Encryption Key Best Practices

Nasuni Corporation – Boston, MA

Summary of Best Practices Recommendations

The best practices for managing encryption keys for the Nasuni Filer include the following:

- If your enterprise has existing OpenPGP-compatible encryption keys that you want to use to encrypt your data, do the following:
  - Upload your encryption keys to the Nasuni Filer. All uploaded encryption keys should be at least 2048 bits long.
  - Safeguard your encryption keys with at least one, if not all, of the following options:
    - Escrow your uploaded encryption keys with Nasuni.
    - Safeguard your original encryption key files with your own encryption key management system.

      ***Warning**: Do **NOT** save encryption key files to a volume on a Nasuni Filer. You will **NOT** be able to use this to recover data. This is **NOT** how to upload encryption keys to a Nasuni Filer. To upload encryption keys to a Nasuni Filer, select **Configuration → Encryption Keys**.*
    - Safeguard your original encryption key files with a trusted third-party escrow service.
- If you use the encryption keys that the Nasuni Filer generates, do the following:
  - Generate encryption keys.

    Important: The time to generate an encryption key can vary widely, depending on the hardware (real or virtual) that the Nasuni Filer is executing on. Encryption keys are generated in the background, so as to not block use of the Nasuni Filer during generation.
  - Download the generated encryption keys from the Nasuni Filer.
  - Safeguard your encryption keys with at least one, if not both, of the following options:
    - Safeguard your original encryption key files with your own encryption key management system.

***Warning**: Do **NOT** save encryption key files on a volume on a Nasuni Filer. You will **NOT** be able to use this to recover data.*

- Safeguard your original encryption key files with a trusted third-party escrow service.

- Be aware that all generated encryption keys are automatically escrowed with Nasuni.

- Download and safeguard encryption keys whenever you create a new volume on the Nasuni Filer for which you have used the Nasuni Filer to generate a new encryption key.
- If you share volumes across multiple Nasuni Filers using the Remote Access feature, use the "custom" setting to explicitly grant access to only specific Filers. Do not simply select "Read/Write" or "Read Only" to apply to all Filers.

Introduction

The Nasuni Filer automatically encrypts your data using the OpenPGP encryption protocol at your premises before transmitting data to cloud storage. Your data remains encrypted in cloud storage. You control the encryption keys to encrypt and decrypt your data.

While this security feature ensures that only you can access your data, you must manage your encryption keys properly. For example, if you ever need to perform a disaster recovery procedure on your Nasuni Filer, you MUST have the encryption keys for ALL volumes owned by that Nasuni Filer to successfully regain access to your data.

The Nasuni Filer offers a number of features that help you to manage your encryption keys. However, you must be proactive about safeguarding your encryption keys, because not all of these features are automatic.

Three Options for Safeguarding Encryption Keys

You have three options for safeguarding your encryption keys, each with advantages and disadvantages:

- **Escrow encryption keys with Nasuni**: You can escrow your encryption keys with Nasuni. Your encryption key is protected on Nasuni servers using the same security practices that we use for our own encryption keys, including access limited to necessary personnel. Escrowing an encryption key with Nasuni means that you can, at any time, request the encryption key from Nasuni during a disaster recovery. One advantage of this option is that it is simple to perform and can offer greater recovery assurance if your internal encryption key management process is less mature or has not been assessed for completeness. One disadvantage is that your encryption keys are not directly under your sole control.

While Nasuni offers escrow capability for encryption keys generated by your Nasuni Filer, we do not mandate that you do so, because many organizations are subject to regulation or internal policies that require internal encryption key management.

> ***Caution**: Any time a third party has access to your encryption keys, they could be less secure.*
>
> ***Tip**: You must have the correct name, company, address, phone number, and email address for your Nasuni.com account before Nasuni will de-escrow your encryption keys. You must keep this information.*

- **Safeguard your encryption keys yourself**: You can keep your encryption keys in a secure location. One advantage of this option is that your encryption keys are directly under your control. One disadvantage is that you must develop and maintain your own system of encryption key management.

