Manage security keys

SANtricity 11.7

NetApp
February 12, 2024

Table of Contents

Manage security keys

Change security key

At any time, you can replace a security key with a new key. You might need to change a security key in cases where you have a potential security breach at your company and want to make sure unauthorized personnel cannot access the drives data.

Steps

1. Select **Settings › System**.
2. Under **Security key management**, select **Change Key**.

   The Change Security Key dialog box opens.

3. Enter information in the following fields.
   - **Define a security key identifier** — (For internal security keys only.) Accept the default value (storage array name and time stamp, which is generated by the controller firmware) or enter your own value. You can enter up to 189 alphanumeric characters without spaces, punctuation, or symbols.

     Additional characters are generated automatically and are appended to both ends of the string you enter. The generated characters help to ensure that the identifier is unique.

   - **Define a pass phrase/Re-enter pass phrase** — In each of these fields, enter your pass phrase. The value can have between 8 and 32 characters, and must include each of the following:
     - An uppercase letter (one or more). Keep in mind that the pass phrase is case sensitive.
     - A number (one or more).
     - A non-alphanumeric character, such as !, *, @ (one or more).
4. For external security keys, if you want to delete the old security key when the new one is created, select the "Delete current security key…" checkbox at the bottom of the dialog.

   Be sure to record your entries for later use — If you need to move a secure-enabled drive from the storage array, you must know the identifier and pass phrase to unlock drive data.

5. Click **Change**.

   The new security key overwrites the previous key, which is no longer valid.

   The path for the downloaded file might depend on the default download location of your browser.

6. Record your key identifier, pass phrase, and the location of the downloaded key file, and then click **Close**.

After you finish

You should validate the security key to make sure the key file is not corrupted.

Switch from external to internal key management

You can change the management method for Drive Security from an external key server to the internal method used by the storage array. The security key previously defined for external key management is then used for internal key management.

About this task

In this task, you disable external key management and download a new backup copy to your local host. The existing key is still used for Drive Security, but will be managed internally in the storage array.

Steps

1. Select **Settings › System**.
2. Under **Security key management**, select **Disable External Key Management**.

   The Disable External Key Management dialog box opens.

3. In **Define a pass phrase/Re-enter pass phrase**, enter and confirm a pass phrase for the backup of the key. The value can have between 8 and 32 characters, and must include each of the following:

   - An uppercase letter (one or more). Keep in mind that the pass phrase is case sensitive.
   - A number (one or more).
   - A non-alphanumeric character, such as !, *, @ (one or more).

   Be sure to record your entries for later use. If you need to move a secure-enabled drive from the storage array, you must know the identifier and pass phrase to unlock drive data.

4. Click **Disable**.

   The backup key is downloaded to your local host.

5. Record your key identifier, pass phrase, and the location of the downloaded key file, and then click **Close**.

Results

Drive Security is now managed internally through the storage array.

After you finish

You should validate the security key to make sure the key file is not corrupted.

Edit key management server settings

If you configured external key management, you can view and edit the key management server settings at any time.

Steps

1. Select **Settings › System**.
2. Under **Security key management**, select **View/Edit Key Management Server Settings**.
3. Edit information in the following fields:

   - **Key management server address** — Enter the fully qualified domain name or the IP address (IPv4 or IPv6) of the server used for key management.

- **Key management port number** — Enter the port number used for the Key Management Interoperability Protocol (KMIP) communications.

  Optional: you can include another key server by clicking **Add Key Server**.

4. Click **Save**.

Back up security key

After creating or changing a security key, you can create a backup copy of the key file in case the original gets corrupted.

About this task

This task describes how to back up a security key you previously created. During this procedure, you create a new pass phrase for the backup. This pass phrase does not need to match the pass phrase that was used when the original key was created or last changed. The pass phrase is applied only to the backup you are creating.

Steps

1. Select **Settings › System**.
2. Under **Security key management**, select **Back Up Key**.

   The Back Up Security Key dialog box opens.

3. In the **Define a pass phrase/Re-enter pass phrase** fields, enter and confirm a pass phrase for this backup.

   The value can have between 8 and 32 characters, and must include each of the following:

   - An uppercase letter (one or more)
   - A number (one or more)
   - A non-alphanumeric character, such as !, *, @ (one or more)

   Be sure to record your entry for later use. You need the pass phrase to access the backup of this security key.

