Installation and Administration Guide v6

Contents

What is Foldr?

Foldr provides a secure gateway between your existing network shares, cloud storage and your connected devices.

The solution has been designed to be lightweight, quick to deploy and easy to administer. Users will be able to access network resources quickly, securely and from virtually any device using an HTML5 web app, Windows & macOS drive mapping applications and native mobile Android and iOS apps. Foldr provides features to allow users able to access, edit and securely share files and folders with users inside and outside of the organisation. Additional features include password control/reset, device approval, MFA and WebAuthn authentication, single sign-on, search, automation and more.

Virtual Appliance

The Foldr appliance is delivered as a pre-configured, performance optimised and ready-to-run virtual machine which has all required software dependencies already installed. The virtual appliance is quick to deploy and can be run on most popular virtualisation platforms such as VMware, Microsoft Hyper-V, Nutanix AHV, Citrix XenServer, Parallels and VirtualBox.

Physical Server / Bare metal Support

The Foldr appliance may also be installed directly on dedicated hardware by imaging the provided disk image onto HDD/SSD. We do not maintain a list of supported hardware due to the varying nature of drivers / chipsets used across vendors, however the small form-factor Intel NUC branded devices work well for smaller environments.

Security

Foldr uses HTTPS exclusively for all user interaction with the server. The Foldr appliance has been designed with security in mind and at the time of writing scores an A+ grade on the widely recognised Qualys SSL labs server test. The server can conform to PCI, HIPPA and NIST SSL requirements and the appliance is updated regularly in terms of both product and operating system security updates. These may be delivered automatically or manually requested over the Internet. Alternatively, updates may be installed using an ISO file provided by support.

The solution does not synchronise or retain files within the appliance itself or send traffic via any cloud service that is not under your control. Foldr is a point-to-point solution between your user's devices, the self-hosted server, and your storage infrastructure. Foldr has been designed to make the most of what you already have in place; users authenticate with their existing credentials and all existing security permission structures and ACLs are automatically respected with no additional configuration. All user activity is logged within a local configuration database up to a maximum of two years and the logs are searchable by user / date and are exportable.

Foldr provides various security features to help ensure your data is secured against unauthorised access such as device approval, built-in or third-party multi-factor authentication, WebAuthn support, PIN/Passcode and Touch ID support in the apps. Any sensitive information stored within the Foldr appliance is encrypted using robust and proven technologies. Corporate or personally owned mobile devices that are lost or stolen can be revoked quickly from the Foldr administrative web interface, blacklisting the device and thereby removing access to corporate resources. Web based user access may be also limited to approved devices.

Active Directory domain password policies are respected and Foldr provides support for expired passwords, password complexity and allows users to change their password from the web, desktop or mobile apps. Foldr enables an administrator to permit delegated (trusted) users to reset others passwords in the organisation and finally offers self-service Active Directory password reset in the event of a user forgetting their network password.

Foldr v4 introduces separate appliances modes for backend infrastructure (database), client access and search roles where appliances responsible for hosting the system configuration may be held upon a central non-internet facing system inside your security perimeter and satellite client access VMs can be presented to users from the DMZ. Backend infrastructure appliances can be clustered for scalability and resilience and in larger deployments client access appliances can be placed behind a load balancer if required.

Benefits

Foldr gives IT administrators a drop-in solution that can be up and running quickly, provisioning access to personal home folders or any other SMB network shares from corporate or personally owned devices. Foldr can also present Google Drive, One Drive, SharePoint, Dropbox, Amazon S3 and Box cloud storage alongside traditional on-premise SMB file server or WebDAV shares. Shared cloud accounts may be presented to multiple users simultaneously from Google Drive, Dropbox or Box as well as traditional network shares.

Office documents can be edited seamlessly in a locally installed MS Office application or edited in browser-based Office Online or Google Apps (Docs, Sheets or Slides), regardless of the file's location. Files are saved back to the originating network and, in the case of Google Apps, converted back to Office format so users may continue working on files in their native application.

On-premise or cloud-based resources can be bookmarked for quick and easy access from web and mobile platforms.

Users can now access resources that were otherwise difficult to access without resorting to using VPNs or unintuitive mobile apps. Chromebooks, Android, macOS and iOS devices can now be easily integrated into the existing Active Directory based infrastructure whilst retaining control. Users can access Foldr via web, mobile apps for iOS / Android and finally through drive mapping applications for Windows and macOS.

Files can be shared easily with others inside and outside of the organisation in a secure manner. Project folders and work hand-in areas can be easily created on your existing storage allowing users to collaborate or submit files back to others. The sharing options extend to those provide access to resources securely for others external to the organisation. The public/external sharing features can be useful for sharing content that is either too sensitive or simply too big to email. Foldr is also able to process email and receive files that are attached to messages and route these to the appropriate shared folder.

Foldr provides password management, two-factor authentication and a powerful unified search feature that can search on-premises and cloud storage to find documents quickly, no matter where they are stored. Foldr expands upon its search features with custom fields, OCR and an optional Captur module to provide contextual metadata and allow you to extract, classify, process and search data from your documents, where ever they are stored. Foldr also provides an optional scripting and module to automate business tasks.

Foldr also includes a powerful Single Sign-On (SSO) solution. Supporting the industry standard SAML v2 standard, Foldr can act as an Identity Provider to web services such as Office 365, Google G-Suite and many others. This provides a convenient way for users to sign into external services using their familiar Active Directory credentials – either through automatic redirection back to Foldr to authenticate the session or via a dashboard of compatible web services. Should the organisation already use another IdP such as Active Directory Federated Services, Foldr can run in Service Provider mode to allow integration with the existing IdP. Foldr also provides an optional Kerberos SSO feature for web, Windows and macOS apps.

Finally, your data remains on your servers, freeing organisations of the data protection and security issues that can be obstacles to adopting cloud solutions.

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/macOS hosted SMB shares.

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

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

Deploy in the cloud in Amazon AWS EC2, Azure Cloud, Digital Ocean and others.

Virtual appliance *minimum* system 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)

Larger deployments with over 50 concurrent users should consider upgrading the appliance as required (4 vCPU and 8GB RAM is typically recommended but depends on usage)

Optional Search appliance *minimum* system 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)

Suitable hardware to run the chosen virtualisation platform.

1. Importing the Virtual Appliance

VMware ESXi

Download the VMware appliance '**Foldr-latest.ova'** and save it locally. Contact *support@foldr.io* or your reseller for more information on how to obtain the latest OVA.

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 disk size should be increased. Right click on the VM and select Edit Settings. Increase the disk size 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 on the console login screen 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 the minimum processor 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.

IMPORTANT – Before powering on the virtual machine, edit the Foldr server settings by right clicking on the VM > Settings. Under **Security > Secure Boot > Template**, change the selected template from Windows to **Microsoft UEFI Certificate Authority**. Failure to make this change will result in the VM being unable to boot. Click OK to confirm changes.

Start the virtual machine 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.

Other Hypervisors

Citrix XenServer

Download **Foldr-latest-XS.ova** 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 on the console login screen 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.

VMware Fusion

VMware Fusion uses the same OVA file as used for ESXi. To import the Foldr appliance select the OVA from:

FILE > IMPORT > Choose File

You will then be prompted where to save the VM and the import process will begin. Note – it is recommended that you do not attempt to move the location of the Foldr VM directory and the files contained within it once you have started the VM.

Once the OVA has been imported, the disk size should be increased. In the VM settings in VMware Fusion, 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 on the console login screen 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.

It is recommended that you add the VMware Fusion bundle associated with the Foldr appliance to the OS X 'Startup Items' so it will power up automatically when the OS X user is signed in. This can be achieved by:
Apple Logo > System Preferences > Users & Groups > Login Items > '+' button > Browse to /Users/Username/Documents/Virtual Machines/Foldr-VM-Bundle.

Oracle VirtualBox

Download the latest **Foldr-latest.ova** and open the VirtualBox console. Click File > Import Virtual Appliance > Open Appliance and browse to the OVA file. Review the default settings, these are ideal for most installations and if necessary modify the path where the Virtual Machine files will be stored. Agree to the licence terms by clicking the Accept button. The OVA is imported and the Foldr virtual machine will be created.

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 on the console login screen 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.

Parallels Desktop

Download the latest **Foldr-latest-PD.zip** - Extract the zip file and move the two files contained within to a suitable location on the OS X computer. Launch the Parallels Desktop application and select the Import Existing Virtual Machines button or File > Open. Browse to and select the Foldr.vmx file and the appliance will be converted and imported into Parallels .pvm format. Once this has completed the appliance will be accessible from the Virtual Machines Directory.

Ignore the warning regarding Parallels being unable to determine OS type and continue.

Once the VMX 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 on the console login screen 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.

IMPORTANT – In older versions of Parallels Desktop (v13 and earlier) you should change the default network adapter type within Parallels before Foldr will be able to connect to the network.

Click on the settings cog for the Foldr v4 appliance > Network > Advanced > Select **Intel PRO ® 1000MT**

To make a Parallels virtual machine to start automatically, follow the instructions shown here (http://kb.parallels.com/en/114824).

Nutanix AHV

Download the latest **Foldr-latest-AHV.zip** - Extract the zip file which contains a single VMDK file. Log into the Nutanix Prism web interface and select the settings cog icon > Image Configuration. Using the **+ Upload Image** button give the Image a suitable name, selecting **DISK** as the Image Type and finally select **Upload a file / Choose File** under Image Source.

Allow the image to upload. Once uploaded the image is then automatically 'processed' for several minutes and you will not be able to use the image until this operation has completed. Check the recent tasks icon to see the progress of these operations

Now that the vmdk Image has been uploaded and processed, the virtual machine can be created. In the VM view, click **+ Create VM** (top right). Give the VM a suitable name and assign a minimum of 2 vCPU and 4GB RAM.

Scroll down and click **+ Add Disk** - From the Add Disk dialog > Operation section, select **Clone from Image Service** ensuring you have the correct Image selected and finally click ADD. Add at least one network connection to the VM by clicking the **Add New NIC** button. Click **Save.**

In the Prism VM view and click **Manage Guest Tools.** Enable and Mount Nutanix Guest Tools and Click Submit.

Increasing the disk size
Once imported, and before powering the VM on, the VM disk must be increased in size in Nutanix from 10GB to 100GB. Once this has been done, 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 on the console login screen 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..

To install the Nutanix Guest Tools, sign into the Foldr console, either directly through the Prism interface or by an SSH client such as PuTTY (SSH port 2082) - log in using default admin account:

fadmin / password

Issue the following command to begin the installation:

```
install-nutanix-guest-tools
```

Once the tools have finished installing, you should be placed back at the shell prompt. Reboot the VM using either the power options in the Prism interface or the 'reboot' command on the console.

Microsoft Azure

To deploy the Foldr appliance in the Microsoft Azure cloud service firstly download the latest Hyper-V appliance(Foldr-latest-HV.zip and save it locally. Extract the contents of the zip and move the VHD file to a suitable location.

Azure requires the virtual hard disk to be fixed in size rather than thin provisioned / dynamic. To do this run PowerShell as an Administrator and execute the conversion cmdlet:

Convert-VHD -Path <path-to-extracted-vhd> -DestinationPath <path-to-converted-vhd> -VHDType Fixed

Wait for the conversion to complete.

Create an Azure storage account if you do not already have one and upload the fixed VHD to a Blob Storage container in your storage account as a page blob. There are several ways to achieve this, but Azure Storage Explorer is probably the most convenient.

Next, create an Image from the VHD:

1. In the Azure portal, browse to *All Services > Images > Add*.

2. Provide a name, subscription and resource group and then select Linux as the OS Disk.

3. Browse to the VHD that was previously uploaded to Blob Storage.

4. Click Create

Next, create the Foldr VM from the Image.

1. In the Azure portal, go to *All Services > Virtual Machines > Create a virtual machine*.

2. Provide a name, subscription and resource group etc, then select Browse all images and disks > My Items and select the image created earlier.

3. Configure the VM size to meet your requirements.

4. Enter a username and password. These credentials will be ignored but are required fields.

5. Permit the recommended inbound ports (80, 443).

6. If other configuration is required then perform it, otherwise click Review + create to deploy.

7. Wait for the deployment to complete.

Add the remaining inbound ports on Networking (30537, 2082). Power on when complete and then refer to section 2 to configure the appliance in Foldr Settings.

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

Headless Setup (Microsoft Azure or Amazon Cloud)

Foldr can be installed and configured on a cloud platform that does not provide traditional console access to the virtual machine.

The steps involved are:

1. Deploy the Foldr virtual machine using the steps required for the chosen platform and power the VM on. Azure specific deployment instructions are available below.

As part of the VM deployment you may need to specify what network ports are required. The following ports are recommended:

TCP 80 (HTTP)
TCP 443 (HTTPS)
TCP 30537 (SSL- Foldr Settings)

TCP 2082 (custom SSH port)

2. Power on the VM and after several minutes, it should be accessible using the IP address acquired via DHCP.

3. Log into the appliance Foldr Settings web admin UI the default fadmin credentials:

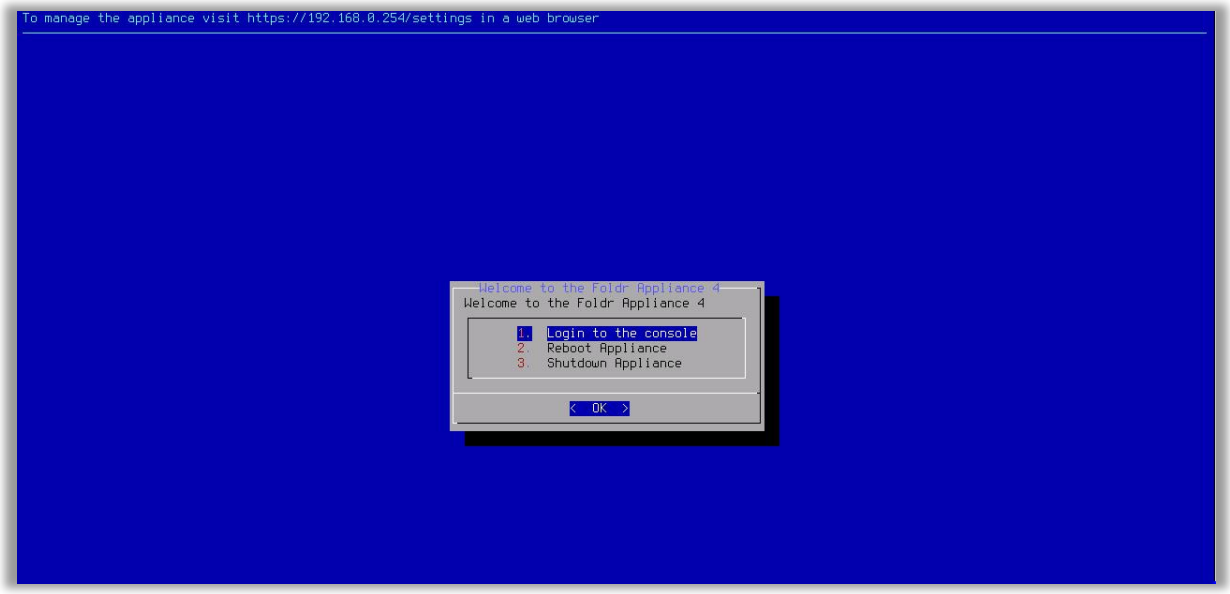
Username: fadmin

Password: password

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:

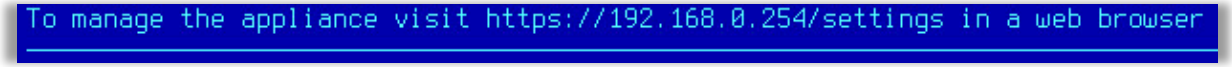
https://address-of-foldr:30537/settings. Only administrative users can sign into the Foldr Settings portal.

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 either 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.

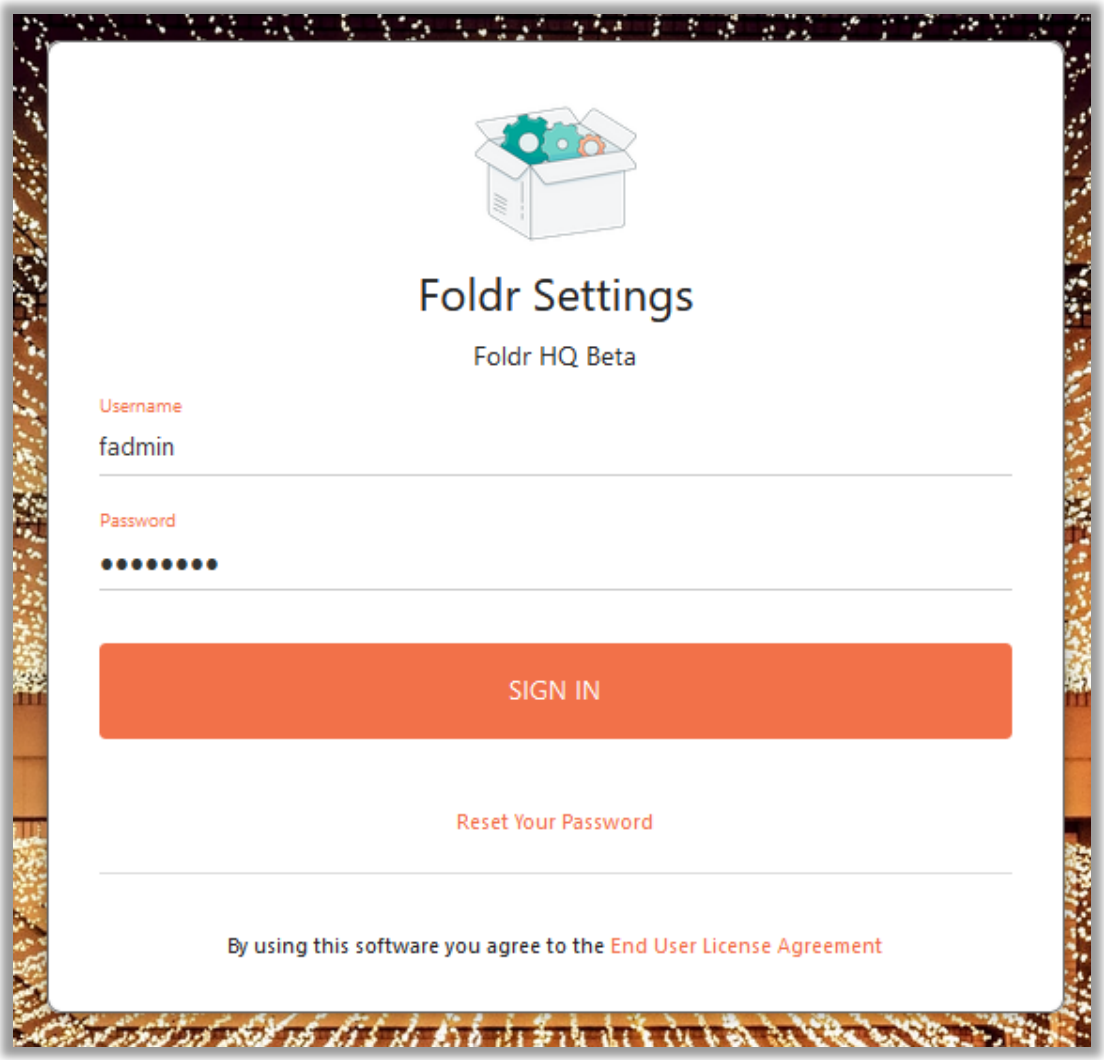
Default admin credentials

USERNAME: fadmin

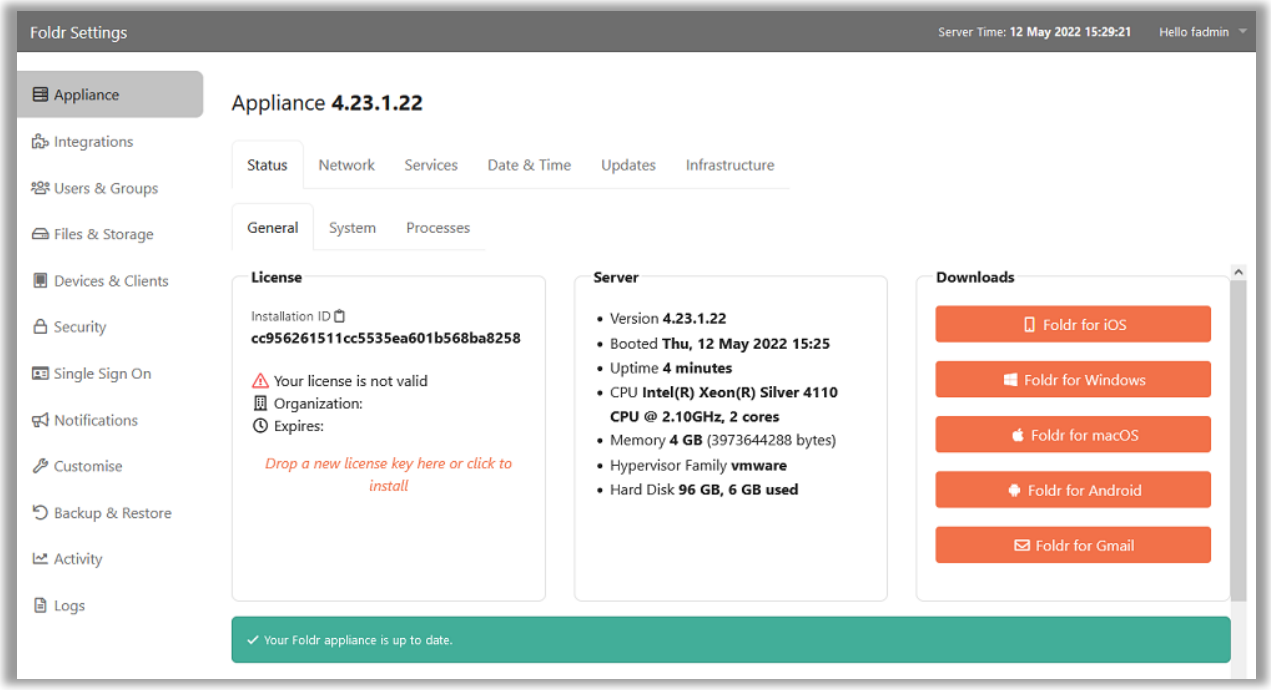
PASSWORD: password

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***)

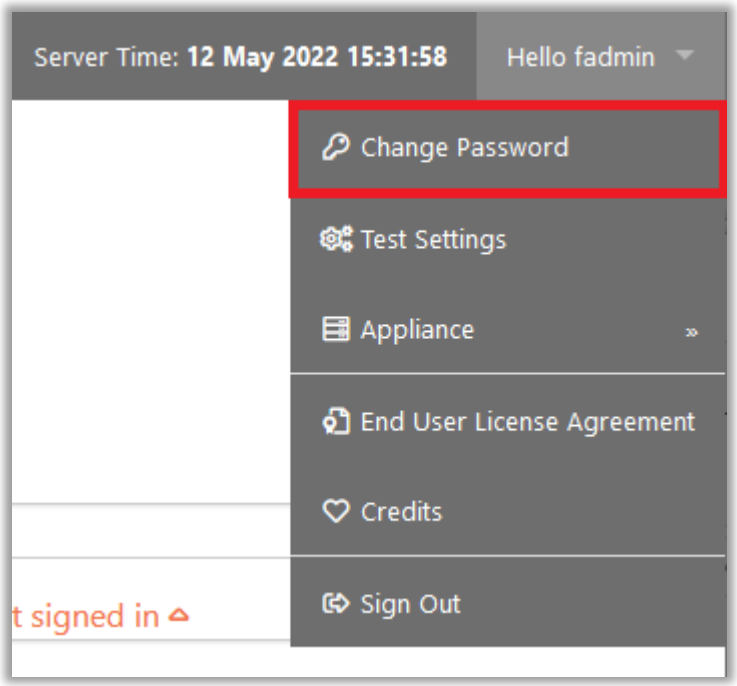
NOTE - If you browse to the local IP address of Foldr and append /settings the browser is redirected automatically to **port 30537**. *Please note that the Foldr Settings configuration portal will not be available externally if you have not opened / forwarded TCP 30537, however it is best practice to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



Foldr Settings web UI:

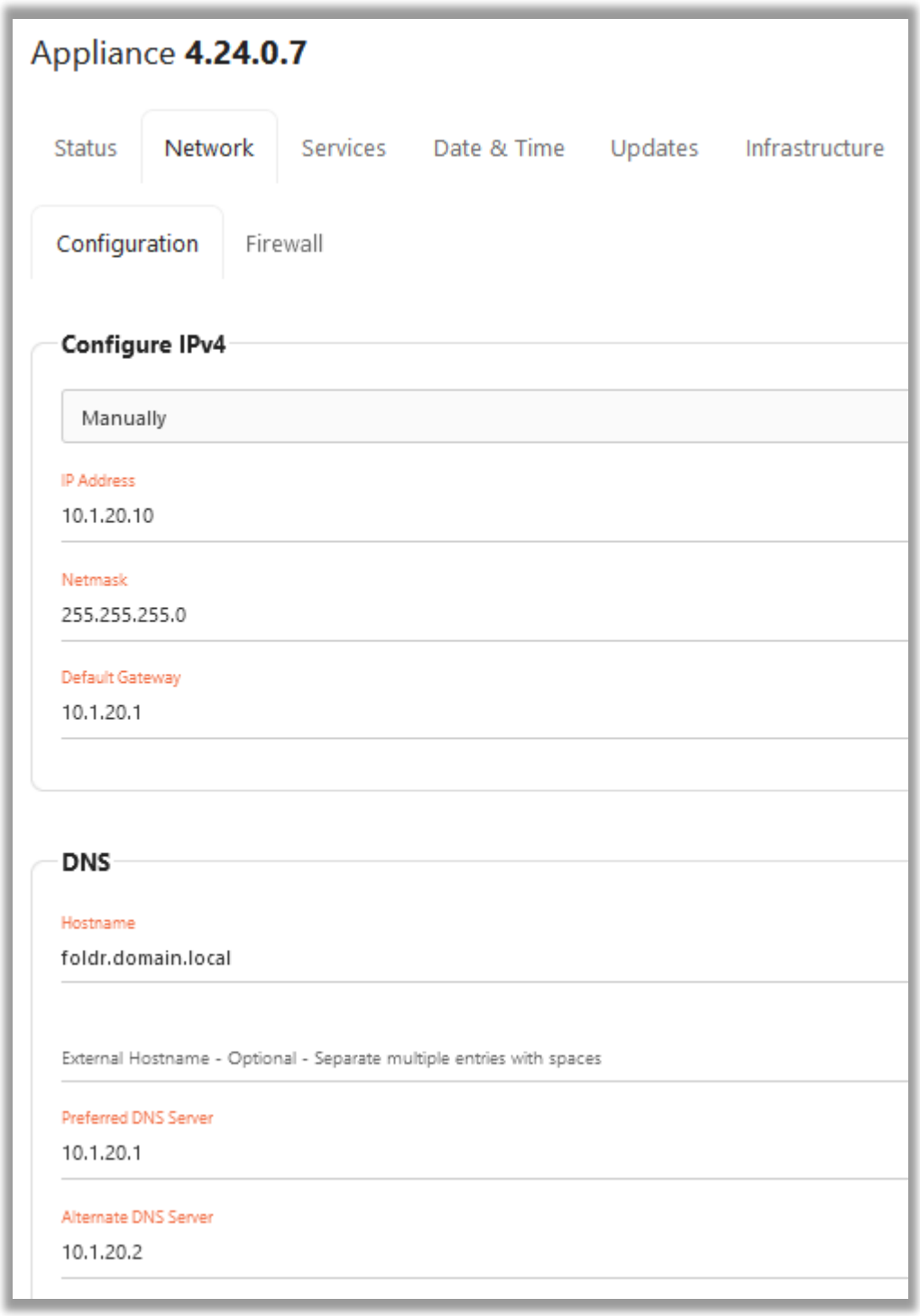


It is recommended that you now change the fadmin account password using the ***top-right menu > Change Password***



Network Configuration

All aspects of the server's network configuration can be configured in Foldr Settings, in the ***Appliance > Network tab***.



Configure network settings that are applicable to your network. IP address, subnet mask, default gateway, preferred and secondary DNS servers.

When this has been completed and the settings saved, enter **a suitable hostname using a fully qualified name relevant to the internal Active Directory domain. i.e. foldr.yourdomain.internal**

It is important that all network settings, including the hostname and the system time/date/zone are configured correctly before attempting to proceed further with the installation. The system hostname should be statically configured or set using a Pointer (PTR) record in the reverse lookup zone on your

internal DNS system, should you wish to use DHCP. A static IP configuration is always recommended.

IMPORTANT – If the Search Domain is not configured, a correctly configured fully qualified hostname on the appliance is vital for a successful Foldr installation as the hostname suffix is automatically used as the search domain for internal unqualified DNS queries. This assists with resolving short/unqualified paths for shares, home folders and so on.

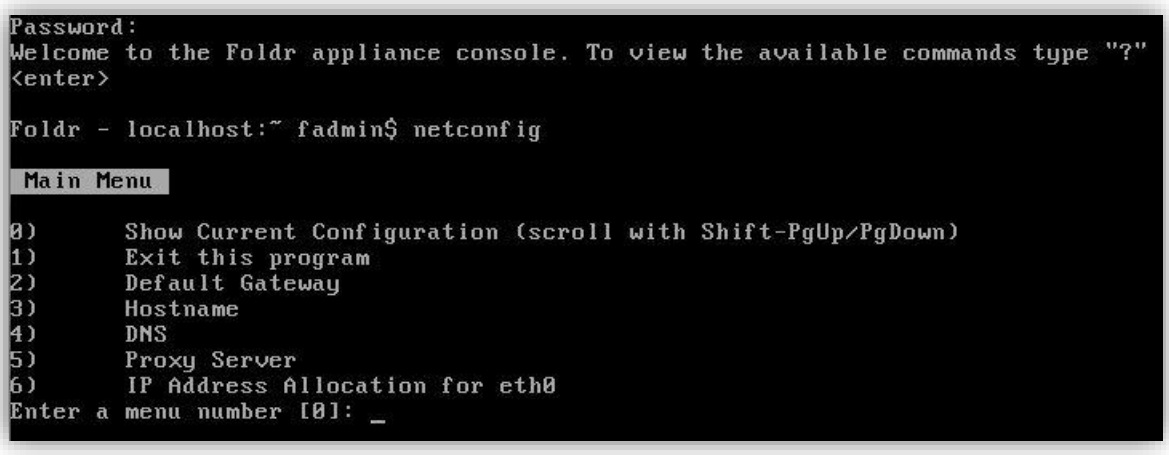
External Hostname

If your users will be connecting to Foldr using a different URL to the internal hostname, you should configure this here. The external hostname is typically configured to the Foldr server's public address/URI. Once configured Foldr will reject any connections made to the server that use a hostname that it different from the internal or external hostname (or IP address) and it is also important to configure the external hostname correctly as it is used with generated links inside email notifications when sharing files/folder. Some legacy third-party WebDAV clients that may warn of compatibility issues without an external hostname being configured.

NOTE 1 - If the IP address of the Foldr appliance is modified, it is applied immediately when clicking 'Save', please adjust the URL in your browser to reflect changes to the IP configuration and log back in.

NOTE 2 – The default appliance time zone is UTC, adjust to local time zone as required within ***Appliance > Date & Time***.

NOTE 3 - You can also configure all network settings from the appliance console if required using the '**`netconfig`**' command which will present an easy-to-use menu.



Adding Additional Network Interfaces

The virtual appliance supports a maximum of 4 network interfaces and by default a single interface is available. In environments where additional NICs are required, in addition to adding the extra network interfaces at the hypervisor level (VMware, Hyper-V etc) y**ou must also add support for these NICs on the console before they can be configured**. All network configuration done via the web interface applies to eth0. To configure any other interfaces, you must use the `netconfig` menu on the appliance console.

To add a new interface, issue the following command after adding the new virtual hardware in your chosen platform. Please note that eth0 already exists after deployment so eth1 – eth3 are valid options:

Example – Add 3 additional interfaces to Foldr:

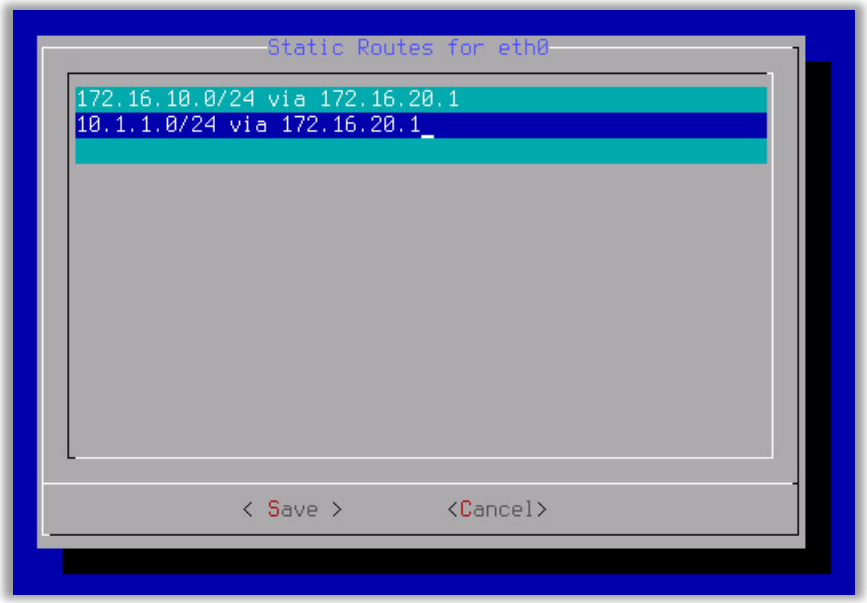
```
add-interface eth1
add-interface eth2
add-interface eth3
```

Static Routes

Static routes can be configured for the default network interface during initial setup; however, the administrator can modify or configure routes for any network interface from the appliance console using the `set-routes` command.

Example – again eth0-3 are valid providing the interfaces have been added correctly.

```
set-routes eth0
```



Use the tab key to switch between route configuration and Save / Cancel.

Modifying the built-in firewall

If you have added more network interfaces or in more complex network environments, such as one running a load balancer in front of multiple Foldr client access appliances, it may be necessary to modify the built-in firewall (IPTables). From the console, the fadmin account has access to add and remove firewall rules using standard **`iptables`** commands. More information on iptables and example commands are available here

For the rules to be persistent after applying software updates, they must be commented with **`-m comment --comment "foldr-admin"`** as shown below. Example command:

```
iptables -A INPUT -m comment --comment "foldr-admin" -i eth1 -p tcp --dport 443 -j ACCEPT
```

Once your rules have been configured, you must SAVE them, or they will be lost when the next system restarts. To commit your changes run the following command:

```
iptables-save
```

Appliance Time Settings

Accurate system time is important for any network device and is vital for Foldr's SSO and two-factor authentication features to function correctly. The Foldr appliance can obtain its system time from either the host it runs upon (VMware only) or use an external time source using NTP (Network Time Protocol). Time settings are configured from ***Foldr Settings > Appliance > Date & Time***.

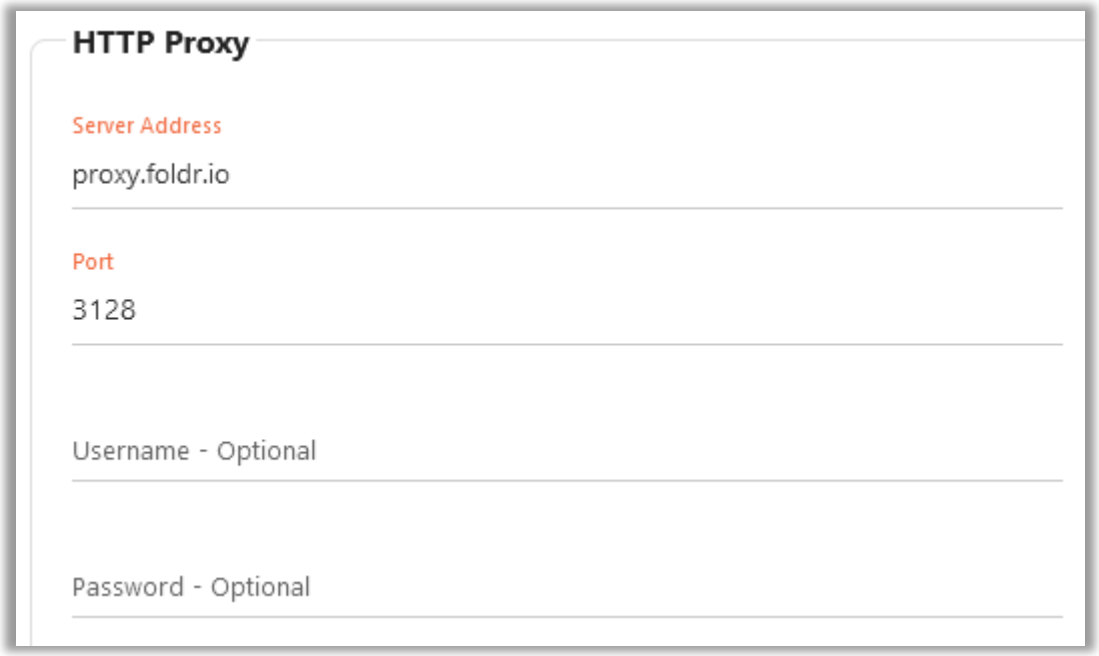
If NTP is selected as the time source, and the ntpd service is enabled/running, the appliance system time can be forced to sync with an NTP server using the following console command:

```
time-sync NTP-server-ip-address
```

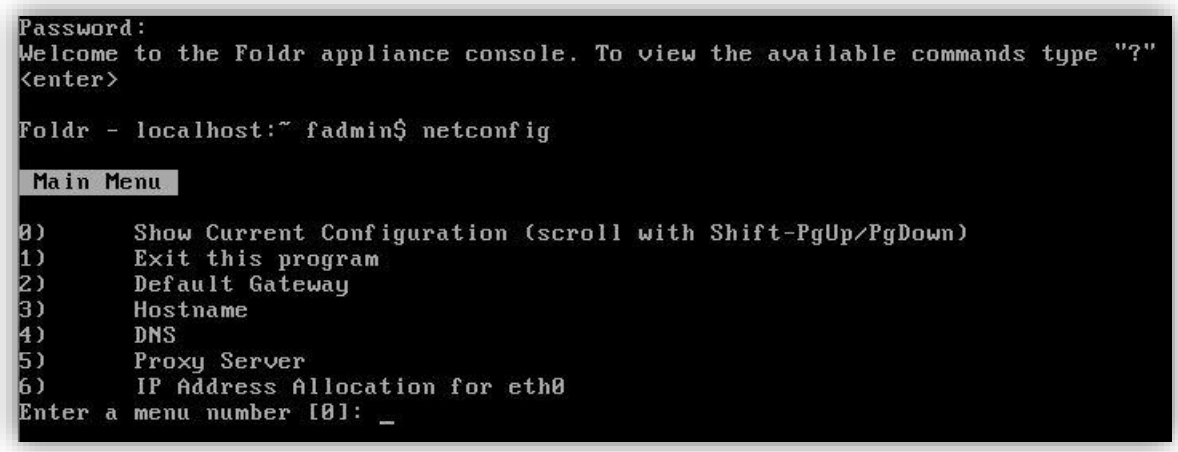
Dedicated KB article for configuring NTP and forcing a time sync can be found here.

Configuring a Proxy Server

If your network environment uses a proxy server to reach the Internet this can be configured within ***Foldr Settings > Appliance > Network > HTTP Proxy.***



Alternatively, the proxy can be configured from the **`netconfig`** menu on the appliance console (option 5)



If a proxy server is used, it must also be configured on the appliance for the Google and OneDrive integration features to work correctly. The software update mechanism also will attempt to connect to the default online update URL via the configured proxy server.

HTTPS inspection/filtering - proxies, web filters and firewalls

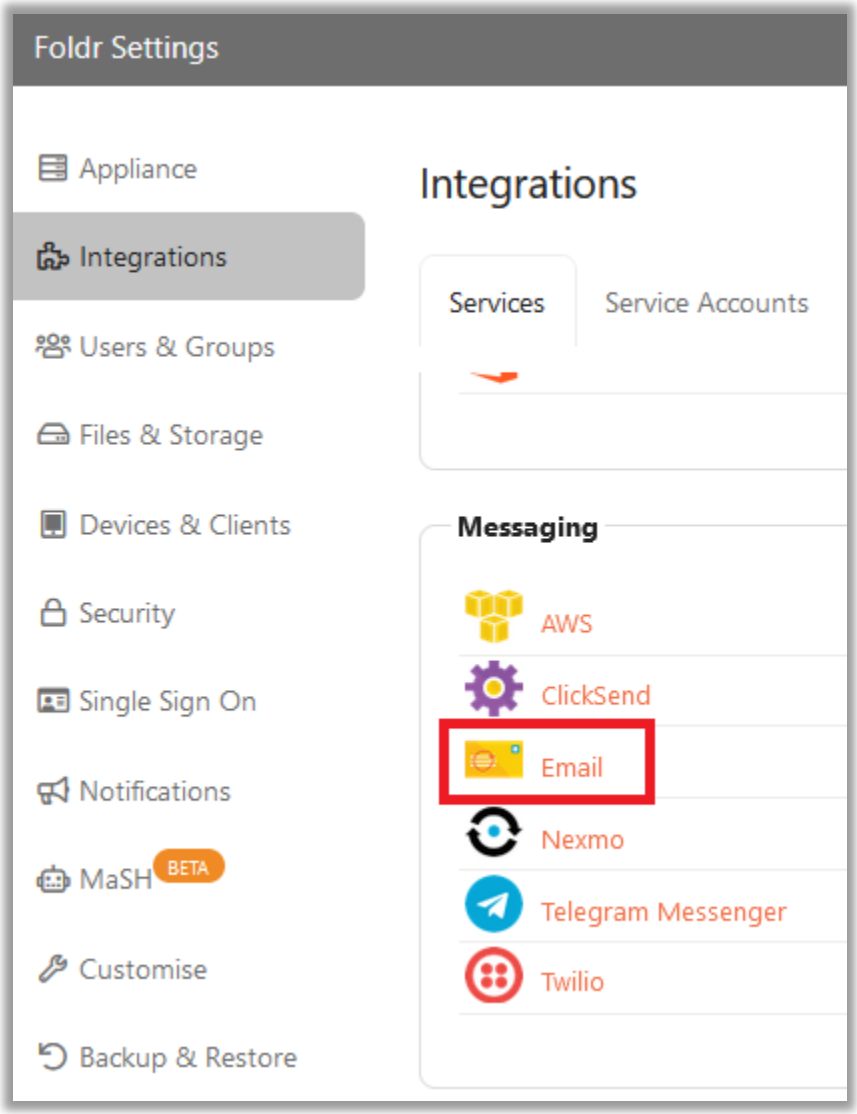
Any upstream HTTPS inspection web filtering service (MITM) will cause issues with the following features and as such the Foldr appliance should be whitelisted / excluded from SSL filtering.

Foldr server updates, **Let's Encrypt SSL certificate** installation and **Office 365 and Google Workspace** integrations may be affected if Foldr is running behind a security device that is using HTTPS

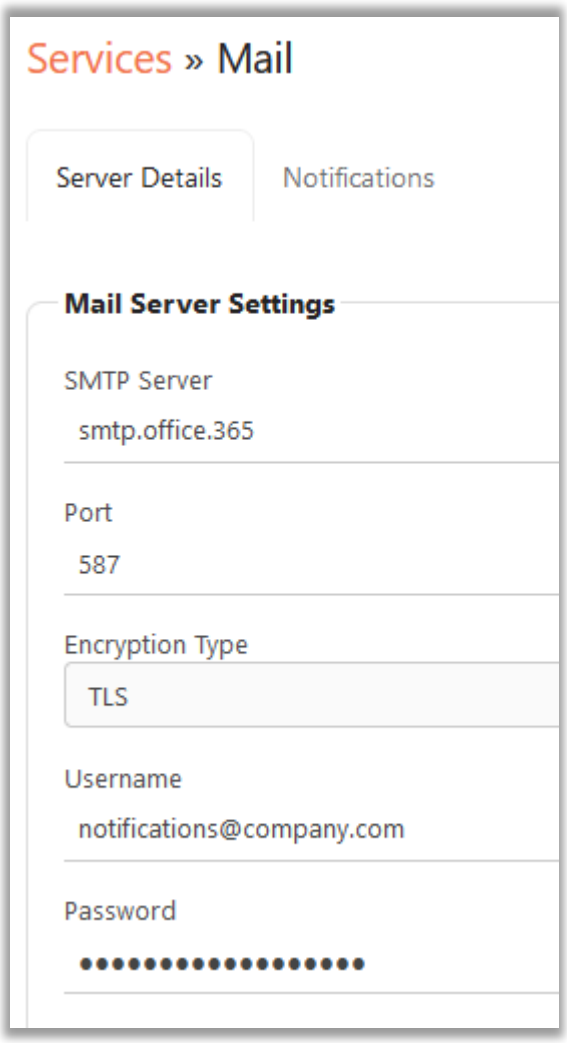
inspection.

Email Settings & Notifications

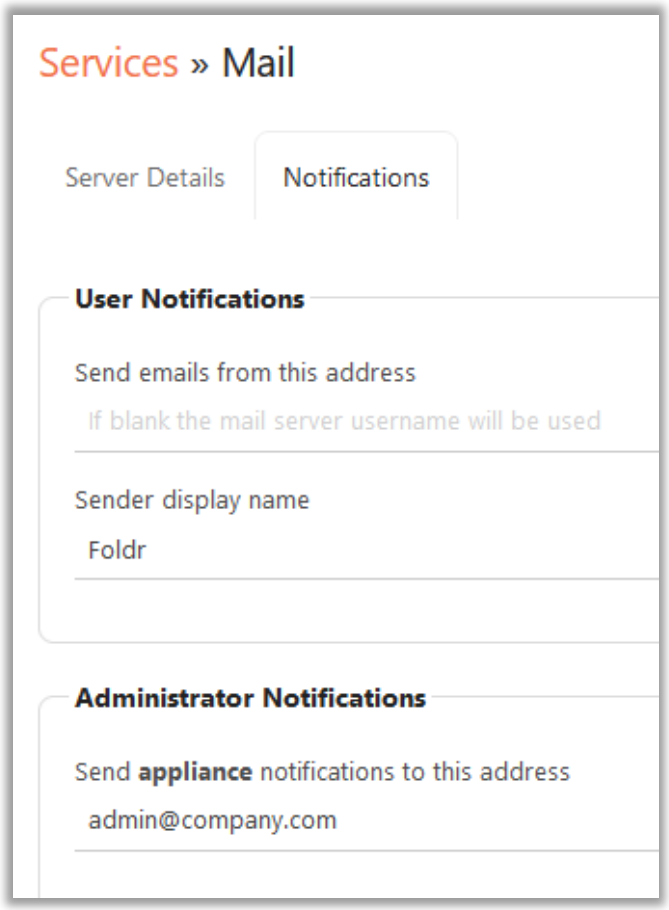
The Foldr appliance can alert the administrator to updates and provide users with notifications for the sharing and password reset features. Email settings should be configured within ***Foldr Settings > Integrations > Services > Messaging > Email*** as appropriate.



Example settings for Office 365 shown below:

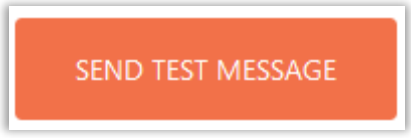


The ***Notifications*** tab should also be configured with the sender address and where system notifications should be sent to (typically monitored by the Foldr admin)

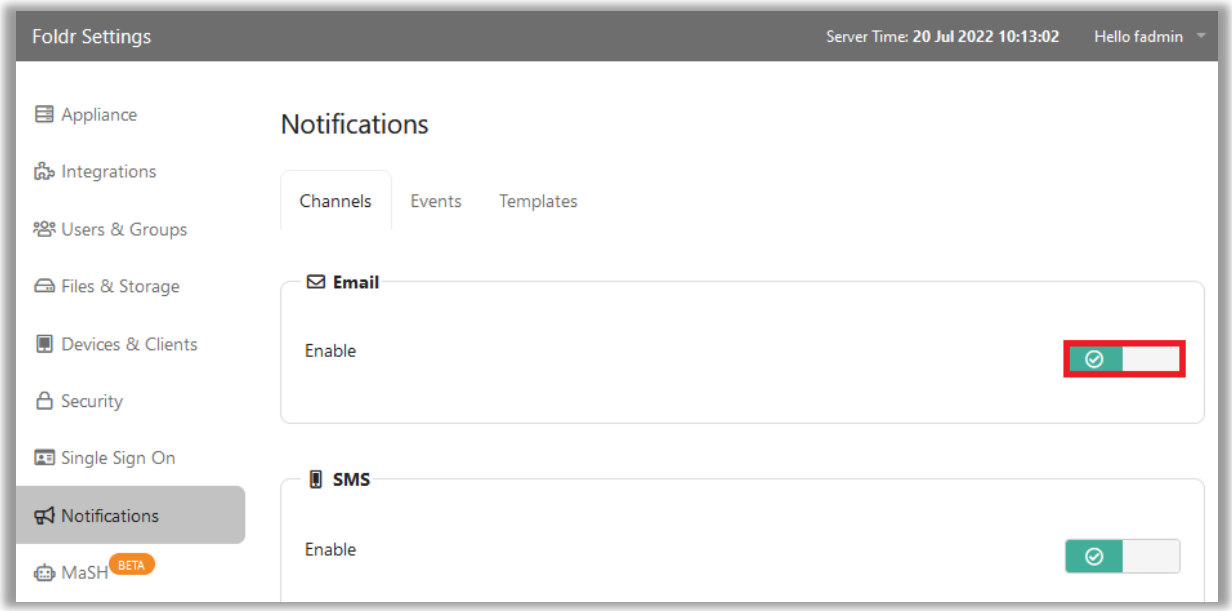


Click **SAVE CHANGES**

You can now attempt to send a test message from the ***Integrations > Mail > Server Details*** screen.



If the message is sent successfully, you should now enable Email Notifications from within the Notifications tab as shown below. This will allow sharing and other Foldr features (such as MaSH) to send email when necessary.



Click **SAVE CHANGES**

If email settings are configured, the Foldr server will automatically email to alert the administrator of the following:

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.

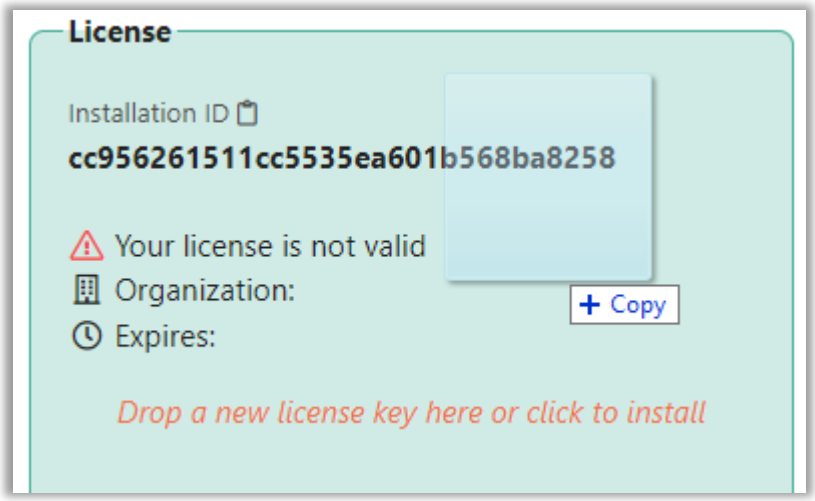
Users may also receive email notifications when items have been shared with them or files have been submitted to shared folders and as part of the Active Directory self-service password reset feature. These features are configured elsewhere and may be found in the administration guide or online KB.

3. Licencing the Server

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.

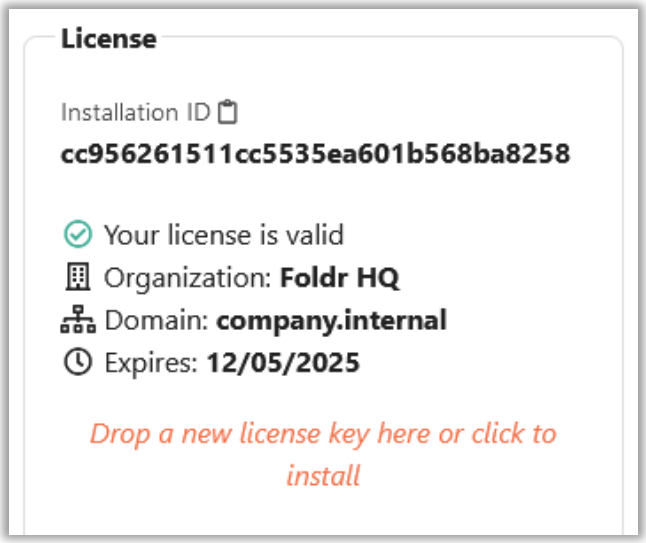


The End User Licence Agreement prompt will be displayed. Click **Yes, Accept** to agree to the terms of the EULA and apply the licence. To view the content of the EULA, click the text link in the prompt.

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**



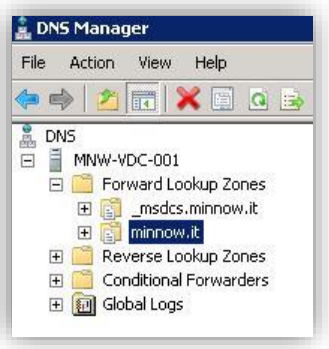
If you are configuring Foldr from a legacy Windows Server using Internet Explorer, you must disable IESC (Internet Explorer Enhanced Security Configuration) within Server Manager.

It is recommended that administration / configuration is done using a desktop machine using a modern web browser (such as Edge, Chrome or Firefox) rather than a server.

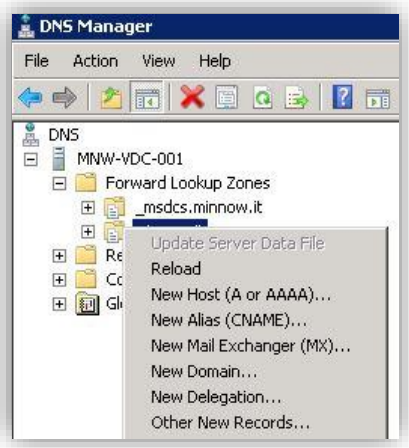
4. Creating an *internal* DNS host (A) record

Unlike a domain bound machine/server, Foldr does **not** automatically create an internal DNS host record, so this needs to be done manually. A correctly configured A record on the internal network lookup zone is important for SMB performance.

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.'



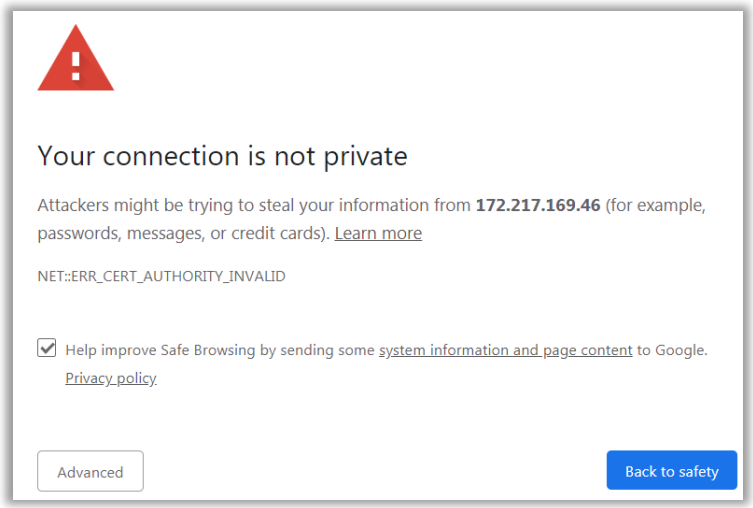
3. Assign a suitable hostname and point the record at the private/internal IP address of the Foldr Server.

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 (or foldr.minnow.it in the example above) from other devices on the network.

DNS & SSL certificate considerations

Foldr ships with a self-signed SSL certificate to ensure that all user and admin sessions are encrypted, however a downside to this is that client browsers (and the companion Foldr apps) would not consider the certificate 'trusted' as it is not provided from a known certificate authority. This will result in trust warnings such as the one shown below (Example showing Chrome browser)



As part of the setup process, the administrator should replace the default SSL certificate with a signed certificate from a trusted provider such as GoDaddy, Verisign or benefit from the built-in support in the Foldr server to obtain fully validated signed certificates from the **Let's Encrypt** service at no charge. Signed certificates can only be issued for a public domain URI/common name and as such users connecting to Foldr using the internal hostname or IP address will always receive certificate warnings.

Creating the internal DNS record above will ensure that the Foldr server runs optimally against on premise SMB file servers, however where the public domain differs from the internal domain, this is not optimal for the users accessing the Foldr service. As all user activity takes place over SSL/TLS, it is important to consider the SSL certificate that is installed on the server and as such it is desirable that that users do not receive SSL/TLS trust warnings in their browsers / Foldr apps. Typically, this would be achieved by ensuring users connect to the public (Internet) address of the Foldr appliance when accessing the service, but by default in most environments, this would involve the users request leaving the local network and coming back in from the public Internet.

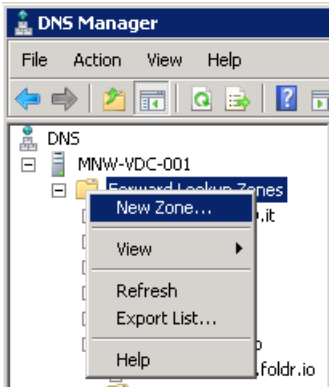
This is not an efficient use of bandwidth.

The solution is to configure the local DNS service so you can resolve the public address of Foldr to the private/internal IP address. This will allow the SSL to validate in the user's browser or app and keep their connection inside the local network.

The steps below assumes that Foldr will be made available using the example public address of https://foldr.public-domain.com – and that a suitable SSL certificate is going to be installed.

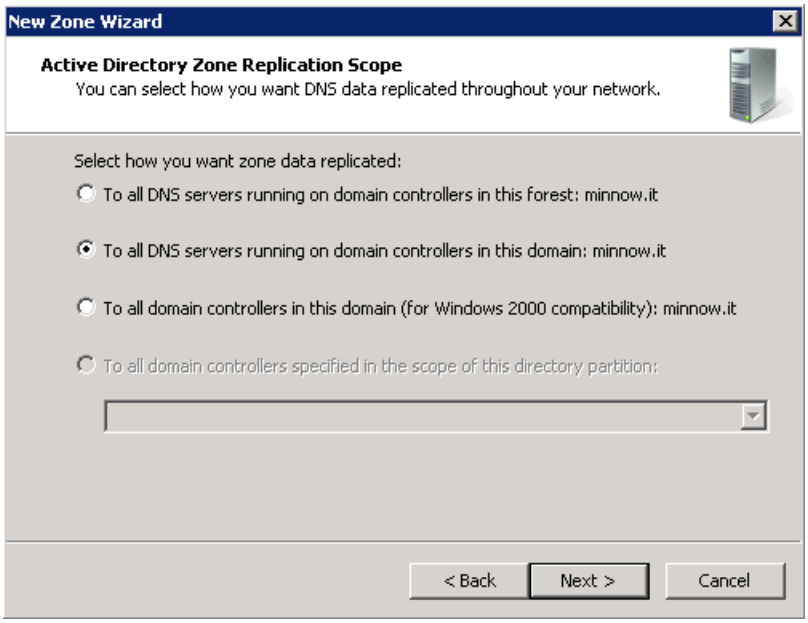
1. On a Windows Server that hosts the DNS Server role (usually a Domain Controller), click START > RUN > type dnsmgt.msc and click OK

2. Create a new Forward Lookup Zone

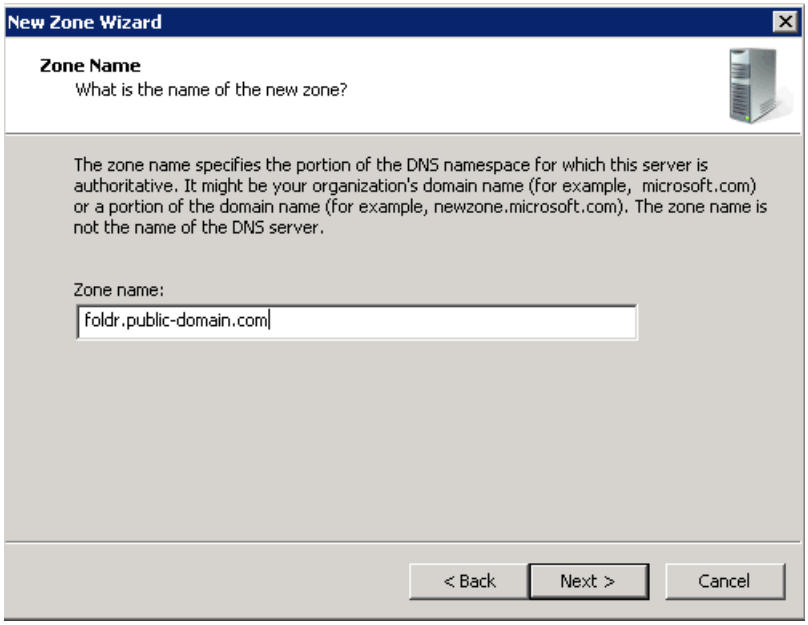


3. Proceed through the New Zone wizard

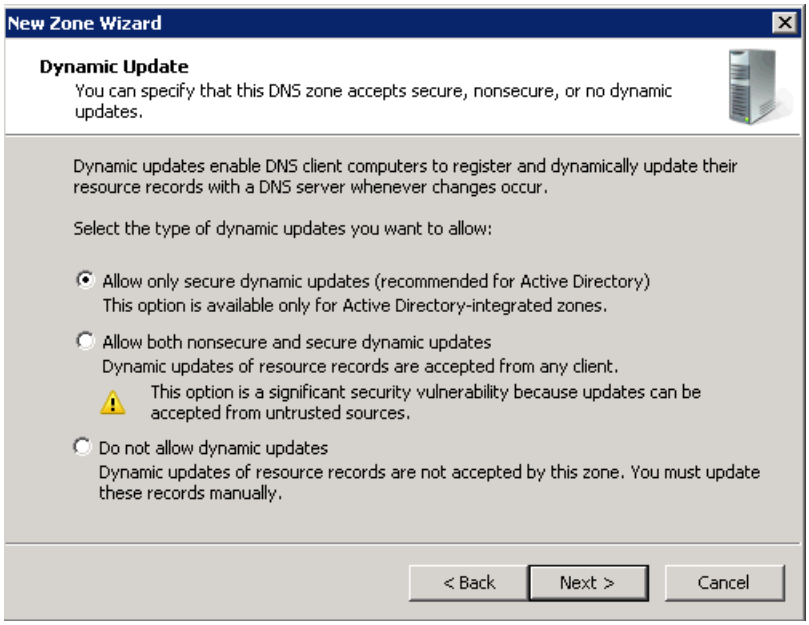
4. The default zone options are suitable in most cases, click Next.



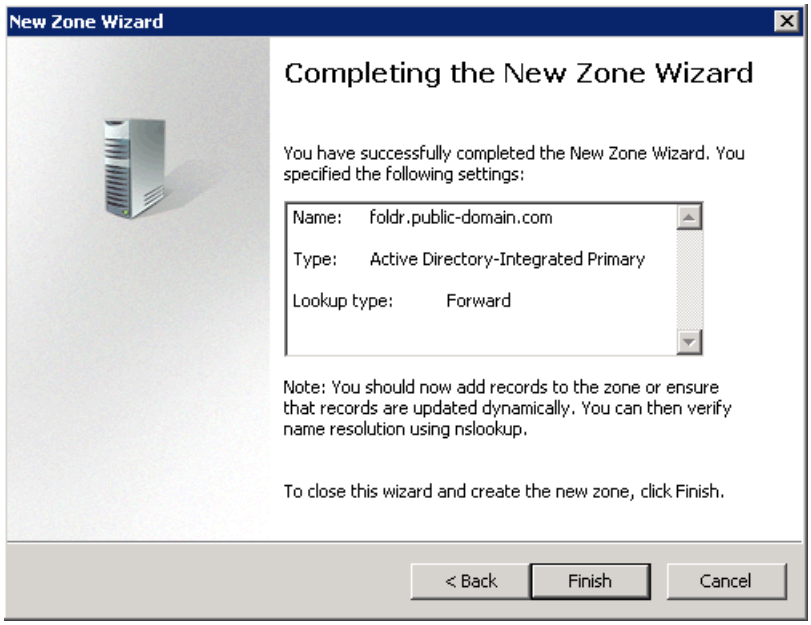
5. Name the zone with the public FQDN that users will access Foldr.



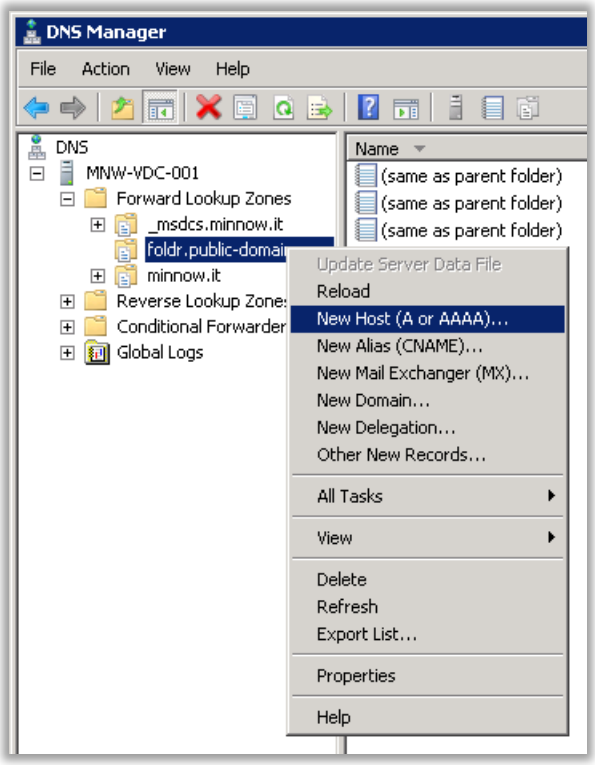
6. In most cases the default options can be used (as shown), click Next.



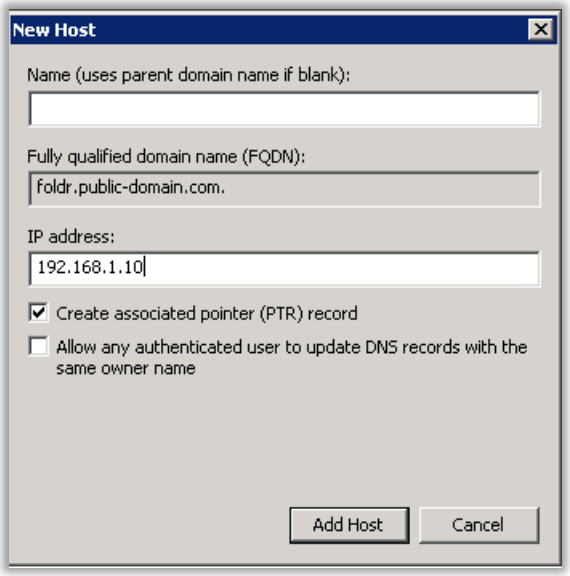
7. Click Finish.



8. Expand the newly created zone and create a new Host/A record using the context menu.



9. The host name should be left **BLANK** and the IP address pointing at the internal IP address of the Foldr server.



The steps are now complete. Users should now be able to connect to Foldr using the public address from inside the organisation network, it will resolve internally and be accessed across the local network and the SSL certificate will validate (providing a signed certificate has been installed).

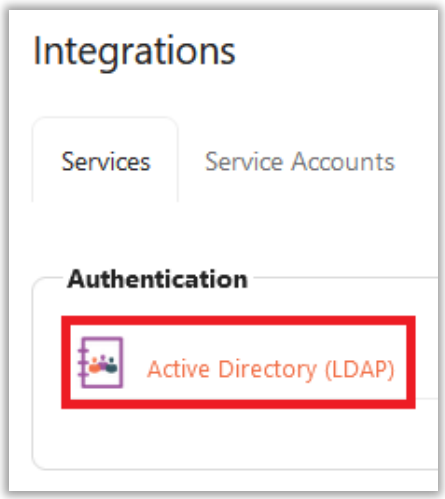
5. Authentication (LDAP)

Now that the system is licenced and the DNS record has been created, you can configure the authentication settings.

Active Directory

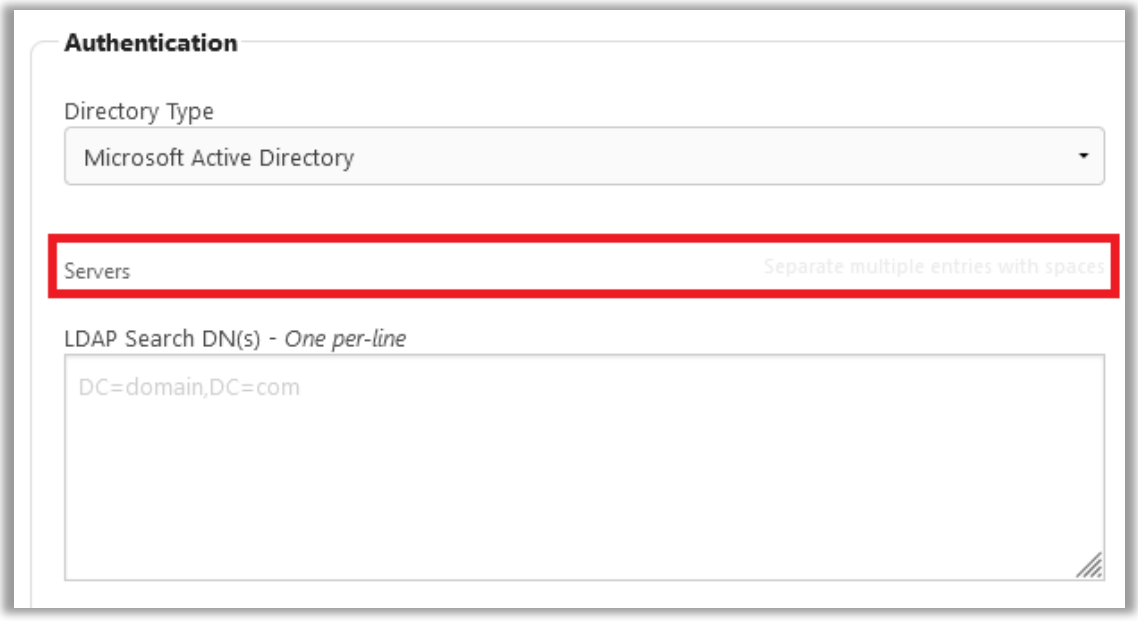
The server must be licenced with a suitable licence key before Active Directory authentication can be configured.

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

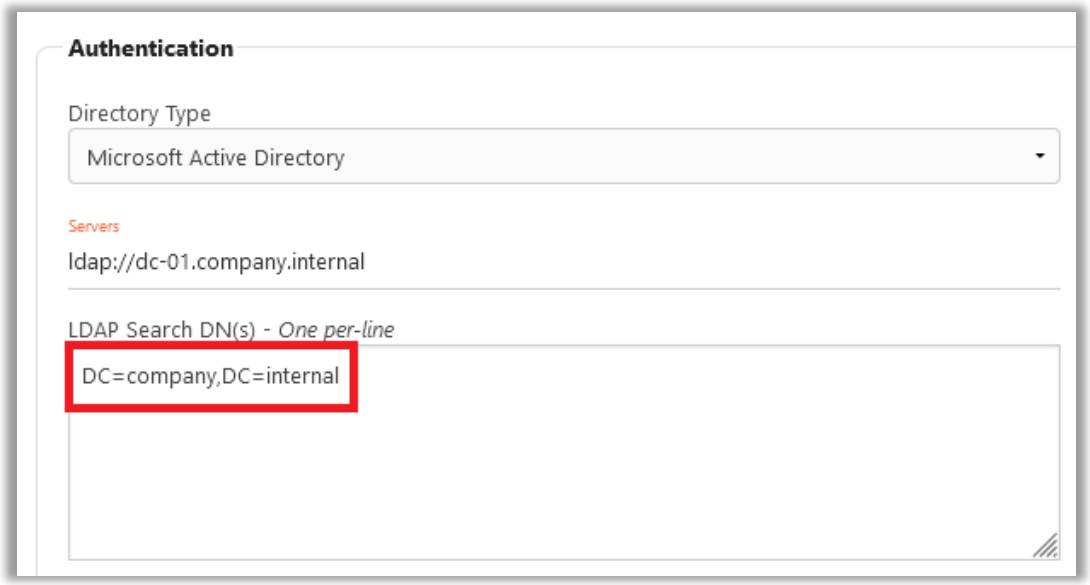
Note – ldap:// prefix)

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.



