NetApp

Drive security

SANtricity software

NetApp
March 12, 2026

Table of Contents

Drive security

Learn about drive security in SANtricity System Manager

You can configure Drive Security and key management from the Security Key Management page.

What is Drive Security?

Drive Security is a feature that prevents unauthorized access to data on secure-enabled drives when removed from the storage array. These drives can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives. When FDE or FIPS drives are physically removed from the array, they cannot operate until they are installed in another array, at which point, the drives will be in a Security Locked state until the correct security key is provided. A *security key* is a string of characters that is shared between these types of drives and the controllers in a storage array.

Learn more:

- How the Drive Security feature works
- How security key management works
- Drive Security terminology

How do I configure key management?

To implement Drive Security, you must have either FDE drives or FIPS drives installed in the array. To configure key management for these drives, you go to **Settings › System › Security key management** where you can create either an internal key from the controller's persistent memory or an external key from a key management server. Finally, you enable Drive Security for pools and volume groups by selecting "secure-capable" in the volume settings.

Learn more:

- Create internal security key
- Create external security key
- Create pool manually
- Create volume groups

How do I unlock drives?

If you configured 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.

Learn more:

- Unlock drives when using internal key management
- Unlock drives when using external key management

Related information

Learn more about tasks related to key management:

- Use CA-signed certificates for authentication with a key management server
- Back up security key

Concepts

How the Drive Security feature works in SANtricity System Manager

Drive Security is a storage array feature that provides an extra layer of security with either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.

When these drives are used with the Drive Security feature, they require a security key for access to their data. When the drives are physically removed from the array, they cannot operate until they are installed in another array, at which point, they will be in a Security Locked state until the correct security key is provided.

How to implement Drive Security

To implement Drive Security, you perform the following steps.

1. Equip your storage array with secure-capable drives, either FDE drives or FIPS drives. (For volumes that require FIPS support, use only FIPS drives. Mixing FIPS and FDE drives in a volume group or pool will result in all drives being treated as FDE drives. Also, an FDE drive cannot be added to or used as a spare in an all-FIPS volume group or pool.)

2. Create a security key, which is a string of characters that is shared by the controller and drives for read/write access. You can create either an internal key from the controller's persistent memory or an external key from a key management server. For external key management, authentication must be established with the key management server.

3. Enable Drive Security for pools and volume groups:

   - Create a pool or volume group (look for **Yes** in the **Secure-capable** column in the Candidates table).
   - Select a pool or volume group when you create a new volume (look for **Yes** next to **Secure-capable** in the pool and volume group Candidates table).

How Drive Security works at the drive level

A secure-capable drive, either FDE or FIPS, encrypts data during writes and decrypts data during reads. This encryption and decryption does not affect the performance or user workflow. Each drive has its own unique encryption key, which can never be transferred from the drive.

The Drive Security feature provides an extra layer of protection with secure-capable drives. When volume groups or pools on these drives are selected for Drive Security, the drives look for a security key before allowing access to the data. You can enable Drive Security for pools and volume groups at any time, without affecting existing data on the drive. However, you cannot disable Drive Security without erasing all data on the drive.

How Drive Security works at the storage array level

With the Drive Security feature, you create a security key that is shared between the secure-enabled drives and controllers in a storage array. Whenever power to the drives is turned off and on, the secure-enabled drives change to a Security Locked state until the controller applies the security key.

If a secure-enabled drive is removed from the storage array and re-installed in a different storage array, the drive will be in a Security Locked state. The re-located drive looks for the security key before it makes the data accessible again. To unlock the data, you apply the security key from the source storage array. After a successful unlock process, the re-located drive will then use the security key already stored in the target storage array, and the imported security key file is no longer needed.

> ⓘ For internal key management, the actual security key is stored on the controller in a non-accessible location. It is not in human-readable format, nor is it user-accessible.

How Drive Security works at the volume level

When you create a pool or volume group from secure-capable drives, you can also enable Drive Security for those pools or volume groups. The Drive Security option makes the drives and associated volume groups and pools secure-*enabled*.

