Quick Start Guide

CONTENTS

System Requirements

Microsoft Active Directory or Azure Active Directory for authentication. Local Foldr accounts are also supported.

SMB shares - Windows Server 2003 > Server 2022 or NAS, Linux or macOS hosted SMB shares.

Cloud storage providers – Google G Suite (Google Drive, Team Drives), Office 365 (OneDrive, SharePoint, Teams), Azure SMB and blob storage, Amazon AWS S3, Dropbox, BackBlaze B2 & Box.

VMware ESXi, Workstation, Fusion, Microsoft Hyper-V, Citrix XenServer, Nutanix AHV, Oracle VirtualBox, and Parallels Desktop are supported.

Main Virtual appliance requirements: 2 vCPU, 4GB RAM, up to 100GB free hard disk space. (Appliance will consume less than 10GB when deployed and dynamically grow as required)

Optional Search appliance requirements: 2 vCPU, 4GB RAM, up to 100GB free hard disk space. (Appliance will consume less than 10GB when deployed and dynamically grow as required)

A server, PC or macOS computer to run the chosen virtualisation platform.

1. Importing the Virtual Appliance

VMware ESXi

Download the VMware appliance '**Foldr-latest.ova'** and save it locally.

From the vSphere client, click Right click on the host/cluster and select Deploy OVF Template and browse to the Foldr-latest.ova file. Proceed through the deployment wizard; the number of steps shown is dependent on whether you are connected to a vCenter management server or directly to an ESXi host. Select a suitable Host and Datastore for the Foldr VM, and the Network that Foldr will connect to. The Foldr virtual machine disk may be thin provisioned if preferred.

Once the OVA has been imported, the VM disk size should be increased. Right click on the VM and select Edit Settings. Increase the disk from 10GB to 100GB.

Power the appliance on and after an automatic setup routine is run, the system will reboot and finally boot to a login screen menu.

The system disk now needs to be expanded – select Option 1 and enter the password 'password' with no quotes. Once at the console prompt, run the following command to expand the disk so the full 100GB is usable to the system:

expand-disk

Confirm the command with y and hit return. The server will reboot automatically, and the server will be ready for configuration after restarting.

The v4 appliance ships with third party VMware Tools installed, you will be unable to update these using the VMware client.

A dedicated KB article for ESXi deployment is available here.

Microsoft Hyper-V

Download the Hyper-V appliance '**Foldr-latest-HV.zip**' and save it locally on your Windows server. Extract the contents of the zip and move the VHDX file to a suitable location. Using the Hyper-V Management console, create a new/blank Virtual Machine by right clicking on the host or using the Actions panel on the right of the screen.

Proceed through the wizard, selecting VM type as Generation 2, giving it a suitable name and location for the Virtual Machine files; assign 4096MB of RAM and a valid network connection. Two vCPU cores are recommended as a minimum specification.

When presented with the 'Connect Virtual Hard Disk' screen, select 'Use an existing virtual hard disk' and browse to the VHDX file from step 2. Click Finish and allow the VM to be provisioned. Please note that Legacy Network Adapters are not supported.

Power the VM and after an automatic setup routine (during the first system boot), the VM will reboot and finally boot to a login screen menu. This may take several minutes.

The system disk now needs to be expanded – select Option 1 and enter the password 'password' with no quotes. Once at the console prompt, run the following command to expand the disk so the full 100GB is usable to the system:

expand-disk

Confirm the command with y and hit return. The server will reboot automatically, and the server will be ready for configuration after restarting.

A dedicated KB article for Hyper-V deployment is available here.

Citrix XenServer

Download Foldr-latest-XS.zip and save it locally on a workstation running the XenCenter client. Extract the XVA file from the zip and select File >> Import from within XenCenter. Proceed through the deployment wizard selecting a host and storage repository.

Once the OVA has been imported, the disk size should be increased. In the VM settings in XenCenter, increase the disk from 10GB to 100GB.

Power the appliance on and after an automatic setup routine is run, the system will reboot and finally boot to a login screen menu.

The system disk now needs to be expanded – select Option 1 and enter the password 'password' with no quotes. Once at the console prompt, run the following command to expand the disk so the full 100GB is usable to the system:

expand-disk

Confirm the command with y and hit return. The server will reboot automatically, and the server will be ready for configuration after restarting.

XenTools – By default XenTools are not installed. If you wish to install these drivers for optimum performance, you must firstly power down the VM, attach a virtual optical drive in XenCenter and select the built-in 'xs-tools' ISO. Once the VM has booted you can install XenTools by running '**`install-xen-guest-utils`**' command when logged into the VM console.

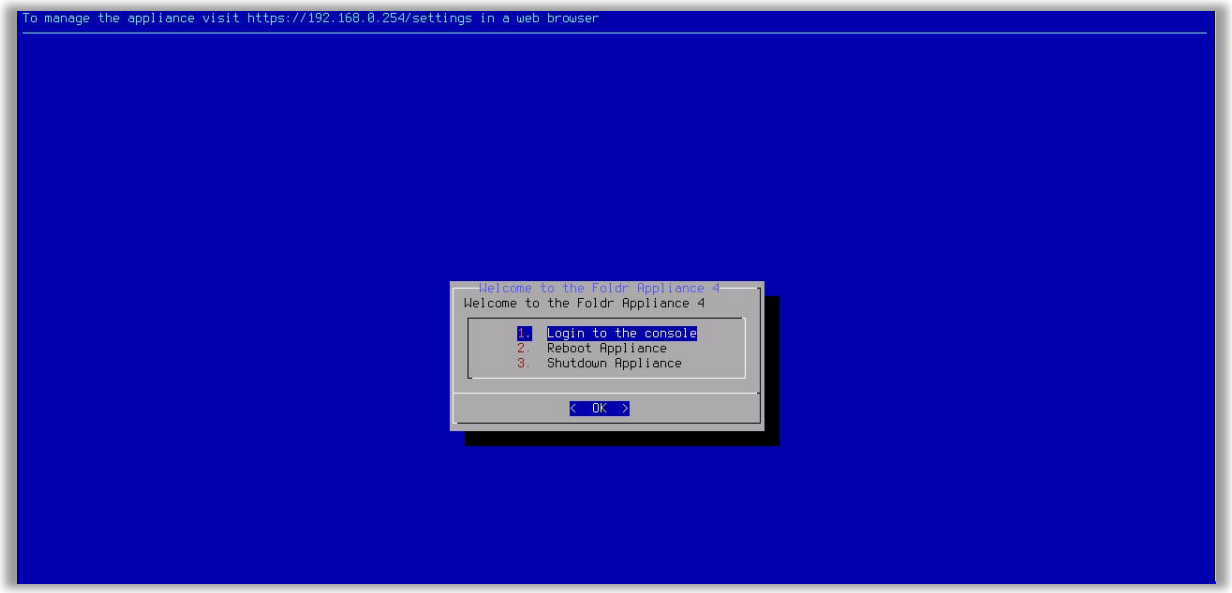
Microsoft Azure

A dedicated KB article is available for deploying the server in Azure.

2. Foldr Settings (https://address-of-foldr:30537/settings)

Once the system has been powered on, it will run through a one-time internal setup routine and reboot. When it is ready to be configured and has restarted, you will be presented with the main system login screen.

NOTE - The system's IP address will be shown at the top of the console screen.



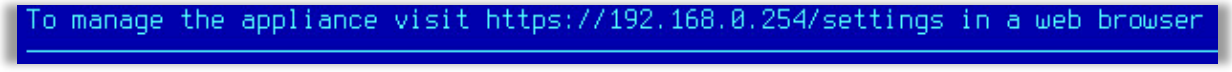
The web based administrative portal (Foldr Settings) where the system is configured is available at:

https://address-of-foldr:30537/settings. Only administrative users can sign into the Foldr Settings portal.

The Foldr server runs an mDNS service, so providing your device is within the same subnet as the Foldr server, the administrative web interface should be reachable at **https://foldr.local:30537/settings**

If the system is not reachable using https://foldr.local:30537/settings, this may be due to the client being in a different subnet/VLAN or working remotely over WAN/VPN.

If Foldr server is not accessible using *foldr.local*, you can browse directly to Foldr Settings using its IP address as shown at the top of the console screen.



NOTE - If '**no IP address**' is shown in the console, you should log into the console using the credentials below and use the '**netconfig**' command menu to configure the network.

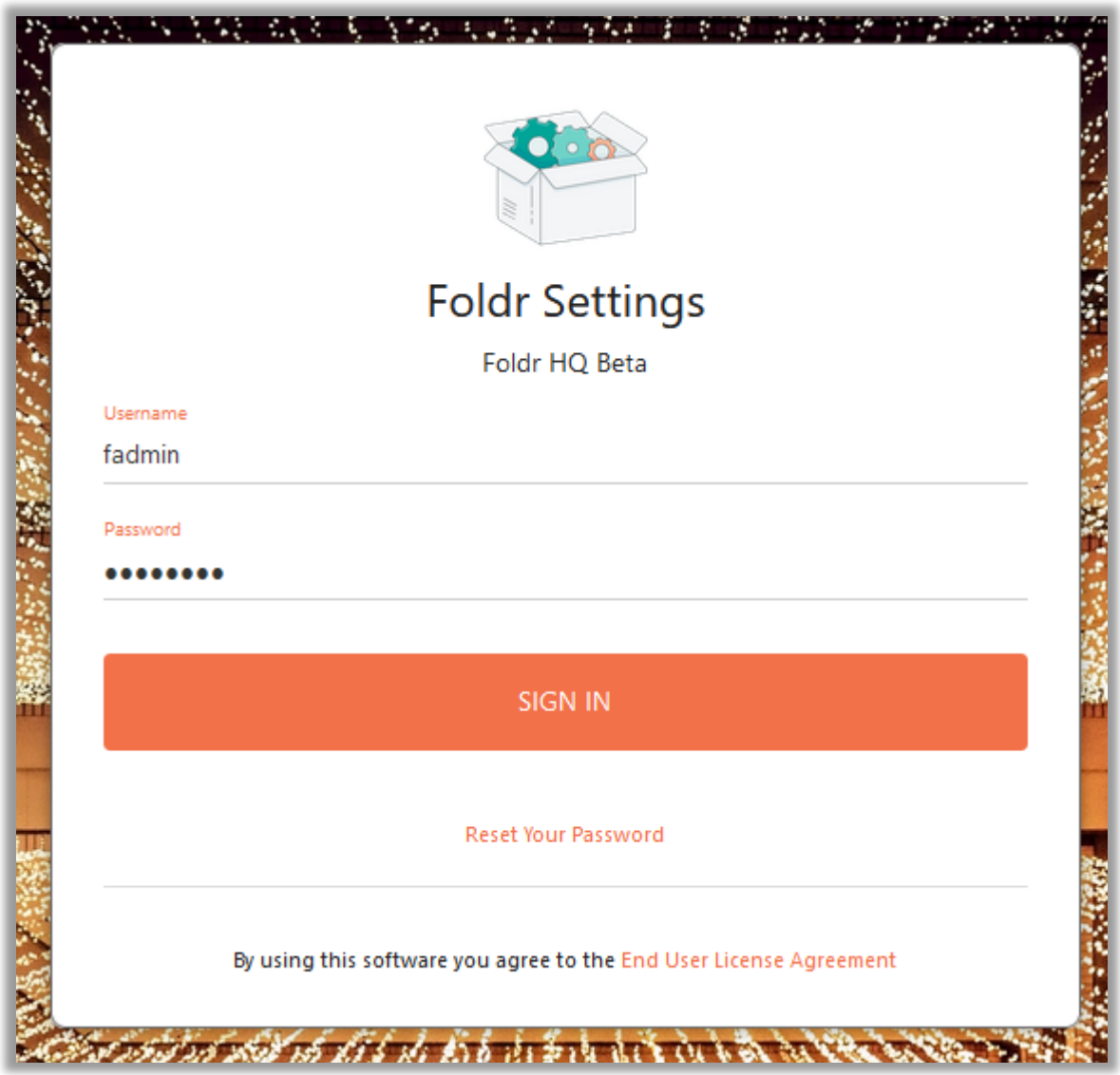
Default admin credentials

USERNAME: fadmin

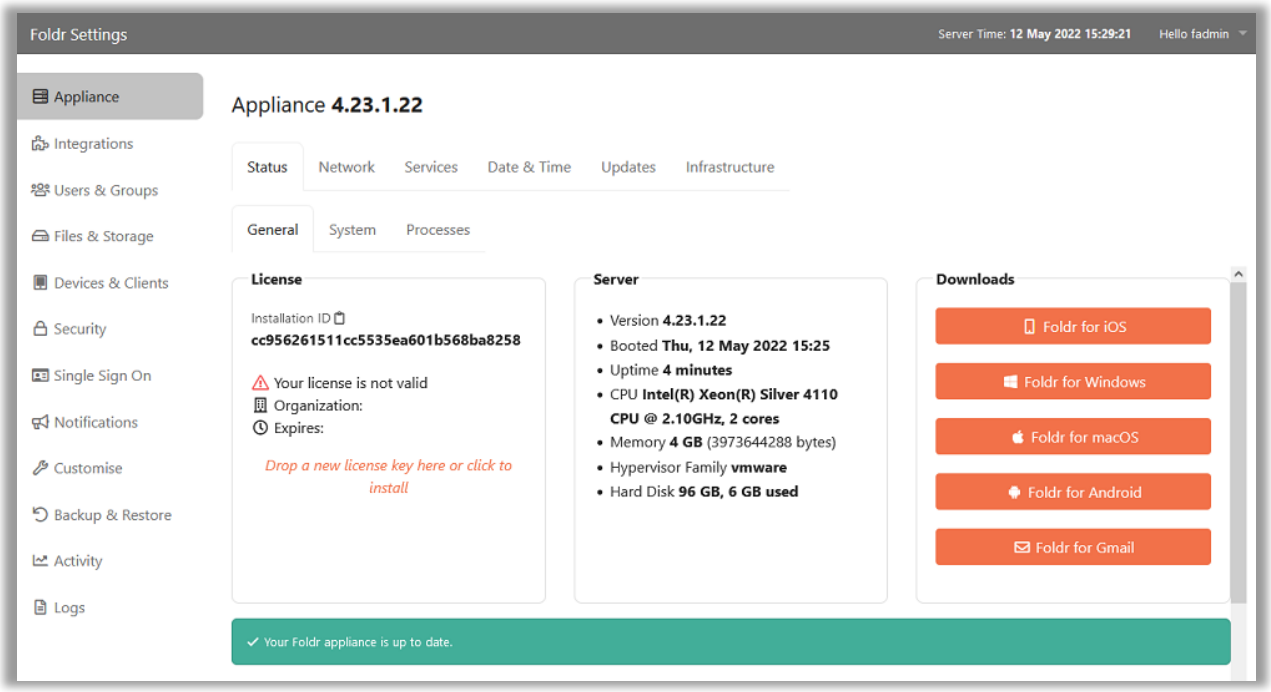
PASSWORD: password

The Foldr server has a single local admin account, however it is possible to delegate other users (on-premise Active Directory or local Foldr users) to sign in as an administrative user. This can be configured within Foldr Settings > Users & Groups> Administrators)