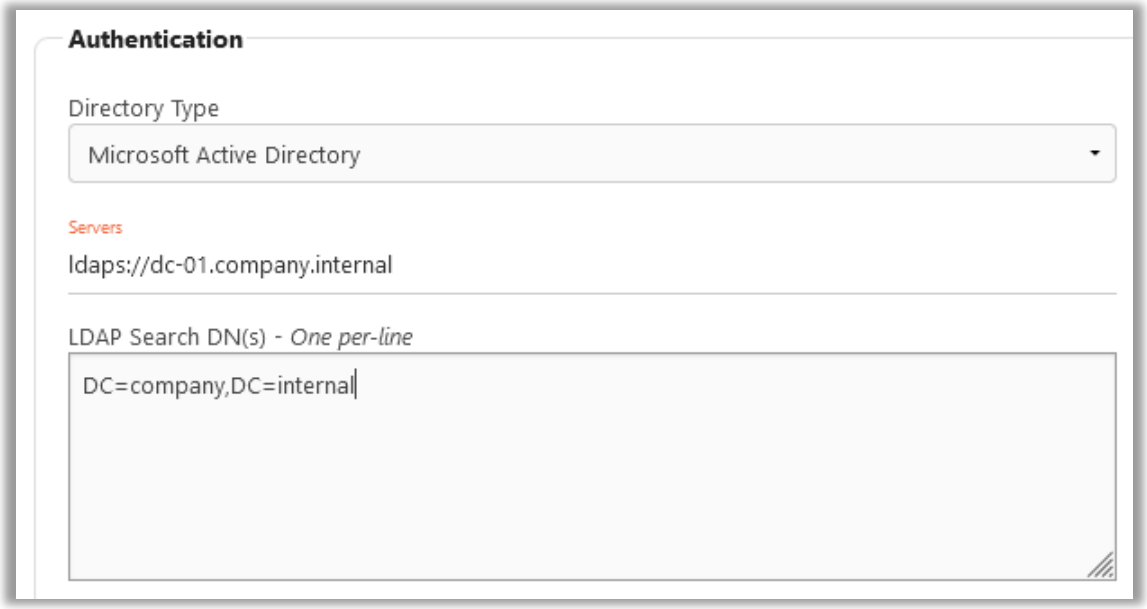
The example shown above will search for users and groups from the **root** of the Active Directory domain (so all OUs contained within are considered). It is possible to specify multiple Search DNs to allow the admin to target specific OUs in the domain, but in most cases, it is best to configure the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

Azure Active Directory (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 must be copied from Azure and saved onto 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**

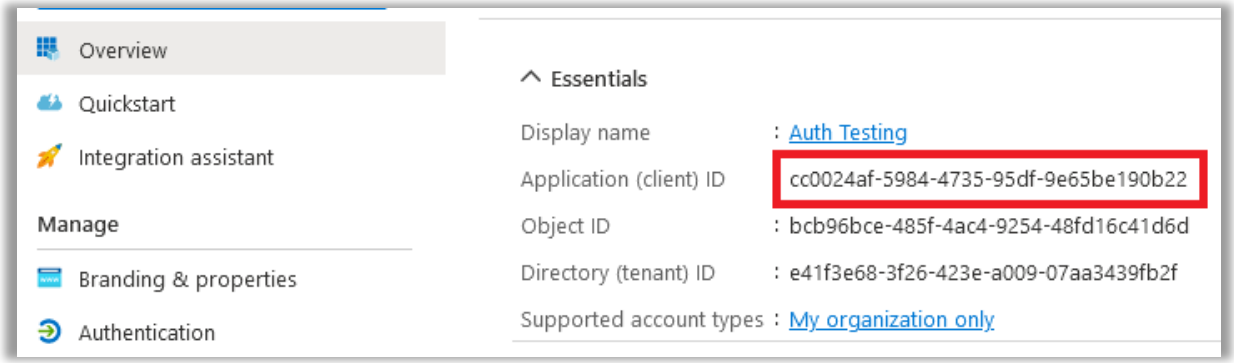
In the New Registration screen, give the app a suitable name, leave the supported account types as default (Accounts in this organizational directory only) and configure a Redirect URI using the platform type 'Web' using a Redirect URI configured as follows:

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

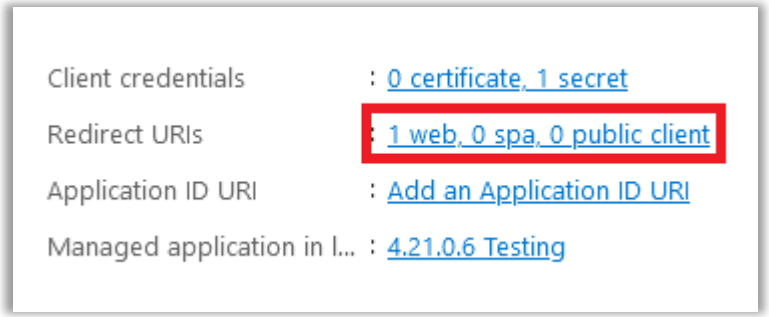
Replacing address-of-foldr with the public FQDN of Foldr.

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**

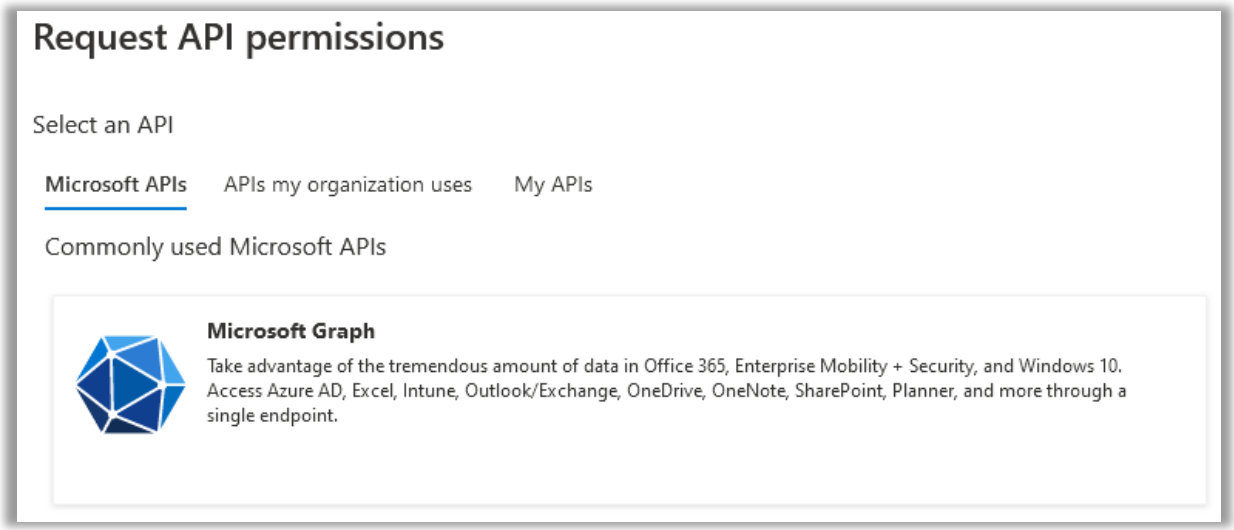
7. Enter a description, select a suitable expiration lifetime, and finally click **ADD**.

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

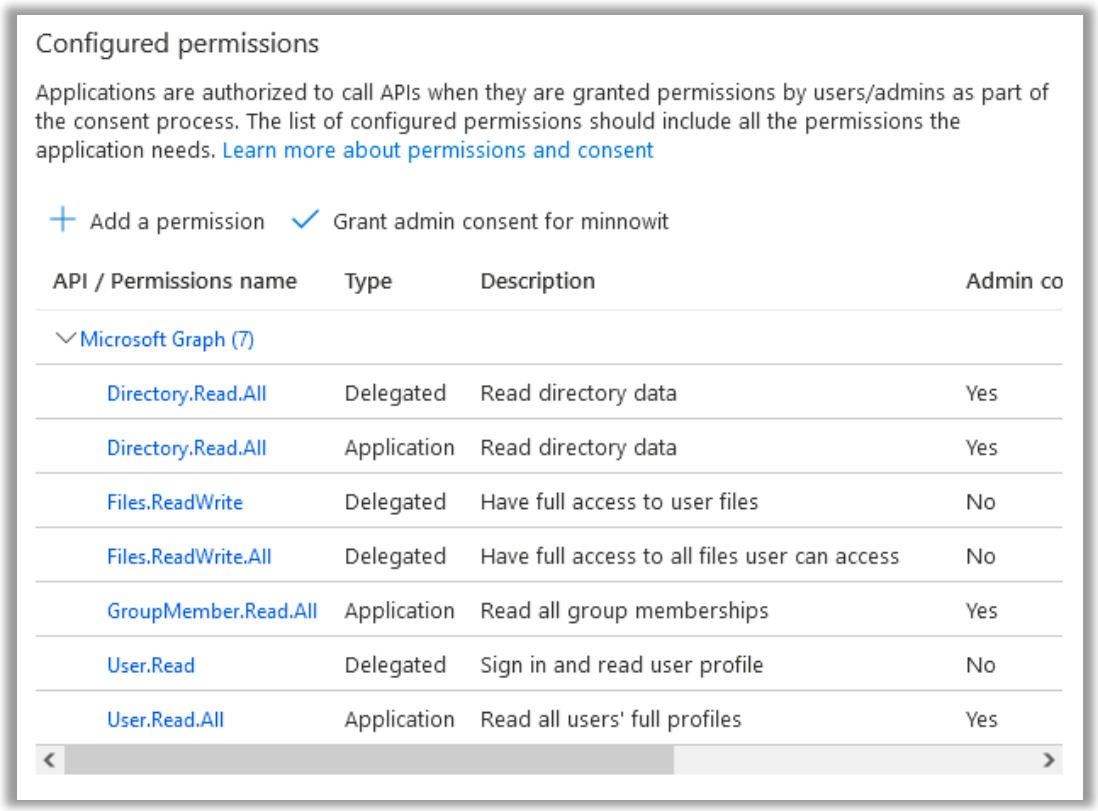
Click the **Application** Permissions box at the top of the Permissions selection panel (or go back to the App Registration overview and use API Permissions > Add a permission > Microsoft Graph > Application Permissions)

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

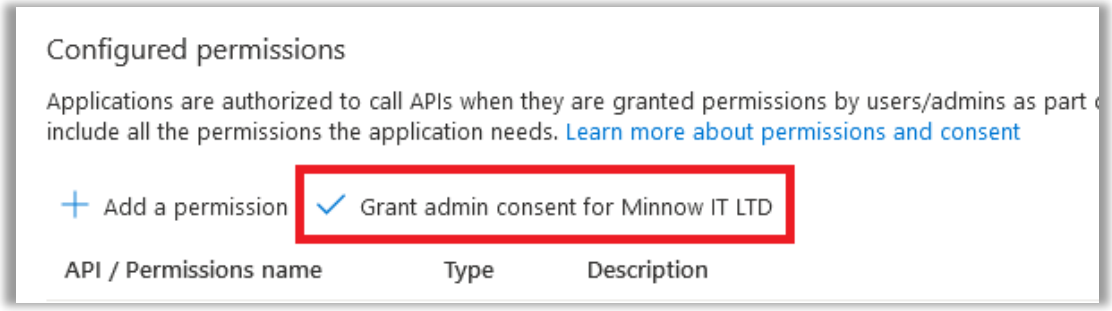
Directory.Read.All
GroupMember.Read.All
User.Read.All

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

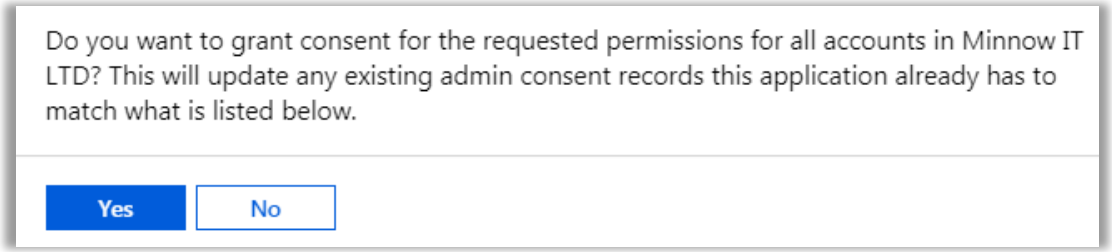
11. The permission summary will now be shown showing the updated delegated and application permissions.



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



Click **Yes** on the confirmation prompt.

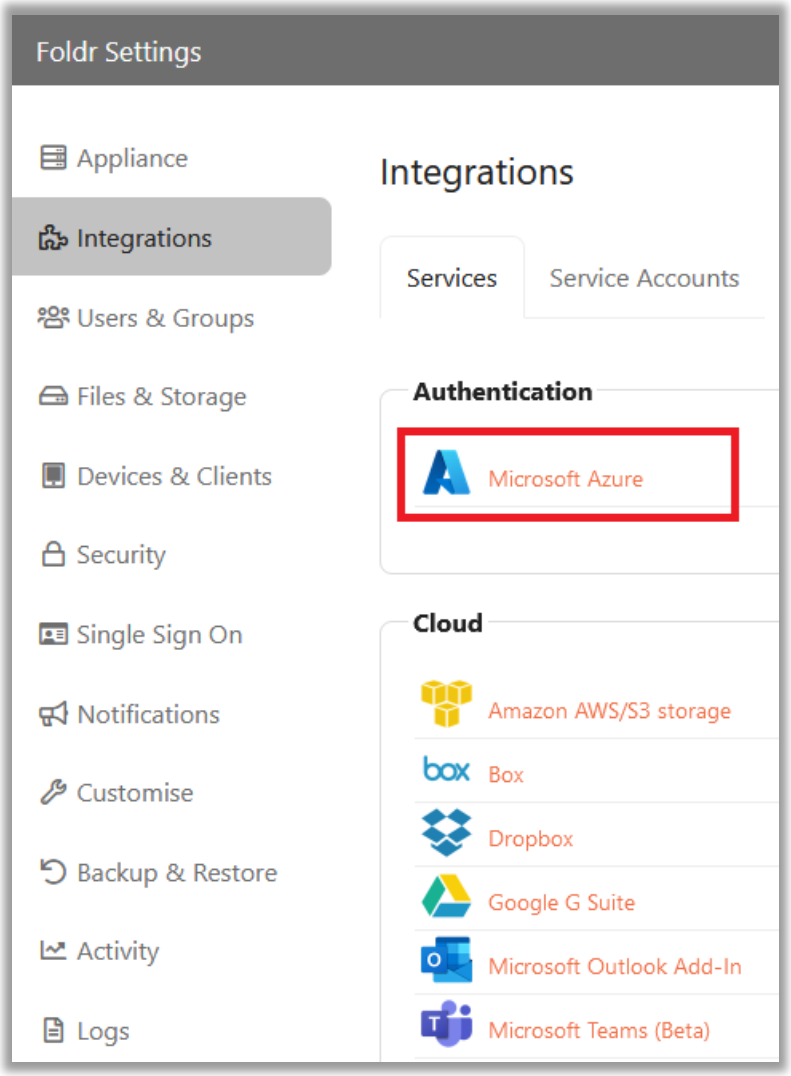


13. A success message will then be shown

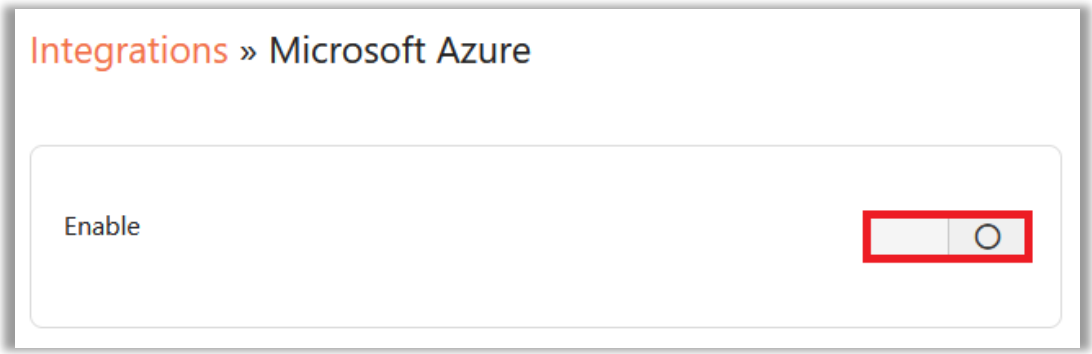
Enabling Azure AD in Foldr

Ensure the Licence key has been applied to the system (***Appliance > Status > General > Licence***) before proceeding.

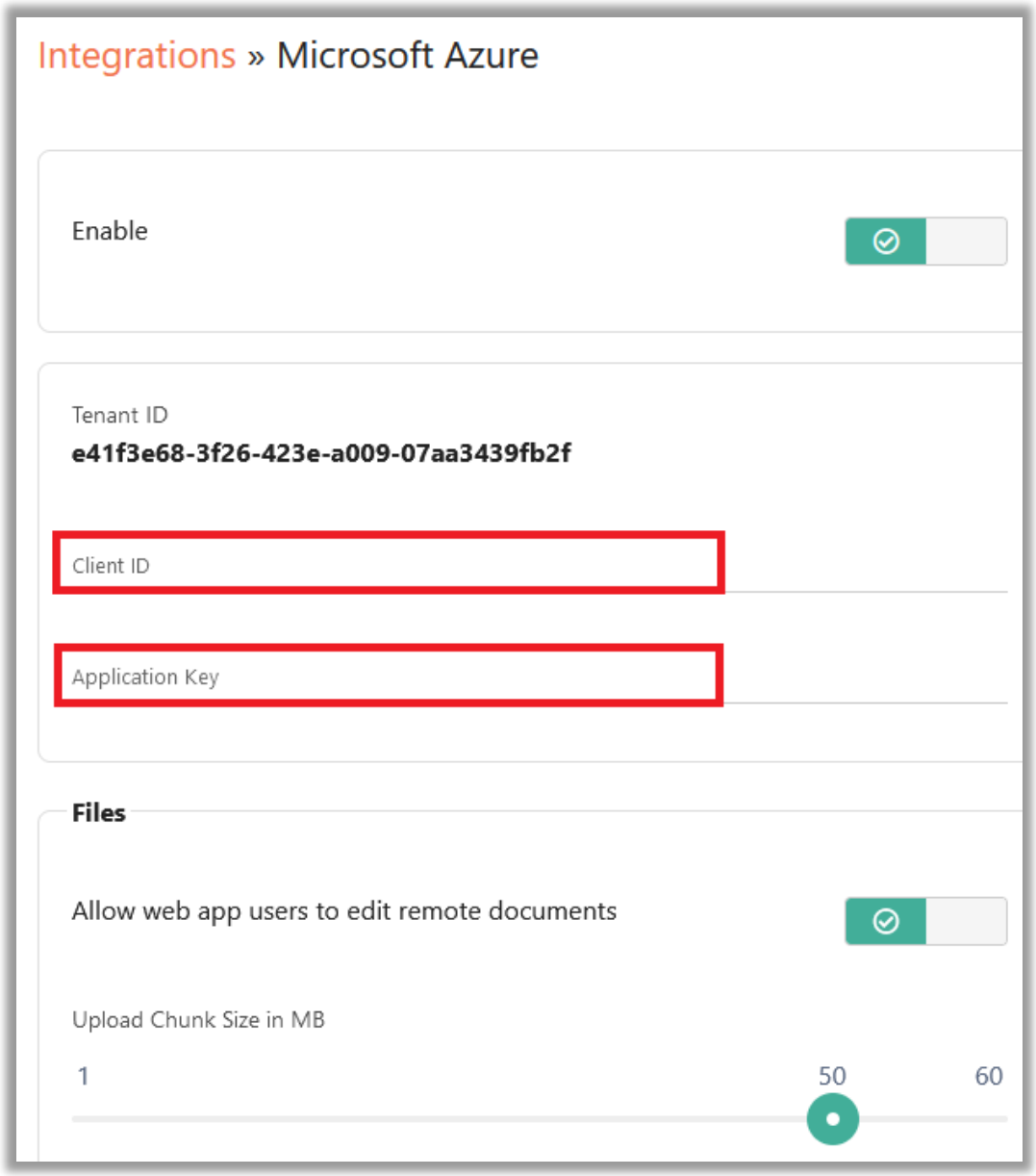
1. Click the **Integrations** tab and select Microsoft Azure under the Authentication section



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.

Local Users

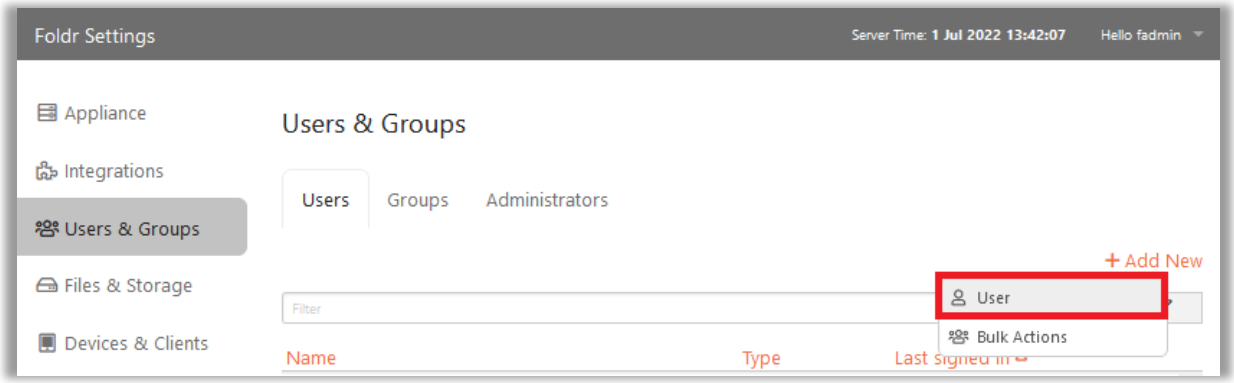
Local users may be created on the Foldr server itself where no Active Directory or Azure AD environment exists, or local users may be used in conjunction with on-premise AD or Azure AD users.

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.

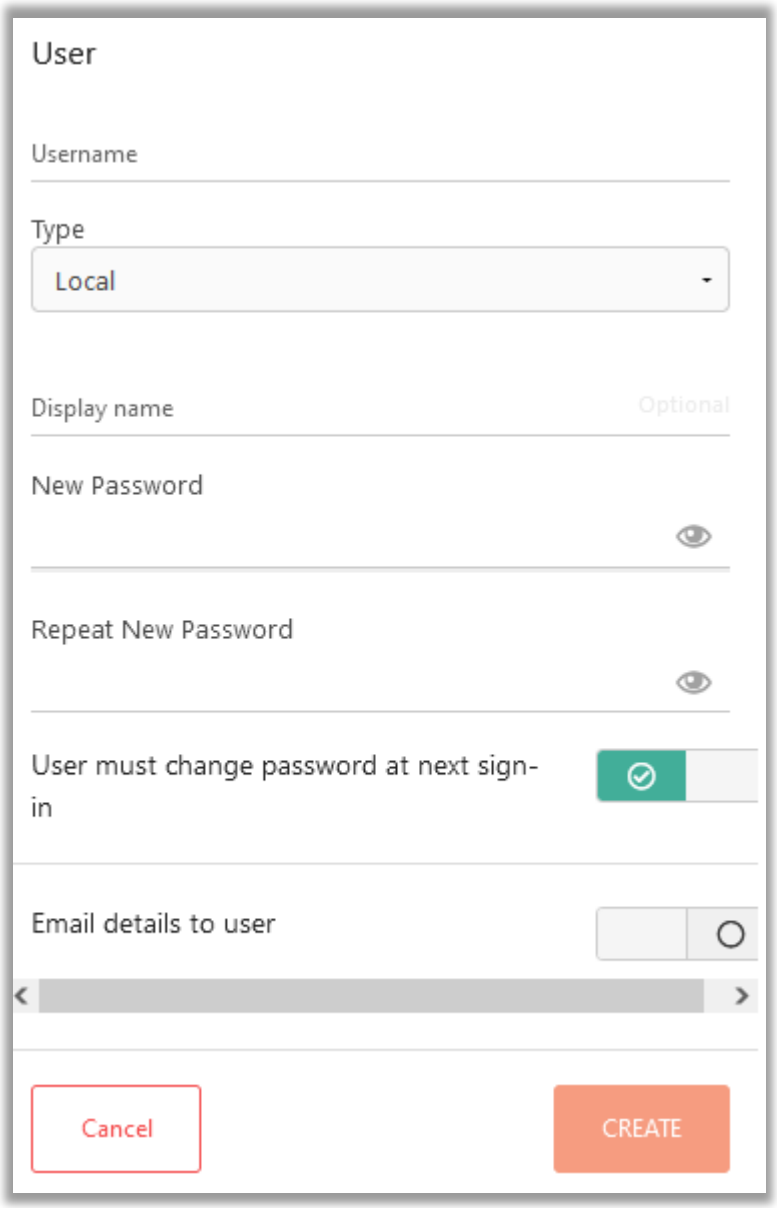
Local users can be created in ***Foldr Settings > Users & Groups***

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 preferred.



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:

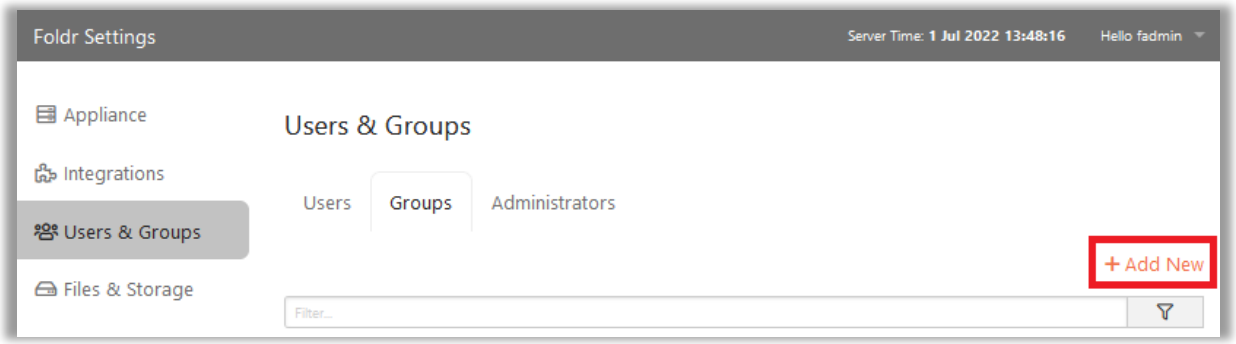
1. Grouping users together to apply Foldr permissions on those users or enabling features (type = **local**)

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.

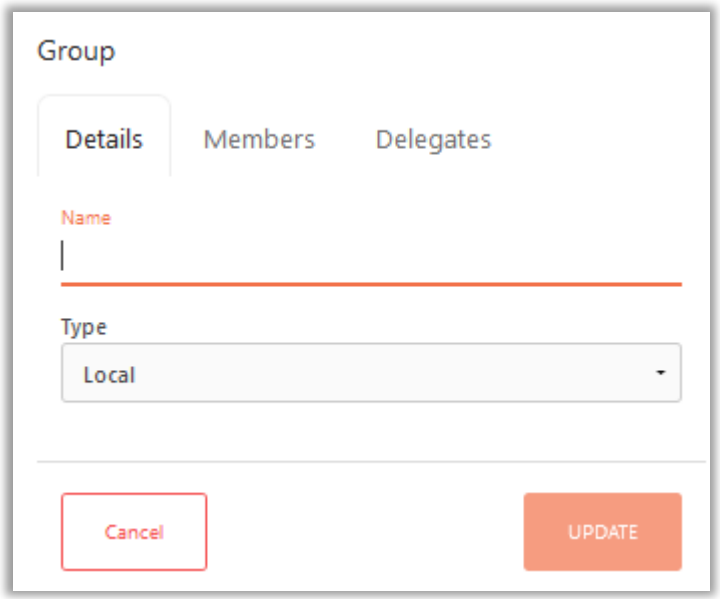
Local Foldr groups can be created in ***Foldr Settings > Users & Groups > Groups tab***

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.



6. Service Accounts

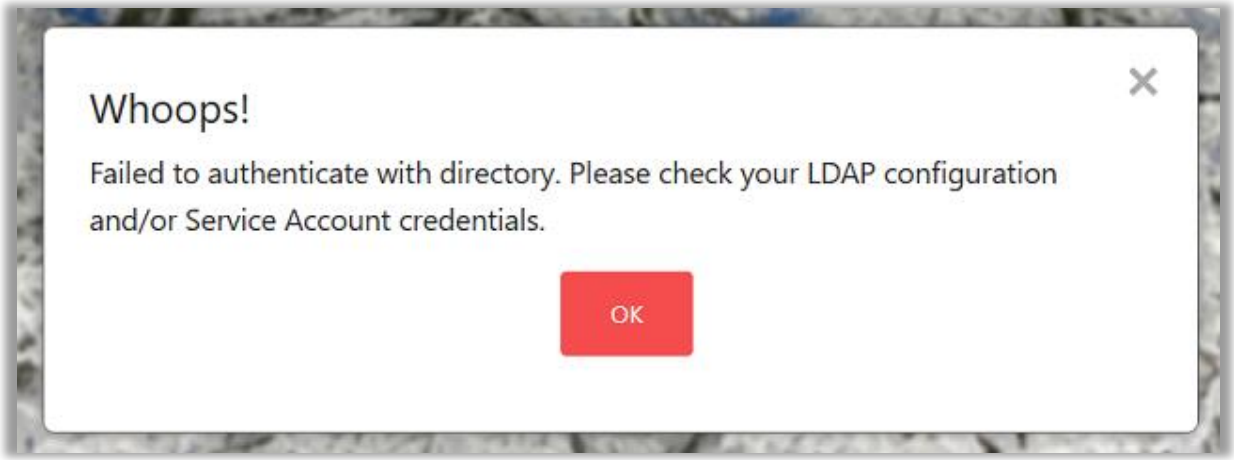
For Active Directory deployments, as part of the setup process, you should now configure the main appliance operations service account. There are three main types of service account in Foldr, these are:

1. Appliance operations service account (Important)

In an **Active Directory deployment**, a domain-based account is used to read the AD domain, query group membership to resolve permissions 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. However even in a mixed environment, using Active Directory and Local Foldr users, a valid service account must be configured even for local users to sign in successfully. In the event of LDAP authentication issues, or the service account not being configured or with an incorrect password, users will see the following error.



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 third-party cloud services, 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***.

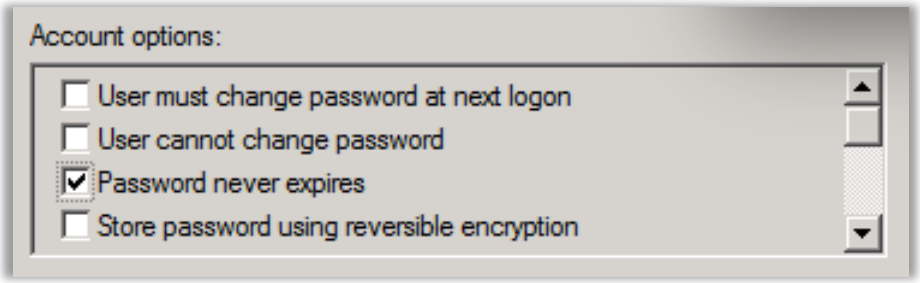
Creating the Service Account for Appliance Operations

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**.

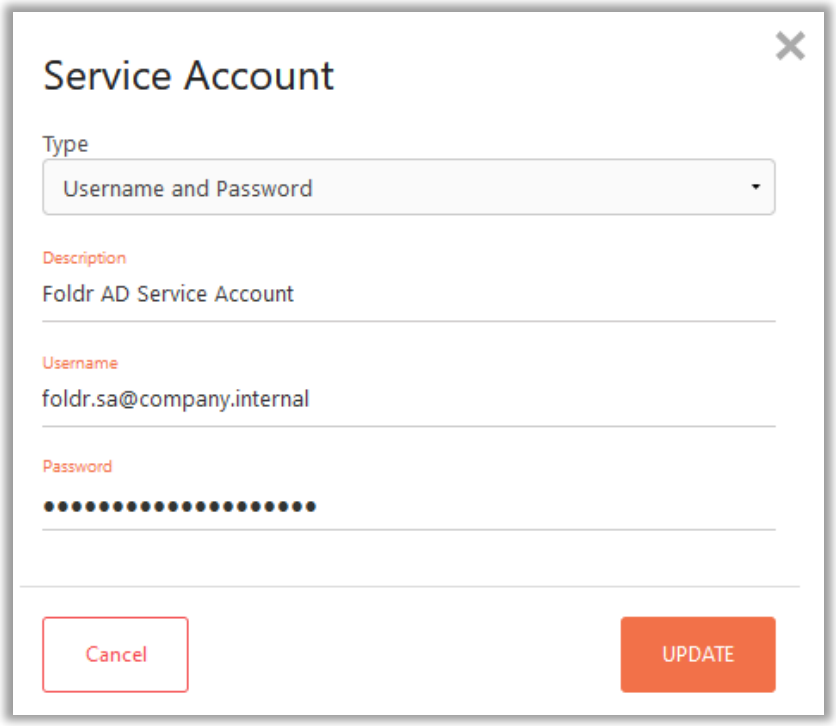
All Active Directory based service accounts should be configured using:

Type = Username and Password

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

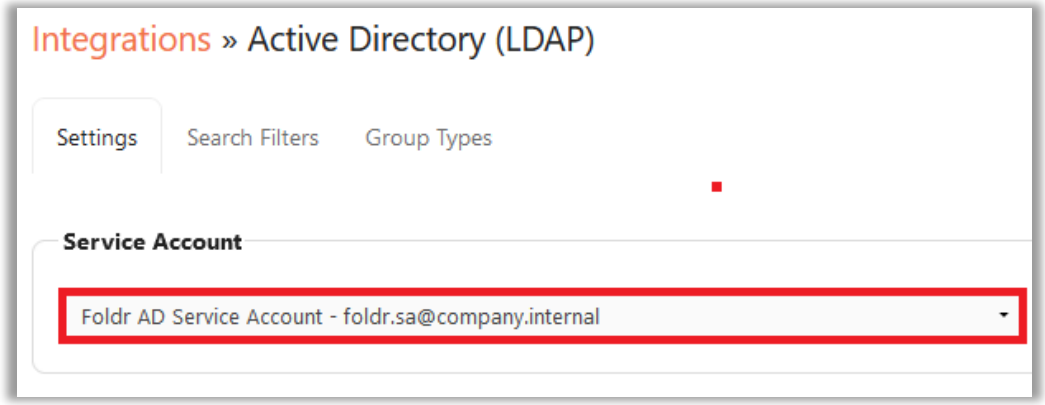
username@company.internal

Do not 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 all users and other features will not function as expected.

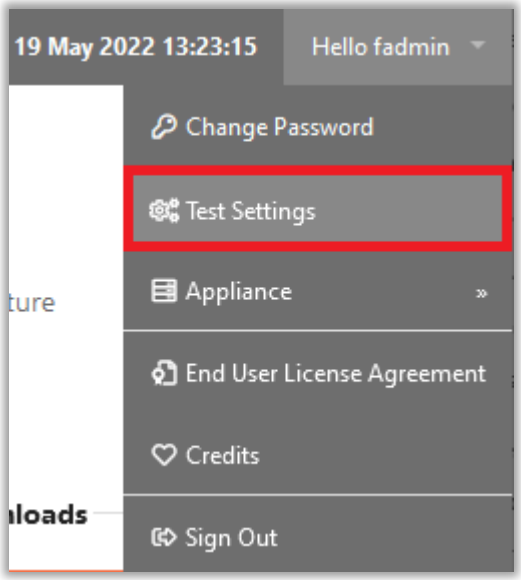
The basic configuration for Active Directory is now complete, and you should proceed to test authentication using the Test Settings function (see section 6)

IMPORTANT – In an Active Directory deployment, a service account **must** be set in ***General > LDAP > Service Account***. Failure to configure this service account will cause various issues with both administrative and user facing features.

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.

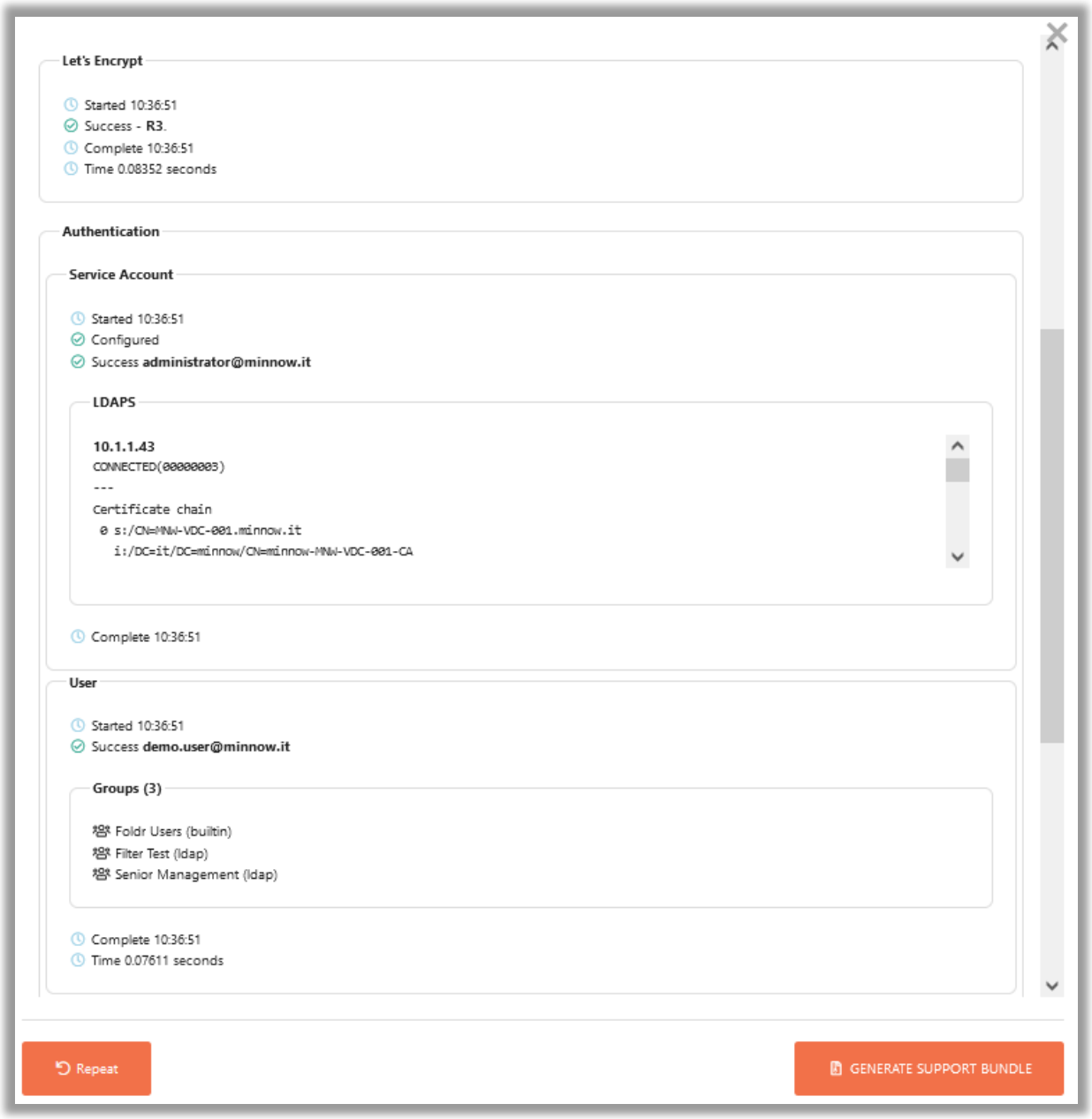


A username and password prompt will be shown. Enter either an Active Directory username (short format/sAMAccountNAme is accepted) or a local Foldr account and the password. Ideally an Active Directory user will have a home folder configured to test SMB connectivity.

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:

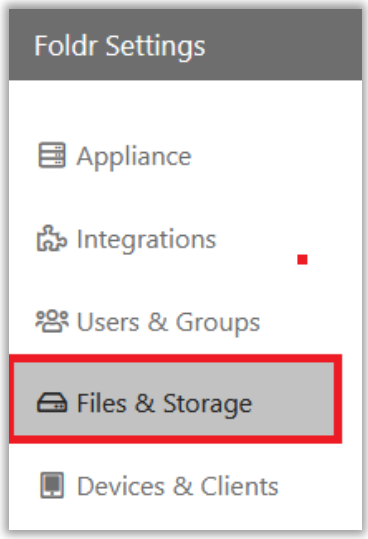


If there is an issue with any step in this process it will be highlighted by the test procedure.

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***

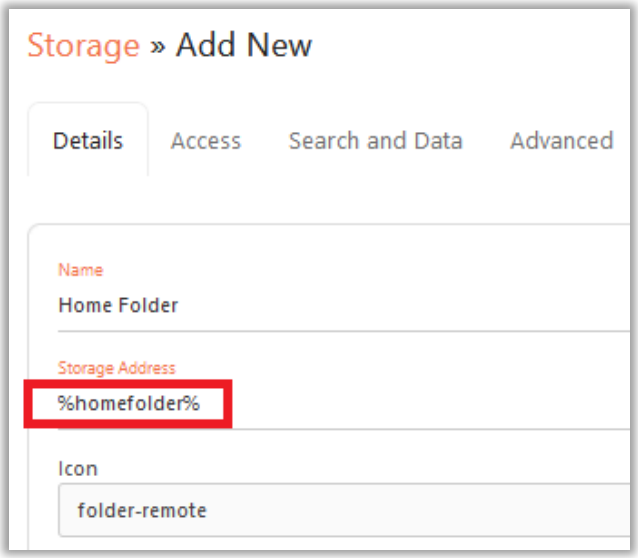


Active Directory (SMB) Home Folders

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

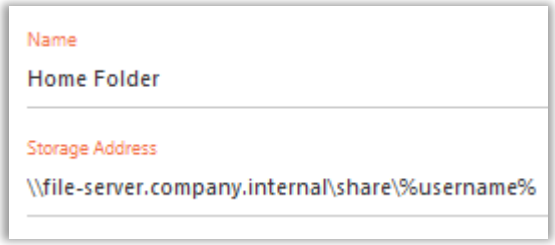
Active Directory Users & Computers > Properties of User object > Profile Tab > Home Folder > Connect

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



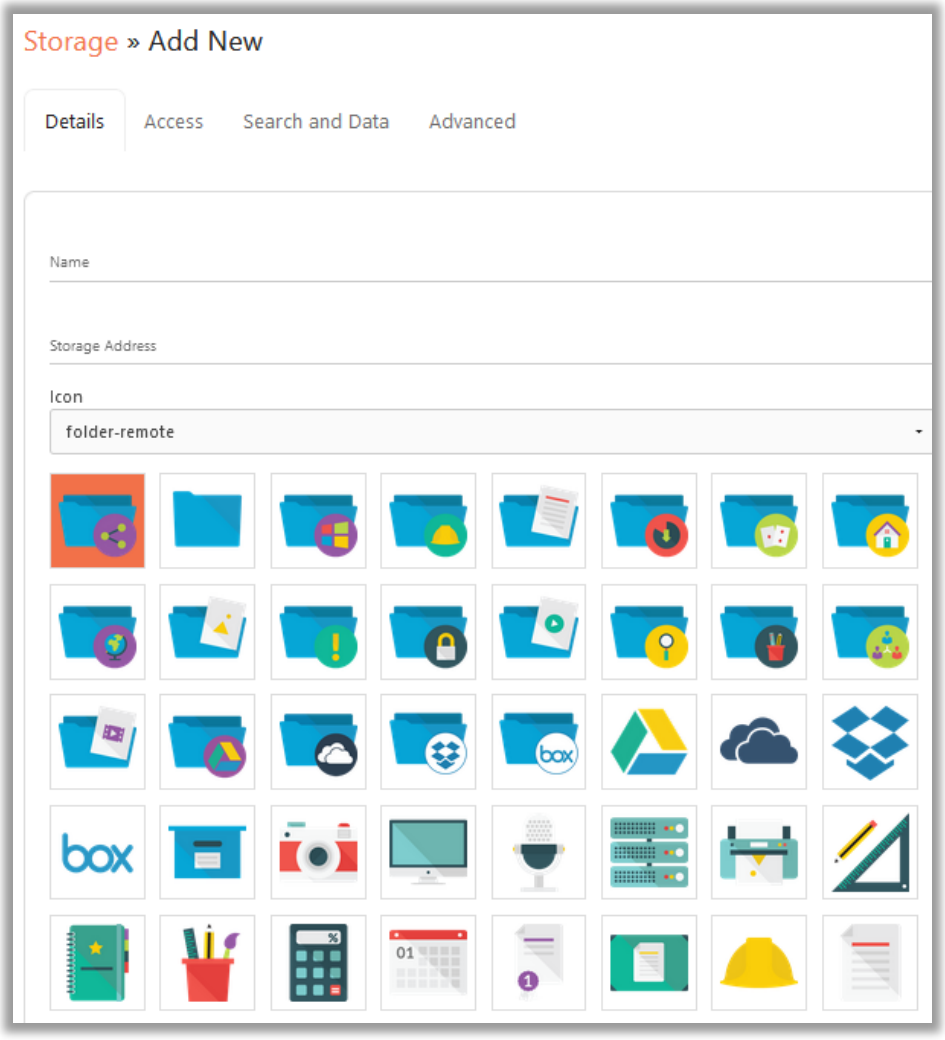
If user's home folders are not configured in Active Directory and presented to users using other methods (for example, login scripts or Group Policy Preferences) the administrator can add one or more additional shares as necessary to map share paths to user's home folder locations as required.

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



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

(Applies to Azure AD deployments)

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 later in this 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 the users 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.

WebDAV

WebDAV shares are supported and must be prefixed with **https://** as shown in the example below:

https://webdav-server/share-name

The storage configuration screen (Advanced tab) provides an optional NTLM authentication toggle which is required with some LMS/VLE systems.

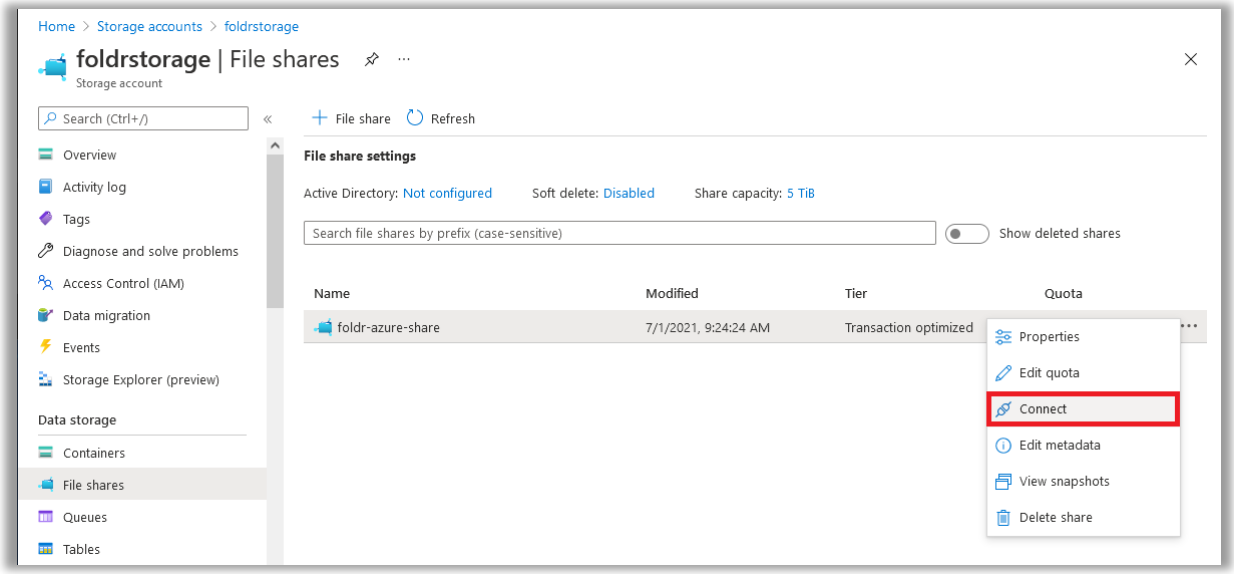
Azure File Shares (SMB)

In the Microsoft Azure platform, an administrator can create SMB shares directly from the management portal without the need to deploy Windows file server VMs to provision SMB shares. These shares are supported and can be presented in the Foldr interface.

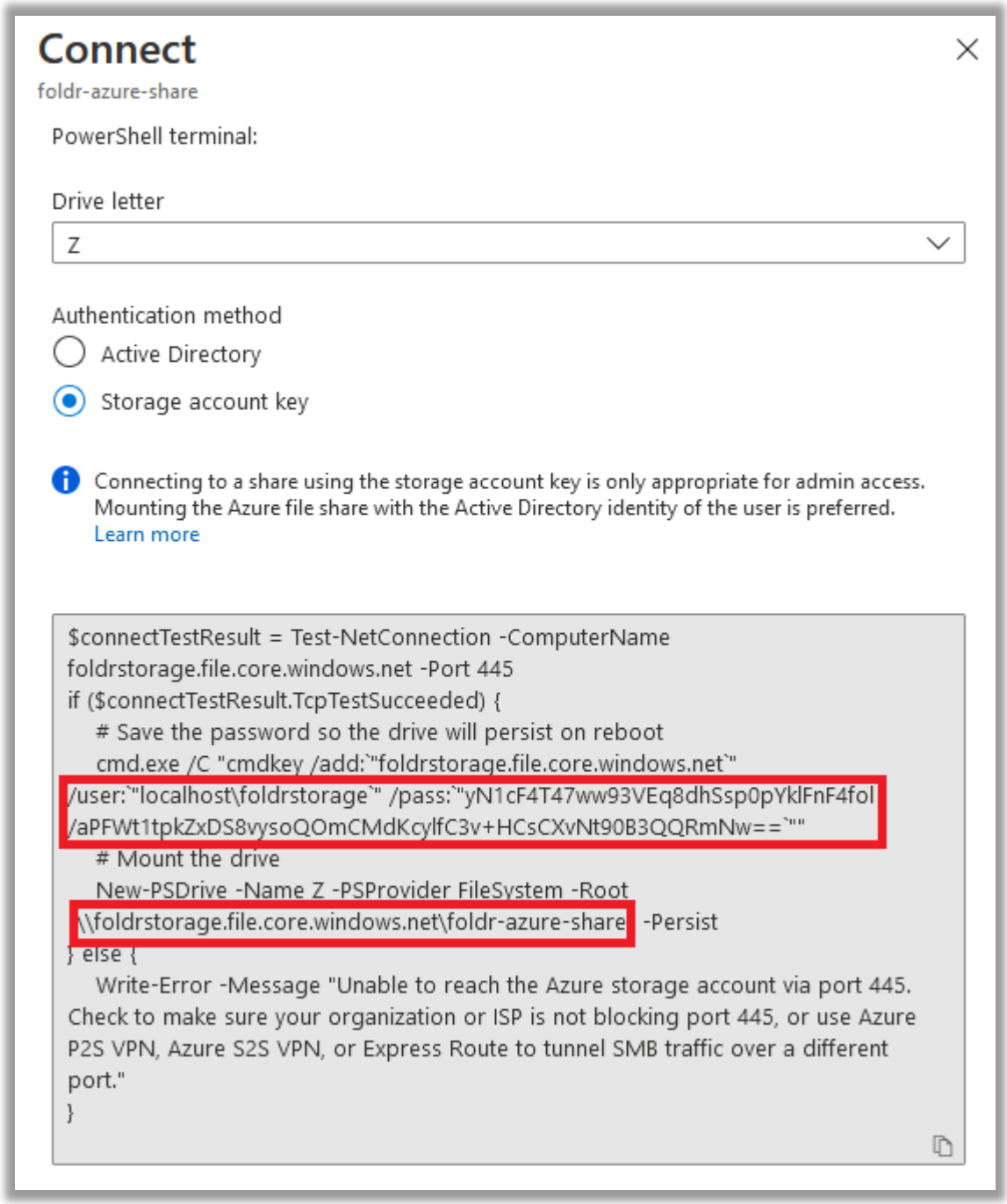
The Foldr appliance can either run on-premise, or in Azure to connect to Azure Storage, however the smb-mode on the appliance must be set to modern to ensure SMB3 is used. Run the following command on the appliance console:

```
smb-mode modern
```

Create the Azure File Share within the storage account as usual and click **Connect** from the ellipsis (...) menu

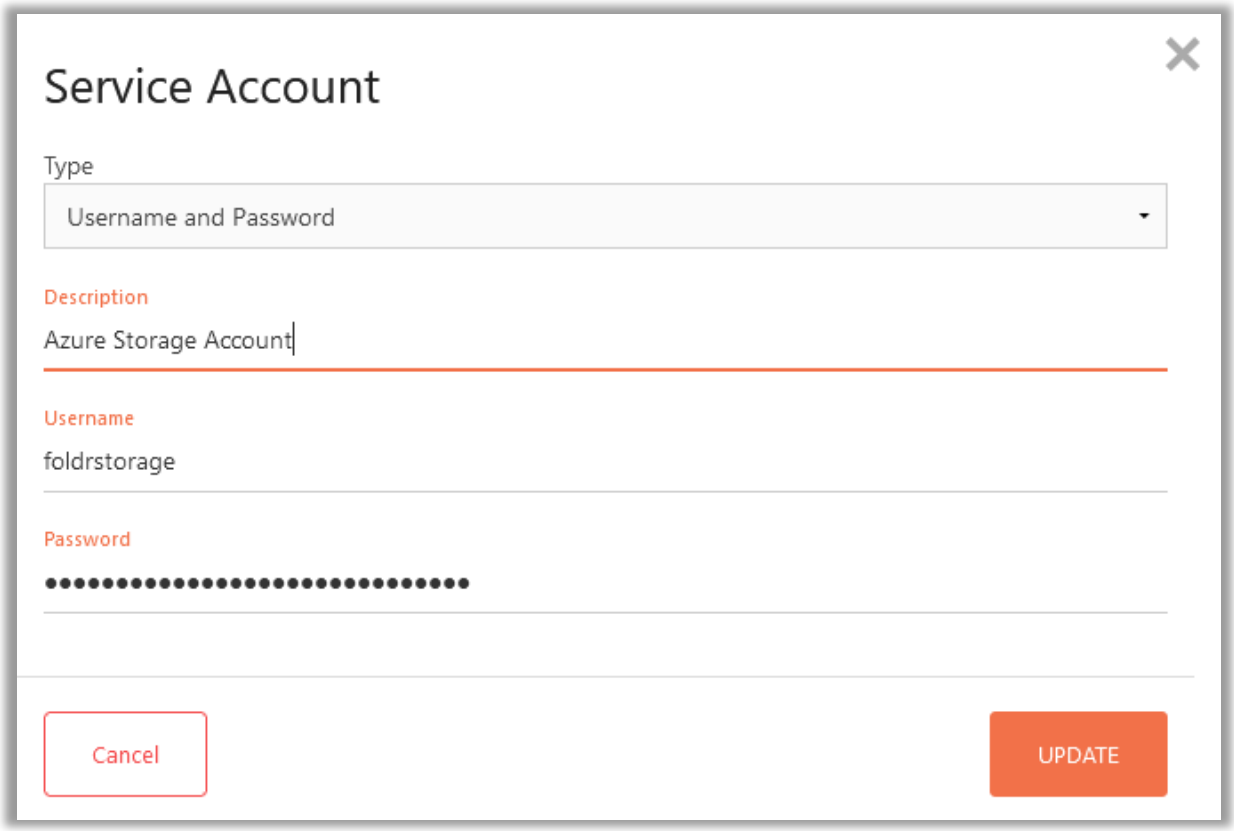


The Connect panel will display and the share's username/password and storage address is shown as below:



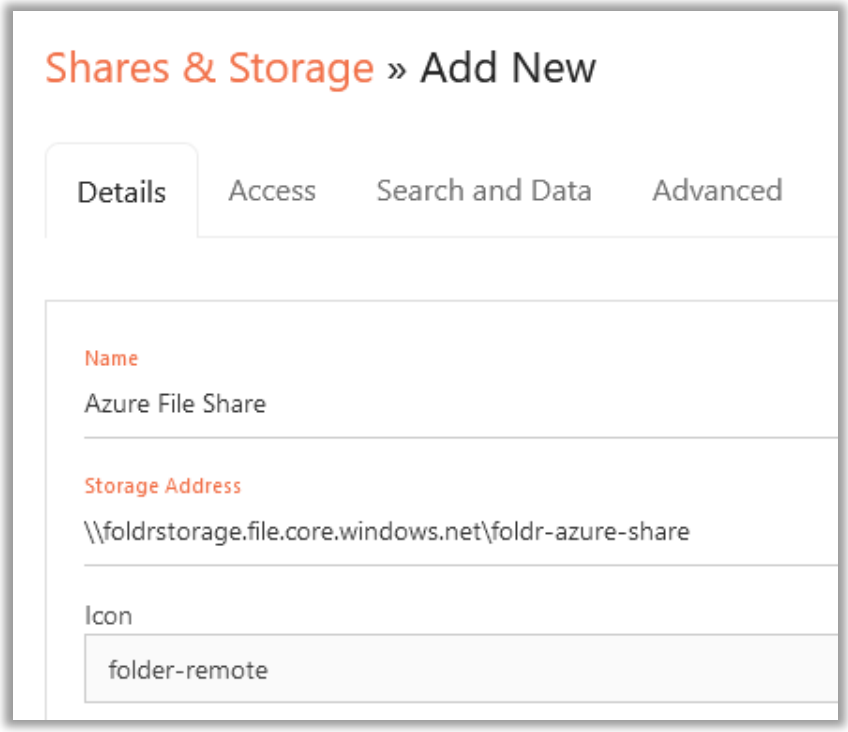
Username: foldrstorage
Password: yN1cF4T47ww93VEq8dhSsp0pYklFnF4fol/aPFWt1tpkZxDS8vysoQOmCMdKcylfC3v+HCsCXvNt90B3QQRmNw== (do not include the `" characters that surround the password)
Storage path: \\foldrstorage.file.core.windows.net\foldr-azure-share

Create a new service account in ***Foldr Settings > Integrations > Service Accounts*** with the type '**Username and Password**' using the username and password above.



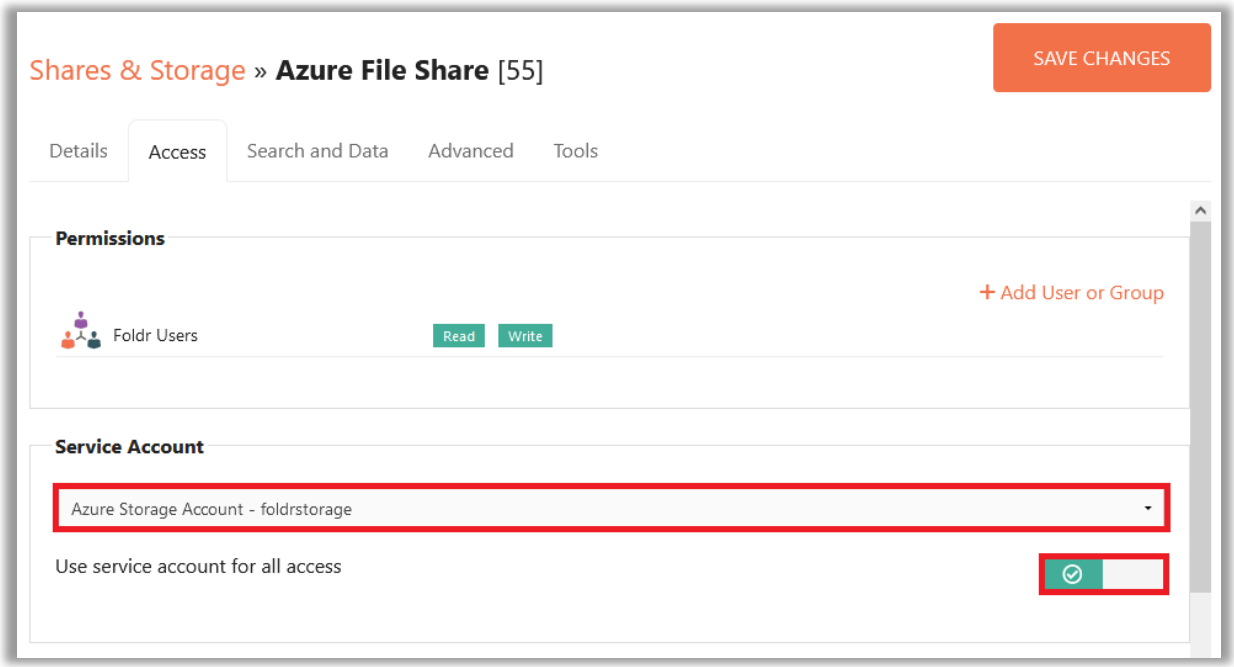
Create a new share in ***Foldr Settings > Files & Storage*** for the Azure File Share.

Enter a suitable share name and use the storage address as taken from the Azure Connect dialog



Click **SAVE CHANGES**. The storage address will automatically change to smb://foldrstorage.file.core.windows.net/foldr-azure-share.

Click the **Access** tab, and select the Azure Storage Account as the service account and enable the toggle to '**Use service account for all access**'



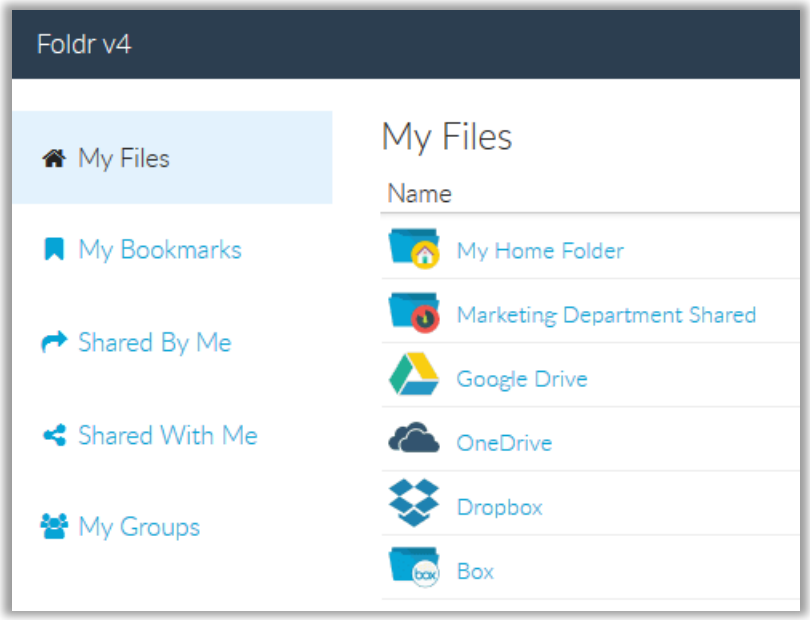
Controlling visibility of the Azure File Share

Notice that the built-in group 'Foldr Users' is configured by default under the ***Access tab > Permissions*** section. This represents all users in Foldr and with this configuration, all users would have access to the Azure File Share. To control visibility/access to the Azure File Share, delete the Foldr Users group object and search for suitable users/groups under *Permissions > +Add User or Group*, granting read/write permission as required.

Click **SAVE CHANGES** and the Azure File Share should now be accessible to users within Foldr.

Other Cloud Storage (Google Drive – OneDrive/SharePoint/Teams – Dropbox – Box – AWS S3)

The administrator can present various cloud storage platforms to users alongside on-premise SMB shares. All cloud services integration is disabled by default and must be enabled/configured by the administrator.



Once enabled and configured, users will be able to access their cloud account in the same way as any other share / drive presented in the Foldr interface. i.e. Files can be uploaded, downloaded, or moved across shares/cloud providers from web app, iOS or Android apps, through a mapped drive or WebDAV client.

Users can share files and folders with others and can bookmark files / folders regardless of the platform or cloud provider. This allows quick and easy access to regularly used files with no regard to their location, whether on-site or in the cloud.

Depending on the cloud platform being used, documents may be edited from either local Office applications, through Google G Suite (Docs, Slides or Sheets) or Office Online (web-based Word, Excel and PowerPoint). Files in Box or Dropbox can be edited may be edited in Google G Suite or Office Online if these services are also enabled.

Through the integration provided in Foldr v4, all cloud storage providers except for OneDrive can also optionally present the same storage account to multiple users (or everyone in the organisation). This allows the administrator to create entire shared drives in the cloud from services which typically only serve personal storage accounts.

Google Drive & Shared Drives

Google G-Suite integration is disabled by default and requires the Foldr administrator to enable and configure this feature, see section 17 for more information.

If the administrator has made Google Drive available a user's Google Drive will be presented in the interface alongside the other shares and Google Team Drives, if available. Additional Google integration also allows users to edit G Suite and Microsoft Office documents held on both Google Drive and local SMB shares seamlessly in Google's editor apps (Docs, Slides or Sheets). Office documents are imported / converted on the fly and all changes are saved back to the network automatically as you would expect when using Google Docs natively.

Google Drive offers the same functionality as on-premise SMB shares through Foldr. i.e. Files and folders can be shared, renamed, deleted, uploaded (drag and drop from desktop) or downloaded from Google Drive. Docs, Slides and Sheets may be downloaded to the local desktop as Word, PowerPoint or Excel as required.

Please note that Google Drive is **not available** using if a user connects to the Foldr server using a WebDAV client due to use of non-standard file naming and path conventions for data stored upon this cloud platform.

Shared Google Drives (Present one Drive to multiple users)

Along with personal Google Drive areas, Foldr can also to present a single, personal Google Drive storage area to groups of users in the same way that you have traditionally done with shared on-premise SMB shares / network drives. This can be done alongside any Google Shared Drives that may be in use to provide departmental collaborative storage locations and granular permissions may be applied to shared areas using share permissions within Foldr itself.

Multiple (shared) Google Drives can be presented to users as required.

OneDrive, SharePoint & Teams Cloud Storage (Office 365)

OneDrive for Business (includes education customers) storage, SharePoint sites and Teams can be presented to the user. Once the administrator has completed the Office 365 integration steps (section 17) the OneDrive or SharePoint sites will become available in the user's My Files section of the interface once they have linked their Microsoft account.

Additional Office 365 integration allows users to edit Microsoft Office documents held on both local SMB shares and 365 storage seamlessly in Office Online (web-based versions of Word, Excel or PowerPoint. When editing a file hosted on local SMB storage all changes are saved back to the original network location after editing in Office Online.

Office 365 storage offers the same functionality as on-premise SMB shares through Foldr. i.e. Files and folders can be shared, renamed, deleted, uploaded (drag and drop from desktop) or downloaded.

Using Foldr for Windows or macOS desktop apps, Office 365 storage can be presented to users in Windows Explorer or Finder as a regular network drive.

Dropbox and Box Cloud Storage

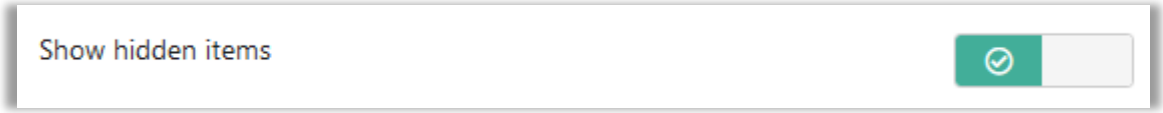
Both personal and shared Dropbox or Box storage accounts can be presented to a user. Once the administrator has completed the Dropbox /Box integration steps (section 17) the cloud account will become available in the user's My Files screen in the Foldr interface.

Dropbox and Box storage offers the same functionality as on-premise SMB shares through Foldr.

Advanced Share Settings

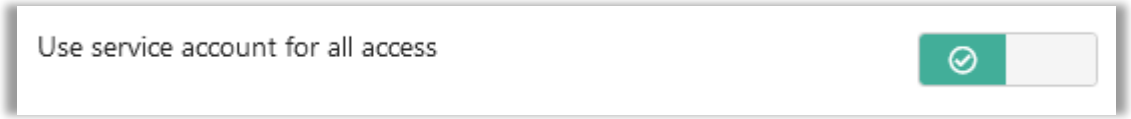
Show Hidden Files (*Advanced tab > Listing*)

By default Foldr will not display hidden files. Enable this setting to allow users to view and access hidden files.



Use Service Account for All Access (*Access tab > Service Account*)

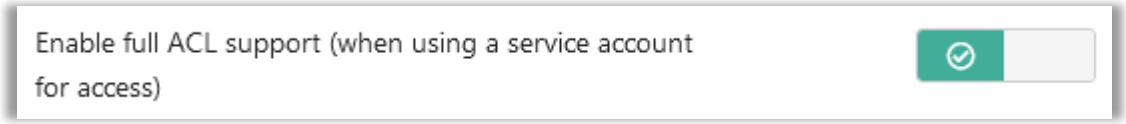
Configures the appliance to connect to the storage location using the service account provided on the main share configuration tab. This can be useful for presenting storage that the signed in account may typically not have permission to access, such as standalone NAS or other non-domain joined SMB server. It could even be used to allow shares to be presented from another Active Directory domain entirely to users. Finally, this option can be used with certain cloud integrations, such as shared Google or Dropbox accounts.



Enable Full ACL Support (*Access tab > Advanced*)

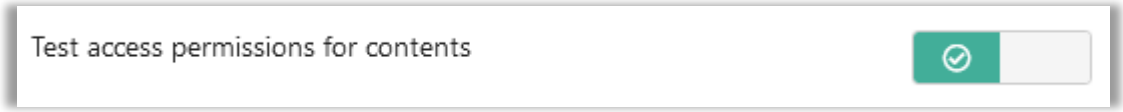
This option is hidden by default as it is intended to be used in conjunction with a share-based service account and the '**use service account for all access**' switch. Once enabled, the Foldr server will parse the NTFS permissions on the SMB share so that even though it is connecting to storage using service account credentials, it will provide the user with the correct access level for their account. Typical usage case for this option is when caching of passwords is disabled (within the Security tab) and shares are being presented to all users via service accounts.

Please note that Foldr will a respect the user's backend file server permissions without enabling this setting, providing the toggle 'use service account for all access' isn't enabled.



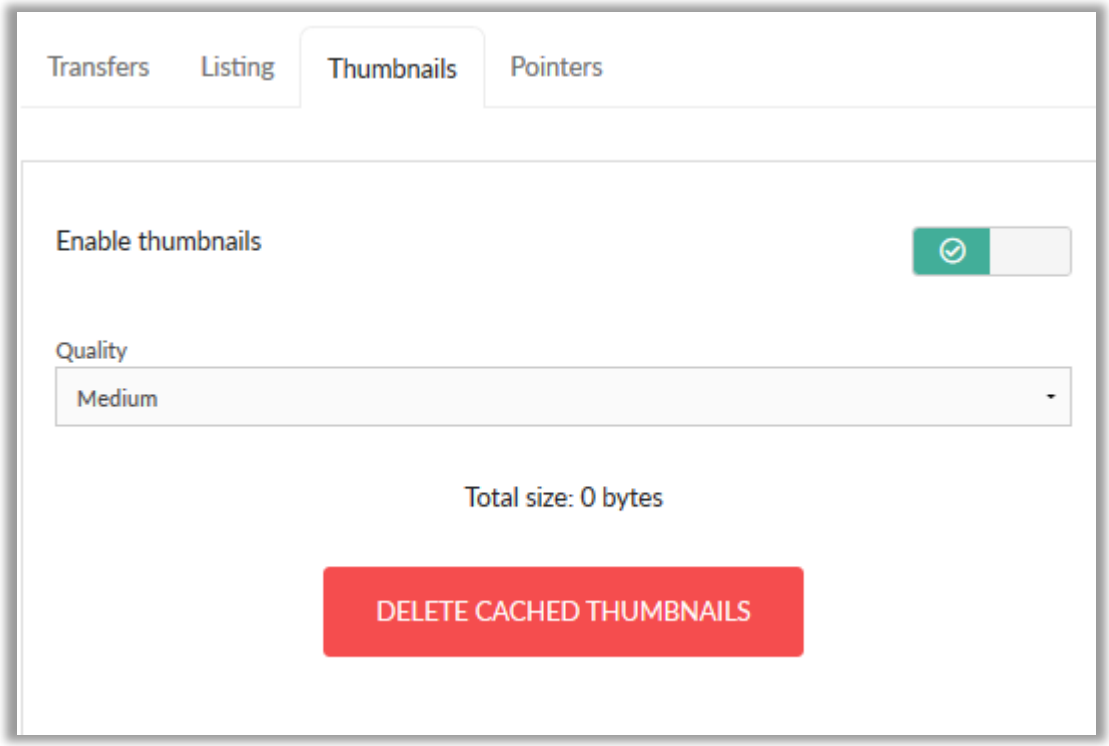
Test Access Permissions for Contents - SMB only (*Access tab > Advanced*)

This option will force the appliance to check the permissions on items within the share and hide it from view if the user does not have at least read access to it. (Similar to access-based enumeration in Windows Server). Note that enabling this option may add a slight delay navigating into folders on the share if they contain many items. This feature can be enabled within ***Files & Storage > Edit-Share > Access tab***.



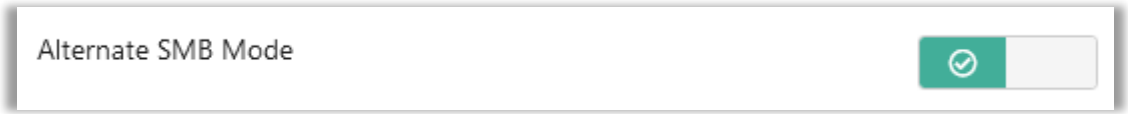
Enable File Thumbnails (*Advanced > Thumbnails*)

Foldr can provide thumbnails of common image formats and PDFs to users connecting via the HTML5 browser interface or iOS app. Please note that you must also enable thumbnail support in the iOS app settings to use this feature. This feature can be enabled within ***Files & Storage > Edit-Share > Advanced > Thumbnails***.



Use Alternate SMB mode (*Access tab > Advanced*)

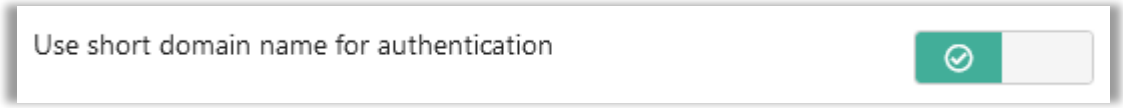
May be required with some SMB storage systems (NAS) where the default SMB mode cannot be used. With this option, the server uses the smbclient binary and parses the output, rather than the libsmbclient natively.



Use Short Domain Name for authentication (*Access tab > Advanced*)

Some storage vendors (Netgear ReadyNAS, FreeNAS and others) require users to connect using the short (NetBIOS) domain name rather than the full UPN (i.e. DOMAIN\username rather than username@domain.internal)

To provide support for these storage devices, the administrator can enable the 'Use short domain name' toggle on a share-by-share basis as required. This feature can be enabled within ***Files & Storage > Edit-Share > Access tab***.

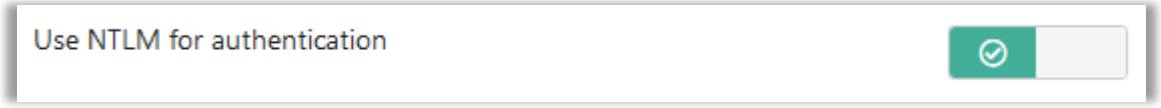


If the network uses a custom **NetBIOS** name, this can be specified within ***Appliance > Network***.

NTLM Authentication (WebDAV only)

Some third-party servers, such as the Firefly learning platform present shares using WebDAV protocol and require clients to connect using NTLM authentication.

To provide support for these solutions, the administrator can enable the 'Use NTLM authentication' toggle. This feature can be enabled within ***Files & Storage > Edit-Share > Access tab***. Note the storage path must be configured with the https:// prefix (and saved) for this option to be visible.



Use Full UPN for Authentication

This feature can be enabled within ***Files & Storage > Edit-Share > Access*** tab. Note the storage path must be configured with the https:// prefix (and saved) for this option to be visible.