Keep the following guidelines in mind before creating secure-enabled volume groups and pools:

- Volume groups and pools must be comprised entirely of secure-capable drives. (For volumes that require FIPS support, use only FIPS drives. Mixing FIPS and FDE drives in a volume group or pool will result in all drives being treated as FDE drives. Also, an FDE drive cannot be added to or used as a spare in an all-FIPS volume group or pool.)
- Volume groups and pools must be in an optimal state.

How security key management works in SANtricity System Manager

When you implement the Drive Security feature, the secure-enabled drives (FIPS or FDE) require a security key for data access. A security key is a string of characters that is shared between these types of drives and the controllers in a storage array.

Whenever power to the drives is turned off and on, the secure-enabled drives change to a Security Locked state until the controller applies the security key. If a secure-enabled drive is removed from the storage array, the drive's data is locked. When the drive is re-installed in a different storage array, it looks for the security key before it makes the data accessible again. To unlock the data, you must apply the original security key.

You can create and manage security keys using one of the following methods:

- Internal key management on the controller's persistent memory.
- External key management on an external key management server.

Internal key management

Internal keys are maintained and "hidden" in a non-accessible location on the controller's persistent memory. To implement internal key management, you perform the following steps:

1. Install secure-capable drives in the storage array. These drives can be Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.

2. Make sure the Drive Security feature is enabled. If necessary, contact your storage vendor for instructions on enabling the Drive Security feature.

3. Create an internal security key, which involves defining an identifier and a pass phrase. The identifier is a string that is associated with the security key, and is stored on the controller and on all drives associated with the key. The pass phrase is used to encrypt the security key for backup purposes. To create an internal key, go to **Settings › System › Security key management › Create Internal Key**.

The security key is stored on the controller in a hidden, non-accessible location. You can then create secure-enabled volume groups or pools, or you can enable security on existing volume groups and pools.

External key management

External keys are maintained on a separate key management server, using a Key Management Interoperability Protocol (KMIP). To implement external key management, you perform the following steps:

1. Install secure-capable drives in the storage array. These drives can be Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.

2. Make sure the Drive Security feature is enabled. If necessary, contact your storage vendor for instructions on enabling the Drive Security feature.

3. Obtain a signed, client certificate file. A client certificate validates the storage array's controllers, so the key management server can trust their KMIP requests.

   a. First, you complete and download a client Certificate Signing Request (CSR). Go to **Settings › Certificates › Key Management › Complete CSR**.

   b. Next, you request a signed client certificate from a CA that is trusted by the key management server. (You can also create and download a client certificate from the key management server using the CSR file.)

   c. Once you have a client certificate file, copy that file to the host where you are accessing System Manager.

   d. Alternatively, you can generate a certificate signing request externally using a private and public key pair.

4. 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.

5. Create an external key, which involves defining the IP address of the key management server and the port number used for KMIP communications. During this process, you also load certificate files. To create an external key, go to **Settings › System › Security key management › Create External Key**.

The system connects to the key management server with the credentials you entered. You can then create secure-enabled volume groups or pools, or you can enable security on existing volume groups and pools.

Learn about drive security terminology in SANtricity software

Learn how the Drive Security terms apply to your storage array.

