.

**Antes de começar**

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.

**Passos**

1. Selecione **Definições › certificados**.
2. Selecione uma das guias para exibir informações sobre os certificados.

| Separador | Descrição |
| --- | --- |
| Gerenciamento de array | Exibir informações sobre os certificados assinados pela CA importados para cada controlador, incluindo o arquivo raiz, o(s) arquivo(s) intermediário(s) e o(s) arquivo(s) do servidor. |
| Confiável | Exibir informações sobre todos os outros tipos de certificados importados para os controladores. Use o campo de filtro em **Mostrar certificados que são…** para exibir certificados instalados pelo usuário ou pré-instalados.<br>• **User-Installed** — certificados que um usuário carregou no storage array, que podem incluir certificados confiáveis quando o controlador atua como cliente (em vez de um servidor), certificados LDAPS e certificados de Federação de identidade.<br>• **Pré-instalado** — certificados autoassinados incluídos com a matriz de armazenamento. |
| Gerenciamento de chaves | Exibir informações sobre os certificados assinados pela CA importados para um servidor de gerenciamento de chaves externo. |

# Importar certificados para controladores quando atua como clientes

Se o controlador rejeitar uma ligação porque não pode validar a cadeia de confiança de um servidor de rede, pode importar um certificado a partir do separador fidedigno que permite ao controlador (agindo como cliente) aceitar comunicações desse servidor.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Os ficheiros de certificado estão instalados no sistema local.

**Sobre esta tarefa**

A importação de certificados da guia confiável pode ser necessária se você quiser permitir que outro servidor entre em Contato com os controladores (por exemplo, um servidor LDAP ou um servidor syslog que usa TLS).

**Passos**

1. Selecione **Definições › certificados**.
2. Na guia confiável, selecione **Importar**.

   Abre-se uma caixa de diálogo para importar os ficheiros de certificado fidedignos.
3. Clique em **Procurar** para selecionar os arquivos de certificado para os controladores.

   Os nomes dos arquivos são exibidos na caixa de diálogo.
4. Clique em **Importar**.

**Resultados**

Os arquivos são carregados e validados.

# Ativar verificação de revogação de certificado

Você pode habilitar verificações automáticas para certificados revogados, de modo que um servidor OCSP (Online Certificate Status Protocol) bloqueie os usuários de fazer conexões não seguras.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Um servidor DNS é configurado em ambos os controladores, o que permite o uso de um nome de domínio totalmente qualificado para o servidor OCSP. Esta tarefa está disponível na página hardware.
- Se você quiser especificar seu próprio servidor OCSP, você deve saber a URL desse servidor.

**Sobre esta tarefa**

A verificação automática de revogação é útil nos casos em que a autoridade de certificação emitiu incorretamente um certificado ou uma chave privada é comprometida.

Durante essa tarefa, você pode configurar um servidor OCSP ou usar o servidor especificado no arquivo de certificado. O servidor OCSP determina se a CA revogou quaisquer certificados antes da data de expiração agendada e, em seguida, bloqueia o usuário de acessar um site se o certificado for revogado.

**Passos**

1. Selecione **Definições › certificados**.
2. Selecione a guia **Trusted**.

   Você também pode ativar a verificação de revogação na guia **Key Management**.

3. Clique em **tarefas incomuns** e selecione **Ativar Verificação de revogação** no menu suspenso.
4. Selecione **quero ativar a verificação de revogação** para que uma marca de seleção apareça na caixa de seleção e campos adicionais apareçam na caixa de diálogo.
5. No campo **OCSP respondedor address**, você pode opcionalmente inserir um URL para um servidor de resposta OCSP. Se não introduzir um endereço, o sistema utiliza a URL do servidor OCSP a partir do ficheiro de certificado.
6. Clique em **Endereço de teste** para garantir que o sistema possa abrir uma conexão com o URL especificado.
7. Clique em **Salvar**.

**Resultados**

Se o storage de armazenamento tentar se conetar a um servidor com um certificado revogado, a conexão será negada e um evento será registrado.

# Excluir certificados confiáveis

Você pode excluir os certificados instalados pelo usuário importados anteriormente da guia confiável.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Se você estiver atualizando um certificado confiável com uma nova versão, o certificado atualizado deve ser importado antes de excluir o certificado antigo.

> Poderá perder o acesso a um sistema se eliminar um certificado utilizado para autenticar os controladores e outro servidor, como um servidor LDAP, antes de importar um certificado de substituição.

**Sobre esta tarefa**

Esta tarefa descreve como eliminar certificados instalados pelo utilizador. Os certificados pré-instalados e auto-assinados não podem ser eliminados.

**Passos**

1. Selecione **Definições › certificados**.
2. Selecione a guia **Trusted**.

   A tabela mostra os certificados confiáveis do storage array.
3. Na tabela, selecione o certificado que deseja remover.
4. Clique em **tarefas incomuns › Delete**.

