NASUNI

Technical white paper

Nasuni Access Anywhere

Table of contents

Overview

One of today's biggest challenges for data storage is the ability to make files accessible to users no matter where they are located as organizations continue to support a distributed workforce.

The Nasuni File Data Platform now offers the Nasuni Access Anywhere add-on service to strategically address the security and performance needs of hybrid and remote workers.

How it enhances the Nasuni File Data Platform

When combined with the Nasuni core platform capabilities, Nasuni Access Anywhere delivers high-performance file access for remote and hybrid (distributed) users along with productivity tools that let them manage files from anywhere on any device. Additionally, integration with collaborative tools provides a seamless workflow across Microsoft Office 365, Microsoft Teams, and corporate file shares to ensure easy and secure access to critical corporate data.

Prerequisites: The Nasuni Access Anywhere add-on service requires the Nasuni Access Anywhere server.

Business Benefits

Better control and management: Maintain a single source of truth for all corporate file data with an auditable hybrid work solution, reducing the risk of shadow IT.

Increased security: Policy-governed solution that supports compliance with data regulations and internal security standards to ensure data is governed effectively.

Accelerated workflows: Built in acceleration of file sharing for hybrid and remote teams that allow them to allow them to synchronize and manage files from anywhere.

Enhanced user productivity: provide a solution that supports multiple file types with no file size limits.

Cost avoidance: Eliminate the need for multiple point solutions. Lower storage costs for corporate file shares backed by limitless, affordable object storage.

Use Cases

Nasuni Access Anywhere is a comprehensive solution for organizations with distributed workers, and should be deployed to ensure a uniform experience is delivered when it comes to accessing corporate files across any location.

Support remote and hybrid users: Users need high-performance file access to stay in sync with ongoing projects irrespective of their location, on-site or remote. It is essential for organizations to provide seamless access to central file data while maintaining centralized control.

Secure two-way external files and folder sharing: Organizations working with clients, contractors, and joint-venture partners need to share content, preferably without file size limits. Adopting third-party isolated solutions for large file transfer often leads to file data sprawl compromising control, performance, or security.

Key Features

Productivity tools:

File Transfer Acceleration: Upload and copy files with remarkable speed despite low bandwidth and network latency. Large files are split into pieces, sent in parallel over multiple streams and reassembled in a continuous file.

File/Folder Share: Supports two-way content sharing. Users can share files with external parties, add watermarks to protect documents and maintain authenticity.

Access & security

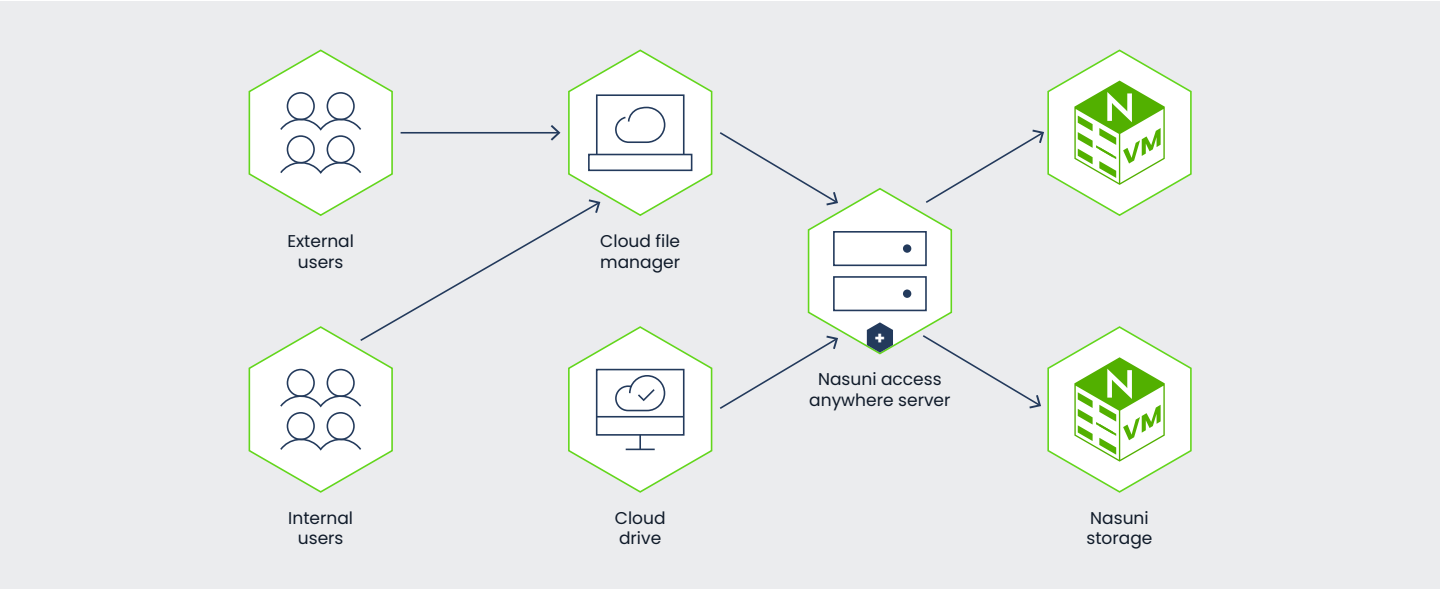
Microsoft Teams and Microsoft Office 365 Integration: Store, search, browse, and edit files from within Teams. Edit documents through Microsoft Office online apps.

2FA Secure Anywhere: Enables users to copy, move, lock, and share files and folders from the web, desktop, and mobile directly and securely with two-factor authentication.

Architecture

Overview

Users access their storage primarily through the Access Anywhere Cloud Drive, or via any web browser through the Cloud File Manager. External users can access shared files and folders through secure links, or through Microsoft Teams.



Cloud File Manager

The Cloud File Manager provides users remote access to all their file systems from any web browser. With support for search support, the ability to preview files, and collaborative web editing for office documents users can quickly find and work with the files they need. With Cloud Edit users can launch desktop applications for files directly from the web browser.

External users can access select files and folders through shared links. Authentication can be required, and users may also be allowed to upload and edit files.

Access Anywhere Server

The Access Anywhere Server supports remote access, search, file sharing and other services by indexing all files and folders - file names, size, timestamps and permissions. Files remain on their respective file systems and are only streamed to (or from) the client applications only when needed. This means user and applications can continue to access file systems directly, and users can access data remotely without needing to reconcile changes.

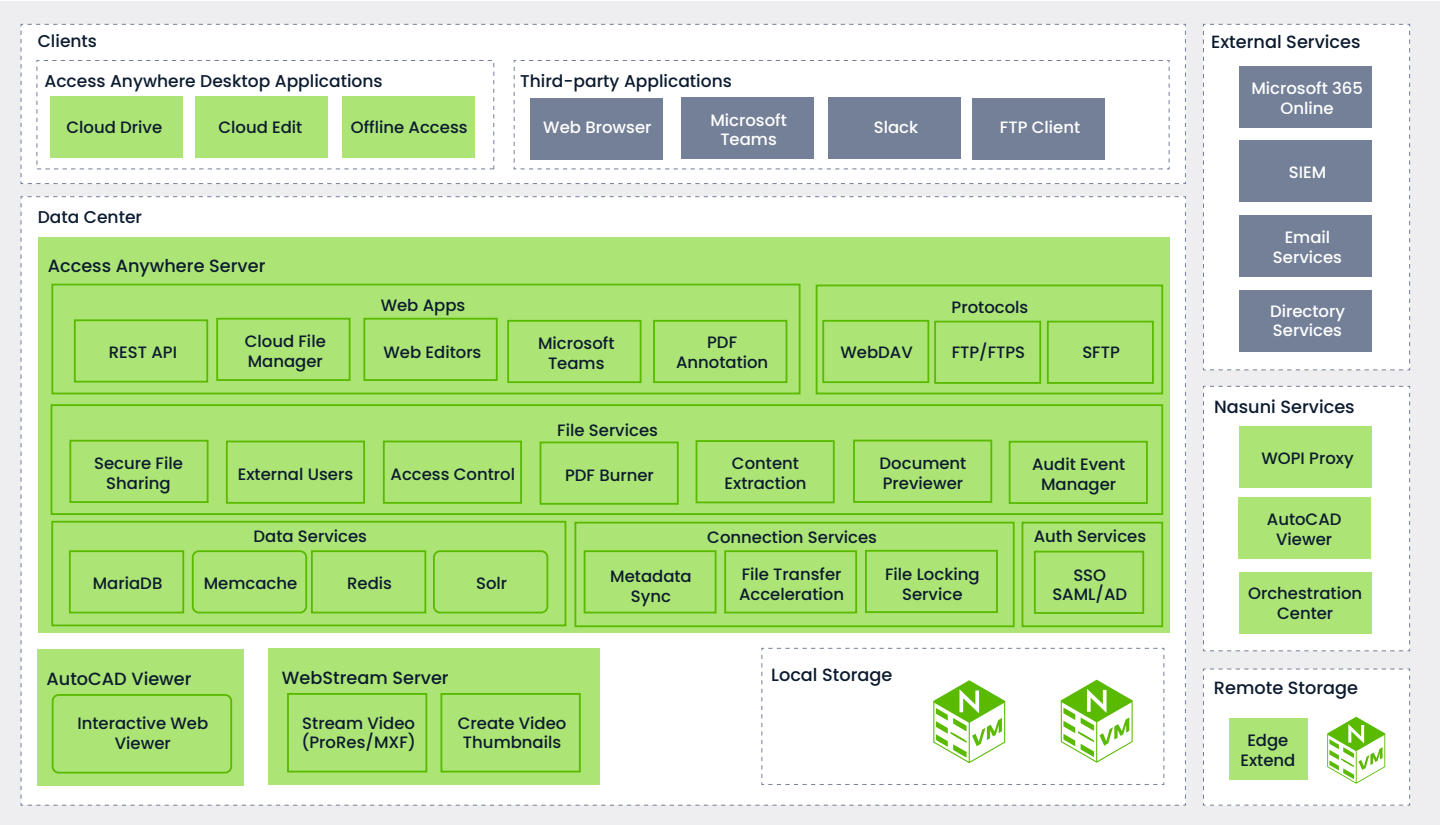
Component Architecture

The Nasuni Access Anywhere Server is built with a service-oriented or component-based architecture. These application and data services can be co-located on a single server or virtual machine or deployed across a cluster of many servers.