Term	Description
Drive Security feature	Drive Security is a storage array feature that provides an extra layer of security with either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives. When these drives are used with the Drive Security feature, they require a security key for access to their data. When the drives are physically removed from the array, they cannot operate until they are installed in another array, at which point, they will be in a Security Locked state until the correct security key is provided.
FDE drives	Full Disk Encryption (FDE) drives perform encryption on the disk drive at the hardware level. The hard drive contains an ASIC chip that encrypts data during writes, and then decrypts data during reads.
FIPS drives	FIPS drives use Federal Information Processing Standards (FIPS) 140-2 level 2. They are essentially FDE drives that adhere to United States government standards for ensuring strong encryption algorithms and methods. FIPS drives have higher security standards than FDE drives.
Management client	A local system (computer, tablet, etc.) that includes a browser for accessing System Manager.
Pass phrase	The pass phrase is used to encrypt the security key for backup purposes. The same pass phrase used to encrypt the security key must be provided when the backed up security key is imported as the result of a drive migration or head swap. A pass phrase can have between 8 and 32 characters. ⓘ The pass phrase for Drive Security is independent from the storage array's Administrator password.
Secure-capable drives	Secure-capable drives can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives, which encrypt data during writes and decrypt data during reads. These drives are considered secure-*capable* because they can be used for additional security using the Drive Security feature. If the Drive Security feature is enabled for volume groups and pools used with these drives, the drives become secure-*enabled*.
Secure-enabled drives	Secure-enabled drives are used with the Drive Security feature. When you enable the Drive Security feature and then apply Drive Security to a pool or volume group on secure-*capable* drives, the drives become secure-*enabled*. Read and write access is available only through a controller that is configured with the correct security key. This added security prevents unauthorized access to the data on a drive that is physically removed from the storage array.

Term	Description
Security key	A security key is a string of characters that is shared between the secure-enabled drives and controllers in a storage array. Whenever power to the drives is turned off and on, the secure-enabled drives change to a Security Locked state until the controller applies the security key. If a secure-enabled drive is removed from the storage array, the drive's data is locked. When the drive is re-installed in a different storage array, it looks for the security key before it makes the data accessible again. To unlock the data, you must apply the original security key. You can create and manage security keys using one of the following methods: • Internal key management — Create and maintain security keys on the controller's persistent memory. • External key management — Create and maintain security keys on an external key management server.
Security key identifier	The security key identifier is a string that is associated with the security key during key creation. The identifier is stored on the controller and on all drives associated with the security key.

Configure security keys

Create an internal security key in SANtricity System Manager

To use the Drive Security feature, you can create an internal security key that is shared by the controllers and secure-capable drives in the storage array. Internal keys are maintained on the controller's persistent memory.

Before you begin

• Secure-capable drives must be installed in the storage array. These drives can be Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.

• 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.

> ⓘ If both FDE and FIPS drives are installed in the storage array, they all share the same security key.

About this task

In this task, you define an identifier and a pass phrase to associate with the internal security key.

> ⓘ The pass phrase for Drive Security is independent from the storage array's Administrator password.

Steps

1. Select **Settings › System**.

2. Under **Security key management**, select **Create Internal Key**.

If you have not yet generated a security key, the Create Security Key dialog box opens.

3. Enter information in the following fields:

   ◦ **Define a security key identifier** — You can either 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, appended to both ends of the string you enter. The generated characters ensure that the identifier is unique.

   ◦ **Define a pass phrase/Re-enter pass phrase** — Enter and confirm a 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).

   > ⚠ **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 **Create**.

   The security key is stored on the controller in a non-accessible location. Along with the actual key, there is an encrypted key file that is downloaded from your browser.

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

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

Results

You can now create secure-enabled volume groups or pools, or you can enable security on existing volume groups and pools.

> ⓘ Whenever power to the drives is turned off and then on again, all the secure-enabled drives change to a Security Locked state. In this state, the data is inaccessible until the controller applies the correct security key during drive initialization. If someone physically removes a locked drive and installs it in another system, the Security Locked state prevents unauthorized access to its data.

After you finish

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

Create an external security key in SANtricity System Manager

To use the Drive Security feature with a key management server, you must create an external key that is shared by the key management server and the secure-capable drives in the storage array.

Before you begin

- Secure-capable drives must be installed in the array. These drives can be Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.

  > ⓘ If both FDE and FIPS drives are installed in the storage array, they all share the same security key.

- 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 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

In this task, you define the IP address of the key management server and the port number it uses, and then load certificates for external key management.

Steps

1. Select **Settings › System**.

2. Under **Security key management**, select **Create External Key**.

   > ⓘ If internal key management is currently configured, a dialog box opens and asks you to confirm that you want to switch to external key management.

   The Create External Security Key dialog box opens.

3. Under **Connect to Key Server**, enter 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 KMIP communications. The most common port number used for key management server communications is 5696.

