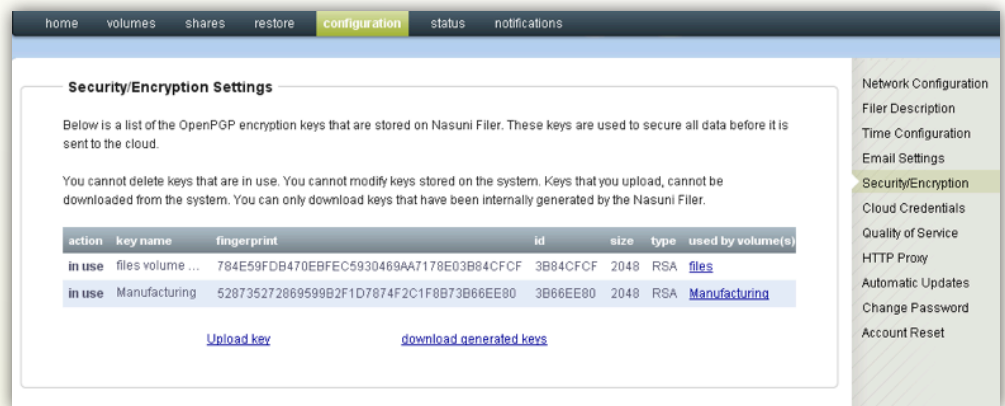


This document explains how to simulate a disaster recovery by powering down your current Nasuni Filer instance. Before you power down Nasuni Filer, make sure you know the names of your volumes and the data data stored in them. After the disaster recovery is complete, you need to check that your new Nasuni Filer instance has the correct volumes and associated data.

You can delete your current Nasuni Filer instance once you have verified that the new instance includes your volumes and data. Nasuni does not currently support running multiple Filers against a single account.

1. Login to Nasuni Filer
2. Click **Configuration**
3. Click **Security/Encryption** in the right pane
4. Click **Download Generated Keys**
5. Click **OK** when prompted

Note: It is strongly recommended you download your keys immediately after installation and keep the keys in a secure location.

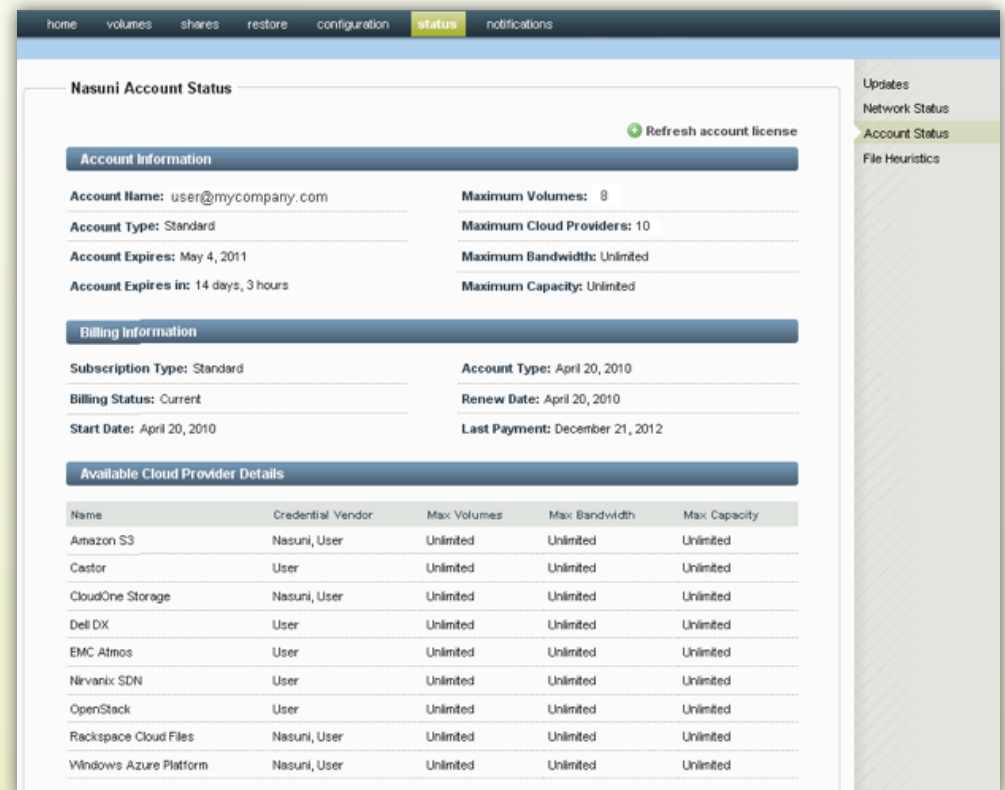


The screenshot shows the 'configuration' tab in the Nasuni Filer interface. The 'Security/Encryption Settings' section is active, displaying a list of OpenPGP encryption keys. Below the list are links for 'Upload key' and 'download generated keys'.