This diagram lists the primary components within the Access Anywhere Server as well as external services that may also be deployed.

Single Node Deployment

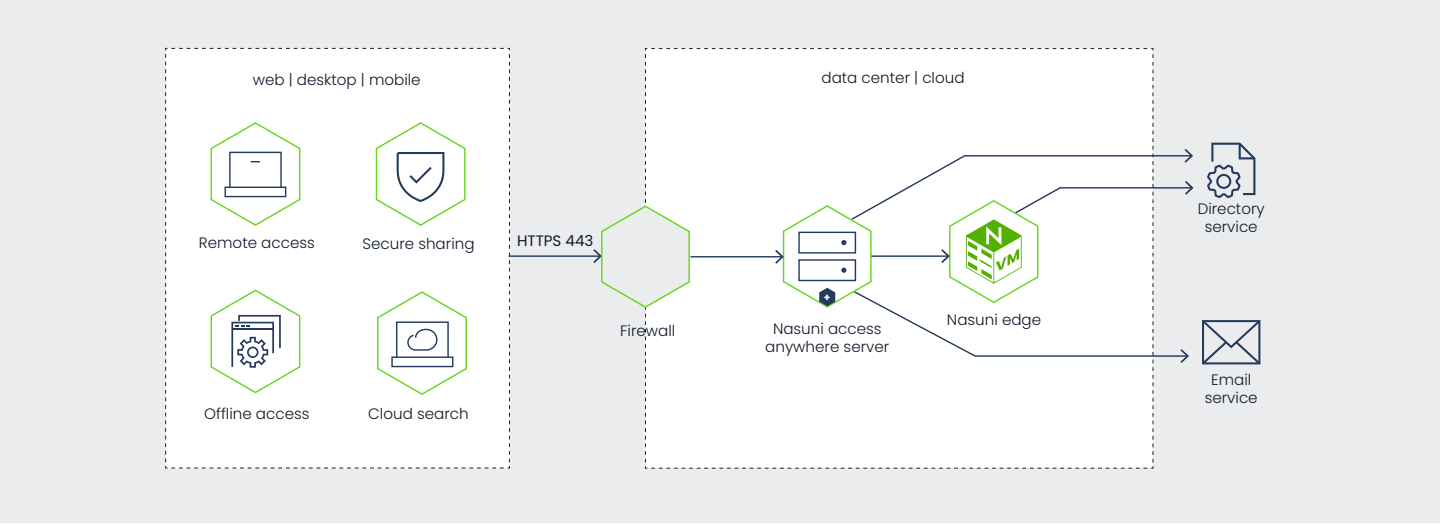
A Nasuni Access Anywhere site is built using a service-oriented or component-based architecture.



Application and data components can be co-located on a single server or virtual machine or deployed across a cluster of many servers. For small to mid-size environments, the solution is typically deployed as a single server or node.

It must be connected to an LDAP or SAML service for authentication, and to an email service for sharing links and sending verifications codes. VPN-less access is provided through desktop tools and a web application through a single public endpoint over HTTPS.

Nasuni Edge Appliances



An Access Anywhere site is deployed alongside one or more Nasuni Edge Appliances with the shares for which it is providing remote access and secure sharing to.

We recommend limiting the number of shares to 25-30 as each Multiuser SMB/ Nasuni provider adds about 0.25 seconds to the login time.

Node Sizing

A nod should be sized based on the expected user load and number of items indexed. As a starting point we recommend the following minimum configurations. For larger numbers of users or files see below for deployment options.

Technical Specifications	Small	Large
Max Users	500	1000
Max number of files	5M	50M
DB disk type	SSD	SSD
DB disk size (GB)	200	250
Processor cores (vCPUs)	8	16
VM memory (GB)	10	32

Access Anywhere - Getting Started

This chapter describes deploying and configuring the Nasuni Access Anywhere Server in a virtualization environment in your data center or cloud. For cloud deployments, see specific guides for Microsoft Azure and AWS.

Before Getting Started

Before you can complete this configuration guide, you will need the following information:

- Virtual machine image for your Hypervisor
- Nasuni Account access (for Serial Number)
- Linux smeconfiguser password
- Linux root user password
- Appliance appladmin password
- Storage system access for default storage and user storage
- (Recommended) Access to request / update DNS names for the appliance
- (Recommended) Outbound mail relay information
- (Optional) Active Directory service account for connecting to AD

Configure Public Endpoint

Applications access the server through a public endpoint, a fully qualified domain name that resolves to a public IP address. The public IP address routes to the virtual appliance usually through a firewall or load balancer. Apply the SSL certificates, and if needed, open ports.

Add DNS Host Records

Name-based virtual hosts are used to provide multiple protocols for the same ports. For single VM installations, the first domain name is typically the name of the host.

Choose three fully qualified domain names (FQDNs). For example:

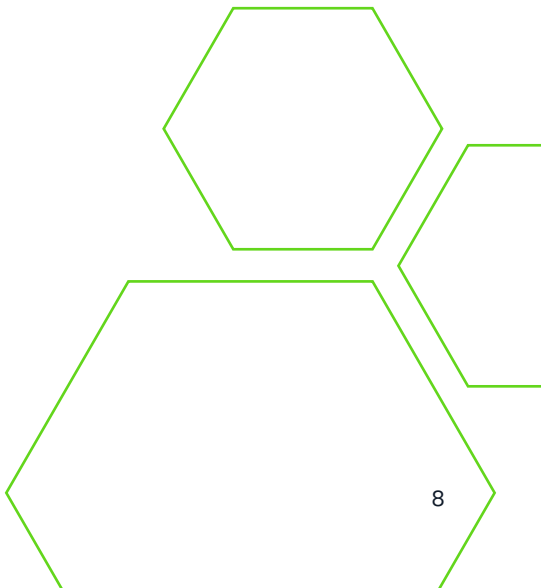
- files.example.com - primary HTTP/HTTPS services (web app and API)
- files-webdav.example.com - used for Cloud WebDAV service

Add DNS type A records for these domain names for the public IP Address. For example:

Type	Name	Value
A	files	35.188.82.62
A	files-webdav	35.188.82.62

Verify that Public DNS records are set up correctly by pinging each FQDN from the appliance.

- ping files.example.com
- ping files-webdav.example.com



Configure Static IP Address

Out of the box, the server comes preconfigured for DHCP. For most environments, you will need a static IP address. You can do this with tools available on the appliance. If you have DHCP with dynamic DNS enabled, connect to “appliance. yourcompany.tld”. If not, and you do not know the IP address of the appliance, connect over a console session from your hypervisor.

To identify the IP addresses, enter the following:

- ip a show dev eth0
  Note: If DHCP is not enabled on your network, you can run the smenetconf script and assign a static address from the command line. This must be run as the smeconfiguser.
- smenetconf

Required Ports to Open

The appliance requires the following ingress ports:

Type	Protocol	Port	Source	Description
SSH	TCP	22	My IP	SSH for initial configuration
HTTP	TCP	808	My IP	Installation website (temporary)
HTTPS	TCP	443	Anywhere	Main website
HTTP	TCP	80	Anywhere	Redirects to the main website

Note: If using FTP/FTPS or SFTP, you must add additional ports.

SSH into Appliance

Log into the appliance through SSH as smeconfiguser. The default password is rari2quum.

- ssh smeconfiguser@<ipaddress>
  Check that you can become root. The default password is boze4wuz.
- su-
  This will be required to complete the configuration.

Core Configuration

Deploy to the hypervisor. Download VMware and Hyper-V images from https://account.nasuni.com.

IP Configuration

The IP configuration provides a web interface for configuring network settings and domain names.

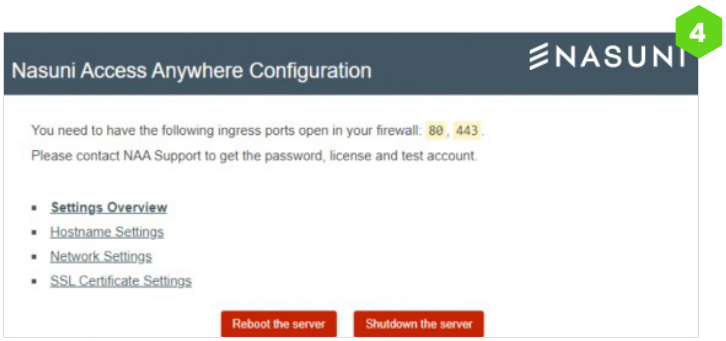
To get started, follow these steps.

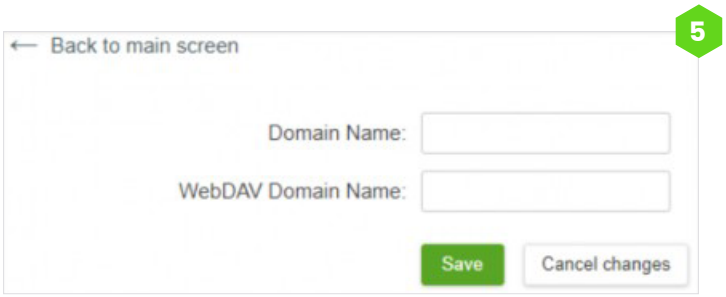
1. Navigate to the Network Configuration via SSH, or a console, using smeconfiguser. If there is DHCP, proceed to UI Configuration.
2. Run the following command: smenetconf
3. Configure the IP information. Provide the DNS access to the Active Directory.
4. Run the following command: sudo reboot to apply.

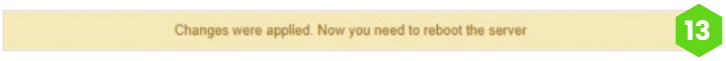
UI Configuration

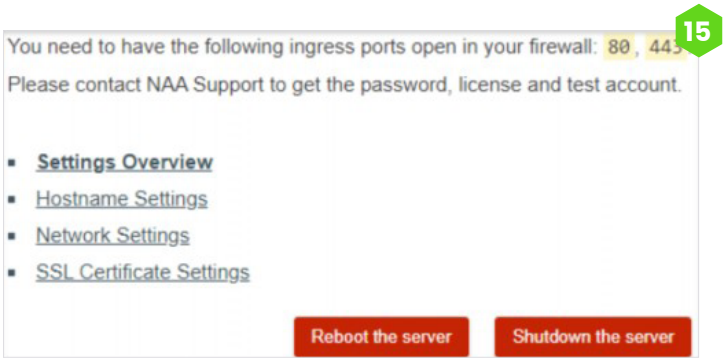
To configure the UI, follow these steps.

