Certificados

SANtricity software

NetApp
March 17, 2026

Índice

Certificados

Visão geral dos certificados

O gerenciamento de certificados permite criar solicitações de assinatura de certificados (CSRs), importar certificados e gerenciar certificados existentes.

O que são certificados?

Certificados são arquivos digitais que identificam entidades online, como sites e servidores, para comunicações seguras na internet. Existem dois tipos de certificados: um *certificado assinado* é validado por uma autoridade certificadora (CA) e um *certificado autoassinado* é validado pelo proprietário da entidade em vez de uma terceira parte.

Saiba mais:

- "Como funcionam os certificados"
- "Terminologia de certificado"

Como faço para configurar os certificados?

Em Gerenciamento de Certificados, você pode configurar certificados para a estação de gerenciamento que hospeda Unified Manager e também importar certificados para os controladores nos arrays.

Saiba mais:

- "Use certificados assinados por CA para o sistema de gerenciamento"
- "Importar certificados para arrays"

Conceitos

Como funcionam os certificados no SANtricity Unified Manager

Certificados são arquivos digitais que identificam entidades online, como sites e servidores, para comunicações seguras na internet.

Certificados assinados

Os certificados garantem que as comunicações web sejam transmitidas de forma criptografada, privada e inalterada, somente entre o servidor e o cliente. Usando Unified Manager, você pode gerenciar certificados para o navegador em um sistema de gerenciamento de hosts e para os controladores nos arrays de storage descobertos.

Um certificado pode ser assinado por uma autoridade confiável ou pode ser autoassinado. "Assinar" significa simplesmente que alguém validou a identidade do proprietário e determinou que seus dispositivos podem ser confiáveis. Os arrays de storage são fornecidos com um certificado autoassinado gerado automaticamente em cada controlador. Você pode continuar a usar os certificados autoassinados ou pode obter certificados assinados por CA para uma conexão mais segura entre os controladores e os sistemas host.

Embora os certificados assinados por uma Autoridade Certificadora (CA) ofereçam melhor proteção de segurança (por exemplo, prevenindo ataques do tipo "man-in-the-middle"), eles também exigem taxas que podem ser caras se você tiver uma rede grande. Em contraste, os certificados autoassinados são menos seguros, mas são gratuitos. Portanto, os certificados autoassinados são mais frequentemente usados em ambientes de teste internos, não em ambientes de produção.

Um certificado assinado é validado por uma autoridade certificadora (CA), que é uma organização de terceiro confiável. Os certificados assinados incluem detalhes sobre o proprietário da entidade (normalmente, um servidor ou site), data de emissão e expiração do certificado, domínios válidos para a entidade e uma assinatura digital composta por letras e números.

Ao abrir um navegador e digitar um endereço da web, seu sistema realiza um processo de verificação de certificado em segundo plano para determinar se você está se conectando a um site que inclui um certificado válido, assinado por uma CA. Geralmente, um site protegido com um certificado assinado inclui um ícone de cadeado e uma designação https no endereço. Se você tentar se conectar a um site que não contenha um certificado assinado por uma CA, seu navegador exibirá um aviso de que o site não é seguro.

A Autoridade Certificadora (CA) toma medidas para verificar sua identidade durante o processo de solicitação. Ela pode enviar um e-mail para o endereço comercial registrado da sua empresa, verificar o endereço comercial e realizar uma verificação HTTP ou DNS. Quando o processo de solicitação estiver concluído, a CA envia arquivos digitais para você carregar em um sistema de gerenciamento de host. Normalmente, esses arquivos incluem uma cadeia de confiança, conforme a seguir:

- **Raiz** — No topo da hierarquia está o certificado raiz, que contém uma chave privada usada para assinar outros certificados. A raiz identifica uma organização CA específica. Se você usar a mesma CA para todos os seus dispositivos de rede, precisará apenas de um certificado raiz.
- **Intermediário** — Ramificando-se a partir da raiz estão os certificados intermediários. A CA emite um ou mais certificados intermediários para atuarem como intermediários entre uma raiz protegida e os certificados do servidor.
- **Servidor** — Na base da cadeia está o certificado do servidor, que identifica sua entidade específica, como um site ou outro dispositivo. Cada controlador em um array de storage requer um certificado de servidor separado.