4. Click **Back Up**.

   A backup of the security key is downloaded to your local host, and then the **Confirm/Record Security Key Backup** dialog box opens.

   The path for the downloaded security key file might depend on the default download location of your browser.

5. Record your pass phrase in a secure location, and then click **Close**.

After you finish

You should validate the backup security key.

Validate security key

You can validate the security key to make sure it has not been corrupted and to verify that you have a correct pass phrase.

About this task

This task describes how to validate the security key you previously created. This is an important step to make sure the key file is not corrupted and the pass phrase is correct, which ensures that you can later access drive data if you move a secure-enabled drive from one storage array to another.

Steps

1. Select **Settings › System**.
2. Under **Security key management**, select **Validate Key**.

   The Validate Security Key dialog box opens.
3. Click **Browse**, and then select the key file (for example, `drivesecurity.slk`).
4. Enter the pass phrase associated with the key you selected.

   When you select a valid key file and pass phrase, the **Validate** button becomes available.
5. Click **Validate**.

   The results of the validation are displayed in the dialog box.
6. If the results show "The security key validated successfully," click **Close**. If an error message appears, follow the suggested instructions displayed in the dialog box.

Unlock drives when using internal key management

If you configured internal key management and then later move secure-enabled drives from one storage array to another, you must re-assign the security key to the new storage array to gain access to the encrypted data on the drives.

Before you begin

- On the source array (the array where you are removing the drives), you have exported volume groups and removed the drives. On the target array, you have re-installed the drives.

  > The Export/Import function is not supported in the System Manager user interface; you must use the Command Line Interface (CLI) to export/import a volume group to a different storage array.

  Detailed instructions for migrating a volume group are provided in the NetApp Knowledge Base. Be sure to follow the appropriate instructions for newer arrays managed by System Manager or for legacy systems.
- The Drive Security feature must be enabled. Otherwise, a Cannot Create Security Key dialog box opens during this task. If necessary, contact your storage vendor for instructions on enabling the Drive Security feature.
- You must know the security key that is associated with the drives you want to unlock.

- The security key file is available on the management client (the system with a browser used for accessing System Manager). If you are moving the drives to a storage array that is managed by a different system, you need to move the security key file to that management client.

About this task

When you use internal key management, the security key is stored locally on the storage array. A security key is a string of characters that is shared by the controller and drives for read/write access. When the drives are physically removed from the array and installed in another, they cannot operate until you provide the correct security key.

> ⓘ You can create either an internal key from the controller's persistent memory or an external key from a key management server. This topic describes unlocking data when *internal* key management is used. If you used *external* key management, see Unlock drives when using external key management. If you are performing a controller upgrade and are swapping all controllers for the latest hardware, you must follow different steps as described in the E-Series and SANtricity documentation center, in Unlock drives.

Once you reinstall secure-enabled drives in another array, that array discovers the drives and displays a "Needs Attention" condition along with a status of "Security Key Needed." To unlock drive data, you select the security key file and enter the pass phrase for the key. (This pass phrase is not the same as the storage array's Administrator password.)

If other secure-enabled drives are installed in the new storage array, they might use a different security key than the one you are importing. During the import process, the old security key is used only to unlock the data for the drives you are installing. When the unlock process is successful, the newly installed drives are re-keyed to the target storage array's security key.

Steps

1. Select **Settings › System**.
2. Under **Security key management**, select **Unlock Secure Drives**.

   The Unlock Secure Drives dialog box opens. Any drives that require a security key are shown in the table.
3. **Optional:** hover the mouse over a drive number to see the location of the drive (shelf number and bay number).
4. Click **Browse**, and then select the security key file that corresponds to the drive you want to unlock.

   The key file you selected appears in the dialog box.
5. Enter the pass phrase associated with this key file.

   The characters you enter are masked.
6. Click **Unlock**.

   If the unlock operation is successful, the dialog box displays: "The associated secure drives have been unlocked."

Results

When all drives are locked and then unlocked, each controller in the storage array will reboot. However, if there are already some unlocked drives in the target storage array, then the controllers will not reboot.