1. Navigate to the UI Configuration via SSH, or a console, using smeconfiguser.
2. Execute the following command smeconfigserver.
3. Navigate to http://ipaddress:8080.
4. Click Hostname Settings.
5. Using the Domain Name field, enter your defined FQDN for Nasuni Access Anywhere.
6. Enter the Web DAV Domain Name. The default name should be the same as the domain but with -webdav added. For example:
   - Domain Name: files.domain.com
   - WebDAV Domain Name: files-webdav.domain.com. Important: Avoid using dots in the hostname as it can imply a different domain and cause certificate issues.
7. Click Save.
8. Click Back to Main Screen.
9. Click Network Settings. Confirm that the information provided matches the CLI setup. If the settings match, click Back to Main Screen. If there are deviations in the information, edit the information, and click Save.
10. Click SSL Certificate Settings.
11. If the customer has a customer certificate, enter this information in the SSL Certificate fields, and click Save.
12. Click Back to Main Screen.
13. Click Settings Overview, followed by Apply. If changes were successfully applied, a confirmation message displays.
14. Click Back to Main Screen.
15. Click Reboot the server, followed by OK.









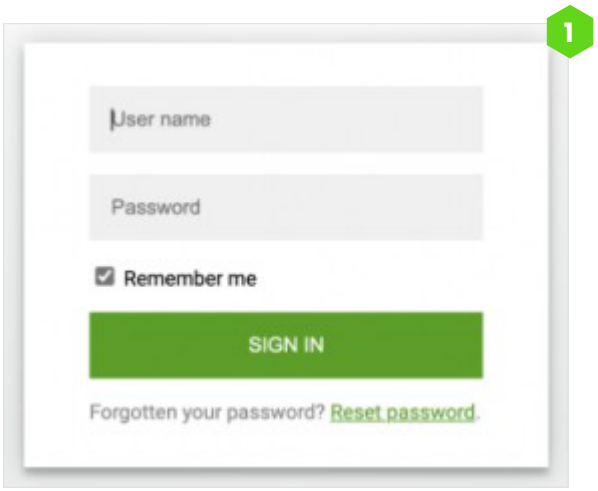
Trusted SSL Certificates

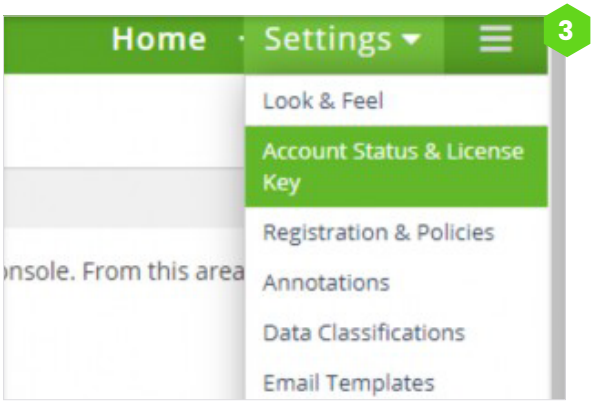
The appliance includes an untrusted SSL certificate. To create a trusted SSL/TLS certificate associated with your domain, see SSL Certificates.

Configure Appliance

To configure the appliance, follow these steps.

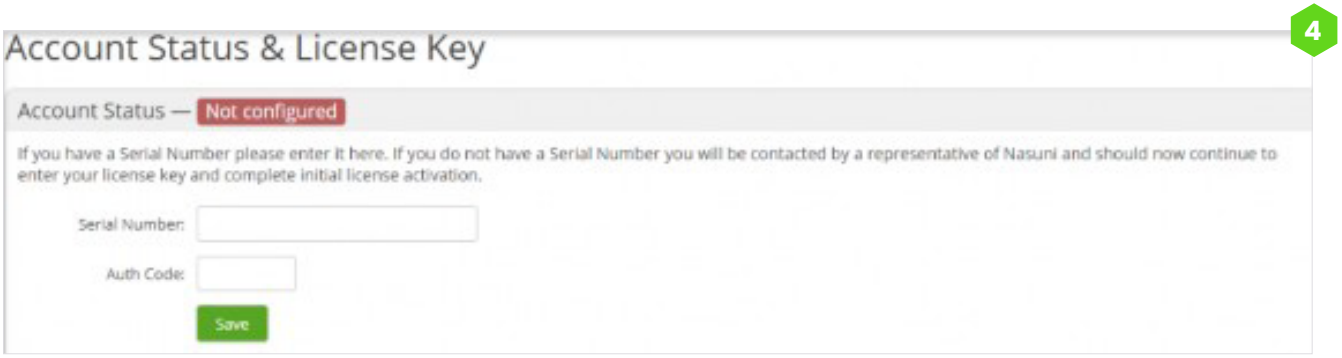
1. Open a browser to the domain name you previously assigned. For example, https://files.example.com. The following login page displays.
   - Note: If you have not set a domain name, use your external IP address: https://3.234.139.146
2. Log into the appliance using appladmin and the password from your trial license.
3. Click Settings > Account Status & License Key.
4. Enter the Serial Number and Auth Code.
5. Click Save to finish.





License Key

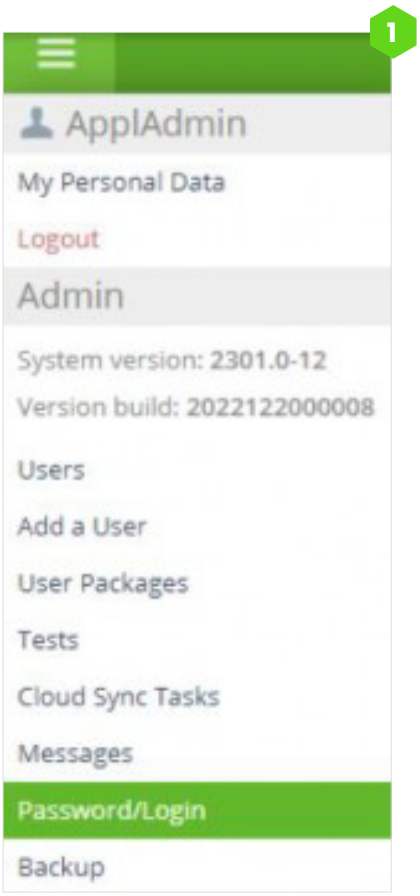
To activate your license key, see Activating your License. If a trial key is needed, please contact your Nasuni Account Manager.



Outbound Email

The appliance uses an SMTP server to send registration and notification emails to users. A daily report and error notices are also emailed to the Notification Email. For more information, see SMTP Configuration.

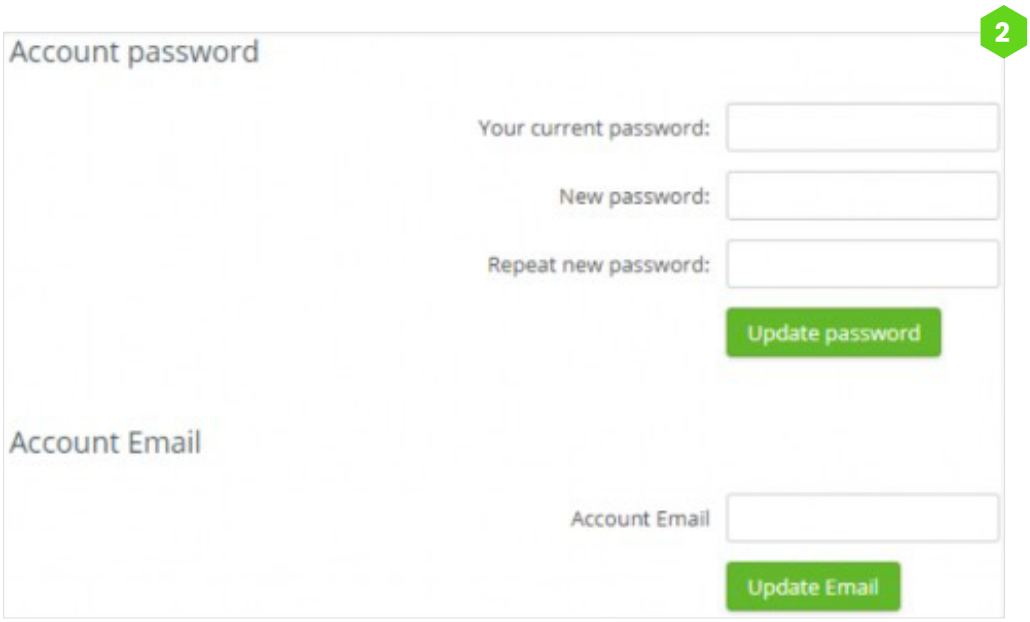
- Note: If you do not initially configure an email server, remember not to use email notifications when adding users.



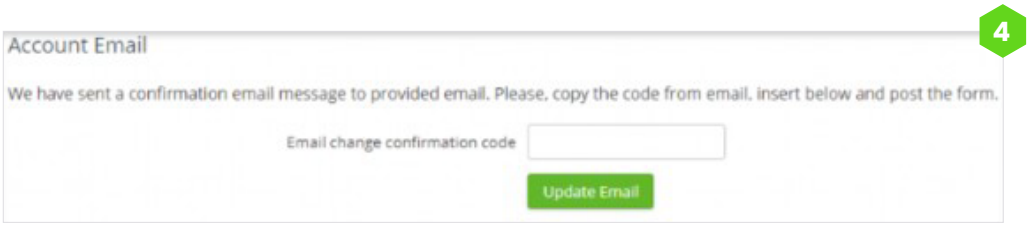
Change Admin Email

The Admin email can be changed after configuring the SMTP server. To change the Appliance Admin email, follow these steps.