Certificados autoassinados

Cada controlador no array de storage inclui um certificado autoassinado pré-instalado. Um certificado autoassinado é semelhante a um certificado assinado por uma CA, exceto que é validado pelo proprietário da entidade em vez de uma terceira parte. Assim como um certificado assinado por uma CA, um certificado autoassinado contém sua própria chave privada e também garante que os dados sejam criptografados e enviados por uma conexão HTTPS entre um servidor e cliente.

Os certificados autoassinados não são "trusted" pelos navegadores. Cada vez que você tenta se conectar a um site que contém apenas um certificado autoassinado, o navegador exibe uma mensagem de aviso. Você deve clicar em um link na mensagem de aviso que permite prosseguir para o site; ao fazer isso, você está essencialmente aceitando o certificado autoassinado.

Certificados para Unified Manager

A interface do Unified Manager é instalada com o Web Services Proxy em um sistema host. Quando você abre um navegador e tenta se conectar ao Unified Manager, o navegador tenta verificar se o host é uma fonte confiável ao verificar a presença de um certificado digital. Se o navegador não localizar um certificado assinado por uma CA para o servidor, ele abre uma mensagem de aviso. A partir daí, você pode continuar

para o site para aceitar o certificado autoassinado para essa sessão. Ou, você pode obter certificados digitais assinados por uma CA para não ver mais a mensagem de aviso.

Certificados para controladores

Durante uma sessão do Unified Manager, você poderá ver mensagens de segurança adicionais ao tentar acessar um controlador que não possui um certificado assinado por uma CA. Nesse caso, você pode confiar permanentemente no certificado autoassinado ou importar os certificados assinados pela CA para os controladores, para que o servidor Web Services Proxy possa autenticar as solicitações de clientes recebidas desses controladores.

Saiba mais sobre a terminologia de certificados no SANtricity Unified Manager

Os seguintes termos aplicam-se ao gerenciamento de certificados.

Termo	Descrição
CA	Uma autoridade certificadora (CA) é uma entidade confiável que emite documentos eletrônicos, chamados certificados digitais, para segurança na Internet. Esses certificados identificam os proprietários de sites, permitindo conexões seguras entre clientes e servidores.
CSR	Uma solicitação de assinatura de certificado (CSR, na sigla em inglês) é uma mensagem enviada por um solicitante a uma autoridade certificadora (CA, na sigla em inglês). A CSR valida as informações que a CA exige para emitir um certificado.
Certificado	Um certificado identifica o proprietário de um site para fins de segurança, o que impede que invasores se façam passar pelo site. O certificado contém informações sobre o proprietário do site e a identidade da entidade confiável que certifica (assina) essas informações.
Cadeia de certificados	Uma hierarquia de arquivos que adiciona uma camada de segurança aos certificados. Normalmente, a cadeia inclui um certificado raiz no topo da hierarquia, um ou mais certificados intermediários e os certificados de servidor que identificam as entidades.
Certificado intermediário	Um ou mais certificados intermediários ramificam-se a partir da raiz na cadeia de certificados. A CA emite um ou mais certificados intermediários para atuarem como intermediários entre uma raiz protegida e os certificados do servidor.
Keystore	Um keystore é um repositório no seu sistema de gerenciamento de hosts que contém chaves privadas, juntamente com suas respectivas chaves públicas e certificados. Essas chaves e certificados identificam suas próprias entidades, como os controladores.
Certificado raiz	O certificado raiz está no topo da hierarquia na cadeia de certificados e contém uma chave privada usada para assinar outros certificados. A raiz identifica uma organização CA específica. Se você usar a mesma CA para todos os seus dispositivos de rede, precisará de apenas um certificado raiz.