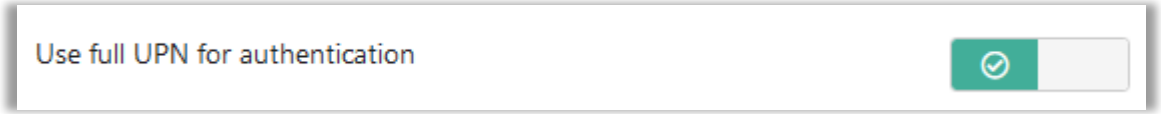


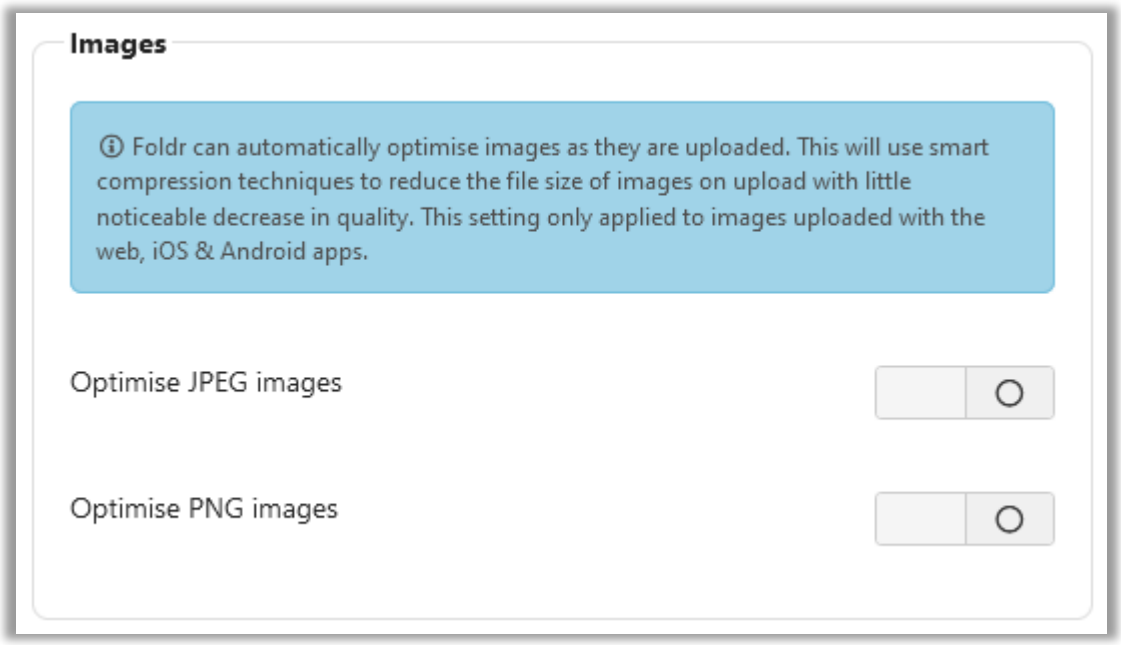
Image Optimisation

Foldr can automatically optimise JPEG and PNG images as they are uploaded by users. This will use smart compression techniques to reduce the file size of images on upload with little noticeable decrease in quality.

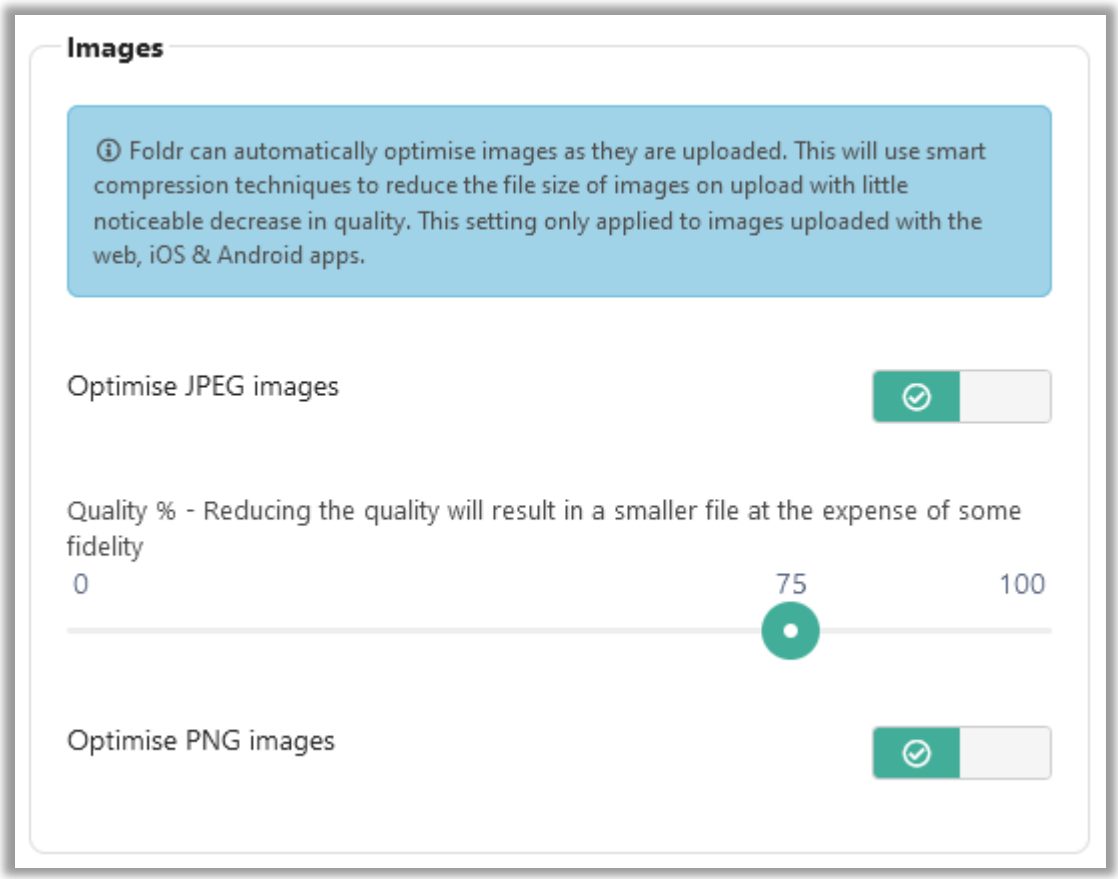
This feature only applies to images uploaded with the web, iOS & Android apps. Images uploaded via the desktop apps are not subject to the optimisation process, if enabled.

This feature can be useful if users are uploading hundreds of images from smartphones to a media type share and you do not need the images in their full/original raw file size.

This feature is enabled on a per-share basis and is configured within ***Foldr Settings > Files & Storage > Edit-Share > Advanced tab > Transfers*** tab. Scroll down to the Uploads section.



Enable the required toggles to optimise JPEG and/or PNG images as required. The JPEG option provides a quality slider, the lower the quality the smaller the resulting uploaded file size will be but with poorer quality. 30-50% is a good starting point.



File size examples:

An **11MB PNG** file will be reduced to **4MB** if optimisation is enabled.
An example **7MB JPEG** (typical smartphone camera image) file will be reduced to roughly **400KB** at 40% quality.

Group Drives

Group Drives allows an administrator to present storage locations that are typically only presented to one user, such as SMB Home folders, OneDrive or Google Drive to another user / group of users – Essentially presenting shares to one user in another users context. This allows the admin to provide oversight and give managers, team leaders or teachers the ability to review users documents no matter where they are stored.

An example use case for Group Drives in a business or educational scenario would be to allow senior management / teaching staff to easily view all employee / student on-premise home folders and cloud storage that is managed by the organisation's IT department. When the manager/teacher signs into Foldr they would see the following structure and Foldr will automatically present the sub-folder structure inside the Group Drive based on the groups selected when configuring the share.

My Files
– Group Drive
— — Student 1
— — — SMB home folder
— — — OneDrive

— — Student 2
— — –SMB home folder
— — — OneDrive

— — Student 3
— — — SMB home folder
— — — OneDrive

The administrator can present one or as many shares as required inside the Group Drive for each user. In this example, an SMB home folder and OneDrive are configured.

Service Accounts (SMB)

All on-premise (SMB only) pointer shares that are presented to another group of users (teaching staff) must use a service account in conjunction with the 'Use service account for all access toggle' found under the Advanced tab in the Share configuration screen.

The service account is used in the background when a user is interacting with a Group Drive to provide access to an SMB share / home folder that they typically would not have permission to read/write data.

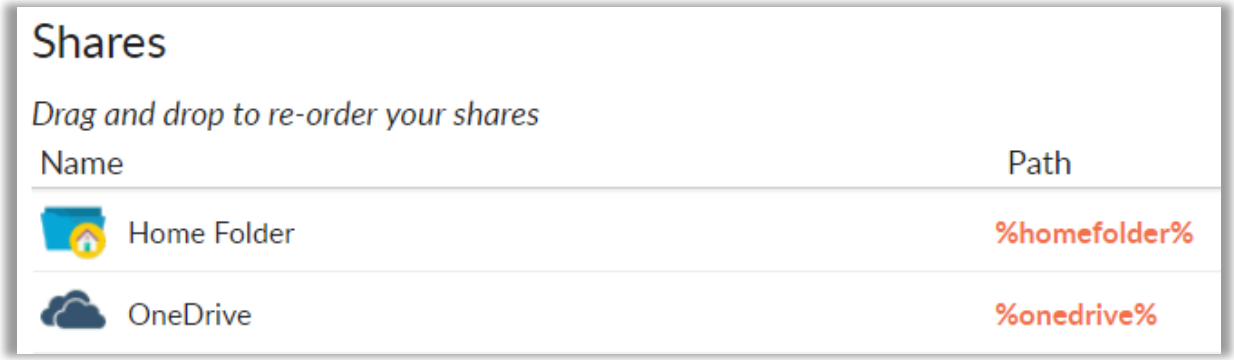
Service accounts are **NOT** mandatory for cloud storage (OneDrive / Google Drive) as both manual and automatic account linking options can be used. i.e. It will depend on the account linking mode being used. In the case of manual linking, the user that 'owns' the cloud account will have to have linked their account in Foldr before the manager / teacher user can access it via a Group Drive successfully. Because of this, service accounts / automatic account linking is recommended.

Configuring an Example Group Drive

In this example, we will configure a group drive to allow all members of the 'Teaching Staff' Active Directory Group read-only access all students Active Directory home folder and each student's OneDrive hosted in Office 365.

1. If they do not already exist, create shares in ***Foldr Settings > Files & Storage*** for the home folder and OneDrive.

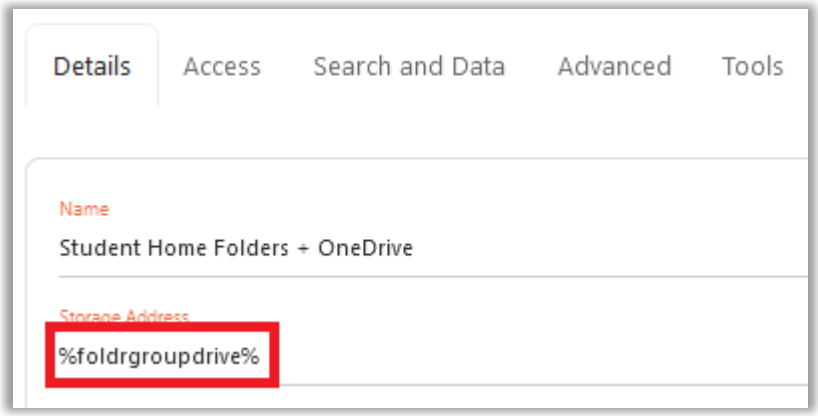
If service accounts are not being used on an existing SMB home folder share, it is possible to create another dedicated home folder share purely for the purpose of use in a Group Drive – NOTE -Each SMB share being presented via Group Drives **must use a service account** and have '**Use service account for all access**' enabled under the Access tab.



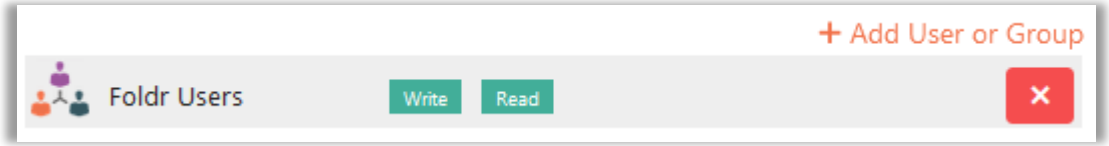
2. Create a new storage item for the Group Drive in ***Foldr Settings > Files & Storage***.

In this example, the group drive will be presented to users in an Active Directory group called 'Teaching Staff'.

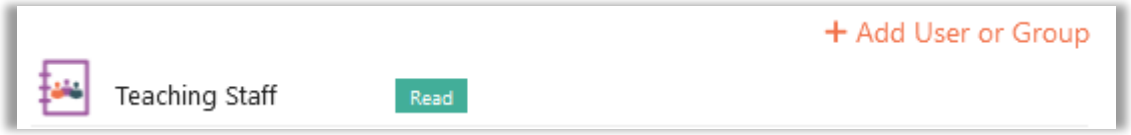
Name the Group Drive share as appropriate and use the Path / Share URI ***%foldrgroupdrive%*** and select an appropriate icon.



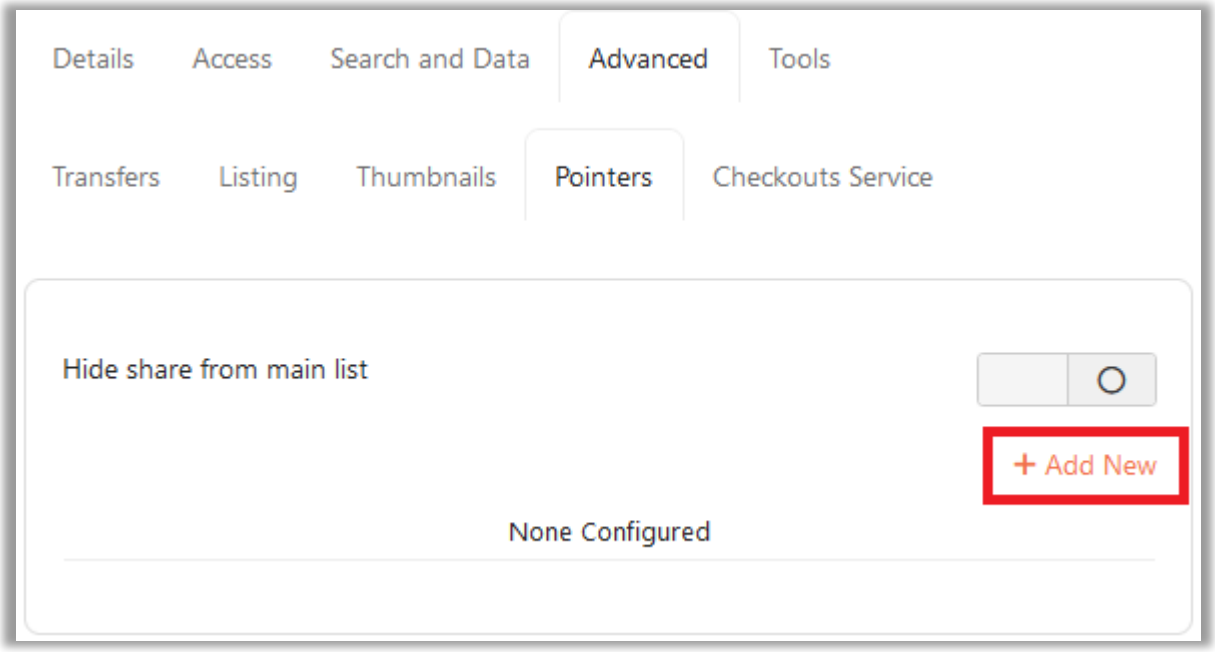
3. Navigate to the **Access** tab to control who will see the Group Drive in Foldr. Remove the default Foldr Users group (everyone) by clicking the in-line X button.



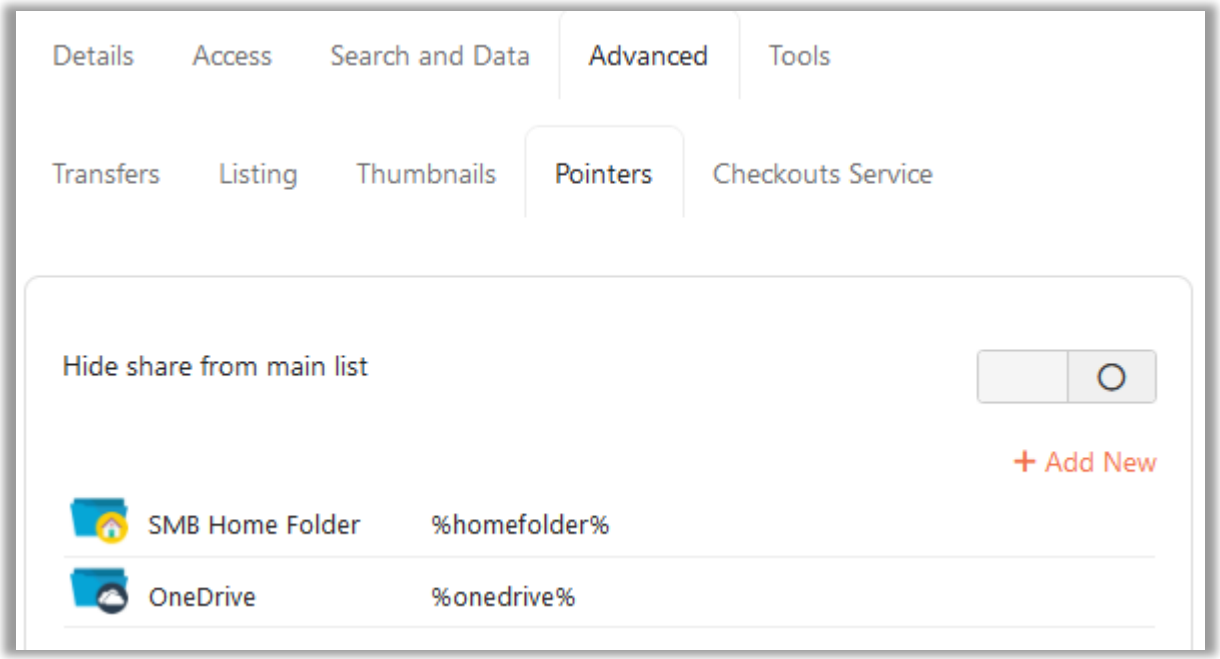
4. Click **+ Add User or Group,** search for the group that should be presented the Group Drive in Foldr and Allow the Read permission. Click Update. Should you want Teaching Staff to have write access to the Student storage locations, the write permission should be included here.



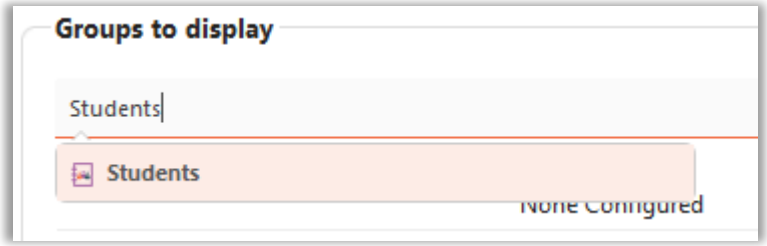
5. Click the ***Advanced*** *tab* > ***Pointers*** and Add a New Pointer



Add the Home Folder and OneDrive shares. i.e. The storage locations that the administrator wishes to present Teaching Staff in the student's context.



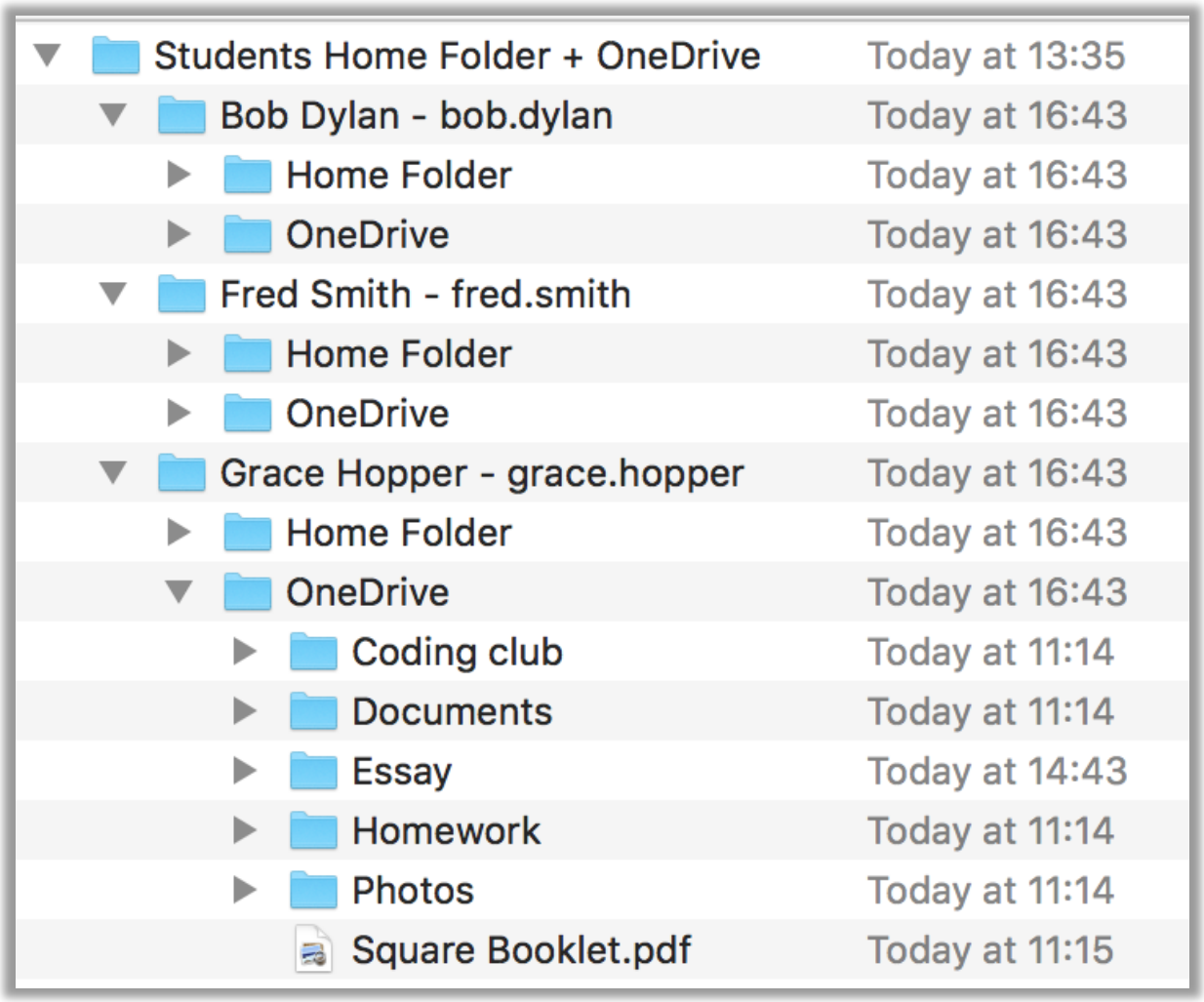
6. In the Groups to Display field, search for the Students group and click **Save**



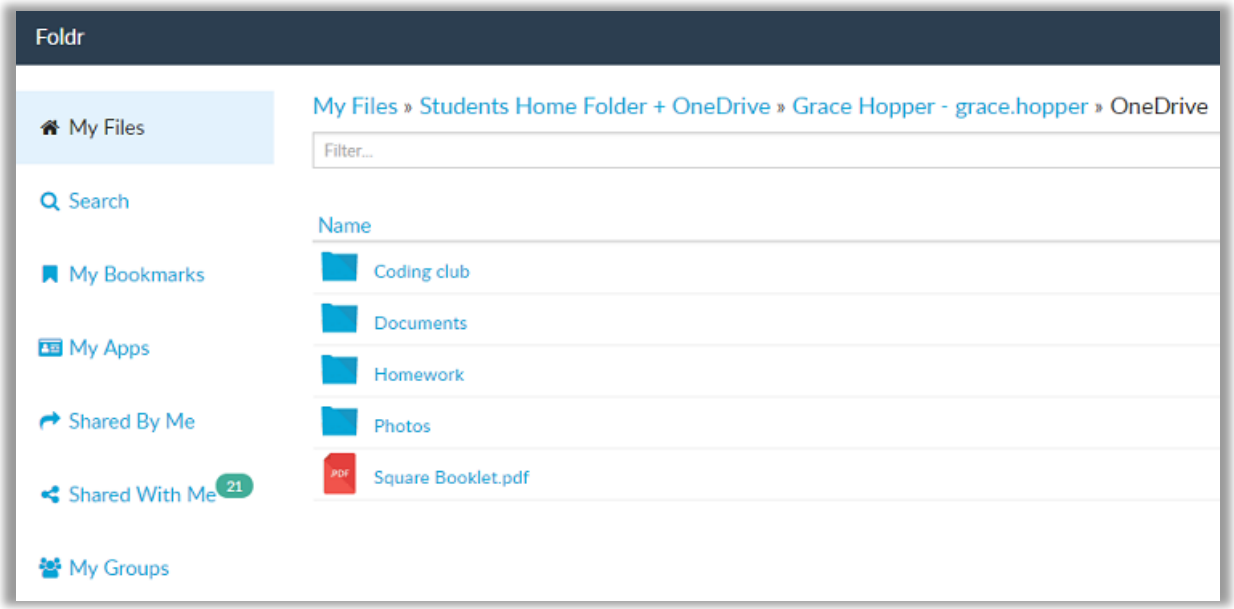
Using the Group Drive

The Group Drive is now ready to use and users in the Teaching Staff Active Directory group will see the Group Drive under My Files in all Foldr apps. Inside the Group Drive a sub folder will be shown for each user that is a member of the Students Active Directory group. Inside each student folder will be another sub-folder for each pointer configured, in this case one that links to their personal home folder and another for the users OneDrive. Files can then be interacted with in the same way as another share in Foldr.

macOS app



Web app



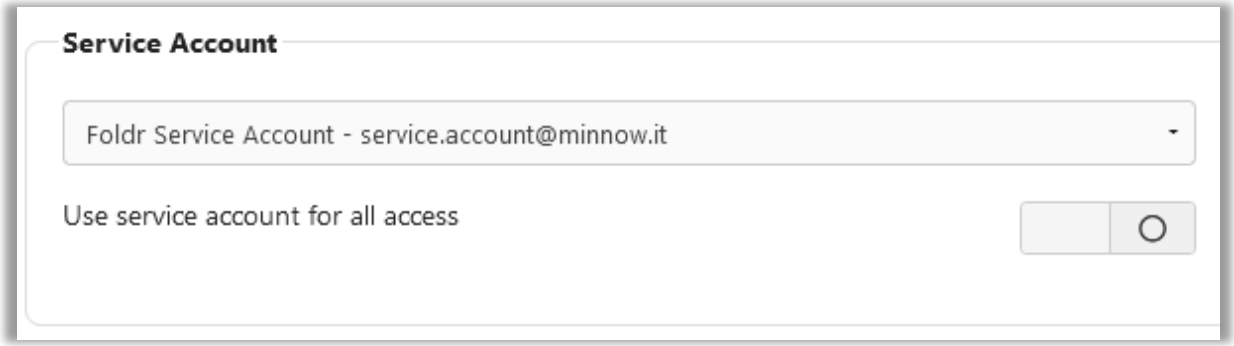
Service Accounts (Share based)

Service accounts in the share configuration screen can be used for the following:

- Provide the backend credentials which are used by the appliance with file sharing and public link functionality (applies to SMB shares).
- Provide the Cloud service account credentials to enable automatic drive provisioning (automatic account linking) to users or for OneDrive, SharePoint, Teams, Google Drive and Dropbox.
- Provide alternative credentials to connect to storage device, such as standalone / non-domain bound devices such as Network Attached Storage (NAS) or macOS server. This is used in conjunction with the '***Use service account for all access***' toggle.

Note – Personal Google Drive and OneDrive do **not** require a service account to be configured for user access or file sharing functionality from these storage locations.

Service Accounts for Sharing & Public Links (SMB shares)



A service account can be configured on a per-share basis, and this is generally used by the system for file sharing purposes with SMB shares. Without a service account configured, file sharing will fail when a user tries to interact with the shared item, as the server has no backend credentials to use to read / write to the appropriate storage locations.

The account used for the service account must have the appropriate permissions on the file server for the chosen sharing mode. More information is available in the Troubleshooting section of this guide.

Service Accounts for connecting to storage with alternative credentials (standalone NAS etc)

If the 'Use service account for all access' toggle is enabled, the appliance will use the Service Account credentials provided to connect to the share. This can be useful for presenting storage running on a standalone / non-domain bound storage device such as NAS or if you wish to connect to shares using alternative credentials. An example use case would be to connect users to storage running on another Active Directory domain.

When enabling this feature, it is important to remember that you are overriding the signed in user's security permissions and connecting with the service account credentials.

Share visibility and permissions can be controlled in the same manner as any other share using the Share Permissions area – see below.

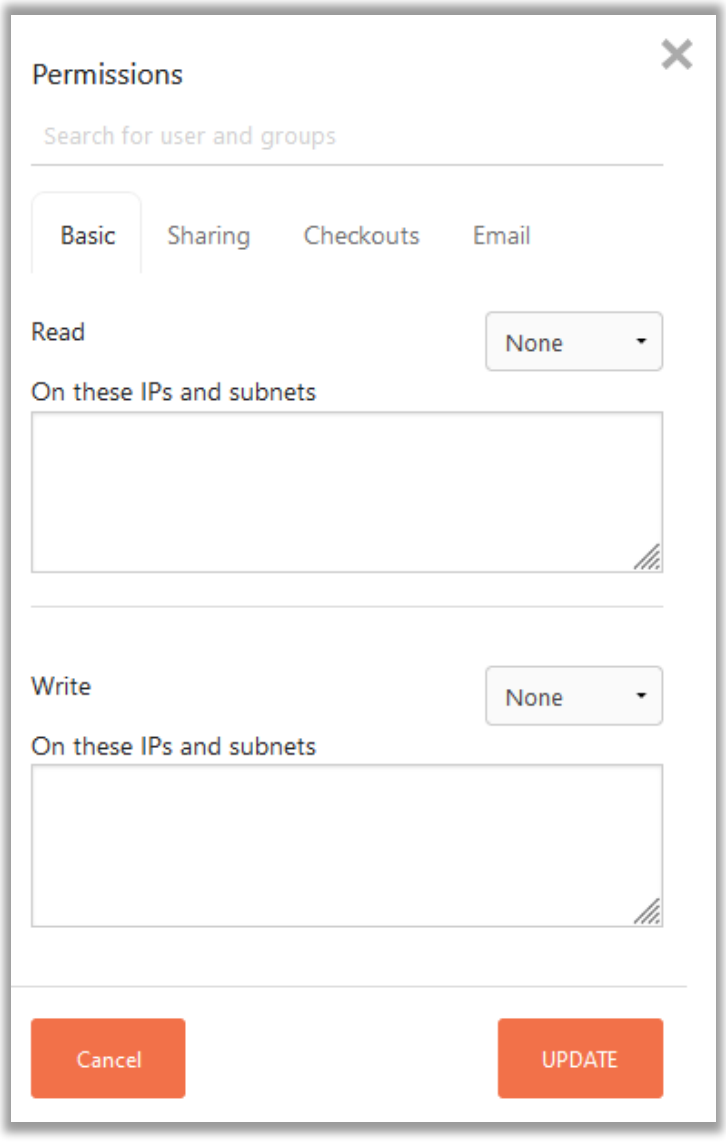
Share Permissions & Share Visibility

Domain & file server security permissions are automatically respected by Foldr. When a user signed into Foldr, in the default configuration, the appliance will attempt to connect to each configured share to check if the user has permission to access it. Any share that a user does not have at least read access to is automatically hidden from the interface.

Foldr continues to respect the existing security permissions / ACLs within shares down to the individual file level. However, in some cases, the backend file server permissions are not as tightly enforced as they should be and there may be operational reasons for not adjusting the permissions on the file server. In this scenario, the Foldr administrator can ensure only appropriate Active Directory users or groups are entitled to access the resource by using the 'Share Permissions' feature found at the bottom of the Share configuration screen.

Note that 'deny' entries always override 'allow'. The exception being where individual user permissions override groups.

Share permissions can be configured for everyone (Foldr Users) or Active Directory users or groups using the Permissions section within ***Foldr Settings > Files & Storage***. The permissions screen is broken into tabs for basic permissions, sharing, check outs and finally email (Inbox).



Basic Tab:

Read **–** User / Group will be permitted or denied file read, preview, and download actions providing they have sufficient permissions on the backend storage.

Write **–** User / Group will be permitted or denied file write, modify, rename, move and upload actions providing they have sufficient permissions on the backend storage. If write permissions are granted, users will be able to use the Edit in Microsoft Office option from the web app to allow direct editing of documents in the Foldr web app using locally installed Office applications on Windows and macOS.

Sharing Tab:

Share **–** User / Group will be allowed to share resources with others inside the organisation and give others Hand In, Hand Out or Manage rights to the resource

Create Public Links **–** User / Group will be permitted or denied the ability to create Public links. Public links are short URLs for use with others generally outside of the organisation

Create Secure Links – User / Group will be permitted or denied the ability to create Secure Links. Secure links are similar to public links (short URLs to files / folders) but the user sharing the item can specify who can access the resource through email invite and secure codes.

Create Secure Writable Links – *As above*, but the external user using the secure link will be able to upload to the shared folder using the web app via drag and drop between desktop and browser. Foldr will automatically organise files that are uploaded from external users to shared folders inside a dynamically created subfolder for each user placed within a directory called 'Foldr Uploads' in the root of the shared directory.

Check Outs Tab:

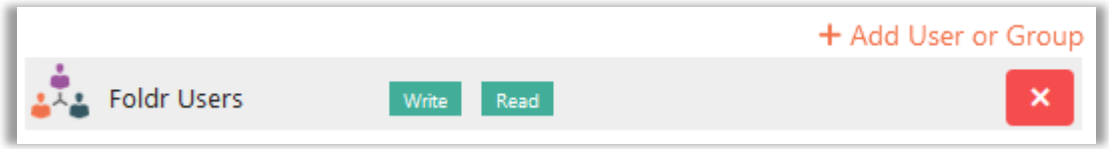
Check Out **–** User / Group will be allowed to check out files which marks them as being worked upon for all other users. Others will be unable to edit files that have been checked out or overwrite them.

Mange Check Outs – User / Group will be able to remove the checked-out status on any file on the share.

Email Tab:

Receive Emails (Inbox) – User / Group will be permitted or denied the ability to use the Inbox feature when sharing a folder. Inbox allows a shared folder to receive files from email attachments received directly to the Foldr appliance.

The Foldr Users Group (Everyone)



Throughout the administrative Foldr Settings area, a built-in security group labelled 'Foldr Users' is used to apply permissions to all users of the system.

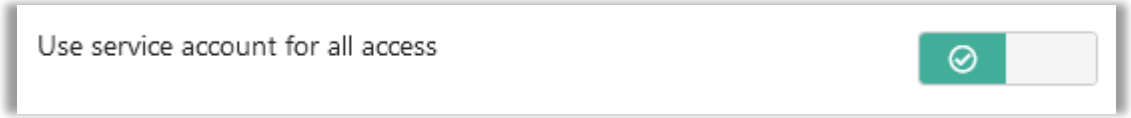
As an example, when a new share is created, a default share permission entry for 'Foldr Users' with Read & Write permissions is assigned. As stated, Foldr automatically respects the existing permissions structures in place. If a user only has read access to the share in question (backend file server permissions) they will only have read access to that resource, even if 'Write' permission is configured to either their specific account, a group that the user is a member of or Foldr Users in the dialog box above.

If the user does not have permission to access a share on the file server, it will be automatically **hidden** from the Foldr interface, regardless of the fact that the Foldr Users group has read/ write.

Overriding Permissions

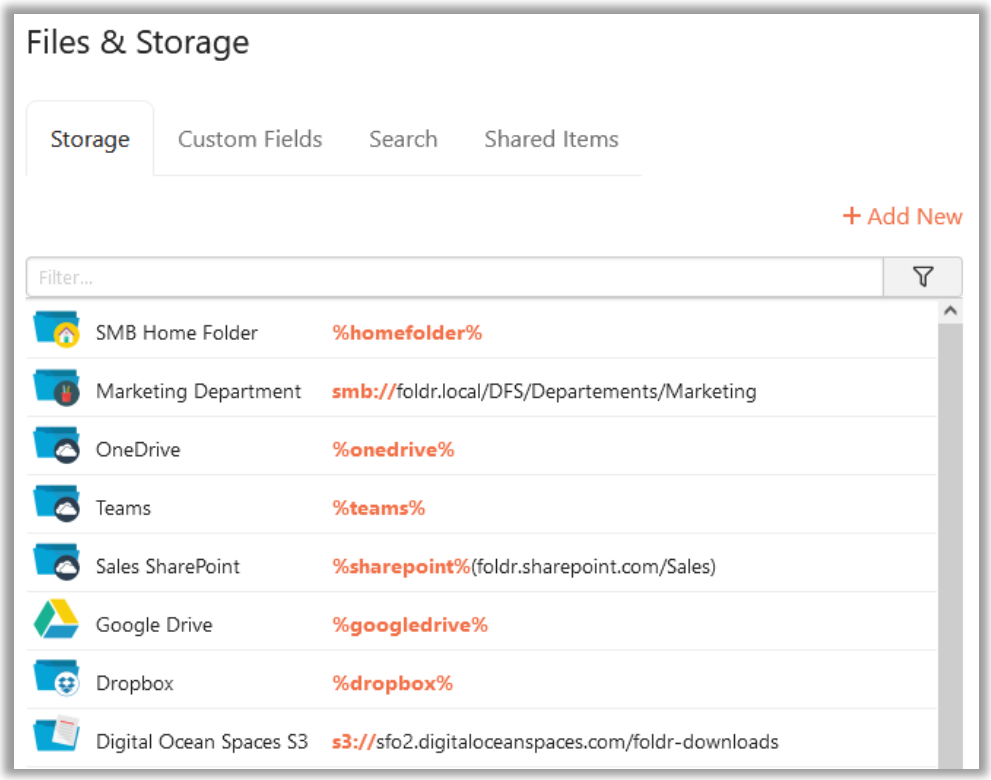
It is possible to override the backend file server permissions by connecting users to storage using alternative credentials in the form of a storage service account. This could be useful to connect to a storage location that a user may not typically have access to or could be hosted on a standalone storage system such network attached storage (NAS).

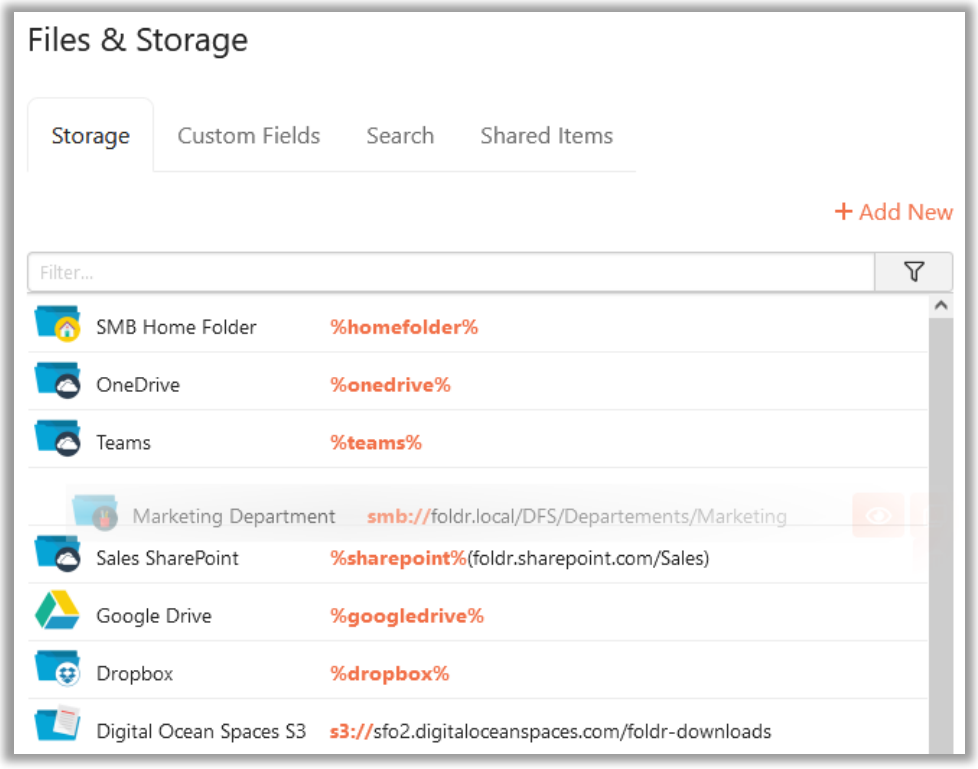
To override a user's permissions, select a service account on the advanced tab in the share configuration screen in Foldr Settings and enable the toggle labelled 'Use service account for all access'



Changing the Order of Shares

The order that shares are presented to users can be changes by **dragging and dropping a storage item** within ***Foldr Settings > Files & Storage*** to its desired location in the share list. Users will see the updated storage list they next time they log into the Foldr web, mobile or desktop apps.





8. Sharing Content in Foldr

Foldr allows users to share individual files or entire folders with users or groups inside your organisation and with external third parties via short URLs, called Public Links. Public links may require no authentication at all to access them, or they can be secured by a static password, or the recipients nominated by their email address. These are referred to as secure links.

By default, the ability to share content internally or externally is disabled and must be enabled by the administrator on a storage item basis. To enable (or deny) file sharing, either add a permission entry for the users or groups that you wish to permit / restrict the feature for, or edit the Foldr Users group permission if you wish to apply the sharing feature to everyone.

IMPORTANT – Where files/folders are being shared from SMB shares, **a service account must be configured on the Access tab in *Foldr Settings > Files & Storage*** and the service account must have sufficient permissions to access the data stored upon it. The service account credentials are used transparently to retrieve the file / folders on behalf of the recipient before delivering it to the user. Likewise, where sharing recipients are allowed to upload to shared locations, the service account is used to perform the write operations in the background.

Share vs Public Links & Secure Links

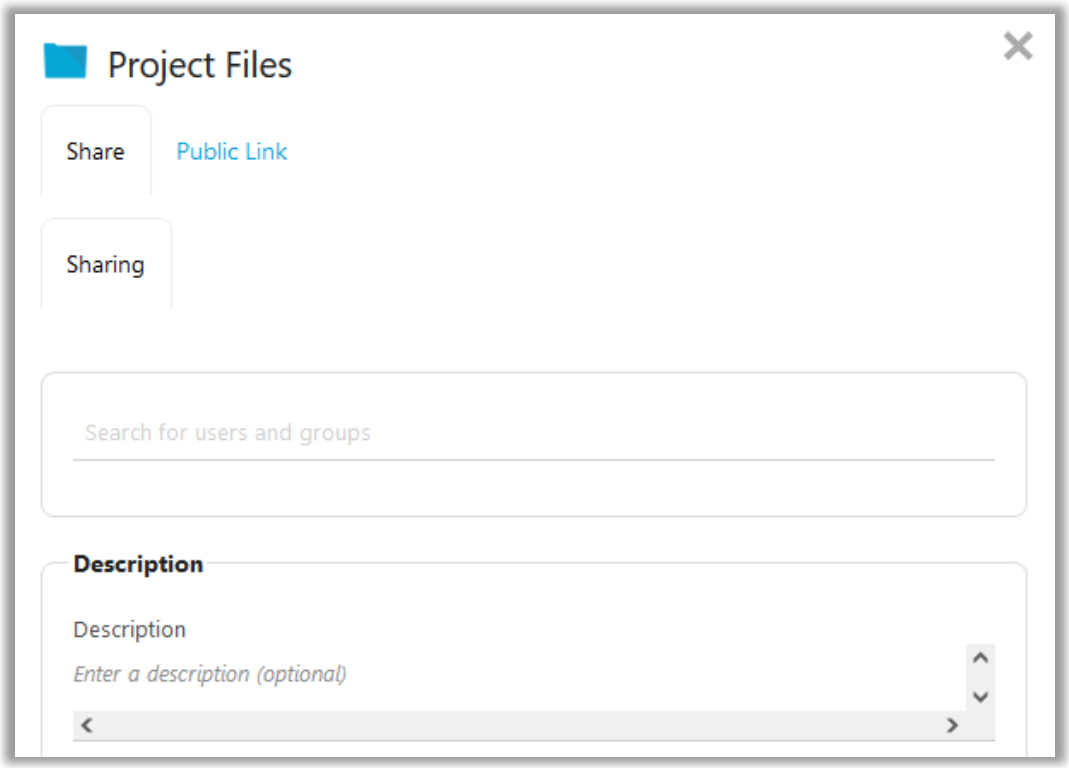
When enabling sharing In the sharing permissions dialog, '**Share with others**' refers to sharing content with other users inside the organisation. i.e. the user will need to sign into Foldr to access the shared items. Shared files and folders will appear in a user's 'Shared with Me / Shared by Me' as appropriate.

'**Create Public Links**', if enabled, allows a user to create short URLs, called Public Links to share content with third parties. By default, no authentication is required by the third party using a Public Link however they may optionally be protected by a static password.

'**Create Secure Links**' if enabled, allows a user to create public links as above, but the links 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. Standard secure links will provide read-only access to files being shared.

'Create Secure Writable Links' if enabled, in conjunction with the permission above, gives the user sharing a folder externally/publicly the option to allow an external user (i.e. the user interacting with a secure link) the ability to upload files to the shared folder. The recipient cannot modify files directly that are shared but can upload their own files to the shared folder. The Foldr server will automatically organise files that are uploaded to secure shared folders using subfolders, one for each Sharee under a root directory labelled 'Foldr Uploads'. These are dynamically created when a user uploads their first file back to the shared folder.

Example sharing UI from Foldr web app:



Public Links are useful for sharing files securely with external organisations or those without an account on your network. Using the granular permissions available you can select which specific users or groups can Share or create Public Links and from which shares. Public links can be restricted so only certain users can access content shared via short URLs.

Enabling Sharing Features for Users

Dedicated knowledgebase articles are available for enabling the various sharing modes in Foldr on the online KB:

Share (with others inside the organisation)

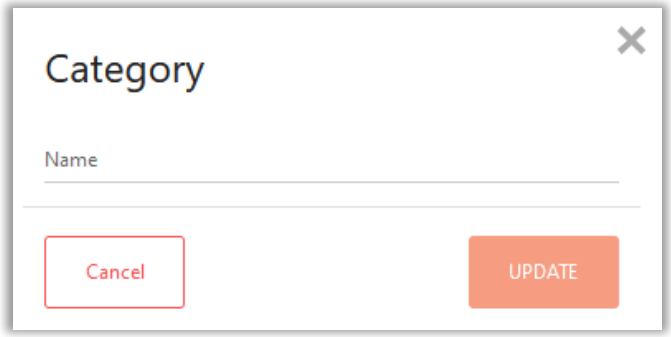
Public Links

Secure Links

Sharing Categories

The Foldr administrator can create categories for use when users are sharing content with others. Categories allow users to sort items that have been shared with them by type and allow for logical organisation of content that is available under 'Shared with Me'. A typical use would be to create a category for each subject in an education environment or per project / department.

Categories can be configured within ***Foldr Settings > Files & Storage > Shared Items.***



Sharing Modes / Permissions

When a user shares a folder with others inside the organisation, they can choose from one of three sharing modes. The default wording of the sharing modes is intended for education-based users. These are 'Hand-out', 'Hand-in' and 'Manage'. In a business / corporate environment, these modes can be changed so they labelled 'Duplicate', 'Submit' and 'Manage' respectively. The sharing mode can be switched between Education and Business within the Customise section of the Foldr Settings interface.

Hand-Out / Distribute (read only) – The folder and all files / subfolders within are available to view / download.

Hand-In / Submit (read all files & write back to a user specific sub-folder) – The folder and all files / subfolders within are available to download, but users can also upload files back to the shared folder. Files can be submitted either using a standard upload action (drag and drop) or by adding (copying) a file using the + button from another share such as the home folder.

Any user files uploaded to the shared folder with HAND-IN permissions are automatically sent to a *Foldr Uploads* directory (upon first upload if it doesn't already exist) and a sub folder for each user handing in files is created by the system automatically. i.e. Foldr organises the files being submitted back to the shared folder ready for collection by the user that owns the shared folder. Example below shows the directory structure of a shared Hand-in folder called 'Project'

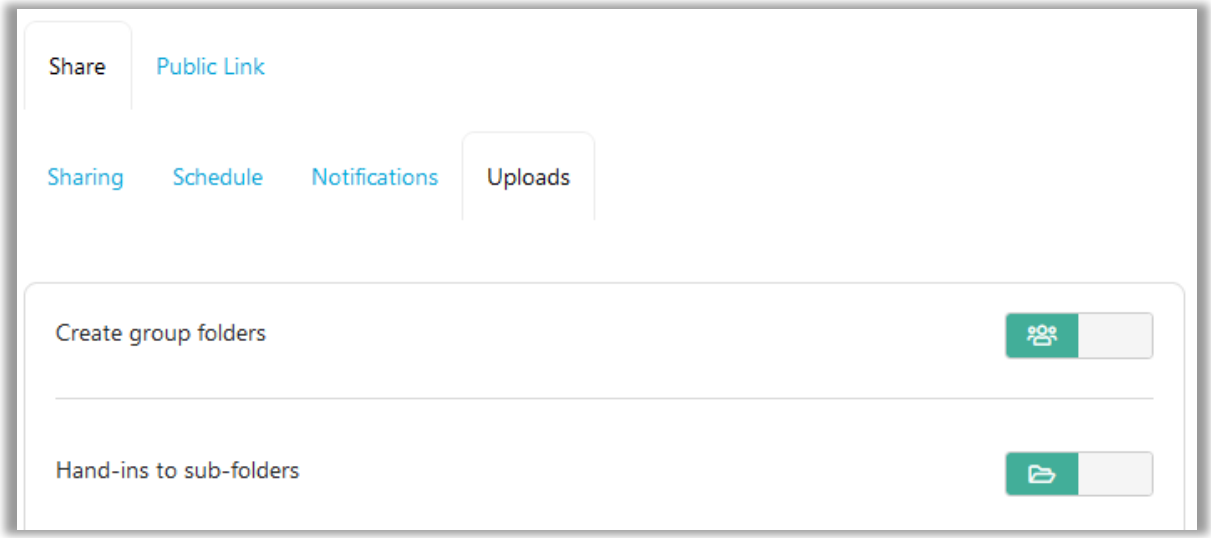
--Project--

- Foldr Uploads
  - User A
  - User B
  - User C

With a hand-in folder, each user using writing files to the shared folder will only see their own files that have been uploaded. This is by design and can be useful in education environments to avoid plagiarism issues.

Hand-in folders are designed for project collaboration or giving educators a quick and easy way to create student work submission areas on a network.

When a user creates a hand-in folder there are some additional options available in the Uploads tab within the Sharing dialog box. By default, these options are disabled.



Create group folders within uploads folder – If enabled, automatically creates a folder within Foldr Uploads named after the group that the content has been shared with. This is designed for situations where a user has shared the same files with multiple groups of users. An example being a collection of resources that an educator has shared with numerous classes and each class is submitting files back to the same Hand-in folder.

Allow *hand-in* uploads to subfolders – If enabled, allows users to upload files anywhere within the folder structure, rather than the default location which is in the root of the hand-in folder.

Upload (read, write new files) – A user / group assigned Upload permissions will have read only to all files inside the shared folder, but will be able to upload files anywhere in the folder structure.

Manage (read, write & delete) – Any user / group assigned manage rights will be given full permission over the files within the shared folder.

Manage permissions can be useful for creating collaboration project folders where it would be desirable for others to have full access to a folder that may reside in a secure location (such as a user's home folder) or assigning higher privileges on a Hand In / Hand Out folder to another user.

Sharing Deadlines

When a folder is shared with others inside the organisation, the user sharing the content can optionally select a deadline.

Three types of deadlines are available: Soft, Hard and Final

Soft Deadlines – A soft deadline is essentially a warning, the person using the shared resource (such as a student) may still access the shared resource after the deadline has passed and download / upload files back to the folder as normal.

Hard Deadlines - When a hard deadline passes, the files within the shared folder are still available to download but the person using the shared resource will be **unable** to upload files back to the folder

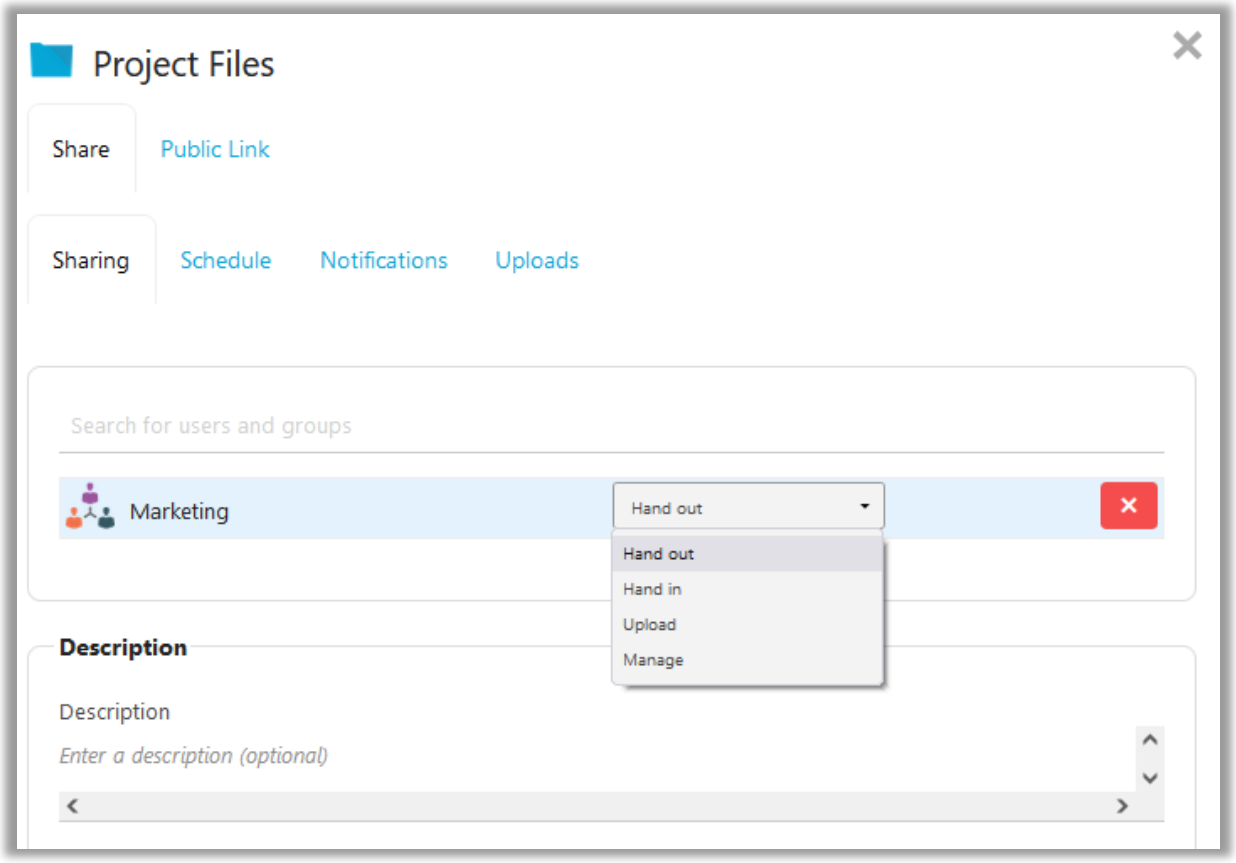
Final Deadlines - When a final deadline passes, the shared folder becomes inaccessible to other users and is automatically removed from their 'Shared with Me' area.

Sharing Example (with others inside the organisation)

Example steps (web app) for a user sharing a folder called 'Project' with others inside the organisation

1. Click Share in the web app context menu or navigate into the folder and click the share icon at the top of the screen.

2. In the Share tab search for users or groups to share the resources with. If the user wishes to create a Public Link instead simply ignore step 2 and move to step



3. Select the sharing mode that applies to the user or group (HAND-OUT, HAND-IN, UPLOAD or MANAGE)

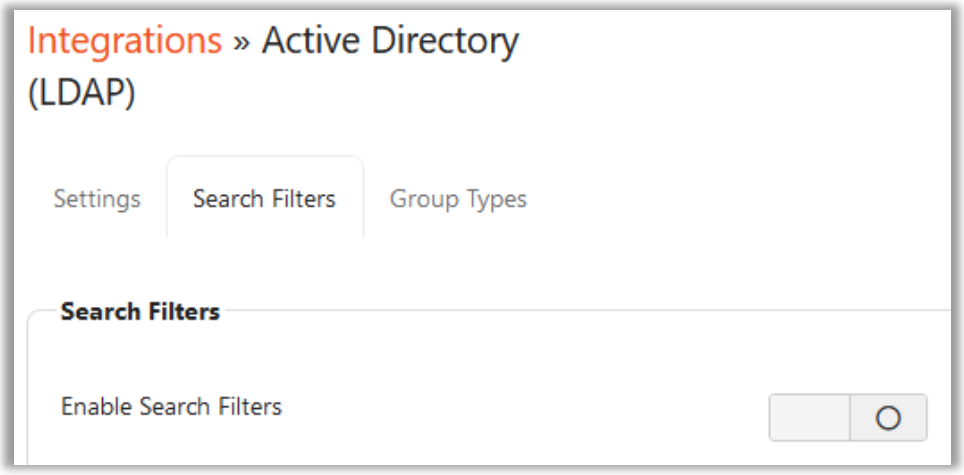
4. Optionally select a category, deadline, and upload options if it is a hand-in folder.

5. Click **SHARE**.

Controlling sharing search results with Search Filters

Providing the appropriate features are enabled, users can search Active Directory within the scope of the configured Search DN when creating groups, sharing files/folders, and using delegated password reset. By default, Foldr will use the main appliance Search DN to query the directory, but in some cases, this may be undesirable, and you need to contain search results to specific groups/objects in the

Active Directory. This can be controlled through the search filter function within ***Foldr Settings > Integrations > Active Directory (LDAP) > Search Filters***

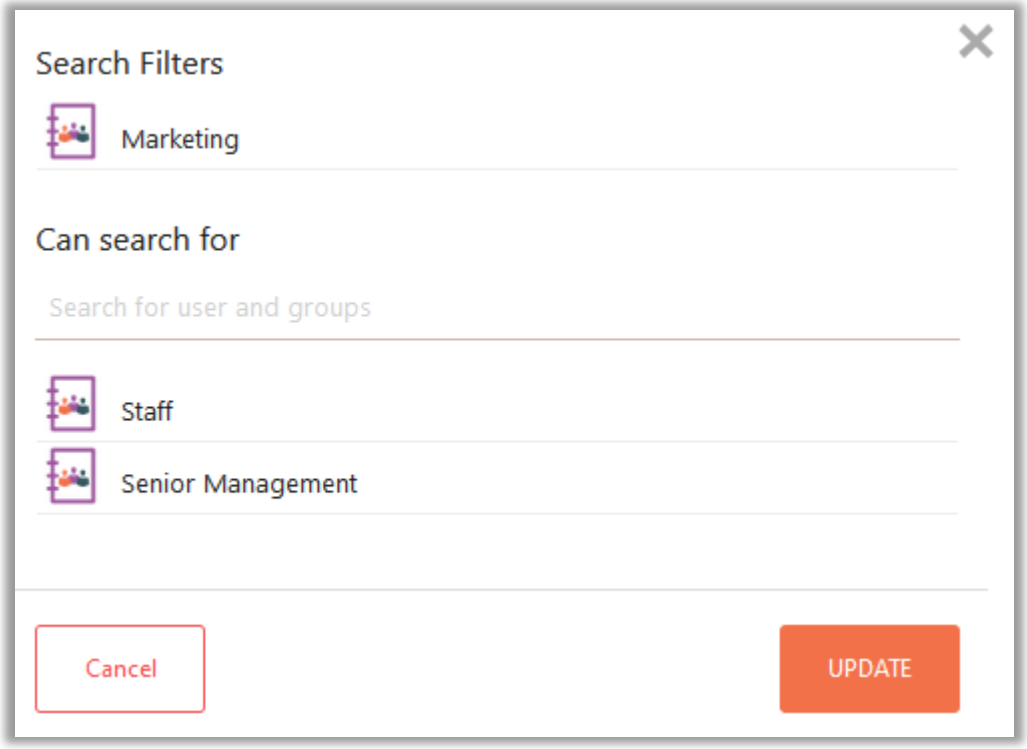


Consider All Users / Groups

IMPORTANT - The search filter is disabled by default and as such users will be able to search the scope of Search DN(s) that are configured within ***Integrations > Active Directory (LDAP)***.

If the search filter is enabled but no users/groups are configured, the result will be that users in Foldr will be unable to search Active Directory when sharing, populating groups or using delegated password reset. As such, you should be mindful to provide suitable search criteria for all groups / users.

Example – Allow Marketing users to only search for users within security groups 'Staff' and 'Senior Management'

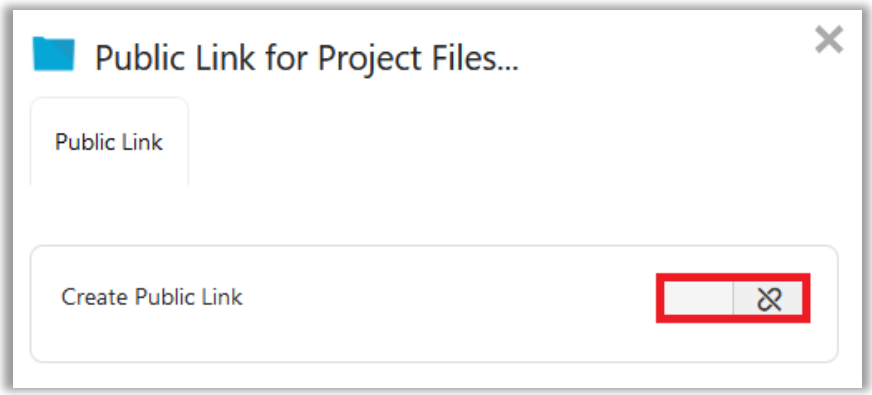


Sharing Example (Public Links)

Example steps (web app) for a user sharing a folder called 'Project' with others outside the organisation:

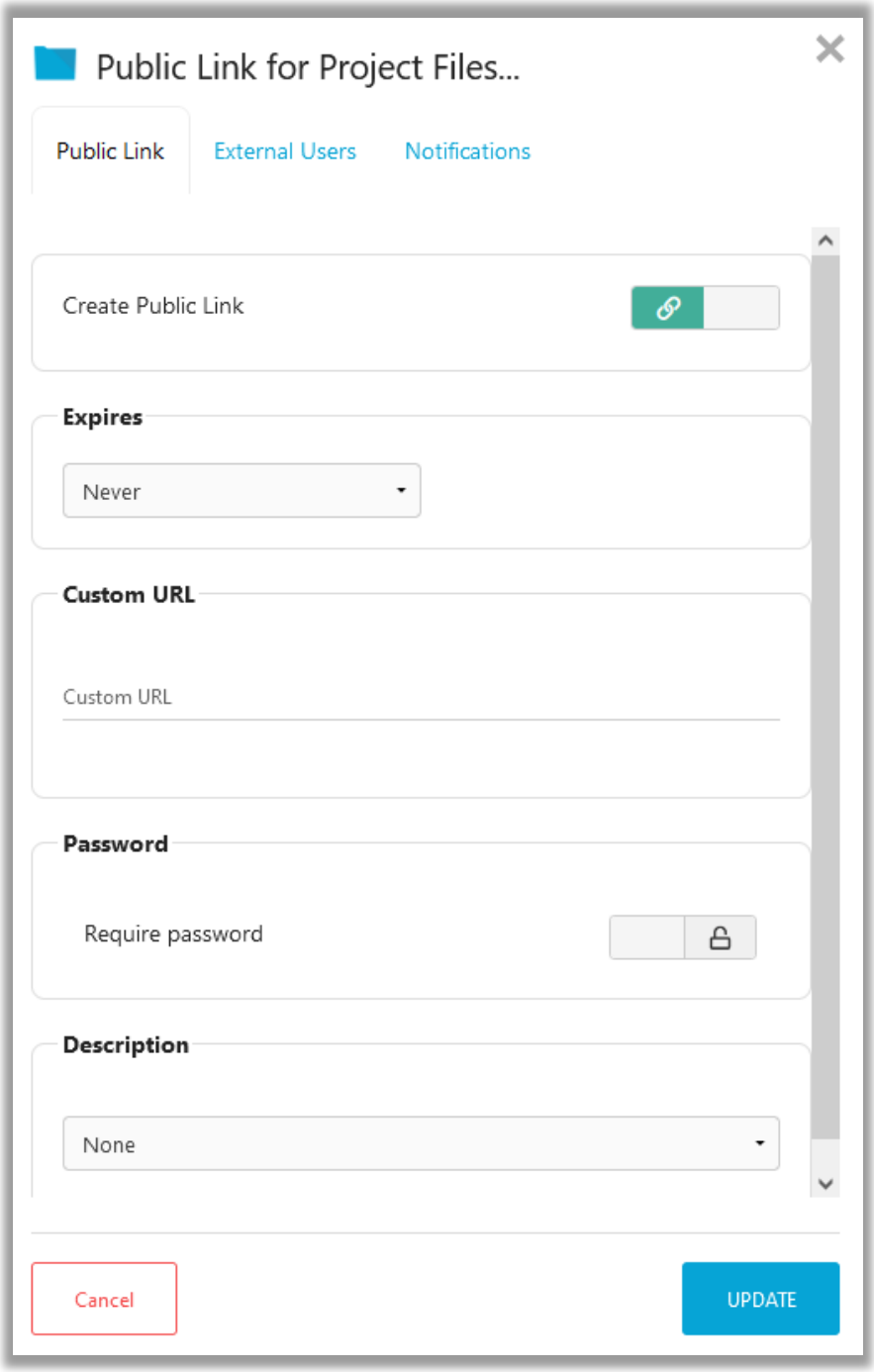
1. Click share icon on the right of the web app interface (alongside the folder name) or navigate into the folder and click the share icon at the top of the screen.

2. Enable the Create Public Link toggle/switch.



New options and tabs will become visible in the sharing dialog.

At this point the user can click Update to create a new basic public link. Additional options are available to set a description, expiry date, friendly/custom URL, and security options to protect access to the link. Static passwords can be configured to protect access to the link. Finally, external users may be entered into the External Users tab by their email address and email notifications will be sent to the recipients (Secure links).



3. Click **Update** and the Public Link to gain access to the file/folder will be displayed.

Customising the appearance of Public Links

Public Links can be customised to change their appearance. This can be useful if they are being embedded into a web page on another service such as a website or LMS /VLE:

The following options are available by appending the following query string options to the URL. The following options may be used:

embed=1|0 (0 is default – 1 removes header text and download button)

modified=1|0 (0 is default – 1 removes the modified date column)

extensions=1|0 (0 is default – 1 removes all file extensions)

order=modified&sort=desc changes the sort order of all files and folders in the link to show the **latest** modified item **first**

order=modified&sort=asc changes the sort order of all files and folders in the link to show the **oldest** modified item **last**

previewonly=1|0 (0 is default – 1 removes the inline download button for all files and hides the download button for files that can be viewed in the browser, such as PDF and images).

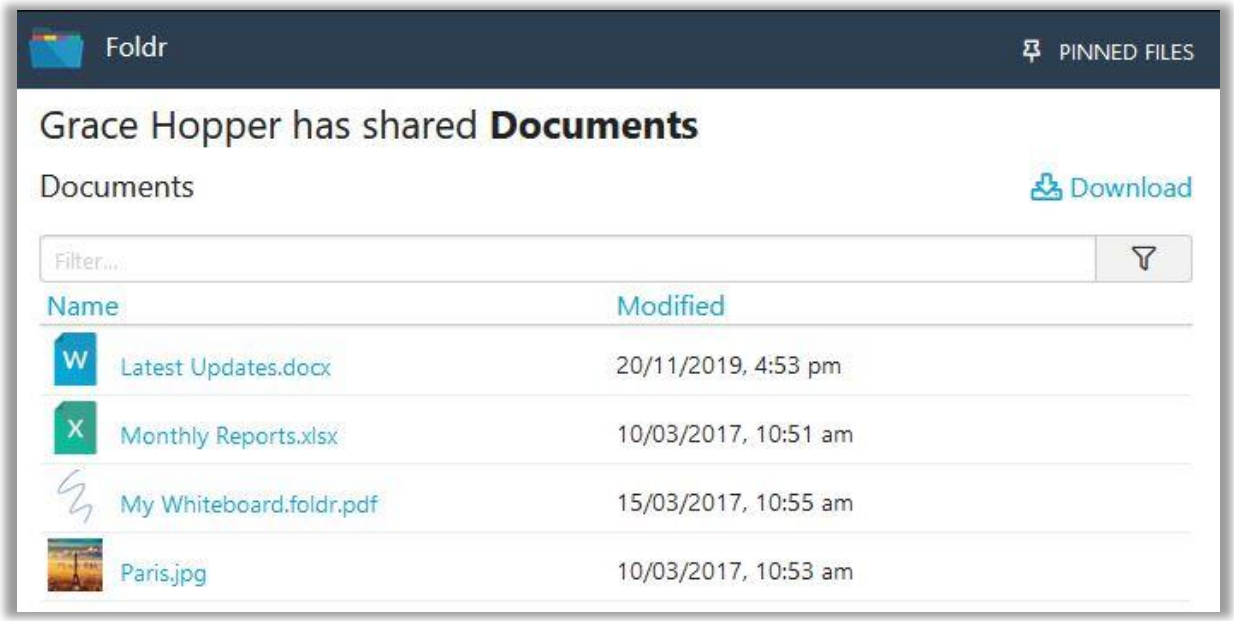
Note – The previewonly option does *NOT* prevent the download of files via other means, such as the browser context menu while previewing files.

One or all these options can be appended to the URL as required.

When testing public links with any of the changes above, it is important that you are not already signed into Foldr as this may change the appearance of the interface.

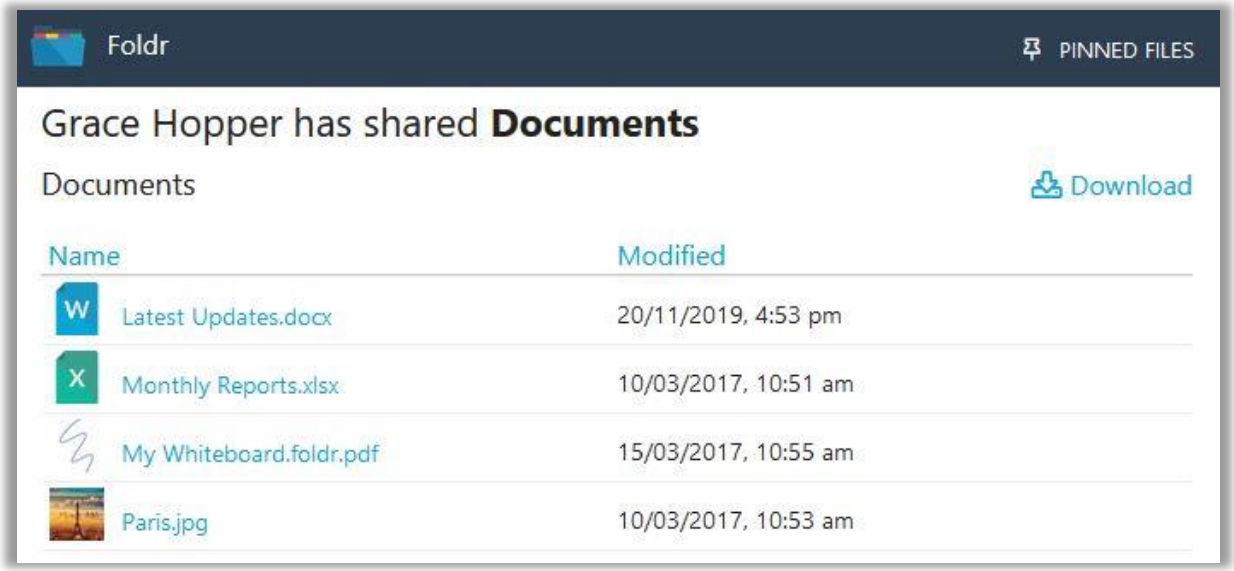
Original Public Link shown below:

https://address-of-foldr/public/link-name/browse



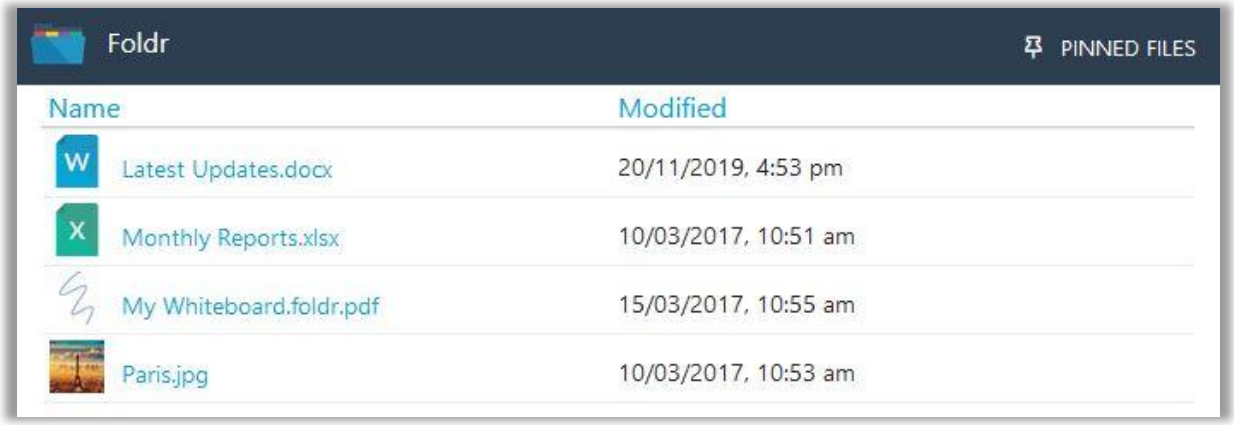
Using **filter=0** to remove the filter box from the public link UI

https://address-of-foldr/public/link-name/browse/?filter=0 (note ../?filter=0)



Using **embed=1** to remove the header text and main download button (note ../?embed=1)

https://address-of-foldr/public/link-name/browse/?*embed=1*



Using **embed=1** and **modified=0** to remove the header text, filter box, main download button and the modified date column

https://address-of-foldr/public/link-name/browse/?*embed=1&modified=0*

Using **embed=1**, **modified=0** and **extensions=0** to remove the header text, filter box, main download button, modified date column and the file extensions

https://address-of-foldr/public/link-name/browse/*?embed=1&modified=0&extensions=0*

Inbox – Receiving Email & Processing Attachments

Inbox is a powerful feature that allows an organisation to use Foldr as an automated mechanism of receiving email attachments and placing them onto a chosen storage location. This can be any location available through Foldr such as an on-premise SMB share or cloud platform such as Google Drive or Dropbox. Users that have been granted permission can enable any shared folder to receive files through the Inbox feature. Each shared folder is given a randomly generated email address, alternatively the user can create a suitable friendly/custom address.