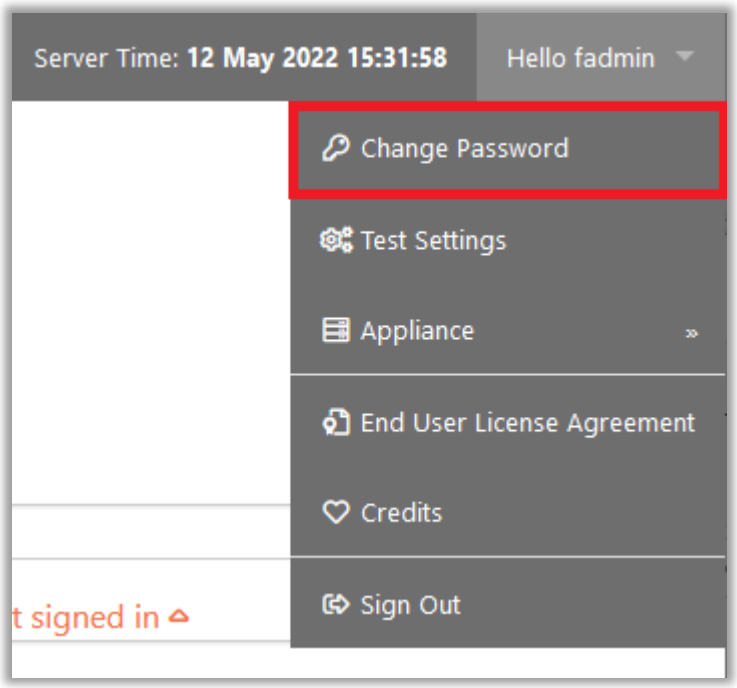
NOTE - If you browse to the local IP address of Foldr and append /settings the browser is redirected automatically to **port 30537**. *Please note that the Foldr Settings configuration portal will not typically be available externally unless you have opened / forwarded TCP 30537, however it is best practice to keep the admin web UI for internal / local network use only.*



Foldr Settings web UI:



It is recommended that you now change the fadmin account password using the **top-right menu > Change Password**

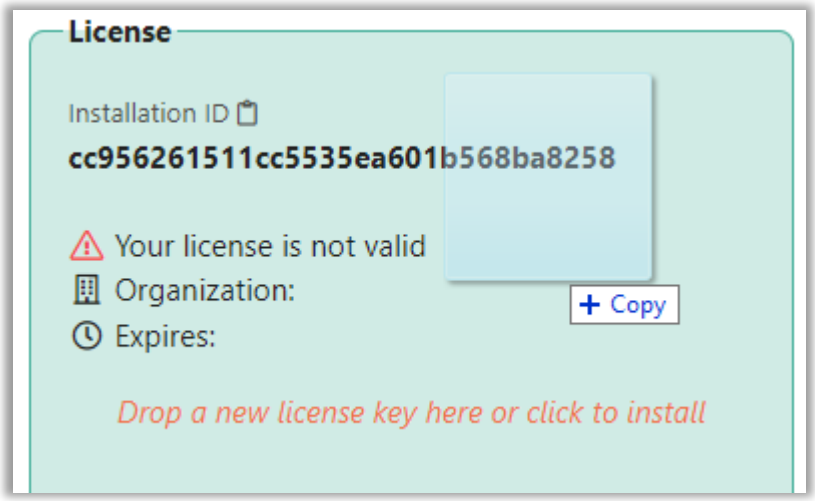


3. Licencing the Server and Initial Setup

Once signed into Foldr Settings interface, the licence key should be applied.

Applying the Licence

Within the **Appliance > Status > General** tab, a licence key can be applied by dragging and dropping the licence file from your local desktop file system into the web browser as shown below. Release the licence file when the box turns green. Alternatively use the text link in the box to open the Explorer / Finder file picker.

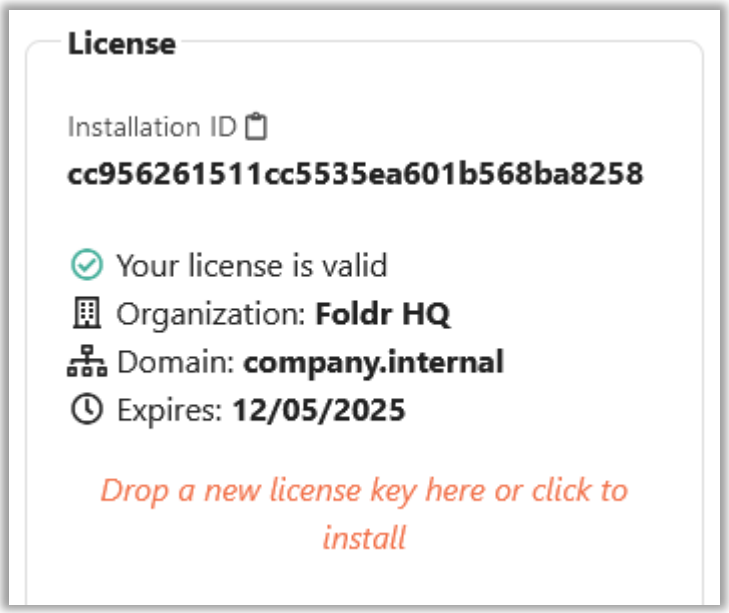


The End User Licence Agreement prompt will be displayed. Click **Yes, Accept** to agree to the terms of the EULA and apply the licence. To view the content of the EULA, click the text link in the prompt.

The unique details for the licence key will be displayed in the summary window as shown below.

If the licence is for an on-premise Active Directory or Azure AD deployment, the relevant option will become visible under Integrations > Authentication.

Note the 'Domain' should match the Active Directory FQDN. In the example below, the Active Directory domain name is **company.internal**



Configure Networking and the Server Hostname

It is recommended to change from DHCP to a statically configured IP address. DHCP may be used with a suitable reservation for the Foldr system, however manual/static configuration for servers is best practice.

All networking configuration can be completed within the **Appliance > Network tab in Foldr Settings,** alternatively the '**netconfig**' command on the Foldr appliance console provides a menu-driven option to configure the various system network settings.

Once the network configuration is configured as required, a **suitable hostname** must be configured using a fully-qualified name set within the **internal** Active Directory domain**.** In the example below the Active Directory domain is *company.internal*. A suitable hostname in this case would be:

foldr.company.internal

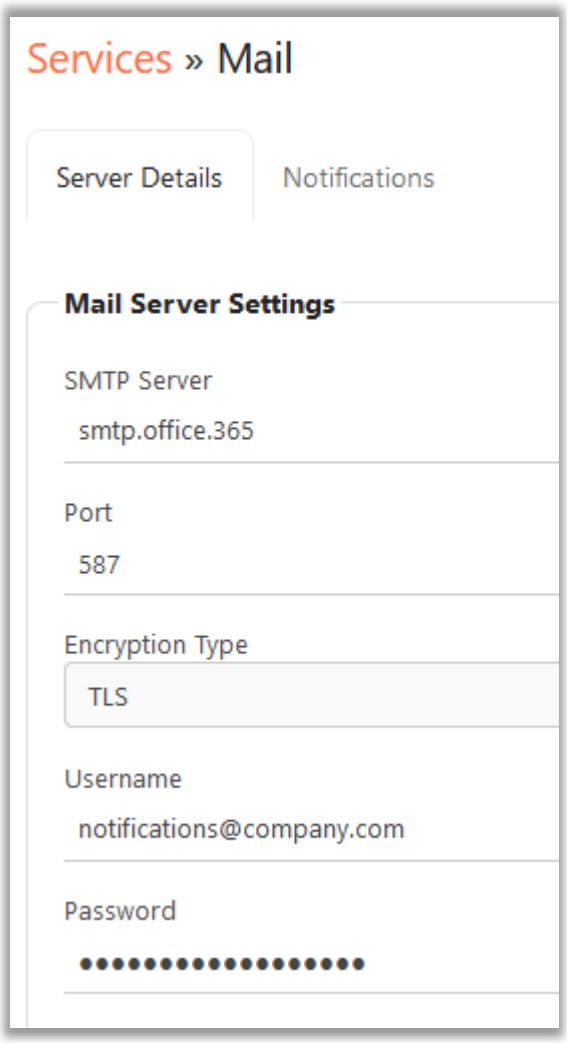
IMPORTANT – The hostname must be set within the internal Active Directory domain. This is important as Foldr uses the system hostname as the DNS search domain to resolve unqualified paths where a search domain is not configured.

Do not configure the hostname to any public domain via which you intend to publish access to Foldr externally. A separate option labelled 'External Hostname is available on the Network tab for this purpose.

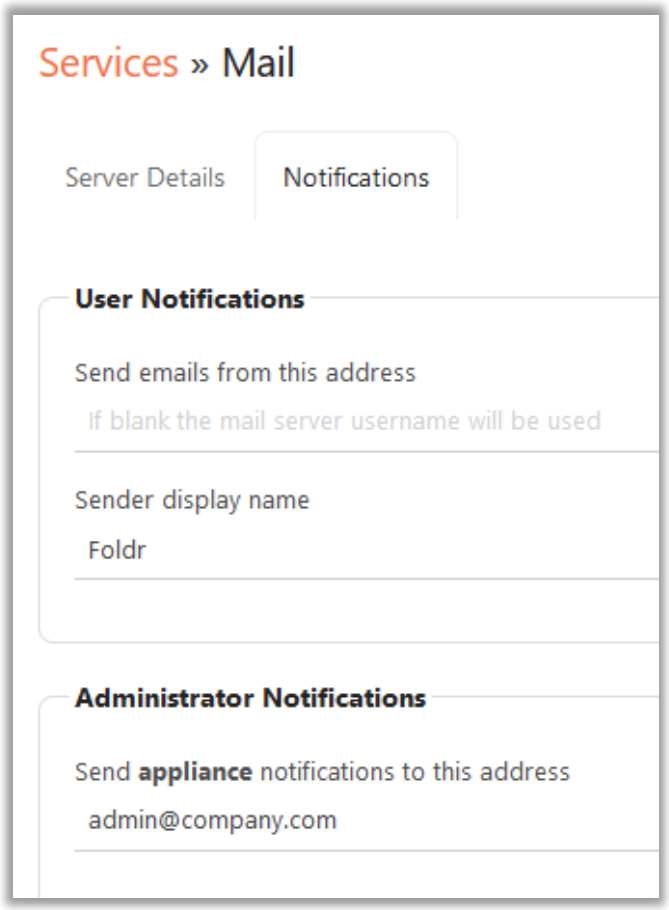
Configure Email Settings for Notifications

The Foldr appliance can alert the administrator to updates and provide users with notifications for the sharing and password reset features. Email settings should be configured within ***Foldr Settings > Integrations > Email*** as appropriate.

Example settings for Office 365 shown below:



The ***Notifications*** tab should also be configured with the sender address and where system notifications should be sent to (typically monitored by the Foldr admin)



Save the configuration, before attempting to send the test message from the Integrations > Mail > Server Details screen. The system will automatically email to alert the administrator of the following: from the

1. Pending licence expiration

2. If an appliance system update is available (requires Updates to be configured to *check automatically* within ***Foldr Settings > Appliance > Updates***)

3. If an appliance update is available and has been installed successfully

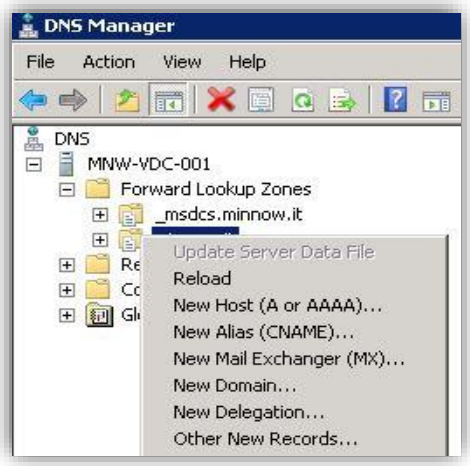
Users may also receive email notifications when items have been shared with them or files have been submitted to shared folders and as part of the Active Directory self-service password reset feature. These features are configured later in the setup process.