  > ***Warning**: Do **NOT** save encryption key files on a volume on a Nasuni Filer. You will **NOT** be able to use this to recover data.*

- **Escrow your encryption keys with a trusted third-party service**: You can entrust your encryption keys to a trusted third-party escrow service. One advantage of this option is that you do not have to develop and maintain your own system of encryption key management. One disadvantage is that you must depend on the third-party service when you want to access your encryption keys.

  > ***Caution**: Any time a third party has access to your encryption keys, they could be less secure.*

You should consider all three options and decide which option makes the most sense for your enterprise, for both security and convenience. Utilizing multiple options can increase the assurance levels for recovering encryption keys, but will also decrease the assurance of the confidentiality of encryption keys. These factors must be uniquely balanced based on your organization's risk management profile.

Two Sources of Encryption Keys

There are two sources for the encryption keys that the Nasuni Filer uses:

- **Uploaded encryption keys**: If your enterprise has existing OpenPGP-compatible encryption keys that you want to use to encrypt your data, you can upload them to the Nasuni Filer. You have three options for safeguarding uploaded encryption keys:
  - Escrow uploaded encryption keys with Nasuni.
  - Safeguard your encryption key files yourself.
  - Escrow your encryption key files with a trusted third party.

  All uploaded encryption keys should be at least 2048 bits long.

Warning: You cannot later download encryption keys from the Nasuni Filer that have previously been uploaded, so it is essential that you safeguard the original encryption key files.

- **Generated encryption keys**: When you create a volume, you have the option of having the Nasuni Filer create (generate) a new encryption key for that volume.

  Important: The time to generate an encryption key can vary widely, depending on the hardware (real or virtual) that the Nasuni Filer is executing on. Encryption keys are generated in the background, so as to not block use of the Nasuni Filer during generation.

  Generated encryption keys are automatically escrowed with Nasuni. You have two additional options for safeguarding generated encryption keys:

  - Download generated encryption keys and safeguard the encryption key files yourself.
  - Download generated encryption keys and escrow the encryption key files with a trusted third party.

  Warning: After performing a disaster recovery procedure on a Nasuni Filer, you can no longer download generated encryption keys. For this reason, you should download generated encryption keys and safeguard them before it is necessary to perform a disaster recovery.

  Note: Any encryption key escrowed with Nasuni remains escrowed, regardless of whether the encryption key was uploaded as part of a disaster recovery process.

Nasuni Filer Features for Managing Encryption Keys

The Nasuni Filer offers several features for managing encryption keys, using the Nasuni Filer itself, or using the Nasuni Management Console if the Nasuni Filer is under the control of the Nasuni Management Console.

Automatic escrow of generated encryption keys

When you create a volume, you have the option of having the Nasuni Filer create (generate) a new encryption key for that volume. Generated encryption keys are automatically escrowed with Nasuni.

Important: The time to generate an encryption key can vary widely, depending on the hardware (real or virtual) that the Nasuni Filer is executing on. Encryption keys are generated in the background, so as to not block use of the Nasuni Filer during generation.

Uploading your existing encryption keys

If your enterprise has existing OpenPGP-compatible encryption keys that you want to use to encrypt your data, you can upload them to the Nasuni Filer. All uploaded encryption keys should be at least 2048 bits long.

On the Nasuni Filer, to upload an encryption key:

1. From the **Configuration** menu, select **Encryption Keys**. The **Encryption Keys** page appears.
2. Click **Upload Encryption Key(s)**. The **Import OpenPGP Key(s)** page appears.
3. Click **Choose File**, then navigate to the encryption key file. This file should be OpenPGP-compatible.
4. Click **Import Key**. The encryption key is imported to the Nasuni Filer.

The uploaded encryption key is now available to assign to a volume.