   Uma caixa de diálogo confirmar Excluir certificado confiável é aberta.
5. Digite `delete` o campo e clique em **Excluir**.

# Use certificados assinados pela CA para autenticação com um servidor de gerenciamento de chaves

Para comunicações seguras entre um servidor de gerenciamento de chaves e os controladores de storage array, você deve configurar os conjuntos apropriados de certificados.

**Antes de começar**

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.

**Sobre esta tarefa**

A autenticação entre os controladores e um servidor de gerenciamento de chaves é um procedimento de duas etapas.

## Etapa 1: Conclua e envie CSR para autenticação com um servidor de gerenciamento de chaves

Primeiro, você deve gerar um arquivo de solicitação de assinatura de certificado (CSR) e usar o CSR para solicitar um certificado de cliente assinado de uma autoridade de certificação (CA) confiável pelo servidor de gerenciamento de chaves. Você também pode criar e baixar um certificado de cliente a partir do servidor de gerenciamento de chaves usando o arquivo CSR baixado. Um certificado de cliente valida os controladores do

storage array, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP (Key Management Interoperability Protocol).

**Passos**

1. Selecione **Definições › certificados**.
2. Na guia Gerenciamento de chaves, selecione **Complete CSR**.
3. Introduza as seguintes informações:
   - * Nome comum* — um nome que identifica este CSR, como o nome da matriz de armazenamento, que será exibido nos arquivos de certificado.
   - **Organização** — o nome completo e legal de sua empresa ou organização. Inclua sufixos, como Inc. Ou Corp.
   - * Unidade organizacional (opcional) * — a divisão da sua organização que está a lidar com o certificado.
   - **Cidade/localidade** — a cidade ou localidade onde sua organização está localizada.
   - **Estado/região (opcional)** — o estado ou a região onde sua organização está localizada.
   - **Código ISO do país** — o código ISO de dois dígitos (Organização Internacional para Padronização), como EUA, onde sua organização está localizada.
4. Clique em **Download**.

   Um ficheiro CSR é guardado no seu sistema local.
5. Solicite um certificado de cliente assinado a partir de uma CA confiável pelo servidor de gerenciamento de chaves.
6. Quando tiver um certificado de cliente, vá para Etapa 2: Importar certificados para o servidor de gerenciamento de chaves.

## Etapa 2: Importar certificados para o servidor de gerenciamento de chaves

Como próxima etapa, você importa certificados para autenticação entre o storage array e o servidor de gerenciamento de chaves. Existem dois tipos de certificados: O certificado do cliente valida os controladores da matriz de armazenamento, enquanto o certificado do servidor de gestão de chaves valida o servidor. Você deve carregar o arquivo de certificado do cliente para os controladores e o arquivo de certificado do servidor para o servidor de gerenciamento de chaves.

**Antes de começar**

- Você tem um arquivo de certificado de cliente assinado (Etapa 1: Conclua e envie CSR para autenticação com um servidor de gerenciamento de chavesconsulte ) e copiou esse arquivo para o host onde está acessando o System Manager. Um certificado de cliente valida os controladores do storage array, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP (Key Management Interoperability Protocol).
- Você deve recuperar um arquivo de certificado do servidor de gerenciamento de chaves e, em seguida, copiar esse arquivo para o host onde você está acessando o System Manager. Um certificado do servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, de modo que o storage array possa confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou servidor para o servidor de gerenciamento de chaves.

> Para obter mais informações sobre o certificado do servidor, consulte a documentação do servidor de gerenciamento de chaves.

**Passos**

1. Selecione **Definições › certificados**.
2. Na guia Gerenciamento de chaves, selecione **Importar**.

   Abre-se uma caixa de diálogo para importar os ficheiros de certificado.

3. Ao lado de **Selecionar certificado de cliente**, clique no botão **Procurar** para selecionar o arquivo de certificado de cliente para os controladores da matriz de armazenamento.

   O nome do arquivo é exibido na caixa de diálogo.

4. Ao lado de **Selecione o certificado do servidor de gerenciamento de chaves**, clique no botão **Procurar** para selecionar o arquivo de certificado do servidor para o servidor de gerenciamento de chaves. Você pode escolher um certificado de raiz, intermediário ou servidor para o servidor de gerenciamento de chaves.

   O nome do arquivo é exibido na caixa de diálogo.

5. Clique em **Importar**.

   Os arquivos são carregados e validados.

# Exportar certificados do servidor de gerenciamento de chaves

Pode guardar um certificado para um servidor de gestão de chaves na sua máquina local.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Os certificados devem ser importados anteriormente.

**Passos**

1. Selecione **Definições › certificados**.
2. Selecione a guia **Key Management**.
3. Na tabela, selecione o certificado que deseja exportar e clique em **Exportar**.

   Abre-se uma caixa de diálogo Guardar.

4. Digite um nome de arquivo e clique em **Salvar**.

## Informações sobre direitos autorais



## Informações sobre marcas comerciais