The email addresses generated by Inbox are typically in the format *email-address@foldr-appliance-fqdn*

For example:

invoices@demo.foldr.io

When emails are received by the appliance, they are processed, and the attachments are moved into the corresponding shared folder. An entry is then placed into the user's Activity Feed and the body of the email is accessible using a link provided in the feed.

SMTP & TLS

The Foldr appliance receives inbound email on **TCP port 25**. However, only encrypted SMTP connections will be accepted and processed by the Inbox feature. Plain text SMTP connections will be discarded. The SMTP service running on the Foldr appliance upgrades the connection from plain text SMTP through the STARTTLS command.

Enabling Inbox on the Foldr Appliance

1. Open the SMTP port the appliance firewall (IPtables)

The SMTP service is already running on the appliance, however without modifying the built-in firewall the system will not receive email. As such, TCP port 25 needs to be permitted as required for your environment. Normally Foldr sits behind a perimeter firewall where you would specify what locations email can be accepted from, however this can also be done from the appliance. To do this from Foldr issue the following commands from the system console:

Accept email from any location:

```
iptables -A INPUT -m comment --comment "foldr-admin" -i eth0 -p tcp --dport
25 -j ACCEPT
```

Accept email only from subnet 52.48.127.192/26:

```
iptables -A INPUT -m comment --comment "foldr-admin" -i eth0 -p tcp -s
52.48.127.192/26 --dport 25 -j ACCEPT
```

Should you need to enter multiple subnets, simply issue multiple separate commands as above.

Once you have configured the firewall as required, save the changes with the command:

```
iptables-save
```

Should your firewall rule allow it you can test SMTP (port 25) is available by using telnet:

telnet foldr-address 25

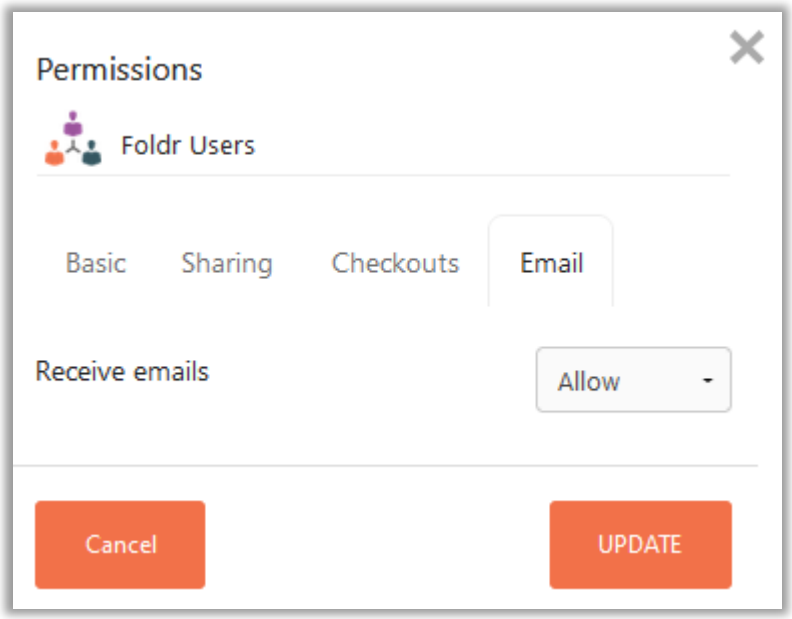
If the system is accepting connections, it will display a *220 ready for transmission message*:

2. Enable the 'Receive Email' permission on shares for users.

As with Share and Public Links, Inbox uses a separate permission entry (labelled Receive Email) available on each storage item configured on the Foldr appliance. As such you can enable this feature for all users by granting '***Receive Email***' permission to the built-in Foldr Users group or individual users or groups as required.

Note that the 'Share with others' permission is also required in the SHARING tab.

Foldr Settings > Files & Storage > Edit Storage Item > Access tab:



3. If the backend storage type is SMB, a suitable **service account** must be configured on the share's Access tab, and this service account must have both read and write permissions to the backend storage / share. If a service account is not configured, the Inbox feature will not work correctly with SMB shares.

Users that have been granted the *Receive Email* and *Share with others* permission will now see the Inbox tab in the Sharing dialog in the web interface.

Routing Email from the Internet to the Foldr Appliance

Domain MX record(s) need to be created so email is sent to the correct host (Foldr)

Whilst you could direct email (using the MX record) directly at Foldr, it is common practice that email is sent through an email security product / third-party service, such as a hosted security provider that processes email before sending it onto the intended recipient server. The example below shows this and points the MX record for email sent to *@demo.foldr.io* at a Trend Micro cloud security product which has been configured to send mail onto the Foldr appliance.

Please note that you cannot point an MX record at an IP address, it should always point to a host, which in turn has an A record pointing at the corresponding IP address.

Example of editing the public DNS zone file:

The '10' prefix in the example shown is a priority value, with zero being highest priority. More information on MX records and priorities can be found here https://en.wikipedia.org/wiki/MX_record.

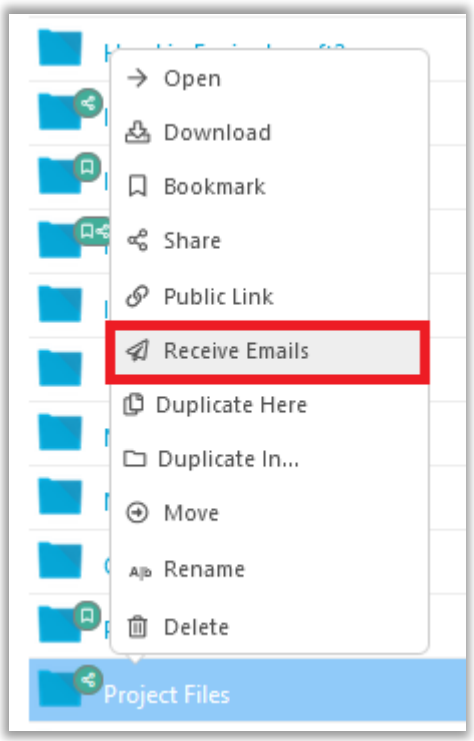
There may be other mechanisms in place inside the organisation to route email internally. The above is given as a basic example of creating a public MX record to allow mail to flow to the Foldr appliance. If Inbox is only to be used inside the organisation, it is not necessary to make any changes to the public domain DNS.

Security Considerations (Spam, Virus & Malware)

The Foldr appliance does **not** provide any form of anti-spam, virus or malware scanning on mail that is received. You should ensure that mail flows through a third-party provider or appropriate security product/service to perform this functionality.

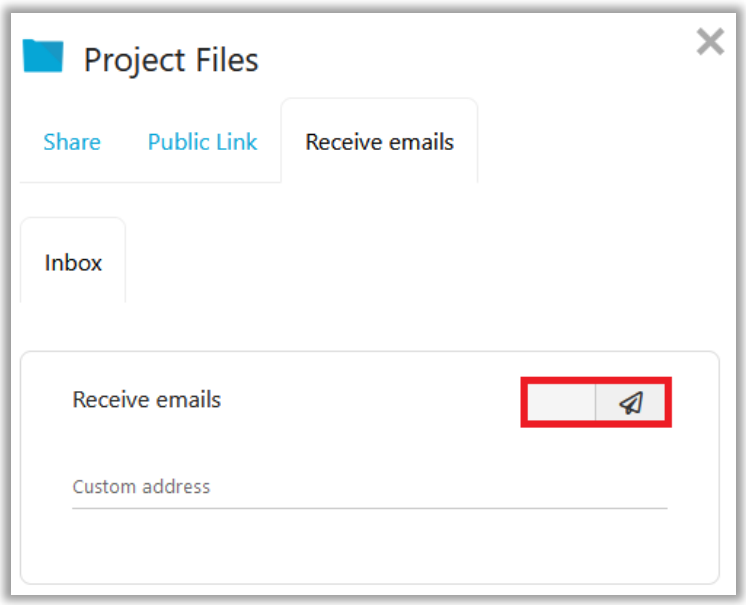
Using Inbox - Web app

On the folder that will be receiving the email attachments / message body using the context menu and select Receive Emails.

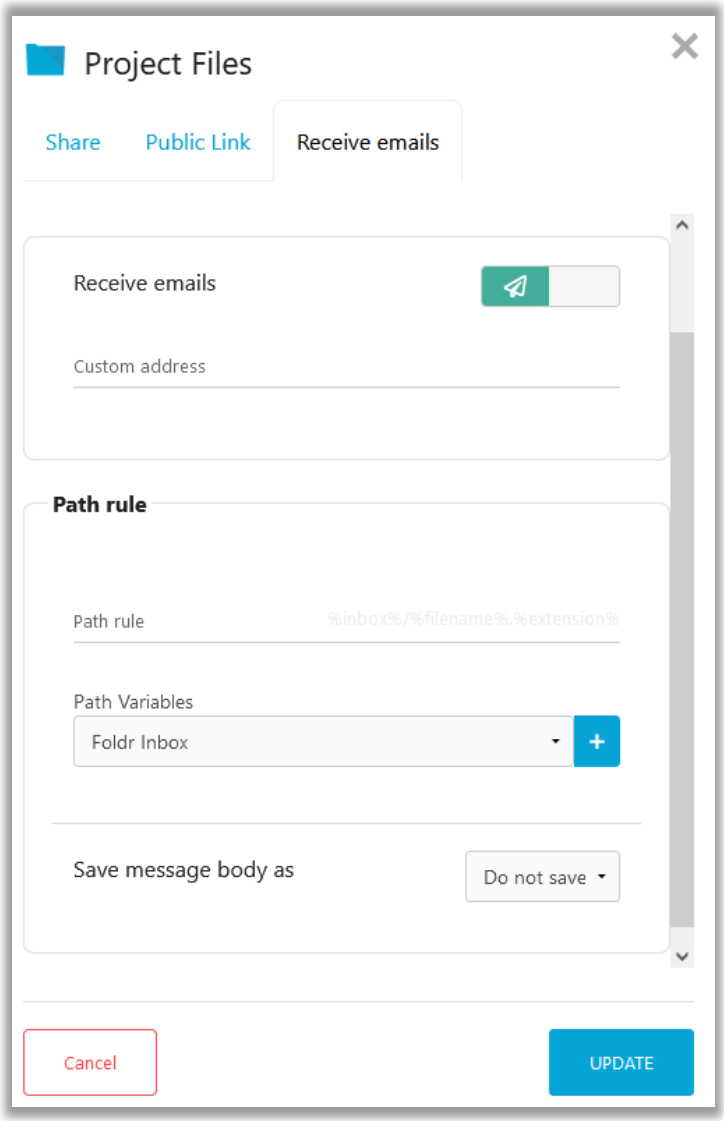


Alternatively navigate into the folder to be shared and click the share icon (top right)

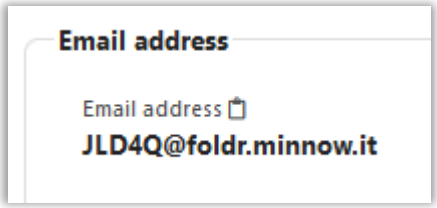
Click the Receive Email tab and enable the toggle for *Receive Emails*



This Receive Email tab will then present you with options for the path rule (where and how to save the attachments), built-in variables to assist building a path rule, whether the message body should be saved along with the attachments and finally if a custom address should be used.

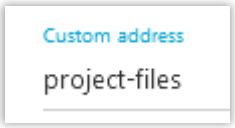


If the Inbox dialog is left with the defaults and you click UPDATE, the appliance will create a randomly generated email address as shown below.

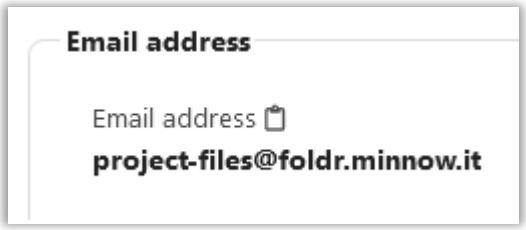


Using a custom email address

It may be preferable to use a custom email address rather than a randomly generated string as the email address for the shared folder. To use a custom address populate the 'custom address' field with the desired address

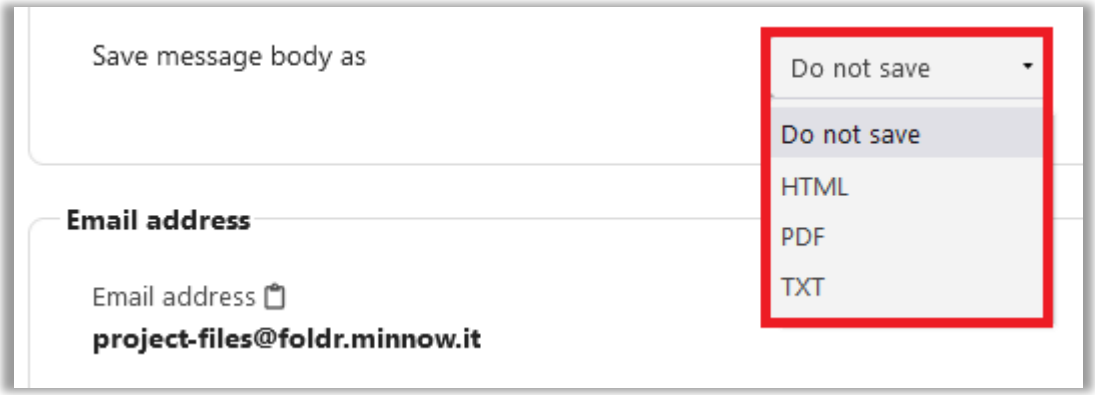


Spaces may be used in the custom address and these will automatically be replaced by hyphens as shown. Click Update and the email address will be changed to reflect the chosen custom address.



Saving the message body of the email

By default, the message body of the email is not saved. However, it is accessible to the end user if they click on the link in the Activity panel on the right of the web app. To save the message body alongside any files that may be attached to the email, use the drop-down menu as shown selecting the file format that the body should be saved in.



Path Rules

You can change the Path Rule for the attachments that are received (i.e. how they are saved within the shared folder). By default, when the first email with attachments is received a directory will be created automatically in the root labelled **Foldr Inbox** and all attachments will be dropped directly into the root of this directory.

This is represented by the default path rule below. You do not need to type over the placeholder text if this rule is suitable.

%inbox%/%filename%.%extension%

Default path rule example - An email with a single attachment is received (called may-invoice.pdf) and would be saved as:

Share-Name/Invoices/Foldr Inbox/may-invoice.pdf

Should another attachment be received with the same name, 'copy' will be appended to the attachment filename.

Using the path rule variables below, it is possible to set custom rules for attachments that are received so they can be organised automatically as required. This could include creating a sub folder for each sender, file type, date received etc:

Available Path Rule Variables for Attachments

%inbox% (maps to “Foldr Inbox”)
%sender_address%
%sender_display%
%subject%
%date%
%time%
%filename%
%extension%

Example 1 - Create a sub folder for each sender's email address to store their received attachments

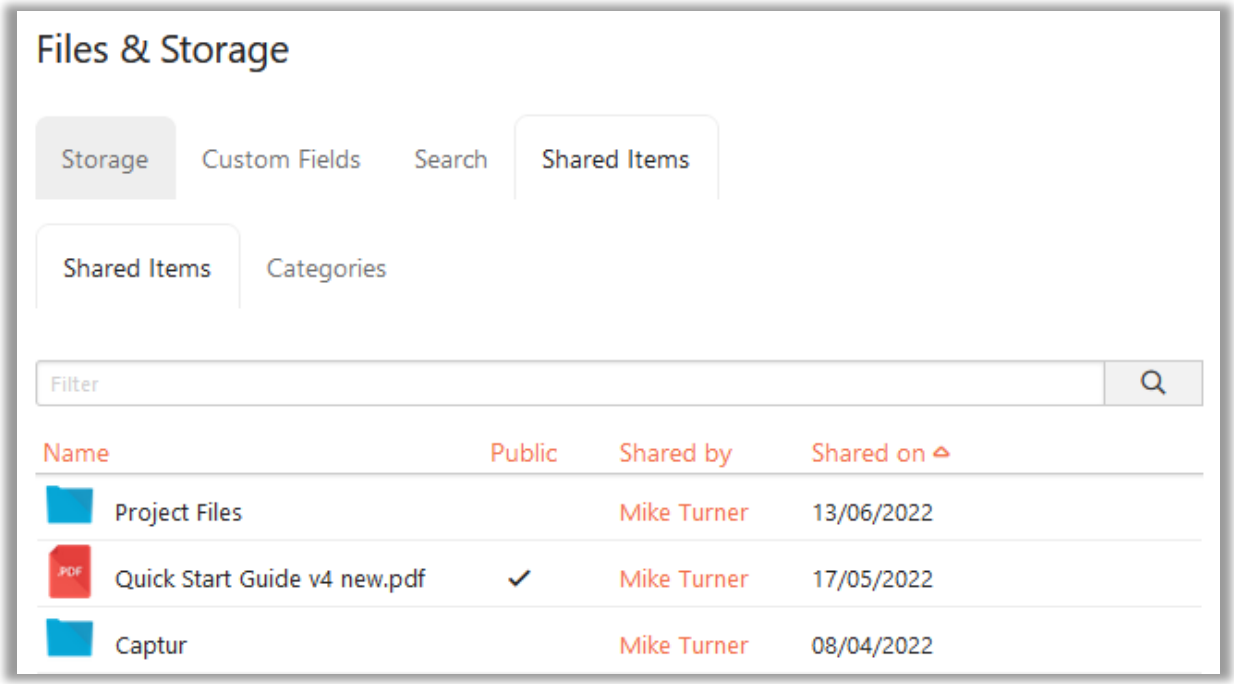
%inbox%/%sender_address%/%filename%.%extension% = Foldr Inbox/sales@minnow.it/may-invoice.pdf

Example 2 - Create a sub folder for each sender's name, with attachments sorted by file type

%inbox%/%sender_name%/%extension%/%filename%.%extension% = Foldr Inbox/Grace Hopper/pdf/may-invoice.pdf

Monitoring Users Sharing

The Foldr administrator can get an overview of what files and folders are currently being shared by using the 'Shared Items' tab in ***Foldr Settings > Files & Storage***. If required, the administrator can remove, and thereby remove access to, any shared item by clicking the in-line X button.



By clicking on a shared item, the Foldr administrator can see further information about the item such as who it has been shared with, what options were selected and file activity logs.

The user that originally shared the file / folder also has access to the activity section in their sharing dialog.

9. Microsoft Office Files, Check Out Permissions and File Locking

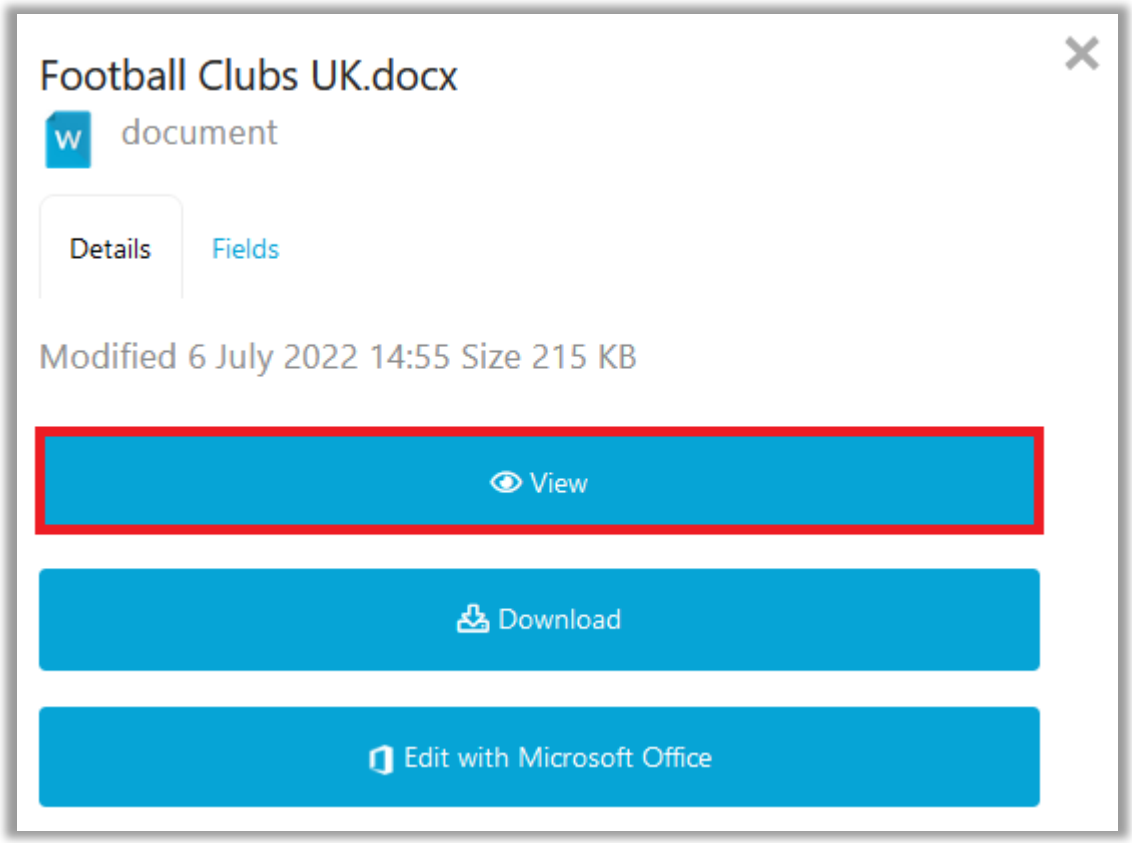
Foldr provides users the ability to edit (and save back directly) Office documents hosted on SMB shares and cloud storage via the web, mobile and desktop apps. Office documents may also be viewed directly in the browser using a Microsoft cloud service to render the files.

Traditional file access over SMB provides a file lock mechanism and Foldr provides checkouts and a supplementary file locking service. The checkout feature informs/alerts users that files are in use and the file lock service prevents other users from making changes or overwriting of files while a Foldr user is working on the file.

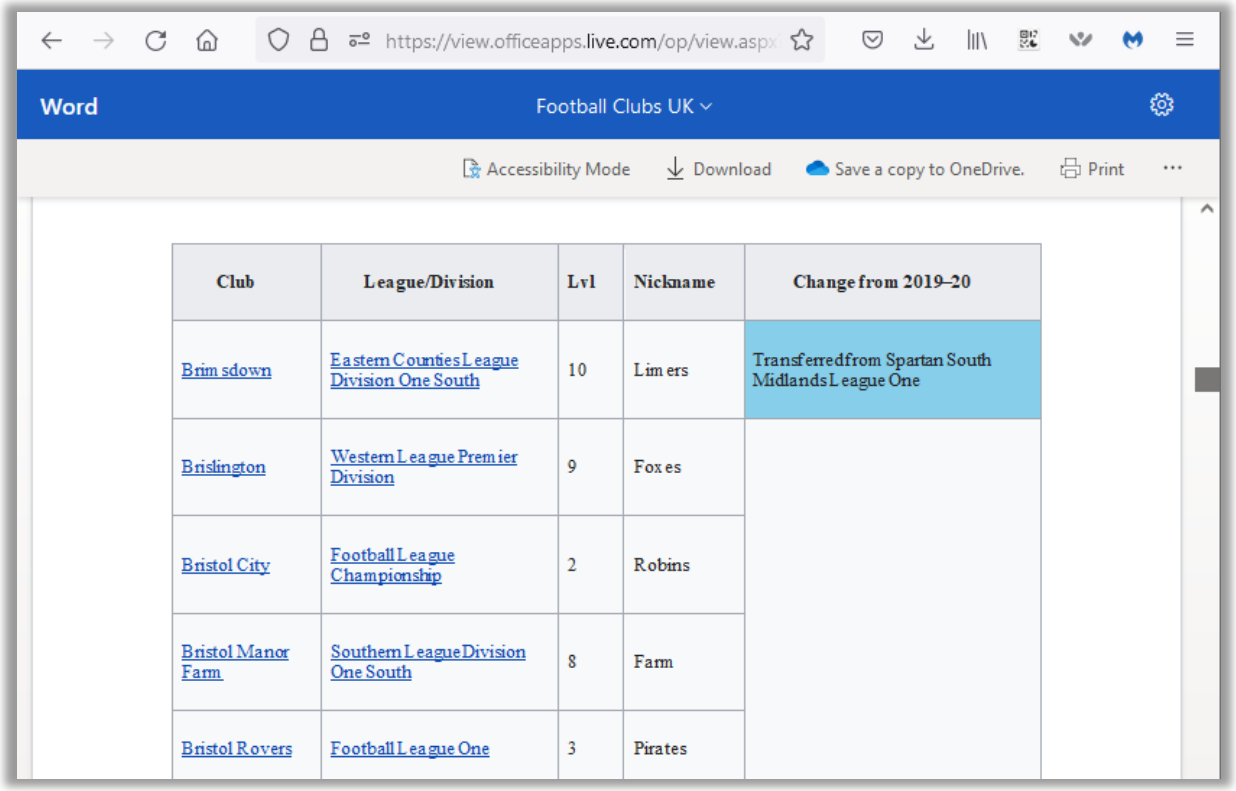
Viewing Microsoft Office documents

While using the Foldr web app, clicking on any Office file (Word, Excel or PowerPoint) will present a dialog where the user can view, edit or download the file.

Clicking View will utilise an online Microsoft service to render the document in the browser. This file will be read only, but provides a convenient way to quickly review files without needing Office applications installed locally.



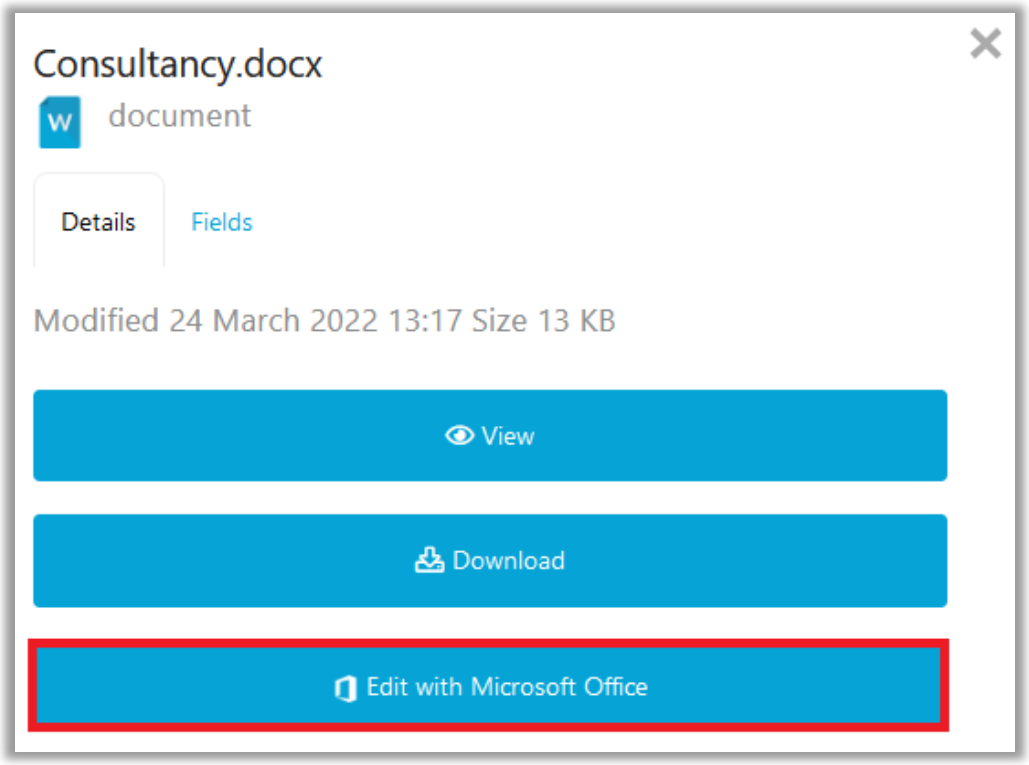
The file will then be displayed in a new browser tab.



Club	League/Division	Lvl	Nickname	Change from 2019–20
Brimsdown	Eastern Counties League Division One South	10	Limers	Transferred from Spartan South Midlands League One
Brislington	Western League Premier Division	9	Foxes	
Bristol City	Football League Championship	2	Robins	
Bristol Manor Farm	Southern League Division One South	8	Farm	
Bristol Rovers	Football League One	3	Pirates	

Editing Office documents

The Foldr web app provides an '**Edit with Microsoft Office'** button when a user clicks on any docx, xlsx or pptx file (legacy Office formats are also supported).



Using the Edit in Microsoft Office button in the web app will launch the relevant locally installed Office application, download/load the file in question where the user can begin editing. When the user clicks Save in the Office app, the file will be saved directly back to the original remote storage location, whether it's on-premise or a cloud-based document hosted in a service such as Office 365 or Google Drive. This direct save-back functionality utilises the built-in Office WebDAV functionality that is also utilised when Office would open/save directly to self-hosted SharePoint sites.

The Edit with Microsoft Office button in the web app removes the need for users to manually download, work locally, save, and then manually upload.

The iOS app provides the same direct editing and save back functionality using either the same backend WebDAV Office support with a dedicated button in the app or using the iOS file provider (Files) mechanism to open and save directly back. The Android app supports direct opening of Office documents and save-back using its file provider.

Users using the Foldr desktop apps for Windows and macOS can interact with Office documents in the same way as any other drive in Explorer or macOS. Double clicking documents in the drive will open the Office application and the file will be ready for editing.

Office documents hosted in Office 365

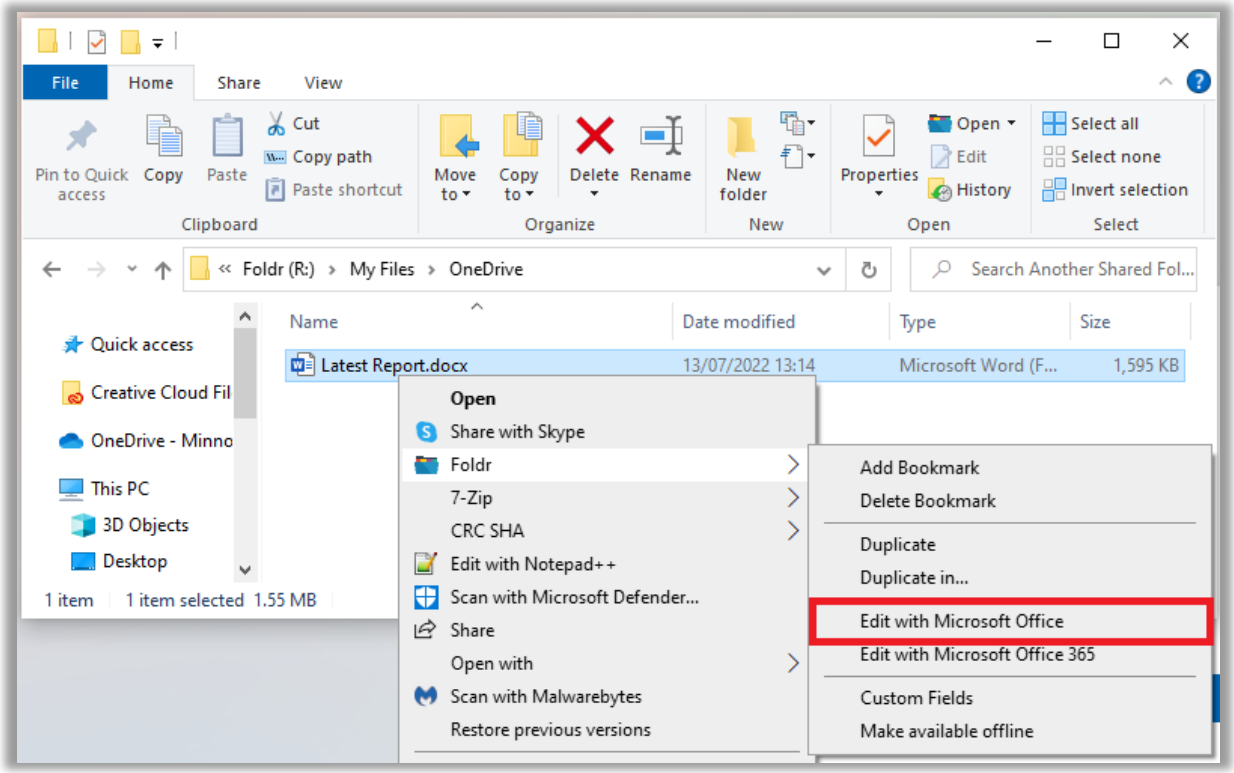
Documents hosted in OneDrive, SharePoint Online or Teams can be edited via Foldr users in various ways. Users using the **Edit with Microsoft Office** button will open the file directly from its Office 365 URL and behaves identically from using the Office applications natively with office.com.

The Office AutoSave function will appear **ON** in the Word, Excel and PowerPoint app and all changes are saved back automatically to OneDrive, SharePoint or Teams as expected as the user makes their changes. The user is not required to click save in the Office apps.

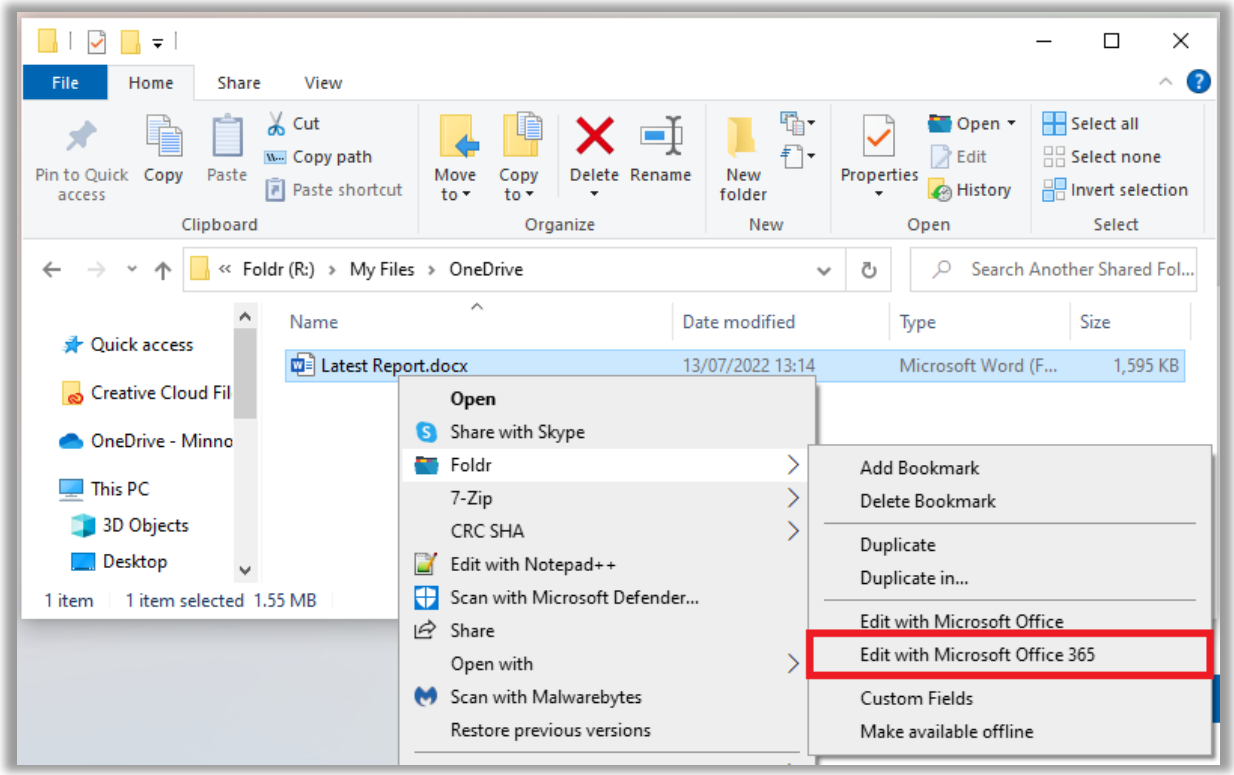
NOTE - Using *Edit with Microsoft Office* from any storage location other than Office 365 will not show AutoSave enabled. However. clicking save in the Office application will save the file back to its original location (SMB share, Google Drive etc)

The Windows and macOS Foldr apps provide a feature called Office Assist to allow the same native/direct editing from Office apps when double clicking Office files from the drive in Explorer or Finder. This may be enabled in the local client app settings, or enabled centrally for clients on Foldr server using an App Profile.

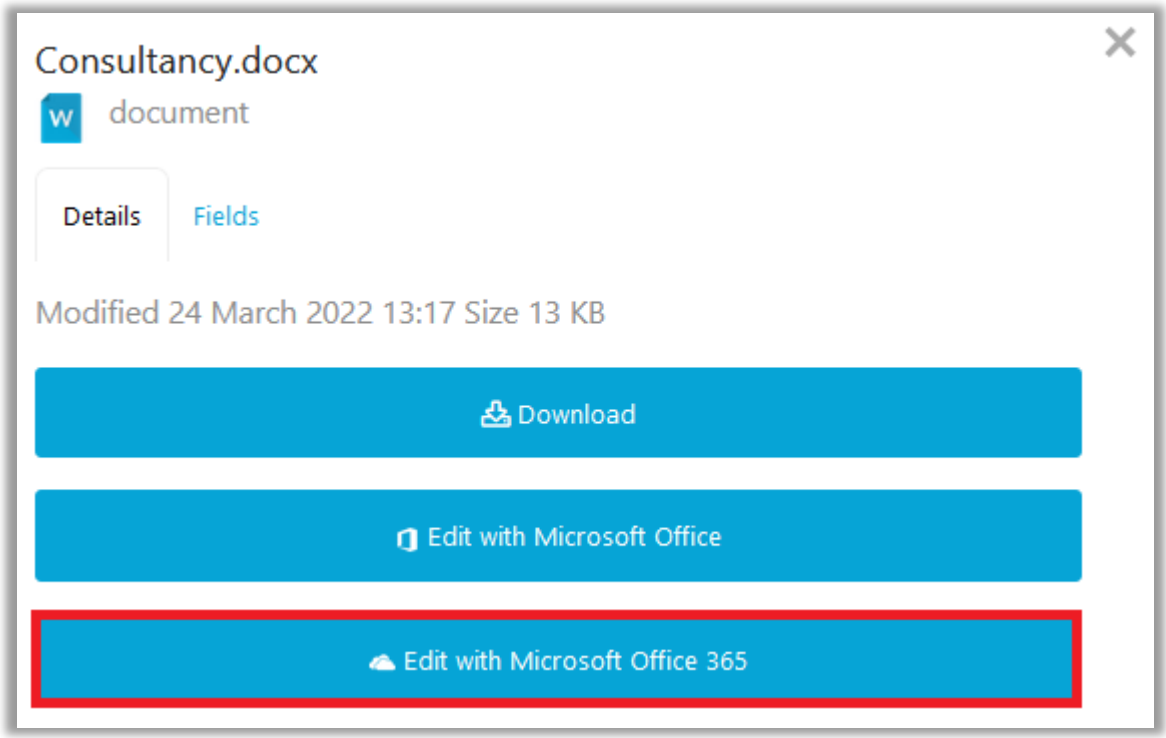
Edit directly with Office Assist (local Office app):



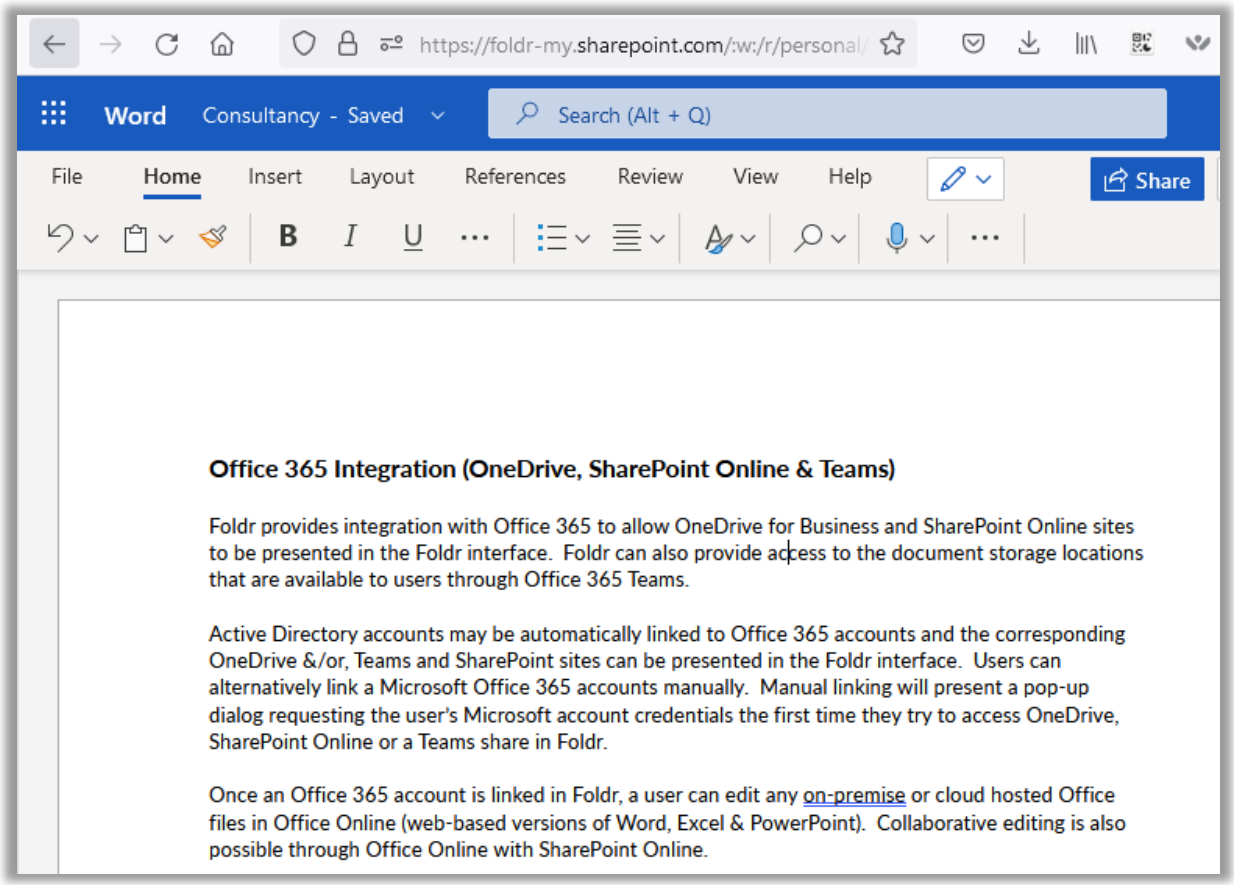
Edit with Office 365 web apps:



Users using the Foldr web app can use **Edit with Microsoft Office 365** button to launch the cloud-based 365 web apps



The browser will open the Office 365 web app with the file ready for editing:



Foldr also provides users the option to launch the locally installed Office apps or browser-based Office

365 web editing apps for Word, Excel and PowerPoint files using the Foldr context menu in Explorer and Finder. The Office 365 web-based apps may be used for documents stored on any storage type (i.e. the files may reside on an on-premise SMB share, or some other cloud storage such as Dropbox or Google Drive). Once the user has completed their edit in the Office 365 web app, the file is sent back to its original storage location.

Office documents hosted in Google Drive & Google Docs, Sheets & Slides

Office documents hosted in Google Drive can be edited using locally installed Office apps, or web-based editing tools hosted in Google Workspace. It is also possible to use web-based Office web apps providing Foldr is integrated with both Google G-Suite/Workspace and Office 365.

Using the web app, users may use the Edit in Microsoft Office function in the same way as documents stored on SMB shares or any other location, note that the AutoSave function in Office will not be active as this only applies to Office 365 storage.

Native Google Docs, Slides and Sheets files may be edited from the Foldr web app using an Edit button or by double clicking on them in the Windows or macOS drive mapping apps. This will launch the Google docs web-based tools. Other Microsoft Office documents hosted elsewhere, such as an SMB share or cloud storage such as Office 365 may also be edited using Google Workspace web apps and the changes are written back to the original location once the user has completed their edit. This feature works by uploading the Office file to the users Google Drive, converts it from .docx, .xlsx or .pptx into the relevant Google format, and once the edit is complete, the file is converted again back into native Office format before being downloaded back to the SMB share or other cloud location.

Check Out Permissions

Foldr provides an optional permission on each share called 'Checkout' that can be used to make other users aware that a file is being worked on. When a file is checked out, other users will see a padlock on the file in question and they will be unable to overwrite or make other changes to the file, such as directly edit the document through Microsoft Office.

The server enhances this feature with the option of using an SMB file lock service to automatically hold files open while they are checked out. This will prevent others from making changes to a file outside of Foldr, such as via a standard mapped drive in Explorer or other application.

Enabling the Check Out Permission for Users

The Check Out feature/permission is enabled on a per-share basis and is granular in the same way as any other share-level permission in Foldr. i.e. it may be enabled for all users or specific users or groups as required.

Edit in Microsoft Office and Automated Check Out / Check In

The Foldr web app 'Edit in Microsoft Office' feature utilises the built-in WebDAV mechanism in Microsoft Office to allow users to easily download, edit Office files and save directly back to the server.

This feature in Office relies on and automatically uses file locks when a document is opened for editing from the browser in both Windows and macOS. The file lock and subsequent file release process is applied automatically in Foldr as a check out and check in when the user closes the document.

NOTE – Because Office relies on the file lock mechanism to function, files are automatically checked out and in when a user uses the Edit in Office button regardless of whether the check out permission is enabled on the share.

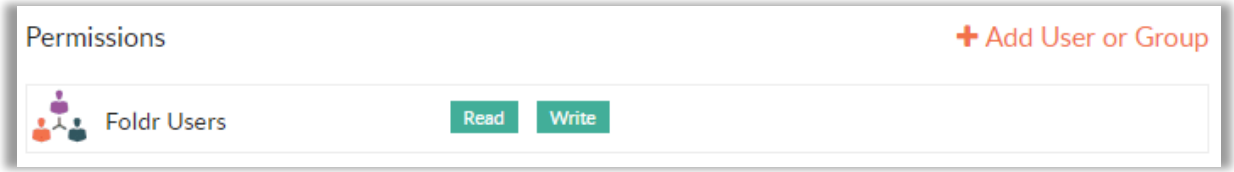
Read-only SMB share recommendations

If read-only shares are being presented to users/groups in Foldr it is recommended that the administrator DENY the check-out permission to any users that have read-only access. By denying the check out permission, the Edit in Office button is hidden from view in the web app. This will prevent the possibility of a user inadvertently checking a document out that they cannot write back to the server. Providing the read-only user closes the Office application, the file will be checked back in automatically by the Foldr server.

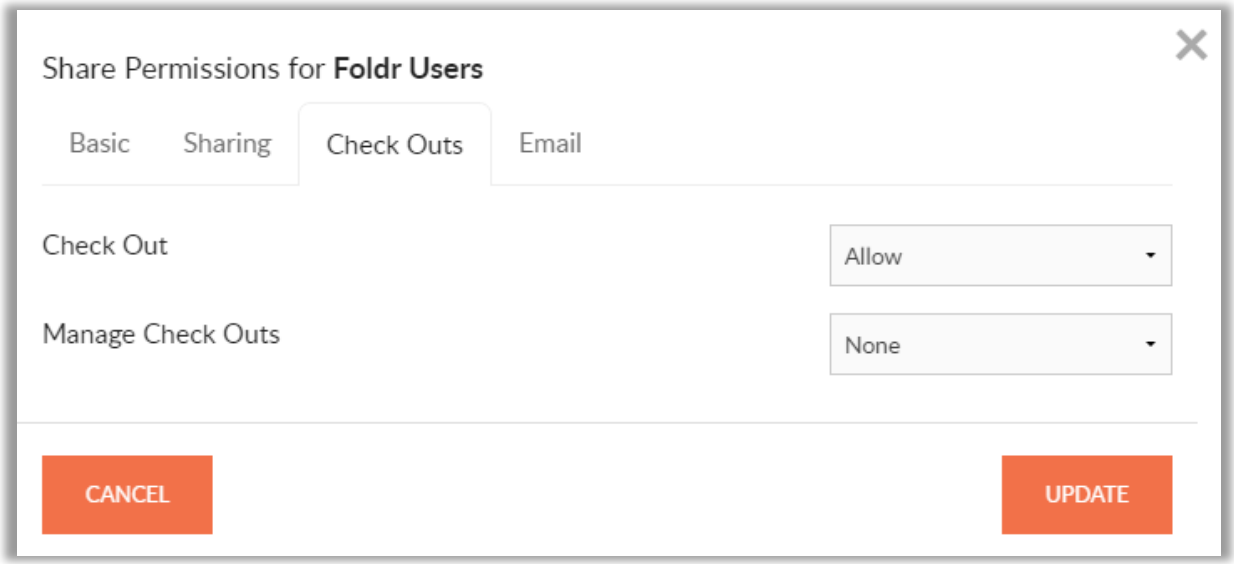
Enabling the Check Out Permission for Users

To enable Checkouts, navigate to ***Foldr Settings > Files & Storage*** and edit the storage item in question. Click the Access tab and scroll down to the permissions section at the bottom of the screen and either edit the 'Foldr Users' group (which represents all users) or add a specific AD user/group as required.

NOTE – Where checkouts are only enabled for a specific group of users, due to the fact the feature relies on checkouts as a background process, the Edit in Office web app button will be hidden for all other users that do not have checkout=allow permission on the share.



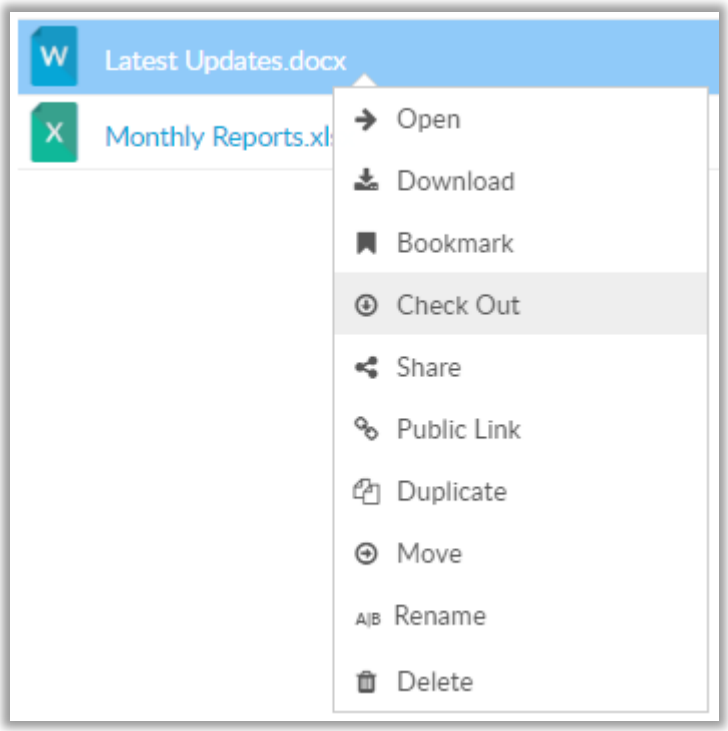
When editing the user / group permission, click on the Check Outs tab and enable the Check Out permissions by selecting **Allow**



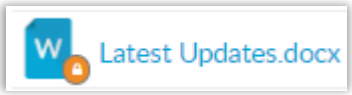
Click **Update**

Check Outs (web app)

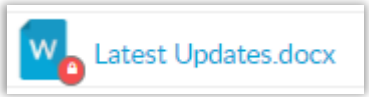
When the user next signs into Foldr, they will be able to check files out – Example below using the web app. The macOS and Windows apps provide access to the Check Out/In feature through the ***context menu > Foldr*** option in Explorer and Finder.



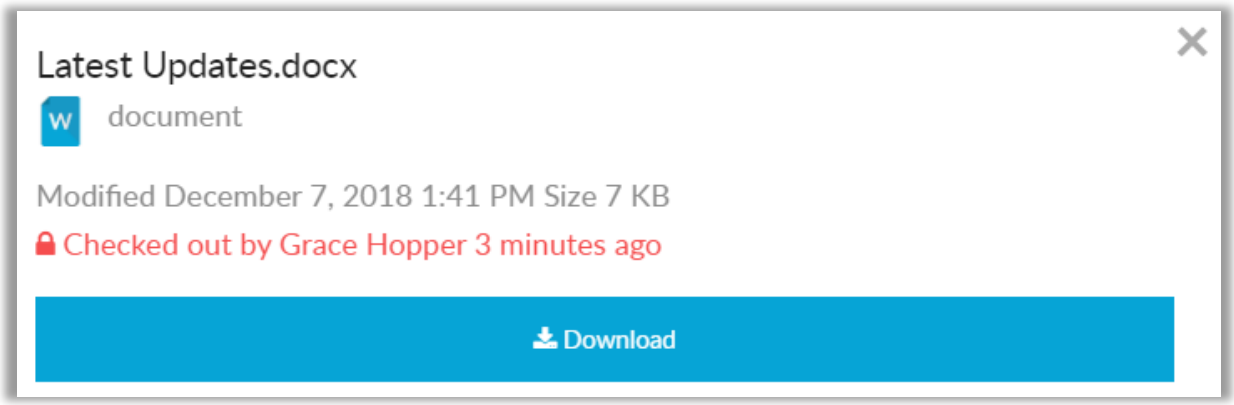
A padlock icon marking that files are checked out will be shown. An orange icon is shown for files you have checked out yourself.



A red icon is shown for files that have been checked out by others.



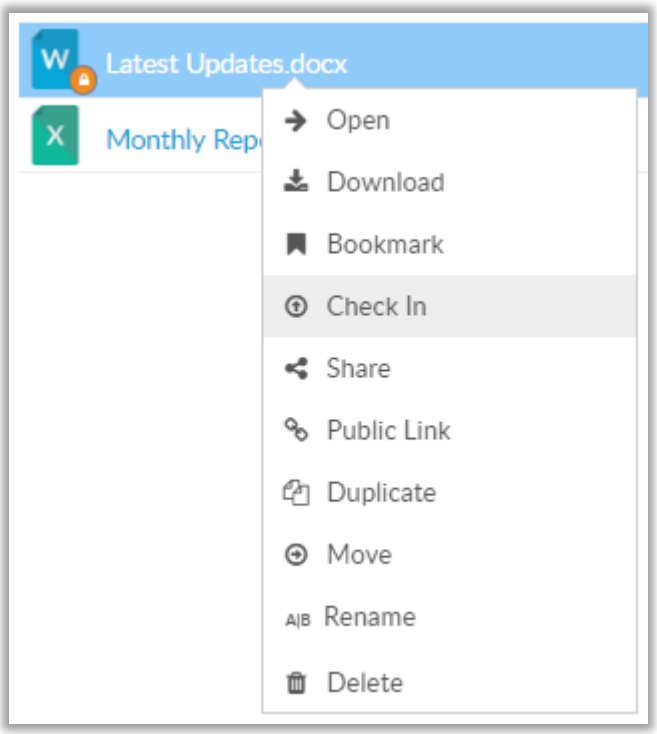
Clicking on a checked-out file will give more information about who checked the file out and when. Note that the Edit in Microsoft Office button is not available.



To check files out in the desktop or mobile apps, the user should use the Finder or Explorer context menu or long press menu on mobile.

Check In

To check a file back in, the user can use the context menu (right-click) or 'Check' In button in the file summary.

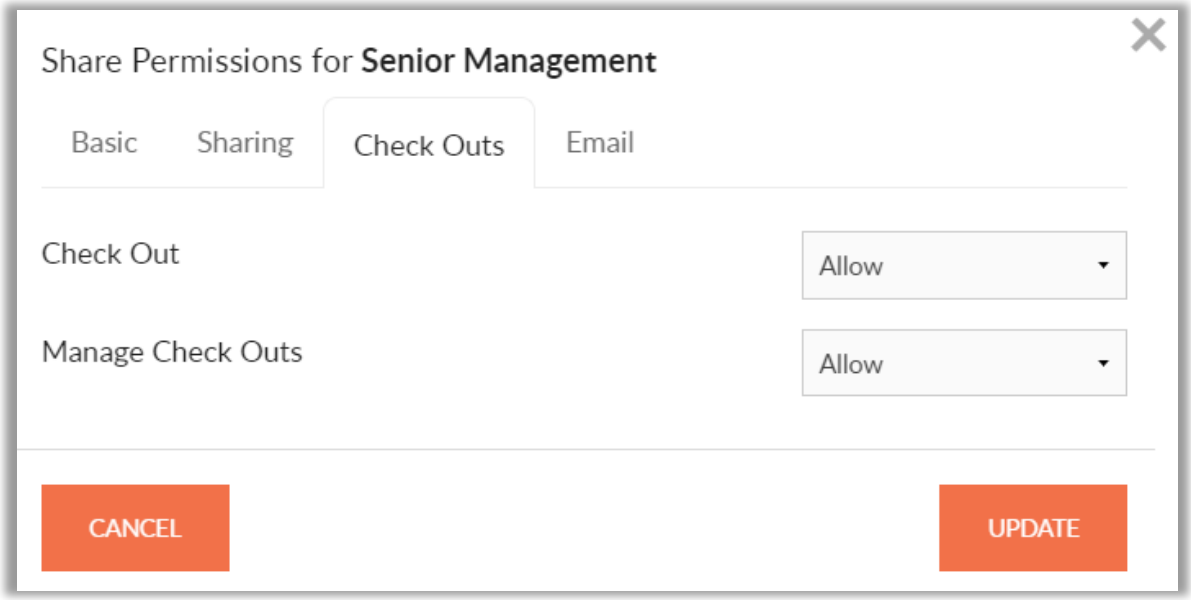


This will remove the padlock and make the file editable by others.

Manage Check Outs Permission

"Manage Check Outs" permission gives users the ability to check files in for other users.

Note – A user with the Manage Check Outs permission must also be granted Check Out in order to use the feature.



Automatic Check Out and Check In – App compatibility.

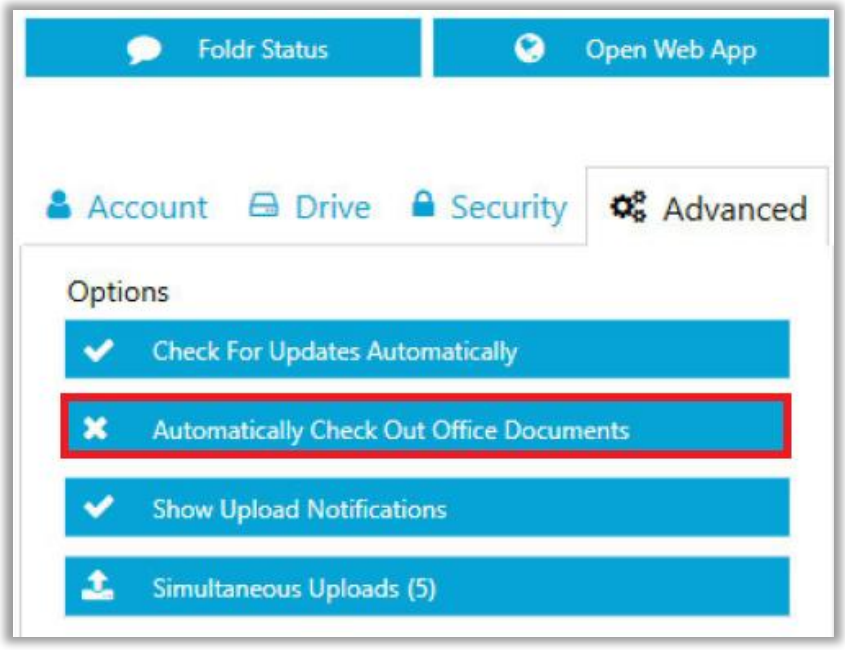
The Foldr web app Edit in Microsoft Office button will automatically check files out and in as they are opened for editing and subsequently closed. The Check Out permission is not required on a share for this to take place.

The Windows and macOS Foldr apps provide an option to automatically Check Out Microsoft Office documents. There are requirements to this feature:

1. The user must have the Check Out permission enabled on the share in Foldr Settings

2. In the Windows app, the Foldr drive must be mounted in network (default) mode rather than removable drive mode.

3. Automatic checkouts must be enabled in the Foldr for Windows client (**Settings > Advanced** tab) – This is enabled by default on macOS.



This setting can be enabled en-masse by the administrator if required by configuring client the registry key 'OfficeAutoCheckouts' as described here.

The mobile Foldr apps (iOS and Android) do not support automatic check outs and the user should perform the checkout manually.

Preventing Changes Outside of Foldr (SMB File Lock Service)

Checkouts exist only when a user is interacting with files from within Foldr (i.e. if signed into the web app, desktop or mobile apps). Other devices such as domain-bound workstations using standard mapped drives or other file access solutions are not aware of checkouts and as such it may be possible to modify/overwrite a file that is checked out through Foldr.

To prevent this there is an optional SMB daemon/service called 'foldr-checkout' on the Foldr server. Once the service is running and enabled/configured on shares it will watch for files that are checked out with specific file extensions and then hold these open over SMB to prevent changes elsewhere, until the file is checked in.

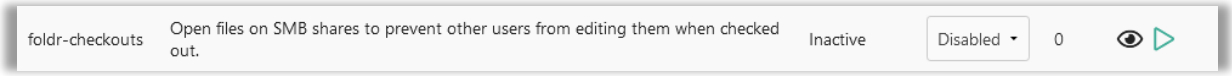
Note 1 – Should the Foldr server be restarted (such as following a software update), the service will attempt to reconnect and hold open any files that were previously checked out.

Note 2 – The foldr-checkout service only works against SMB shares.

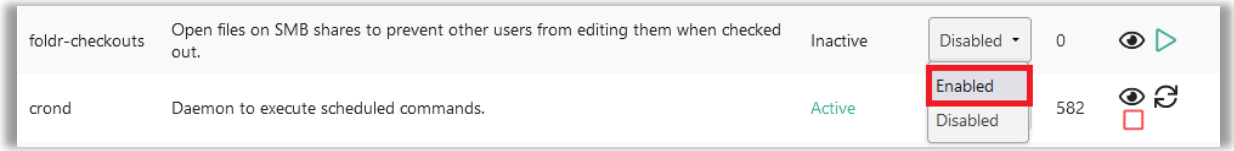
Note 3 – A suitable **service account** must be selected on the share in ***Files & Storage > Access*** tab for the checkouts service to function.

Enabling the Foldr-Checkout SMB Service

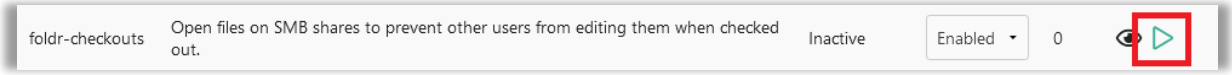
1. Navigate to ***Appliance > Services*** and scroll down to the **foldr-checkouts** service



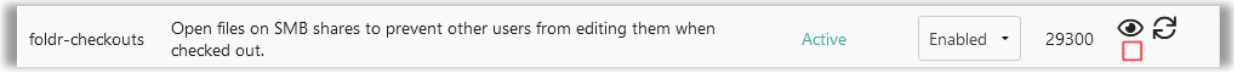
2. Click the drop-down menu and select **Enable**



3. Start the service



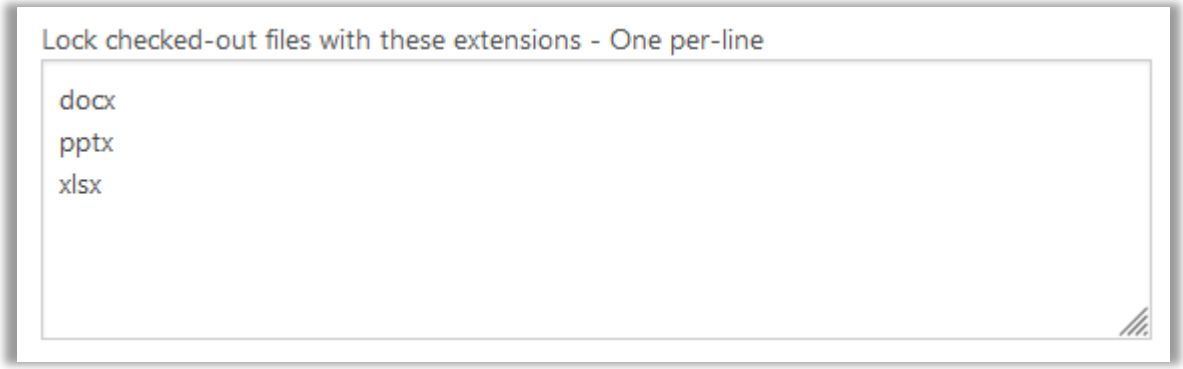
4. Note the service is now 'Active'



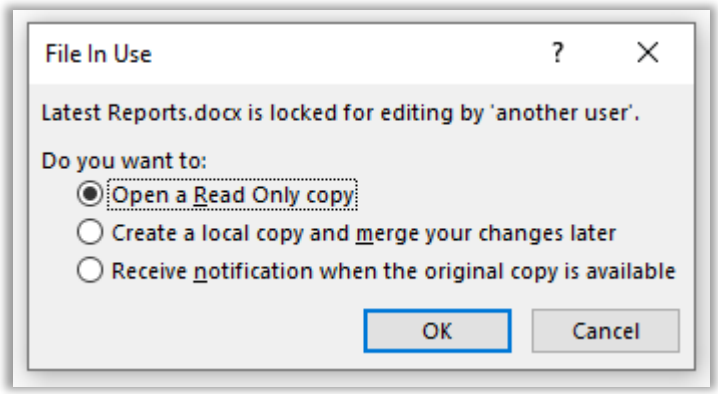
5. Navigate to **File & Storage > Edit share > Advanced > Checkout Service tab**, scroll down and enable the switch labelled 'Lock checked-out files?'

Note – the share must also have the 'Check Out' Permission enabled for users (everyone or specific users/groups) for the SMB lock to be effective and a service account that has permission to the share/files must be selected on the Access tab.

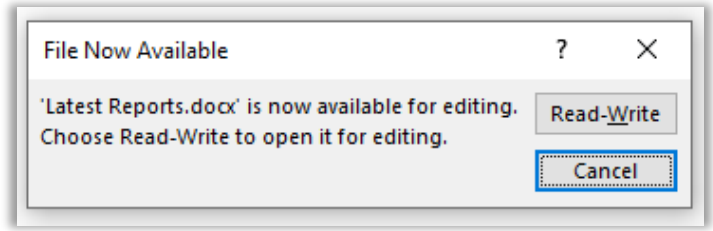
6. Configure the file extensions that the server should hold open if checked out by users (MS Office file extensions are enabled by default)



Foldr-checkout service setup is now complete. When a user checks out a file with a matching file extension (as above) it will be held 'open' by the Foldr server on their behalf. Should another user attempt to edit a document outside of Foldr (such as via native mapped drive in Explorer) they will receive the usual native file 'in use' prompt.



The Receive notification when the original copy is an available option and will work as expected. When the Foldr user checks the file back in, they will receive the notification in their Office application where they can click Read-Write to start editing the file.



Administrative Console Commands

Two checkout specific commands are available to the Foldr administrator on the appliance console.

`list-checkouts`

The 'list-checkouts' command will list all checked out files on the server, whether checked out manually or automatically by Edit in Office sessions in the web app or editing Office files via the desktop apps.

`remove-checkouts <days>`

The '**`remove-checkouts x`**' command, will remove all checkouts on the server older than x days specified. To remove all existing checkouts on the server use '**`remove-checkouts 0`**'

10. Search

Introduction

The Foldr server includes a powerful search function that allows users to perform searches across multiple storage platforms at once. Users can search both SMB shares and the following cloud platforms with a single search query: Google Drive, OneDrive, SharePoint Online, Box and Dropbox. Alternatively, a user can select to search a specific storage location.

By default, the search feature is disabled and must be enabled and configured by the administrator before it is available for use.

It is possible to search for files by name, filter results by modified date, or search for specific keywords within files. Foldr Search contains an optional Optical Character Recognition (OCR) engine to read text from images, such as scanned documents or graphical PDFs. OCR is not required to search for keywords inside common file formats such as Microsoft Office documents or textual PDFs.

Search results for SMB shares are returned by querying an index held within a dedicated Foldr appliance. This provides incredibly fast search results, regardless of the number of storage areas being indexed and searched. The index itself is built up from crawl jobs that are run on a scheduled basis. The initial crawl process of a share may take some time depending on the amount of data to be indexed, however, subsequent crawls will only index changed or new files so the index jobs will complete much faster. Cloud locations such as Office 365 OneDrive, SharePoint, Teams, Google Drive and Dropbox do not require indexing by Foldr as the server can query the cloud provider's own search APIs.

Foldr can ensure that only appropriate search results are returned to users, based upon the shares that are available to them under My Files and by parsing the file server backend NTFS permissions / ACLs.

App Compatibility

Foldr search is available in the web, desktop (Windows & macOS) and mobile apps (iOS/Android). Note that desktop app search is implemented using a web search view. This is available from the Foldr icon in the system tray/menu bar. Alternatively, Windows users can use shortcut keys (Win + Shift + F), macOS users can use (Alt + Space) to launch the desktop search UI.

Search is not accessible from the native search bar in Explorer or Finder.

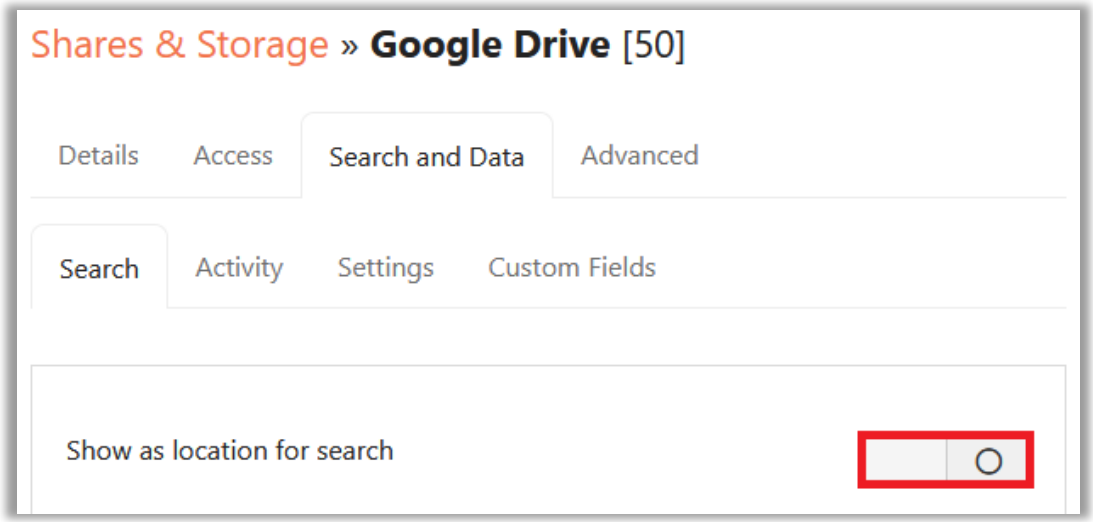
Enabling Search for Google Drive, Office 365 locations, Box or Dropbox

NOTE - If only cloud locations are being searched, the Foldr indexing server/service is *not* required. Search can be quickly enabled in ***Foldr Settings > Files & Storage > Edit share > Search*** using the 'Use Service API' option. To provide search results for **on-premise SMB shares**, they must be indexed by a Foldr server.

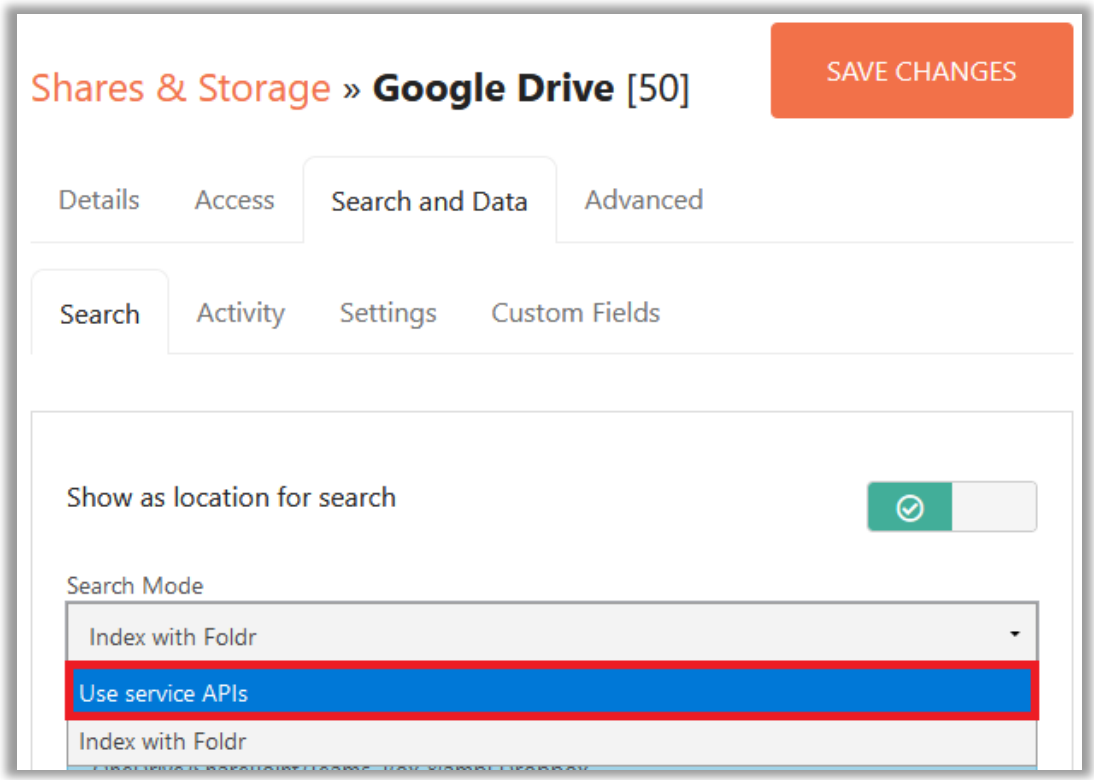
Where advanced features such as OCR are required, you can use Foldr's own index engine to process files held in cloud locations, however, it should be noted that ***searching for keywords inside common file types is already available*** with the default 'Use service APIs' option described below.