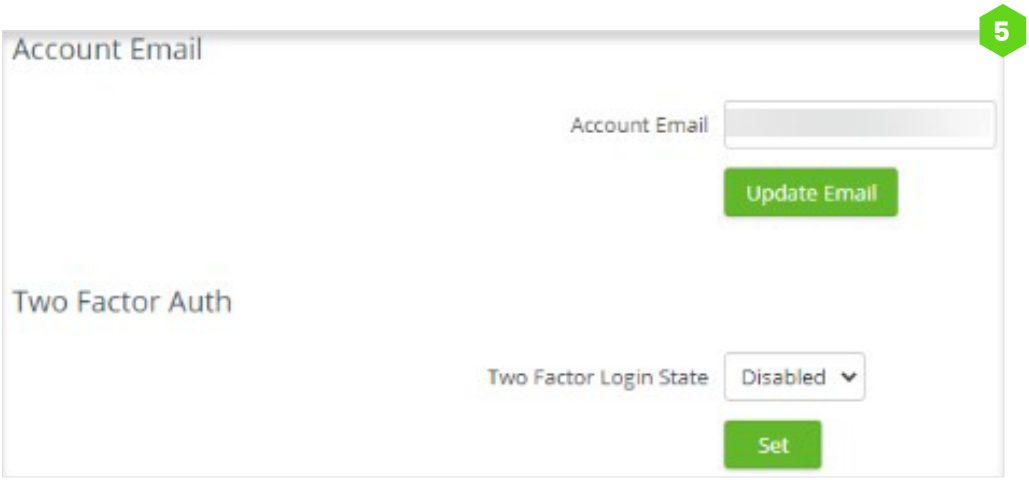
1. Navigate to the hamburger menu and select Password/Login.
2. Update your Account Email.
   - Important: When populating Account Email, this field must be populated by an email or distribution list that will not log in as a user to the system.
3. Click Update Email. An email with a confirmation code is sent to the new email address.
4. Enter the confirmation code and click Update Email.



5. If the email was successfully updated, the field displays the new email address, and the Two Factor Login State box is highlighted. Choose to enable or disable the two-factor login, and click Set.



Note: To avoid unnecessary lockouts, consider the use of TOTP if the email is a team or distribution list.



Change Admin Password

It is recommended that you change the admin password after logging in. To change the admin password, follow these steps.

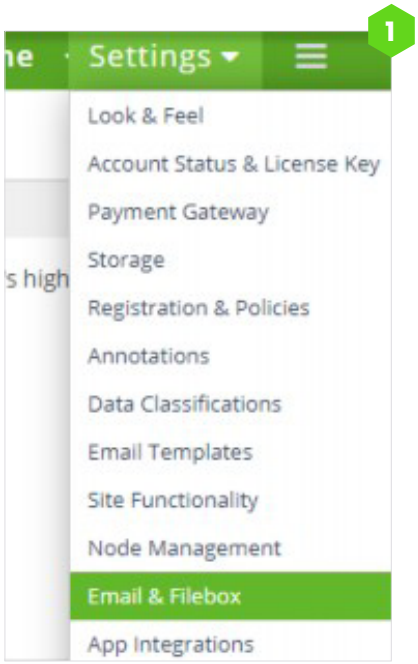
1. Navigate to the hamburger menu and select Password/Login.
2. Enter your Current Password, followed by your New Password, twice.
3. Click Update password. You will be logged out.
4. Log back in using your new password.
   - Note: There is no notification of a password update success.

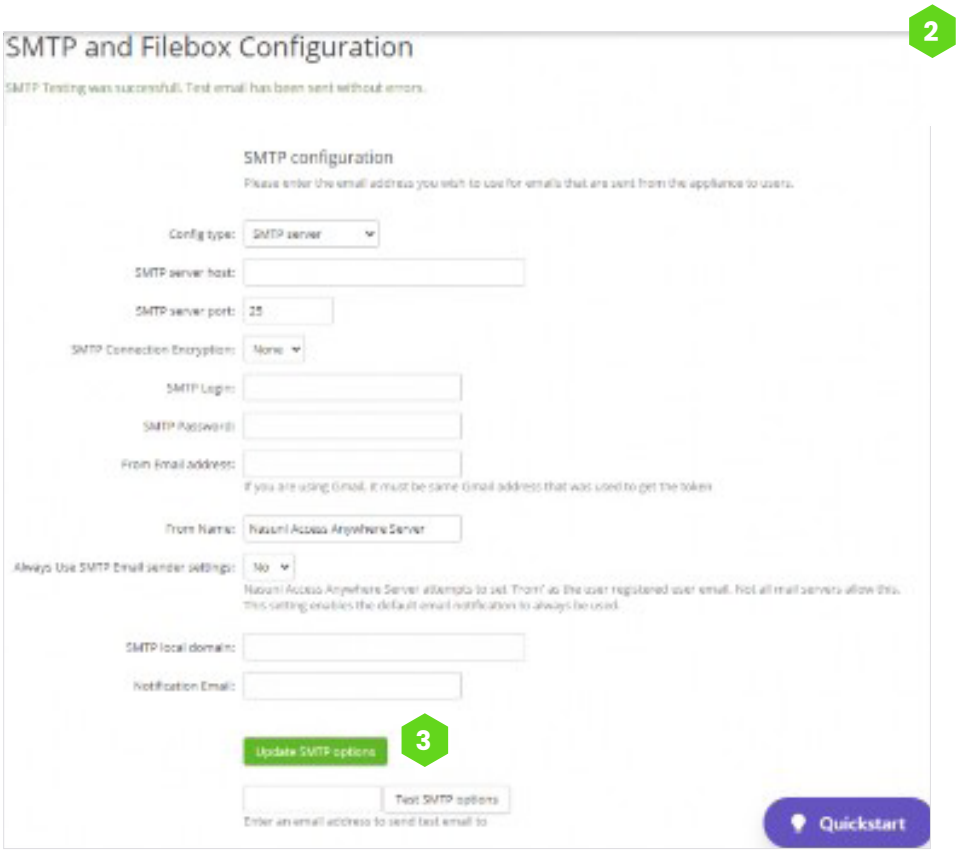
Server Notification Email

Email notifications are not configured by default. However, the Appliance Administrator can configure an email containing server errors and a daily report.

To configure a notification email, follow these steps.

1. Click Settings Email and Filebox.
2. Enter the SMTP information.





3. Click Update SMTP options to finish. If the information was entered correctly, the message “SMTP Testing was successful. Test Email has been sent without errors” displays across the top of the page.

Site Functionality

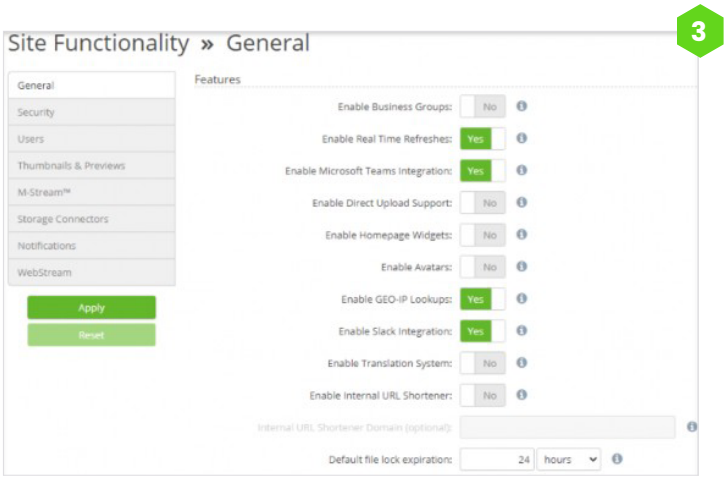
The Site Functionality page allows users to enable or disable various customizable functionality and features. The default configuration provides most organizations with a great starting point for their initial deployment; however, it is recommended that you review this setup and update the settings to your preference.

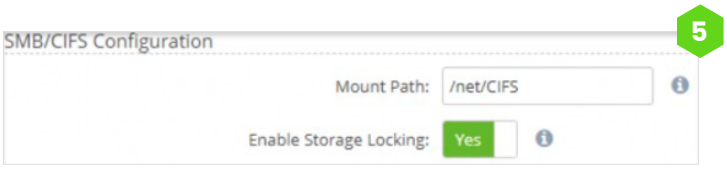
This section describes the recommended initial deployment settings for the Site Functionality.

- Note: If providing SFTP access through the Cloud SFTP gateway, you must regenerate the SFTP RSA keys. For more information, see the SFTP Configuration page.

To get started, follow these.

1. Click Settings Site Functionality.
2. From the list of categories on the left, click General.
3. Confirm Enable Real Time Refreshes is enabled.
4. Click the Users category and set the Delay User Deletion feature to No Delay.
5. Click the Storage Connectors category and select Yes for Enable Storage Locking.
6. Leave the Storage Locking Service URL field blank.
7. Click the Notifications category and disable the PDF Burner Warning feature.
8. Click Apply to finish.





Post Installation

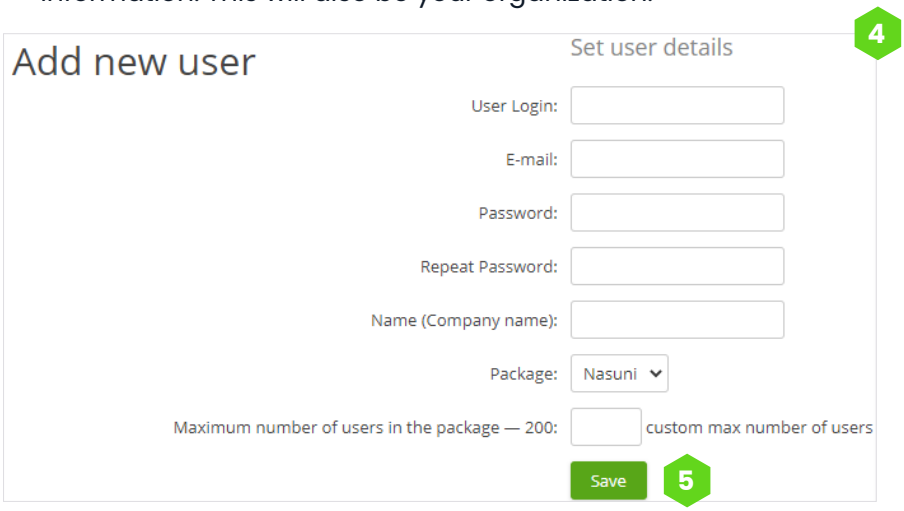
For further customizing and securing the appliance, see Post Installation Tasks.