4. Creating the internal DNS host record

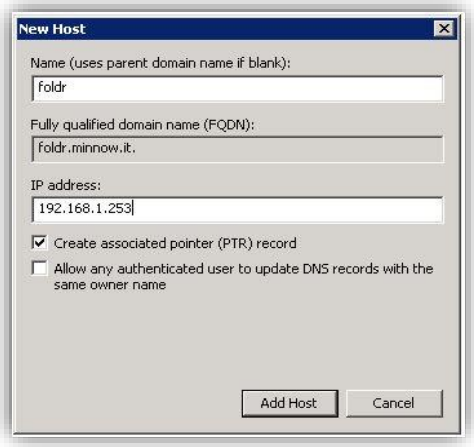
Foldr does **not** automatically create the internal DNS host record so you will need to do this manually. A correctly configured A record on the internal network is important for optimum SMB performance. In the example below, the Active Directory domain name is *minnow.it*.

1. On a Windows Server that hosts the DNS Server role (usually a Domain Controller), click START >> RUN >> type dnsmgt.msc and click OK

2. Expand 'Forward Lookup Zones' >> right click on the internal domain and select 'New Host (A or AAAA)'. Ignore the zone with the prefix '_msdcs.'



3. Assign a suitable hostname and point the record at the private/internal IP address of the Foldr Server.



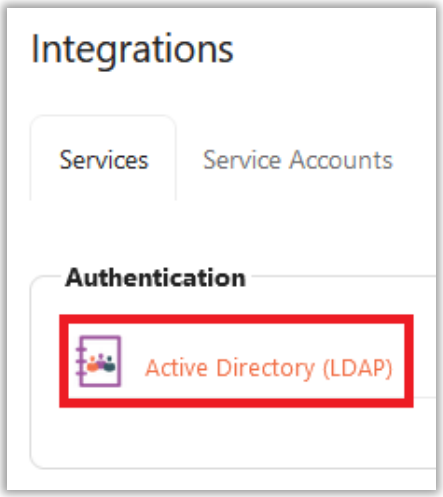
If you have a reverse lookup zone configured on the network, leave 'Create associated pointer (PTR) record' checked, otherwise uncheck it and click 'Add Host'. You should now be able to ping foldr.yourdomain.internal (foldr.minnow.it in the example above) from other devices on the network.

5. Authentication

Now the system is licenced, and the internal DNS record has been created, the authentication settings should be configured.

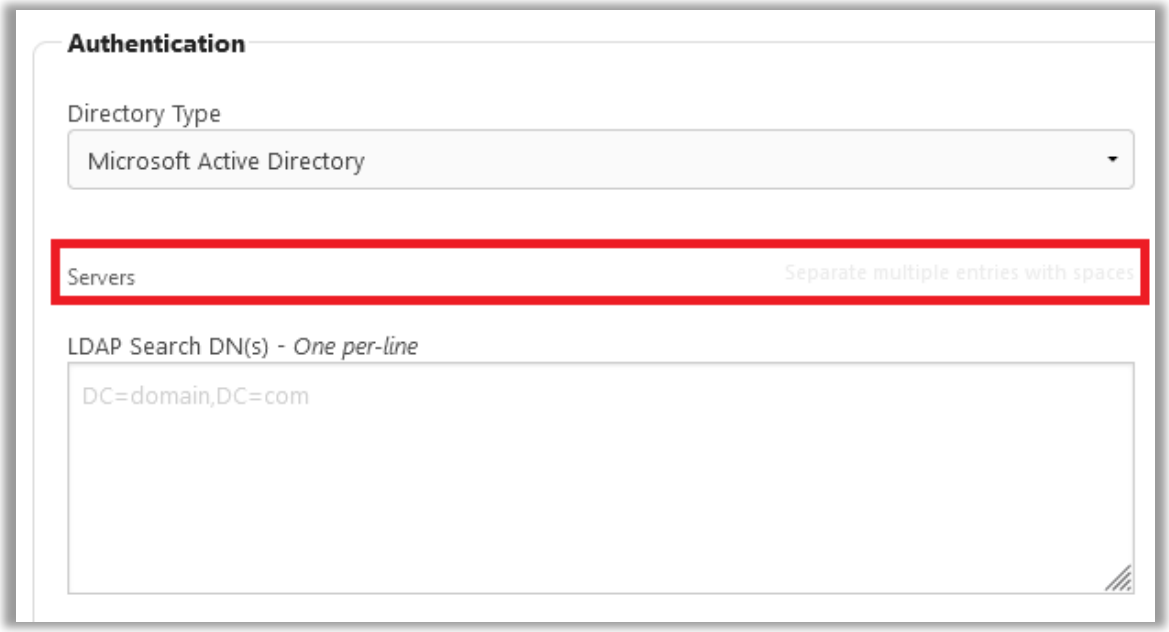
Active Directory

The server must be licenced with a suitable licence key before Active Directory authentication can be configured. Browse to ***Foldr Settings > Integrations > Active Directory (LDAP).*** If Active Directory is not being used, this section can be skipped, and local user accounts created directly in the Users & Groups tab in Foldr Settings.



Active Directory (LDAP) Authentication Settings

Click the Servers field, to configure one or more domain controllers that Foldr will use to authenticate users:



The domain controller(s) should be prefixed with **ldap:// or ldaps:// (if enabled)** and use either the FQDN or IP address of the server. For example:

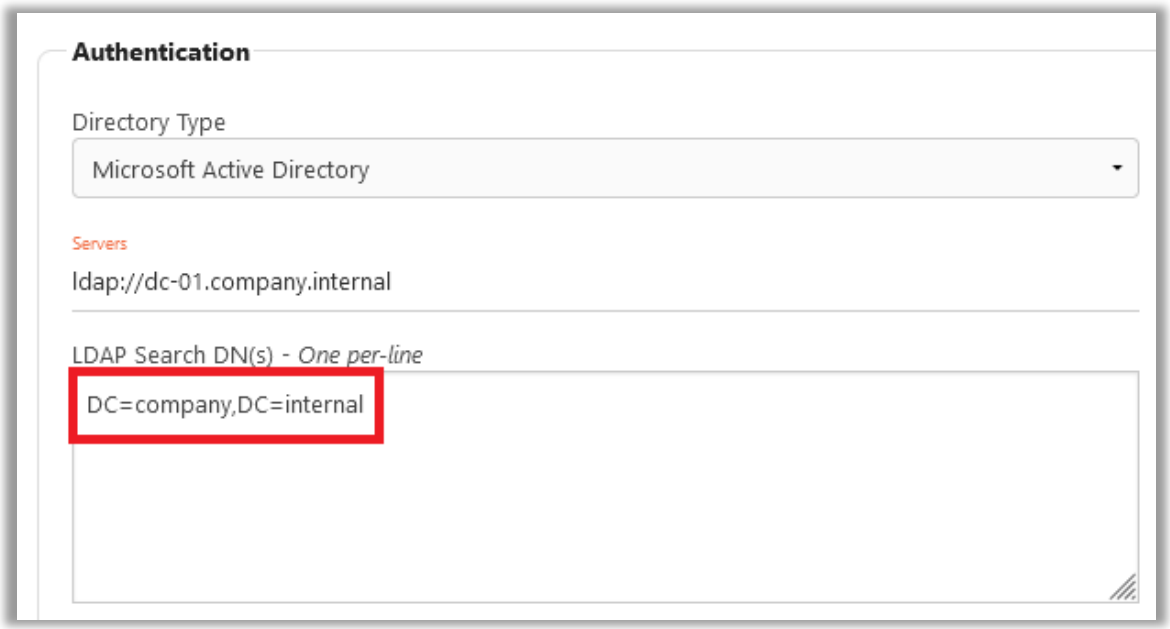
ldap://domain_controller.company.internal

Multiple servers may be configured, and these should be separated with a space. For example:

ldap://dc-01.company.internal ldap://dc-02.company.internal

LDAP Search DN:

The Search DN should now be configured. This setting configures Foldr with a starting point to search for users and groups.



The example shown above will search for users and groups from the **root** of the Active Directory domain (so all OUs contained within are considered) where the domain in the example is *company.internal*. It is possible to specify multiple Search DNs to allow the admin to target specific OUs in the domain, but in most cases it is best to configure the root as the Search DN.

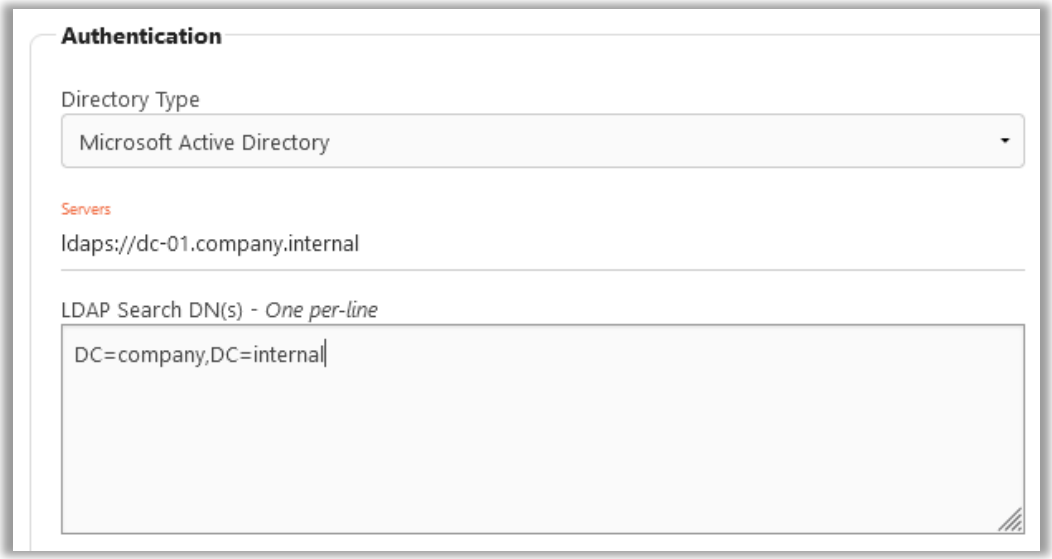
While the Search DN could be used to also control which users are allowed to sign into Foldr, there is a dedicated area to control access to Foldr in ***Foldr Settings > Security > Permissions***.

LDAPS Support

If the Active Directory domain supports LDAPS, this may be used instead of LDAP. To use LDAPS, prefix the Server address with '**ldaps://**'

You can optionally append a port; if this is not done Foldr will use the default LDAPS port of 636.

Example LDAPS Settings:



LDAPS is a requirement for any of the Active Directory password features in Foldr (password change control, delegated or self-service password reset)

Enabling LDAPS on a Windows domain controller is typically done by default after installing the Domain Certificate Services >> Enterprise CA role in Server Manager. However, there are other methods and considerations to be made when enabling this feature in your Active Directory infrastructure:

https://www.petri.com/enable-secure-ldap-windows-server-2008-2012-dc

Local Foldr Users

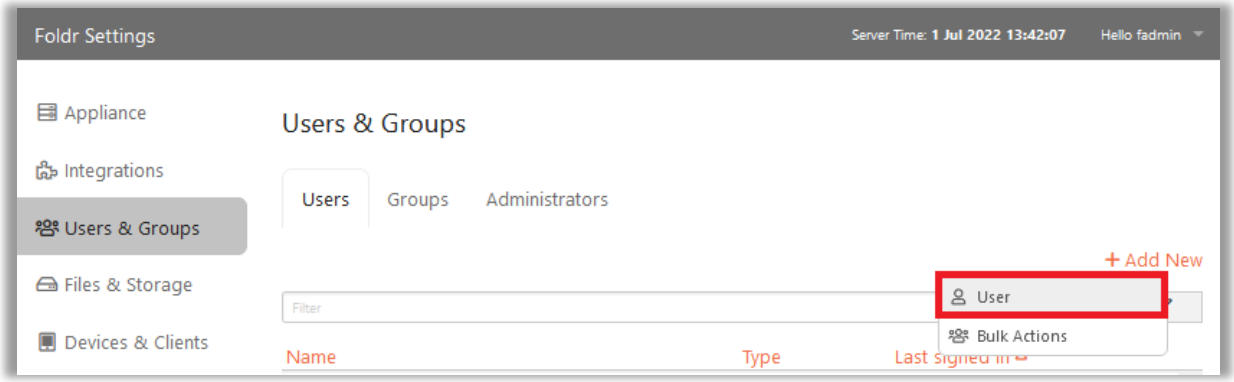
Local users may be created on the Foldr server itself where no Active Directory or Azure AD environment exists, or local users may be used in conjunction with on-premise AD or Azure AD users. If the licence key installed is set for an Active Directory domain, the server will still need to bind/authenticate with the Active Directory, even if local users are being used.

Where a per user licence is being used, each local user will consume 1 user licence slot in the same way as an Active Directory or Azure AD user. A built-in mechanism is available on the Foldr server to automatically delete local users that have been inactive for a configurable duration. When a local user is deleted, either manually or as part of the above schedule its user licence will become available again.

Local users may use SSO, security features such as 2FA/WebAuthn and be presented SMB shares or cloud storage platforms as usual. However, where SMB shares are being used, a service account must be configured on the share and the 'Use service account for all access' toggle must be enabled.