   Optional: If you want to configure a backup key server, click **Add Key Server**, and then enter that server's information. The second key server will be used if the primary key server cannot be reached. Make sure that each key server has access to the same database of keys; otherwise, the array will post errors and cannot use the backup server.

   > ⓘ Only a single key server is used at a time. If the storage array cannot reach the primary key server, the array will contact the backup key server. Be aware that you must maintain parity across both servers; failure to do so may result in errors.

- **Select client certificate** — Click the first **Browse** button to select the certificate file for the storage array's controllers.

- **Select private key file** — If needed, click the second **Browse** button to select a private key file file for the storage array's controllers.

- **Select key management server's server certificate** — Click the third **Browse** button to select the certificate file for the key management server. You can choose a root, intermediate, or server certificate for the key management server.

4. Click **Next**.

5. Under **Create/Backup Key**, you can create a backup key for security purposes.

   - (Recommended) To create a backup key, keep the checkbox selected, and then enter and confirm a 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).

   > ⚠ **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 pass phrase to unlock drive data.

   - If you do not want to create a backup key, deselect the checkbox.

   > ⚠ Be aware that if you lose access to the external key server and you do not have a backup key, you will lose access to data on the drives if they are migrated to another storage array. This option is the only method for creating a backup key in System Manager.

6. Click **Finish**.

   The system connects to the key management server with the credentials you entered. A copy of the security key is then stored on your local system.

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

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

   The page displays the following message with additional links for external key management:

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

8. Test the connection between the storage array and the key management server by selecting **Test Communication**.

   Test results display in the dialog box.

Results

When external key management is enabled, you can create secure-enabled volume groups or pools, or you can enable security on existing volume groups and pools.

> ⓘ Whenever power to the drives is turned off and then on again, all the secure-enabled drives change to a Security Locked state. In this state, the data is inaccessible until the controller applies the correct security key during drive initialization. If someone physically removes a locked drive and installs it in another system, the Security Locked state prevents unauthorized access to its data.

After you finish

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

Manage security keys

Change a security key in SANtricity System Manager

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 in SANtricity System Manager

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 in SANtricity System Manager

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 keys in SANtricity System Manager

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 in SANtricity System Manager

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 in SANtricity System Manager

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 in SANtricity System Manager

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.

> ℹ️ 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.

Storage drive security FAQ for SANtricity System Manager

This FAQ can help if you're just looking for a quick answer to a question.

What do I need to know before creating a security key?

A security key is shared by controllers and secure-enabled drives within a storage array. If a secure-enabled drive is removed from the storage array, the security key protects the data from unauthorized access.

You can create and manage security keys using one of the following methods:

- Internal key management on the controller's persistent memory.
- External key management on an external key management server.

Internal key management

Internal keys are maintained and "hidden" in a non-accessible location on the controller's persistent memory. Before creating an internal security key, you must do the following:

1. Install secure-capable drives in the storage array. These drives can be Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.
2. Make sure the Drive Security feature is enabled. If necessary, contact your storage vendor for instructions on enabling the Drive Security feature.

You can then create an internal security key, which involves defining an identifier and a pass phrase. The identifier is a string that is associated with the security key, and is stored on the controller and on all drives associated with the key. The pass phrase is used to encrypt the security key for backup purposes. When you are finished, the security key is stored on the controller in a non-accessible location. You can then create secure-enabled volume groups or pools, or you can enable security on existing volume groups and pools.

External key management

External keys are maintained on a separate key management server, using a Key Management Interoperability Protocol (KMIP). Before creating an external security key, you must do the following:

1. Install secure-capable drives in the storage array. These drives can be Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.
2. Make sure the Drive Security feature is enabled. If necessary, contact your storage vendor for instructions on enabling the Drive Security feature.
3. Obtain a signed, client certificate file. A client certificate validates the storage array's controllers, so the key management server can trust their KMIP requests.
   a. First, you complete and download a client Certificate Signing Request (CSR). Go to **Settings › Certificates › Key Management › Complete CSR**.
   b. Next, you request a signed client certificate from a CA that is trusted by the key management server. (You can also create and download a client certificate from the key management server using the

downloaded CSR file.)

    c. Once you have a client certificate file, copy that file to the host where you are accessing System Manager.