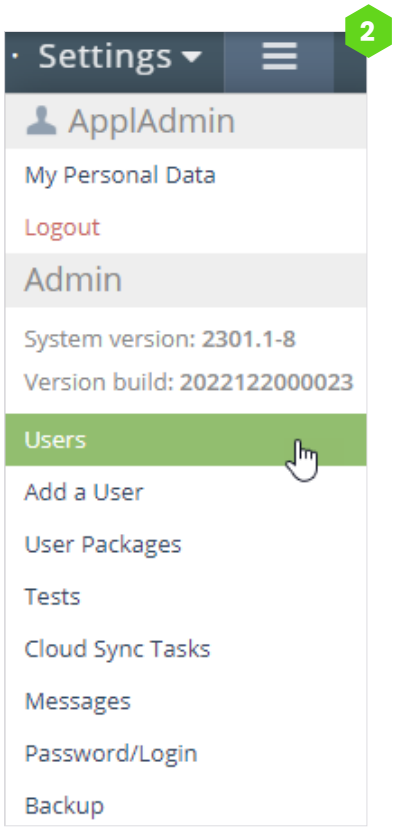
Creating an Organization

Before adding users and storage providers, you must first create an organization. An organization is an administrative unit for a set of users. It includes policies, storage resources, and permissions for those users. A single instance of an appliance can host multiple organizations. Once created, organizations, also called tenants, are self-managed by their users and not accessible or visible from other organizations on the same appliance. An appliance administrator creates an organizations by creating a user account for the Organization Administrator (Org. Admin.), who must log in to complete the setup of organization policies and users.

To create an Org. Admin. user, follow these steps:

1. Log in as an Appliance Admin.
2. Navigate to the hamburger menu and select Users.
3. Click Add a User.
4. Use the following fields to enter the organization admin user information. This will also be your organization.





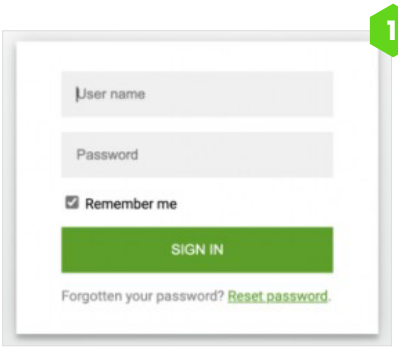
- User Login: The Organization's short name and super user's username. We recommend the domain name of your company. For example, nasuni.com.
- Email: The email address of the organization admin must be unique to the system.
- Password: Enter a unique password.
- Name (Company Name): Full Organization name. Package: Choose the user package template from earlier. Users in the package: Leave blank or specify a number 200 or less.

5. Click Save to finish.

Requirements for Creating Org. Users

Users are created manually or can be imported from a delegated Active Directory, LDAP, or SAML authentication system. All users require a username and an email address.

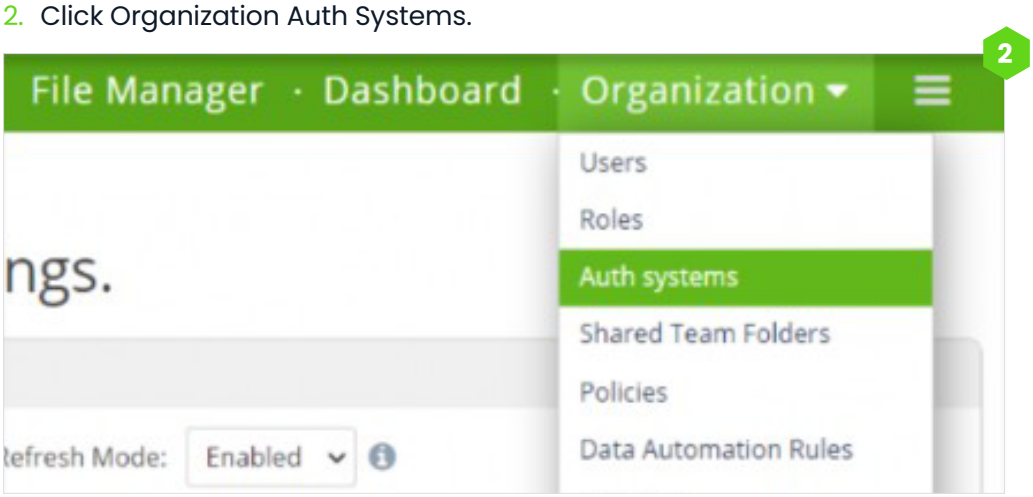
- Note: If using a service account for a user without an email address, consider using the User Principal Name (UPN), i.e., the name of a system user in an email address format.



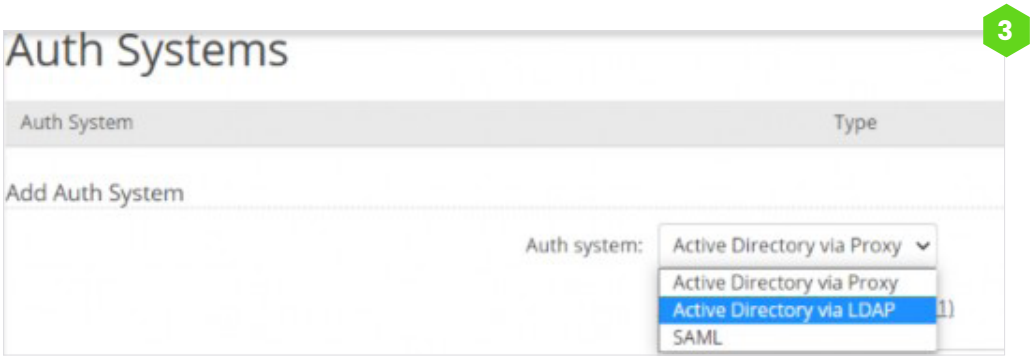
Org Setup

The following section describes how to set up and configure the organization. To get started, follow these steps.

1. Log in using the Org Admin account.
2. Click Organization Auth Systems.



3. Click the Auth System dropdown and select Active Directory via LDAP.



4. The following fields require information entered or toggled on.
    - Auth System Name – Enter a description for the connector.
    - LDAP Server host or IP - Enter a DC the appliance can query. Subsequent servers should be predicated with ldap://
    - LDAP Server port – Set LDAP to 389 and LDAPS to 636.
    - Connection Encryption – Choose a connection.
    - Base DN – The base of the AD Distinguished Name selects which OU
    - (user accounts) can have Authentication queries.
    - Administrator User DN – The account user that will be able to query the AD.
    - Enable Auto create user on login.
    - Enable Refresh role/group membership on login.
    - Enable Auto create new roles/groups on login.
    - Enable Assign parent roles/groups.
    - Nasuni Access Anywhere Server Administrator role maps to the following group use Get-ADGroup <groupname> to return the DN.
    - User Object Class – User
    - Login Field – SAMAccountName
    - Unique User Attribute – userPrincipalName
    - User Name – cn
    - Group ID Field – cn
    - Group Object Class – group
    - Click Add Auth System.

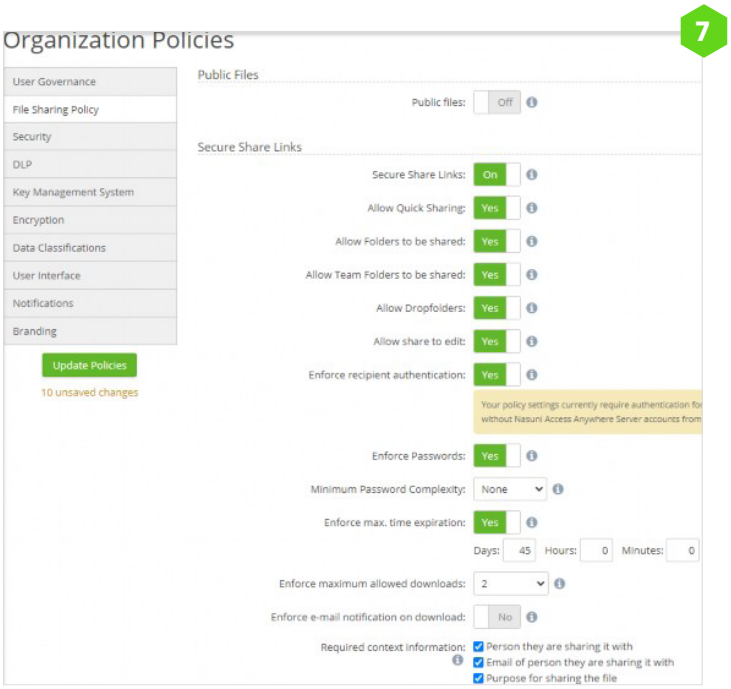
Organization Policies

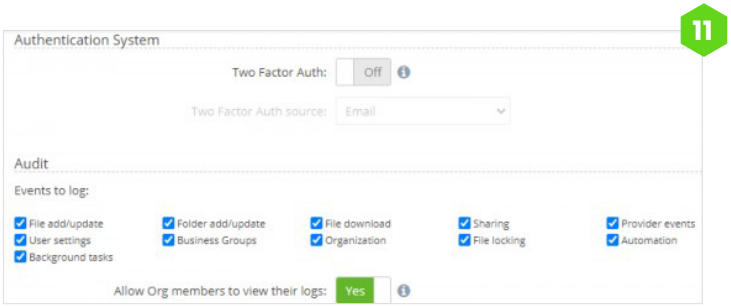
The settings described in the following steps provide a starting point configuration. It is recommended that you review each category and option and decide which options best suit your organization and workflow.