action	key name	fingerprint	id	size	type	used by volume(s)
in use	files volume ...	784E59FDB470EBFEC5930469AA7178E03B84CFCF	3B84CFCF	2048	RSA	files
in use	Manufacturing	528735272869599B2F1D7874F2C1F8B73B66EE00	3B66EE00	2048	RSA	Manufacturing

6. Click **Status**
7. Click **Account Status**
8. Shutdown the Filer and Power off the Virtual Machine

Note the email address in the Account Name field under Account Information. This is the Nasuni.com account to which your current Filer is associated.



The screenshot shows the 'status' tab in the Nasuni Filer interface. The 'Nasuni Account Status' section is active, displaying account information, billing information, and available cloud provider details.

Account Information

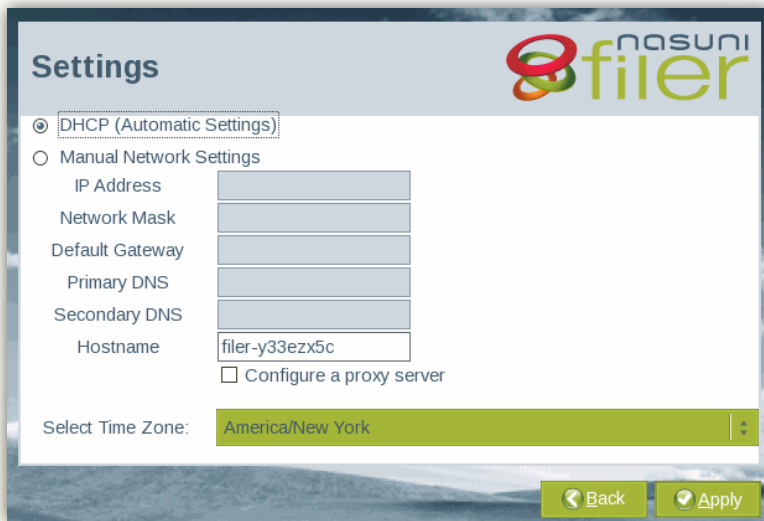
- Account Name: user@mycompany.com
- Account Type: Standard
- Account Expires: May 4, 2011
- Account Expires in: 14 days, 3 hours
- Maximum Volumes: 8
- Maximum Cloud Providers: 10
- Maximum Bandwidth: Unlimited
- Maximum Capacity: Unlimited

Billing Information

- Subscription Type: Standard
- Billing Status: Current
- Start Date: April 20, 2010
- Account Type: April 20, 2010
- Renew Date: April 20, 2010
- Last Payment: December 21, 2012

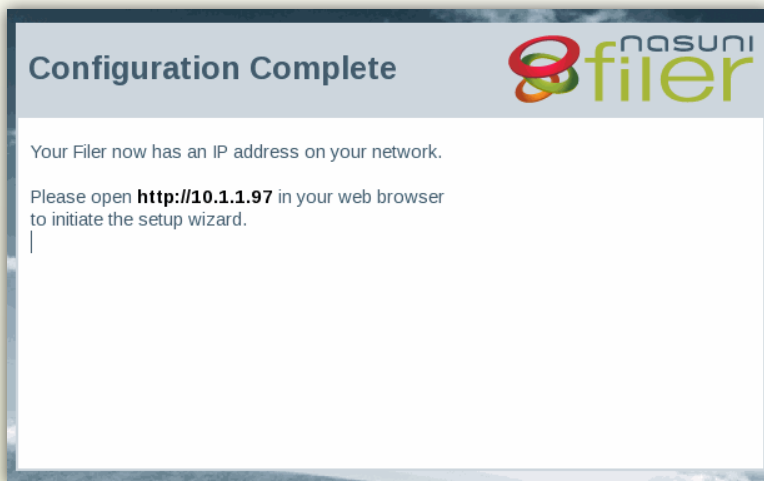
Available Cloud Provider Details

Name	Credential Vendor	Max Volumes	Max Bandwidth	Max Capacity
Amazon S3	Nasuni, User	Unlimited	Unlimited	Unlimited
Castor	User	Unlimited	Unlimited	Unlimited
CloudOne Storage	Nasuni, User	Unlimited	Unlimited	Unlimited
Dell DX	User	Unlimited	Unlimited	Unlimited
EMC Atmos	User	Unlimited	Unlimited	Unlimited
Nirvanix SDN	User	Unlimited	Unlimited	Unlimited
OpenStack	User	Unlimited	Unlimited	Unlimited
Rackspace Cloud Files	Nasuni, User	Unlimited	Unlimited	Unlimited
Windows Azure Platform	Nasuni, User	Unlimited	Unlimited	Unlimited



1. Select either **DHCP (Automatic Settings)** or **Manual Network Settings**. (Select *Manual Network Settings* to use the same IP address and hostname as the original Filer prior to the “disaster.”)
2. Select a **time zone** for your region. (The time zone is used for notifications and file sharing purposes.)
3. Click **Apply**.