To enable search service to users for Google Drive, OneDrive/SharePoint/Teams or Dropbox, navigate ***to Files & Storage > Edit-Cloud-Storage-Item > Search and Data*** tab

1. Enable the toggle labelled '**Show as location for search**'



2. Select '**Use service APIs**' as the search type/mode

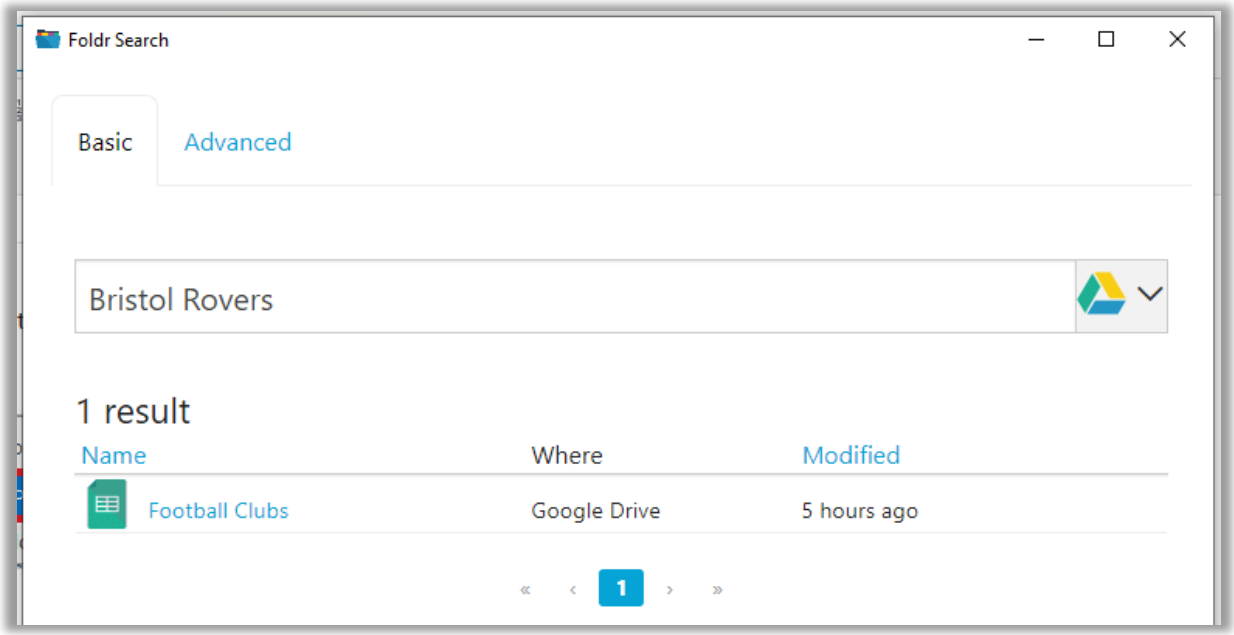


3. Click **Save Changes**

Search will now be available for the share (Google Drive in this example) in the web, desktop and mobile apps.

Please note that any new files that are created in the cloud location may not immediately be displayed in Foldr search results until the cloud providers search has indexed the file. Google Drive for example takes a few minutes for this to take place and happens automatically.

Windows app search below using service APIs to search for content in Google Drive. Note that clicking the search results Google Sheets file, will launch the browser with the file ready to edit in the corresponding Google web app.



System Requirements

Where searching of on-premise SMB shares is required the Foldr index service must be used. The Search role can be resource-intensive both in terms of CPU and memory and as such, it is strongly recommended that a separate virtual appliance is deployed specifically to host the search indexes and perform crawl operations. If regular client access and search is hosted upon a single appliance, it may have an impact on the user experience when performing regular file access operations, even when increasing the specifications of the VM. The following *minimum* specifications are recommended for the Foldr appliance that is going to be hosting the search role:

2 vCPU
4GB RAM

If you provide more CPU / RAM resources to the search appliance beyond the specification above, the crawl process will, within reason, consume most of the resources it is provided with during an indexing operation. The above specification is the recommended minimum for Search to operate correctly.

This article will describe configuring two Foldr appliances. One will act as our primary client access/infrastructure (database) appliance, and the other our Search appliance. In an existing installation, the primary appliance is the virtual machine that is currently being accessed by users, however, with version 2 Search it is vital that the Search appliance is set to use the same backend configuration database as the primary appliance.

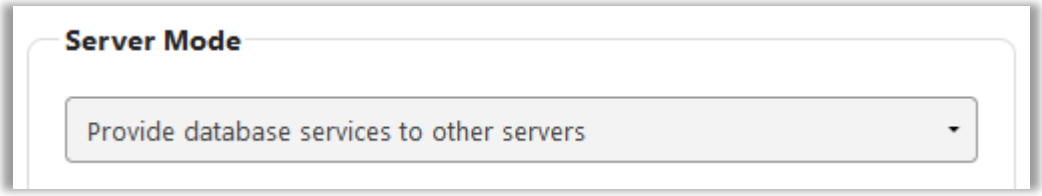
Ensuring both appliances are using the same backend configuration database:

To allow version 2 Search to function correctly, it must be able to read the main configuration database from the primary (or other appliances). To do this:

This step should be done on the **CLIENT ACCESS/PRIMARY** appliance.

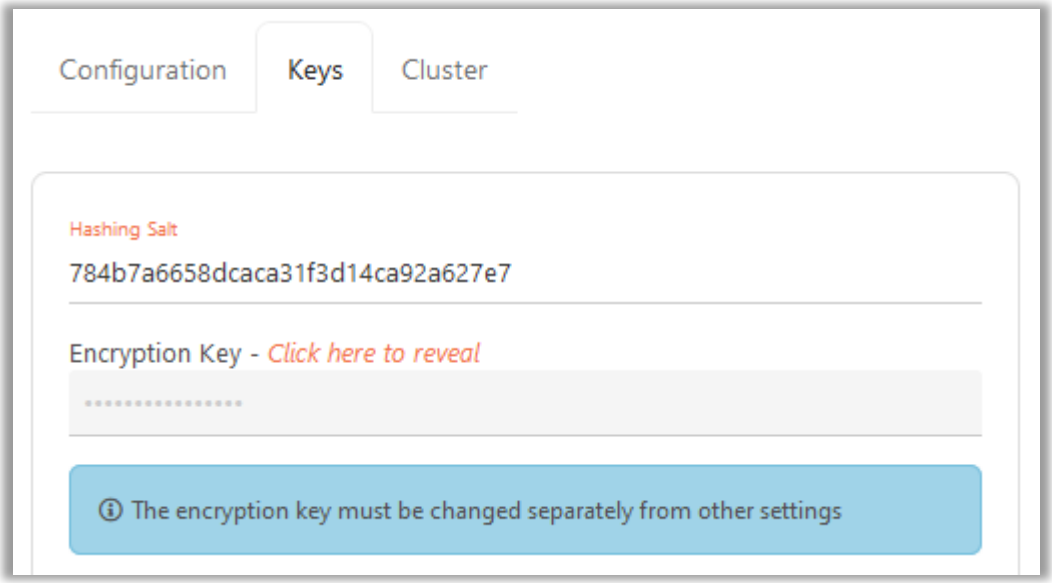
1. Log into ***Foldr Settings > Appliance > Infrastructure tab*** and set the Configuration > Server Mode to:

Provide database services to other appliances

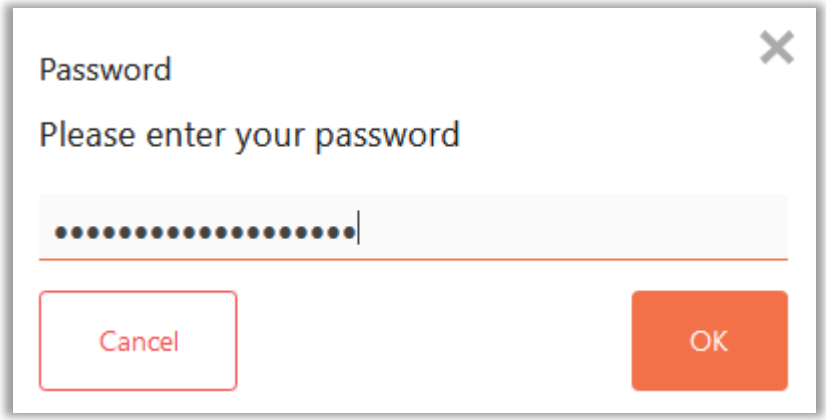


2. Enter the IP address of the SEARCH appliance in the box labelled 'Trusted Servers'

3. Navigate to the **Keys** tab and make a note of the Hashing Salt - this will be required later.



4. Click the orange text link in the keys tab to reveal the current Encryption Key and supply the fadmin password in the pop-up dialog

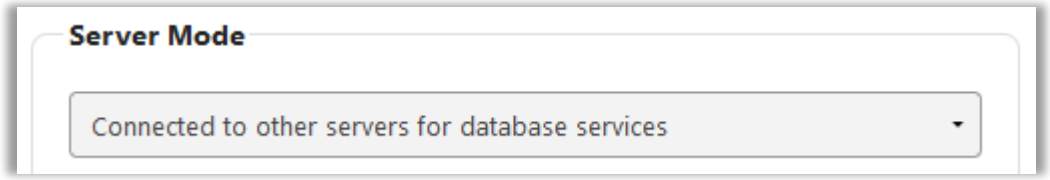


5. Make a note of the Encryption Key, this will be required later

The following should be done on the SEARCH appliance:

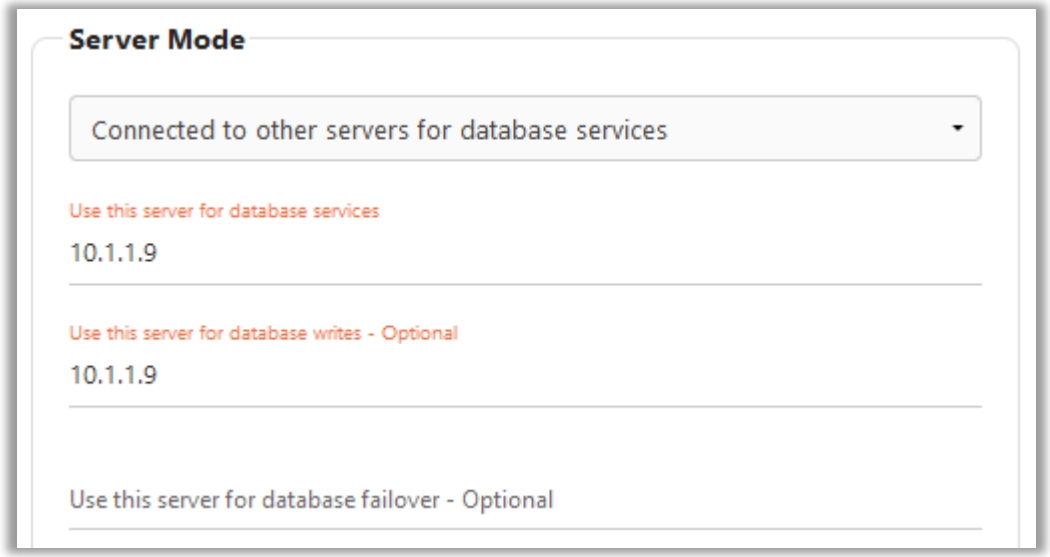
6. On the SEARCH appliance, browse to ***Foldr Settings > Appliance > Infrastructure tab > Configuration*** and set the Server Mode to:

Connected to other appliance(s) for database services

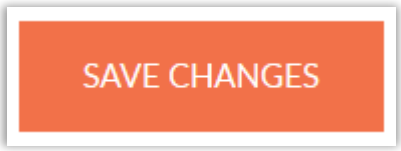


7. Enter the IP address of the CLIENT ACCESS/PRIMARY Foldr appliance in the two fields labelled:

- Use this server for database services
- Use this server for database writes - Optional



8. Click the Keys tab and copy/paste the **Hashing Salt** from the CLIENT ACCESS\PRIMARY DB appliance. Click **SAVE CHANGES**.



9. Copy / paste the **Encryption Key** from the CLIENT ACCESS\PRIMARY DB appliance. Click **SAVE CHANGES**.

NOTE - You must not change both the Hashing Salt and the Encryption Key at the same time (with one Save action) as the encryption key will not be saved successfully.

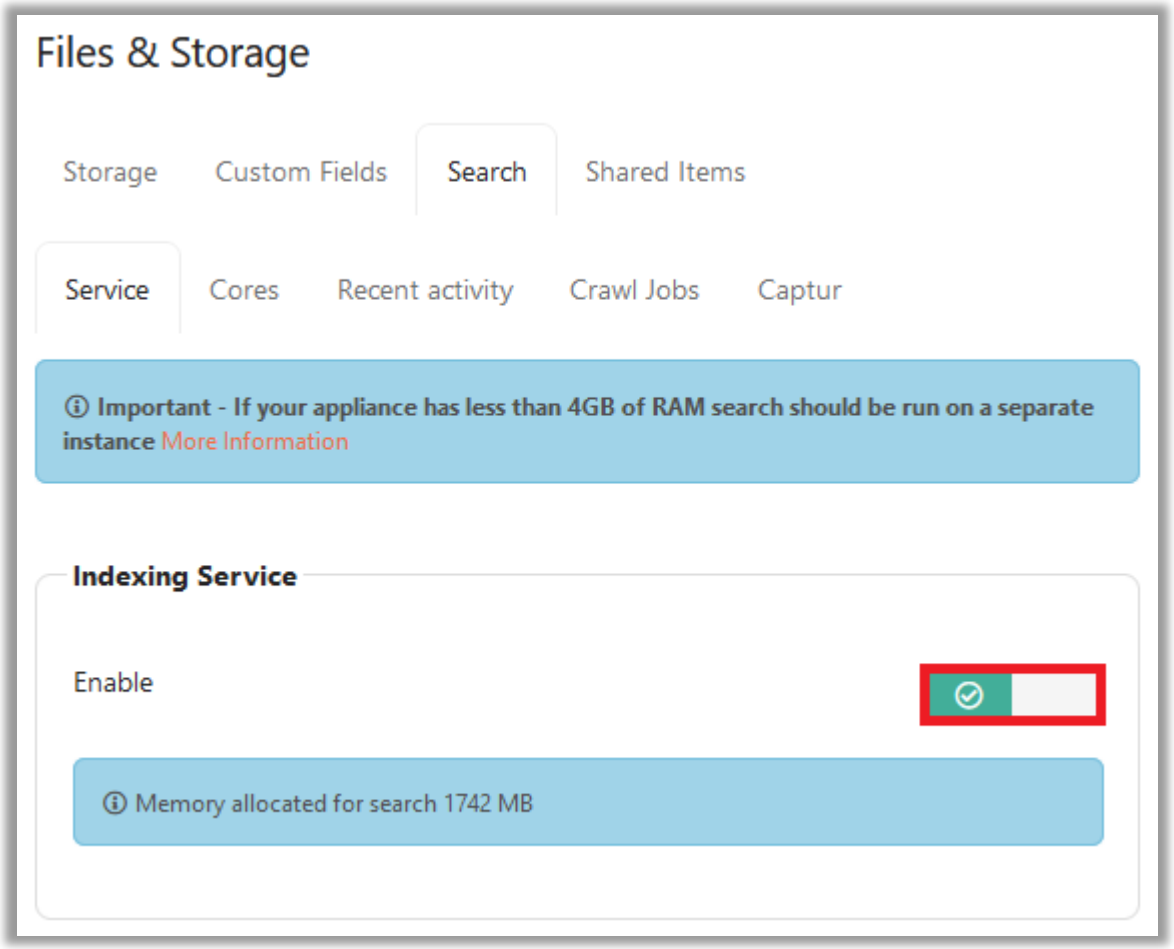
Confirm database availability

The Search appliance should now be able read/write the database hosted on the primary Clicking the General tab or Shares should confirm that the configuration (licence keys, service accounts, shares etc) is now being read from the Primary appliance. Configuration changes can be made on either appliance and these changes will be reflected on the other server immediately.

Enabling the search index service

The following should be done on the SEARCH appliance:

Within Foldr Settings, navigate to the ***Files & Storage > Search tab*** and enable the Index Service.

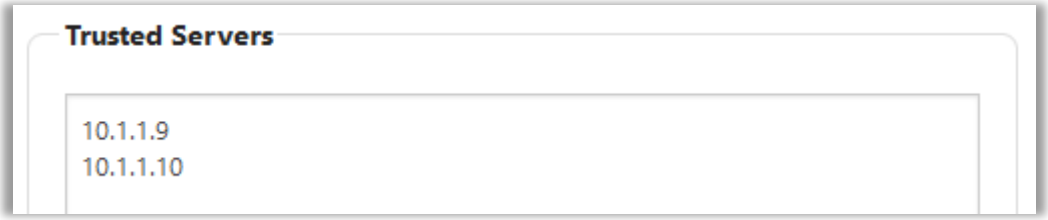


Specify other Foldr appliances (Trusted Servers)

This should be done on the SEARCH appliance:

Enter the IP address of all Foldr appliance(s) that will be using search (including the search server itself) within the Trusted Servers field. Each server entered onto a separate line.

This will change the configuration of the built-in firewall to allow connections from these IP addresses.



Creating a Search Core

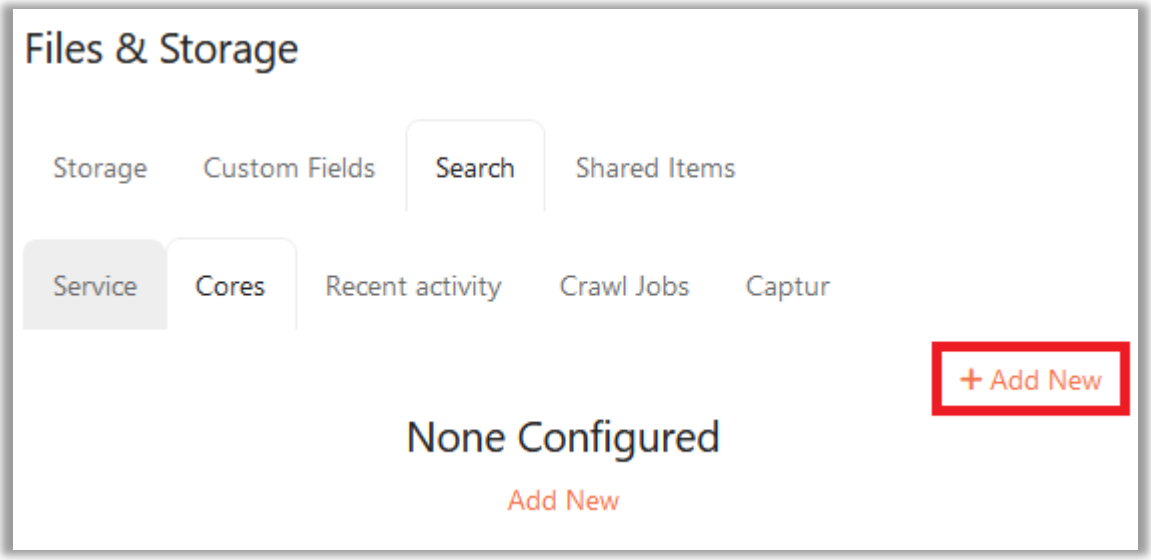
This should be done on the SEARCH appliance:

A 'Core' can be thought of as a container that holds both the configuration and the index files for one or more share paths (URIs).

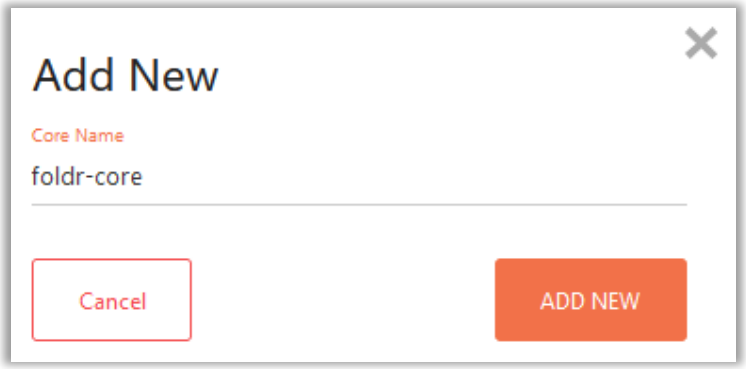
Whilst the search function can host multiple cores with numerous share URIs in each, it is generally recommended to configure a single core with all share URIs within it.

On a multi-tenant installation, you should use one core per tenant.

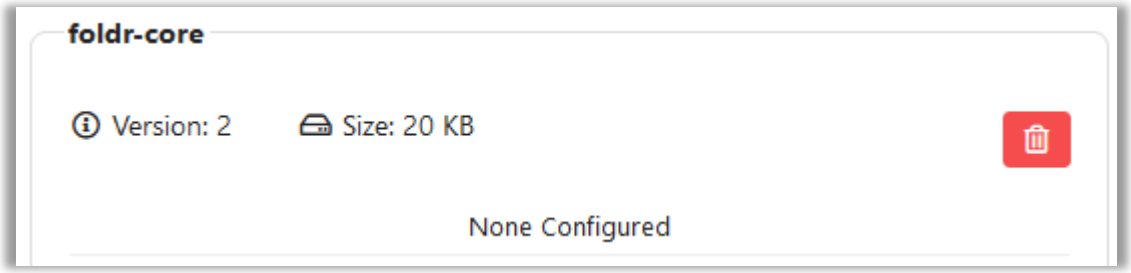
1. To create a core, click the **Cores tab > + Add Core**



2. Give the Core a suitable name and click **ADD NEW**. The core version should be left as Version 2 - Note only lowercase characters are permitted.



3. An empty core will be created



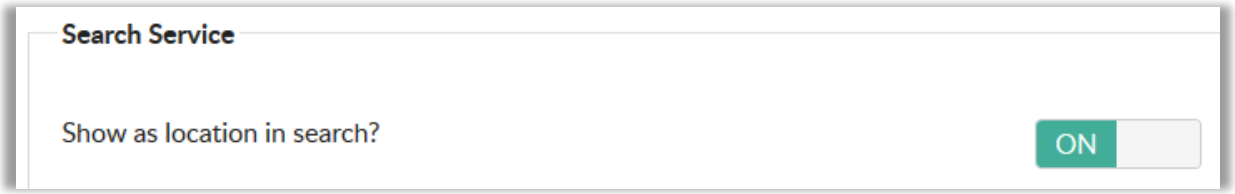
The core should now be populated by editing Shares and configuring the search tab inside each to use the Search appliance.

Enabling Search for SMB shares

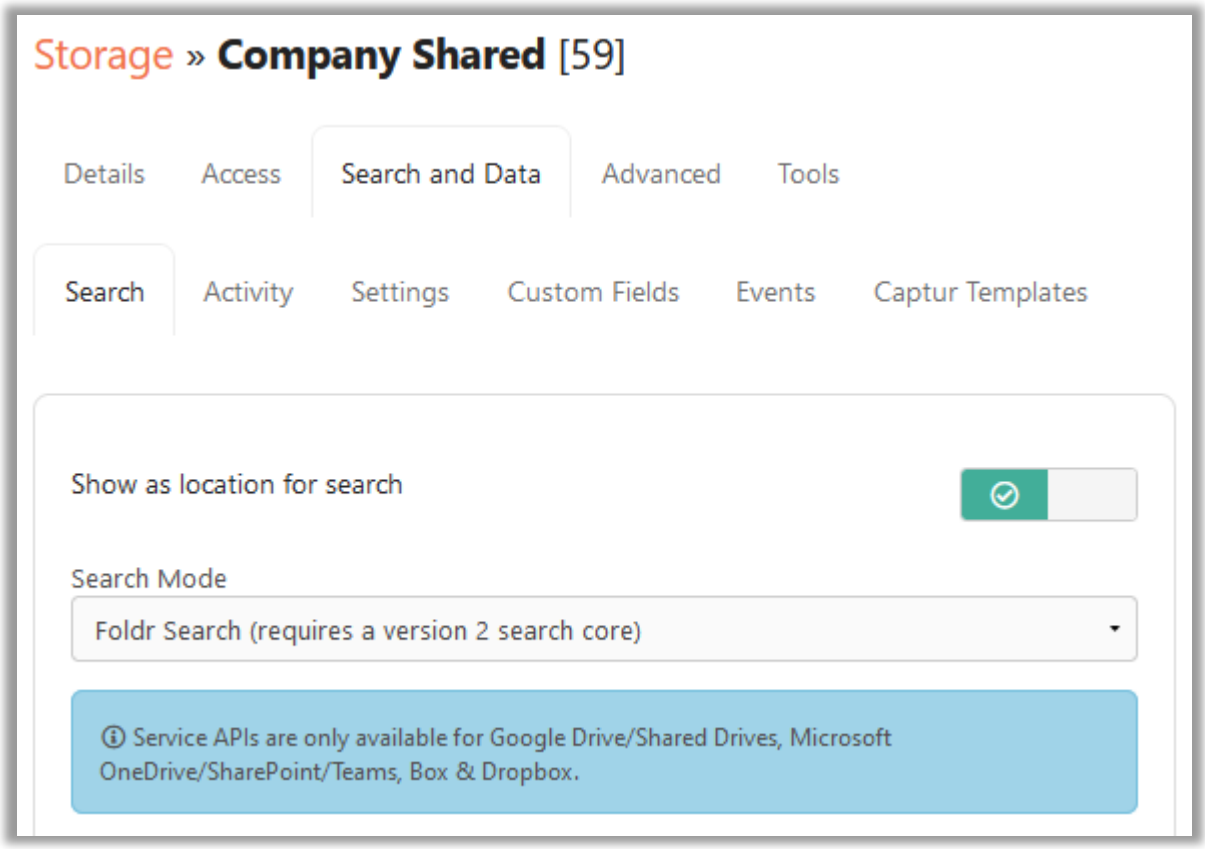
*This step should be done on the **SEARCH** appliance.*

1. You should now populate the core with shares to be indexed by Foldr search. To do this, navigate to ***Foldr Settings > Files & Storage*** and edit a share (double click the share to edit)

2. Click the Search tab and enable the toggle labelled '***Show as location in Search?***'



3. Ensure that the Search mode is set to 'Foldr Search (requires a version 2 search core)'

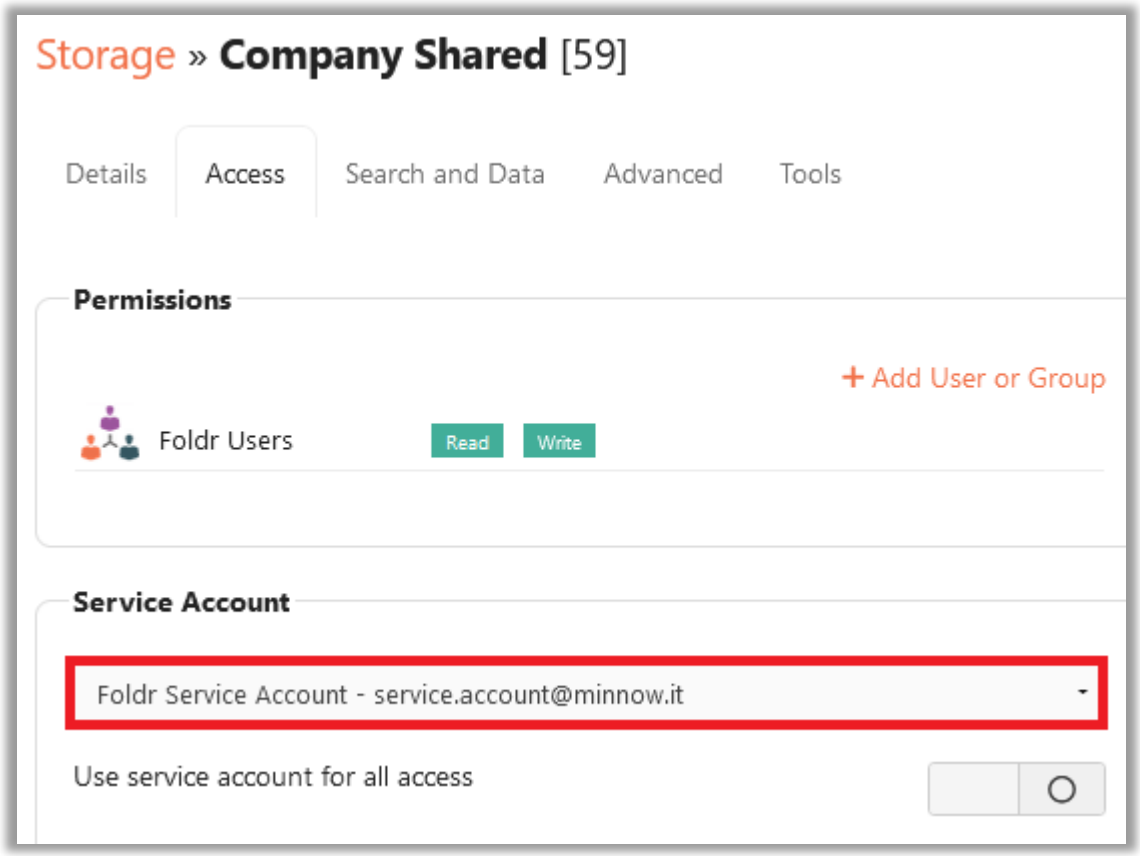


4. Below the Search mode drop-down menu, populate the search server's IP address and core name within the box labelled 'Server' – NOTE - This should point to the Search appliance

IMPORTANT!

5. Navigate to the **Access** tab in the storage item's configuration screen and select a *suitable service* account that has at least **read** permission to the share and all data contained within it. Note that service accounts being used with SMB shares, should have their username configured using the UPN.

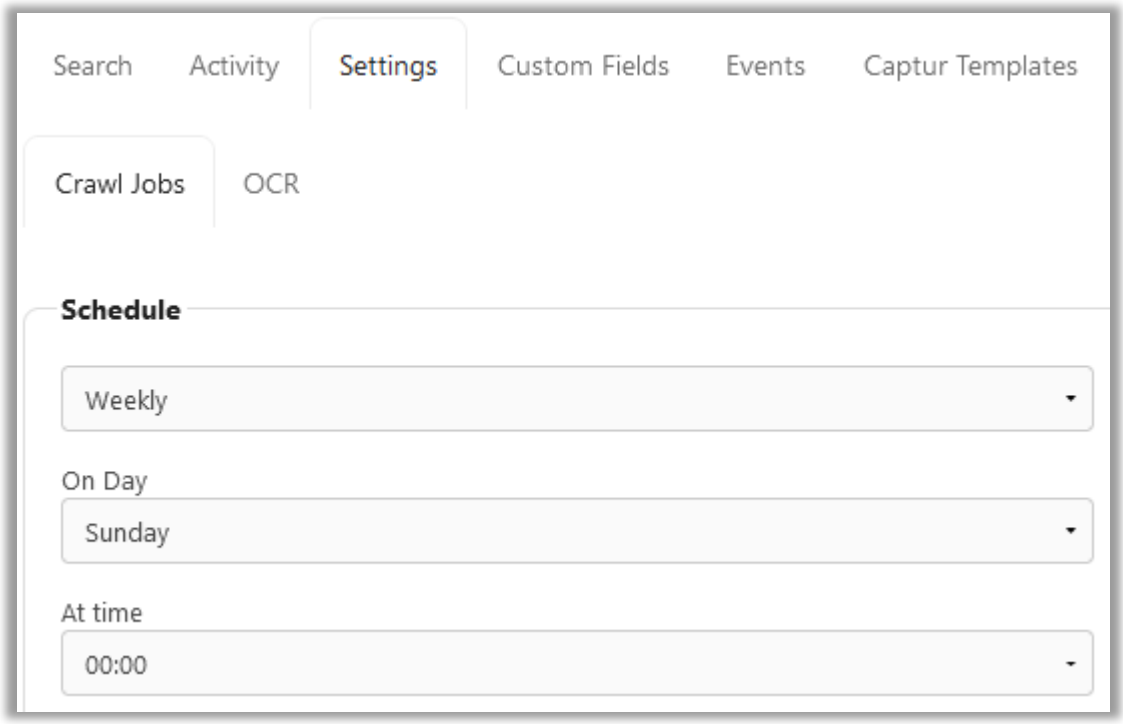
Additional service accounts may be configured within the ***Foldr Settings > Integrations > Service Accounts tab***.



Scheduling Index Operations

*This step should be done on the **SEARCH** appliance.*

Within ***Foldr Settings > Files & Storage >Edit-Storage-Item > Search and Data > Settings > Crawl Settings*** you can select a suitable schedule from daily, weekly, or monthly options to crawl the share, however more granular scheduling is available using the Cron option. This will change the configuration of the built-in firewall to allow connections from these IP addresses.



Using Cron for advanced scheduling

Using the Cron option, it is possible to configure granular schedules. Example Cron syntax is shown in the graphic below:

```
# Use the hash sign to prefix a comment
# +---------------- minute (0 - 59)
# |  +------------- hour (0 - 23)
# |  |  +---------- day of month (1 - 31)
# |  |  |  +------- month (1 - 12)
# |  |  |  |  +---- day of week (0 - 7) (Sunday=0 or 7)
# |  |  |  |  |
# *  *  *  *  *
#-------------------------------------------------------
```

As an example, to crawl a URI every Monday, Wednesday and Friday at 8pm you would use:

'Crawl As' vs 'Indexing ACLs' (Permissions)

When a share is indexed the crawl job can be run as an individual user (or users of a group) or if that is unavailable (lack of credentials / user is unknown to Foldr) then the crawl will be performed as the service account set on the share.

In most cases, **'Crawl As' should only be used on personal shares such as SMB home folders** where the %username% Share URI is used on the share, or cloud storage such as OneDrive, Google Drive. Using Crawl As, allows Foldr to resolve paths for each user in turn (i.e. pull these from Active Directory and index as required). When using Crawl As, the administrator would typically enter one or more security groups that contains users whose home folders you wish to index. NOTE Domain Users and other 'built-in' groups should not be used.

Indexing of ACLs should generally be used on common network shares that contain granular sub-folder / file permissions.

Crawl As and Indexing ACLs are mutually exclusive options when configuring Search on a Share. If the share being indexed is 'flat' in that all users have the same level of access to its contents, you do not need to enable Index ACLs or use Crawl As.

Recommended settings for Active Directory Home Folders (%homefolder%)

Where SMB shares are configured in ***Foldr Settings > Files & Storage*** using the **%homefolder%** variable, to dynamically obtain the user's home folder path from the Active Directory homeDirectory attribute (as represented in the profile tab > Home Folder in ADUC) the following should be configured:

Crawl Settings:

1. Crawl As – Select one or more Active Directory Security Group that contains users that the share applies to – NOTE Domain Users and other 'built-in' groups should not be used.

2. Index ACLs – toggle should be disabled

Recommended settings for central/common shares (SMB)

Common network shares that are flat (no granular permissions)

Crawl Settings:

1. Crawl As – unconfigured

2. Index ACLs – toggle should be **disabled**

Common network shares that contain files/folders with granular permissions

Crawl Settings:

1. Crawl As – unconfigured

2. Index ACLs – toggle should be **enabled**

A suitable **service account** should always be selected on the share within the Permissions & Access tab that has permission to read the data being indexed. Service accounts for SMB shares must always be configured using the UPN (username@domain) format.

Using the cloud provider's search API (direct search cloud service with no indexing required)

Foldr can use the cloud providers search API directly or crawl/index cloud locations in the same way as on-premise SMB shares. On shares using cloud related variables for the Share URI (%onedrive%, %googledrive% and so on) you can select the required mode within the Search Settings tab.

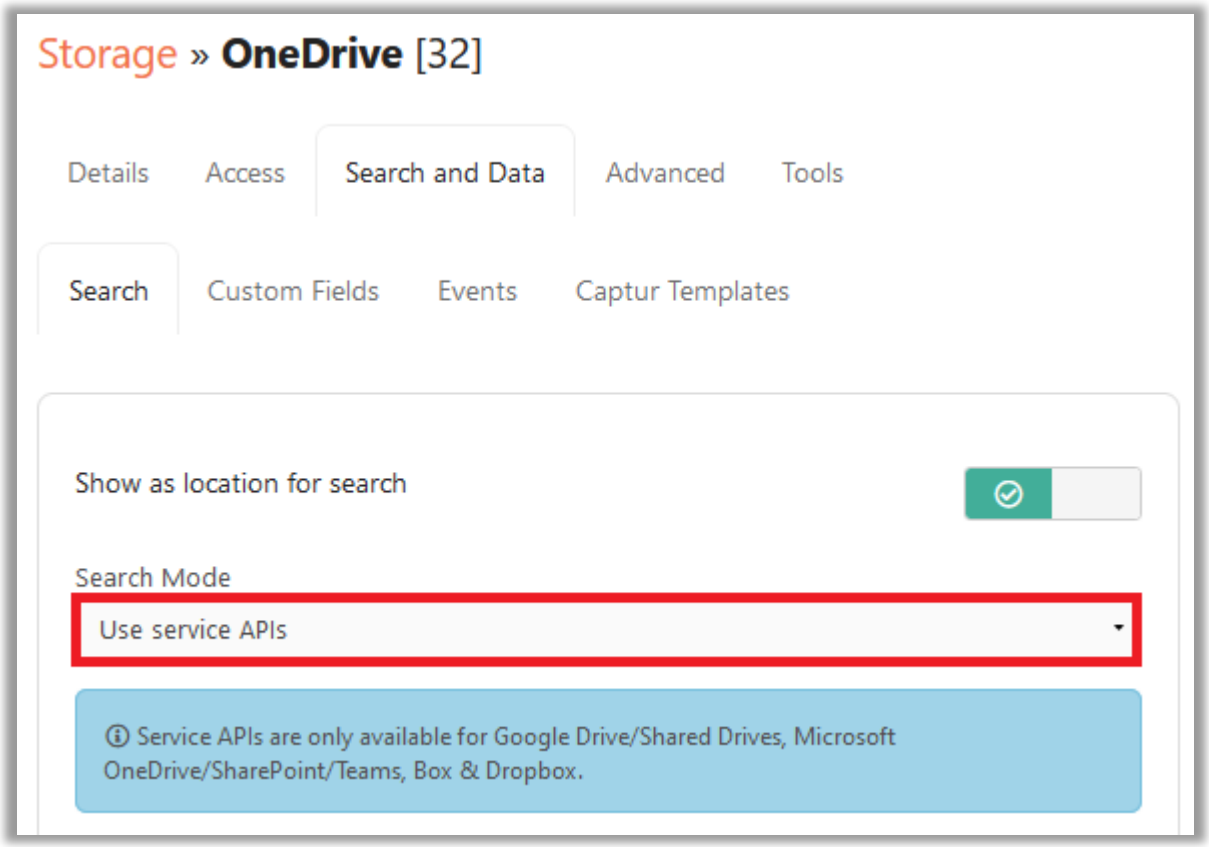
Using the cloud provider's search API (no indexing required)

Note this option does not use the search appliance as no indexing takes place and all search queries are performed 'live' against the relevant cloud provider. Using the cloud providers API will provide basic search capabilities but certain features (indexing ACLs, file content, scheduling, OCR and so on) do not apply. Some search terms/queries may not be supported.

To configure:

1. Edit the storage item in question (OneDrive, Google Drive etc) in ***Foldr Settings > Files & Storage***

2. Select the Search and Data tab and select **Use service APIs**



3. Click SAVE CHANGES

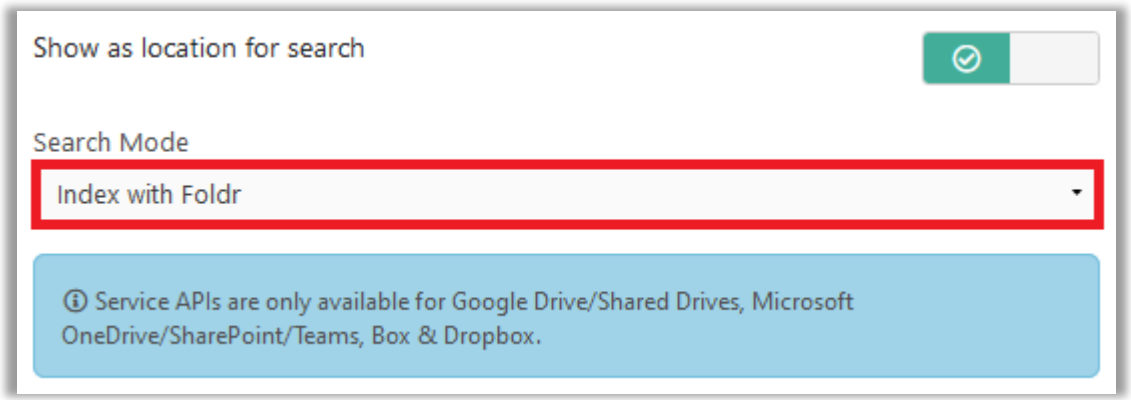
Indexing cloud services with Foldr

All cloud services that Foldr can present to a user, may be indexed and stored in the Search appliance. This allows Foldr to index file content, schedule crawls and use the same search terms/queries as on-premise shares.

To Configure:

1. Edit the storage item in question (OneDrive, Google Drive etc) in ***Foldr Settings > Files & Storage***

2. Select the Search and Data tab and select **Index with Foldr**



3. The search server IP address and core name should be configured in the Server section below the Search Mode drop-down menu.

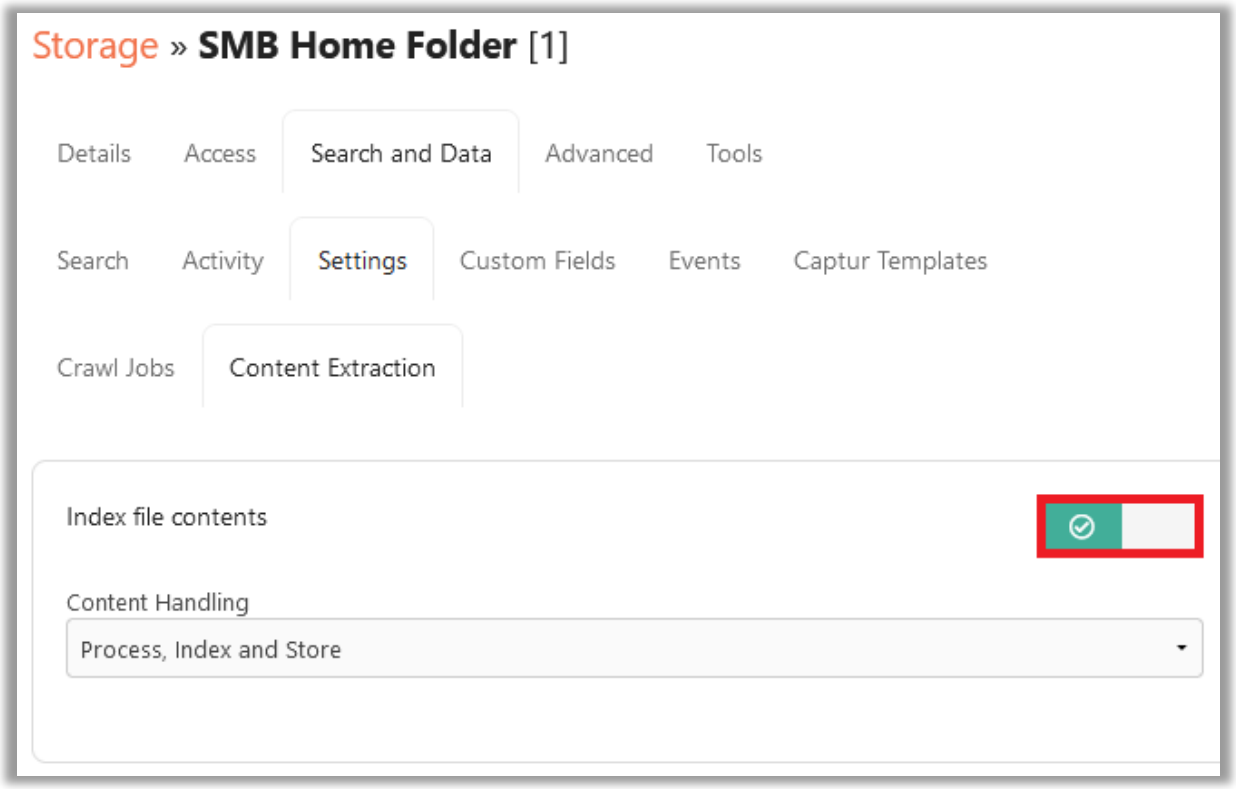
1. Crawl As - Specify an Active Directory Security Group that contains all users that the share applies to

2. Index ACLs toggle should be disabled

All other Search options can be configured as required.

Indexing File Content / Content Extraction

By default Foldr search will index file names only. To index textual content found in common Office formats, PDF, txt and so on, enable the '**Index file contents'** toggle in ***Foldr Settings > Files & Storage > Search and Data > Settings > Content Extraction***. A predefined template / list of common files formats is already configured by default, but this can be amended as required.



Optical Character Recognition (OCR)

During an index job Foldr can optionally process image files (jpg, png and gif) or graphical PDF documents with a built-in OCR engine to extract text which is then stored in the Search index. This text is then searchable by the user.

Note – OCR is not **required** to index the content of Microsoft Office, PDF or other textual files. This is a resource heavy feature and will dramatically slow down index processing rate as each file is analysed by the OCR engine.

An example use case, with OCR enabled, would be a user searching for scanned documents and being able to quickly locate a specific invoice by its invoice number file contained within the file.

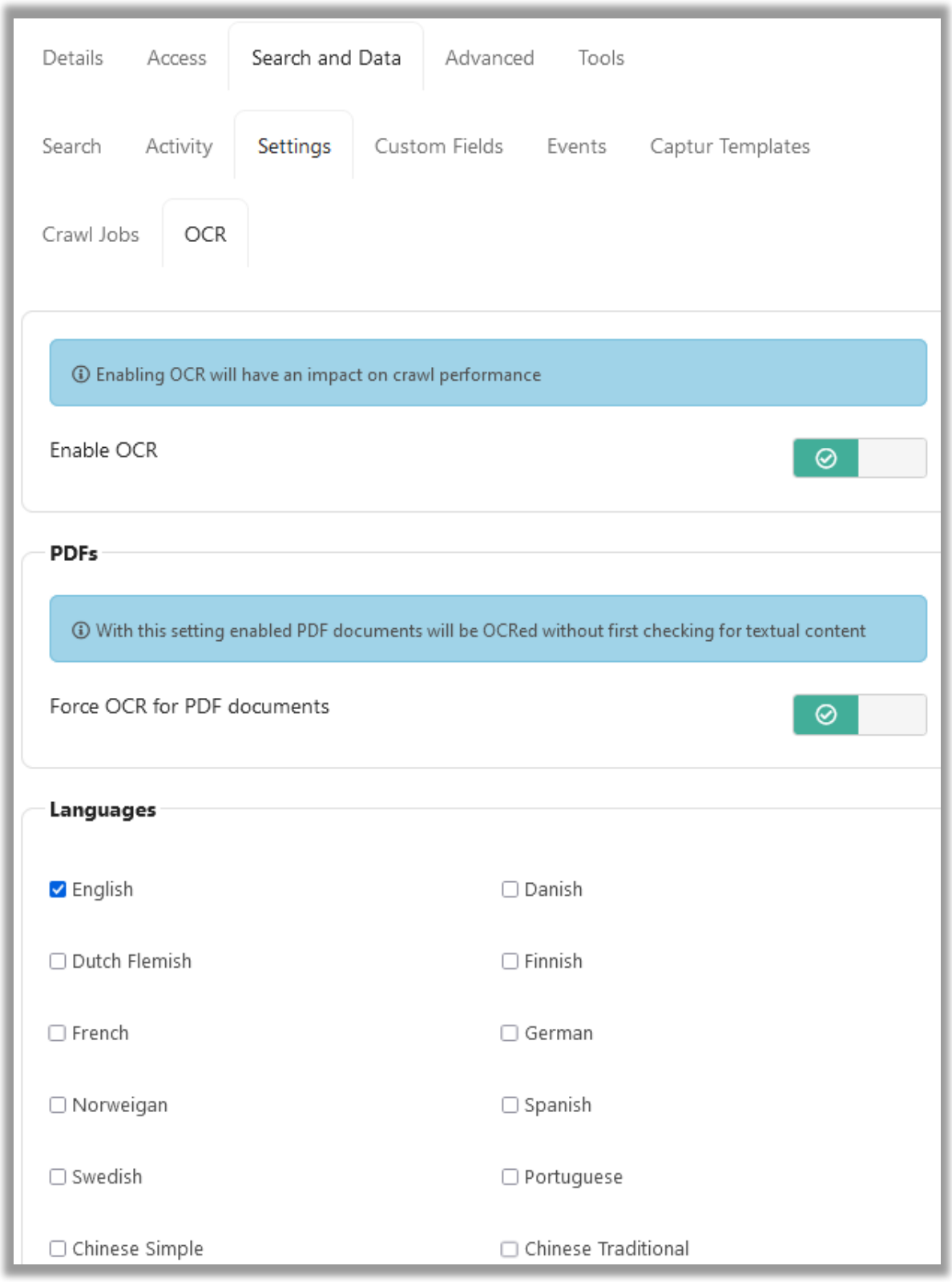
To enable the OCR feature, do this on a per share basis by enabling the OCR toggle ***Foldr Settings > Files & Storage > Search and Data > Settings > Content Extraction*** (note, index file contents toggle must firstly be enabled).

Exclusions

Within the Exclusions section in Crawl Settings, the administrator can exclude certain file types or files / folders matching naming patterns using wildcards (*) from the index. Foldr has pre-defined exclusions for common files that are not usually of interest to a user (such as temporary files, system generated or .dsstore files and so on). Additional exclusions can be entered one per line. If the exclusion contains a / it is assumed to be a directory rather than a file.

Example syntax:

temp.docx – Excludes any file called temp.docx from the index
*.png – Excludes all PNG files from the index
temp – Excludes all files containing 'temp' in the file name
Temp/* will exclude any directories called Temp (and also exclude all subdirectories / files within)



OCR Language Support

By default, Foldr will use English language only when performing the OCR feature, however the administrator can optionally enable the following languages if required: French, German, Spanish, Dutch (Flemish), Chinese Simple and Chinese Traditional. If support for an additional language is required that is not currently listed, contact support@foldr.io

Exclusions

Within the Exclusions section in Search Settings the administrator can exclude certain file types or files / folders matching certain naming patterns using wildcards (*) from the index. Foldr has pre-defined exclusions for common files that are not usually of interest to a user (such as temporary, system generated or .dsstore files and so on) and additional exclusions can be entered one per line. If the exclusion contains a / it is assumed to be a directory rather than a file.

Example syntax:

temp.docx – Excludes any file called temp.docx from the index
*.png – Excludes all PNG files from the index
temp – Excludes all files containing 'temp' in the file name
Temp/* will exclude any directories called Temp (and also exclude all subdirectories / files within)

Search Results & Permissions

Foldr Search will respect the backend file server permissions / ACLs providing the administrator is indexing the ACLs. However, a user will only be able to perform search queries against an SMB share if it is firstly accessible to them from My Files. This ensures only search results are returned to a user for shares that are available to them and by using the backend ACLs it ensures only files that are available to that user are returned in the results.

Indexing New Files

The search feature will automatically index files as they are uploaded by users and it will also update the index as files are moved or deleted through Foldr. If new files are placed onto an SMB share outside of Foldr (for example via a domain-bound workstation in Explorer) the files will be added to the Foldr search index when the next scheduled crawl job takes place. You can manually start an index / crawl job at any time from the Activity tab.

Manually Starting a Crawl / Index Job

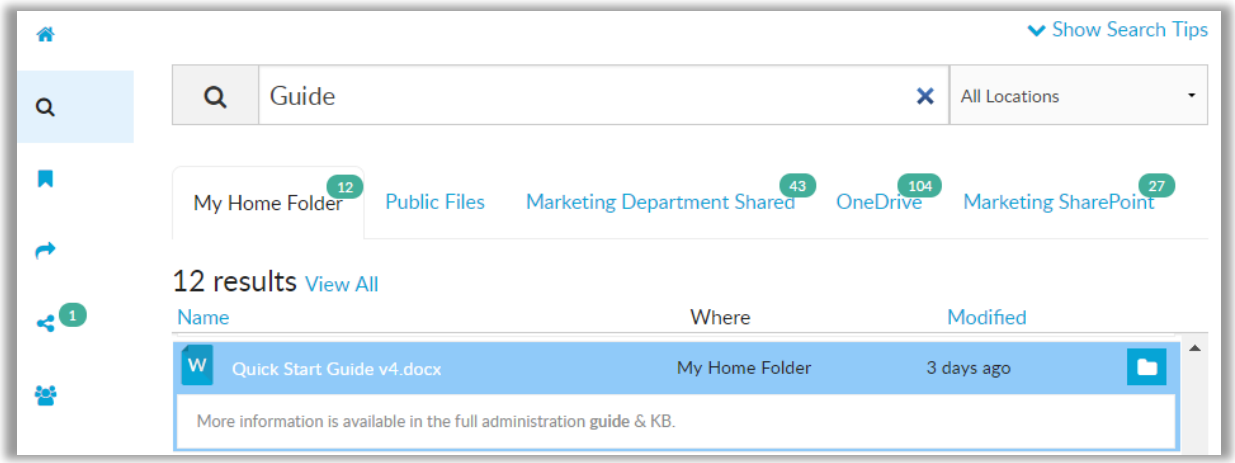
*This step should be done on the **SEARCH** appliance.*

To start a crawl job manually, browse to ***Foldr Settings > Files & Storage > Search > Activity*** and click the + Crawl Now button.

Search Highlighting

Search results from SMB shares will include text highlighting for content inside of files that match a user's search (i.e. those held in the index). This provides useful excerpts to be displayed to the user in the web app.

Web app Search:

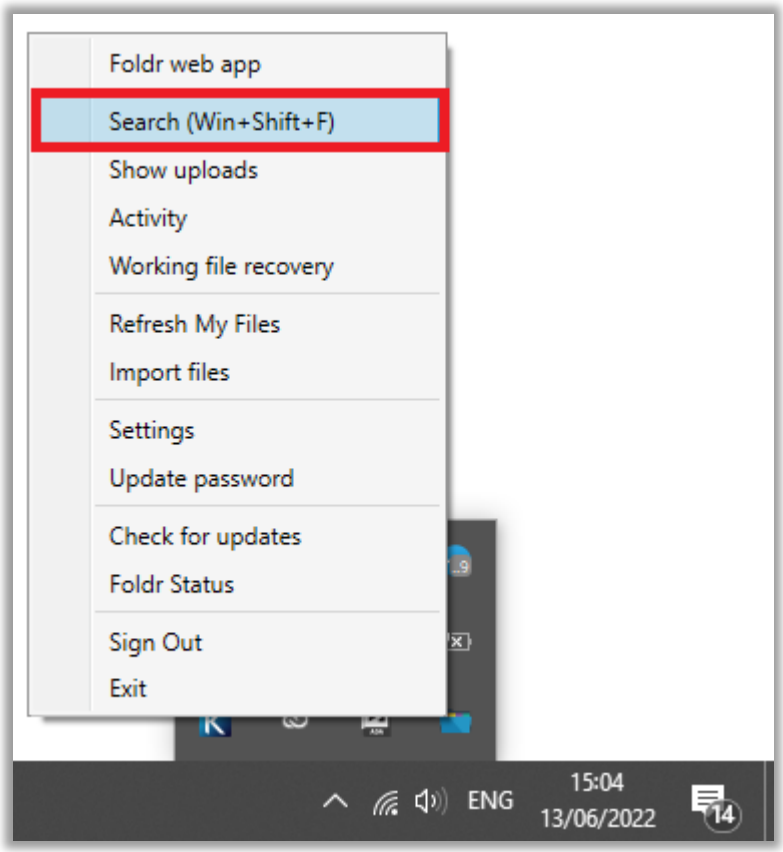


Note that it is possible to search across any number of storage locations with one search query in the web app.

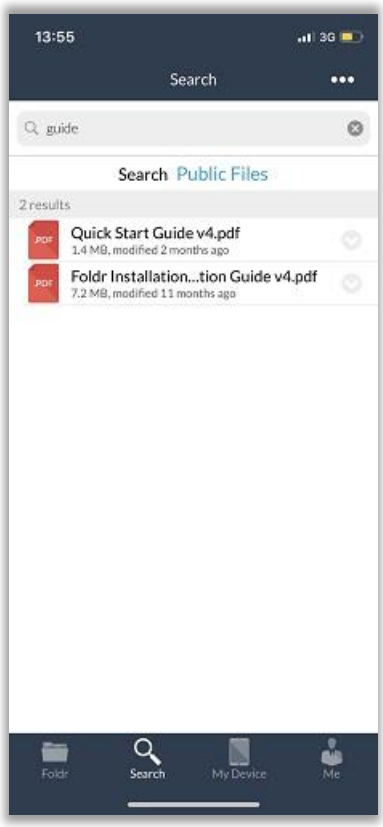
Desktop Search (web view) can be launched from the system tray/menu bar Foldr icon or using the keyboard shortcut

Windows keyboard shortcut - **Windows Key, Shift + F**
macOS keyboard shortcut - **Alt + Space**

Windows search:



Mobile Search (iOS shown):



The following search tips are available for users using the on-screen link in the web and mobile apps:

You can **search by file name, contents, or modified date**

To search by **file name only** use `name:myfile.txt`

To search **file contents only** use `contents:my term`

You can **substitute letters, words, and phrases with an asterisk** `name:myfile*`

To search for an **exact phrase use quote marks** `"my exact phrase"`

To search for **files modified on a specific date** use YYYY-MM-DD `modified:2017-08-05`

Dates can be **whole months or years** `modified:2017-08` or `modified:2017`

You can **search within date ranges using square brackets and the TO keyword** `modified:[2017-08 TO NOW]`

You can **combine search terms using the AND keyword** `name:myfile.txt AND modified:[2017-08 TO NOW]`

11. Security & Password Features

Controlling who can access Foldr

Within ***Foldr Settings > Security > Permissions***, the Foldr administrator can control which users are permitted to use Foldr (from any client app or web app), Foldr Drive (legacy WebDAV access) and create and join Foldr groups used when sharing content. There are options available here to also permit or deny access to Foldr by location.

By default, the built-in Foldr Users group has an 'Allow' permission to 'Use Foldr' (web, mobile and desktop apps) and 'Connect via WebDAV'. This will allow any domain user or local Foldr user to log into Foldr. To restrict access to specific users or group, remove 'Foldr Users' and replace as appropriate with users or groups.

Click 'Add User or Group' to search for the LDAP or local users or groups that you wish to apply the permission. Note that Foldr will only search the Active Directory domain within the scope the LDAP Search DN(s) configured in **Integrations > Active Directory (LDAP).**

'Deny' entries always override 'Allow', the exception being where individual user permissions override groups.

The Foldr server also provides **Device Approval** which can be used where granular control is required over which users can use specific devices / apps. See section 12 for more information.

Location Based Access Permissions

Foldr allows the administrator to control *where* users are able sign in from. Rules can be created to permit or deny users or Active Directory groups based on the client IP address, IP address ranges or entire subnets.

Location based rules can be applied to all apps / connection methods globally within ***Foldr Settings > Security*** or granular location-based access rules can be configured on a per app basis within ***Foldr Settings > Devices & Clients***.

By default, users will be allowed to sign in from any location.

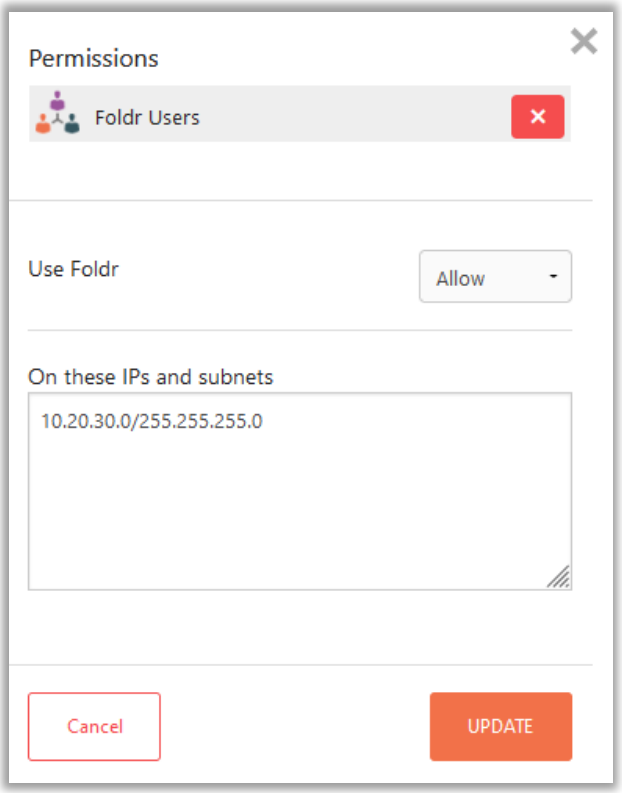
This feature can be useful to permit a security group access from inside the organisation network only, and/or to restrict exactly where users can sign in remotely.

From ***Foldr Settings > Security***, the field to configure the network details is available within '**Use Foldr**' and '**Use Foldr Drive**' (WebDAV connections). Networks should be configured one per line if multiple entries are required.

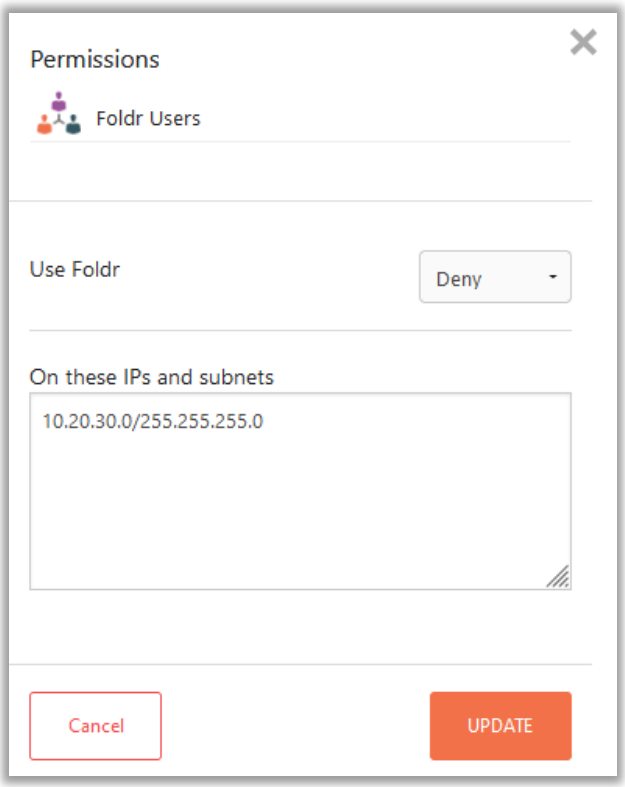
Accepted values are:

- Wildcard format: **1.2.3.***
- CIDR format: **1.2.3.0/24** OR **1.2.3.4/255.255.255.0**
- Start-End IP format: **1.2.3.0-1.2.3.255**

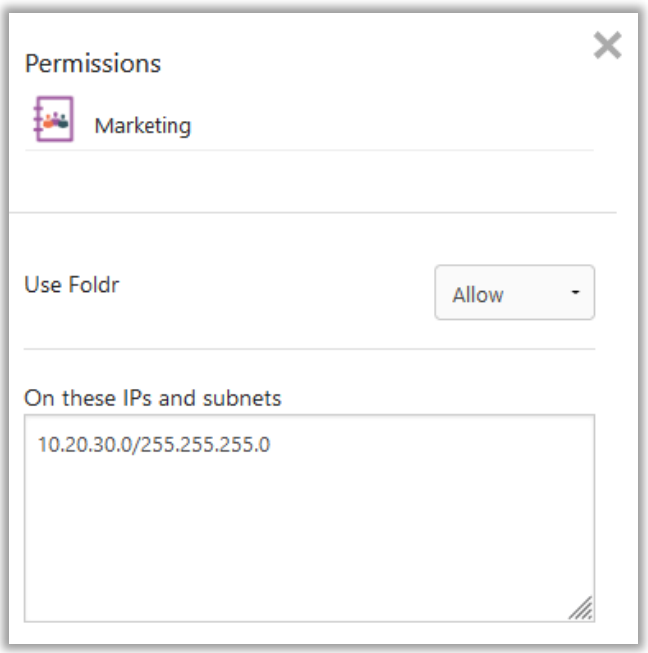
In the example below, the built-in group 'Foldr Users' (Everyone) is being configured with an allow rule for subnet 1.2.3.0/255.255.255.0 – This rule will result in all users ONLY being permitted to sign in from a client device on the 10.20.30.0 network. (client IP address of 1.2.3.1 – 1.2.3.254).



In the second example, the built-in Foldr Users group (everyone) is denied access from the same subnet. The result of this ACL rule would allow users to sign in from any location except network 10.20.30.0 using subnet mask 255.255.255.0



In the final example, the Active Directory group ‘Marketing’ is only allowed to sign from client devices on the network 10.20.30.0. Users in this group will be denied access if attempt to sign in from any other location, due to use of the ‘Allow’ rule.



Location Based Share Access

As well as being able to control where users / groups can sign in from, the same applies to storage permissions and share visibility.

Using the granular share access permissions, this gives the administrator the ability to only present a share if the client is signing in from a particular IP address or subnet, or you can force a share to be read only or writable from specific locations.

Password Settings

Password Caching

To provide support for existing and future product functionality (such as integration with other services), Foldr v4 automatically stores user's passwords once they have authenticated. Passwords are stored within an internal database and all values are encrypted using OpenSSL and the AES-256-CBC cipher. Furthermore, all encrypted values are signed with a message authentication code (MAC) to detect any modifications to the encrypted string.

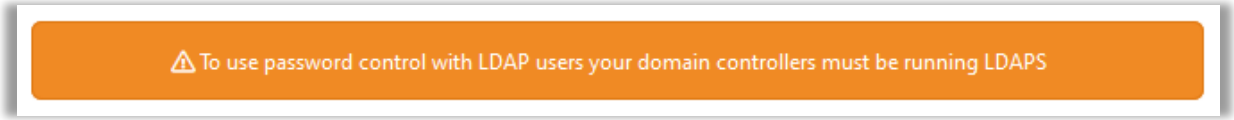
The administrator can disable password caching within ***Foldr Setting > Security > Password Settings*** if required. However, in this scenario a user's individual ACL permissions are not available and the appliance must connect to each SMB share using a global service account. This must be selected on the share configuration screen Access tab in conjunction with the 'Use service account for all access' toggle.

The Foldr administrator can optionally deploy Foldr so that the database containing configuration and other data (such as user credentials) is stored on a central, non-internet facing system and all user interaction takes place via satellite client access appliances.

Password Change Control

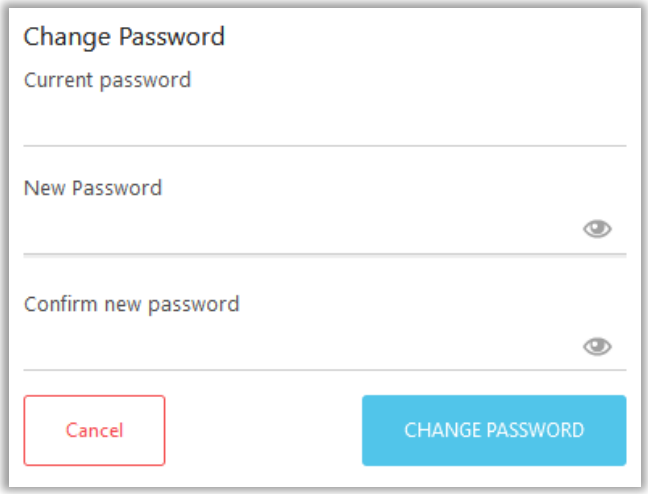
Foldr v4 provides users with Active Directory password control and password expiration handling for users connecting via a web browser or any of the desktop / mobile apps.

IMPORTANT – **Password change control requires the Active Directory domain to be using LDAPS. If LDAPS is not being used, you will see the following message:**



Users are able change the network password at a time of their choosing from 'Security Settings' in the web browser interface. If the organisation has a password expiration policy, and a user attempts to log into Foldr using an expired password they will be prompted to change it. If the 'user must change password at next login' flag is enabled for a user on the domain, Foldr will also allow the user to change their password as they log in.

Web app password change shown below:



By default, password control is ***disabled***, however the administrator can enable this feature within the ***Security > Passwords > Delegated Reset*** tab.

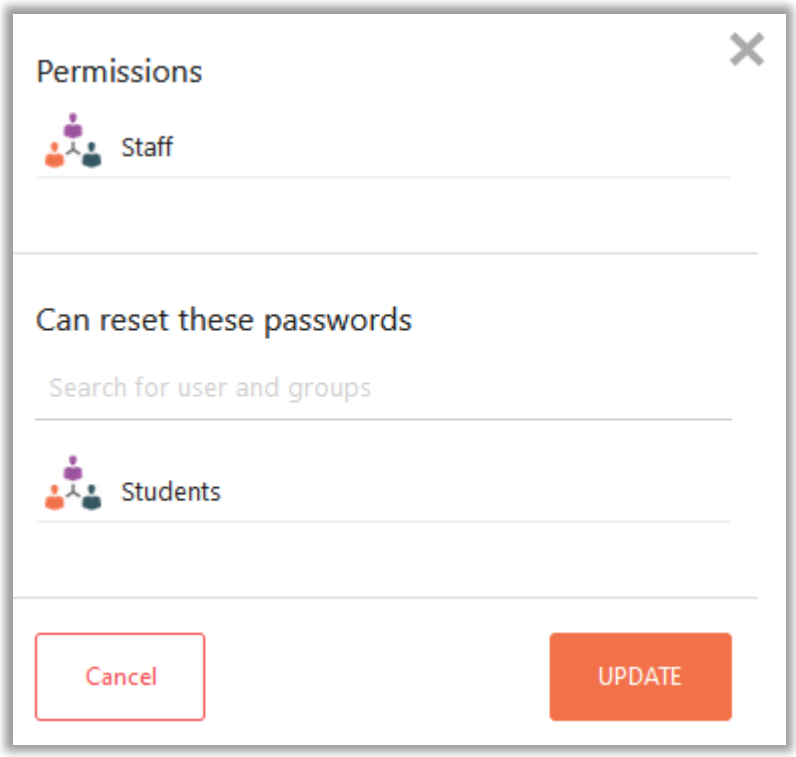
Delegated Password Reset (Grant permission to reset other user's passwords)

The Foldr administrator can also enable delegated password control to allow selected Active Directory users or groups reset other users network passwords. A new fixed password can be set by the delegated / trusted user at the time of the reset and they can optionally set the 'user must change password at next logon' flag.

This feature can be used to provide a convenient and secure way to allow trusted users to reset other user passwords. One use case for delegated password reset would be in an education environment where teachers could reset student network passwords from their mobile phone, tablet or desktop computer.

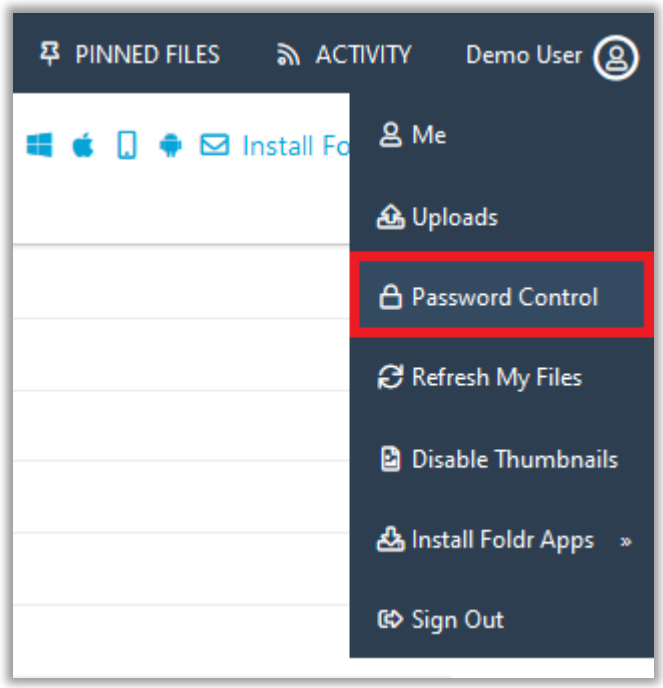
Delegated password reset is currently available in the web, iOS and Android apps.

Foldr Settings interface – Delegating Password Control to a Staff group to reset Student passwords in Active Directory

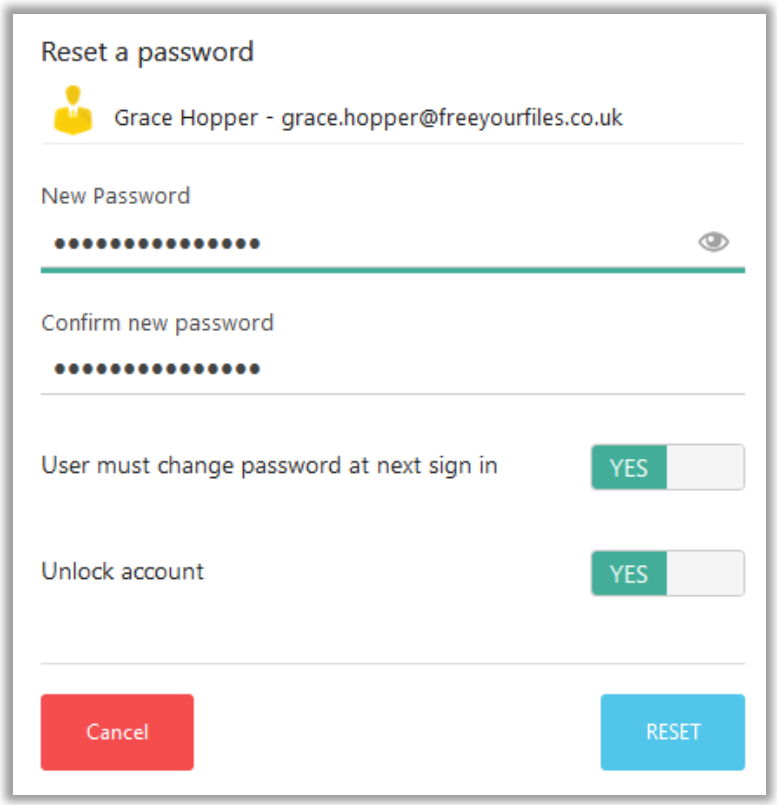


User web app interface – Resetting another user's password

Selecting **Password Control** form the top right menu in the web app will present the following dialog.