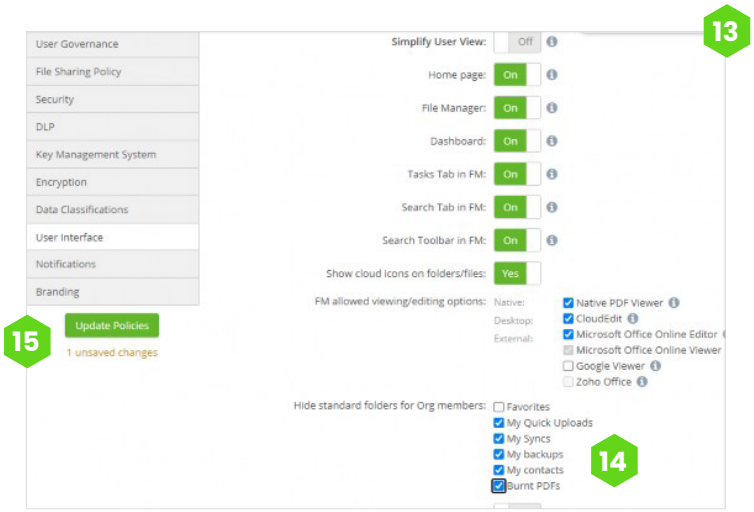
To configure the organization's policies, follow these steps.

1. Click Organization Policies.
2. Click the User Governance category located on the left side.
3. Configure the following Main User Policies.
    - Messaging – Access Anywhere has an integrated messaging and IM service. This is off by default.
    - Download from Web – This allows downloading from the web UI. This is on by default.
    - Files/folders commenting – Enables the comment metadata (resides only on AA). This is on by default.
    - Folder download – Allows users to download compressed versions of folders. This is on by default.
4. By default, users are not permitted to add their own providers or shares. To enable, toggle on Org members can add private clouds.
5. Click the File Sharing Policy category located on the left side.
6. The Public Files option is On by default and enables an RSS feed for anonymous public file access. Set this option to Off.
7. Use the Secure Share Links set of configurations to define the security requirements for downloading files and folders.

8. Click the Security category located on the left side.
9. Review and enable your preferences in the Main Policies set of configurations.
10. (Optional) If your organization does not have Two Factor Authorization. (TFA) from an external provider, you can enable TFA in the Authentication System set of configurations. Toggle Two Factor Auth to On and choose a TFA method. Options include email, a predefined passphrase, or a time-based one-time password (TOTP).
11. Under the Audit set of configurations, check the boxes for the events you want logged.
12. Click the User Interface category located on the left side.
13. Use the On/Off toggle to customize the user interface.
14. (Optional) It is recommended that you check the following options under the Hide standard folders for Org Members.
    - My Quick Uploads
    - My Syncs
    - My backups
    - My contacts
    - Burnt PDFs
15. Click Update Policies to save all your policy preferences.







Storage Providers

For users to access files through Nasuni Access Anywhere, SMB shares must be added as “storage providers”. Storage providers are added to organizations (tenants) and can be managed by designated organization administrators. Access Anywhere caches and indexes metadata, information about where and what files are available, and who has access. The files themselves are not cached or copied.

File shares are added using either the “Nasuni” or “SMB Single User” provider.

- The “SMB Single User” provider connects to an SMB share as a single system user. Non-admin users cannot access these shares until they are granted permission within Access Anywhere through “Shared Folders”.
- The “Nasuni” provider connects to an SMB share as a system user for indexing but will connect as each specific user for data access. Additionally, the provider synchronizes permissions with the Nasuni Edge Application. Access Anywhere users will have access immediately based on their existing SMB permissions. You will also need to register an AD or SAML directory service for this provider.

The Default Storage Provider

One storage provider is designated as the “default”. This must be added through the “SMB Single User” provider. Using a “Nasuni” or “Multi-User SMB” provider for default storage is not supported.

Default storage provides a location for storing files and folders created by each user in their root directory. This is also the default location for system files (thumbnails, previews, comment attachments, and contacts).

The default provider can be changed at any time. This changes where future files are created. We recommend creating a new Nasuni volume just for default storage and adding it as an “SMB Single User” provider.

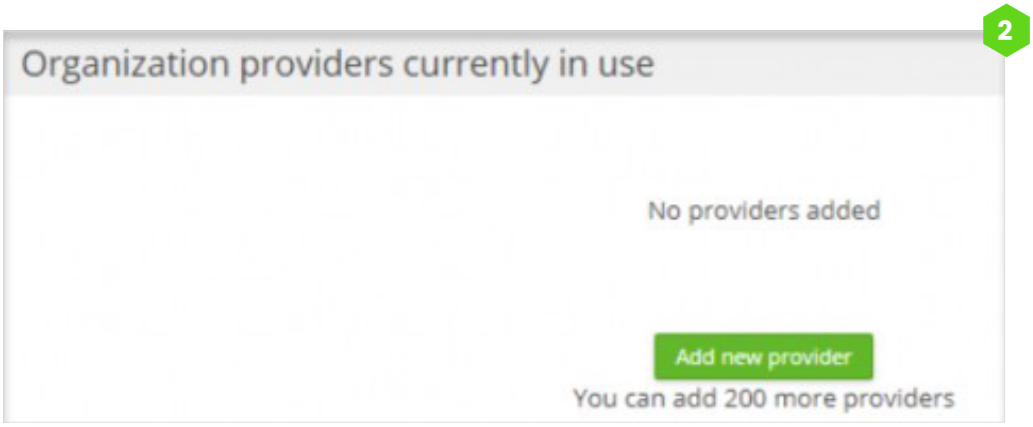
Setting Up Nasuni as a Default Storage Provider

This section describes how to set up Nasuni as the default storage provider for Access Anywhere.

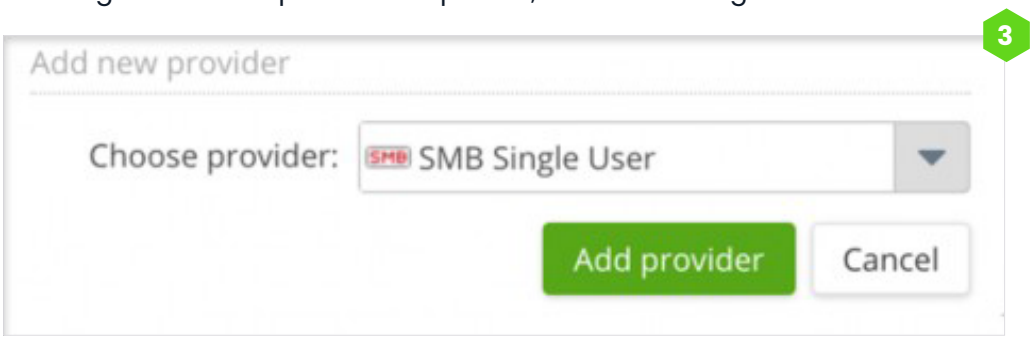
- Note: Before beginning, create a new volume and obtain access credentials.

It does not need to be part of the AD domain. To get started, follow these steps.

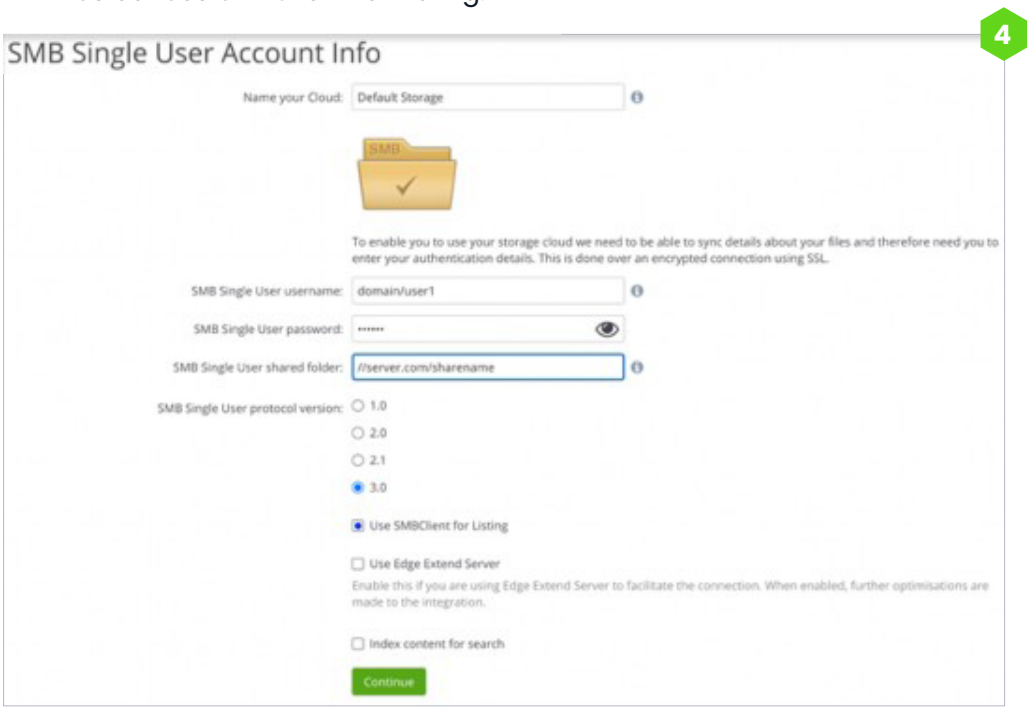
1. Navigate to the dashboard.
2. Under the Organization providers currently in use header, click Add new provider.



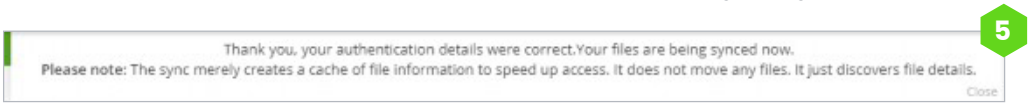
3. Using the Choose provider dropdown, select SMB Single User.