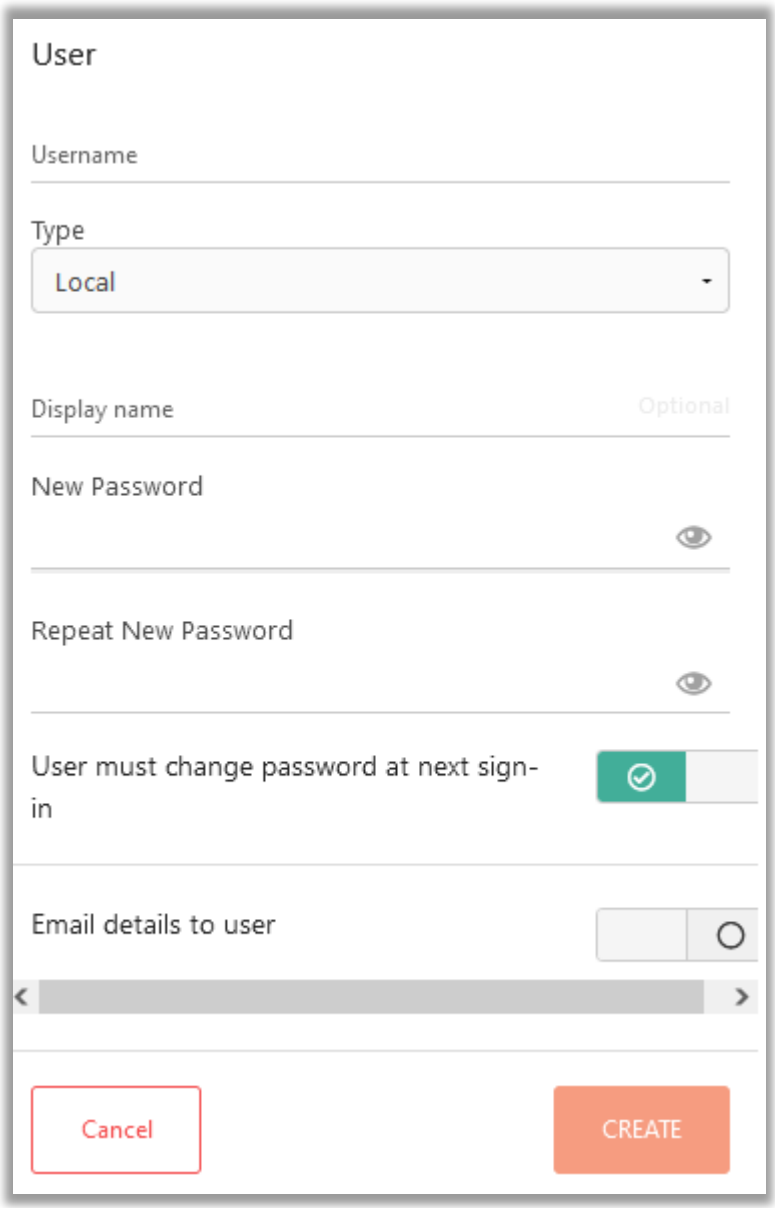
Local users can be created in ***Foldr Settings > Users & Groups***

Click **+ Add New > User**



Specify the username, display name, and password options. Note the type is 'LOCAL'.

The username should ideally be set to a UPN/email address style format, although short usernames may be used.



If the email settings have been configured to allow the Foldr server to send email, you may also enable the 'Email details to user' toggle to send a welcome email (this will be sent to the username)

Click **Create**

Local Groups

Local groups may be created on the Foldr server for the purpose of:

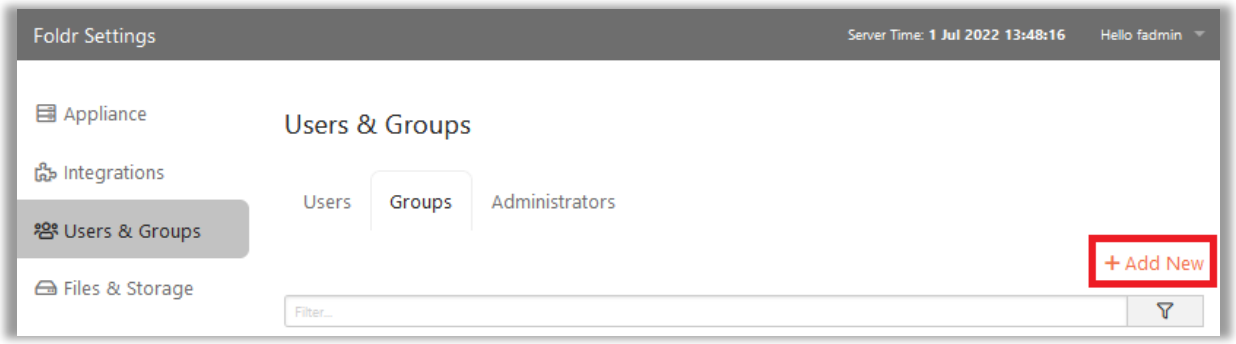
1. Grouping users together to apply Foldr permissions on those users or enabling features (type = **local**)

2. Grouping users together for the purpose of sharing files/folders with other local users on the server (type = **sharing**)

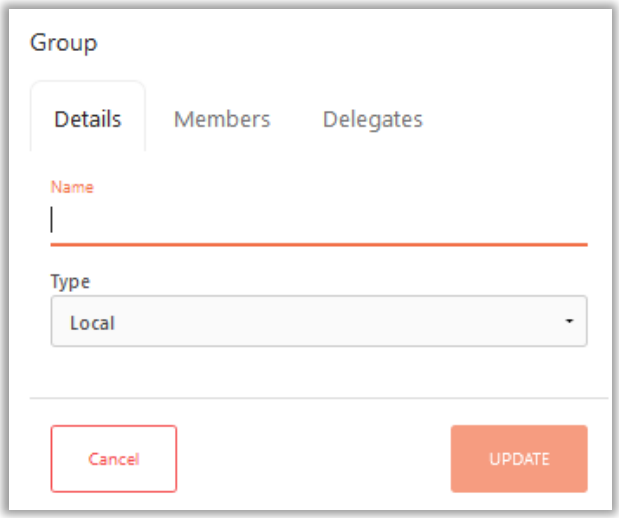
Typically local groups would only need to be created in Foldr, if existing groups in Active Directory or Azure AD don't already exist, or if the admin wishes to create groups for a specific purpose without creating groups on the external directory service.

Local Foldr groups can be created in ***Foldr Settings > Users & Groups > Groups tab***

Click **+ Add New**



Give the group a suitable name and use the Members tab to populate the group with users. Local groups may be populated by either Active Directory, Azure AD or Local Foldr Users.



Service Accounts

As part of the initial setup process, you must now configure the main appliance operations service account. There are three main types of service account in Foldr, these are:

1. Appliance operations service account (Important)

In an on-premise Active Directory deployment, a domain-based account is required to read the Active Directory domain, query group memberships and search for users / groups within the administrative and user facing app interfaces. The main appliance service account is created within ***Integrations > Service Accounts*** and must then be selected within ***Integrations > Active Directory***. The service account username MUST use the **UPN format** of username@domain.fqdn using **type 'Username/Password'**.

This type of service account is **not** required for Azure AD deployments.

IMPORTANT - Failure to configure a service account will cause authentication issues against Active Directory when users attempt to sign into any of the apps. If local accounts or Azure AD is being used, this service account is not required.

2. Share based service accounts

This type of service account is used primarily to facilitate file sharing, public links or Inbox (receive email) features. A share-based service account can use either Active Directory based or standalone credentials if the target storage system is not bound to the domain.

If they are required, share-based service accounts can be selected within ***Files & Storage > Edit-Share > Access tab > Service Account*** within each share configuration screen. The main appliance service account can also be used where a share-based service account is used, or separate service accounts can be created if necessary. More information is available in the full administration guide & KB.

Where **local users** are being used, a service account must be set on all SMB shares in conjunction with the **'Use service account for all access toggle'** to present SMB shares to local Foldr users.

3. Cloud platform service accounts

In any deployment type (Active Directory, Azure AD or local accounts) the administrator may also configure a service account that is used by Foldr to interact with a cloud service, such as Google Workspace, Office 365, Dropbox, Box or Amazon AWS/S3 etc. Generally, a cloud-based service account is used to either automatically provision a user's personal cloud storage to them or present one cloud account storage location to multiple users simultaneously. More information is available in the full administration guide & KB.

Multiple service accounts can be configured as required within ***Integrations >> Service Accounts***.

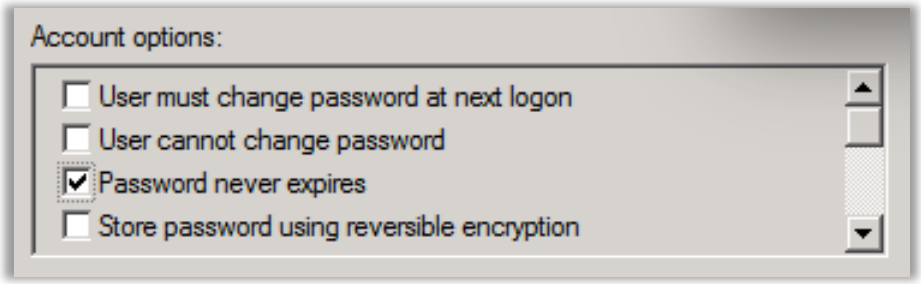
Creating the Service Account for Appliance Operations

As mentioned previously, with an on-premise Active Directory deployment, to enable Foldr to function correctly and search the directory service, query group memberships and provide more advanced capabilities such as delegated / password reset control and file sharing, the Foldr administrator must provide the system with at least one Active Directory based service account.

It is recommended that you create dedicated service account(s) specifically for use with Foldr, rather than use existing user accounts. While not mandatory, these accounts should ideally:

1. Use a complex password

2. Have the '**password never expires**' flag set.



3. Have minimal permissions required for the functionality required. Membership of the built-in **Domain Users** group is sufficient for basic functionality (authenticating users) for the main system service account configured within ***Foldr Settings > Integrations > Active Directory (LDAP)***.

4. Be restricted from logging onto domain computers. This can be done centrally via Group Policy using the 'Deny Logon Locally' option under *Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment*

A standard Active Directory account that is solely a member of **'Domain Users'** should have sufficient privileges to read the domain for basic functionality such as authenticating users. File sharing, public links, delegated password control and self-service password reset will require additional service account permissions.

To create the main appliance service account, browse to ***Foldr Settings > Integrations > Service Accounts*** and click **+ Add Service Account**.

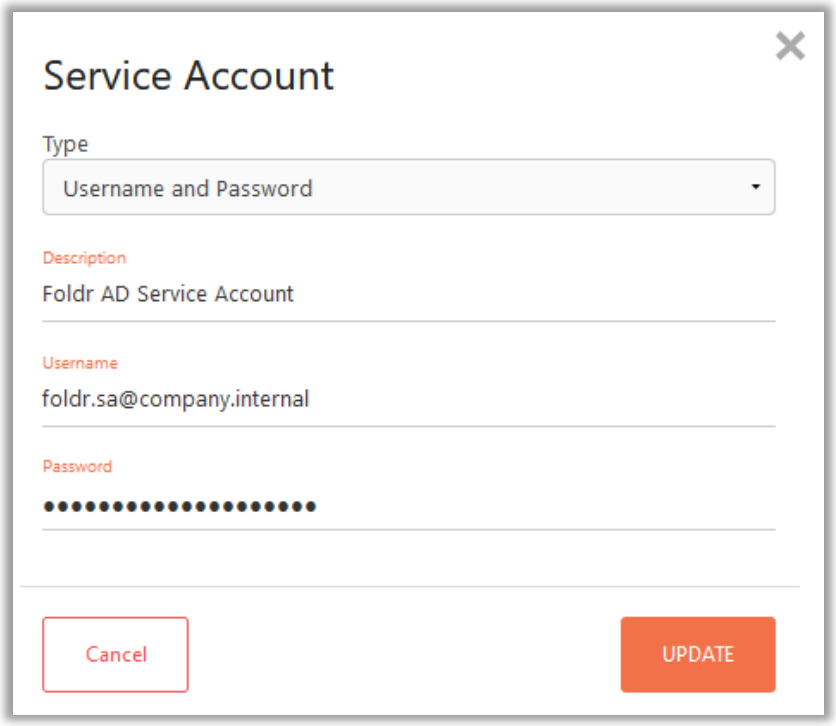
All Active Directory based service accounts should be configured using:

Type = Username and Password

Username must be using the UPN of the account. For example:

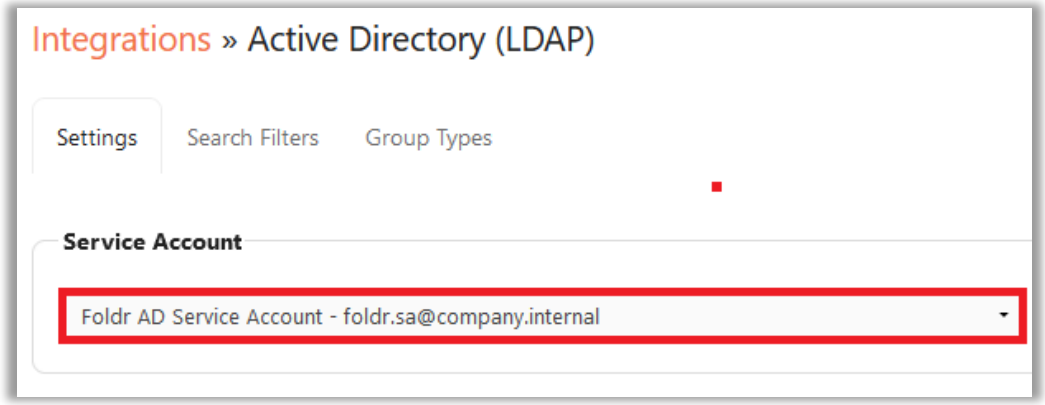
username@company.internal

Do not attempt to use *DOMAIN\username* or other format to specify a Foldr service account.



If the Active Directory domain uses custom UPN suffixes for integration with other services, it is recommended to **default Active Directory domain suffix** is used for the service account.

Click **Save** and navigate to ***Integrations > Active Directory (LDAP)*** and select the service account to be used for appliance operations.



IMPORTANT – In an Active Directory deployment, a service account **must** be set in ***Integrations > Active Directory (LDAP)***. Failure to configure a service account will result in authentication issues for users and other features will not function as expected.