On the Nasuni Management Console, to upload an encryption key:

1. Click **Filers**, then select **Encryption Keys**. The **Filer Encryption Keys** page appears.
2. Click **Upload Encryption Keys**. The **Import Key(s)** dialog box appears.
3. Select the managed Nasuni Filers to which you want to upload the encryption key.
4. Click **Choose File**, then navigate to the encryption key file. This file should be OpenPGP-compatible.
5. Click **Import Key**. The encryption key is imported to the Nasuni Filer.

The uploaded encryption key is now available to assign to a volume on the selected managed Nasuni Filers.

Escrowing uploaded encryption keys with Nasuni

You can escrow your uploaded encryption key with Nasuni.

> **Note**: Generated encryption keys are automatically escrowed with Nasuni.

On the Nasuni Filer, to escrow an uploaded encryption key with Nasuni:

1. From the **Configuration** menu, select **Encryption Keys**. The **Encryption Keys** page appears.
2. For the encryption key that you want to escrow with Nasuni, click "**Escrow key with Nasuni**". The "**Escrow your encryption key with Nasuni**" page appears.
3. Enter a **Username** (case-sensitive) and **Password** (case-sensitive) that has permission to perform this operation.

4. Click **Escrow Key**. Your encryption key is escrowed with Nasuni.

The escrowed encryption key is now available from Nasuni whenever you need it.

On the Nasuni Management Console, to escrow an uploaded encryption key with Nasuni:

1. Click **Filers**, then select Encryption **Keys**. The **Filer Encryption Keys** page appears.
2. For the encryption key that you want to escrow with Nasuni, click **Escrow Key with Nasuni**. The **Escrow Encryption Key** dialog box appears.
3. Enter a **Username** (case-sensitive) and **Password** (case-sensitive) that has permission to perform this operation.
4. Click **Escrow Key**. Your encryption key is escrowed with Nasuni.

The escrowed encryption key is now available from Nasuni whenever you need it.

Downloading generated encryption keys (to safeguard or escrow)

You can download generated encryption keys, either to safeguard encryption keys yourself or to escrow encryption keys with a trusted third party.

On the Nasuni Filer only, to download a generated encryption key:

1. From the **Configuration** menu, select **Encryption Keys**. The **Encryption Keys** page appears.
2. Click **Download Generated Keys**. Depending on your browser, a message box may appear; if so, navigate to an appropriate folder and save this file. The file containing the encryption key is saved with a .pgp extension.

The file containing the generated encryption key is now available for you either to safeguard yourself or to escrow with a trusted third party.

> ***Warning**: Do **NOT** save encryption key files on a volume on a Nasuni Filer. You will **NOT** be able to use this to recover data.*

Encryption Keys and Remote Access

When using the Remote Access feature of a Nasuni Filer, a given volume is made available for access on multiple Filers. To make this work, the encryption key for the volume must be replicated to the other Filers selected to have access. This replication is performed securely by encrypting that volume's encryption key with a key specific to each Filer, which Nasuni does not have access to. To ensure that this key is not transmitted to an unintended Filer, you should explicitly select those Filers to be given access to the volume, and thus the associated key, rather than automatically allowing any Filer on the account to be given access.

You do this by selecting "custom" when configuring Remote Access Permissions, not Read Only or Read/Write.

Best Practices

Based on the two sources of encryption keys, and the three options for safeguarding encryption keys, the best practices for managing encryption keys for the Nasuni Filer are summarized at the beginning of this document.

Conclusion

Safeguarding your encryption keys is a necessary part of securing your data. Make sure that you have either escrowed your encryption keys with Nasuni, downloaded and safeguarded your encryption keys yourself, or escrowed your encryption keys with a trusted third party. Utilizing multiple methods can serve to increase the assurance of recovering encryption keys, but reduces the confidentiality assurance due to multi-party encryption key distribution. Depending on your unique risk profile, you can adjust your approach to best balance these considerations.