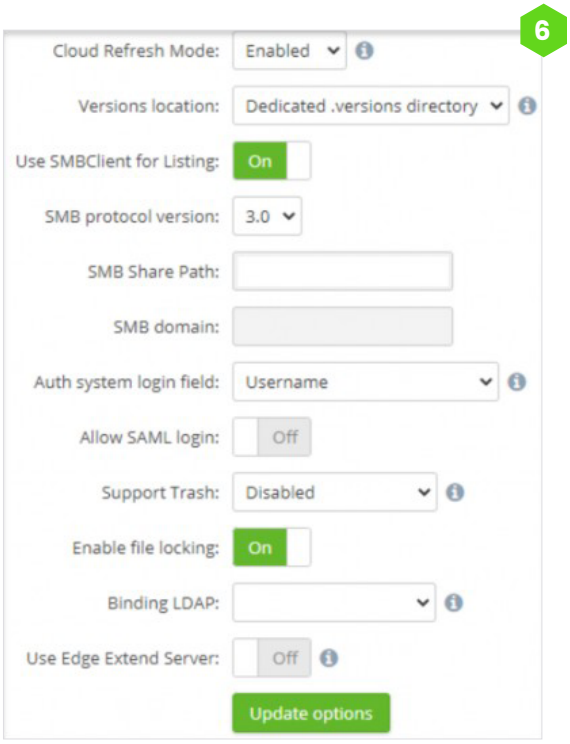
4. Use the following fields to configure the provider information.
   - Name your Cloud: Enter a name for the connector such as "Default Storage"
   - Nasuni username: This is a service account configured as a filer admin on the target appliance. Note: Use the format domain\user. A format like user@domain or domain.suffix\user will be rejected.
   - Nasuni shared folder: This folder should contain the UNC path to the connected share level.
   - Nasuni protocol version: Select 3.0.
   - Select Use SMBClient for Listing.



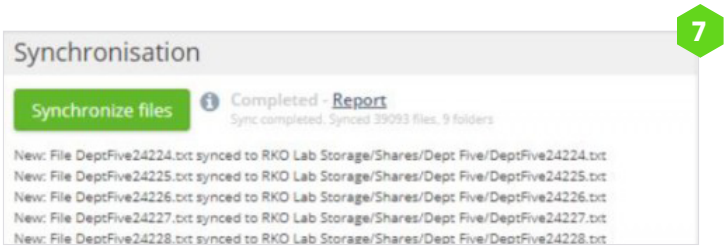
5. Click Continue. If the connection is successful, the following message displays, and you are directed to the Provider Settings page.



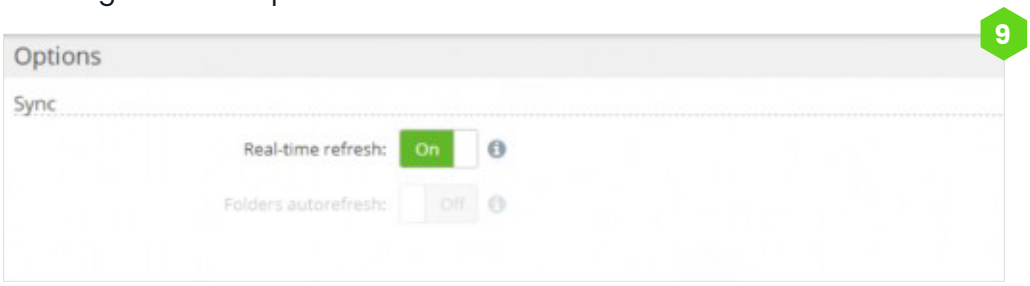
6. On the Provider Setting page, enable the following settings.
   - Versions location: Select Dedicated. versions directory.
   - Support Trash: Select Disabled.
   - Enable file locking: Toggle On.



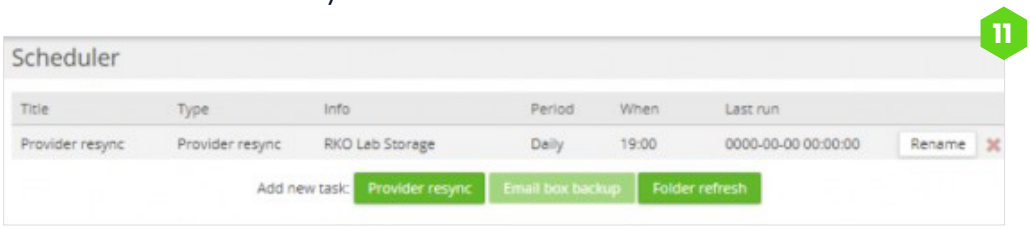
7. Navigate to Synchronization to confirm the connection is functioning and files are syncing.



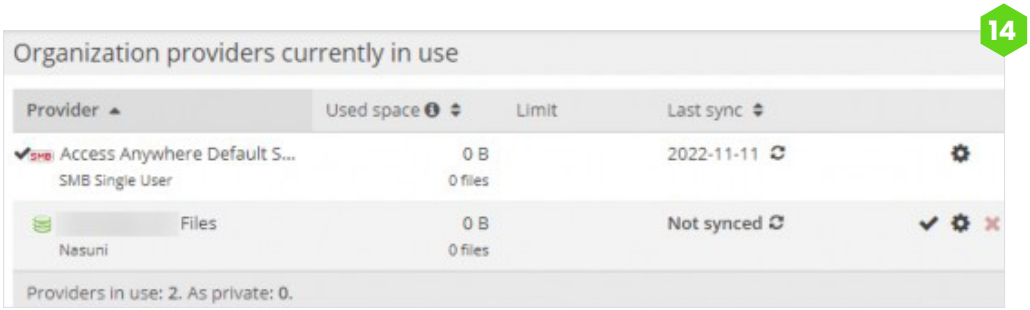
8. Click Dashboard.
9. Navigate to the Options header and enable Real-time refresh.



10. Navigate to the Scheduler header and click Provider resync.
11. Click Add Provider resync task.



12. Use the provided fields to create a daily resync task.
13. Scroll down to the Extended Options header and click Update Options.
14. Navigate to the Organization providers currently in use header and confirm that Nasuni storage has been linked. If the Last sync column displays Not synced, click the refresh loop to trigger the sync request.

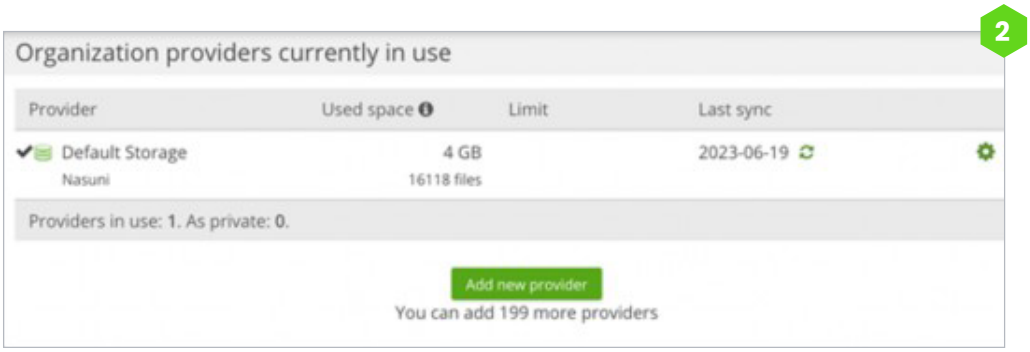


Setting Up Nasuni as a Storage Provider

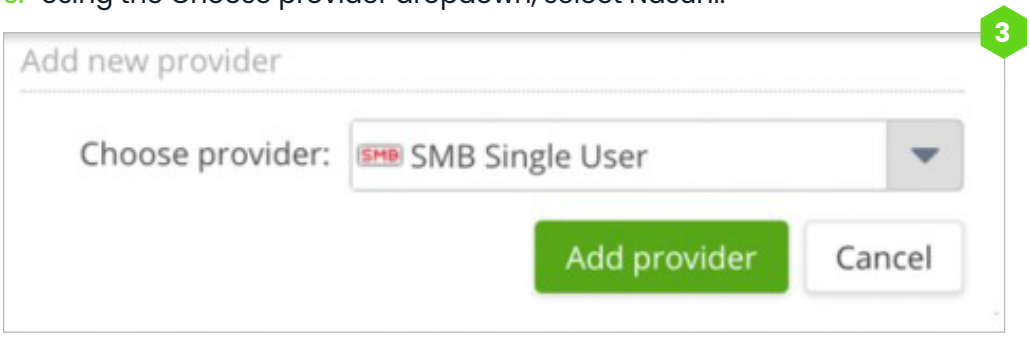
This section describes how to set up Nasuni as storage provider for Access Anywhere.

- Note: Before beginning, create a new volume and obtain access credentials. It does not need to be part of the AD domain. To get started, follow these steps.

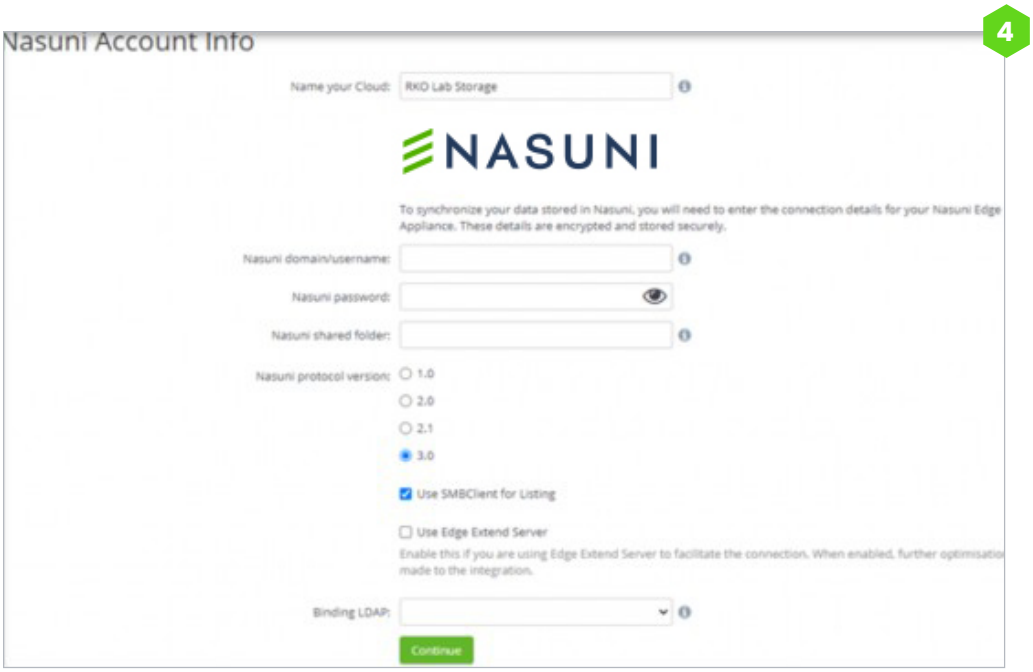
1. Navigate to the dashboard.
2. Under the Organization providers currently in use header, click Add new provider.