The basic configuration for Active Directory is now complete, and you should proceed to test authentication using the Test Settings function (see section 6)

Azure AD (AAD)

The server must be licenced with a suitable licence key before Azure AD authentication can be configured.

To allow Foldr to authenticate natively against AAD, an app registration for Foldr must be created in the Azure portal, API permissions are configured, and an application ID and client secret taken from Azure needs to be saved on the Foldr server.

1. Log into the Azure portal at https://portal.azure.com using a suitable administrative account

2. Create an App Registration for Foldr, by clicking Azure Active Directory > App Registrations > + New Registration

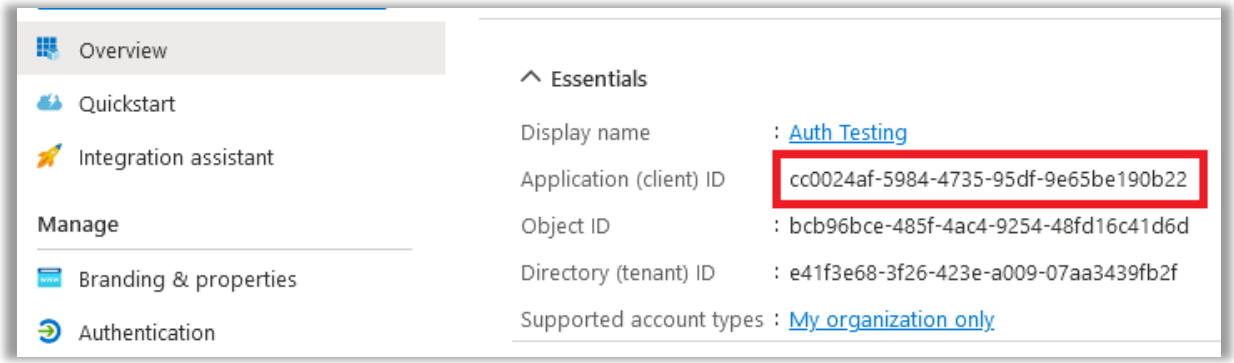
In the New Registration screen, give the app a suitable name, leave the supported account types as default (Accounts in this organizational directory only) and configure a Redirect URI using the platform type 'Web' using a Redirect URI configured as follows:

https://address-of-folder/services/microsoft/connect

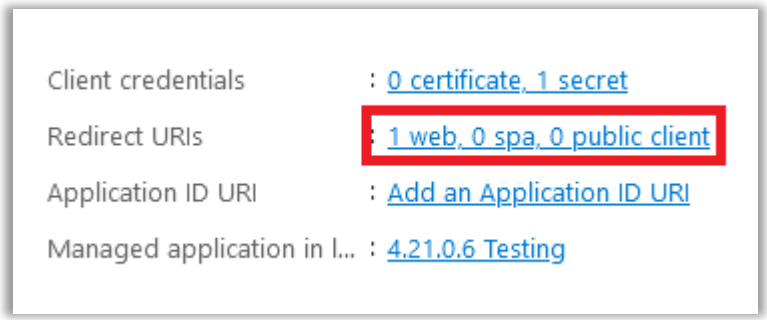
Replacing address-of-foldr with the public FQDN of Foldr.

Finally, confirm by clicking **Register**.

4. The Overview panel will be displayed. From this, take a note of the 'Application (client) ID' – this will be required later.



5. From the Overview panel, click the Redirect URI link



Add a second Redirect URI for:

https://address-of-foldr/services/microsoft/signin

Replacing address-of-foldr with the public FQDN of Foldr.

6. Click **Certificates & secrets** from the left-hand panel > **+ New Secret**

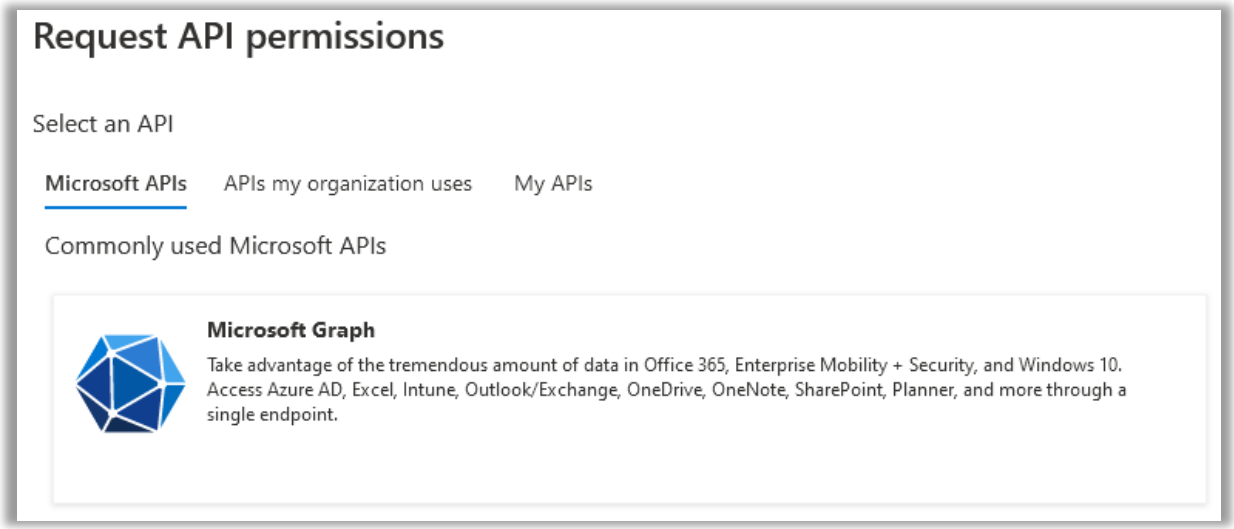
7. Enter a description, select a suitable expiration lifetime, and finally click **ADD**.

The new client secret will be displayed.

IMPORTANT – You should take a copy of the key at this point (the **VALUE**) as you cannot retrieve it again later, however new keys can be generated later, if required.

8. Click API Permissions > + **Add a permission**

9. Select **Microsoft Graph**



10. Click **Delegated** Permissions

Select the following Delegated permissions from the Directory, Files and User sections:

Directory.Read.All
Files.ReadWrite
Files.ReadWrite.All
User.Read

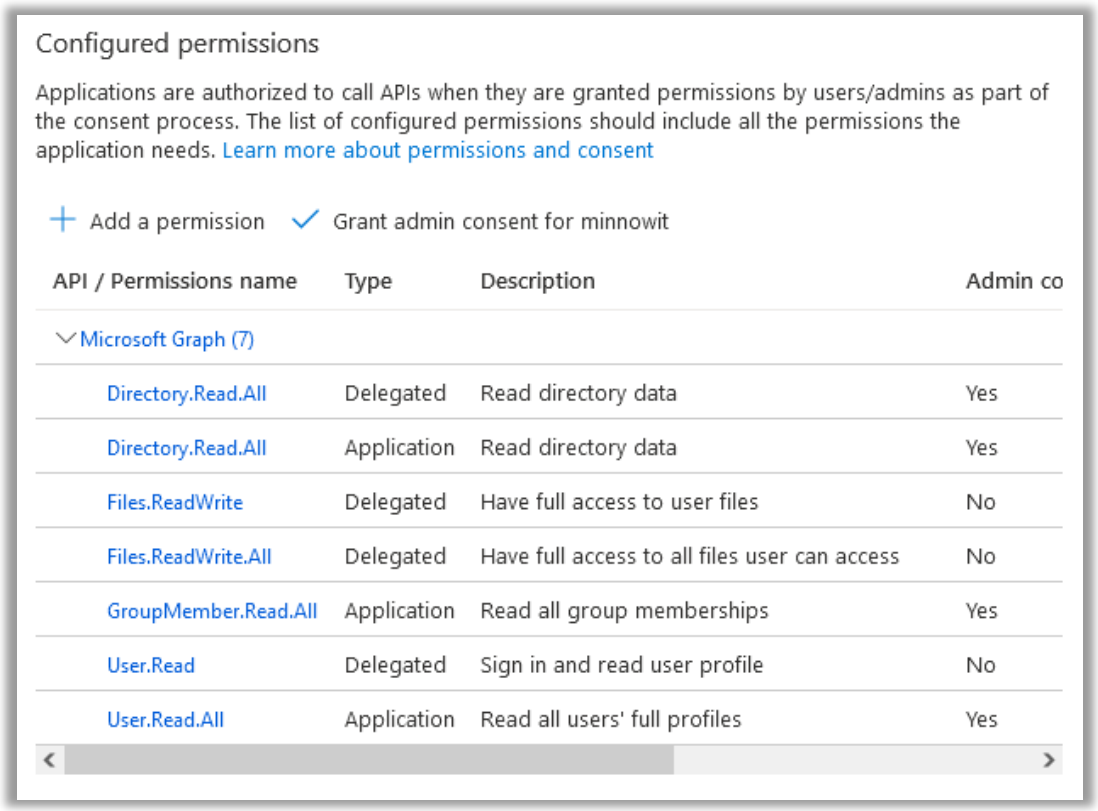
Click the **Application** Permissions box at the top of the Permissions selection panel (or go back to the App Registration overview and use API Permissions > Add a permission > Microsoft Graph > Application Permissions)

Select the following **Application** permissions from the Directory, GroupMember and User sections:

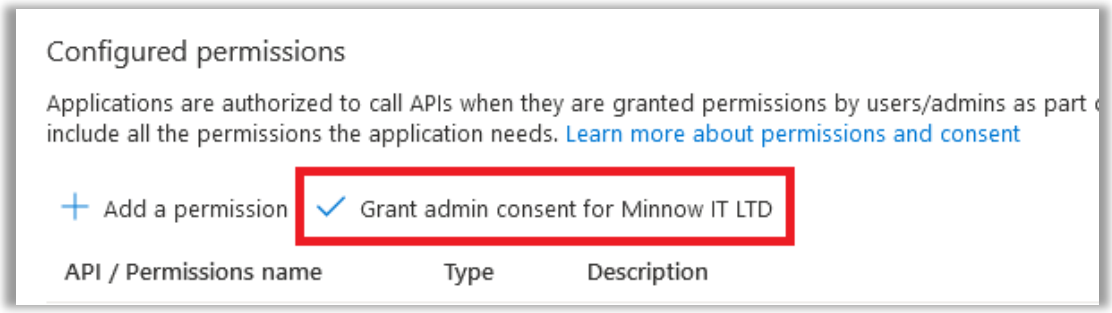
Directory.Read.All
GroupMember.Read.All
User.Read.All

Once the Permissions have been selected. Click **Add Permissions** to confirm.

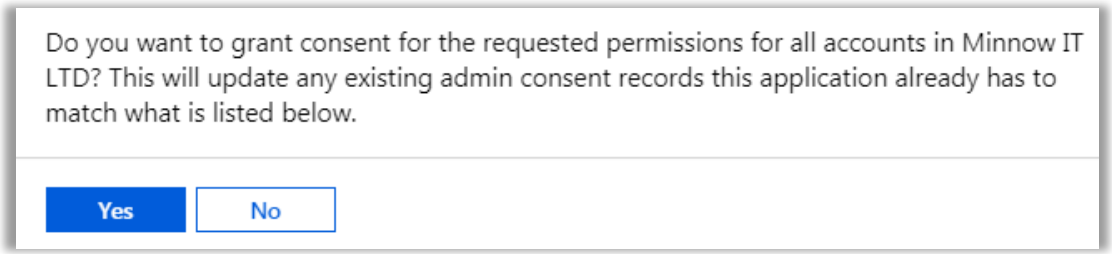
11. The permission summary will now be shown showing the updated delegated and application permissions.



12. Click the **GRANT ADMIN CONSENT** for <organisation> button.



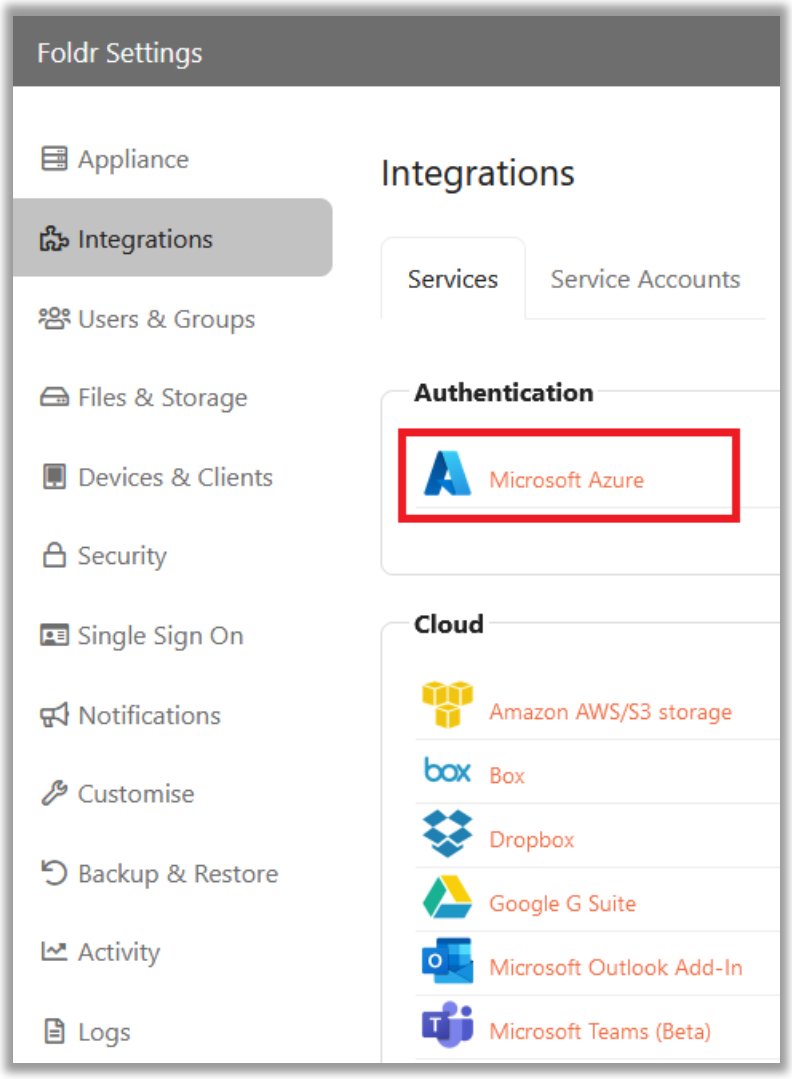
Click **Yes** on the confirmation prompt.



