# Configurar chaves de segurança

SANtricity software

NetApp
March 17, 2026

# Índice

# Configurar chaves de segurança

## Crie uma chave de segurança interna no SANtricity System Manager

Para usar o recurso de Segurança de Unidade, você pode criar uma chave de segurança interna que é compartilhada pelos controladores e unidades com capacidade de segurança no array de storage. As chaves internas são mantidas na memória persistente do controlador.

**Antes de começar**

- Unidades com capacidade de segurança devem ser instaladas no array de storage. Essas unidades podem ser unidades com criptografia de disco completa (FDE) ou unidades com o padrão Federal Information Processing Standard (FIPS).
- O recurso Drive Security deve estar ativado. Caso contrário, uma caixa de diálogo Cannot Create Security Key será exibida durante esta tarefa. Se necessário, entre em contato com o fornecedor do seu array de storage para obter instruções sobre como ativar o recurso Drive Security.

> Se ambas as unidades FDE e FIPS estiverem instaladas no array de storage, todas compartilharão a mesma chave de segurança.

**Sobre esta tarefa**

Nesta tarefa, você define um identificador e uma frase secreta para associar à chave de segurança interna.

> A senha para Segurança da Unidade é independente da senha de Administrador do array de storage.

**Passos**

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Criar chave interna**.

   Se você ainda não gerou uma chave de segurança, a caixa de diálogo Criar chave de segurança é aberta.

3. Insira informações nos seguintes campos:

   - **Defina um identificador de chave de segurança** — Você pode aceitar o valor padrão (nome do array de storage e carimbo de data/hora, que é gerado pelo firmware do controlador) ou inserir seu próprio valor. Você pode inserir até 189 caracteres alfanuméricos, sem espaços, pontuação ou símbolos.

     > Caracteres adicionais são gerados automaticamente, anexados às duas extremidades da sequência que você inserir. Os caracteres gerados garantem que o identificador seja único.

   - **Definir uma frase secreta/Digitar novamente a frase secreta** — Digite e confirme uma frase secreta. O valor pode ter entre 8 e 32 caracteres e deve incluir cada um dos seguintes:
     - Uma letra maiúscula (ou mais). Lembre-se de que a senha diferencia maiúsculas de minúsculas.
     - Um número (um ou mais).

- Um caractere não alfanumérico, como !, *, @ (um ou mais).

**Certifique-se de registrar suas anotações para uso posterior**. Se precisar mover uma unidade com segurança habilitada do array de storage, você deve saber o identificador e a pass phrase para desbloquear os dados da unidade.

4. Clique em **Create**.

   A chave de segurança é armazenada no controlador em um local inacessível. Junto com a chave real, há um arquivo de chave criptografado que é baixado do seu navegador.

   O caminho para o arquivo baixado pode depender do local de download padrão do seu navegador.

5. Anote o identificador da chave, a frase secreta e o local do arquivo de chave baixado e, em seguida, clique em **Fechar**.

**Resultados**

Agora você pode criar grupos ou pools de volumes com segurança habilitada, ou pode habilitar a segurança em grupos de volumes e pools de volumes existentes.

Sempre que a alimentação das unidades é desligada e ligada novamente, todas as unidades com segurança habilitada passam para o estado Security Locked. Nesse estado, os dados ficam inacessíveis até que o controlador aplique a chave de segurança correta durante a inicialização da unidade. Se alguém remover fisicamente uma unidade bloqueada e instalá-la em outro sistema, o estado Security Locked impede o acesso não autorizado aos seus dados.

**Depois que você terminar**

Você deve validar a chave de segurança para garantir que o arquivo de chave não esteja corrompido.

# Crie uma chave de segurança externa no SANtricity System Manager

Para usar o recurso de segurança de unidade com um servidor de gerenciamento de chaves, você deve criar uma chave externa que é compartilhada pelo servidor de gerenciamento de chaves e pelas unidades com capacidade de segurança no array de storage.

**Antes de começar**

- Unidades de armazenamento com capacidade de segurança devem ser instaladas no array. Essas unidades podem ser unidades com criptografia de disco completa (FDE) ou unidades Federal Information Processing Standard (FIPS).

  Se ambas as unidades FDE e FIPS estiverem instaladas no array de storage, todas compartilharão a mesma chave de segurança.

- O recurso Drive Security deve estar ativado. Caso contrário, uma caixa de diálogo Cannot Create Security Key será exibida durante esta tarefa. Se necessário, entre em contato com o fornecedor do seu array de storage para obter instruções sobre como ativar o recurso Drive Security.

- Você possui um arquivo de certificado de cliente assinado para os controladores do array de storage e copiou esse arquivo para o host onde está acessando System Manager. Um certificado de cliente valida os controladores do array de storage, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações do Key Management Interoperability Protocol (KMIP).
- Você deve obter um arquivo de certificado do servidor de gerenciamento de chaves e, em seguida, copiar esse arquivo para o host onde você está acessando System Manager. Um certificado de servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, então o array de storage pode confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.