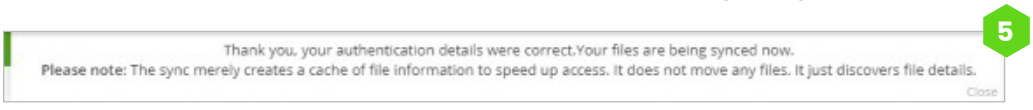
3. Using the Choose provider dropdown, select Nasuni.



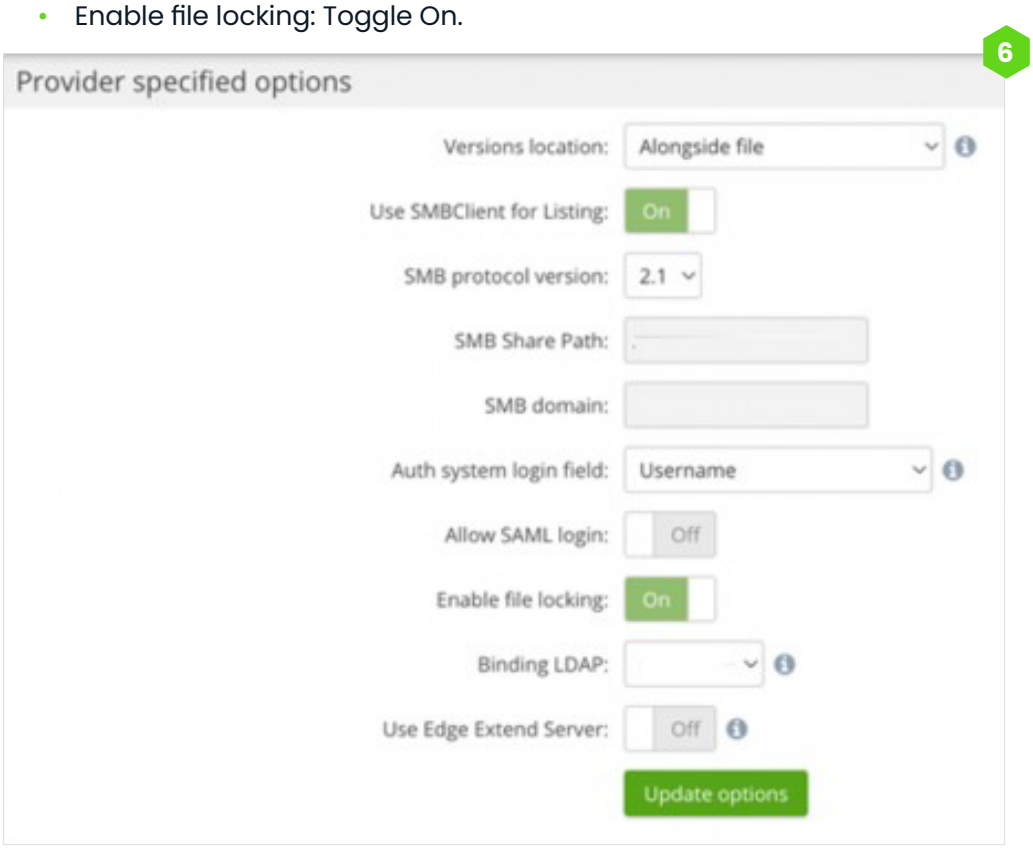
4. Use the following fields to configure the provider information.
   - Name your Cloud: Enter a name for the connector such as the name of the volume.
   - Nasuni username: This is a service account configured as a filer admin on the target appliance.
   - Note: Use the format domain\user. A format like user@domain or domain.suffix\user will be rejected.
   - Nasuni shared folder: This folder should contain the UNC path to the connected share level.
   - Nasuni protocol version: Select 3.0.
   - Select Use SMBClient for Listing.



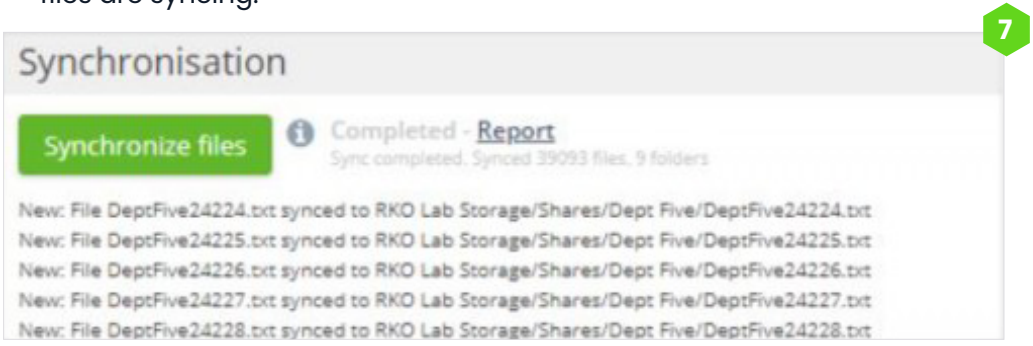
5. Click Continue. If the connection is successful, the following message displays, and you are directed to the Provider Settings page.



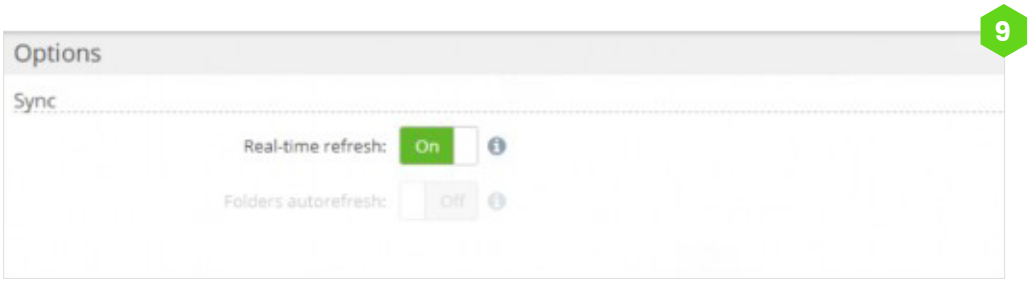
6. On the Provider Setting page, check the following settings.
   - Cloud Refresh Mode: Enabled (if this option is not visible it is enabled on your version)
   - Versions location: Select Dedicated .versions directory. (may not be visible on your version).
   - Enable file locking: Toggle On.



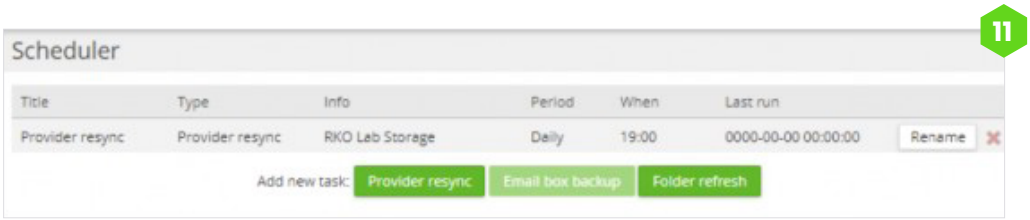
7. Navigate to Synchronization to confirm the connection is functioning and files are syncing.



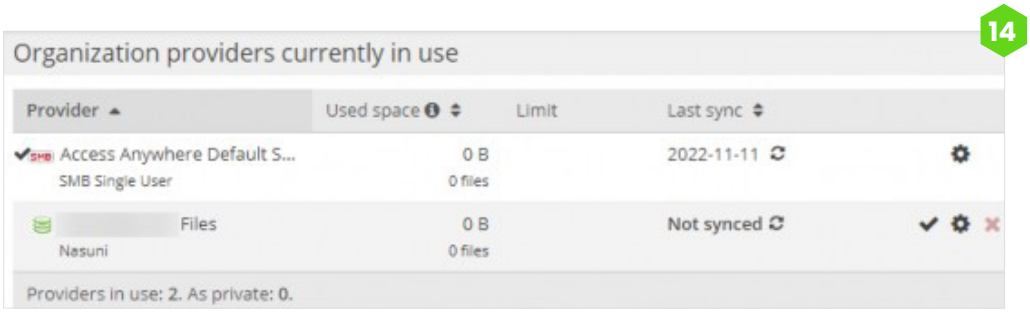
8. Click Dashboard.
9. Navigate to the Options header and enable Real-time refresh.



10. Navigate to the Scheduler header and click Provider resync.
11. Click Add Provider resync task.



12. Use the provided fields to create a daily resync task.
13. Scroll down to the Extended Options header and click Update Options.
14. Navigate to the Organization providers currently in use header and confirm that Nasuni storage has been linked. If the Last sync column displays Not synced, click the refresh loop to trigger the sync request.



NAA Self-Guided User Interface Training

This documentation-style course provides an overview of the functions and uses of Nasuni Access Anywhere (NAA). Content is provided for the NAA web app as well as Cloud Drive for Windows and Mac. Searchable how-to content is presented in organized modules containing short silent videos, screenshots, and quick steps for common workflow tasks. Each module ends with a suggested hands-on learning activity designed to help users retain what they've learned and how to apply it to their daily workflows.

To learn more about the user interface, check out the NAA End User Training

To submit feedback on the training, email Nasuni-customer-academy@nasuni.com

Let’s talk

Want to find out more about how Nasuni can provide your business with a fluid data infrastructure designed for the hybrid cloud world?

Nasuni’s hybrid cloud platform unifies file and object data storage to deliver effortless scale and control at the network edge.

Learn more

Nasuni is a scalable data platform for enterprises facing an explosion of unstructured data in an AI world, eliminating the choice between expensive tinkering or an overwhelming transformation of your entire data infrastructure.

The Nasuni File Data Platform delivers effortless scale in hybrid cloud environments, enables control at the network edge, and meets the modern enterprise expectation for protected, insight- and AI-ready data. It simplifies file data management while increasing access and performance.

Consolidate data, cut costs, and empower users – all while transforming your data from obstacle into opportunity.

NASUNI