After you finish

On the destination array (the array with the newly installed drives), you can now import volume groups.

> The Export/Import function is not supported in the System Manager user interface; you must use the Command Line Interface (CLI) to export/import a volume group to a different storage array.

Detailed instructions for migrating a volume group are provided in the NetApp Knowledge Base.

Unlock drives when using external key management

If you configured external key management and then later move secure-enabled drives from one storage array to another, you must re-assign the security key to the new storage array to gain access to the encrypted data on the drives.

Before you begin

- On the source array (the array where you are removing the drives), you have exported volume groups and removed the drives. On the target array, you have re-installed the drives.

  > The Export/Import function is not supported in the System Manager user interface; you must use the Command Line Interface (CLI) to export/import a volume group to a different storage array.

  Detailed instructions for migrating a volume group are provided in the NetApp Knowledge Base. Be sure to follow the appropriate instructions for newer arrays managed by System Manager or for legacy systems.

- The Drive Security feature must be enabled. Otherwise, a Cannot Create Security Key dialog box opens during this task. If necessary, contact your storage vendor for instructions on enabling the Drive Security feature.
- You must know the key management server's IP address and port number.
- You have a signed client certificate file for the storage array's controllers, and you have copied that file to the host where you are accessing System Manager. A client certificate validates the storage array's controllers, so the key management server can trust their Key Management Interoperability Protocol (KMIP) requests.
- You must retrieve a certificate file from the key management server, and then copy that file to the host where you are accessing System Manager. A key management server certificate validates the key management server, so the storage array can trust its IP address. You can use a root, intermediate, or server certificate for the key management server.

> For more information about the server certificate, consult the documentation for your key management server.

About this task

When you use external key management, the security key is stored externally on a server designed to safe-guard security keys. A security key is a string of characters that is shared by the controller and drives for read/write access. When the drives are physically removed from the array and installed in another, they cannot operate until you provide the correct security key.

You can create either an internal key from the controller's persistent memory or an external key from a key management server. This topic describes unlocking data when *external* key management is used. If you used *internal* key management, see Unlock drives when using internal key management. If you are performing a controller upgrade and are swapping all controllers for the latest hardware, you must follow different steps as described in the E-Series and SANtricity documentation center, in Unlock drives.

Once you reinstall secure-enabled drives in another array, that array discovers the drives and displays a "Needs Attention" condition along with a status of "Security Key Needed." To unlock drive data, you import the security key file and enter the pass phrase for the key. (This pass phrase is not the same as the storage array's Administrator password.) During this process, you configure the storage array to use an external key management server and then the secure key will be accessible. You are required to provide contact information of the server for the storage array to connect and retrieve the security key.

If other secure-enabled drives are installed in the new storage array, they might use a different security key than the one you are importing. During the import process, the old security key is used only to unlock the data for the drives you are installing. When the unlock process is successful, the newly installed drives are re-keyed to the target storage array's security key.

Steps

1. Select **Settings › System**.
2. Under **Security key management**, select **Create External Key**.
3. Complete the wizard with the prerequisite connection information and certificates.
4. Click **Test Communication** to ensure access to the external key management server.
5. Select **Unlock Secure Drives**.

   The Unlock Secure Drives dialog box opens. Any drives that require a security key are shown in the table.
6. **Optional:** hover the mouse over a drive number to see the location of the drive (shelf number and bay number).
7. Click **Browse**, and then select the security key file that corresponds to the drive you want to unlock.

   The key file you selected appears in the dialog box.
8. Enter the pass phrase associated with this key file.

   The characters you enter are masked.
9. Click **Unlock**.

   If the unlock operation is successful, the dialog box displays: "The associated secure drives have been unlocked."

Results

When all drives are locked and then unlocked, each controller in the storage array will reboot. However, if there are already some unlocked drives in the target storage array, then the controllers will not reboot.

After you finish

On the destination array (the array with the newly installed drives), you can now import volume groups.

The Export/Import function is not supported in the System Manager user interface; you must use the Command Line Interface (CLI) to export/import a volume group to a different storage array.

Detailed instructions for migrating a volume group are provided in the NetApp Knowledge Base.

Copyright information

Trademark information