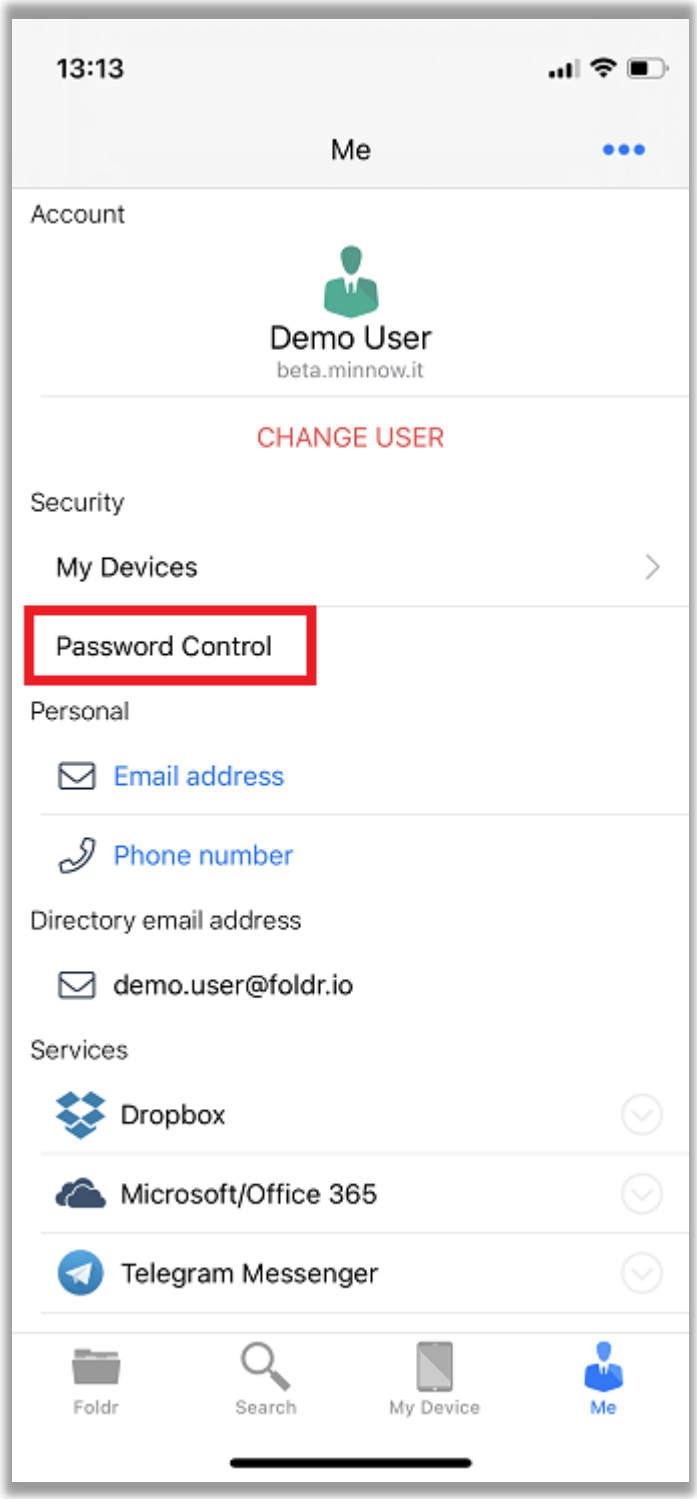
The user can then search the Active Directory domain, set the new password, and optionally toggle the 'User must change password at next login' flag.



If the change password at next login flag is set, the *grace.hopper* account in the example above will be able to change this at next logon through Foldr web, mobile desktop apps.

iOS and Android – Resetting another user's password

Once signed into the app as a user with permission to use delegated password control, tap the ME tab the bottom of the screen > Password Control.



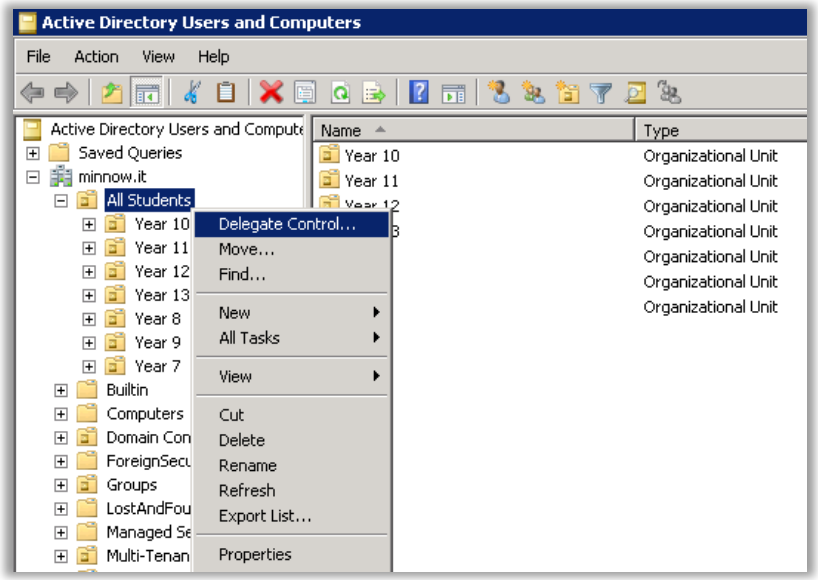
A search dialog will be displayed, where the user can search Active Directory. Once the user has been selected, you can then reset their password and optionally toggle the 'use must change at next sign in' if required.

Permissions Required for Delegated & Self-Service Password Reset

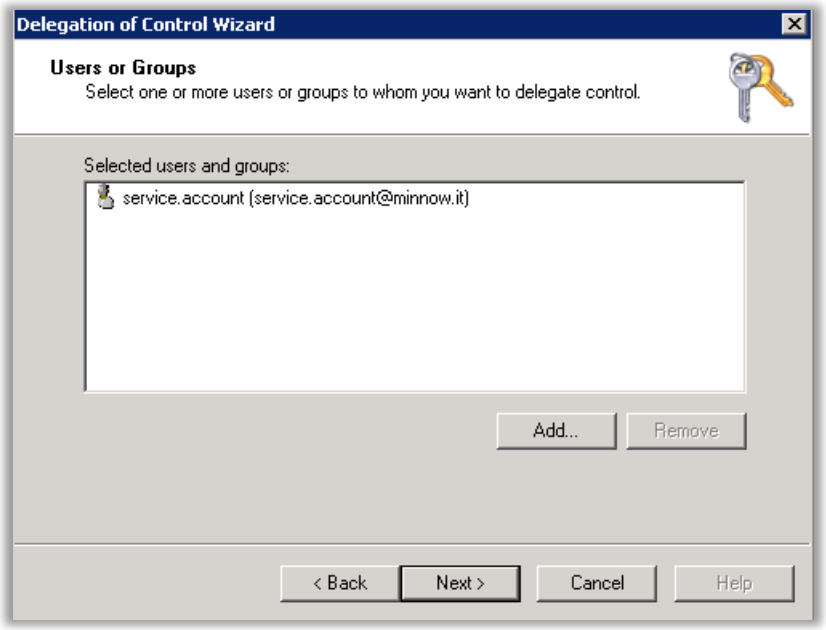
The Foldr appliance uses the main service account configured within ***Foldr Settings > General > Configuration*** to perform the password reset request on behalf of the delegated (trusted) user. As such, the service account configured requires the appropriate permission to reset the target user's password within Active Directory.

Windows Domain Controller – Granting permissions to the Service Account

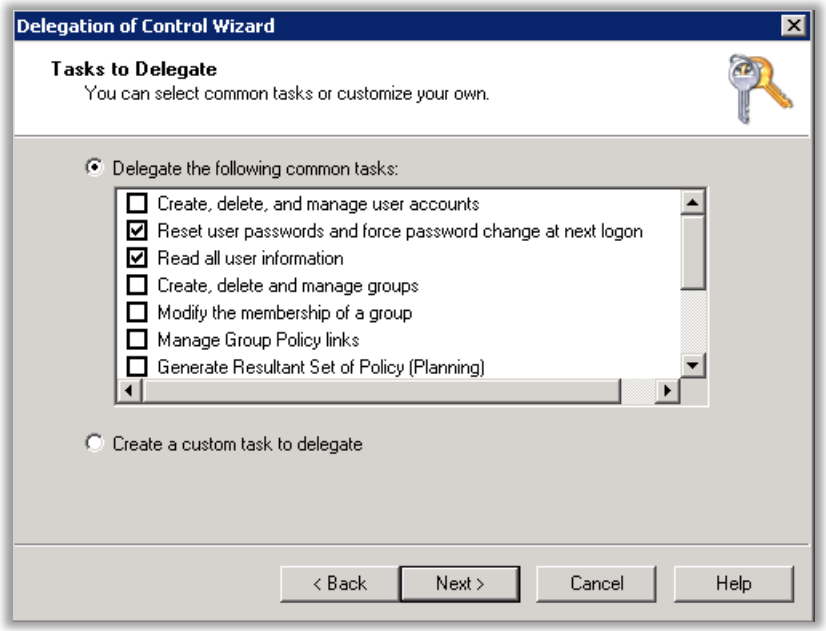
To grant the service account user password reset permissions on the domain controller you can use the Delegation of Control wizard within Active Directory Users & Computers.



Right click the target OU and select Delegate Control



Select the Foldr service account on the domain and click Next



Check '*Reset user passwords and force password change at next logon*' and '*Read all user information*' and click Next

Complete the Delegation of Control Wizard by clicking Finish

Self-service Password Reset (SSPR) & Notifications

Using this feature, users will be able to reset / change a forgotten Active Directory password. As with the other password features in Foldr, it requires **LDAPS** to be enabled on the Domain Controllers and the LDAP Server in Foldr Settings prefixed appropriately with ldaps://

Self-service password reset allows the user to click a forgotten password link on the web app sign in screen, passing a captcha and then selecting a notification method to receive a reset code. Once the user receives the code, they can enter it into the SSPR reset interface and change their password. The Foldr administrator can enable one or more notification channels as required.

Notification channels:

Directory Email Address – This is the email address as specified for the user in Active Directory (the AD attribute labelled 'mail'). If available, this will be automatically populated in and shown in Foldr within the 'Me' menu item in the web app.

User Email Address – User configurable email address, typically a personal email address will be used. This must be configured in advance by the user before it can be used for self-service password reset.

Directory Mobile Number – This is the mobile telephone number as specified in Active Directory > Telephones > Mobile (the attribute labelled 'mobile'). If available, this will be automatically populated in Foldr within the 'Me' menu item in the web app.

User Mobile Number – User configurable mobile telephone number, typically a personal mobile number would be used. This must be configured in advance by the user before it can be used for self-service password reset.

Telegram Messenger – Allows a user to sign up for notifications to be delivered via the Telegram Messenger app. Telegram must be configured in advance by the administrator, which involves creating a Telegram 'bot' for the organisation which will automatically send codes to users as they are requested.

Requirements

1. **LDAPS** must be enabled on the Active Directory domain.

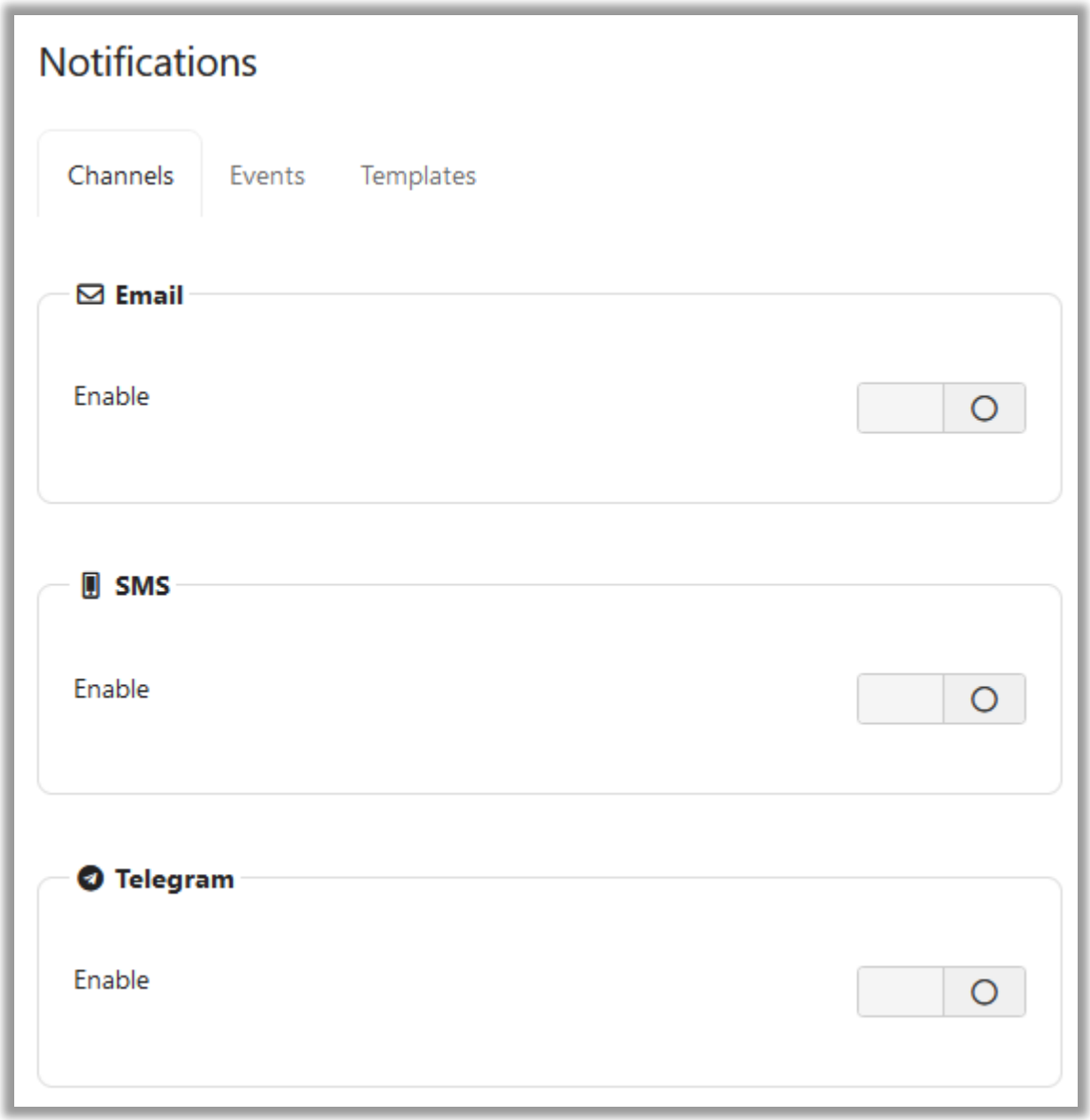
2. The main service account (configured under ***Foldr Settings > Integrations > Active Directory (LDAP)*** must have permission to reset user's passwords and read user information, this is used to query group membership. Follow the delegation of control wizard instructions above.

Notifications

Before notifications are available to the administrator for use with the Self-Service Password Reset feature in Foldr, they must be enabled and configured:

Security > Notifications provides an overview of the Notification Channels that are enabled on the Foldr server.

If no notification channels are enabled on the appliance, the administrator will be unable to make them available to users with the self-service password reset option.



Email – By enabling this notification, users will be able to select from either the email address specified for their account in Active Directory, or a personal email address which can be set within the Top right menu > 'Me' item in the web app.

SMS – When enabled, the administrator can choose between the following SMS providers:

Nexmo
Twillio

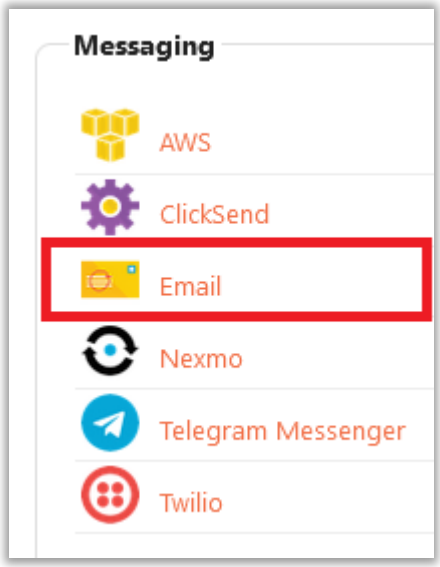
Amazon AWS

In order to use one of these providers, you will need to sign up with one of the above and generate an API key / secret and paste it within ***Foldr Settings > Integrations*** as appropriate.

Telegram Messenger – When enabled, users can receive notifications / password reset codes through the popular Telegram Messenger app.

Configuring Email Notifications

Email notifications require the Foldr server's email settings to be configured correctly within ***Integrations > Messaging > Email*** so the Foldr system can send email.



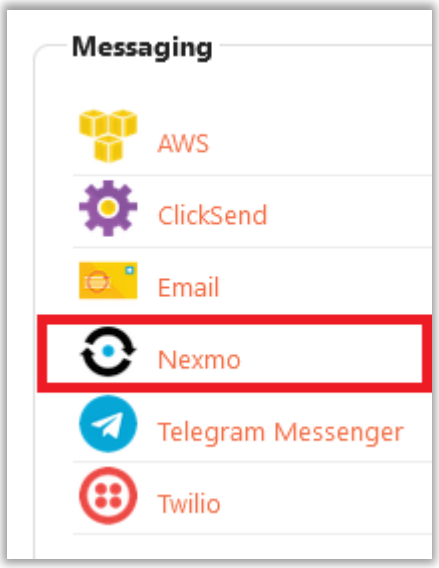
A user's corporate email address is stored in Foldr automatically (this is pulled from Active Directory as they sign in) and users can register their own personal email in Foldr. Personal email addresses for users may also be bulk imported by an administrator

Configuring SMS Notifications

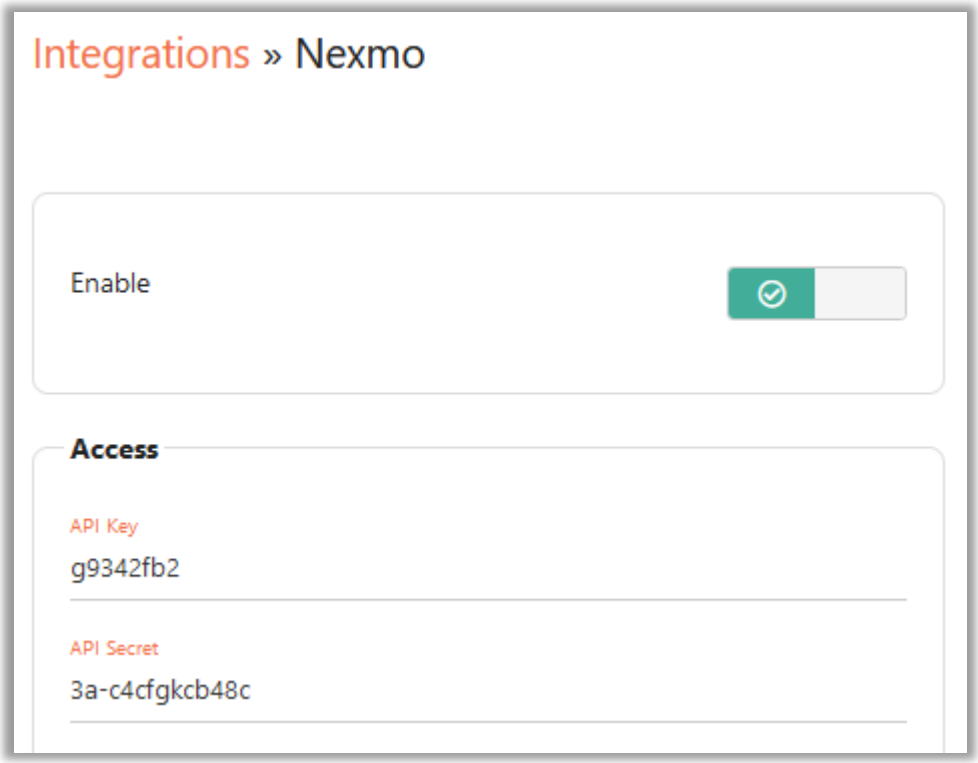
1. Firstly, sign up for an account with the SMS provider and obtain your Nexmo API key and secret. Twilio refer to this as the 'Account SID' and 'Auth Token', Amazon uses a service account which can be configured under ***Integrations > Service Accounts.*** You can create multiple Amazon service accounts if you require different credentials for presenting S3 storage areas and SMS services.

Example - Configure the Nexmo SMS Service within ***Integrations > Messaging***

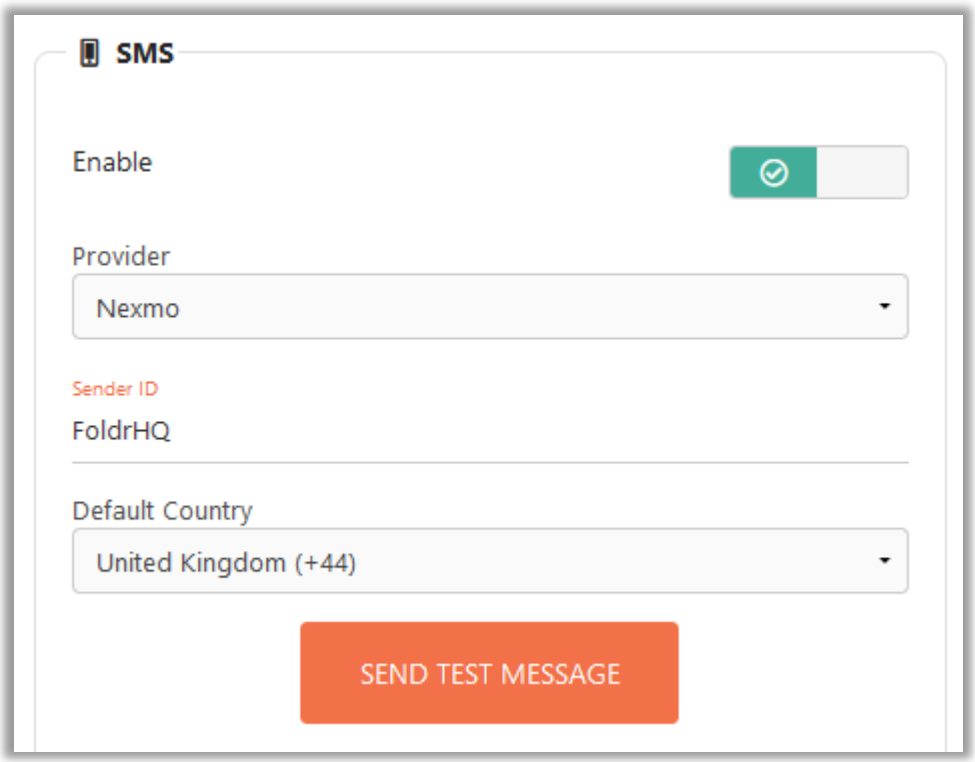
Select Nexmo



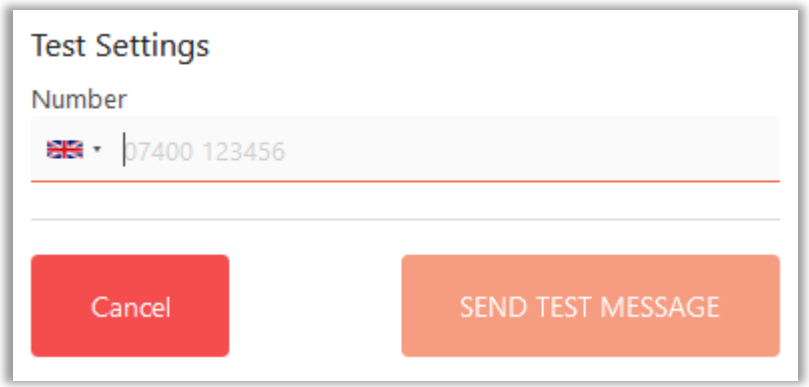
Enable the integration and enter the API Key and API Secret



*Navigate to **Foldr Settings > Notifications** and Enable the SMS option, select Nexmo as the provider and enter your Sender ID and Default Country code.*


SMS
Enable
Provider
Nexmo
Sender ID
FoldrHQ
Default Country
United Kingdom (+44)
SEND TEST MESSAGE

At this point you can test the integration by entering a valid mobile number and click ‘SEND TEST MESSAGE’ button.



If the SMS is successfully received, the integration is complete.

Configuring Telegram Messenger Notifications

Telegram Messenger is a popular instant messenger service and has client apps for all major platforms. Foldr can integrate with the Telegram API to provide self-service reset codes to users, without the cost associated with using an SMS provider. Users are required to link a Telegram account in Foldr before it can be used for SSPR.

Password reset codes are sent via a Telegram bot (an automated service that receives the self-service notification from the Foldr appliance and delivers the codes to end users)

Creating the Bot

If you haven't already done so, sign up for Telegram by downloading the app from the iOS / Android app store and register with the service by entering your mobile number.

Once you have Telegram on your device, send a blank message to @BotFather and proceed through the following steps:

1. You will receive a welcome message.

2. Type **/newbot** to create your bot.

3. Give your bot a name.

4. Enter a username for your bot

5. You will receive a confirmation message stating the bot was created and the unique API token will be displayed.

6. The username and API token can now be copied into the Telegram Messenger service within ***Foldr Settings > Integrations > Messaging > Telegram Messenger***.

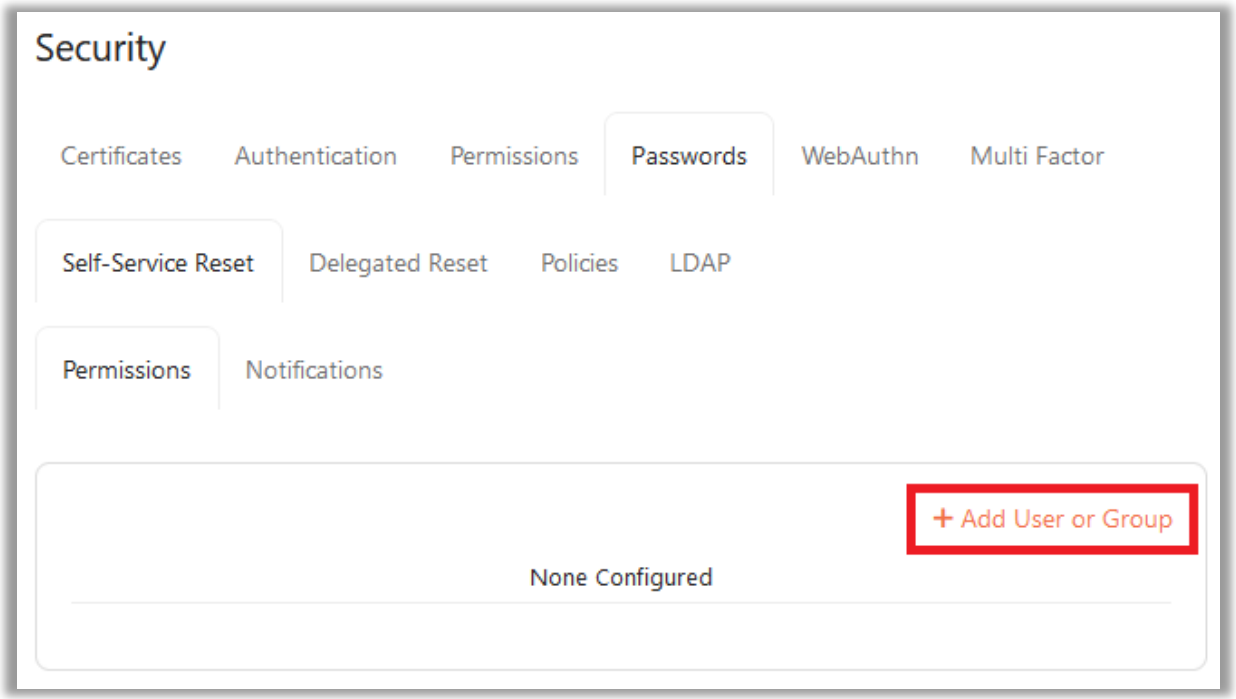
The integration steps are now complete. The administrator can now enable Telegram Messenger within ***Foldr Settings > Notifications*** and make it available for use with self-service password reset through ***Foldr Settings > Security > Passwords > Self-Service Reset***.

Before it can be used in a self-service password reset scenario, users will need to link their Telegram account from within the ***Foldr web app > Me (Top right menu) > Services*** and it is recommended this is done on a PC or Mac with the Telegram client installed.

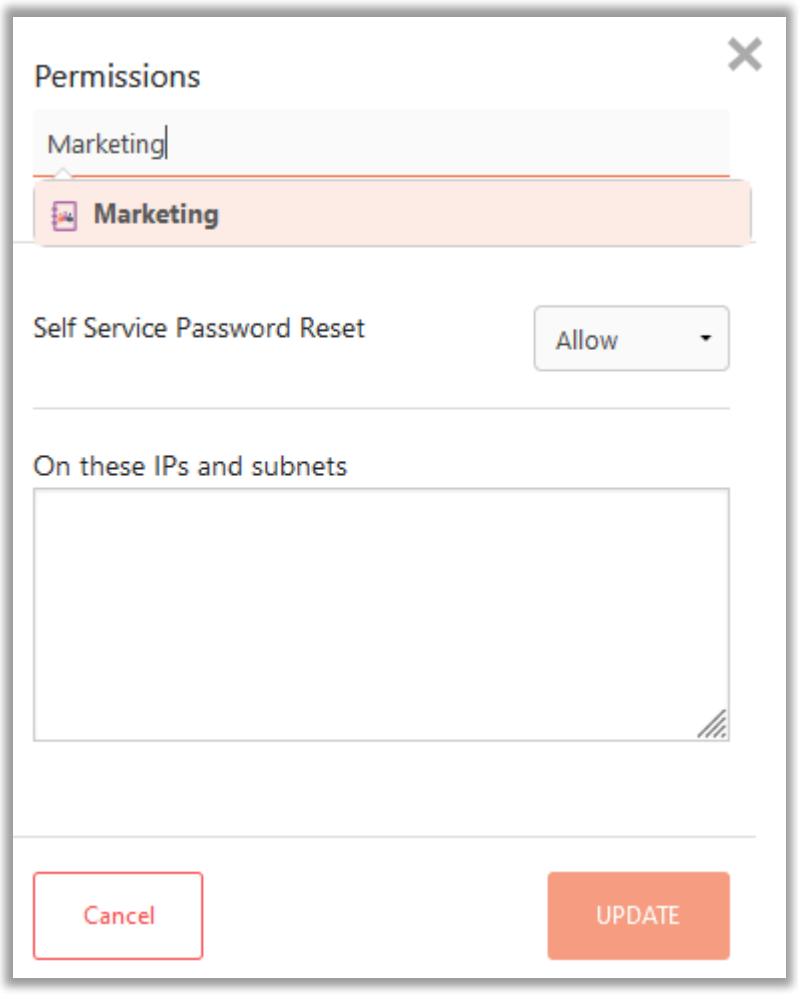
Enabling Self-Service Password Reset

Now the chosen notifications have been configured and enabled, the self-service password reset feature must be enabled.

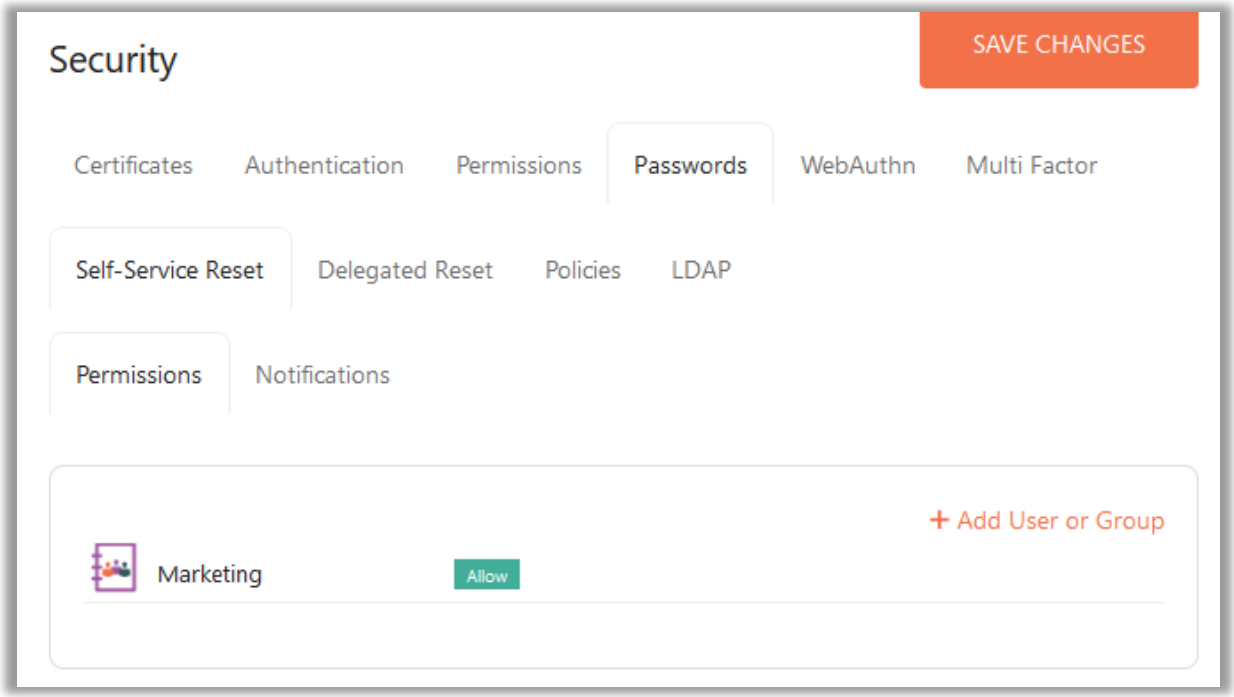
Within ***Foldr Settings > Security > Passwords > Self-Service Reset*** on the Permissions tab, click + Add User or Group



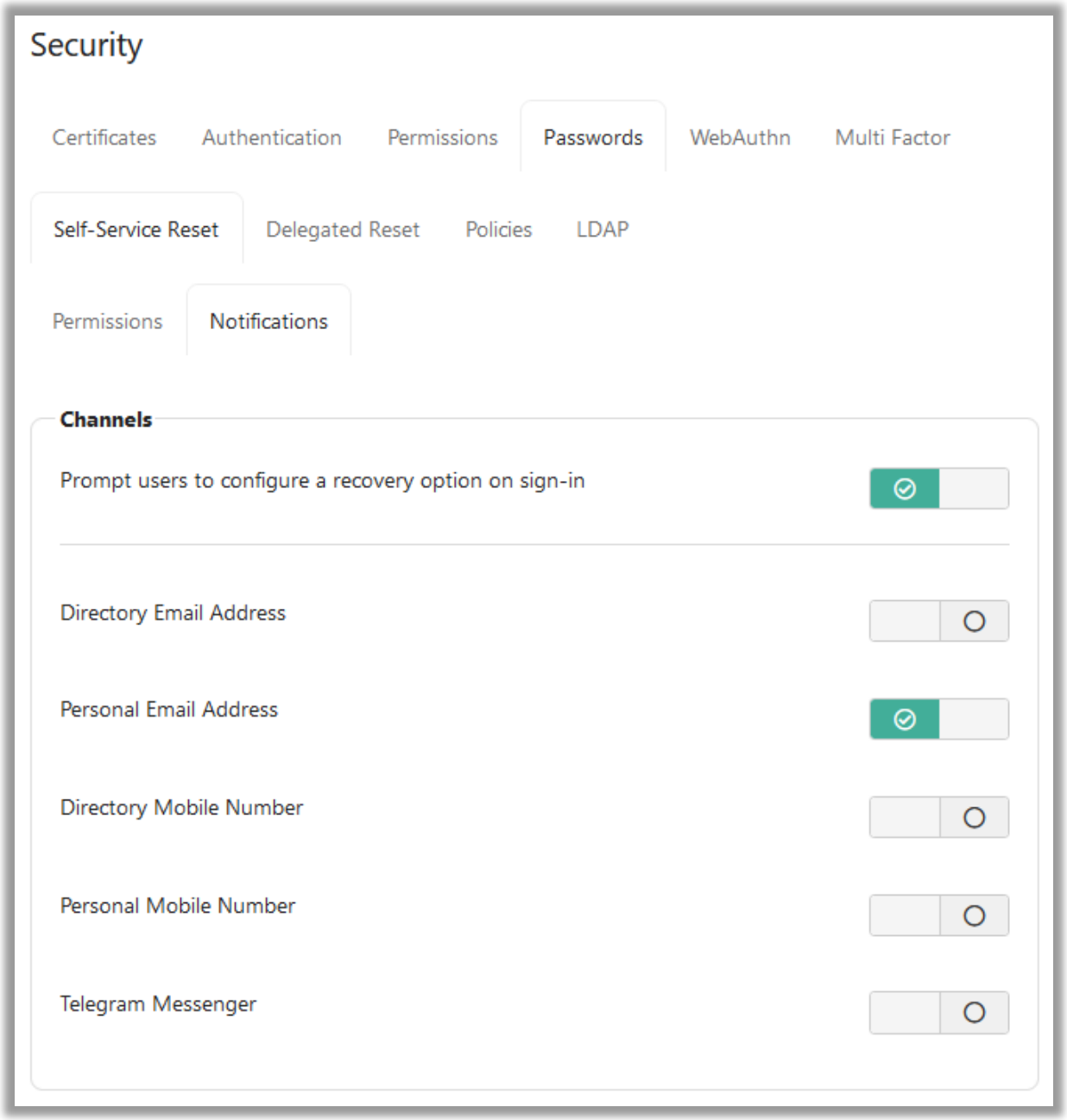
Search for a group or individual user that is to be permitted to use the Self-Service Reset feature. In the example below, a security group in Active Directory called 'Marketing' is being used.



Click **Update**. Now click the **Notifications** tab



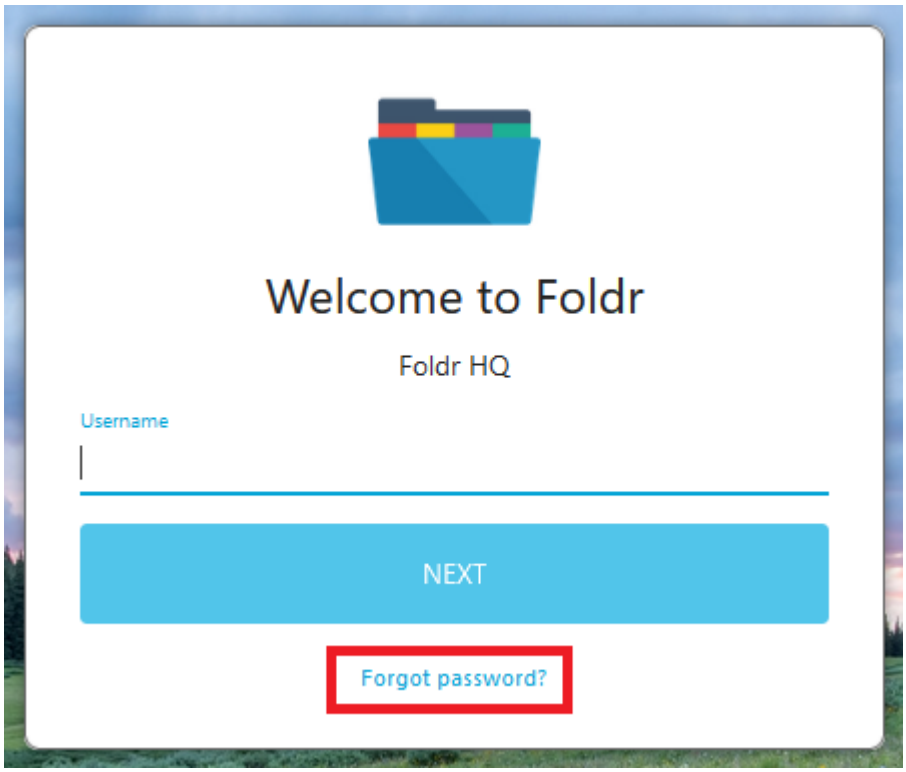
On the Notiifications tab, enable the notification channels / methods that you want users to use to receive their reset codes. In the example below, only Personal Email Address will be used.



Note that '**Prompt users to configure a recovery option on sign-in'** is enabled by default. With this toggle enabled, any user of the Marketing group will be prompted automatically to provide their personal email address for self-service reset purposes when they sign into the Foldr web app – this only applies to the web app, users are not prompted for recovery information in the mobile or desktop apps.

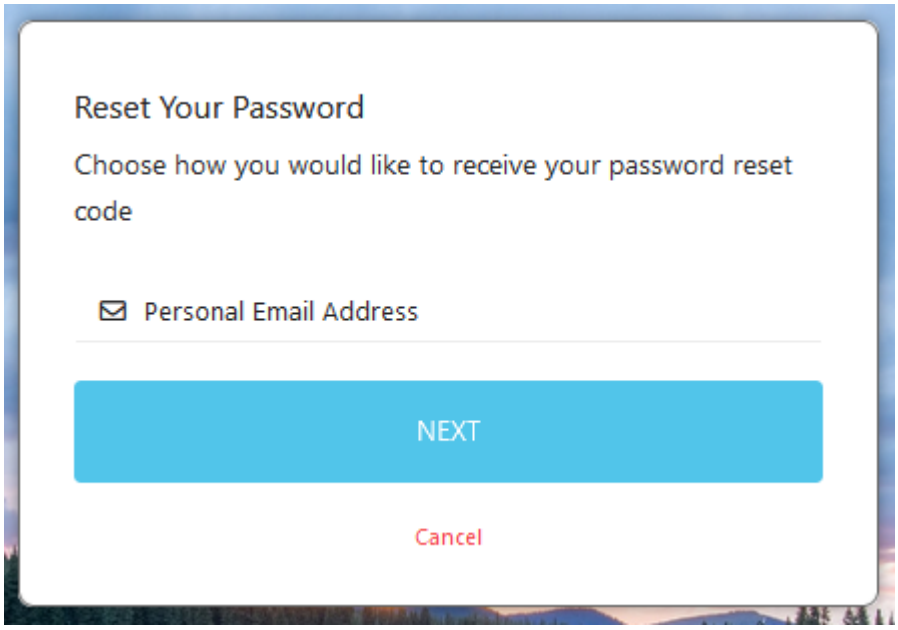
User Experience – Using Self-Service Password Reset

1. The user clicks the '*Forgot Password?*' link in the web app login box.

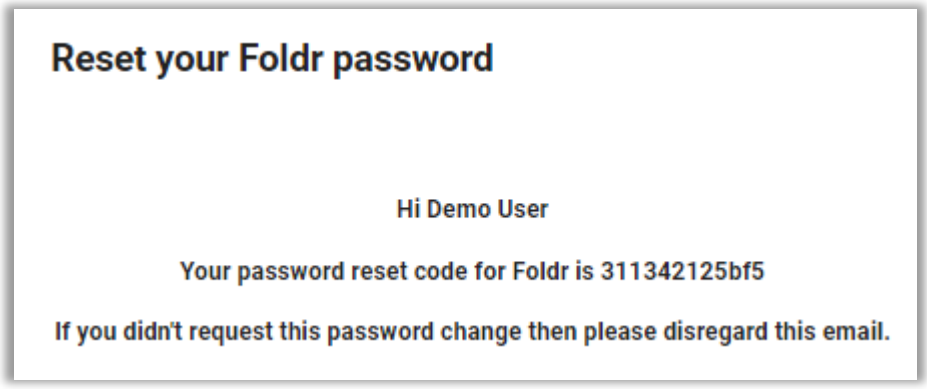


2. The user enters their username, and the browser will briefly display a puzzle that will be solved by the client automatically (similar to passing a captcha).

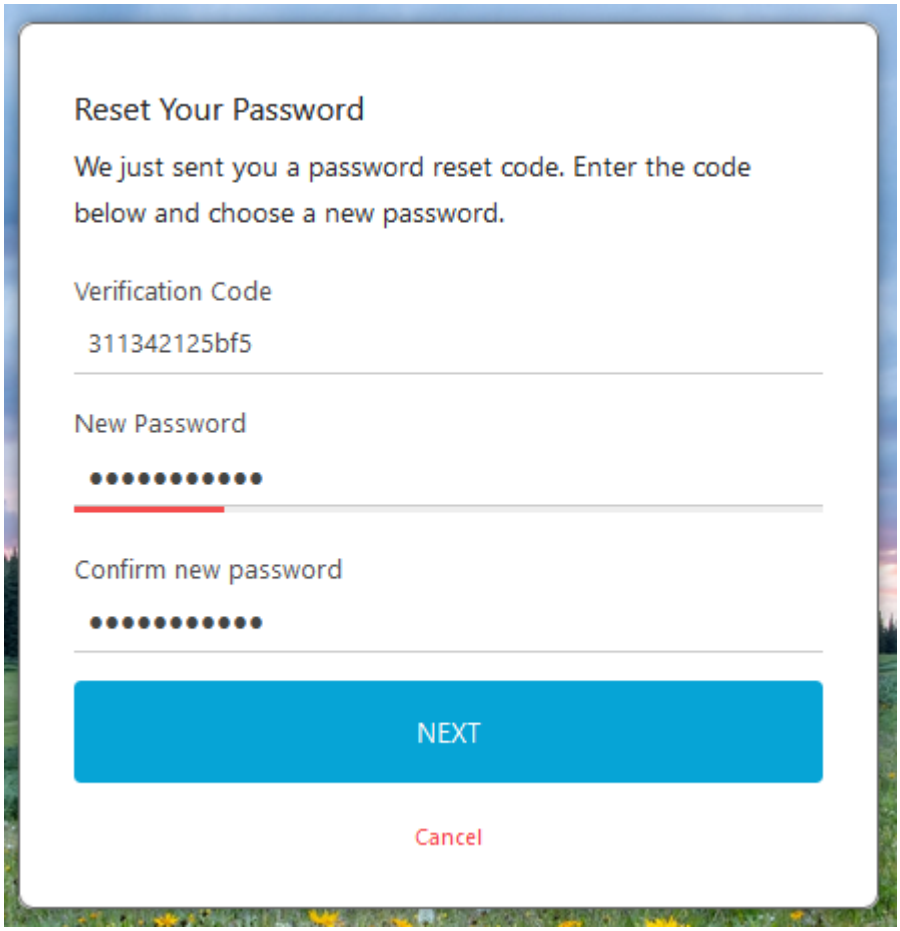
3. The user selects the notification method to receive their password reset code. Note that only Personal Email Address is available as an option to receive the code.



4. Obtain the reset code – in this example we selected personal email.



5. The user enters the reset code into the verification code field and then enters a new password into both 'new password' and 'confirm new password'. Click Next.



6. The user clicks **Next**.

If the password was changed successfully, you will receive a success notification and you will be placed back at the login screen.

12. Device Approval

By default, the Foldr server will allow any client device / browser to connect and users will be able to sign in.

For environments that require tighter control over who can sign in, and from what device, the Foldr server includes with a powerful security feature called Device Approval. If enabled, this feature will require client devices to be pre-approved by an administrator before users can sign-in and access corporate files. Device approval may be enabled on an individual per-app basis (web, Windows, macOS, iOS and Android) and may be used in conjunction with other security features, such as two factor authentication or WebAuthn.

Automatic approval policy rules may be configured to automatically approve users and their devices when connecting from devices on specific IP addresses or subnets.

When Device Approval is enabled for an app, any user that attempts to sign in will be prompted by an alert informing them that approval is required, and a unique approval identifier (ID) is shown. The approval ID is unique for each user on each device. The ID must be sent to the Foldr administrator, who can then use it to search quickly across all devices and then grant specific users the ability to use that app or browser.

Web app support

The web app is fully supported for Device Approval with all modern browsers, and each browser (Chrome, Firefox etc) is considered a separate 'device' – so a user permitted to use Chrome on a Windows 11 PC will be unable to use any other browser, such as Edge, until the administrator also approves the Edge browser. Note that a browser will remain approved by the server, until the user clears their browser cookies. As such, incognito / private browser sessions are not recommended with this feature.

Note - Internet Explorer (all versions) do not support device approval.

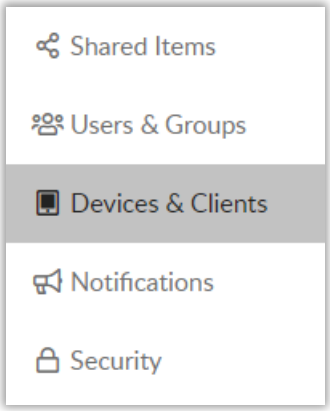
App compatibility

All Foldr apps (desktop and mobile) support device approval.

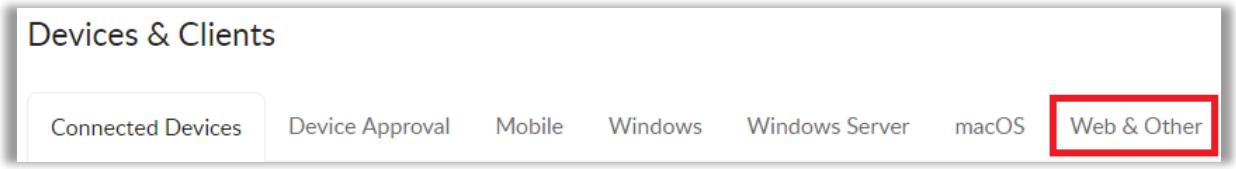
Enabling Device Approval

In this example, device approval will be enabled for the web app, but the process is the same for any other app (desktop or mobile)

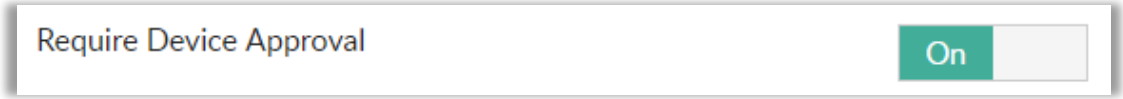
1. Sign into the Foldr Settings admin UI and navigate to the **Devices & Clients** tab



2. Click on the **Web & Other** tab



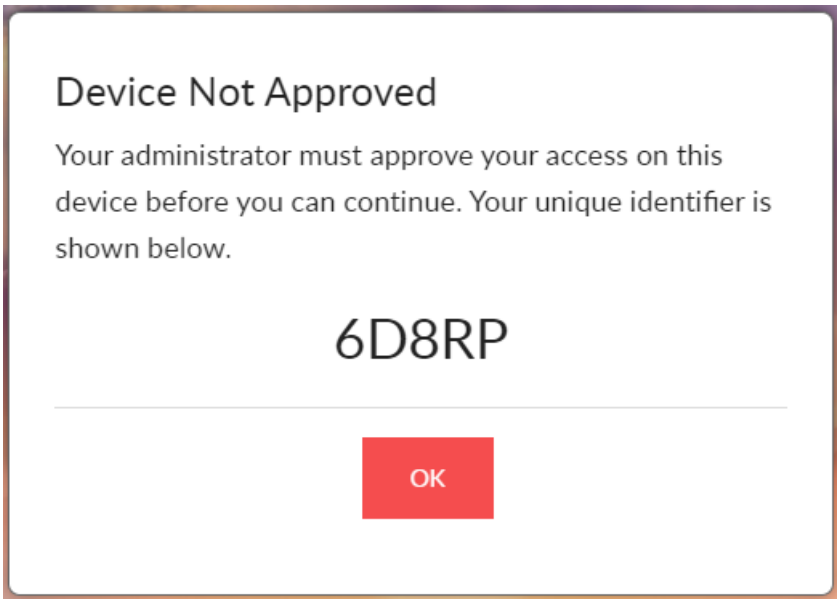
3. Enable the toggle '**Require Device Approval**'



4. Click **Save Changes**

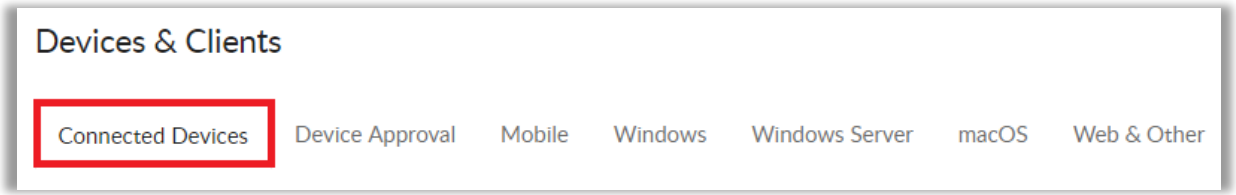
This is a global setting that will apply to all users of the web app in this case.

A user trying to sign into the web app will now be presented with the following after signing in:

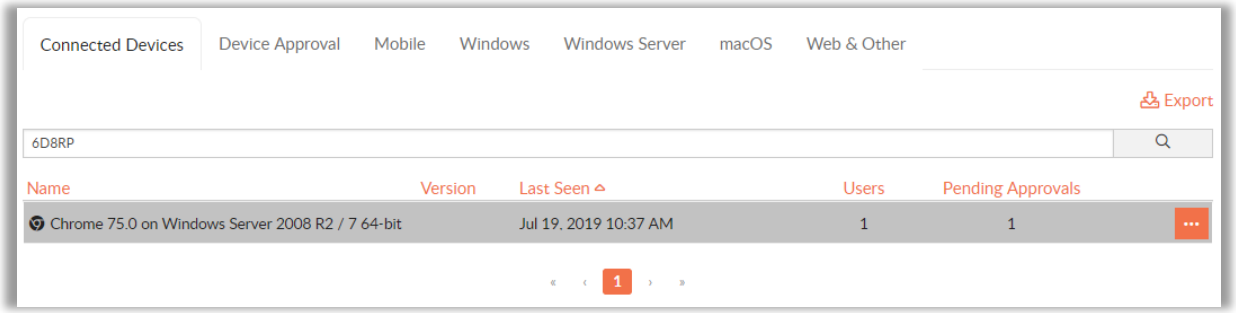


The user would need to pass their unique identifier above to the administrator (6D8RP in this case)

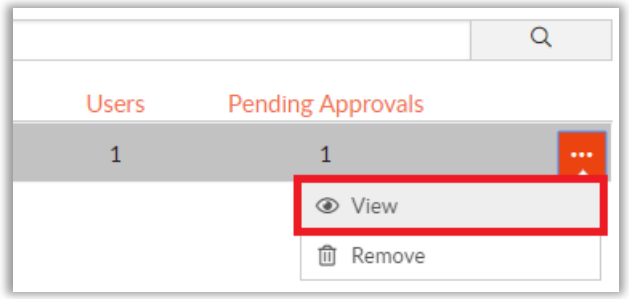
5. The administrator can then search for the user's device/app in ***Foldr Settings > Devices & Clients > Connected Devices***



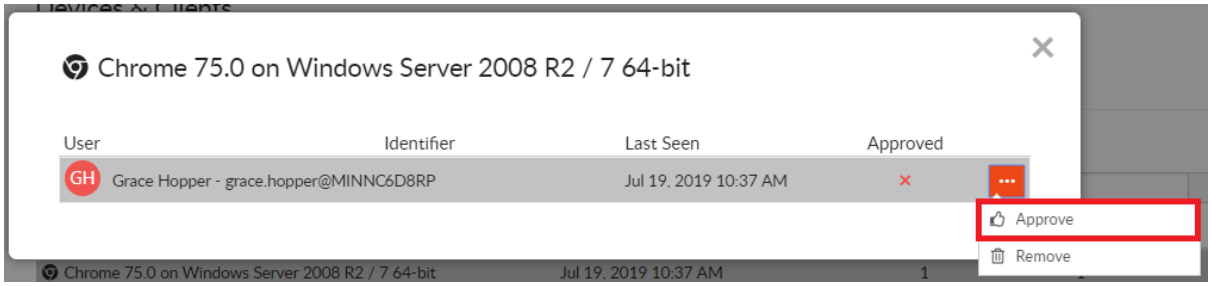
6. Enter the identifier into the filter box to quickly locate the user's device:



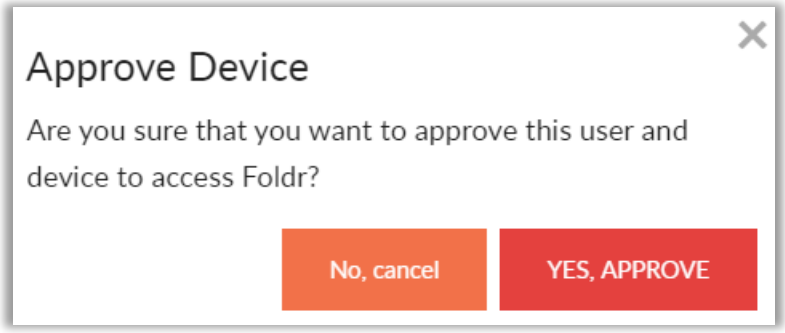
7. Click the in-line button > View to view any users associated with the device/browser



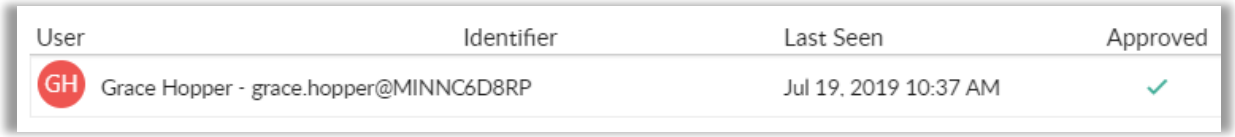
8. Click the in-line button > Approve to approve the user for this browser



9. Confirm the selection by clicking Yes, Approve



10. The user's status will change to show a green tick, signalling that the user 'grace.hopper' in this case is approved and will now be able to sign into the web app.



Revoking user's access (using Device Approval)

In the event that an administrator needs to revoke access for a user, this can be achieved either by deleting the device/browser item from ***Foldr Settings > Devices & Clients > Connected Devices*** or by removing their 'approved' status on that device.

To do this, click the in-line button for the user concerned and select REMOVE

The users status will update to show a red cross, signalling that they are not approved to use the device/browser and should they attempt to sign in they will be presented with a new unique identifier.

13. Other Security Features and Considerations

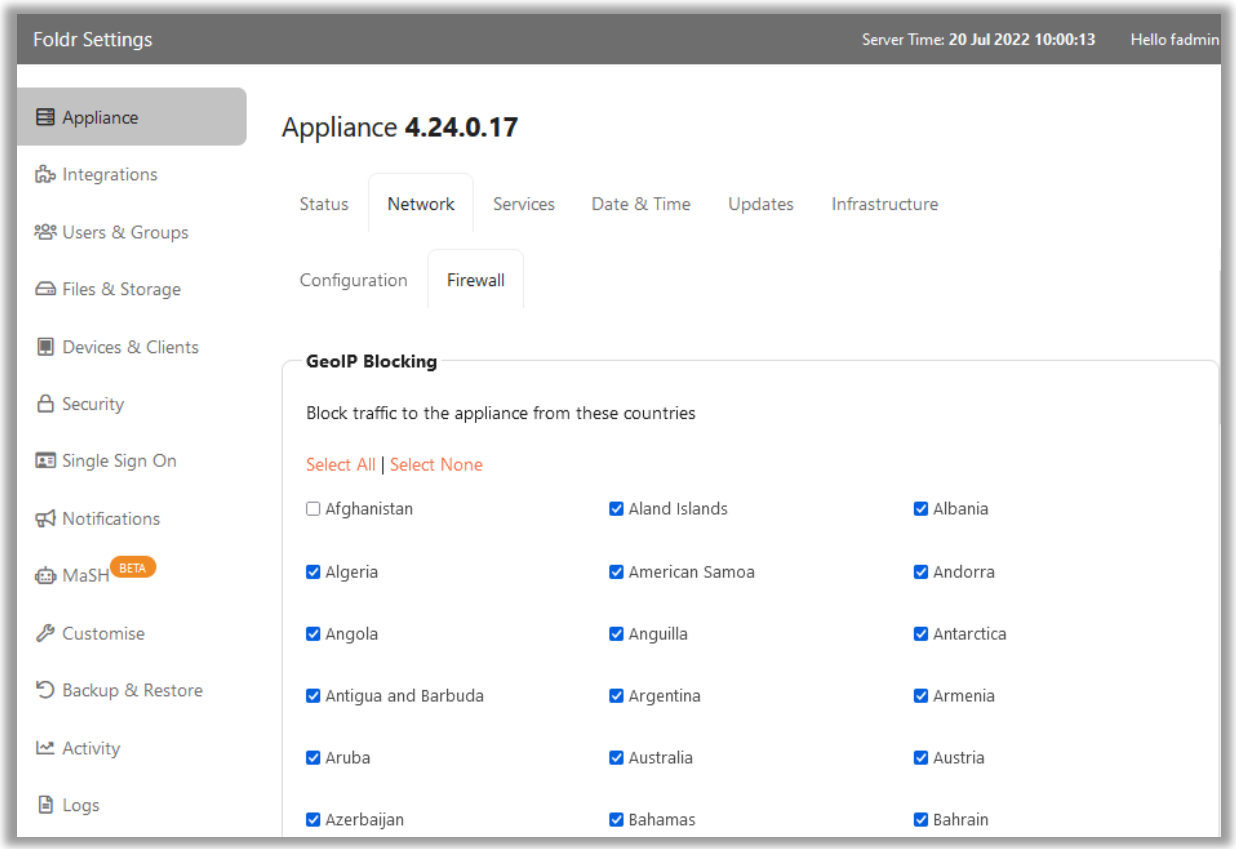
Geo-Location Blocking

The Foldr Server release includes a geo-location blocking feature for the server's built-in firewall. This allows administrators to block/permit access to Foldr by specific country.

Important - Let's Encrypt SSL Certificates

Where Let's Encrypt SSL certificates are being used on the Foldr server, it is important to **allow access from the United States** as they are based there. Failure to permit US access to the Foldr server, will result in the SSL certificate installation or renewal (which occurs every 60 days) to fail.

To configure geo-blocking, navigate to ***Foldr Settings > Appliance > Network > Firewall***



Check each country manually that you wish to *__BLOCK__* or alternatively (recommended) use the *Select All* option and uncheck the specific countries that you wish to permit access from.

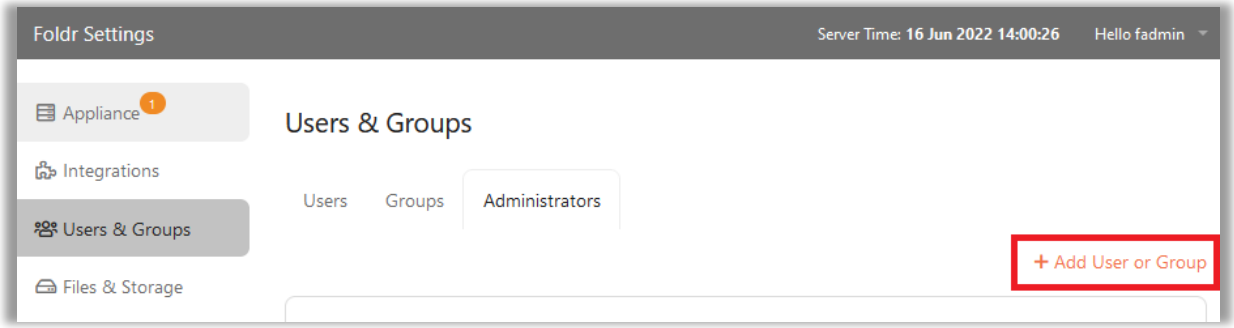
To confirm your selection, click **SAVE CHANGES**

Delegated Administrators

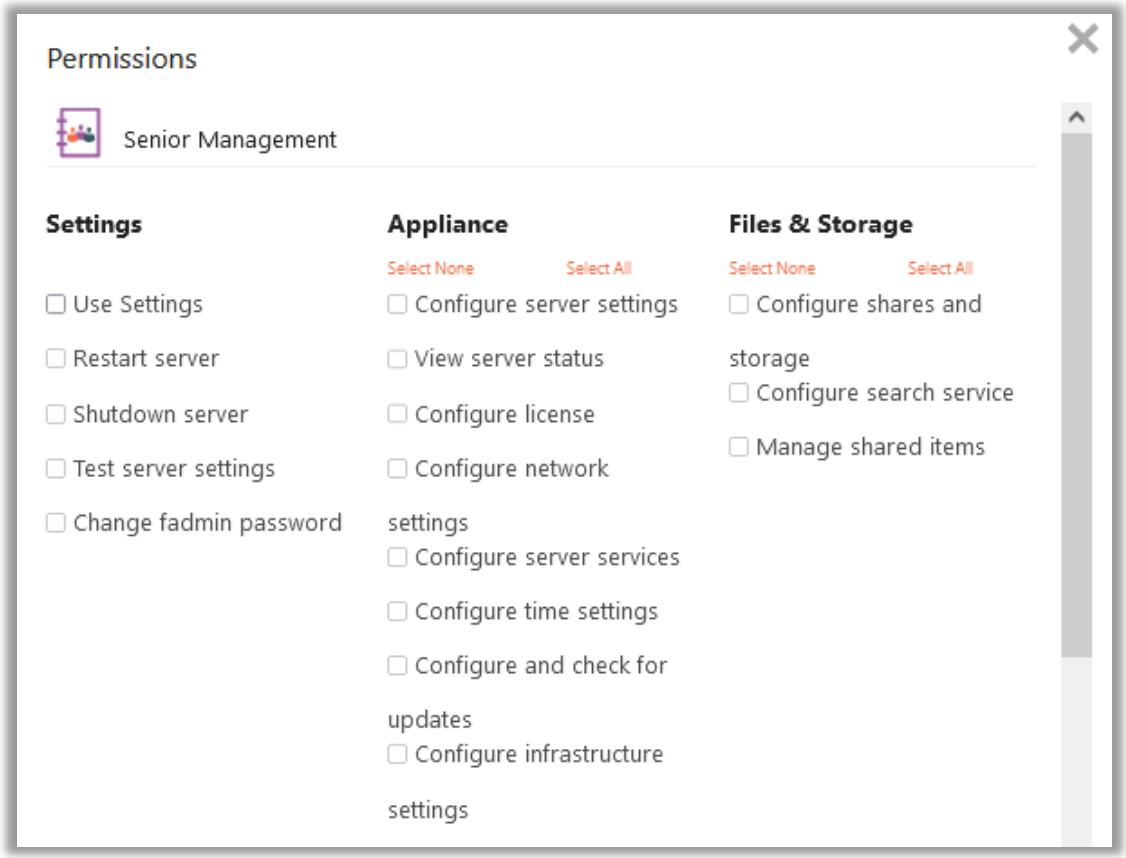
The Foldr server supports sub administrators to delegate access to Foldr Settings. Local or external LDAP (Active Directory) users/groups can be granted access. The main built-in fadmin administrative account can still be used alongside any nominated LDAP/local accounts.

There is a comprehensive set of permissions and users can be presented with only specific areas of the Foldr Settings admin interface as required. As an example, this could be used to allow a group of users to sign in and view the user Activity logs only, while not being able to view or make other changes to the system.

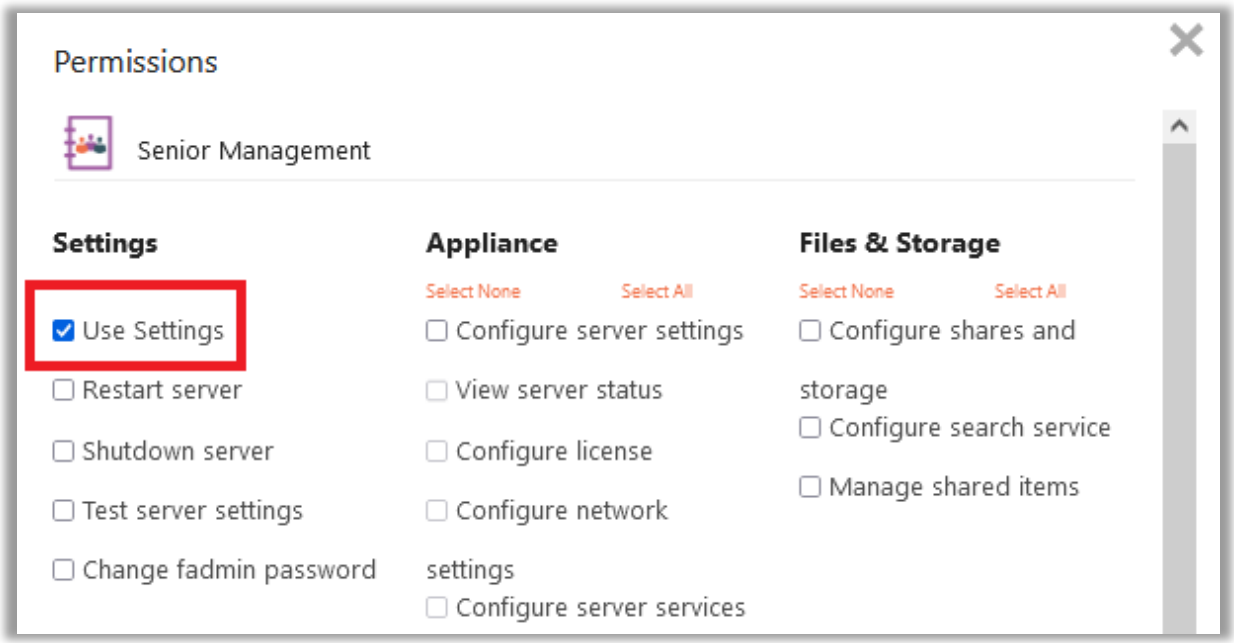
1. Navigate to ***Foldr Settings > Users & Groups > Administrators*** and click **+ Add User or Group**



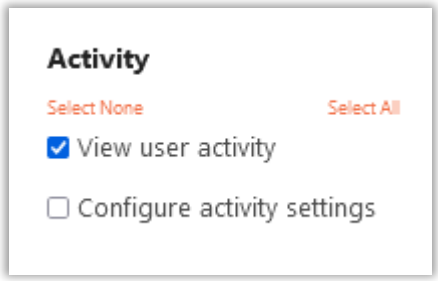
2. Search for a user or group as required.



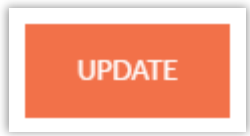
3. Select '**Use Settings**' – This is vital, or the user will be unable to sign in. Other permission elements become active when this is checked.



4. Check the additional permissions that you wish to grant to the user / group. In this example we will be allowing anyone in Senior Management to view the user activity logs.

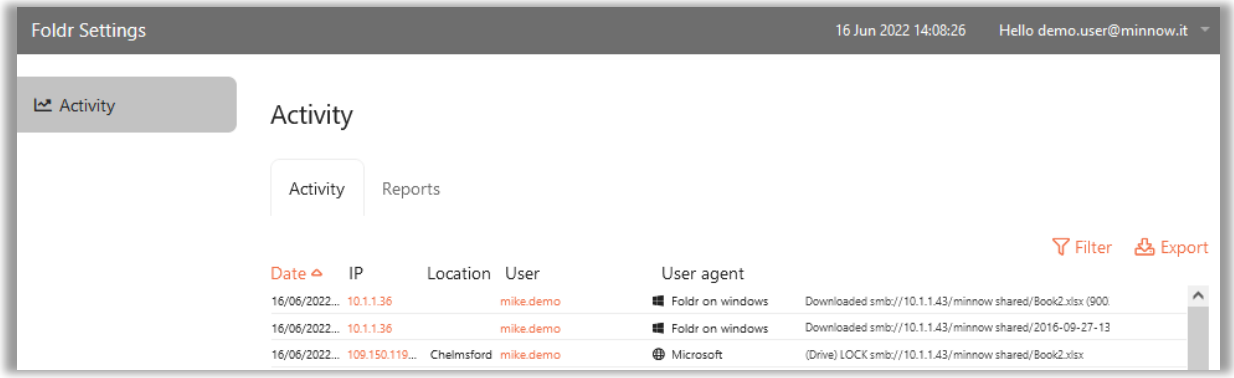


5. When you have finished selecting the permissions required, click Update (bottom right)



6. Click **SAVE CHANGES** to confirm (top right)

In the example above, any member of the Active Directory group 'Senior Management' can now sign into the Foldr Settings interface (https://address-of-foldr:30537/settings) and will only have access to the Activity menu.



Root Console Access

The root account on the Foldr appliance is **not accessible to the end user or Foldr technical support**. By design, there is no backdoor account with a static password into the appliance (other than ***fadmin*** *or* ***tadmin*** *in multi-tenant mode*). The root account has a complex, randomised password and this password is automatically changed again upon each system boot.

In the event of technical support requiring greater access to the appliance console for troubleshooting purposes, a dedicated account (fsupport) is available which can then sudo as required to run commands.

The fsupport User (Foldr Support)

The fsupport account password is randomised upon each system boot and is accessible only to Foldr technical support by decrypting the password once the customer enables 'Technical Support Mode' (option 2 from the VM console menu or issuing the command support-enable from the console)

When the menu option is selected, an encrypted string is available to technical support in the browser (on SSL port 30537) – the encryption key to decrypt this is composed of a unique hardware identifier on each appliance and a unique support ID string stored within the customer licence key.

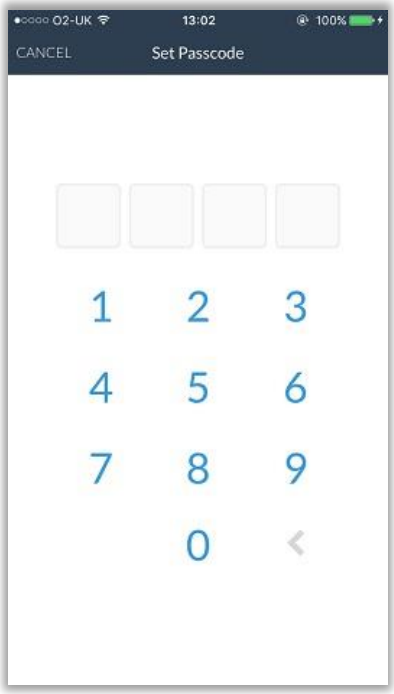
Authentication Rate Limiting

Foldr v4 includes a default limit set that will prevent a user signing in after 10 failed attempts in one minute. The user will then need to wait a further 60 seconds before any login attempts will be processed. This feature has been designed to mitigate against malicious attacks on the service such as brute force attempts on account passwords.

Mobile Devices & Security

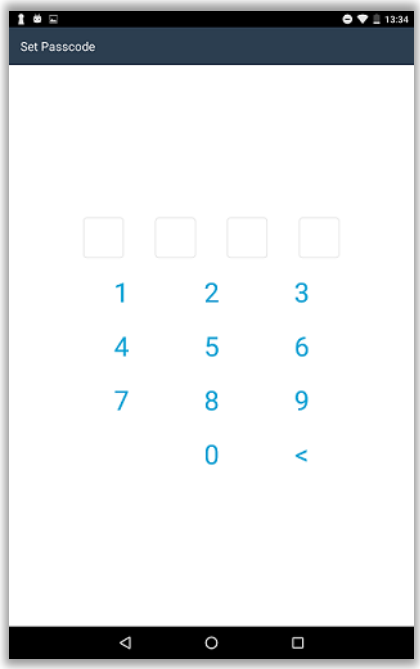
Foldr v4 provides built-in two factor authentication for web, desktop and mobile devices running the Foldr apps. Mobile devices (iOS & Android) running the native Foldr apps also have the ability to enforce passcodes, PIN or Touch ID (iOS only) to protect access to corporate resources.