Termo	Descrição
Certificado assinado	Um certificado validado por uma autoridade certificadora (CA). Este arquivo de dados contém uma chave privada e garante que os dados sejam enviados de forma criptografada entre um servidor e um cliente por meio de uma conexão HTTPS. Além disso, um certificado assinado inclui detalhes sobre o proprietário da entidade (normalmente, um servidor ou website) e uma assinatura digital composta por letras e números. Um certificado assinado utiliza uma cadeia de confiança e, portanto, é mais frequentemente usado em ambientes de produção. Também conhecido como "certificado assinado por CA" ou "certificado de gerenciamento".
Certificado autoassinado	Um certificado autoassinado é validado pelo proprietário da entidade. Este arquivo de dados contém uma chave privada e garante que os dados sejam enviados de forma criptografada entre um servidor e um cliente por meio de uma conexão HTTPS. Ele também inclui uma assinatura digital composta por letras e números. Um certificado autoassinado não utiliza a mesma cadeia de confiança que um certificado assinado por uma CA e, portanto, é mais frequentemente usado em ambientes de teste. Também é conhecido como um certificado "pré-instalado".
Certificado do servidor	O certificado do servidor está na base da cadeia de certificados. Ele identifica sua entidade específica, como um site ou outro dispositivo. Cada controlador em um sistema de storage requer um certificado de servidor separado.
Truststore	Um truststore é um repositório que contém certificados de terceiros confiáveis, como CAs.

Use certificados assinados por CA para o sistema de gerenciamento

Você pode obter e importar certificados assinados por CA para acesso seguro ao sistema de gerenciamento que hospeda SANtricity Unified Manager.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.

Sobre esta tarefa

Utilizar certificados assinados por uma CA é um procedimento de três etapas.

Etapa 1: preencha um arquivo CSR

Primeiro, você deve gerar um arquivo de solicitação de assinatura de certificado (CSR), que identifica sua organização e o sistema host onde o Web Services Proxy e Unified Manager estão instalados.

Alternativamente, você pode gerar um arquivo CSR usando uma ferramenta como OpenSSL e pular para Etapa 2: enviar o arquivo CSR.

Passos

1. Selecione **Certificate Management**.
2. Na guia Management, selecione **Complete CSR**.
3. Insira as seguintes informações e clique em **Avançar**:
   - **Organização** — O nome completo e legal da sua empresa ou organização. Inclua sufixos, como Inc. ou Corp.
   - **Unidade organizacional (opcional)** — A divisão da sua organização que está lidando com o certificado.
   - **Cidade/Localidade** — a cidade onde seu sistema host ou empresa está localizado.
   - **Estado/Região (opcional)** — O estado ou região onde seu sistema host ou empresa está localizado.
   - **Código ISO do país** — O código ISO (Organização Internacional de Normalização) de dois dígitos do seu país, como US.
4. Insira as seguintes informações sobre o sistema host onde o Web Services Proxy está instalado:
   - **Nome comum** — O endereço IP ou o nome DNS do sistema host onde o Web Services Proxy está instalado. Certifique-se de que este endereço esteja correto; ele deve corresponder exatamente ao que você digita para acessar Unified Manager no navegador. Não inclua http:// ou https://. O nome DNS não pode começar com um caractere curinga.
   - **Endereços IP alternativos** — Se o nome comum for um endereço IP, você pode, opcionalmente, inserir quaisquer endereços IP ou aliases adicionais para o sistema host. Para várias entradas, use o formato separado por vírgulas.
   - **Nomes DNS alternativos** — Se o nome comum for um nome DNS, insira quaisquer nomes DNS adicionais para o sistema host. Para múltiplas entradas, use o formato separado por vírgulas. Se não houver nomes DNS alternativos, mas você tiver inserido um nome DNS no primeiro campo, copie esse nome aqui. O nome DNS não pode começar com um caractere curinga.
5. Certifique-se de que as informações do host estejam corretas. Se não estiverem, os certificados retornados pela CA falharão quando você tentar importá-los.
6. Clique em **Concluir**.
7. Vá para Etapa 2: enviar o arquivo CSR.

Etapa 2: enviar o arquivo CSR

Após criar um arquivo de solicitação de assinatura de certificado (CSR), você o envia para uma Certificate Authority (CA) para receber certificados de gerenciamento assinados para o sistema que hospeda Unified Manager e o Web Services Proxy.

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 o arquivo CSR baixado.

   A localização da pasta do download depende do seu navegador.

2. Envie o arquivo CSR para uma Autoridade Certificadora (por exemplo, Verisign ou DigiCert) e solicite certificados assinados no formato PEM.