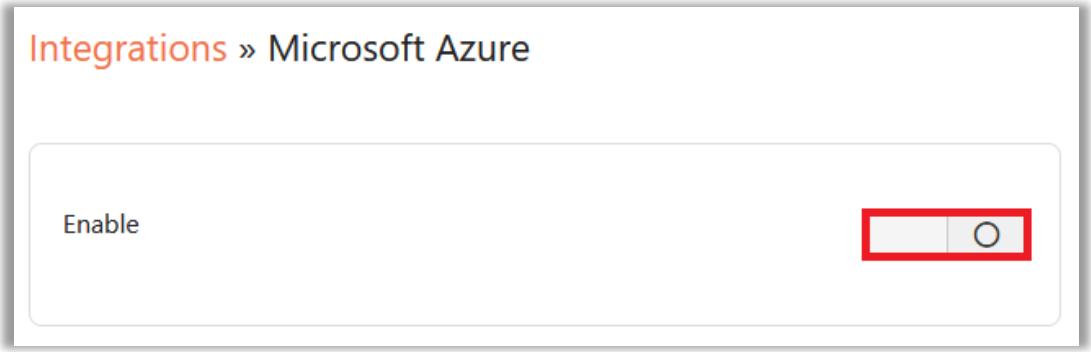
13. A success message will then be shown

Enable Azure AD Authentication in Foldr
Ensure the Licence key has been applied to the system (Appliance > Status > General > Licence) before proceeding.

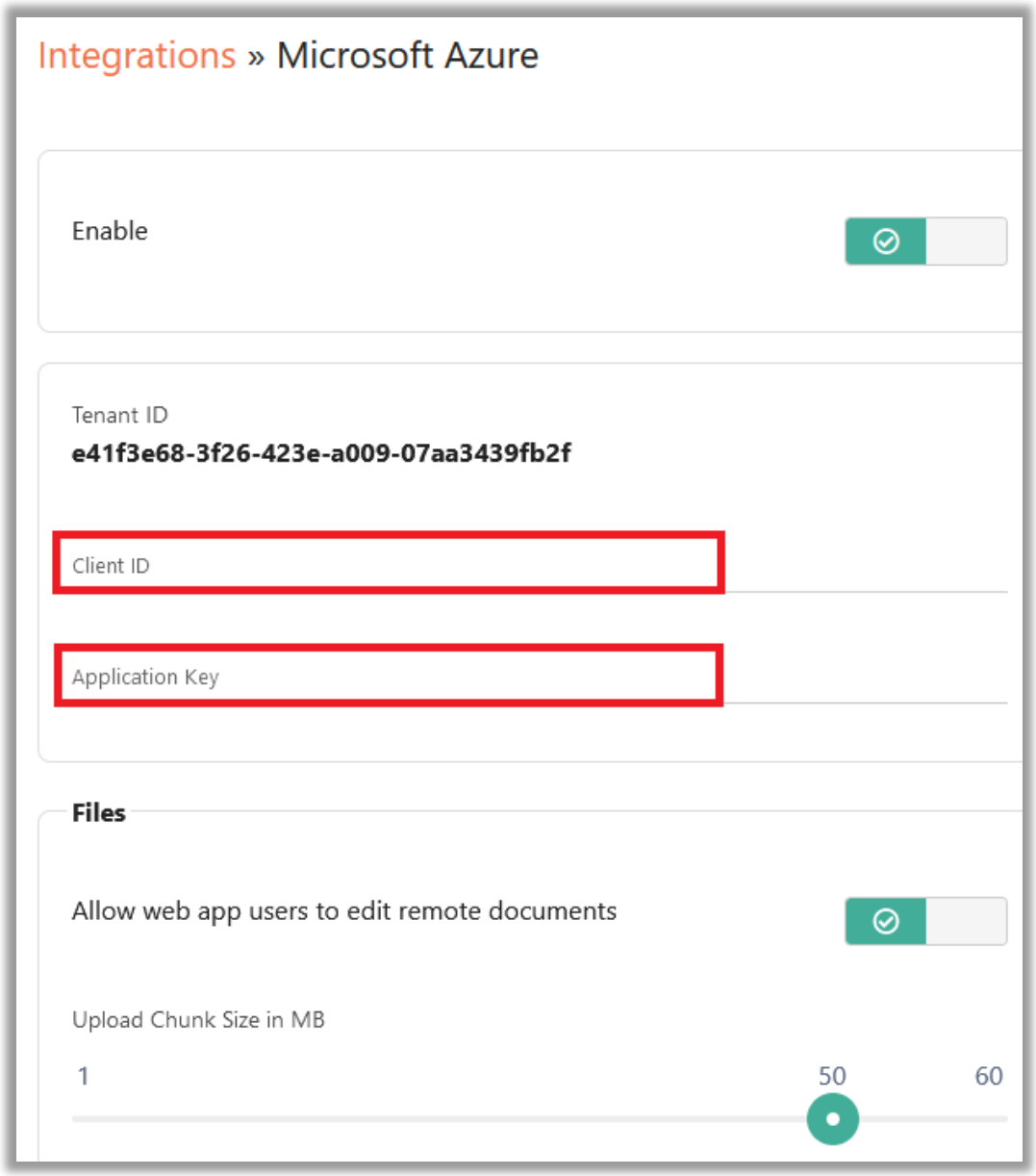
1. Click the **Integrations** tab and select Microsoft Azure under the Authentication section



2. Enable the Integration by using the toggle



3. Copy and Paste the Client ID and Application Key values created earlier in App Registration in Azure.



Client ID = **Application (client) ID** in Azure

Application Key = **Client secret** in Azure

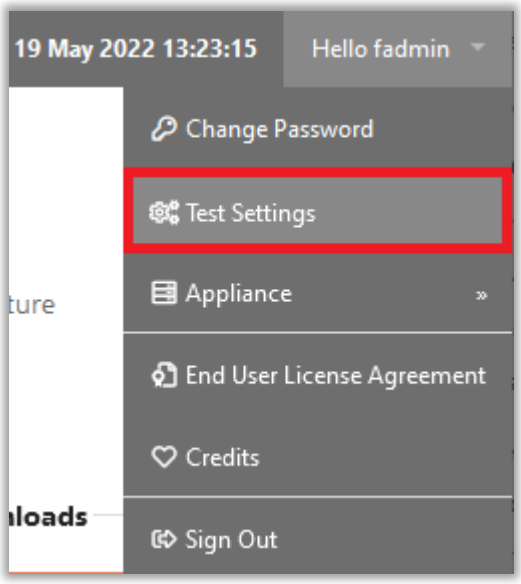
4. Save Changes

AAD authentication is now configured, and users should be able to sign into the Foldr web, mobile and desktop apps using their Office 365 credentials. If MFA is enabled on the account in Office 365, the user will need to complete this to sign into Foldr.

6. Testing Authentication

Note - **This section applies only to Active Directory and local user accounts in Foldr**. Azure AD authentication is not compatible with the Test Settings feature.

Now the appliance has been configured to authenticate against Active Directory (or using local accounts), and a service account has been configured, you can test authentication using the 'Test Settings' feature. Test Settings is accessible in the top-right menu in Foldr Settings.

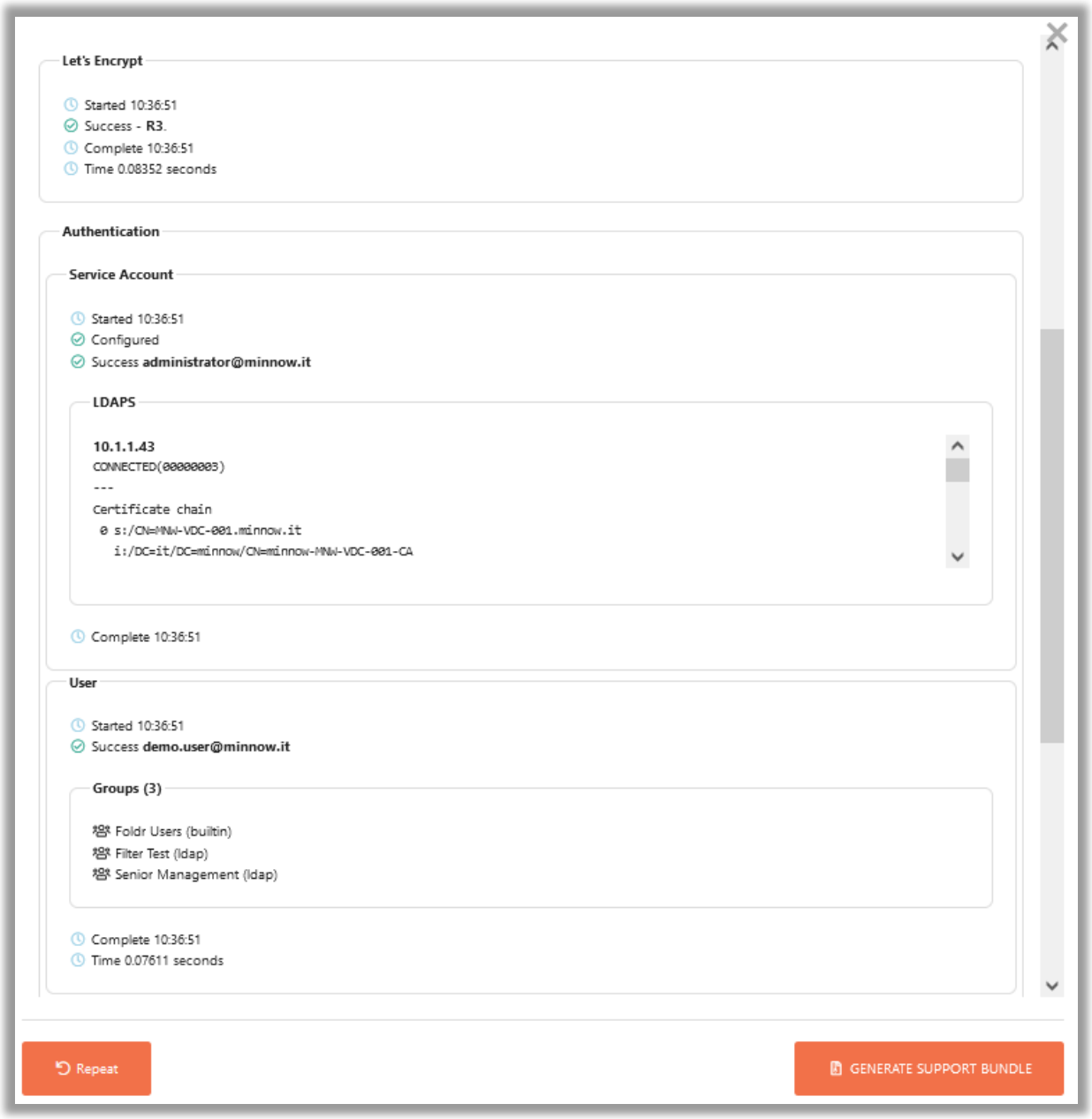


A username and password prompt will be shown. Enter either an Active Directory username (short format/sAMAccountNAme is accepted) or a local Foldr account and the password. Ideally an Active Directory user will have a home folder configured to test SMB connectivity.

Click the Test Settings button. The Foldr server will perform various tests, including DNS (including local and AD domain), authentication for both the service account and user entered in to Test Settings, group membership, SMB connectivity to the home folder (if present) and HTTP tests for online services such as Google, Office 365 and Let's Encrypt).

When the test is complete a results dialog will be displayed. Note that if no home folder is configured for the user entered, or online services such as Google Workplace or Office 365 are not configured/enabled, the Test Results dialog will not show that section of the results output.

An example excerpt of the Test output is shown below:

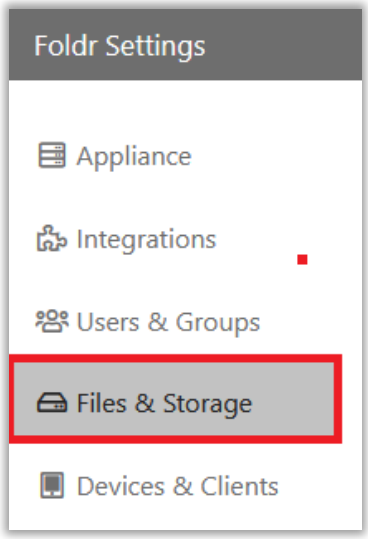


If there is an issue with any step in this process it will be highlighted by the test procedure.

7. Presenting Storage to Users

Users can now authenticate but were they to sign into Foldr at this point no storage locations would be available to them. The administrator should now configure the storage locations that you wish to users to access (i.e., SMB file shares, home folders, cloud storage etc.)

