Gerenciar certificados de segurança

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/pt-br/active-iq-unified-manager-918/config/task_view_https_security_certificate_ocf.html on November 13, 2026. Always check docs.netapp.com for the latest.

Índice

Gerenciar certificados de segurança . . . 1
- Visualize o certificado de segurança HTTPS no Active IQ Unified Manager . . . 1
- Faça o download de uma solicitação de assinatura de certificado HTTPS no Active IQ Unified Manager . . . 1
- Instale um certificado HTTPS assinado por uma Autoridade Certificadora (CA) no Active IQ Unified Manager . . . 2
  - Exemplo de cadeia de certificados . . . 2
- Saiba mais sobre certificados HTTPS gerados usando ferramentas externas no Active IQ Unified Manager Unified Manager . . . 3
  - Formato para carregar um certificado com um par de chaves EC . . . 3
  - Formato para carregar um certificado com um par de chaves RSA . . . 4
  - Verificações ao carregar certificados gerados externamente . . . 4
- Descrições de páginas para gerenciamento de certificados . . . 5
  - Saiba mais sobre a página de certificado HTTPS em o Active IQ Unified Manager . . . 5
  - Regenerar a caixa de diálogo de certificado HTTPS em Active IQ Unified Manager . . . 6

Gerenciar certificados de segurança

Visualize o certificado de segurança HTTPS no Active IQ Unified Manager

Você pode comparar os detalhes do certificado HTTPS com o certificado obtido no seu navegador para garantir que a conexão criptografada do seu navegador com o Unified Manager não esteja sendo interceptada.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

A visualização do certificado permite verificar o conteúdo de um certificado regenerado ou visualizar os Nomes alternativos do assunto (SAN), a partir dos quais você pode acessar o Unified Manager.

Etapa

1. No painel de navegação esquerdo, clique em **Geral** > **Certificado HTTPS**.

   O certificado HTTPS é exibido na parte superior da página

Caso você precise visualizar informações mais detalhadas sobre o certificado de segurança do que as exibidas na página HTTPS Certificate, você pode visualizar o certificado de conexão no seu navegador.

Faça o download de uma solicitação de assinatura de certificado HTTPS no Active IQ Unified Manager

Você pode baixar uma solicitação de assinatura de certificado para o certificado de segurança HTTPS atual para que você possa fornecer o arquivo a uma Autoridade Certificadora (AC) para assiná-lo. Um certificado assinado por uma AC ajuda a evitar ataques do tipo "man-in-the-middle" e oferece melhor proteção de segurança do que um certificado autoassinado.

Antes de começar

Você precisa ter a função de Application Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Certificado HTTPS**.
2. Clique em **Baixar Solicitação de Assinatura de Certificado HTTPS**.
3. Salve o `<hostname>.csr` arquivo.

Você pode fornecer o arquivo a uma autoridade de certificação para que ela o assine e, em seguida, instale o certificado assinado.

Instale um certificado HTTPS assinado por uma Autoridade Certificadora (CA) no Active IQ Unified Manager

Você pode fazer upload e instalar um certificado de segurança depois que uma Autoridade Certificadora (AC) o assinar e devolver. O arquivo que você faz upload e instala deve ser uma versão assinada do certificado autoassinado existente. Um certificado assinado por uma AC ajuda a evitar ataques "man-in-the-middle" e oferece melhor proteção de segurança do que um certificado autoassinado.

*O que. Antes de começar

Você deve ter concluído as seguintes ações:

- Baixou o arquivo de solicitação de assinatura de certificado e o enviou para assinatura por uma autoridade certificadora
- Salvou a cadeia de certificados no formato PEM
- Inclui todos os certificados na cadeia, do certificado do servidor do Unified Manager até o certificado raiz de assinatura, incluindo quaisquer certificados intermediários presentes

Você precisa ter a função de Application Administrator.

Se a validade do certificado para o qual um CSR foi criado for superior a 397 dias, a CA reduzirá essa validade para 397 dias antes de assinar e devolver o certificado

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Certificado HTTPS**.
2. Clique em **Instalar certificado HTTPS**.
3. Na caixa de diálogo que aparece, clique em **Escolher arquivo…** para localizar o arquivo que deseja carregar.
4. Selecione o arquivo e clique em **Instalar** para instalar o arquivo.

   Para informações, consulte "Instalando um certificado HTTPS gerado com ferramentas externas".

