Configure security keys

SANtricity 11.7

NetApp
February 12, 2024

Table of Contents

Configure security keys

Create internal security key

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 external security key

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 key management server's server certificate** — Click the second **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.

Copyright information

Trademark information