All storage locations are configured within **Foldr Settings > Files & Storage**

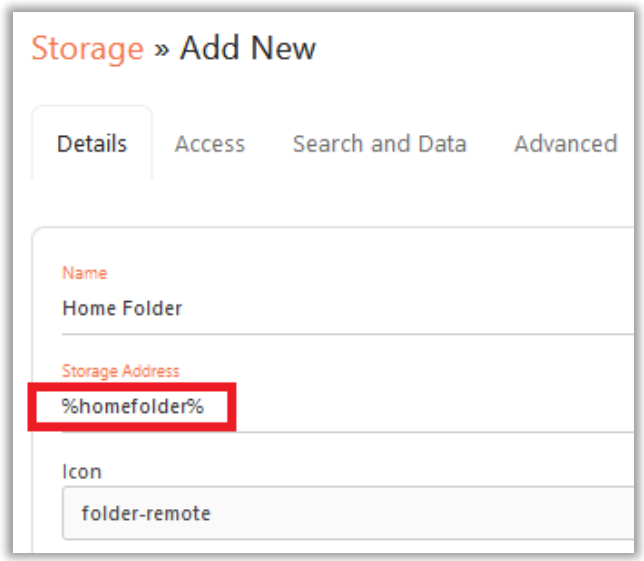


SMB Home Folders / Home Directories

Foldr can automatically discover and connect user accounts to their corresponding home folder, providing one is configured within Active Directory - inside:

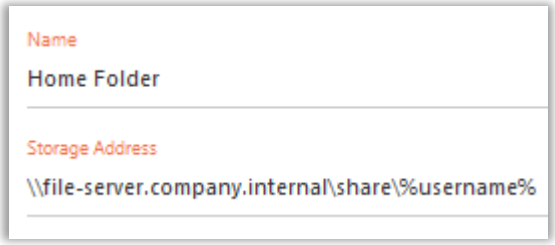
Active Directory Users & Computers > <Properties of User object> > Profile Tab > Home Folder > Connect

To perform automatic home folder provisioning, a single storage items can be configured as using the Storage Address variable **%homefolder%**



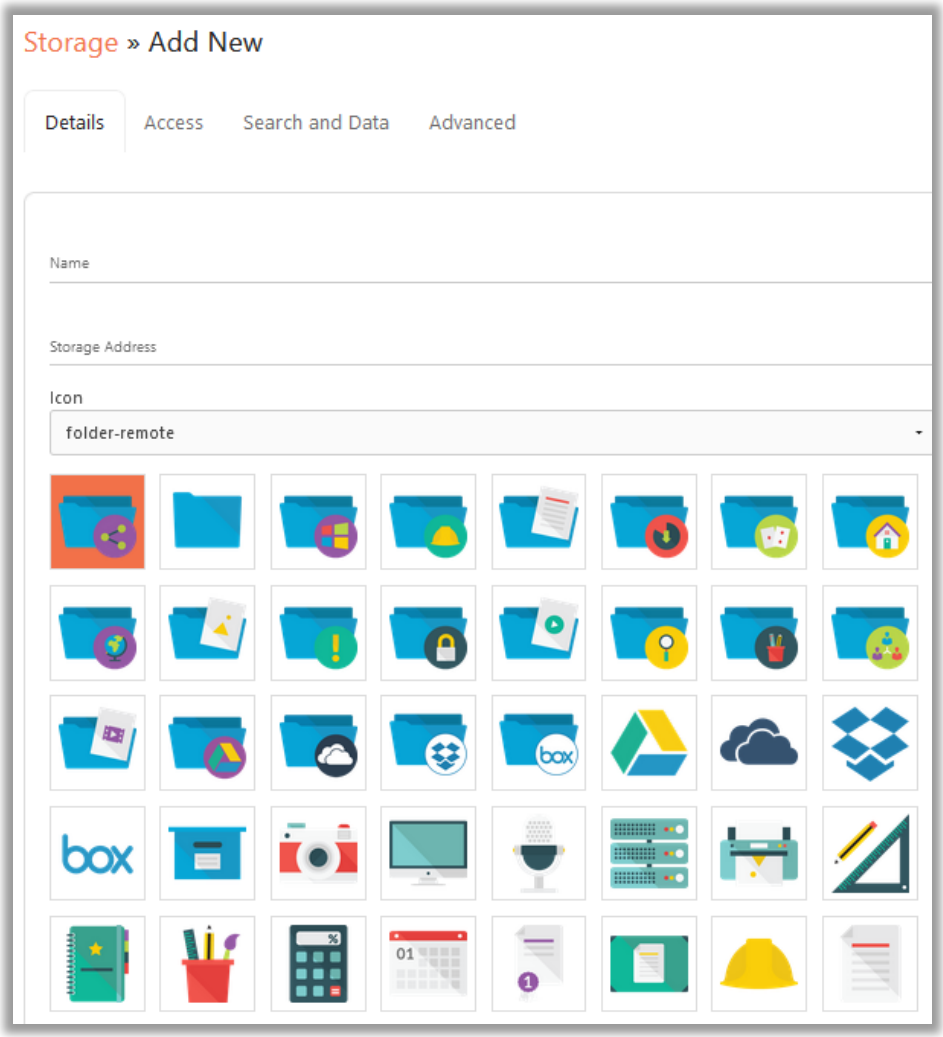
If user's home folders are not configured in Active Directory and presented to users using other methods (for example, login scripts or Group Policy Preferences) the administrator can add one or more additional shares as necessary to map share paths to user's home folder locations as required.

The standard environment variable **%username%** is supported so you can bulk provision home folders to suit the network environment.



Other SMB Shares

To present network shares other than the home folder, add another share and configure the Storage Address as required.



Name: This is the name of the storage item that is presented to the end user in the Foldr web, mobile or desktop apps

Storage Address: Enter the **fully qualified network path** to the share, prefixed with smb:// - This should be configured as shown below:

smb://file server FQDN or IP address/share name

Example: ***smb://fileserver1.company.internal/Resources***

Windows style UNC paths are accepted and are automatically converted into a compatible format by the appliance:

\\fileserver1.company.internal\Resources is automatically converted to

smb://fileserver1.company.internal/Resources

DFS Shares

DFS Shares are supported, however DFS shares must be configured **fully qualified and use folder targets** as shown:

smb://company.internal/namespace_root/folder_name_or_folder_target

Unqualified DFS paths or incorrectly configured DFS environments (such as storing user data in the namespace root share) may not work as expected through Foldr.

Office 365 Storage Objects (OneDrive, SharePoint and Teams)

Office 365 storage can be added to Foldr regardless of the authentication type (Active Directory, Azure AD or local users). **The following steps apply ONLY to Azure AD deployments**. The steps to configure Office 365 storage for Active Directory and local authentication deployments can be found in the Full Administration Guide, or on the support knowledge base at https://kb.foldr.io

1. Navigate to the **Files & Storage** tab in Foldr Settings

2. On the Storage tab, click **+ Add New**

3. To configure the storage item for *OneDrive*, give it a suitable name and using one of the following built-in variables as the Storage Address:

%onedrive% = All files and folders in the user's OneDrive

%onedrivewithshared% = As above but in addition will include a folder containing items that are shared with the user in Office 365. These are accessed in Foldr using a subfolder in the root of the user's OneDrive labelled 'Shared with Me' as shown below.

%onedriveshared% = Only shared items in Office 365 will be shown in this storage item in Foldr.

4. Create additional storage objects in Foldr Settings > Files & Storage for *SharePoint* sites as required using the same steps above but using a Storage Address of:

%sharepoint%(tenant.fqdn/sites/site-name)

A dedicated online KB article is available regarding presenting specific SharePoint sites and document libraries at https://kb.foldr.io

5. Create additional storage objects in Foldr Settings > Files & Storage for *Teams* as required using the same steps above but using a Storage Address of %teams%

The integration is now complete, and users should be able to sign into Foldr using their Office 365 credentials. If MFA is enabled on the account in Office 365, the user will need to pass this to sign into Foldr.

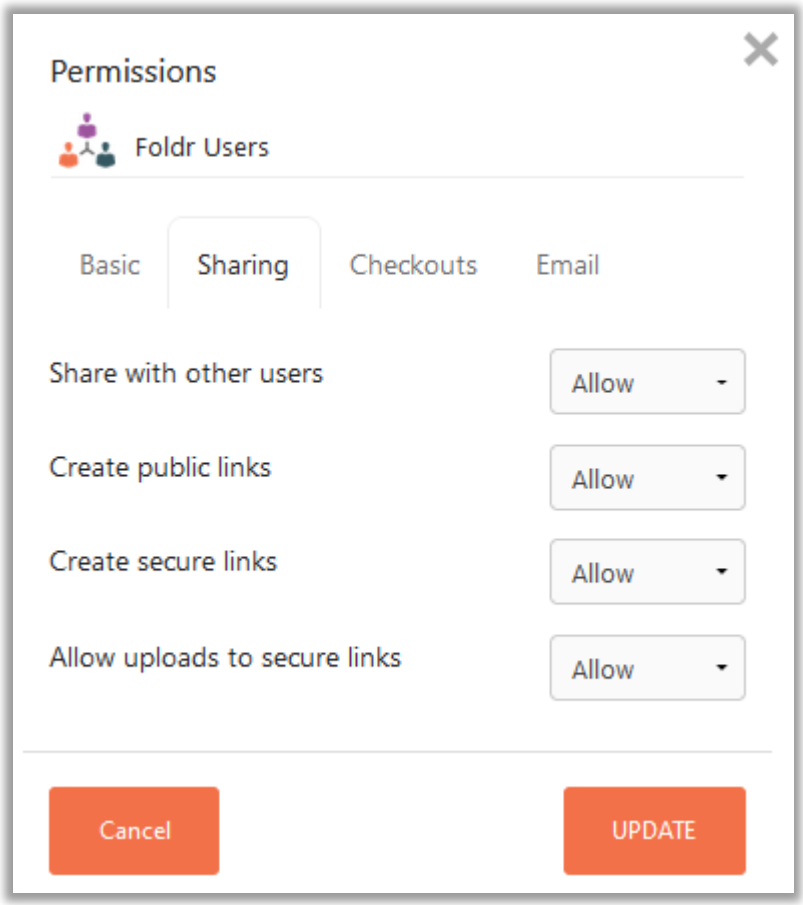
Other Storage Locations

For instructions configuring any other type of storage locations - SFTP, WebDAV or Cloud Storage such as Google Drive, Office 365, Box, AWS/S3 please consult the full administration guide or online KB at https://kb.foldr.io

8. File Sharing

Foldr comes with powerful file sharing features to allow users to securely share files / folders with others in the organisation and third parties. All sharing features are disabled by default and must be enabled by the administrator on a per user basis for the users / groups that require them.

Within the Permissions section in the share configuration screen, the administrator can enable Sharing features, check outs and other features. All permissions may be enabled for EVERYONE (Foldr Users) or on specific users or groups as required.



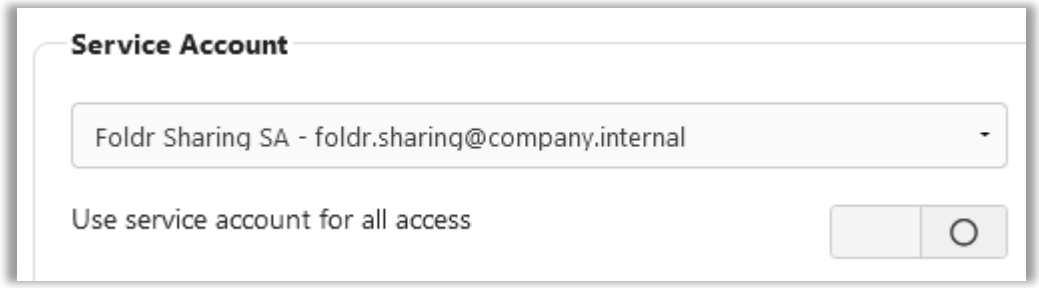
'**Share with other users**' refers to sharing content with other users *inside* the organisation. Items will appear in a user's 'Shared with Me / Shared by Me' as appropriate. The recipient requires an account in the Active Directory to receive shared items. There are different types or sharing available to the user to provide read only, work hand-in/submission and full collaboration rights to the recipient.

'**Create Public Links**', if enabled, allows a user to create special short URLs, called Public Links to share content with third parties. No authentication is required by the third party using a Public Link.

'**Create Secure Links**' if enabled, allows a user to create public links as above, but they are only accessible by specific external users. These external users are identified by their email address and receive notifications from the Foldr system that files have been shared with them. An external user will be prompted to create an account password to access shared items the first time they try to access a shared item.

'**Create Secure Writable Links'** will offer the user a toggle to allow the external user to upload back to the shared folder.

NOTE - If the files/folders being shared are hosted on SMB shares, the sharing features require a **service account must be configured on the storage object** and the account must have sufficient permissions to read data stored upon it as a minimum. In the case of hand-in / manage shared folders or secure links where external users are permitted to upload, the service account will need write permission to the shared storage location.



The service account credentials are used transparently to users to read / write shared files on behalf of the recipient using the shared item.

More information on the sharing features in Foldr is available in the full administration guide and online KB

9. External Access

Foldr requires only TCP port 443 (HTTPS) to be open inbound from the Internet to allow users to use any of the client apps. However, it is also recommended to open TCP port 80 (HTTP) for user's convenience (otherwise they are forced to type 'https://' into their browser to initiate a connection). Opening port 80 also allows you to benefit from using free signed SSL certificates from the Let's Encrypt service. Any user connection that is initiated on port 80 (HTTP) is automatically redirected to port 443 (HTTPS)

1:1 static NAT / MIP using a dedicated public IP address (or standard port forwarding) is the recommended method of providing external access to Foldr. Alternatively, for customers that are not able to dedicate a public IP address to Foldr, you can publish Foldr as a standard web resource using Microsoft Forefront TMG Server or through another reverse proxy service such as Nginx or Windows IIS / ARR.

Please consult your Firewall documentation, IT Support Department, or Internet Service Provider for assistance.

A dedicated KB article to assist with external access is available here.