> Para obter mais informações sobre o certificado do servidor, consulte a documentação do seu key management server.

**Sobre esta tarefa**

Nesta tarefa, você define o endereço IP do servidor de gerenciamento de chaves e o número da porta que ele utiliza e, em seguida, carrega certificados para o gerenciamento externo de chaves.

**Passos**

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Criar chave externa**.

> Se o gerenciamento de chaves interno estiver atualmente configurado, uma caixa de diálogo será aberta e solicitará que você confirme que deseja mudar para o gerenciamento de chaves externo.

   A caixa de diálogo Criar chave de segurança externa é aberta.

3. Em **Conectar ao Key Server**, insira informações nos seguintes campos.
   - **Endereço do servidor de gerenciamento de chaves** — Insira o domínio totalmente qualificado ou o endereço IP (IPv4 ou IPv6) do servidor usado para o gerenciamento de chaves.
   - **Número da porta de gerenciamento de chaves** — Insira o número da porta usado para comunicações KMIP. O número de porta mais comum usado para comunicações com o servidor de gerenciamento de chaves é 5696.

     **Opcional:** Se você quiser configurar um servidor de chaves de backup, clique em **Add Key Server** e insira as informações desse servidor. O segundo servidor de chaves será usado se o servidor de chaves primário não puder ser acessado. Certifique-se de que cada servidor de chaves tenha acesso ao mesmo banco de dados de chaves; caso contrário, o array exibirá erros e não poderá usar o servidor de backup.

> Apenas um servidor de chaves é usado por vez. Se o array de storage não conseguir alcançar o servidor de chaves primário, o array entrará em contato com o servidor de chaves de backup. Esteja ciente de que você deve manter a paridade entre ambos os servidores; a falha em fazê-lo pode resultar em erros.

   - **Selecionar certificado do cliente** — Clique no primeiro botão **Procurar** para selecionar o arquivo de certificado para os controladores do array de storage.
   - **Selecionar arquivo de chave privada** — Se necessário, clique no segundo botão **Procurar** para selecionar um arquivo de chave privada para os controladores do array de storage.

- **Selecione o certificado do servidor de gerenciamento de chaves** — Clique no terceiro botão **Procurar** para selecionar o arquivo de certificado do servidor de gerenciamento de chaves. Você pode escolher um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.

4. Clique em **Next**.
5. Em **Criar/Fazer Backup da Chave**, você pode criar uma chave de backup para fins de segurança.
   - (Recomendado) Para criar uma chave de backup, mantenha a caixa de seleção marcada e, em seguida, insira e confirme uma senha. O valor pode ter entre 8 e 32 caracteres e deve incluir cada um dos seguintes:
     - Uma letra maiúscula (ou mais). Lembre-se de que a senha diferencia maiúsculas de minúsculas.
     - Um número (um ou mais).
     - Um caractere não alfanumérico, como !, *, @ (um ou mais).

     **Certifique-se de anotar suas entradas para uso posterior**. Se precisar mover uma unidade com segurança habilitada do array de storage, você precisa saber a senha para desbloquear os dados da unidade.

   +

   - Se não quiser criar uma chave de backup, desmarque a caixa de seleção.

     Esteja ciente de que, se você perder o acesso ao servidor de chaves externo e não tiver uma chave de backup, perderá o acesso aos dados nas unidades caso elas sejam migradas para outro array de storage. Esta opção é o único método para criar uma chave de backup no System Manager.

6. Clique em **Concluir**.

   O sistema se conecta ao servidor de gerenciamento de chaves com as credenciais que você inseriu. Uma cópia da chave de segurança é então armazenada em seu sistema local.

   O caminho para o arquivo baixado pode depender do local de download padrão do seu navegador.

7. Anote sua frase secreta e o local do arquivo de chave baixado e, em seguida, clique em **Fechar**.

   A página exibe a seguinte mensagem com links adicionais para gerenciamento externo de chaves:

   ```
   Current key management method: External
   ```

8. Teste a conexão entre o array de storage e o servidor de gerenciamento de chaves selecionando **Test Communication**.

   Os resultados dos testes são exibidos na caixa de diálogo.

**Resultados**

Quando o gerenciamento de chaves externas está ativado, você pode criar grupos ou pools de volumes com segurança habilitada, ou pode habilitar a segurança em grupos e pools de volumes existentes.

Sempre que a alimentação das unidades é desligada e ligada novamente, todas as unidades com segurança habilitada passam para o estado Security Locked. Nesse estado, os dados ficam inacessíveis até que o controlador aplique a chave de segurança correta durante a inicialização da unidade. Se alguém remover fisicamente uma unidade bloqueada e instalá-la em outro sistema, o estado Security Locked impede o acesso não autorizado aos seus dados.

**Depois que você terminar**

Você deve validar a chave de segurança para garantir que o arquivo de chave não esteja corrompido.

## Informações sobre direitos autorais



## Informações sobre marcas comerciais