The mobile apps can be run in Personal or Shared modes and for personal devices, Foldr also provides the ability to store credentials to allow convenient login from these devices (using best practices such as the *iOS Keychain* and *Android Private Shared Preferences*). Finally, the server-side Device Approval feature can be used to only allow pre-approved devices to be used against the Foldr server.



iOS – PIN / Passcode entry

iOS – Touch ID being used to unlock access to the app



Android – PIN / Passcode entry

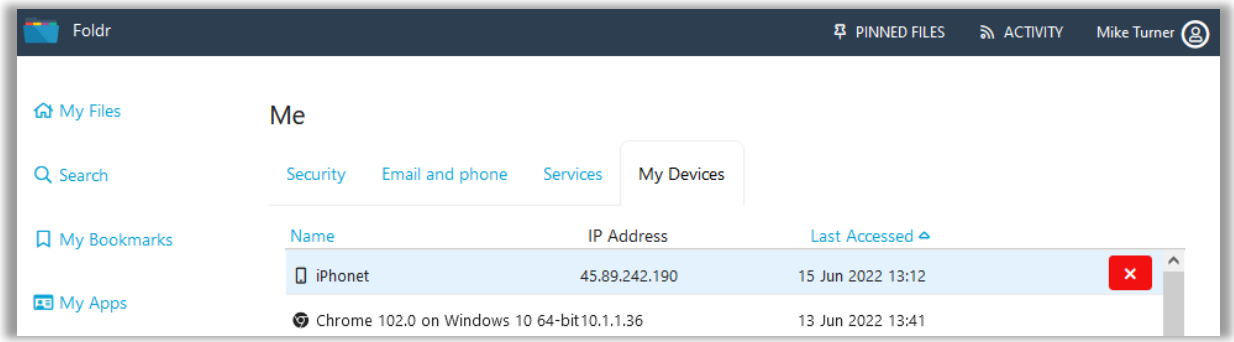
On both Android and iOS platforms, a complex passcode can be optionally used instead of a 4-character PIN and both can be configured to force PIN/Passcode or Touch ID entry to unlock the app each time it is backgrounded and reopened (**Lock on Wake**).

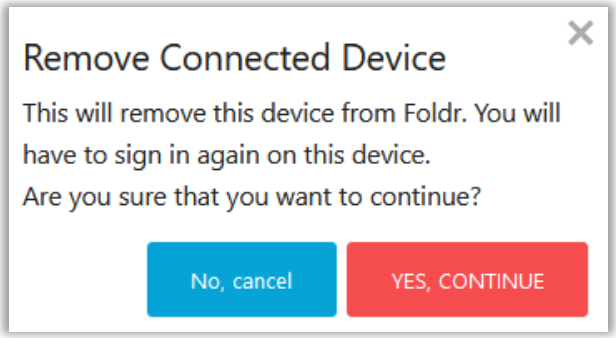
Lock on Wake can be configured within the app settings menu (cog icon) or enforced via MDM on iOS. See section 23 for more information of managing the app configuration via MDM.

iOS app – Security settings

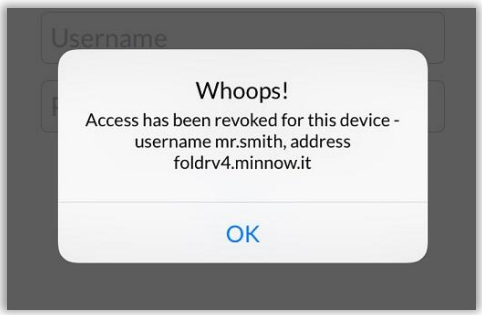
Revoking Mobile Device Access

In the event of a mobile device becoming lost or stolen it is best practice to remove the ability to sign in from the lost device, or continue a user session if the device is running a session of the Foldr app and it is already signed in. Using Foldr v4, a user can quickly revoke access to the device by logging into the Foldr (user) ***web app > ME > My Devices*** and clicking the red box next to the device.





After clicking *YES, CONTINUE* the device will be revoked and anyone using the device will be unable to log in, even if credentials are stored. Should a user attempt to use the app on a revoked device (and connect to the appliance or interact with it if already logged in) the users account profile in the app is also automatically removed.



iOS app – Device revoked message

Any existing session is automatically logged out if the user tries to interact and the local account profile is removed.

If the user has two factor authentication enabled on their account, they can remove trusted devices from the Web App menu > Me > Security The administrative *fadmin* user can also revoke user's devices from within ***Foldr Settings > Users & Groups***.

Find the user in question, double click the user to bring up a summary dialog and navigate to the Devices tab and remove the device in question to revoke access.

If the user has two factor authentication enabled, the administrator can reset their 2FA status within ***Foldr Settings > Security > Multi-Factor > Active Users***

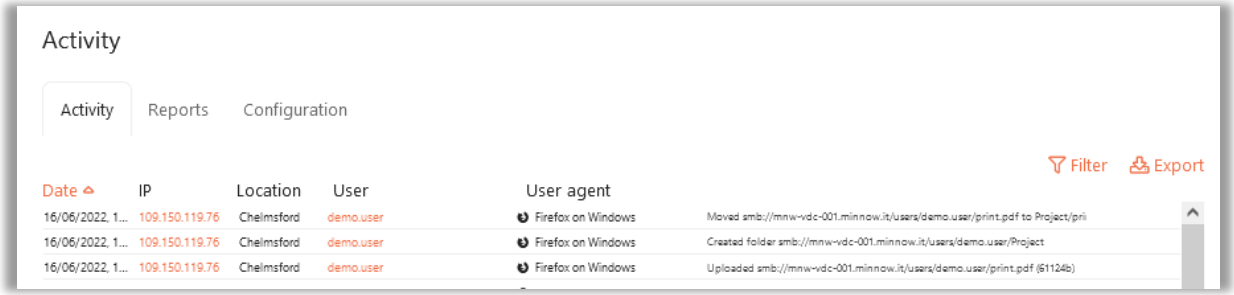
Logging User Activity

The Foldr appliance automatically records all user activity and retains the data for 3 calendar months. The logs are accessible from ***Foldr Settings > Activity***. The logs are stored within the configuration database (infrastructure appliances in a multi-appliance deployment) and are searchable by user and/or date.

The following entries are logged:

- Authentication success or failure, including MFA/two factor authentication
- Client IP address
- Username
- Date/time
- User agent string
- File action taken (list folder, move, edit, delete, upload, share etc.)

User activity logs can be downloaded to a local workstation in text format or exported directly into a web browser.



14. Appliance Modes (Infrastructure & Client Access)

Administrators have the option of deploying Foldr in a multi-appliance scenario where the central configuration database(s) can be held on a non-internet facing appliance(s) and one or more client access Foldr appliances can be deployed for handling user sessions.

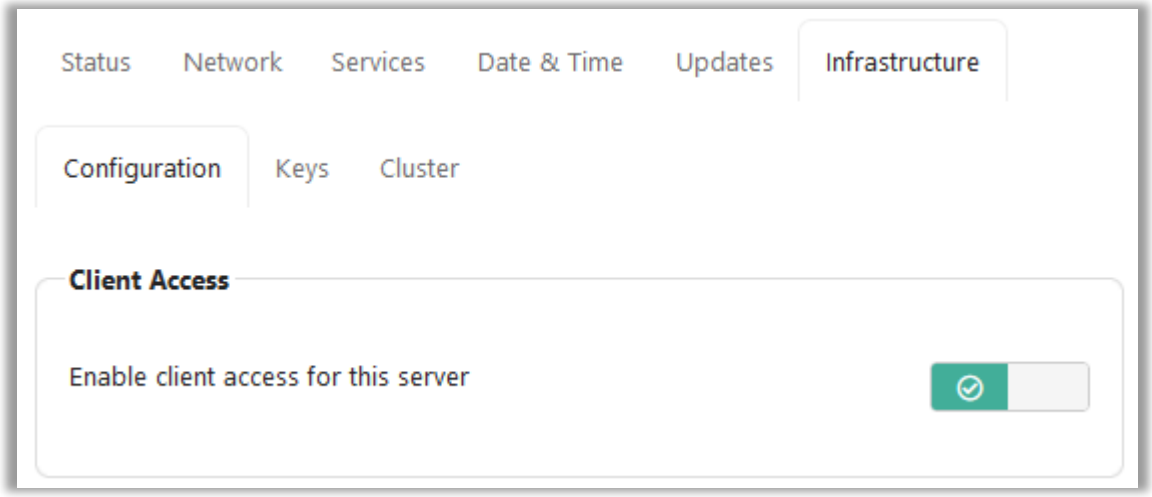
To configure the appliance mode, use the drop-down menu available within ***Appliance > Infrastructure > Configuration > Appliance Mode.***

Infrastructure (Database) Appliance

To designate an appliance in Infrastructure mode select '**Provide database services to other appliances**. All servers must be entered using the IP address rather than DNS hostnames. Based upon the values entered, the firewall on the appliance is automatically configured when the settings are applied.

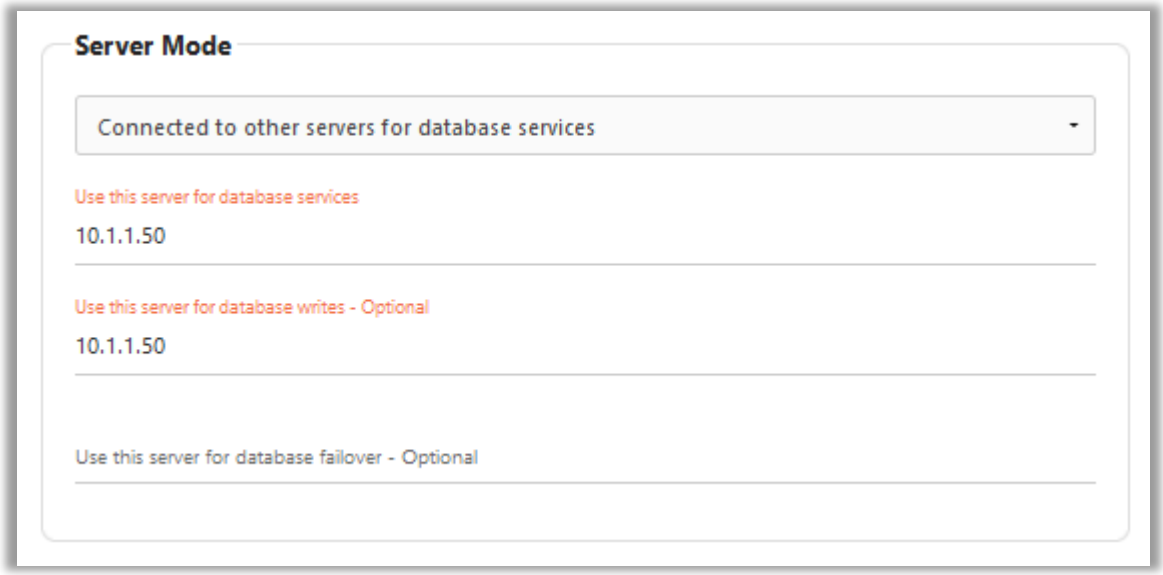
Disabling User Sessions (Client Access) on the Infrastructure / Database appliance

By default this setting is enabled, however it may be desirable for an administrator to disallow user access to an appliance in Infrastructure mode.



Client Access Appliance

To designate an appliance in Client Access mode, select **'Connect to another appliance for database services**. Enter the IP address of the infrastructure appliance(s) in the field provided. Again, based upon the values entered, the firewall on the appliance is automatically configured when the settings are applied.



Encryption Keys in an Infrastructure & Client Access deployment

IMPORTANT – When deploying Foldr v4 in multi-appliance design, the **encryption key and hashing salt must match across all appliances**.

You can reveal the encryption keys being used from ***Foldr Settings > Infrastructure > Keys*** and you will be prompted to supply the fadmin account password to unhide the encryption key itself. To replace the key & salt, highlight the existing value from another appliance and copy/paste in the new desired value, finally click Save. Once the encryption key has been changed your session will be logged out and you will need to log back into Foldr Settings.

Creating an Infrastructure Cluster

Foldr v4 supports clustering the infrastructure role across any number of appliances from 2-20 instances. This may be desirable for environments that have the server resources available to create a scalable and highly available Foldr deployment.

The clustering technology used in Foldr v4 provides synchronous multi-master replication and as such any database changes made on one cluster node are immediately replicated to others in the cluster with no risk of data loss, even in the event of a cluster node going offline.

It is recommended to use an odd number of appliances with a minimum of 3 nodes (infrastructure appliances) when creating a clustered environment to avoid a possible split-brain scenario. A 3-node cluster strikes a good balance between cluster size, performance and gives the ability to support a single appliance failure and will continue to run without disruption.

The steps to create a multi-node cluster are:

1. Configure each appliance with a static IP address (or use reservations in DHCP to avoid possible IP configuration changes)

2. Select 'Provide database services to other appliances' from ***Foldr Settings > Infrastructure***, entering the IP address of each cluster member in the Cluster tab. IMPORTANT – It is vital that you include the IP address of the appliance that you're currently configuring on each.

3. Once all cluster members have been configured and the changes saved. You should power down all potential cluster members, except one. Once all cluster members are offline, reboot the remaining cluster member and wait for the system to complete the boot sequence.

4. All other cluster members can now be powered on. It is recommended that you allow each system to complete the boot process (So the login screen is shown on the console) before powering on the next cluster member.

5. If using satellite client access appliances to work with the infrastructure cluster, enter the IP address of each under TRUSTED SERVERS within ***Foldr Settings > Infrastructure***.

Checking Cluster Status

When the database cluster is operational you should be able to make changes on any cluster member or client access appliance (Add service account, install licences add shares, service accounts and so on) and all changes should be quickly reflected across all other members of the cluster.

You can check the size and health and of your cluster using the verbose information displayed on the Cluster tab. You should pay attention to the following three options.

wsrep_cluster_size – This will display the number of nodes currently in the cluster (recommended minimum of 3) – Note that client access appliances do not count towards the total cluster size.

Checking Replication Health

wsrep_local_send_queue avg and **wsrep_local_recv_queue_avg** – In normal circumstances both values should remain at 0.0 (or very close to it). A higher value indicates replication throttling or network throughput/connectivity issues.

Configuring Client Access Appliances with a Cluster

For best performance and failover, it is recommended that you configure each client access appliance to use one cluster member for main database operations (read), another for database writes and select a third cluster member for failover.

15. Multi-Tenancy (sub-domains)

Multi-tenancy allows you to run multiple independent instances of Foldr, with each being accessible as a subdomain. Each subdomain / customer tenant instance is licenced and configured separately and provides the ability to support environments that run different Active Directory domains from a single virtual appliance or cluster of appliances.

Typical usage scenarios for multi-tenant mode would be a service provider providing hosted file access services to multiple customers. Each tenant organisation (customer) would access Foldr using their dedicated tenant subdomain. i.e.

https://apples.yourdomain.com
https://oranges.yourdomain.com

Multi-tenant mode can only be managed from the virtual appliance console using the following commands.

To enable multi-tenant mode:

tenant-enable

To create a tenant:

tenant-add "name-of-customer" s* *ubdomain*

For example, to create a tenant called Apples Corp that will use the subdomain apples. The use of quote marks as shown is important when creating a multi-worded tenant name:

```
tenant-add "Apples Corp" apples
```

The tenant and the default built-in security groups will be created automatically:

```
Creating group Foldr Users
Creating group Foldr Mandatory 2FA Users
Creating group Foldr Optional 2FA Users
Tenant Apples Corp added successfully.
```

To list all tenants and show the user count for each instance:

tenant-list

```
+--------------+-----------+------------+--------+
| Name         | Subdomain | User count | Status |
+--------------+-----------+------------+--------+
| Oranges Corp | oranges   | 0          | OK     |
| Apples Corp  | apples    | 0          | OK     |
+--------------+-----------+------------+--------+
```

To remove a tenant:

tenant-remove *subdomain*

Please note that this does not remove any user files. Just the tenant subdomain and its configuration are deleted.

Tenants in an Infrastructure and Client Access Deployment

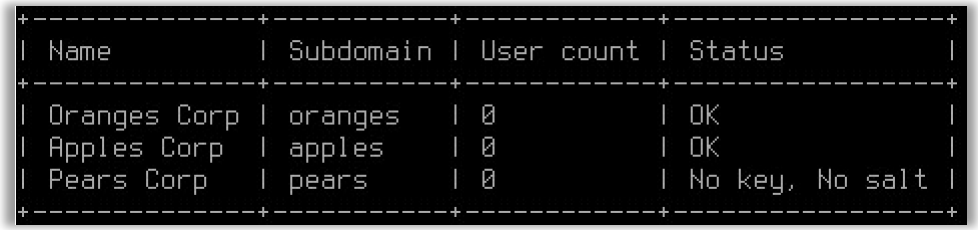
If you have deployed Foldr with infrastructure and client access appliances, each appliance in the deployment should firstly be placed into multi-tenancy mode by running **'tenant-enable'**. Once this has been done you can create your tenants as required on one of the appliances in the cluster.

Syncing Tenants

IMPORTANT – After creating your tenants you must synchronise the tenant's encryption keys across all *other* Foldr appliances before the tenant subdomains are usable. The following command should be run from the Foldr appliance upon which all the tenants were created on.

The STATUS column when running **`tenant-list`** should state 'OK', if the appliance is missing the keys you must run tenant-sync from another appliance that can provide them. If you attempt to run tenant-sync from an appliance with missing keys, an error will be displayed, and the sync operation will be aborted.

In the example below, Pears Corp (https://pears.yourdomain.internal) is currently unusable on this system due to missing encryption keys:



```
+--------------+-----------+------------+------------------+
| Name         | Subdomain | User count | Status           |
+--------------+-----------+------------+------------------+
| Oranges Corp | oranges   | 0          | OK               |
| Apples Corp  | apples    | 0          | OK               |
| Pears Corp   | pears     | 0          | No key, No salt  |
+--------------+-----------+------------+------------------+
```

Tenant-sync command example:

`tenant-sync appliance-ip-1 appliance-ip-2 appliance-ip-3 -p` ***`password`***

The -p argument used above is optional and will only work if all appliances are using the same fadmin password. Otherwise, you will be asked to provide a password for each appliance individually.

This command ensures that all appliances use the same encryption and hashing keys for individual tenants. For correct operation, these keys must be synced between all client access appliances. It is also recommended that you sync them with your infrastructure appliances as well.

To disable multi-tenant mode :

`tenant-disable`

DNS & Multi-Tenant Mode

IMPORTANT – DNS must be correctly configured, both internally and externally for multi-tenant mode to work correctly. If one does not already exist, a lookup zone should be created for the domain name and Host / A records created for each tenant. Each A record must be configured to resolve to the IP address of the Foldr appliance. If a load balancer is being used in front of multiple client access appliances, the host record should resolve to the IP address of the load balancer.

It is also important that the preferred and secondary DNS servers that are configured on the Foldr appliance can resolve all customer Active Directory domains that are used. Also, all paths (LDAP servers, shares, home folders and so on) must configured **fully qualified**.

Configuring & Licencing Tenants

The administrative *fadmin* account can configure each tenant by browsing to:

https://tenant-subdomain.yourdomain.com/settings

The tenant instance can then be configured as normal.

NOTE – The default /settings admin UI at https://IP-address-of-Foldr/settings serves no purpose in multi-tenant mode and should not be used.

Delegated Administration of the Tenant

When a new tenant is created, the Foldr administrator can sign into the tenant's settings admin UI (https://tenant-subdomain.yourdomain.com/settings) as fadmin and delegate administrative permissions to either local or Active Directory users.

Granular administrative access can be granted to local or Active Directory users or groups under ***Foldr Settings > Users & Groups > Administrators.***

16. Multi Factor Authentication (MFA/2FA)

What is 2FA?

Also commonly known as two-factor authentication (2FA), multi factor authentication in Foldr is an optional security feature and is a method of confirming users' claimed identity as they sign in. Essentially MFA provides additional assurance that user A logged into a system, such as Foldr is indeed user A, and not another person that may have simply obtained their network credentials. This assurance is provided as the user must provide 2 factors to complete the authentication process, namely something they ***have***, in conjunction with something they ***know***.

In the use case with Foldr, something the user *knows* is their username and password. Something they *have* is an ever-changing *time-based one-time password* (TOTP / OTP) delivered via a third-party application. The third party application in this case being an authenticator app installed on a smartphone or tablet.

The OTP based two factor authentication mechanism used in Foldr v4 has been adopted by many of the leading software vendors as a robust method of authenticating users; more information on the TOTP algorithm is available here.

This feature enables the administrator to require selected individuals or groups of users to comply with the 2FA requirement at login before they are granted access to resources via Foldr. 2FA can be optional or enforced upon users/groups depending on local security policy. If 2FA is optional a user can enable it within 'Security Settings' when logged into the Foldr apps. A user is always required to enter their username and password when enabling or disabling the 2FA feature.

To use the built-in 2FA feature with Foldr, the recommended method of generating the user's one-time passwords is by using an authenticator app on a smartphone. There are numerous free apps that provide this facility for all major mobile platforms, however two that work well are Authy and Google Authenticator:

Authy

Google Authenticator

If a user does not own a compatible device to run an authenticator app, OTP plugins are also available for desktop browsers (for example, Authy is available for Google Chrome)

IMPORTANT – It is vital that the Foldr appliance system clock is accurate to ensure MFA works correctly.

The system time can be confirmed by running the **date** command on the appliance console. The time is also shown in the Foldr Settings.

If you find that your system time in not correct, it is recommended that you firstly ensure your Time Zone is correct within ***Foldr Settings > Appliance > Time Settings***. If NTP is being used, the administrator can force the system clock to synchronise with a chosen time server (usually local domain controller) using the following console command:

```
time-sync x.x.x.x
```

Time settings are covered in a dedicated online KB article here.

Enabling Multi Factor Authentication for Users

The administrator can enable 2FA for specific users or groups within ***Foldr Settings > Security > Multi Factor > Users & Groups tab***. There are two deployment methods:

- **Required** (Enforced)

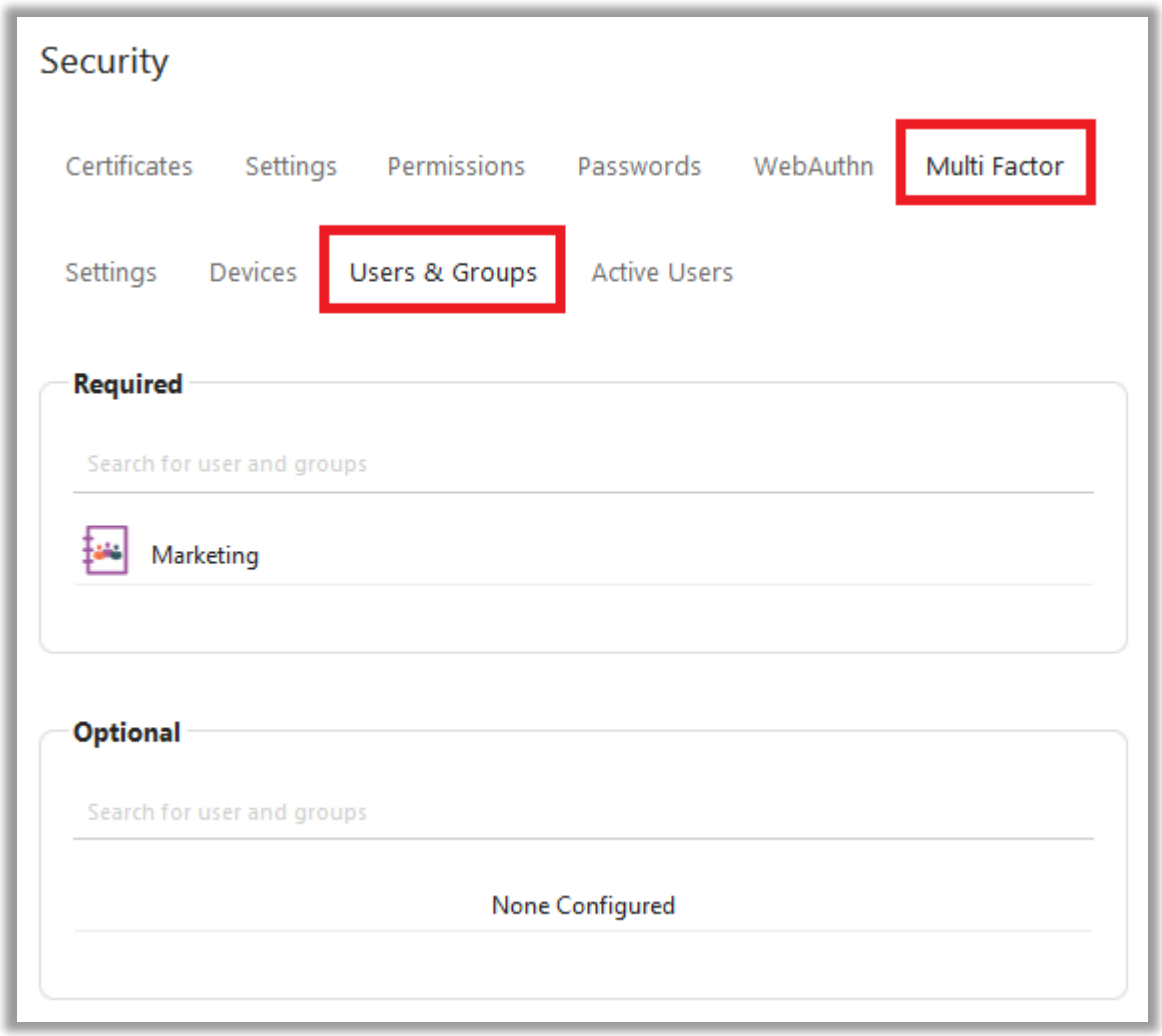
Users will be forced to enroll in 2FA immediately when they next access Foldr via the web, mobile or desktop apps.

- **Optional**

The user can enable 2FA through the web or mobile apps at a time of their choosing).

The example below shows enforcing 2FA for all members of the Active Directory security group 'Marketing'.

1. Browse to ***Foldr Settings > Security > Multi Factor > Users & Groups***:

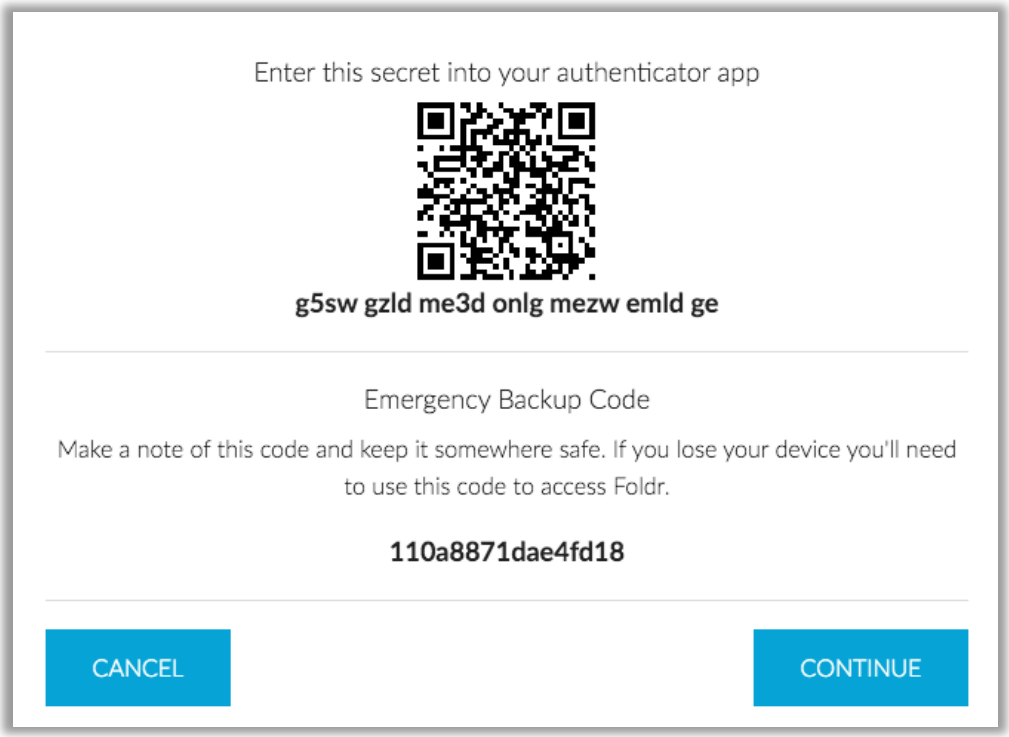


User Enrolment

The basic process of user enrolment is as follows:

- User installs their chosen authenticator app on smartphone or tablet
- User logs into Foldr using Active Directory credentials
- The user opens the authenticator app and scans the QR code of their shared secret and optionally notes emergency backup code
- User verifies enrolment by entering 6-digit OTP shown in the authenticator app to complete login
- User is now enrolled in 2FA

When a user logs into Foldr and 2FA is marked as required, they will be prompted with the enrolment screen the first time they log into Foldr.

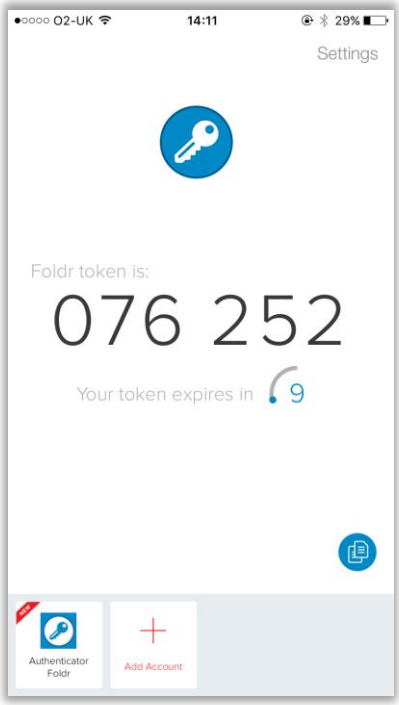


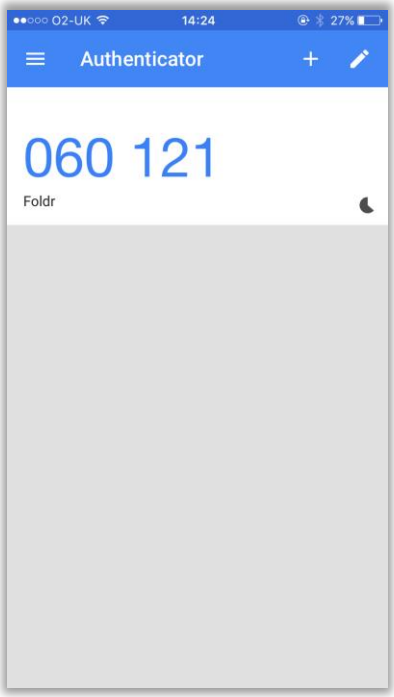
If a user has 2FA configured as optional then the backup code will simply allow the user to log in and 2FA will be disabled until manually re-enabled within Security Settings in the Foldr interface.

To enrol successfully, the user must create an account within their chosen authenticator app and select SCAN QR CODE.

If the scan QR Code option is not available, you can manually enter the 28-alphanumeric secret shown below the QR code image.

Authy and Google Authenticator screenshots shown below after completing the enrolment process, note the six-digit OTP code being shown in each app.





The user will now be prompted to enter their OTP each time they authenticate with Foldr.

NOTE – The one-time password changes every 60 seconds (30 second countdown per code within the authenticator app, plus a 30 second grace period). Since the OTP relies upon the current time and the shared secret associated with the user, it is **important that the system clock on the Foldr server is correct and remains in sync**.

It is recommended to use NTP as the Foldr server time source.

Trusted Devices

By default, this option is enabled. Once a user has successfully passed 2FA they can mark the device as a 'trusted' by using the checkbox provided. From this point on they will not be required to enter the OTP code using that device or browser, however, trust status is not linked between web browsers on the same computer. i.e. If a user marks trust this device in Google Chrome, they will still be forced to enter the OTP in Internet Explorer or Mozilla Firefox.

The admin can disable the ability for users to trust devices globally using the toggle 'Allow users to trust devices' off, or the option to trust may be set on a per-app/client basis.

A users trusted devices can be viewed within Security Settings, when logged into the web app. Trusted devices may be deleted if required.

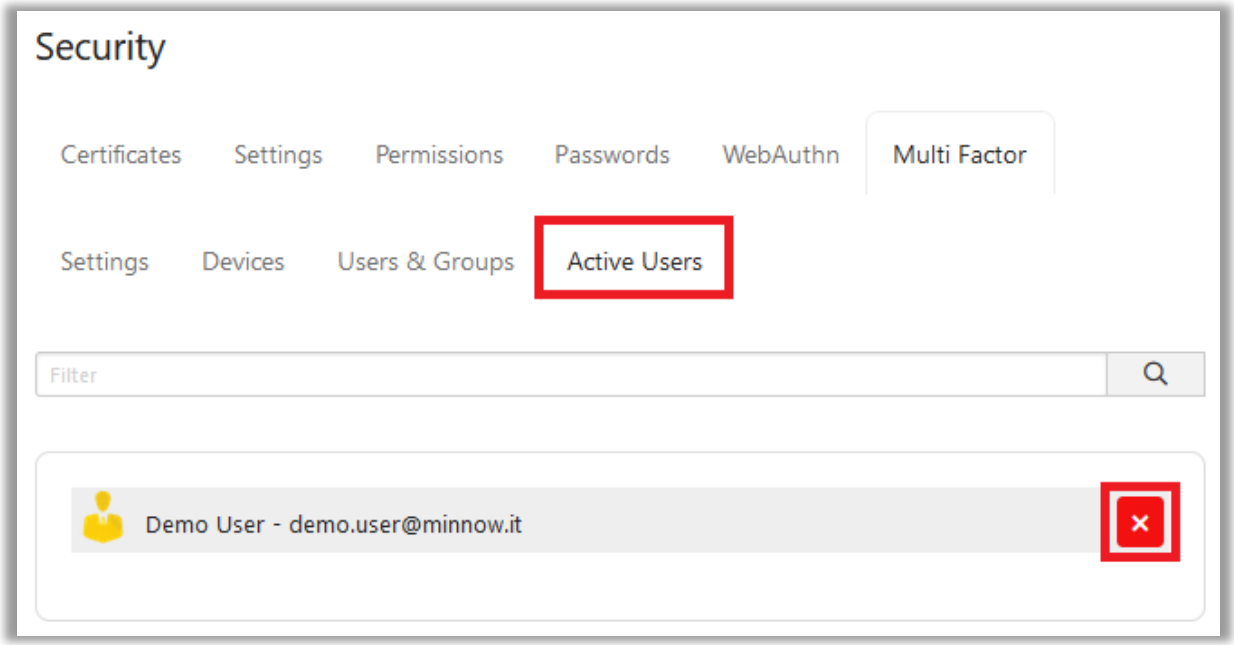
Allow Backup Codes

Emergency backup codes are enabled by default. The user will be presented with an emergency backup code that can be used to reset the 2FA status of their account, without the administrators assistance.

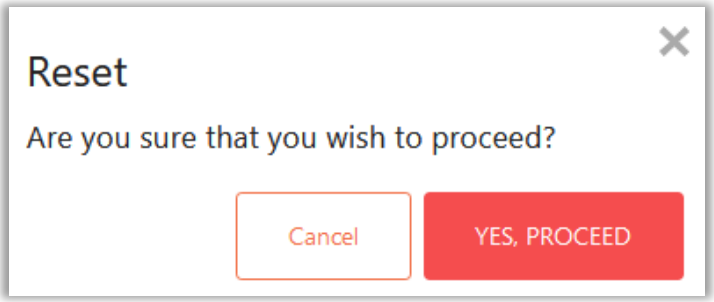
The user will then be prompted to re-enrol upon next login. This feature may be useful if the user loses access to their authenticator app (mobile phone is lost/ stolen).

Resetting 2FA Enrolment Status

Within ***Foldr Settings > Security > Multi Factor > Active Users***, the administrator can reset a user's existing 2FA status by clicking the in-line reset button next to their username.



The following prompt will be displayed, and when Yes, Proceed is clicked the user is removed from the list, and they will be forced to re-enrol at next login if they fall under the mandatory 2FA policy.



Security Considerations – 2FA & Foldr Drive (WebDAV)

Foldr allows users to connect and access their storage areas using a third-party WebDAV client, this includes the ability to map a drive in Windows or Mac OS X using Explorer / Finder. Foldr Drive acts as a WebDAV endpoint to provide this functionality and because of this, it is not possible to provide

support for two factor authentication.

If you have a mandatory requirement for users to log in using 2FA then *Connect with WebDAV* should be disabled for users. This can be achieved by configuring an appropriate DENY rule under ***Foldr Settings > Security > Permissions > Connect with WebDAV***.

If mapping a drive is desirable for users that must comply with a 2FA policy, the Foldr Windows and macOS apps both provide full support for the built-in 2FA feature or Duo 2FA. Mobile apps mobile apps only support Foldr 2FA at the time of writing (March 2019).

Support for third-party 2FA (Duo)

If the organisation has already invested in the popular 2FA solution from Duo, this can be used instead of the built-in 2FA feature in the appliance. Full integration steps are available on the online KB here.

WebAuthn

As well as traditional MFA/2FA with one-time passcodes, Foldr is also supports secure user sign in using Web Authentication API protocol (WebAuthn). Webauthn was developed by Yubico, Microsoft, Google and others to create a standardised phishing-resistant authentication mechanism.

WebAuthn allows users to register one or more authenticators in Foldr and they can then sign in to the web and desktop apps using a hardware device (physical security keys, such as the YubiKey) or biometrics by leveraging technologies such as Windows Hello (facial recognition or PIN entry) or macOS FaceID/TouchID.

More information about WebAuthn can be found here:

https://webauthn.guide/

https://developers.google.com/codelabs/webauthn-2fa-key#1

The Foldr administrator can enable WebAuthn for users/groups as required by the organisation and can even remove a user's ability to sign in using a standard password, enforcing the use of a registered WebAuth compatible authenticator. Alternatively, the admin can offer both traditional user sign-in using passwords (with 2FA) if required or the option of using a WebAuthn compatible device using a dedicated button on the web sign-in screen.

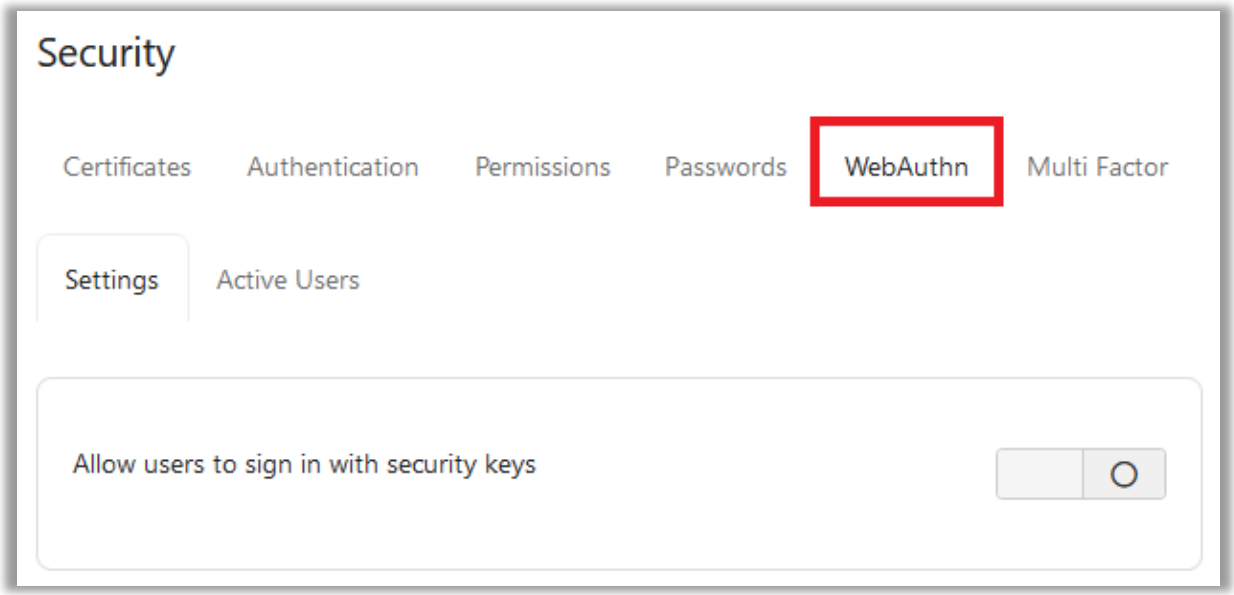
App Compatibility

Signing in with a security key is supported in the Foldr web, Windows and macOS desktop apps.

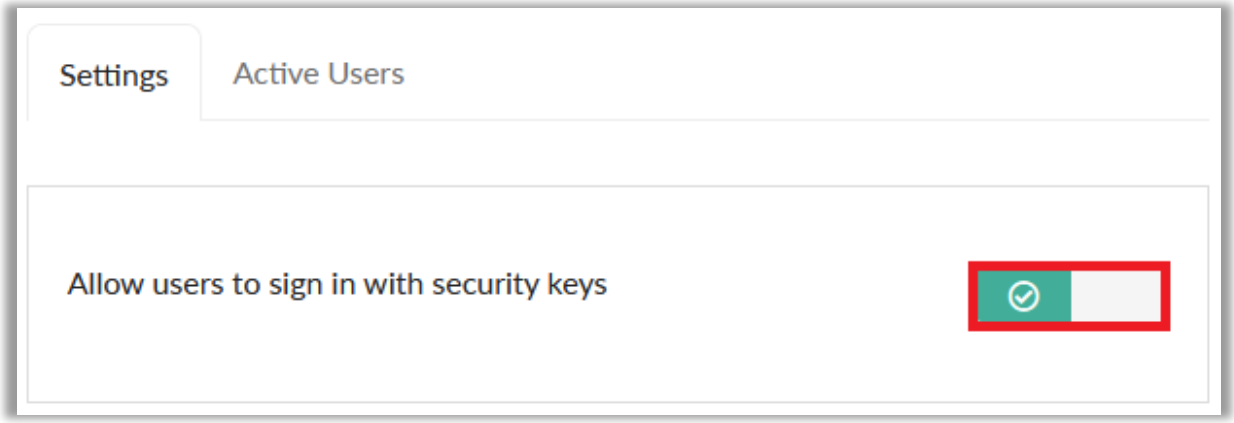
Enabling Security Key Sign-In for Users

WebAuthn is disabled by default and can be enabled for users/groups as required. In the example below, WebAuthn will be enabled for members of the Marketing department in Active Directory:

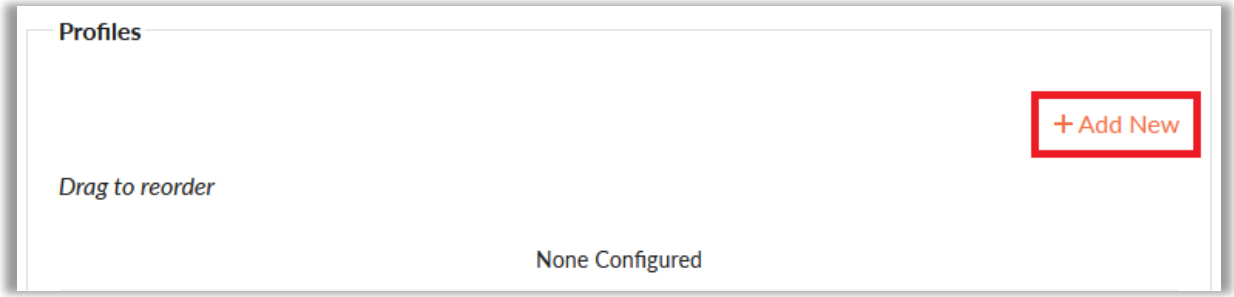
1. Sign into Foldr Settings and browse to the ***Security > WebAuthn*** tab.



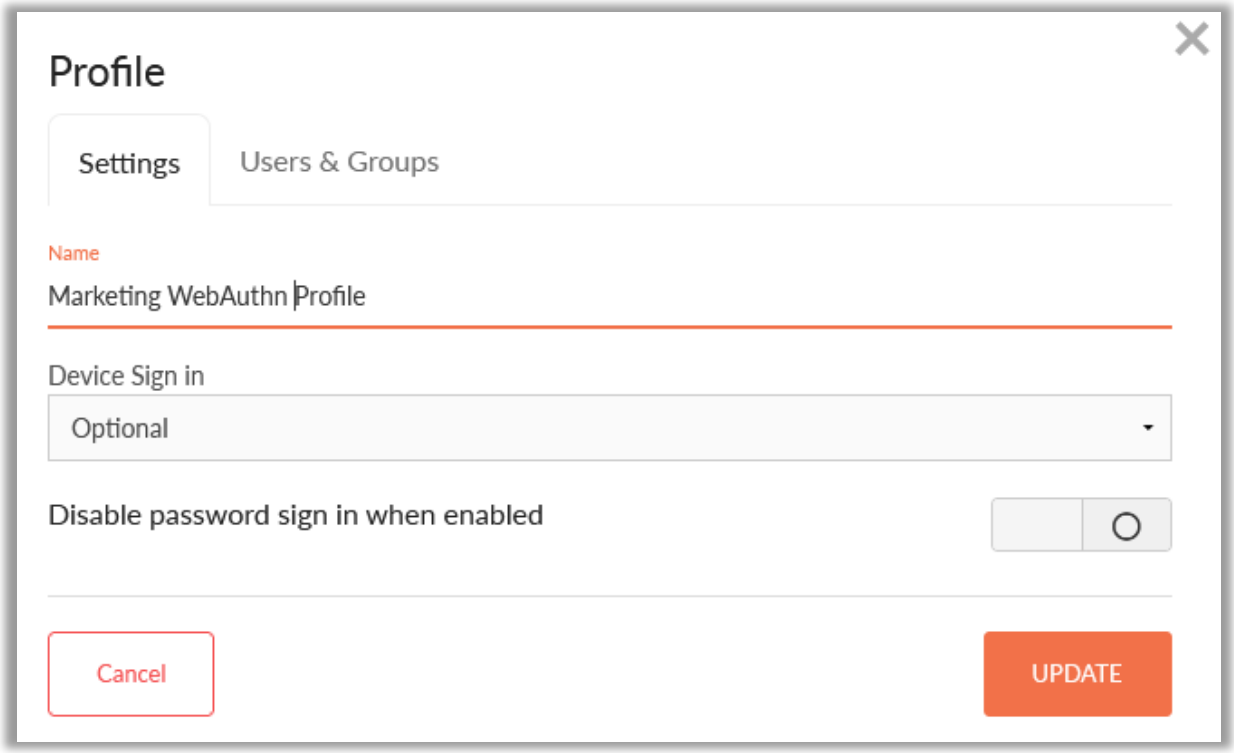
2. Enable WebAuthn by toggling on '**Allow users to sign in with security keys**'



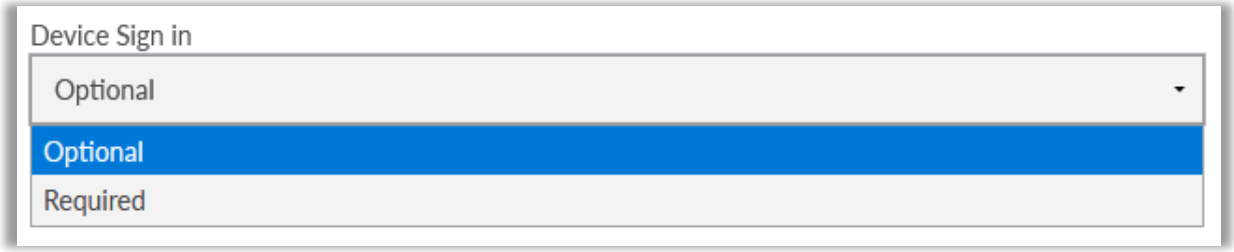
3. Create a WebAuthn profile and assign it to users/groups. Click **+ Add New**



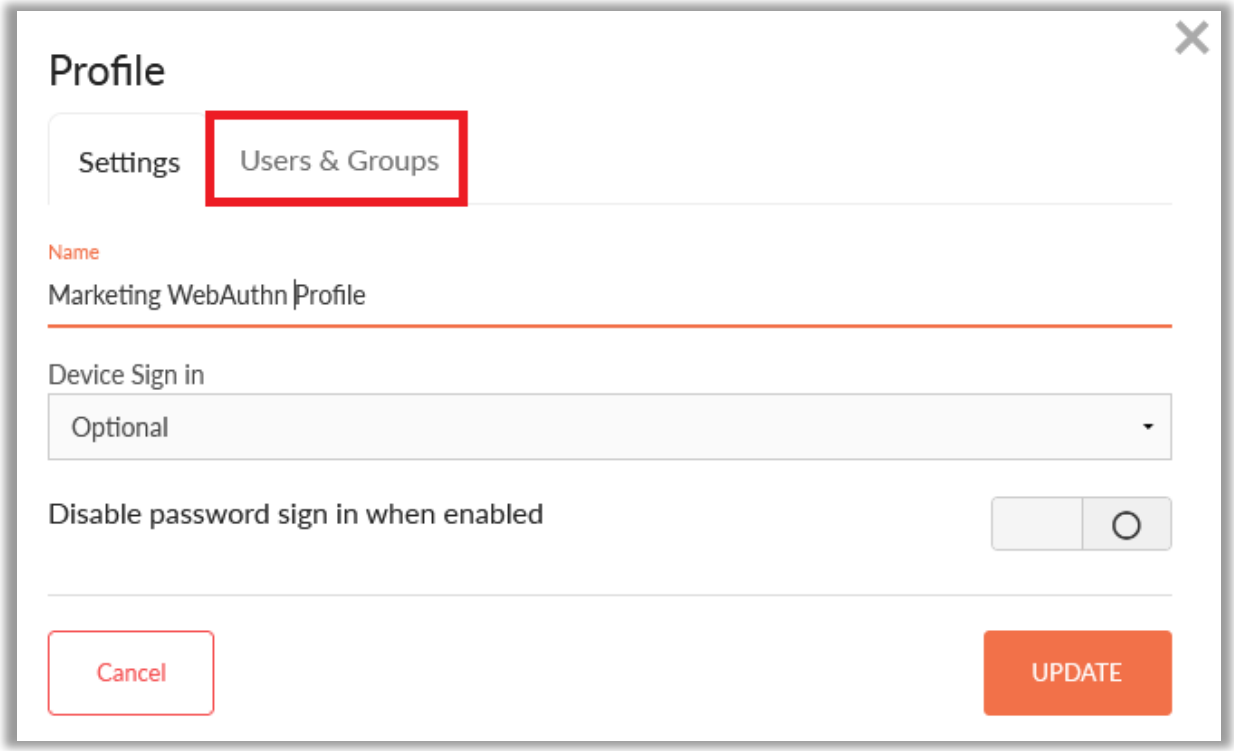
4. Give the Profile a suitable name



5. Decide if users should be forced (Required) to register a security device when they next sign into Foldr, or if they can add a device later at a time of their choosing (Optional).

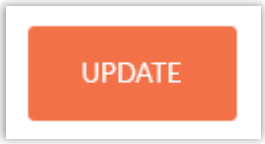


6. Click the Users & Groups tab

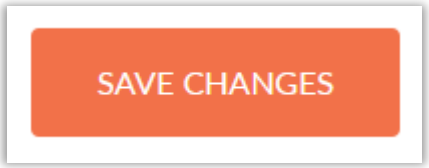


7. Search for the User or Group that you wish to assign the profile. In the example below an Active Directory group 'Marketing' is being used.

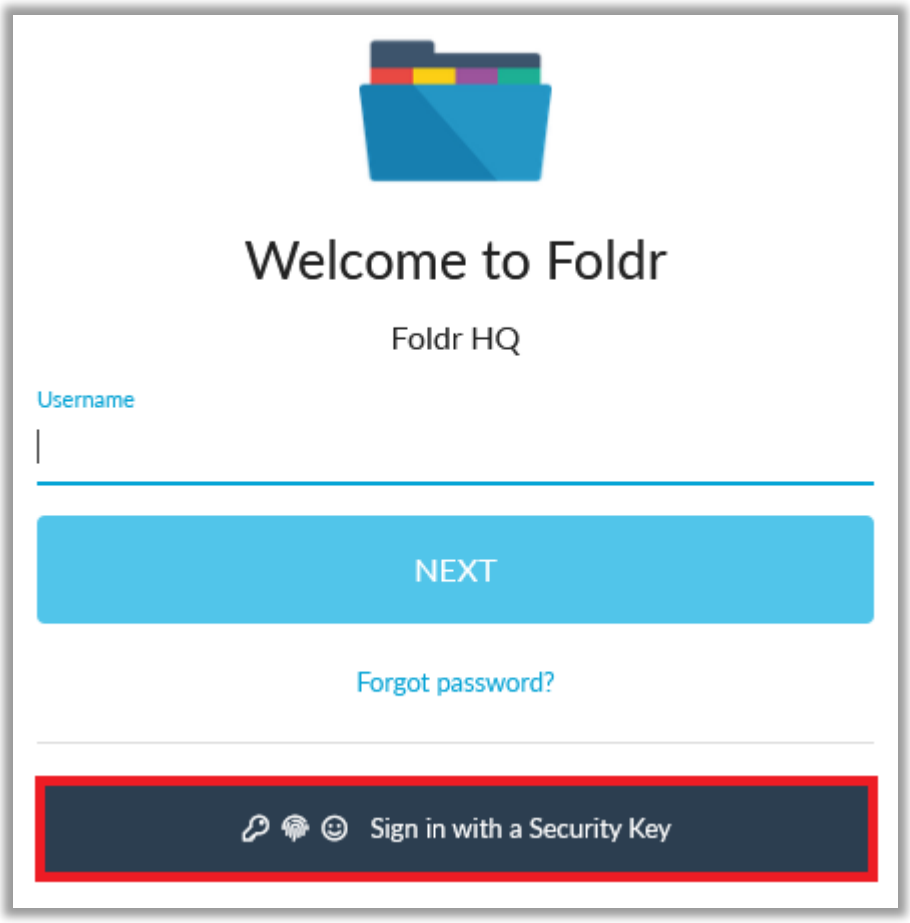
8. Click the Update button



9. This will return you to the main WebAuthn screen. Click Save Changes to commit changes or add another profile if required.

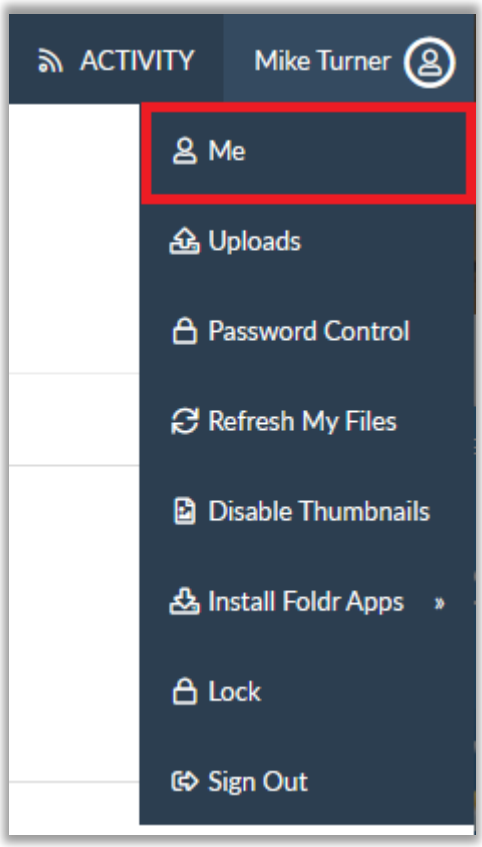


The setup process is complete. Users will now see a 'sign in with a security key' button at the bottom of the web sign-in dialog:

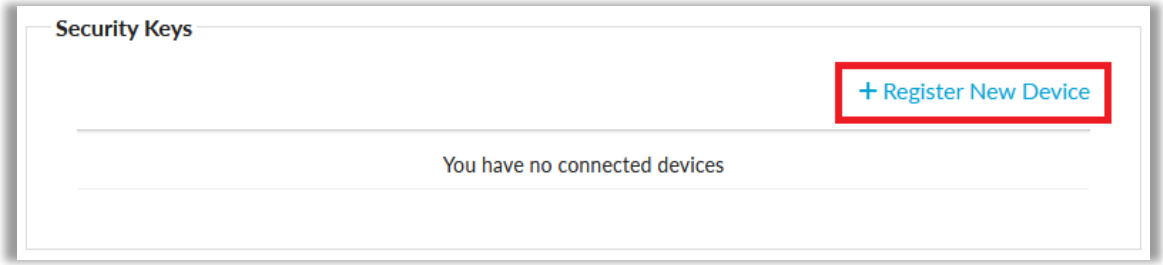


User Experience – Registering a WebAuthn Device

If a user signs in and their WebAuthn profile is set as **optional**, they can enable/register their security key or Windows Hello/macOS TouchID within the Me menu in the Foldr web app.



Within the ME screen, click **+ Register New Device.**



If Windows Hello (Pin, Face or Fingerprint) is enabled in Windows or TouchID is enabled in macOS you will be prompted to register at this point.

Otherwise, the user is prompted to enter a compatible WebAuthn/FIDO2 physical security key (typically USB Type-A or Type-C) and the PIN for the device will be requested.

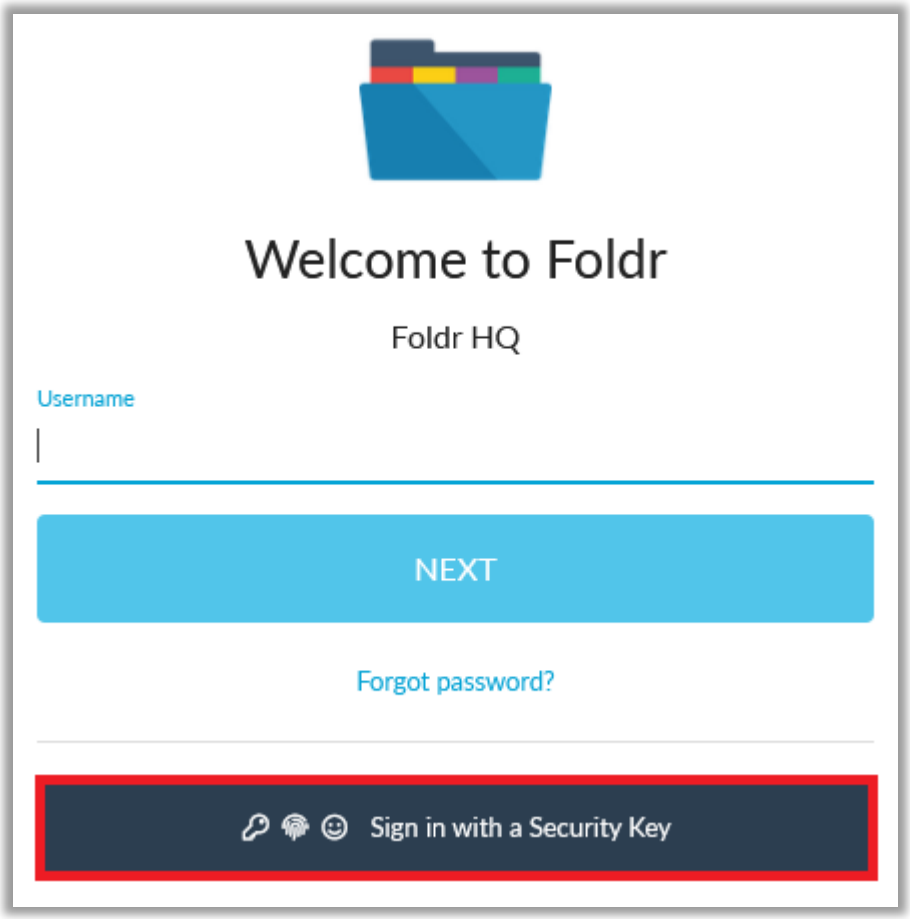
Once the PIN has been entered, the user will be prompted to touch the security key to complete the registration.

The device will now show within the user's Me tab > WebAuthn section with the date/time also shown when registered.

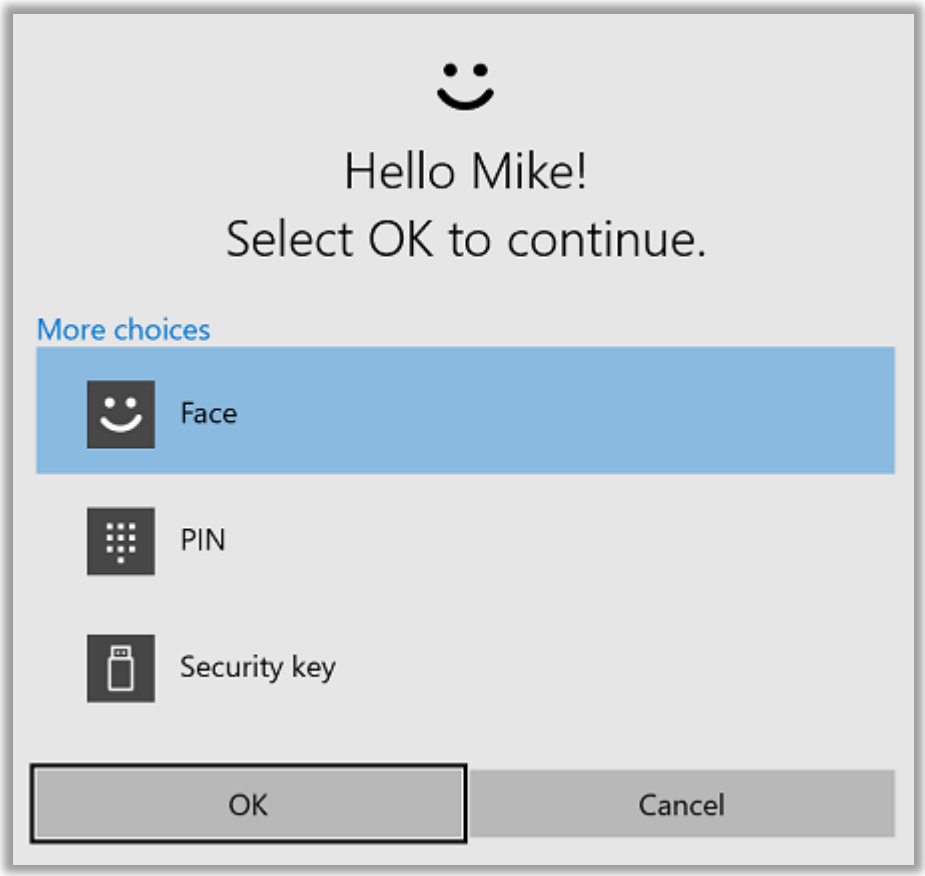
Multiple devices may be registered as required (Windows Hello may be registered, along with physical USB keys)

User Experience – Signing in with a Security Key

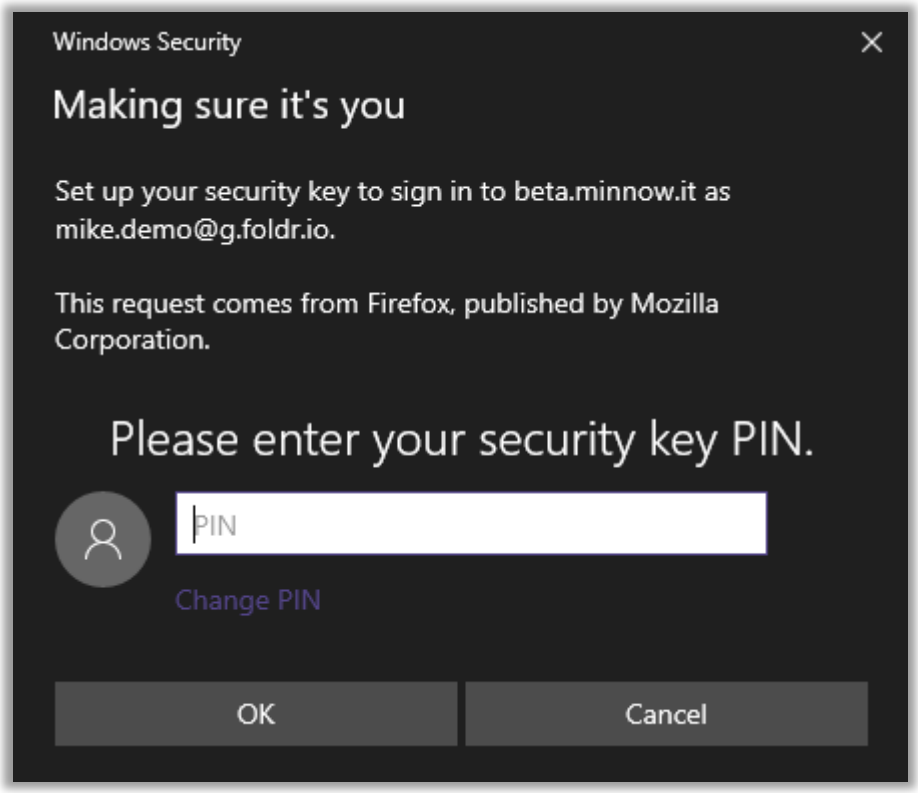
On the web app sign-in screen, click the Sign-In with a security key button



The standard Windows/macOS dialog will be shown to provide the security key/provide PIN or biometric input. In the example below the Windows Hello Face prompt appears and the web app will sign in etc.



If a physical USB device is being used, you are prompted to provide the PIN



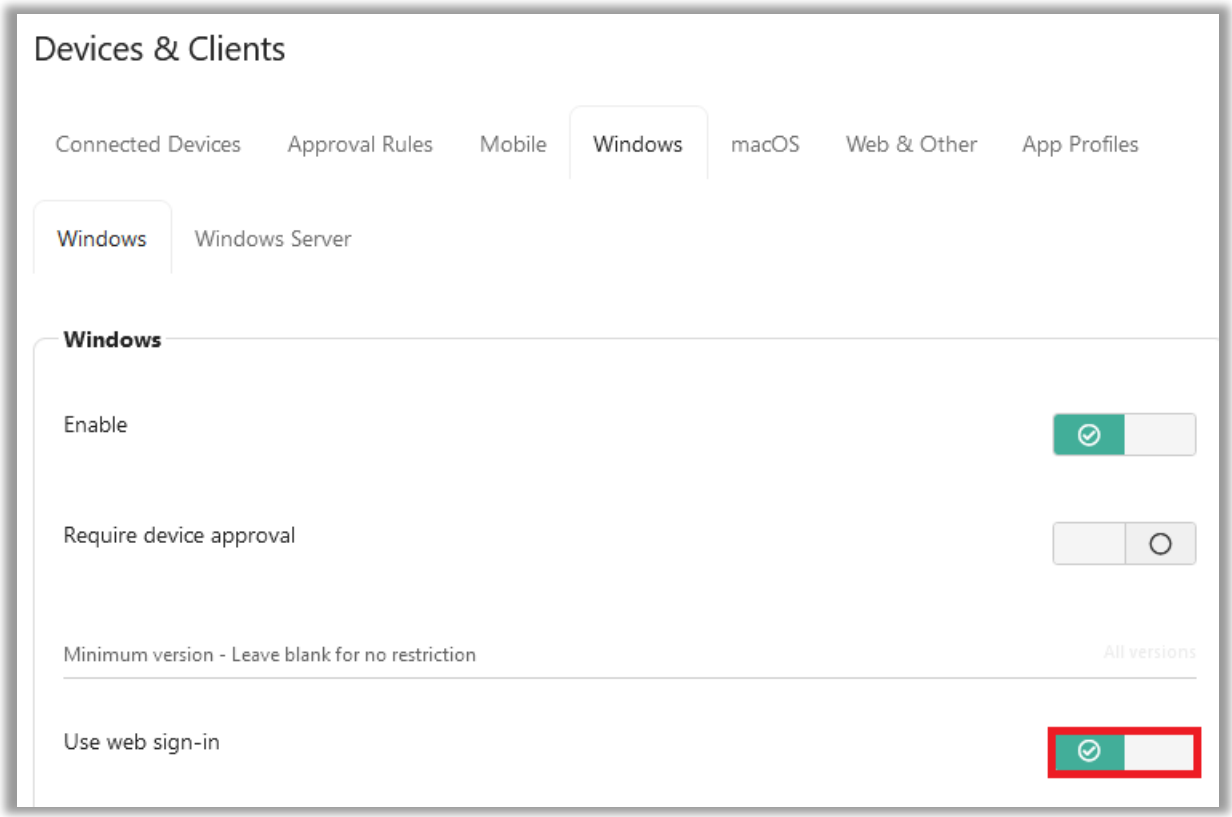
The user is then prompted to touch the device.

The app will then sign in.

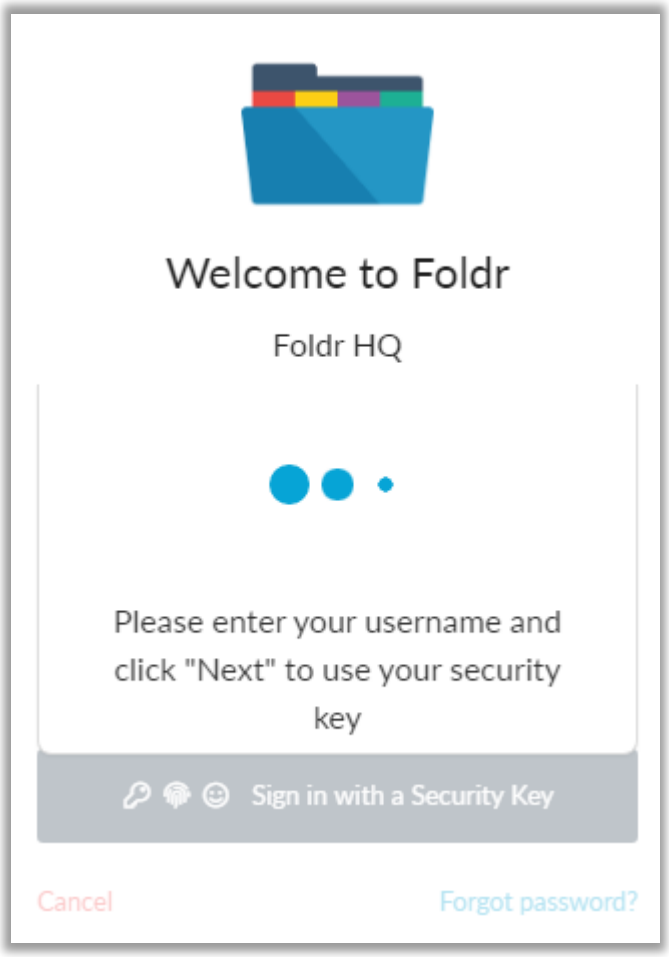
Windows/macOS App Sign-In Process

Requirements:

Web sign-in must be enabled for the desktop apps to support WebAuthn Security Key sign-in. This is configured on the server under ***Foldr Settings > Devices & Clients > Windows/macOS***. Note – Web sign-in is enabled by default.



The process to sign in to the desktop apps is very similar to the web app (above), however, the user must provide their username first. If the user doesn't provide their username, they will see the following prompt.



Managing Security Keys

A user can manage their registered security keys in the web app's ***Me*** menu screen.

Foldr administrators can search for and view/remove user's registered security keys in ***Foldr Settings > Security > WebAuthn > Active Users***.

17. SSL Certificates

All user activity, regardless of the method of connection (web app, iOS app, Android app or WebDAV) takes place over HTTPS. As such Foldr is supplied with a self-signed certificate to encrypt user and administrative sessions. A self-signed certificate will, by default, always 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 certificate provider such as GoDaddy, Verisign, GlobalSign, Thawte etc. This will then enable your users to connect without certificate prompts and additional features are also available such as the ability to map a network drive from a Windows based client and use the media streaming features in iOS.

HSTS Considerations

The Foldr v4 appliance has a security feature enabled by default called HTTP Strict Transport Security (HSTS) – This means that once the appliance has been switched from using the built-in self-signed SSL certificate to a signed (trusted) certificate, all client browsers that have connected to the system will **expect a valid SSL connection from that point moving forwards**. You **CANNOT** revert to a self-signed certificate or temporarily run the system with an expired signed certificate. (All client browsers that have connected previously will reject the connection)

As such it is important that the administrator manages the SSL certificate correctly on the Foldr appliance (ensure the SSL certificate does not expire!) to ensure no disruption of service to end users.

In the event of the Foldr appliance moving from a valid signed certificate to either an expired or self-signed certificate, the appliance is accessible via **public or private IP address only until a valid SSL certificate installation is restored.**

Let's Encrypt SSL Certificates (at no charge)

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.

Let's Encrypt intermediate certificates are cross signed by IdentTrust Certificate Authority and as such are trusted by all major web browsers and mobile devices. The built-in integration within ***Foldr Settings Security > Certificates*** provides a quick, automated, and convenient mechanism of requesting and installing the signed certificate which are ready to use immediately.

To get started with Let's Encrypt, enable the 'Use Let's Encrypt' switch and enter the external URL of the Foldr appliance. Note – this service requires the appliance to be available externally (over both HTTP & HTTPS) due to automatic certificate request and domain validation process used by Let's Encrypt.

Once the certificate domain has been entered and you click Save there will be a short delay (5-10 seconds) while the certificate request is sent to Let's Encrypt, and the signed certificate installed.

Troubleshooting Let's Encrypt SSL Installation

Due to the nature of the validation process, **Let's Encrypt will not successfully issue the SSL certificates where any form of HTTPS inspection / MITM web filtering or firewall product intercepts and re-signs the network traffic between Foldr and the Certificate Authority.** If a product of this type is deployed at the site, then the Foldr appliance IP address should be whitelisted. The external domain of '*letsencrypt.org*' should also be marked for exclusion from the HTTPS web filtering policy.

The Foldr appliance must be accessible externally over both **TCP port 80 (HTTP) and TCP port 443 (HTTPS)** for Let's Encrypt to successfully complete the certificate request, challenge handshake and installation.

More information on the Let's Encrypt project is available here and on their official website

Requesting and Installing a purchased signed SSL certificate

If instead of using Let's Encrypt, you wish to purchase an SSL certificate from a traditional Certificate Authority such as GoDaddy or Verisign you must firstly generate a Certificate Signing Request (CSR) and private key pair.