10. SSL Certificates

All user activity, regardless of the method of connection (web, desktop, mobile apps or WebDAV) takes place over HTTPS. As such the Foldr server is provided with a self-generated (self-signed) SSL certificate to encrypt user and administrative sessions. However, any self-signed certificate will, by its very nature, present the user with certificate trust / server identity warnings in web browsers and on mobile devices. Whilst these can be bypassed (or suppressed in the mobile apps), it is recommended that you install a signed certificate, either using the free Let's Encrypt certificate authority that Foldr provides support for or from a recognised certificate provider such as GoDaddy, Verisign, GlobalSign etc. Certain features in Foldr require a signed certificate to be present, such as media streaming in iOS and certain cloud storage integrations.

Let's Encrypt (free) SSL Certificates

Foldr v4 provides built-in support for the Let's Encrypt Certificate Authority. This service provides signed SSL certificates at **no charge with ongoing automatic renewal**. This is a good option for sites that do not already own a wildcard or UCC/SAN certificate that can be used with Foldr.

Instructions for using Let's Encrypt certificates can be found in the full administration guide or online KB

Installing / Purchasing a Signed SSL Certificate (Using a paid-for certificate)

To purchase an SSL certificate from a traditional Certificate Authority such as GoDaddy or Verisign the Foldr appliance can create the Certificate Signing Request (CSR) and Private Key pair. This can be achieved in various ways, but a recommended method is to use DigiCert's EasyCSR tool online. This will produce the required OpenSSL commands, which can be run locally to generate your CSR and private key files. The configuration steps to do this are available in the online KB

Using an Existing SSL Certificate

If you have an existing UCC/SAN or wildcard certificate, this can be imported into Foldr.

In the case of a SAN certificate, you will need to add the Foldr common name (appliance URL) to the list of Subject Alternative Names. Wildcard certificates are usually available / exported from other existing servers in PFX format which is commonly used in Microsoft Windows Server environments.

Wildcard (PFX format) Certificate Installation

Full instructions for installing an existing wildcard or SAN certificate can be found in the full administration guide or online KB

11. Connecting to Foldr (Users)

NOTE – You will need to manually create the host (A) record on your internal and public DNS server(s).

Desktop web browser and all other Foldr apps:

https://foldr.yourdomain.com

iOS & Android app:

Foldr mobile apps are available in the App Store and Google Play

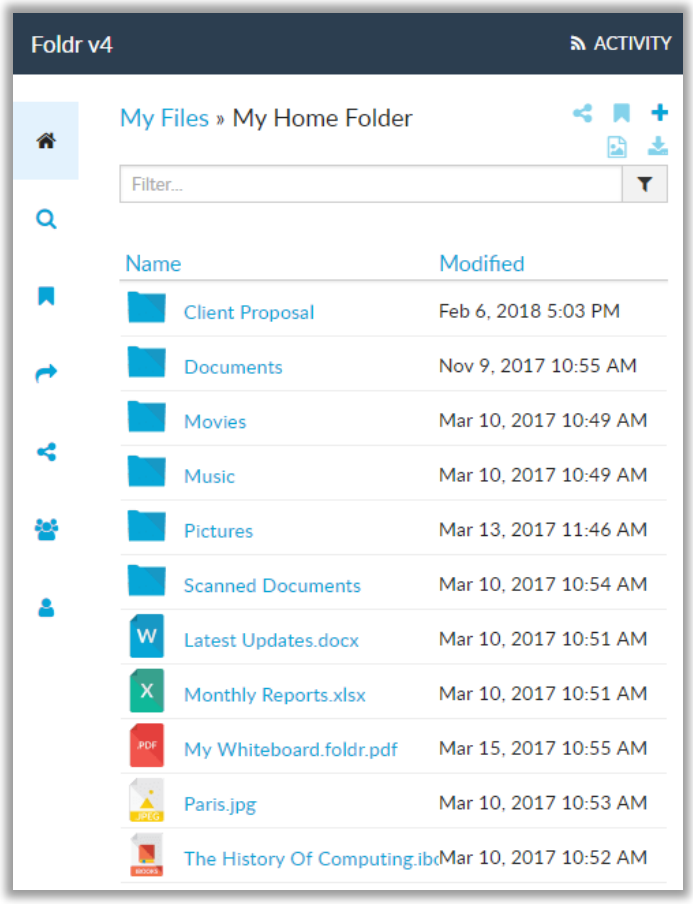
Desktop apps

Windows app is available here – macOS here

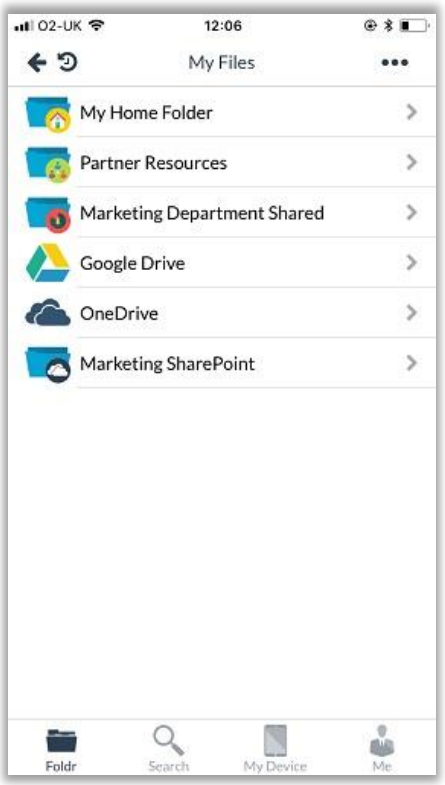
WebDAV clients

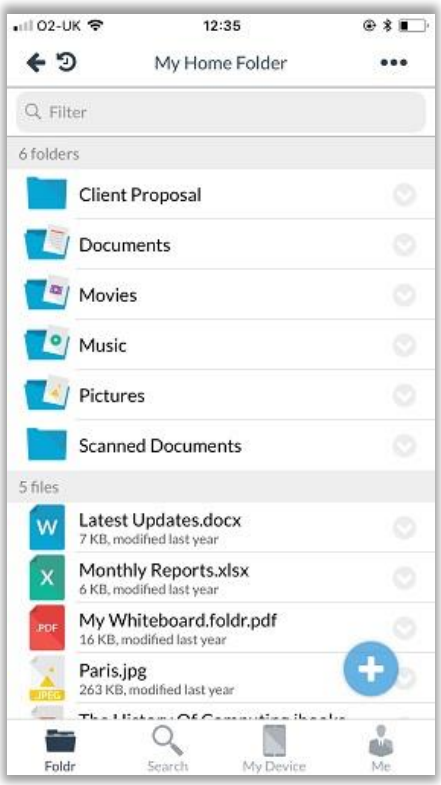
https://foldr.yourdomain.com/drive (note /drive)

Web app:

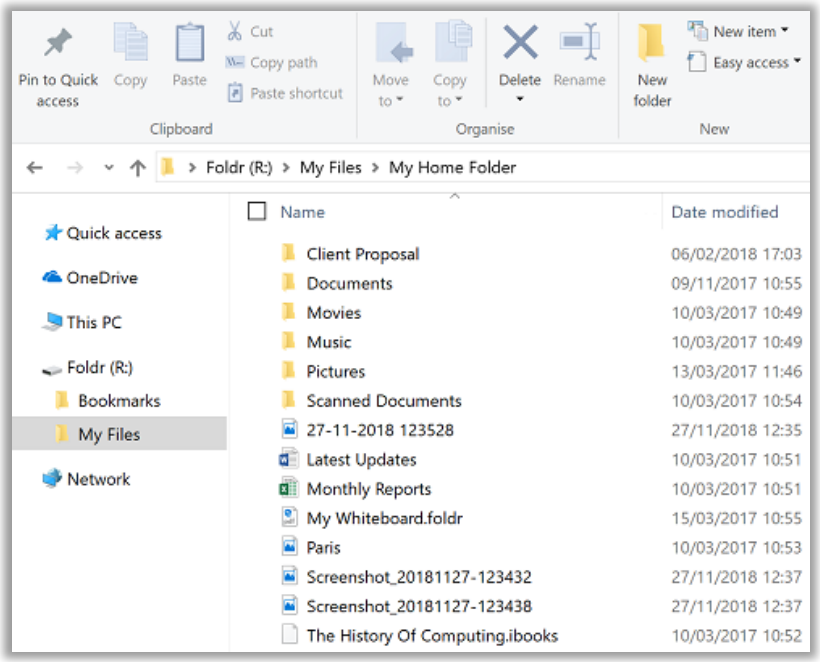


Mobile app (iPhone shown):



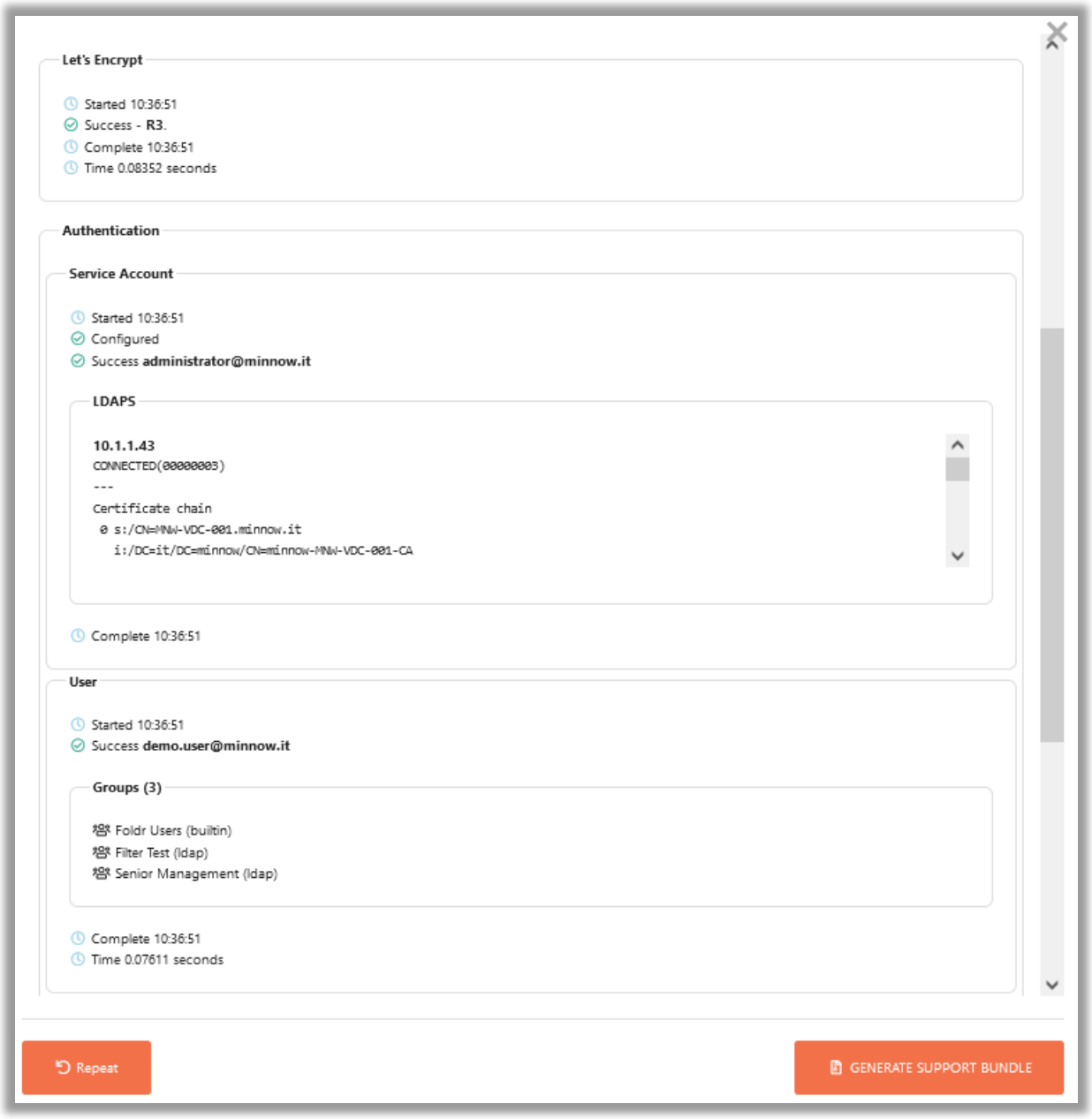


Desktop app (Windows shown)



12. Troubleshooting

If users are unable to authenticate or SMB shares / home folders aren't accessible once signed in it is recommended to run the **Test Settings** feature in Foldr Settings > top-right menu > Test Settings. This can highlight problems with the configuration, user and service accounts, incorrectly set system hostname / DNS and SMB connectivity.



Various console commands are available on the appliance console to assist with troubleshooting connectivity including as ping, nslookup, dig, ldapsearch and smbclient.

Additional support resources are available on the online KB – Should you still require additional support, generate a support ticket at support@foldr.io

More information on the many other powerful features that are available in Foldr can be found in the full administration guide or online KB

Other features include:

Password Control - (Not available with AAD) Password change, delegated and self-service reset
Search / Indexing –Provide fast file search results to users for both on-premise and cloud storage from a locally hosted index or cloud APIs
Granular Controls - Storage permissions, visibility and location based policies
Multi-factor authentication & WebAuthn – Protect access to your sensitive data / web services with through 2FA or physical security keys and biometrics.
File Sharing – Secure file sharing between internal users (project work submission folders, collaboration) and external users (public links, password protected links and secure links with email notifications)
Cloud integrations - Office 365, Google Workplace, Dropbox, AWS/S3 and Box
Single Sign-On – Use Foldr as a SAML v2 IdP or service provider against AD FS or other third party IdP.