Exemplo de cadeia de certificados

O exemplo a seguir mostra como o arquivo da cadeia de certificados pode aparecer:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

```
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Saiba mais sobre certificados HTTPS gerados usando ferramentas externas no Active IQ Unified Manager Unified Manager

Você pode instalar certificados autoassinados ou assinados por uma Autoridade Certificadora (CA) e gerados usando uma ferramenta externa, como OpenSSL, BoringSSL, LetsEncrypt.

Você deve carregar a chave privada junto com a cadeia de certificados, porque esses certificados são um par de chaves pública-privada gerado externamente. Os algoritmos de par de chaves permitidos são “RSA” e “EC”. A opção **Install HTTPS Certificate** está disponível na página HTTPS Certificates, na seção General. O arquivo que você enviar deve estar no seguinte formato de entrada.

1. Chave privada do servidor que pertence ao host do Active IQ Unified Manager
2. Certificado do servidor que corresponde à chave privada
3. Certificados das ACs em ordem inversa até a raiz, que são usados para assinar o certificado acima

Formato para carregar um certificado com um par de chaves EC

As curvas permitidas são “prime256v1” e “secp384r1”. Exemplo de certificado com um par EC gerado externamente:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Formato para carregar um certificado com um par de chaves RSA

Os tamanhos de chave permitidos para o par de chaves RSA pertencente ao certificado de host são 2048, 3072 e 4096. certificado com um **par de chaves RSA** gerado externamente:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Após o upload do certificado, você deverá reiniciar a instância do Active IQ Unified Manager para que as alterações entrem em vigor.

Verificações ao carregar certificados gerados externamente

O sistema realiza verificações durante o upload de um certificado gerado usando ferramentas externas. Se alguma das verificações falhar, o certificado será rejeitado. Há também validações incluídas para os certificados gerados a partir da CSR no produto e para os certificados gerados usando ferramentas externas.

- A chave privada informada é validada em relação ao certificado do host informado.
- O Common Name (CN) no certificado do host é verificado em relação ao FQDN do host.
- O nome comum (CN) do certificado do host não deve estar vazio ou em branco e não deve ser definido como localhost.
- A data de início da validade não deve estar no futuro, e a data de expiração da validade do certificado não deve estar no passado.
- Se existir CA intermediária ou CA, a data de início da validade do certificado não deve estar no futuro e a data de expiração da validade não deve estar no passado.



A chave privada na entrada não deve estar criptografada. Se houver chaves privadas criptografadas, elas serão rejeitadas pelo sistema.

Exemplo 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
```

```
-----END ENCRYPTED PRIVATE KEY-----
```

Exemplo 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Exemplo 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Se a instalação do certificado falhar, consulte o artigo da base de conhecimento (KB): "O ActiveIQ Unified Manager falha ao instalar um certificado gerado externamente"

Descrições de páginas para gerenciamento de certificados

Saiba mais sobre a página de certificado HTTPS em o Active IQ Unified Manager

A página de Certificado HTTPS permite visualizar o certificado de segurança atual, baixar uma solicitação de assinatura de certificado, gerar um novo certificado HTTPS autoassinado ou instalar um novo certificado HTTPS.

Se você não gerou um novo certificado HTTPS autoassinado, o certificado exibido nesta página é o certificado gerado durante a instalação.

Botões de comando

Os botões de comando permitem realizar as seguintes operações:

- **Baixar solicitação de assinatura de certificado HTTPS**

  Faz o download de uma solicitação de certificação para o certificado HTTPS atualmente instalado. Seu navegador solicitará que você salve o arquivo <hostname>.csr para que você possa fornecê-lo a uma Autoridade Certificadora para assinatura.

- **Instalar certificado HTTPS**

  Permite fazer upload e instalar um certificado de segurança após uma Autoridade de Certificação tê-lo assinado e devolvido. O novo certificado entra em vigor após você reiniciar o servidor de gerenciamento.

- **Regenerar certificado HTTPS**

  Permite gerar um novo certificado HTTPS autoassinado, que substitui o certificado de segurança atual. O

novo certificado entra em vigor após reiniciar o Unified Manager.

Regenerar a caixa de diálogo de certificado HTTPS em Active IQ Unified Manager

A caixa de diálogo "Regenerar certificado HTTPS" permite personalizar as informações de segurança e, em seguida, gerar um novo certificado HTTPS com essas informações.

As informações atuais do certificado aparecem nesta página.

As opções “Regenerar usando os atributos atuais do certificado” e “Atualizar os atributos atuais do certificado” permitem regenerar o certificado com as informações atuais ou gerar um certificado com novas informações.

- **Nome comum**

  Obrigatório. O nome de domínio totalmente qualificado (FQDN) que você deseja proteger.

  Em configurações de alta disponibilidade do Unified Manager, use o endereço IP virtual.

- **E-mail**

  Opcional. Um endereço de e-mail para contato com sua organização; normalmente, o endereço de e-mail do administrador de certificados ou do departamento de TI.

- **Empresa**

  Opcional. Normalmente, o nome registrado da sua empresa.

- **Departamento**

  Opcional. O nome do departamento em sua empresa.

- **Cidade**

  Opcional. A cidade onde sua empresa está localizada.

- **Estado**

  Opcional. O estado ou província onde sua empresa está localizada, sem abreviação.

- **País**

  Opcional. O país onde sua empresa está localizada. Normalmente, trata-se de um código ISO de duas letras do país.

- **Nomes Alternativos**

  Obrigatório. Nomes de domínio adicionais, não primários, que podem ser usados para acessar este servidor além do localhost existente ou de outros endereços de rede. Separe cada nome alternativo com uma vírgula.

  Selecione a caixa de seleção “Excluir informações de identificação local (por exemplo, localhost)” se você quiser remover as informações de identificação local do campo Nomes Alternativos no certificado. Quando esta caixa de seleção estiver marcada, somente o que você inserir no campo será usado no campo Nomes Alternativos. Se você deixar o campo em branco, o certificado resultante não terá um campo Nomes Alternativos.

- **TAMANHO DA CHAVE (ALGORITMO DA CHAVE: RSA)**

  O algoritmo de chave está definido como RSA. Você pode selecionar um dos tamanhos de chave: 2048, 3072 ou 4096 bits. O tamanho de chave padrão é 2048 bits.

- **PERÍODO DE VALIDADE**

  O período de validade padrão é de 397 dias. Se você atualizou de uma versão anterior, poderá ver que a validade do certificado anterior permaneceu inalterada.

Para obter mais informações, consulte "Gerando certificados HTTPS".

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em http://www.netapp.com/TM são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.