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

3. Quando a CA retornar os certificados assinados, vá para Etapa 3: importar certificados de management.

Etapa 3: importar certificados de management

Após receber os certificados assinados da Autoridade Certificadora (CA), importe os certificados no sistema host onde o Web Services Proxy e a interface Unified Manager estão instalados.

Antes de começar

- Você recebeu certificados assinados da CA. Esses arquivos incluem o certificado raiz, um ou mais certificados intermediários e o certificado do servidor.
- Se a CA forneceu um arquivo de certificado em cadeia (por exemplo, um arquivo .p7b), você deve descompactar o arquivo em cadeia em arquivos individuais: o certificado raiz, um ou mais certificados intermediários e o certificado do servidor. Você pode usar o utilitário do Windows `certmgr` para descompactar os arquivos (clique com o botão direito e selecione **All Tasks › Export**). A codificação Base-64 é recomendada. Quando as exportações forem concluídas, um arquivo CER será exibido para cada arquivo de certificado na cadeia.
- Você copiou os arquivos de certificado para o sistema host onde o Web Services Proxy está em execução.

Passos

1. Selecione **Certificate Management**.
2. Na aba Management, selecione **Import**.

   Uma caixa de diálogo é aberta para importar os arquivos de certificado.

3. Clique em **Procurar** para selecionar primeiro os arquivos de certificado raiz e intermediário e, em seguida, selecione o certificado do servidor. Se você gerou o CSR a partir de uma ferramenta externa, você também deve importar o arquivo de chave privada criado juntamente com o CSR.

   Os nomes dos arquivos são exibidos na caixa de diálogo.

4. Clique em **Importar**.

Resultados

Os arquivos são carregados e validados. As informações do certificado são exibidas na página de Certificate Management.

Redefinir certificados de gerenciamento

Você pode reverter o certificado de gerenciamento para o estado original, autoassinado de fábrica.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso

contrário, as funções de certificado não aparecem.

Sobre esta tarefa

Esta tarefa exclui o certificado de gerenciamento atual do sistema host onde o Web Services Proxy e Unified Manager estão instalados. Após a redefinição do certificado, o sistema host volta a usar o certificado autoassinado.

Passos

1. Selecione **Settings > Certificates**.
2. Selecione a aba **Gerenciamento de Array** e, em seguida, selecione **Redefinir**.

   Uma caixa de diálogo Confirm Reset Management Certificate é aberta.

3. Digite `reset` no campo e clique em **Redefinir**.

   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 ocorre quando você volta a usar certificados autoassinados. Para limpar a condição que está bloqueando o acesso ao destino, você deve limpar os dados de navegação do navegador.

Resultados

O sistema volta a usar o certificado autoassinado do servidor. Como resultado, o sistema solicita que os usuários aceitem manualmente o certificado autoassinado para suas sessões.

Use certificados de array

Importar certificados para arrays em SANtricity Unified Manager

Caso necessário, você pode importar certificados para os arrays de storage para que eles possam se autenticar com o sistema que hospeda SANtricity Unified Manager. Os certificados podem ser assinados por uma autoridade certificadora (CA) ou podem ser autoassinados.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.
- Se você estiver importando certificados confiáveis, os certificados deverão ser importados para os controladores do array de storage usando System Manager.

Passos

1. Selecione **Certificate Management**.
2. Selecione a guia **Trusted**.

   Esta página exibe todos os certificados relatados para os arrays de storage.

3. Selecione **Import › Certificados** para importar um certificado de CA ou **Import › Self-signed storage array certificates** para importar um certificado autoassinado.

   Para limitar a visualização, você pode usar o campo de filtro **Mostrar certificados que são…** ou pode classificar as linhas de certificados clicando em um dos cabeçalhos de coluna.

4. Na caixa de diálogo, selecione o certificado e depois clique em **Importar**.

   O certificado é carregado e validado.

Excluir certificados confiáveis no SANtricity Unified Manager

Você pode excluir um ou mais certificados que não são mais necessários, como um certificado expirado.

Antes de começar

Importe o novo certificado antes de excluir o antigo.

> Tenha em mente que a exclusão de um certificado raiz ou intermediário pode afetar vários arrays de storage, já que esses arrays podem compartilhar os mesmos arquivos de certificado.