4. 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.

You can then create an external key, which involves defining the IP address of the key management server and the port number used for KMIP communications. During this process, you also load certificate files. When you are finished, the system connects to the key management server with the credentials you entered. You can then create secure-enabled volume groups or pools, or you can enable security on existing volume groups and pools.

Why do I need to define a pass phrase?

The pass phrase is used to encrypt and decrypt the security key file stored on the local management client. Without the pass phrase, the security key cannot be decrypted and used to unlock data from a secure-enabled drive if it is re-installed in another storage array.

Why is it important to record security key information?

If you lose the security key information and do not have a backup, you could lose data when relocating secure-enabled drives or upgrading a controller. You need the security key to unlock data on the drives.

Be sure to record the security key identifier, the associated pass phrase, and the location on the local host where the security key file was saved.

What do I need to know before backing up a security key?

If your original security key becomes corrupted and you do not have a backup, you will lose access to the data on drives if they are migrated from one storage array to another.

Before backing up a security key, keep these guidelines in mind:

- Make sure you know the security key identifier and pass phrase of the original key file.

  (i) Only internal keys use identifiers. When you created the identifier, additional characters were generated automatically and appended to both ends of the identifier string. The generated characters ensure that the identifier is unique.

- 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 only applied to the backup you are creating.

  (i) The pass phrase for Drive Security should not be confused with the storage array's Administrator password. The pass phrase for Drive Security protects backups of a security key. The Administrator password protects the entire storage array from unauthorized access.

- The backup security key file is downloaded to your management client. The path for the downloaded file might depend on the default download location of your browser. Be sure to make a record of where your

security key information is stored.

What do I need to know before unlocking secure drives?

To unlock the data from a secure-enabled drive, you must import its security key.

Before unlocking secure-enabled drives, keep the following guidelines in mind:

- The storage array must already have a security key. The migrated drives will be re-keyed to the target storage array.
- For the drives you are migrating, you must know the security key identifier and the pass phrase that corresponds to the security key file.
- The security key file must be available on the management client (the system with a browser used for accessing System Manager).
- If you are resetting a locked NVMe drive, you must enter the drive's security ID. To locate the security ID, you must physically remove the drive and find the PSID string (maximum of 32 characters) on the drive's label. Make sure the drive is reinstalled before you start the operation.

What is read/write accessibility?

The Drive Settings window includes information about the Drive Security attributes. "Read/Write Accessible" is one of the attributes that displays if a drive's data has been locked.

To view Drive Security attributes, go to the Hardware page. Select a drive, click **View settings**, and then click **Show more settings**. At the bottom of the page, the Read/Write Accessible attribute value is **Yes** when the drive is unlocked. The Read/Write Accessible attribute value is **No, invalid security key** when the drive is locked. You can unlock a secure drive by importing a security key (go to **Settings › System › Unlock Secure Drives**).

What do I need to know about validating the security key?

After creating a security key, you should validate the key file to make sure it is not corrupt.

If the validation fails, do the following:

- If the security key identifier does not match the identifier on the controller, locate the correct security key file and then try the validation again.
- If the controller cannot decrypt the security key for validation, you might have incorrectly entered the pass phrase. Double-check the pass phrase, re-enter it if necessary, and then try the validation again. If the error message appears again, select a backup of the key file (if available) and re-try validation.
- If you still cannot validate the security key, the original file might be corrupted. Create a new backup of the key and validate that copy.

What is the difference between internal security key and external security key management?

When you implement the Drive Security feature, you can use an internal security key or an external security key to lock down data when a secure-enabled drive is removed from the storage array.

A security key is a string of characters, which is shared between the secure-enabled drives and controllers in a storage array. Internal keys are maintained on the controller's persistent memory. External keys are maintained

on a separate key management server, using a Key Management Interoperability Protocol (KMIP).