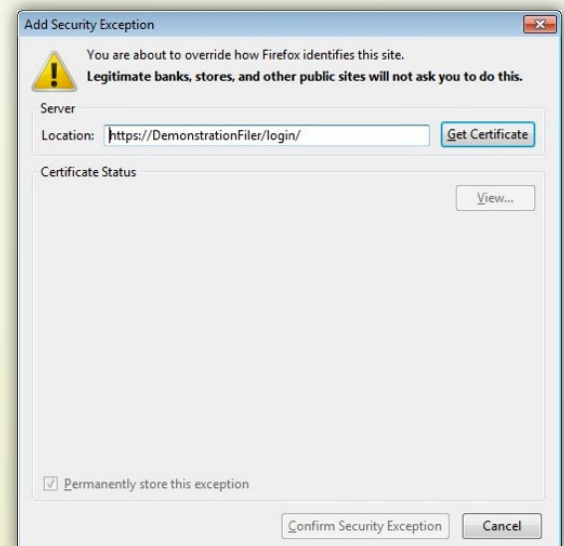
Note: Optionally, you can enable the Configure a proxy server checkbox to configure a proxy server if needed. If you check this option, the Proxy page appears where you can enter a proxy server, proxy port, username, and password. All HTTP traffic will then go through the specified proxy server.



In a few moments, a message appears telling you that setup is complete and specifies the IP address to use. **Configuration is now complete**

Adding a Security Exception

1. Launch your **web browser** and go to the **specified URL**.
2. The steps for adding a security certificate differ depending on the web browser you are using. For example, if you are using Mozilla Firefox: At the “This Connection is Untrusted Page,” click **I Understand the Risks**.
3. Click **Add Exception...**



Welcome to the Nasuni Filer wizard, which will guide you through the **quick, four-step** setup of your Filer. If you need help at any point, click on a nearby question mark icon.

Enter your nasuni.com credentials

Username

Password

Continue ▶

Click [here](#) if you are a new user or have lost your account password.

1. Enter the email address and the password for the Nasuni.com account associated with the Filer that you are recovering.
2. Click **Continue** to proceed.
3. You are prompted to recover your configuration.

Note : If you have forgotten or lost your account password, click on the hyperlink "click here" to go to www.nasuni.com where you can reset your password.

Previous Filer configuration detected!

We have detected a previous Filer attached to this account. To recover this configuration, you will need to have all your encryption keys on hand, unless you have escrowed your keys with Nasuni, in which case we will provide them for you.

Did you escrow any of your encryption keys with Nasuni?

Select one

Back **Continue** ▶

4. Confirm that you are recovering a previous Filer.

Upload Encryption Keys

As part of recovery, we are going to prompt you for each of the keys required to bring the system online. The table below lists each OpenPGP key needed. You will not be able to complete recovery unless we have all the required encryption keys.

You can upload key files containing single or multiple keys - please note that passphrases are only supported when uploading a single key at a time.

Key ID	Key Name	Acquired
776E1182	not uploaded	No

OpenPGP Keyfile **Browse...**

Key Passphrase

Upload Key ▶

5. **Browse** to your encryption keys and click **Upload Key**.



Filer Recovery Complete!

We have restored your previous configuration including metrics, share and configuration data. However, some configuration information such as network, proxy and Active Directory settings may have to be reconfigured.

The system will now reboot for the changes to take effect - your Filer will become available momentarily. Once rebooted, you will automatically be redirected to the Filer's login page. Alternatively, you can click [here](#) to proceed to the login page when the filer is done rebooting.

Note: If the previous Filer was in Active Directory mode, you need to re-join Active Directory to maintain ACL support. Refer to "Joining Nasuni Filer to an Active Directory Domain" in the Nasuni "How To" series for more information.

By following the steps in this document, you now understand the ease of restoring Nasuni Filer in a disaster recovery scenario. If you have other questions about the Nasuni Filer, or how it can benefit your organization, please visit www.nasuni.com or contact the Product Evaluation Team at (800) 208-3418.