Passos

1. Selecione **Certificate Management**.
2. Selecione a guia **Trusted**.
3. Selecione um ou mais certificados na tabela e clique em **Delete**.

   > A função **Excluir** não está disponível para certificados pré-instalados.

   A caixa de diálogo Confirmar Exclusão de Certificado Confiável é aberta.

4. Confirme a exclusão e, em seguida, clique em **Excluir**.

   O certificado é removido da tabela.

Resolver certificados não confiáveis

Certificados não confiáveis ocorrem quando um array de storage tenta estabelecer uma conexão segura com SANtricity Unified Manager, mas a conexão falha ao ser confirmada como segura.

Na página de Certificado, você pode resolver certificados não confiáveis importando um certificado autoassinado do array de storage ou importando um certificado de autoridade certificadora (CA) emitido por uma terceira parte confiável.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security Admin.
- Se você planeja importar um certificado assinado por uma autoridade certificadora (CA):
  - Você gerou uma solicitação de assinatura de certificado (arquivo .CSR) para cada controlador no array de storage e a enviou para a CA.
  - A CA retornou arquivos de certificado confiáveis.
  - Os arquivos de certificado estão disponíveis no seu sistema local.

Sobre esta tarefa

Você pode precisar instalar certificados de CA confiáveis adicionais se alguma das seguintes condições for verdadeira:

- Você adicionou recentemente um array de storage.
- Um ou ambos os certificados expiraram.
- Um ou ambos os certificados estão revogados.
- Um ou ambos os certificados estão sem um certificado raiz ou intermediário.

Passos

1. Selecione **Certificate Management**.
2. Selecione a guia **Trusted**.

   Esta página exibe todos os certificados relatados para os arrays de storage.

3. Selecione **Import › Certificados** para importar um certificado de CA ou **Import › Self-Signed storage array certificates** para importar um certificado autoassinado.

   Para limitar a visualização, você pode usar o campo de filtro **Mostrar certificados que são…** ou pode classificar as linhas de certificados clicando em um dos cabeçalhos de coluna.

4. Na caixa de diálogo, selecione o certificado e clique em **Import**.

   O certificado é carregado e validado.

Gerenciar certificados

Ver certificados

Você pode visualizar informações resumidas de um certificado, que incluem a organização que utiliza o certificado, a autoridade que emitiu o certificado, o período de validade e as impressões digitais (identificadores únicos).

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.

Passos

1. Selecione **Certificate Management**.
2. Selecione uma das seguintes abas:
   - **Gerenciamento** — Exibe o certificado do sistema que hospeda o Web Services Proxy. Um certificado de gerenciamento pode ser autoassinado ou aprovado por uma autoridade certificadora (CA). Ele permite acesso seguro ao Unified Manager.
   - **Confiável** — Mostra os certificados que Unified Manager pode acessar para arrays de storage e outros servidores remotos, como um servidor LDAP. Os certificados podem ser emitidos por uma autoridade certificadora (CA) ou podem ser autoassinados.
3. Para ver mais informações sobre um certificado, selecione a linha correspondente, selecione as reticências no final da linha e clique em **View** ou **Export**.

Exportar certificados no SANtricity Unified Manager

Você pode exportar um certificado para visualizar seus detalhes completos.

Antes de começar

Para abrir o arquivo exportado, você deve ter um aplicativo visualizador de certificados.

Passos

1. Selecione **Certificate Management**.
2. Selecione uma das seguintes abas:
   - **Gerenciamento** — Exibe o certificado do sistema que hospeda o Web Services Proxy. Um certificado de gerenciamento pode ser autoassinado ou aprovado por uma autoridade certificadora (CA). Ele permite acesso seguro ao Unified Manager.
   - **Confiável** — Mostra os certificados que Unified Manager pode acessar para arrays de storage e outros servidores remotos, como um servidor LDAP. Os certificados podem ser emitidos por uma autoridade certificadora (CA) ou podem ser autoassinados.
3. Selecione um certificado na página e, em seguida, clique nas reticências no final da linha.
4. Clique em **Exportar** e, em seguida, salve o arquivo de certificado.
5. Abra o arquivo no seu aplicativo visualizador de certificados.

Informações sobre direitos autorais

Informações sobre marcas comerciais