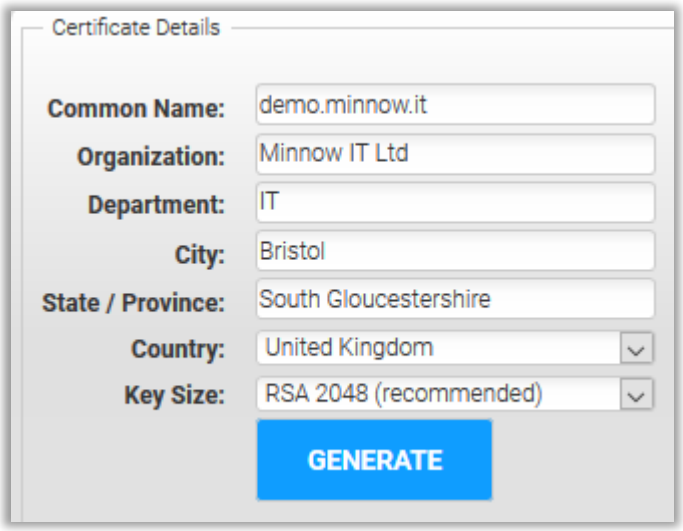
Steps required:

1. Generate your Certificate Signing Request (CSR) and Private Key pair:

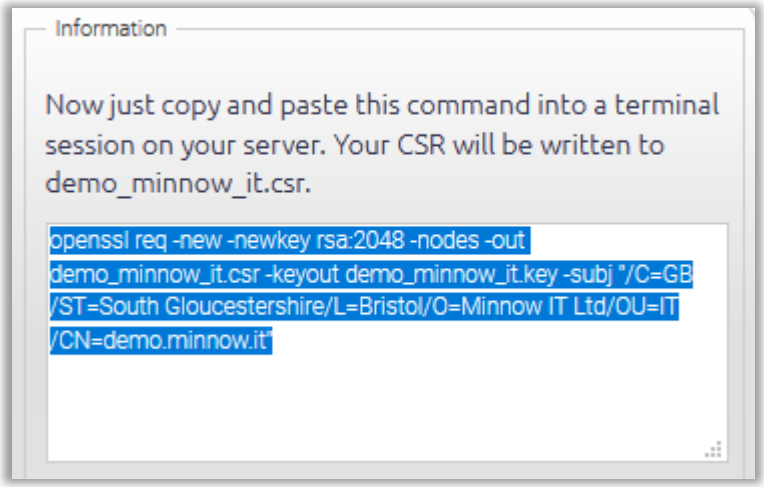
This can be done several ways, but a quick/easy route is to use the Easy CSR tool on the DigiCert website which will produce a single command to run which will use a locally installed version of OpenSSL to generate your CSR and private key.

[DigiCert Easy CSR]

2. Complete the required fields and click Generate.



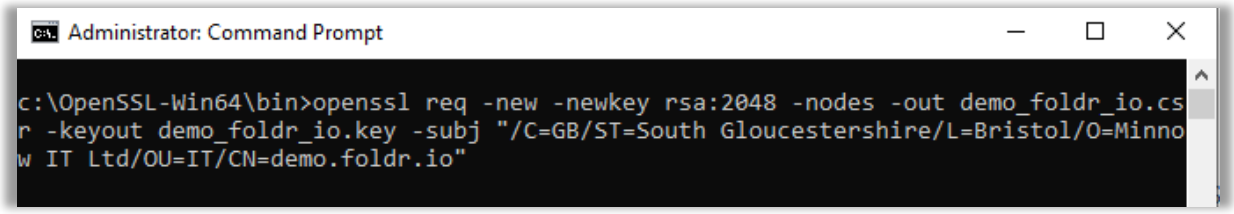
3. This will output the required OpenSSL command to generate a CSR and Private Key pair. Copy the command to the clipboard.



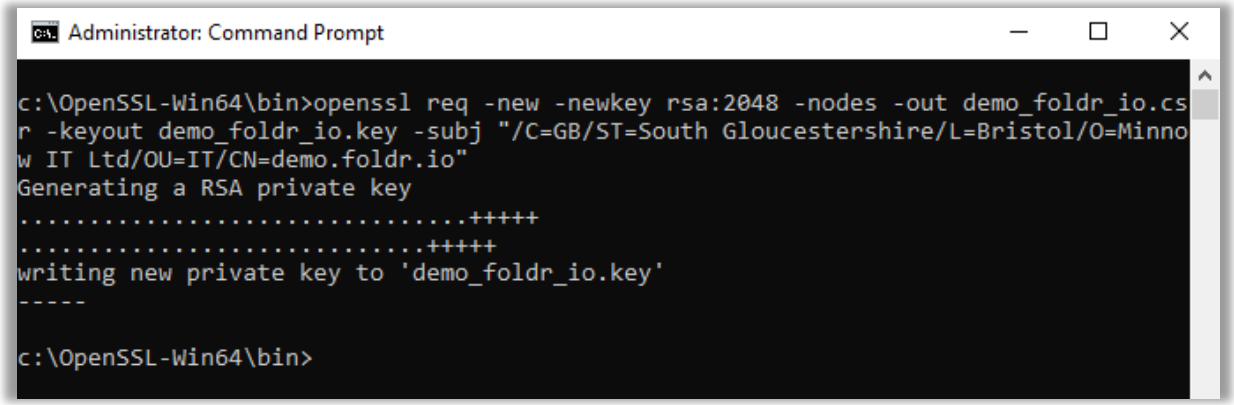
OpenSSL is available by default on macOS and most Linux installations. If using a Windows workstation, OpenSSL must be installed separately and can be obtained here – the smaller 'Light' version is fine for this purpose, selecting Win32 or Win64 as appropriate.

Run the OpenSSL command in Linux/macOS Terminal as given. For Windows systems, open an elevated command prompt (run as Administrator) and cd to \bin inside the OpenSSL directory (C:\OpenSSL-Win64\bin for x64)

OpenSSL may also be installed (depending on version) in C:\Program Files\OpenSSL-Win64, adjust the command as required.



The CSR and Private Key will be created in the working directory.



5. Save both the entire private key and CSR as separate text files to your computer. You will need to send the CSR to your chosen certificate provider as part of the process of requesting your certificate.

6. You will be required to confirm your ownership of the domain, usually by way of an email to the registered contact of the domain held by the registrar.

Once you have validated your certificate request / domain ownership, you will receive a second email to tell you that the signed certificate is ready for download. There can be a slight delay between confirming your domain ownership and your signed certificate being created by your provider.

When ready and downloaded, open the signed certificate and Private Key into a text editor and paste into the relevant boxes on the ***Foldr Settings > Security > Certificates*** screen.

You should also obtain your Certificate Provider's Root and Intermediate Chain certificates from their support portal and paste these in at the same time. Some certificate authorities issue a bundle certificate (which is the CA Root and Intermediate Chain combined into a single file) you need to install this into the Certificate chain box and leave the CA Root box blank.

8. Click SAVE and your certificate will be installed after a few seconds.

Your SSL certificate installation should now be complete, and you will no longer receive warnings in the browser or apps when accessing Foldr through the URL (Common Name) protected in the certificate.

The SSL installation can be verified by using an online validation tool such as https://www.sslshopper.com/ssl-checker.html

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

A certificate in PFX format contains both the signed certificate and private key, as such you must extract each as an individual file, so they are available to install into the Foldr appliance.

If using a Windows workstation install OpenSSL complete package from (Mac OS X has OpenSSL built in):

http://gnuwin32.sourceforge.net/packages/openssl.htm
Open an elevated command prompt and change directory to:
C:\Program Files\GnuWin32\bin (copy your PFX here also) and issue the following commands:

1. Extract the private key from the PFX file (assuming your PFX is called certificate.pfx) and write it to a PEM file called (privateKey.pem)

```
openssl.exe pkcs12 -in certificate.pfx -nocerts -out privateKey.pem
```

2. Extract the certificate from the PFX file (called publicCert.pem):

```
openssl.exe pkcs12 -in certificate.pfx -clcerts -nokeys -out publicCert.pem
```

3. Remove the password from the private key file (writes a new file called private.pem):

```
openssl.exe rsa -in privateKey.pem -out private.pem
```

Both files that you create at steps 1 & 2 will be written to the bin directory. Please note, it is **vital** that you remove the password from the private key otherwise the certificate installation will fail.

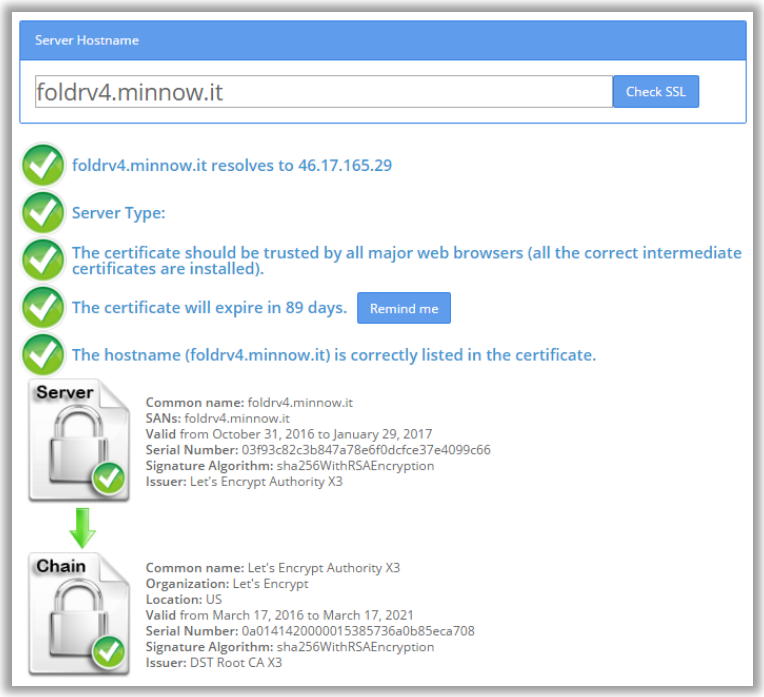
Now browse to https://IP_of_Foldr:30537/settings and log in as fadmin. Browse to ***Foldr Settings > Security > Certificates*** and open your certificate (publicCert.pem), decrypted /password removed private key (private.pem), root and intermediate certificates for your CA in a text editor and paste into the relevant boxes. The latter can be obtained from your certificate authorities support portal on their website.

Finally, click SAVE and your certificate will be installed after several seconds.

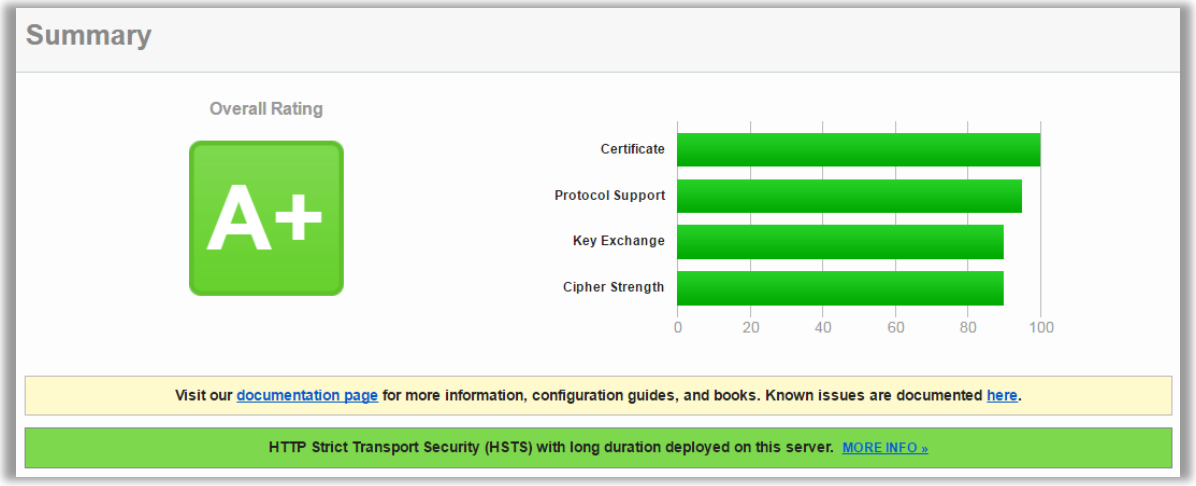
Verifying the SSL certificate installation

If the appliance is accessible externally, it is recommended to use an online SSL certificate validation service to check the installation. This can highlight issues such as a missing root / intermediate certificates (broken chain) which may cause issues for users connecting from certain device types.

Basic SSL Installation Test – https://www.sslshopper.com/ssl-checker.html



Qualys SSL Server Test (Deep analysis) – https://www.ssllabs.com/ssltest/



SSL/TLS Ciphers

In its default mode, Foldr uses a 'modern' SSL cipher configuration. This disables weaker SSL protocols such as TLS 1.0/1.1 and ciphers such as RC4/3DES and only permits clients to connect using TLS 1.2 and TLS 1.3.

The SSL configuration can be modified to re-enable older protocols / ciphers. This may be necessary due for compatibility reasons with legacy firewalls in use in the network environment. To downgrade the SSL configuration and re-enable TLS 1.0 and 1.1 use the following console command:

```
set-ciphers legacy
```

To set the SSL configuration back to default:

```
set-ciphers modern
```

With a signed SSL certificate installed and using the modern configuration the Foldr server will pass HIPAA, NIST and PCI DSS compliance testing.

18. Integrating Cloud Services

Google G Suite (WorkSpace) Integration

Google integration allows users Google Drive and shared Google drives to be presented through Foldr. The system can be configured to either **automatically** link an on-premise Active Directory user's Google account and present the corresponding Google Drive, or a user can link their Google account **manually** at a time of their choosing. For organisations with corporate G Suite domains, automatic account linking is recommended (integration 1 below)

Google Integration 1 – Automated Google Account Linking

Foldr can automatically link an on-premise Active Directory user account with the corresponding user in Google G Suite / Google Workspace. This is the recommended method of integrating Foldr with an organisations managed Google G-Suite/WorkSpace.

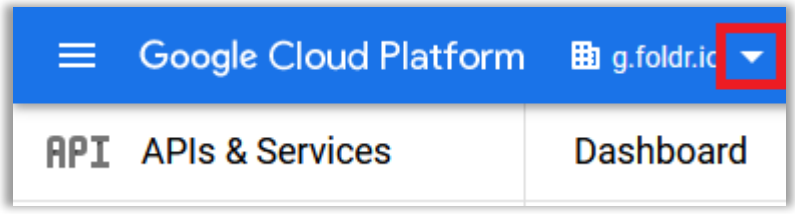
The G Suite/Workspace integration allows the administrator to present a user's personal Google Drive storage and Shared Google Drives to users as soon as they sign in (removing the need for the user to link accounts manually). The automatic linking option works by using a Google service account and mapping a predefined Active Directory attribute to provide access to the correct cloud storage account. i.e. the Foldr appliance will match the user's email address or UPN attribute to the user in the organisation's Google G Suite domain.

Configuring Automated Linking with Google G Suite/Workspace:

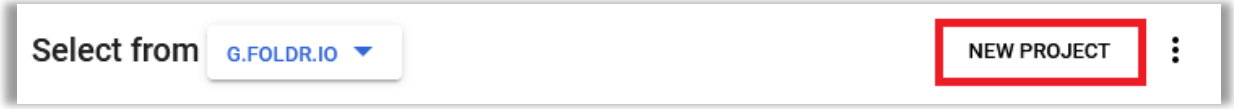
1. Browse to https://console.cloud.google.com/apis using your administrative account.

2. Create a new project

Create a new project - Click the chevron shown below. *Depending on the view, it may be at the organisation level or another existing project*

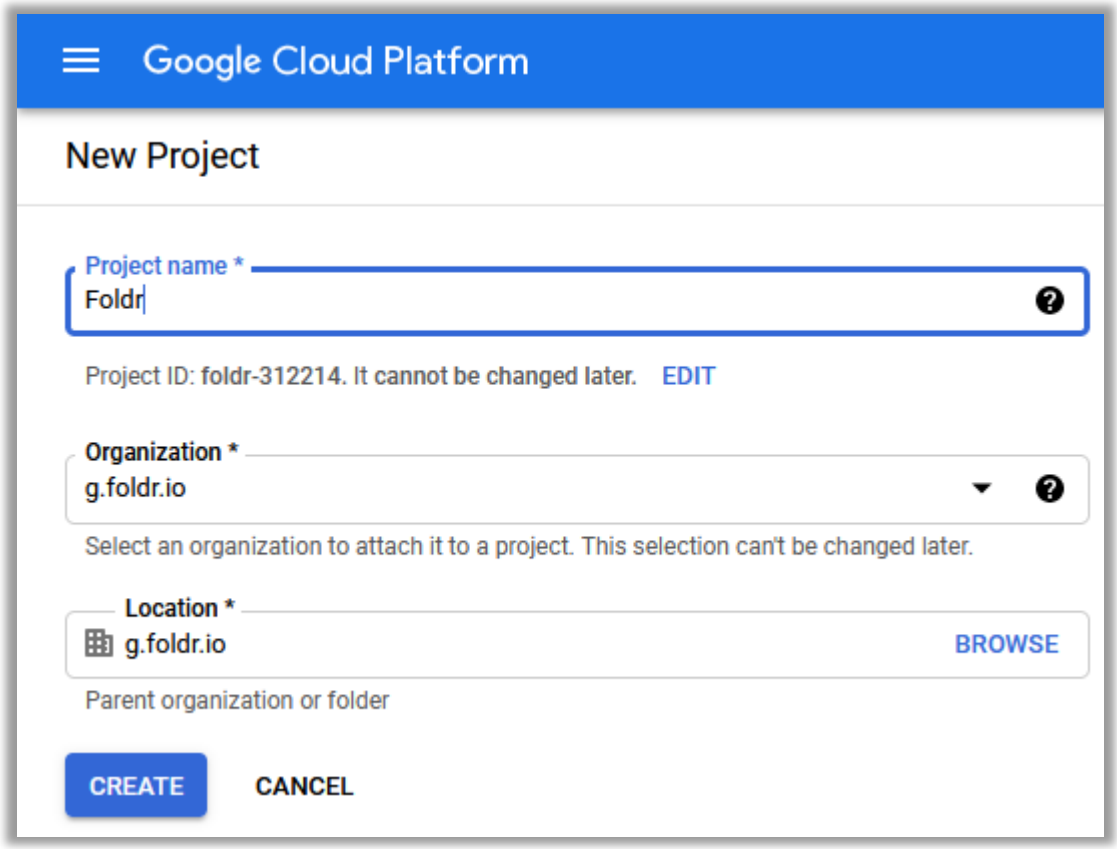


3. Click New Project

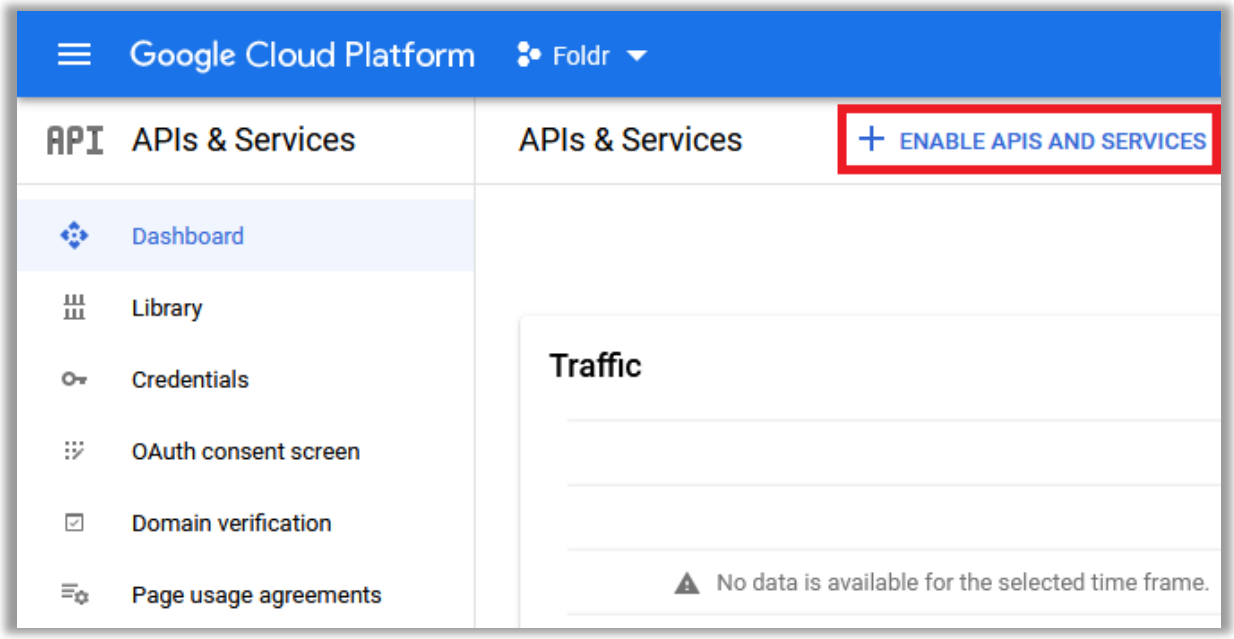


If desired, you can select the location of the app engine (Europe West, US etc.) to be used under Advanced

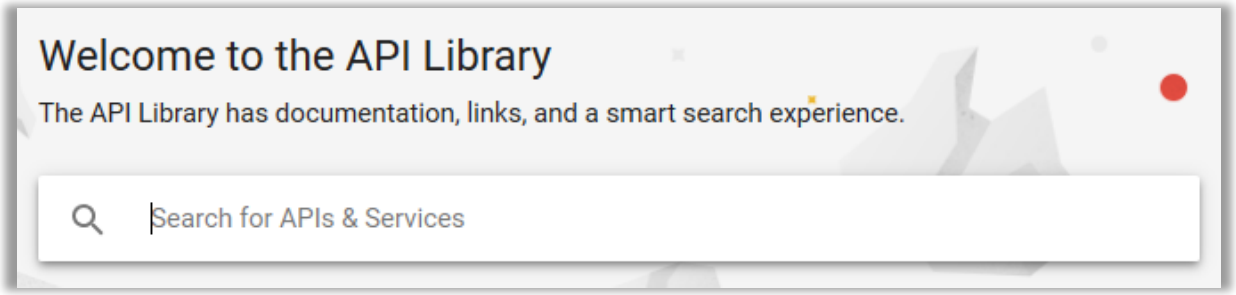
4. Give the Project a suitable name and click **Create**



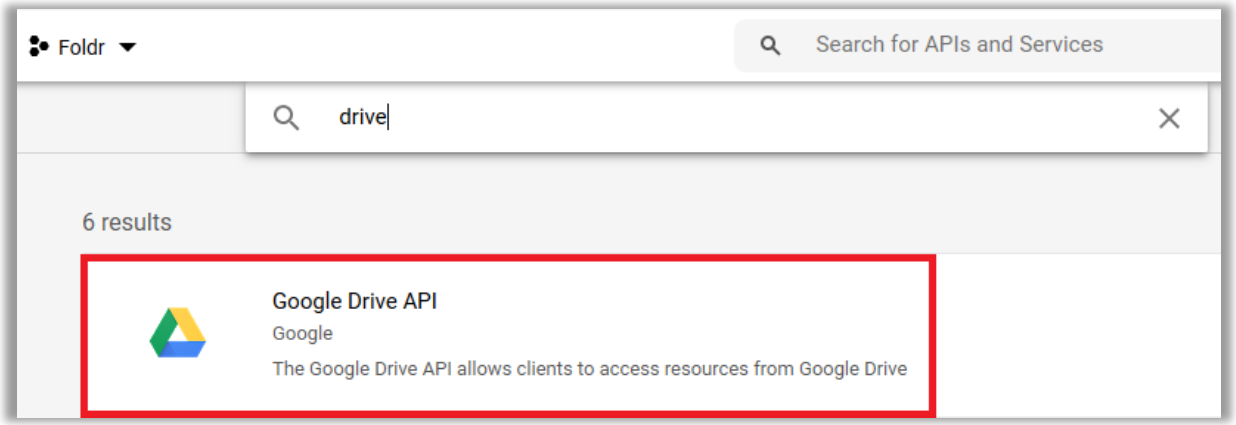
5. This will drop you to the APIs and Services panel. Click **+ ENABLE APIS AND SERVICES**



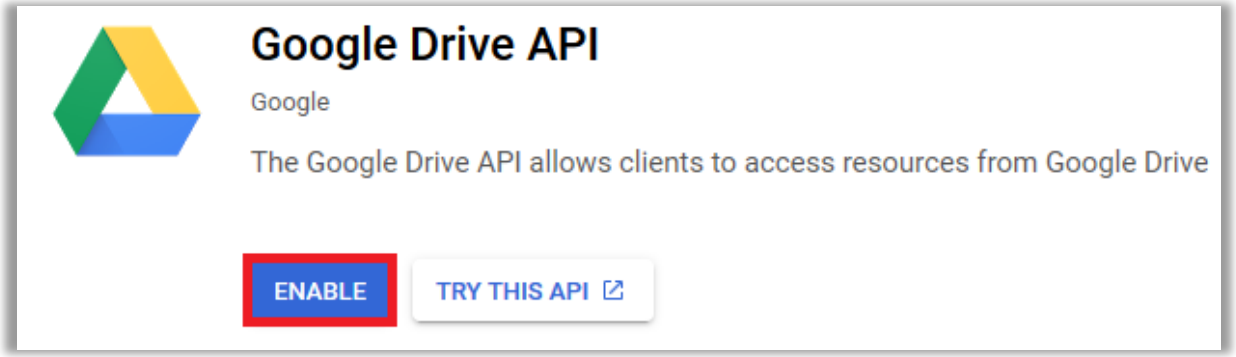
6. Search for 'drive' in the API library



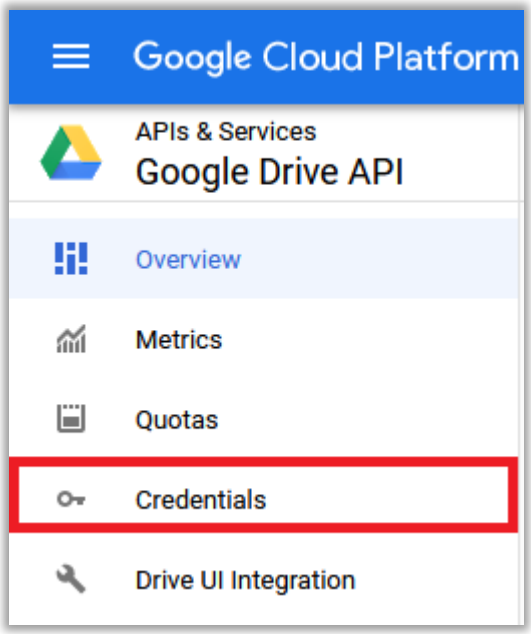
7. Select the Google Drive API



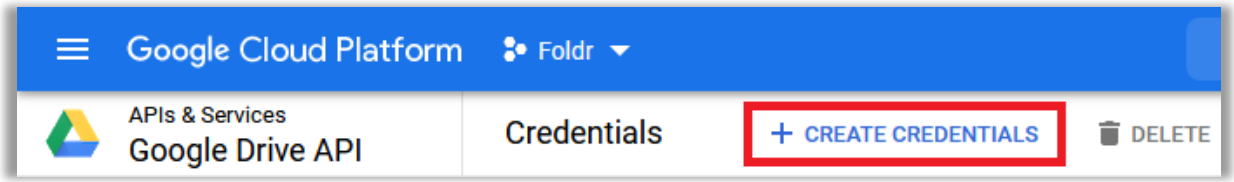
8. Click the **Enable** button



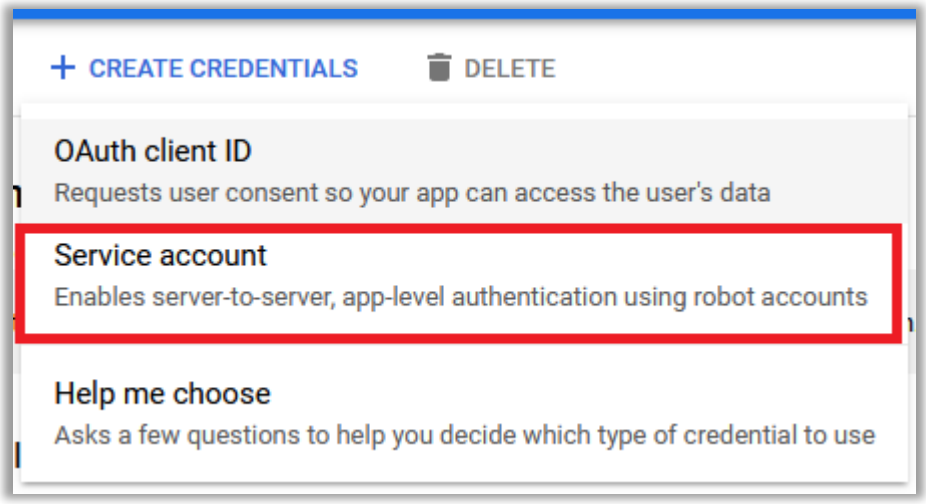
9. This will drop you at the Google Drive API panel. Click **Credentials**



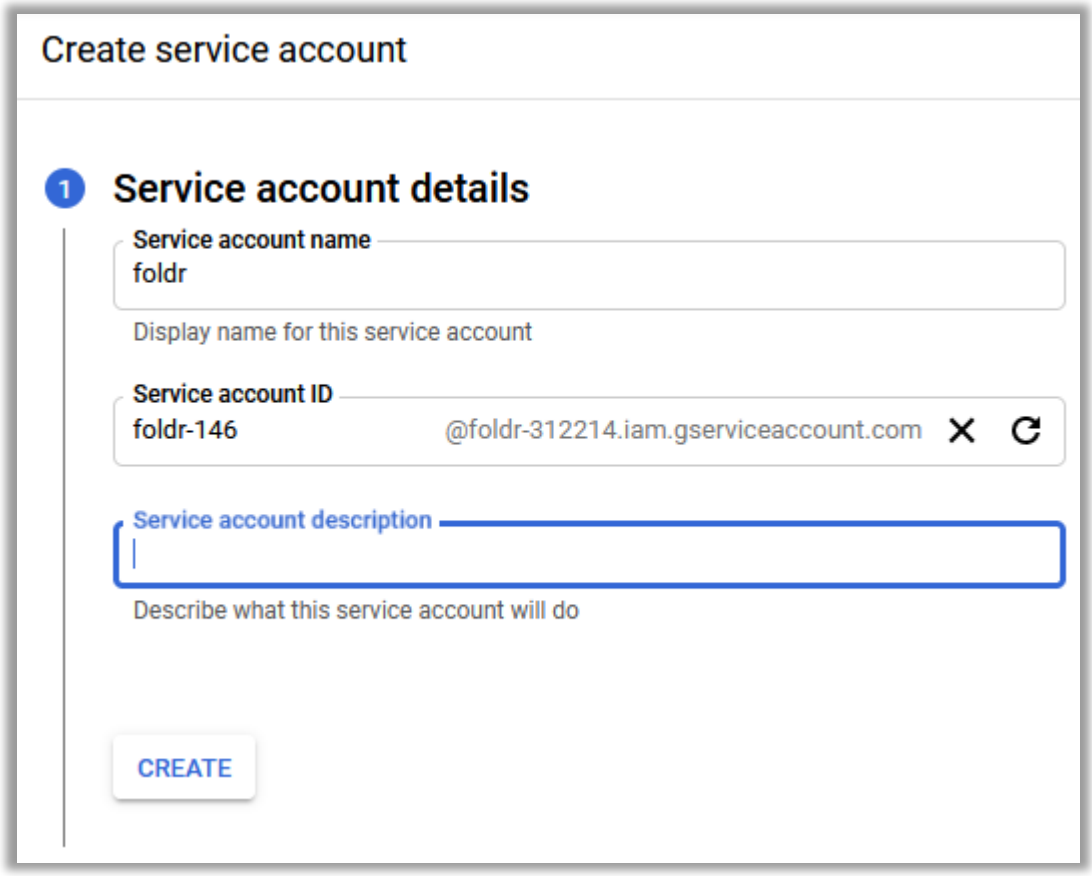
10. Click **+ Create Credentials**



11. Click **Service account**

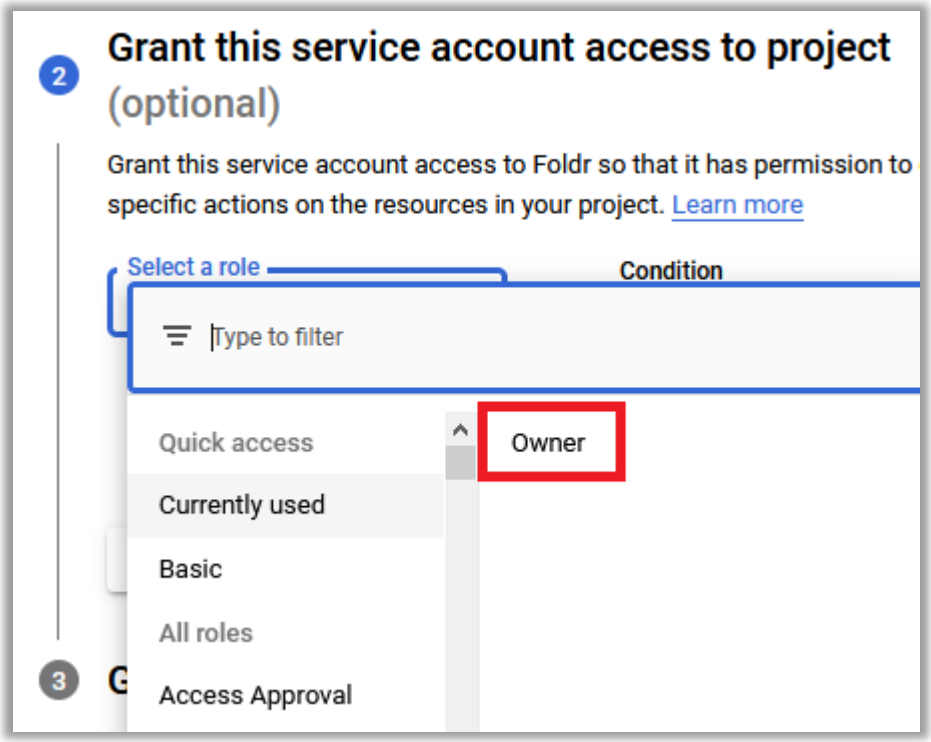


12. Give the service account a suitable name and click **CREATE**

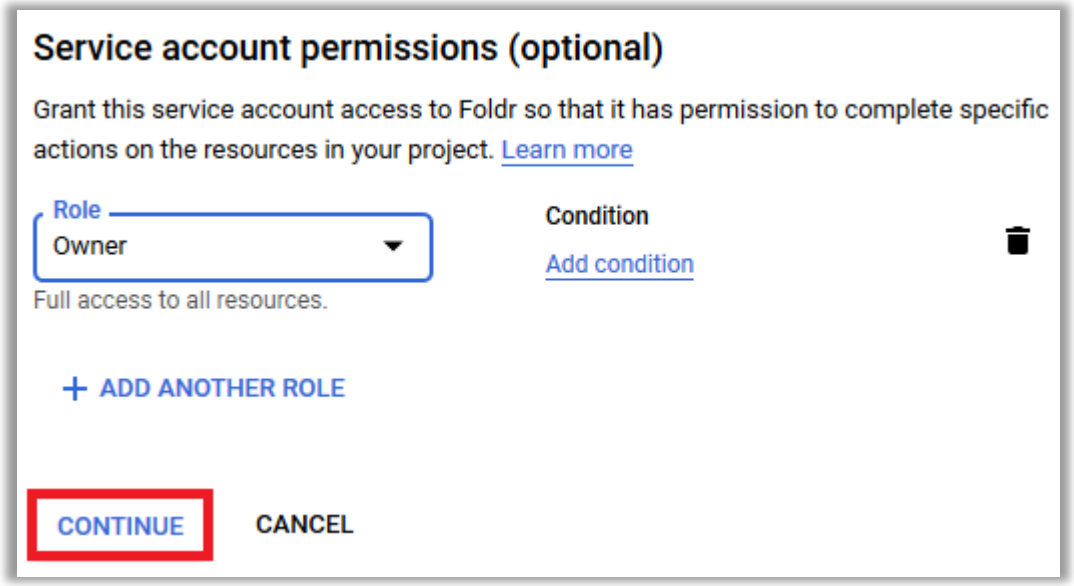


Note - The 'service account ID' is automatically populated

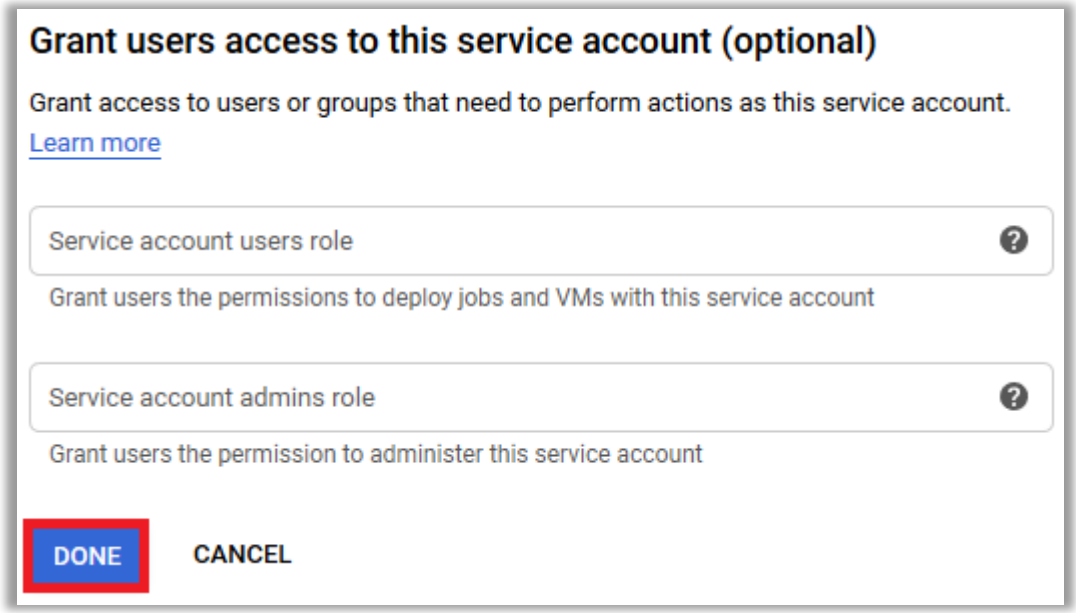
13. The service account permissions panel will display. Select the role as **Project > Owner**



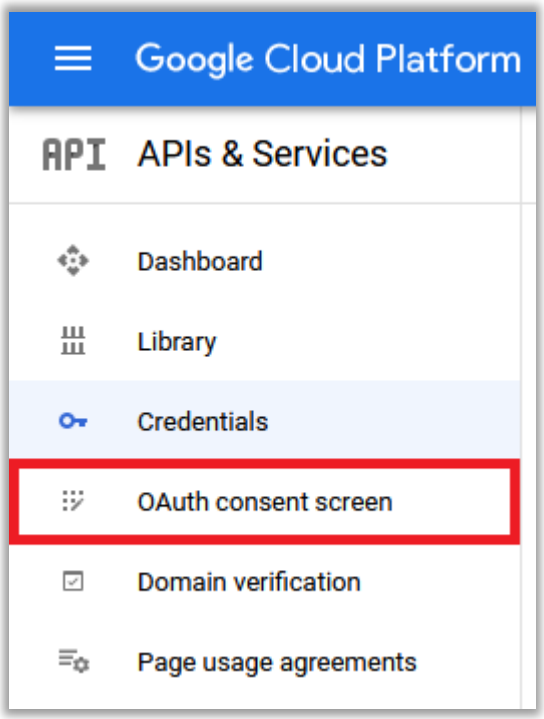
14. Click **Continue**



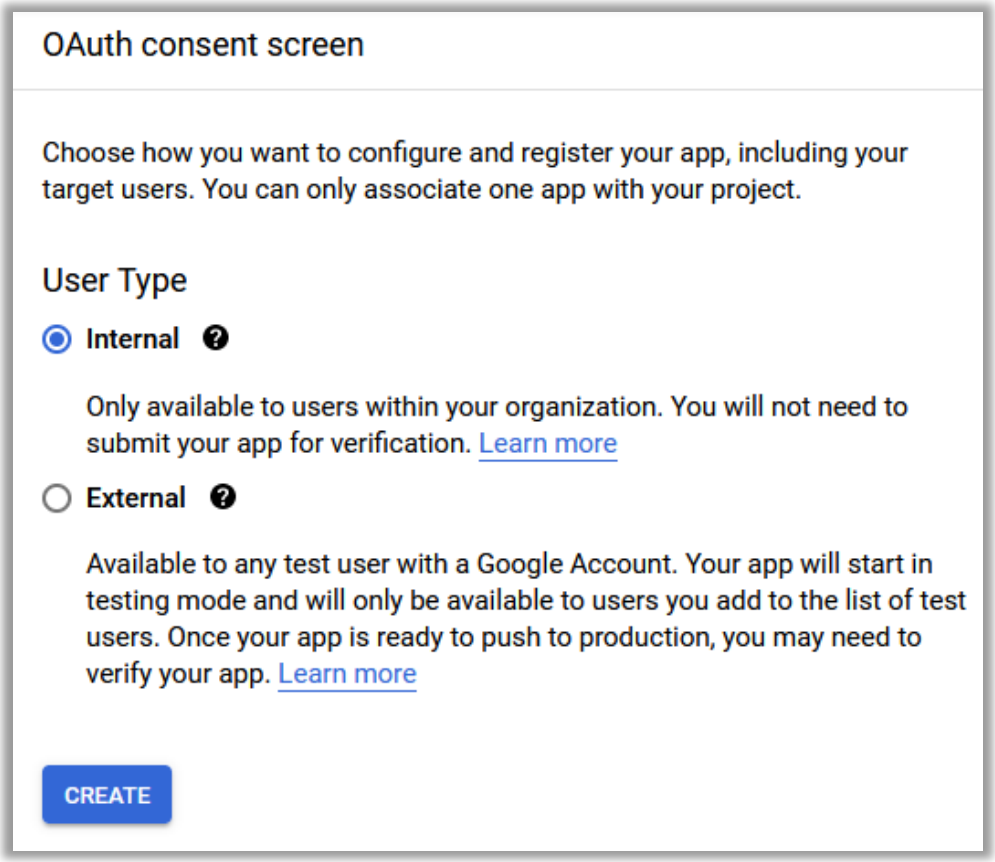
15. The grant users access to this service account dialog will display. Do not configure any options here and click **Done**



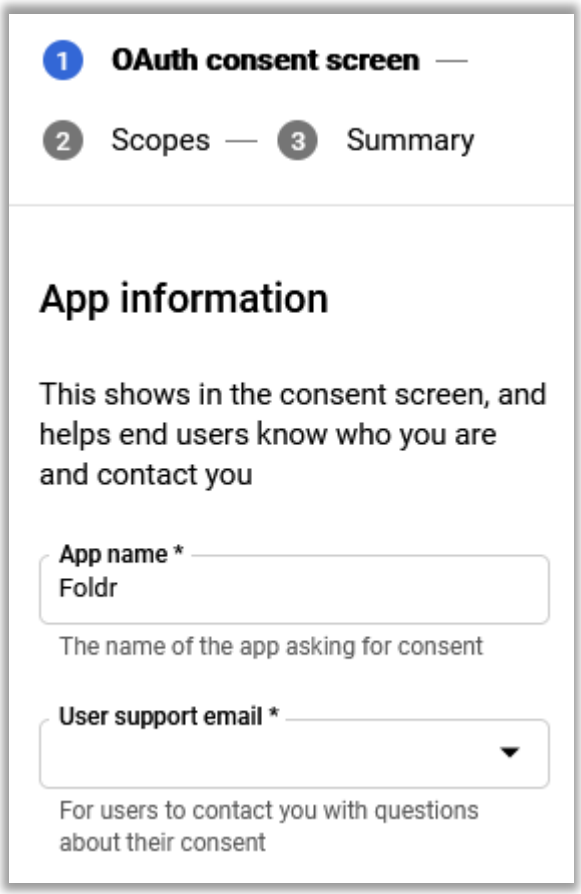
16. Next, configure the consent screen by clicking the **OAuth consent screen** option in the API & Services menu.



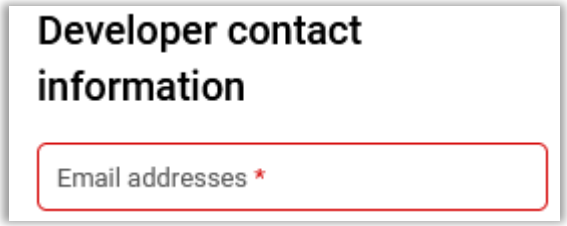
17. Select Internal as User Type and click **Create**



18. Enter a suitable **App name** and **User support email address**



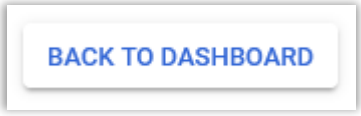
19. Scroll down and enter Developer contact information as an email address



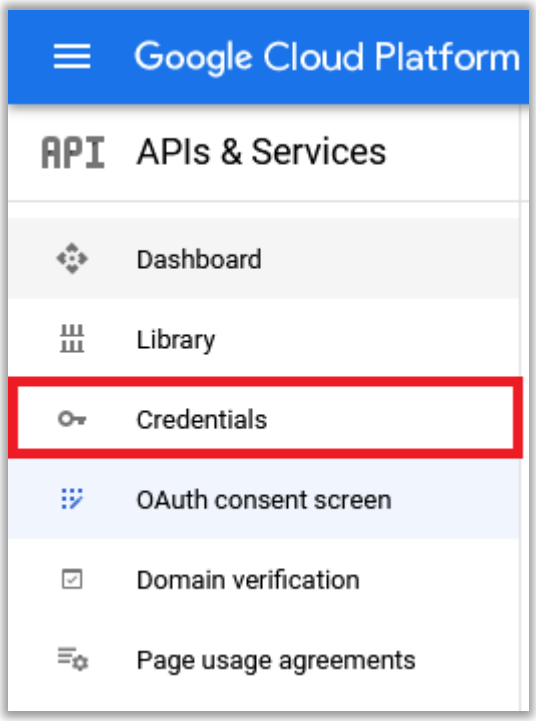
20. Click **Save and Continue**

21. The Scopes panel will display, do not configure any options here and again click **Save and Continue**

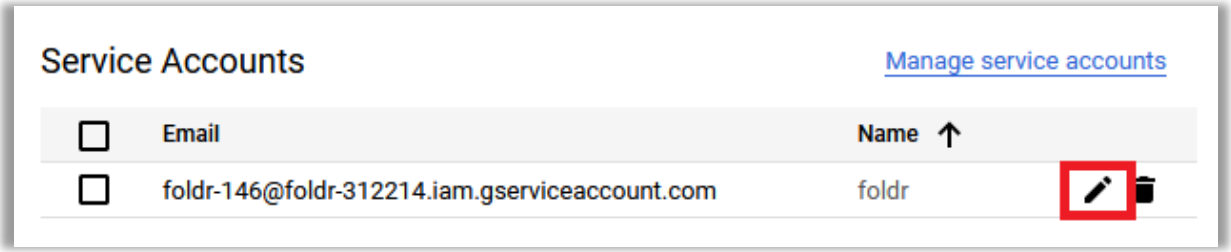
22. Scroll down on the Summary screen and click **Back to Dashboard**



23. Click **Credentials** in the API & Services menu

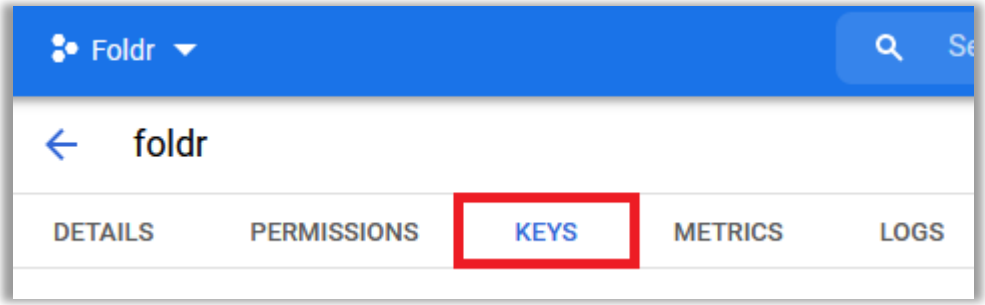


24. Click the **Edit** button highlighted below on the service account created earlier.

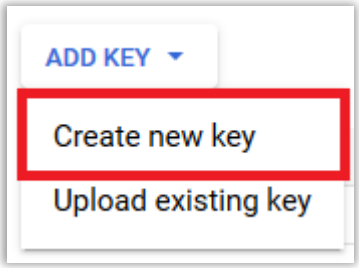


25. The service account details panel with be shown. Scroll down and click the **Show Advanced Details** button. Then under the **Domain-wide Delegation** section, **c**opy the *CLIENT ID* shown here and make a note of it as it will be used later.

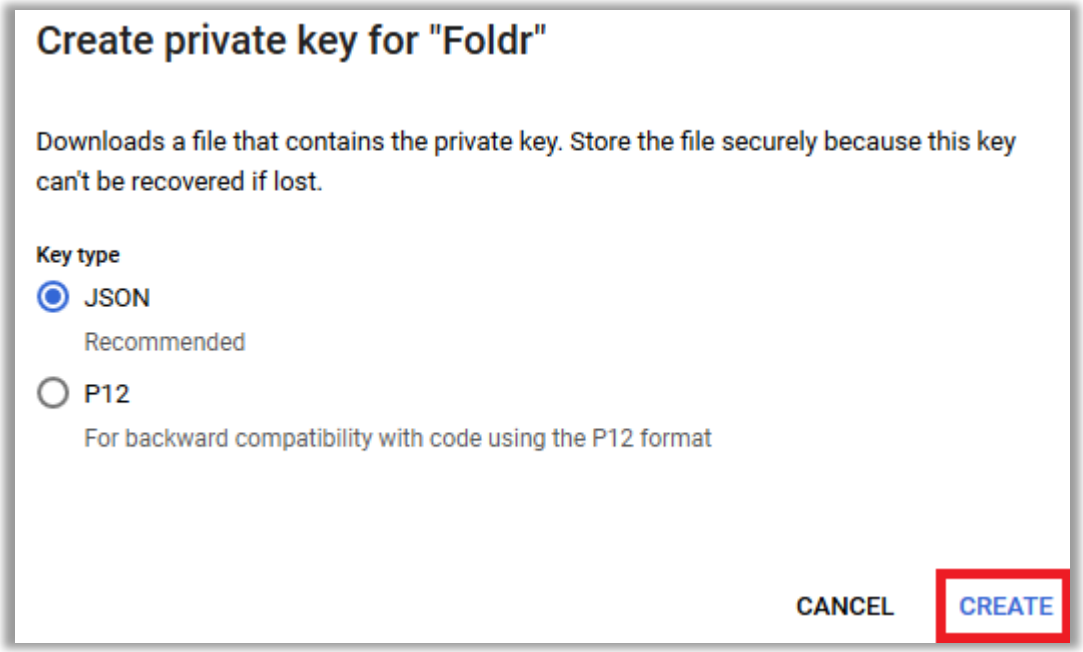
26. Click the **Keys** tab at the top of the screen



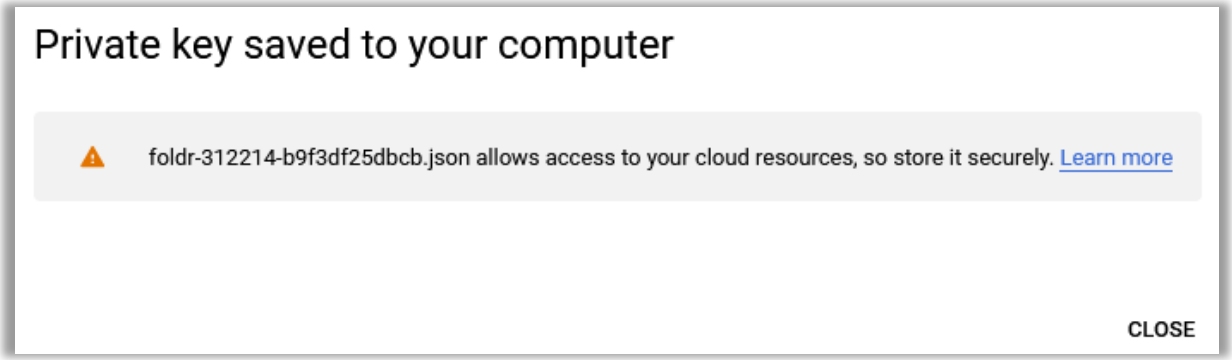
27. Click **Create new key**



28. Leave the key type as '**JSON**' and click **Create**

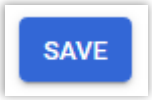


29. A notice will appear that the private key (.JSON file) has been created and this is saved to the local machine. Depending on your browser, you may get a Save As dialog appear asking where to save the .json private key. Keep this file in a secure place as it will be required later in the integration.



Click Close and the key will be shown in the summary

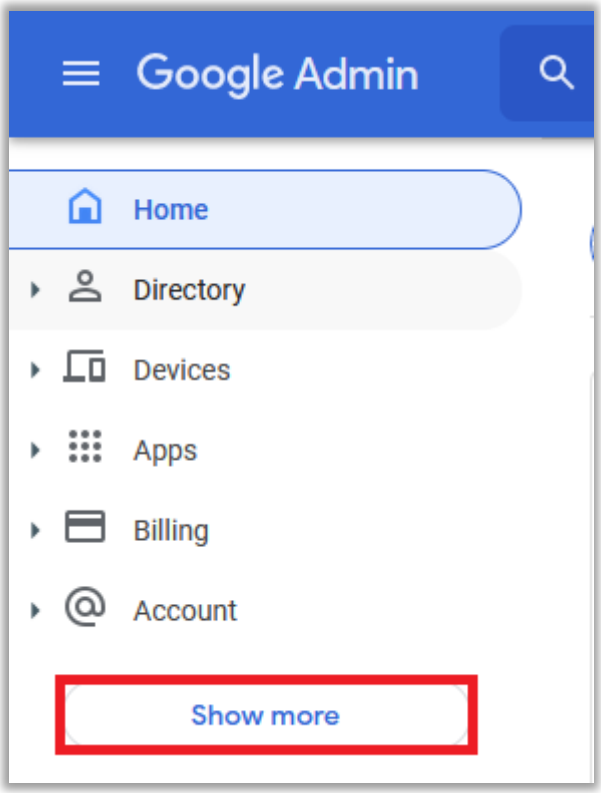
30. Click **SAVE** (directly under the key shown)



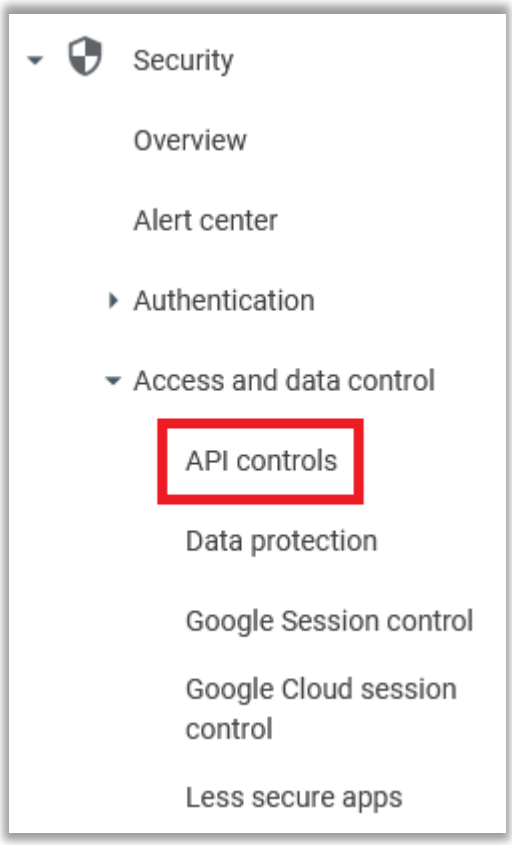
31. Click on the ***Details*** tab at the top of the screen and then select Show Advanced Settings (if shown) – under Domain-Wide Delegation click the **VIEW GOOGLE WORKSPACE ADMIN CONSOLE** button

32. The new browser tab will open at https://admin.google.com

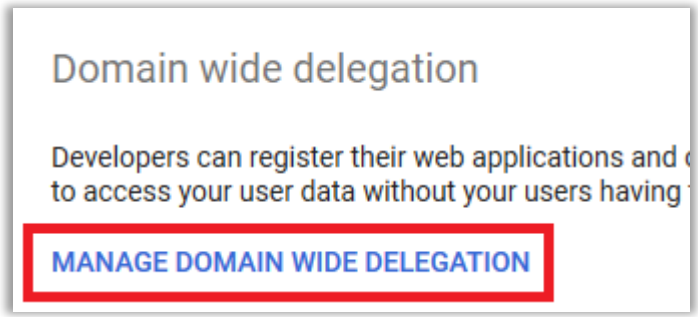
Click **SHOW MORE**



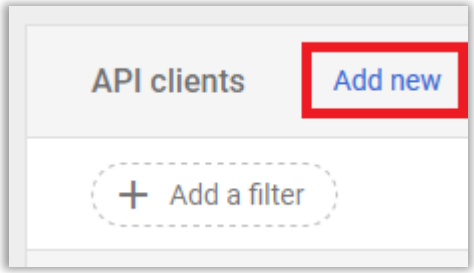
33. Expand **Security > Access and data control** and select **API controls**



34. At the bottom of API Controls page select **Manage domain-wide delegation**

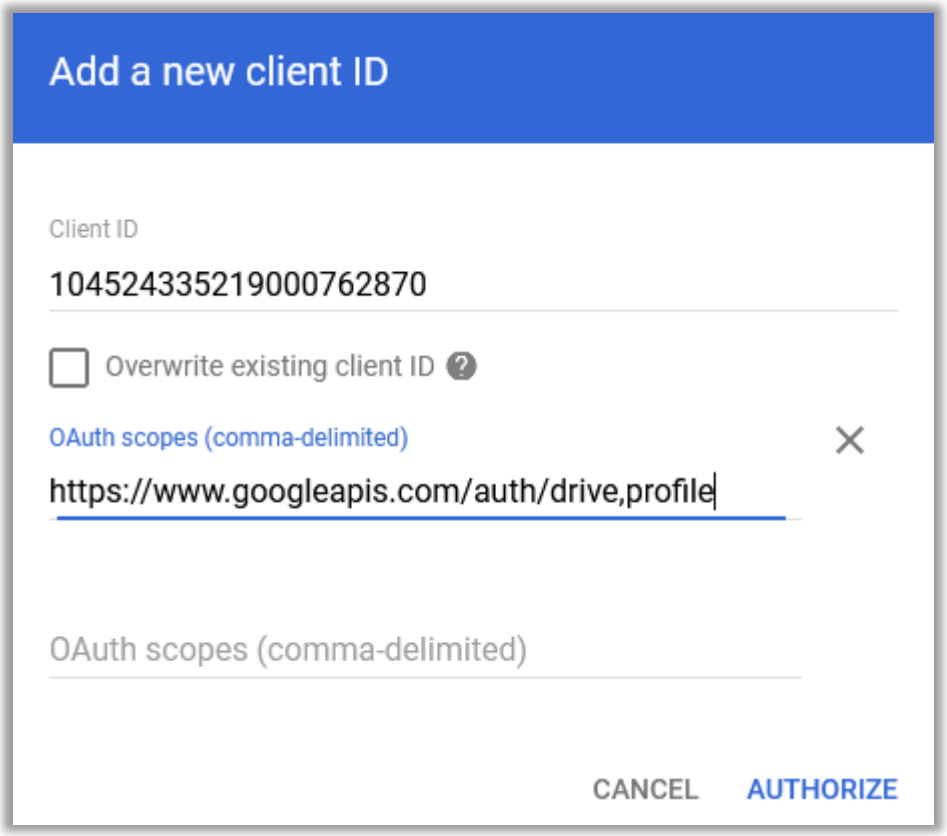


35. Click **Add New**



36. Paste the OAuth 2.0 Client ID as taken from step 25. In the OAuth scope field paste the following exactly as shown:

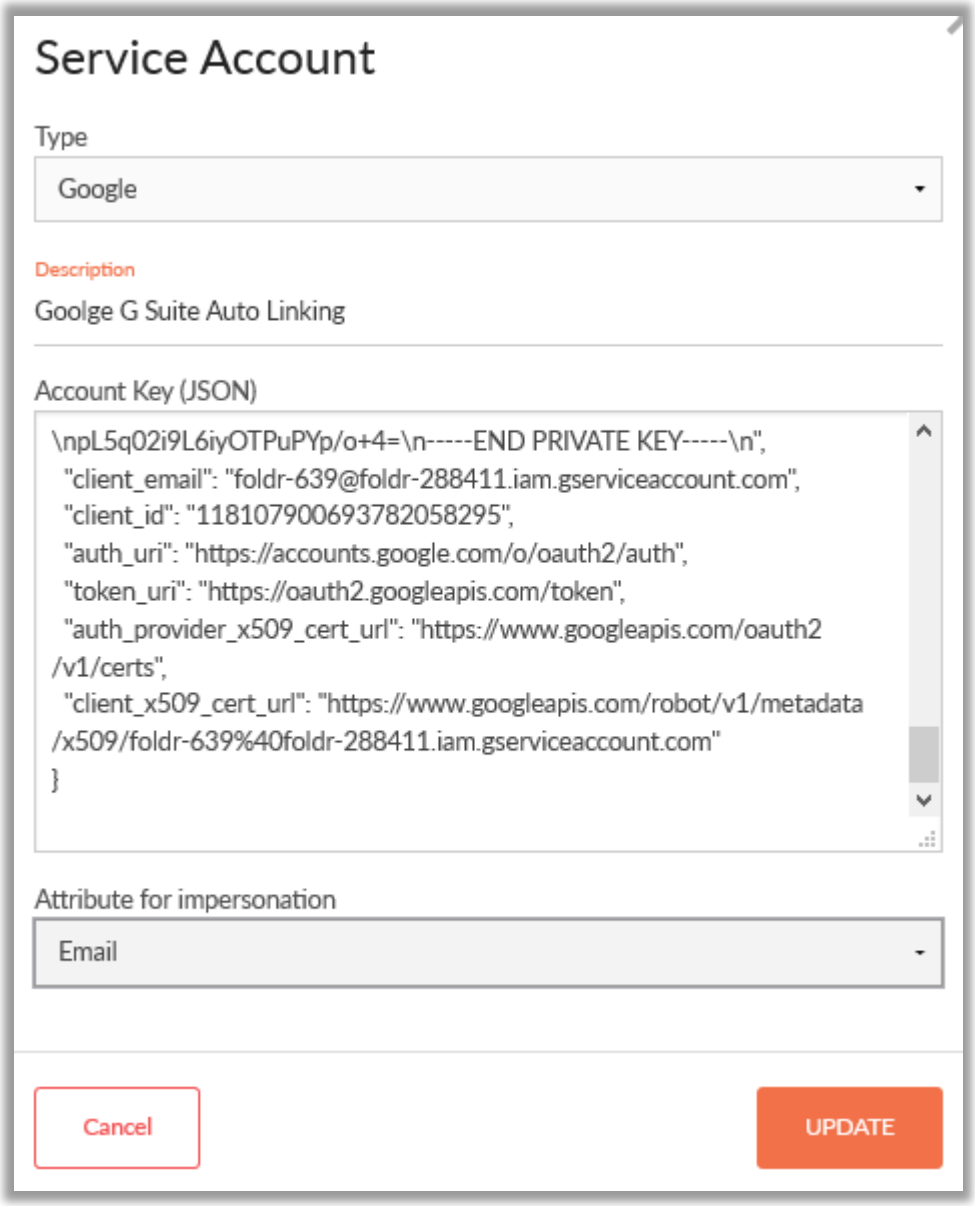
https://www.googleapis.com/auth/drive,profile



Click **AUTHORIZE**

37. Browse to Foldr Settings and create a new Service Account with Type '**Google**' within **Integrations > Service Accounts > +Add New**

38. Paste in the .JSON files (service account key) downloaded earlier into the Account Key (JSON) box.

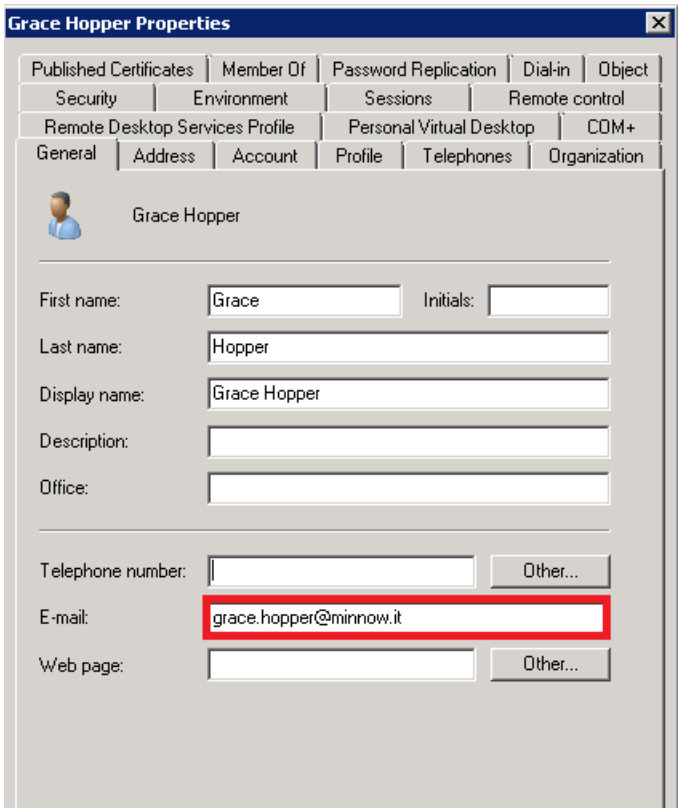


Note that the 'Attribute for impersonation' being used in the example above is **Email** (i.e. the ***mail*** attribute in Active Directory) – you can alternatively select the **UPN** (***userPrincipalName*** in Active Directory) or '**Custom**'.

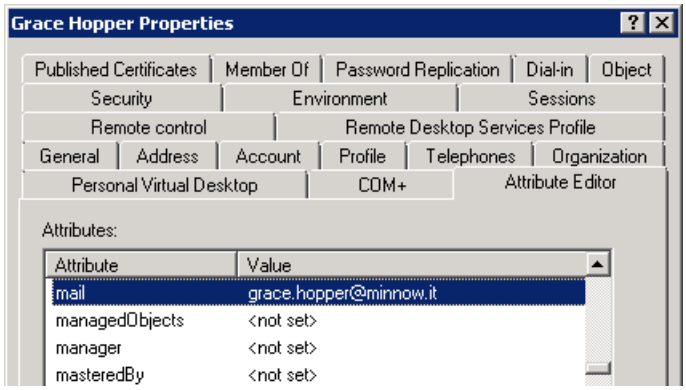
The ***Custom*** option is useful if neither the user's G Suite email address is populated as the Email or UPN attributes in Active Directory and allows the administrator to enter an example of:

%username%@domain.com

Note that the 'Attribute for impersonation' being used here is Email (i.e. the *mail* attribute in Active Directory). The user's E-mail field in the General tab populates the mail attribute automatically:

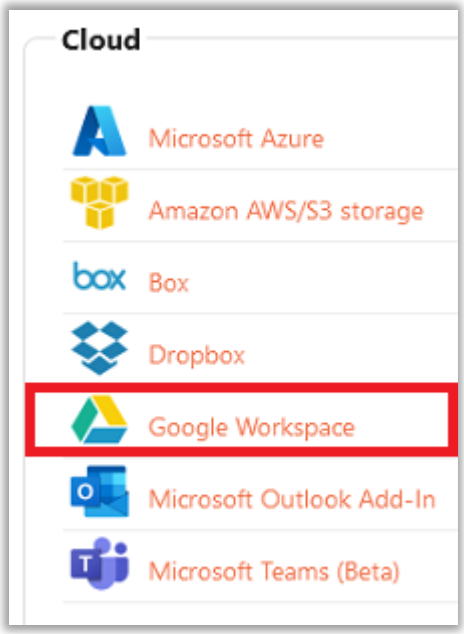


Email Address (mail) attribute in Active Directory:

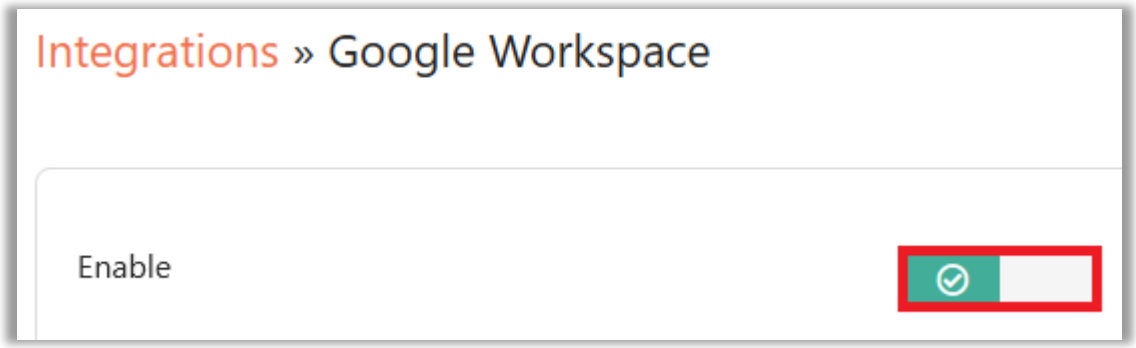


39. Click **UPDATE**

40. Navigate to ***Foldr Settings > Integrations > Cloud >*Google Workspace**



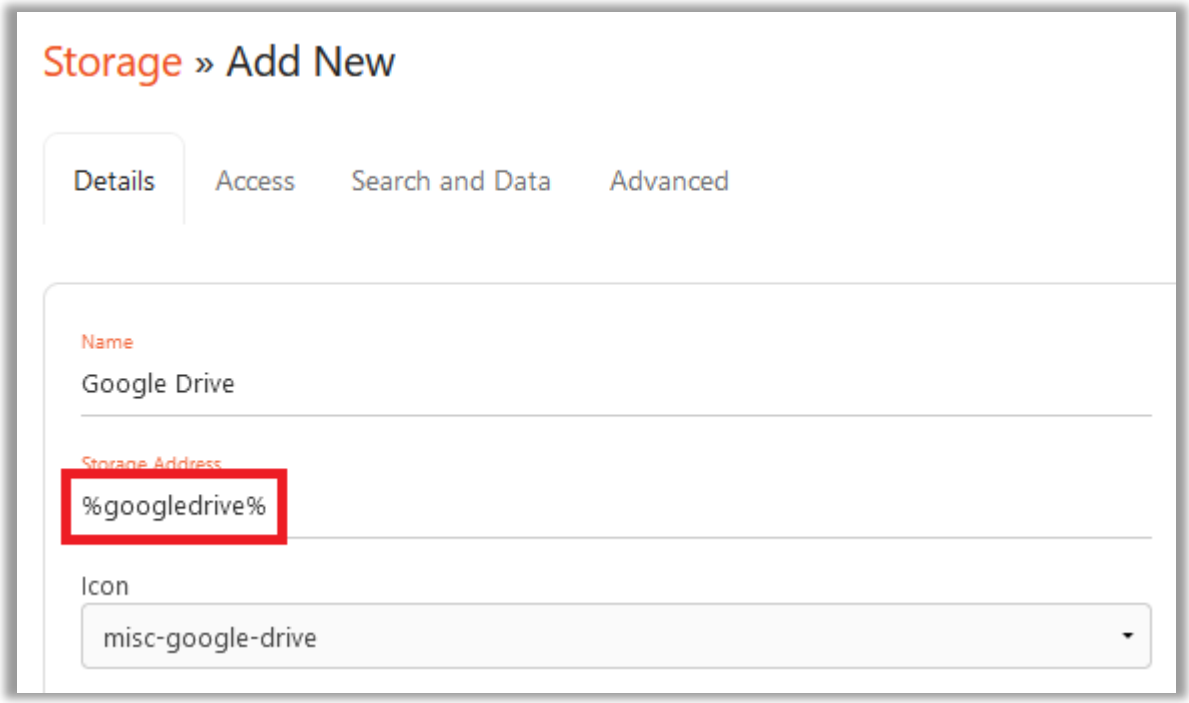
41. Enable the integration



42. Under the Access section select 'Use Service Account' and select the service account created earlier.

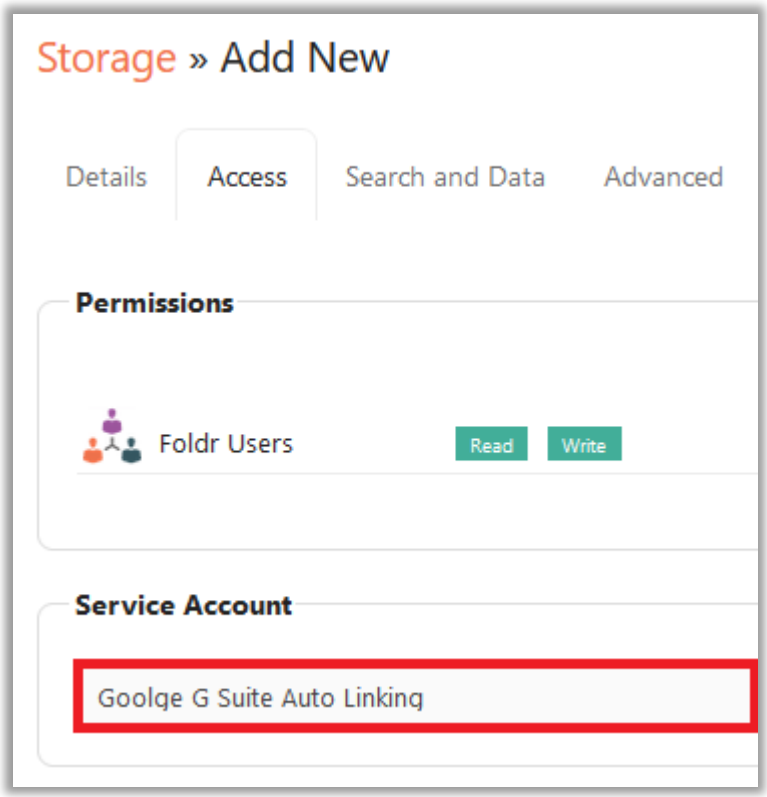
43. Next, create the storage object for Google Drive in Foldr Settings. Navigate to ***Foldr Settings*** > ***Files & Storage*** -create a new storage item by clicking **+Add New**

44. Give the storage location a suitable name and use the Storage Address of **%googledrive%**



Select the Google Drive icon (or other as required). Click **SAVE CHANGES**

45. Click the **Access tab** and select the Google service account that was created earlier. Click **SAVE CHANGES**

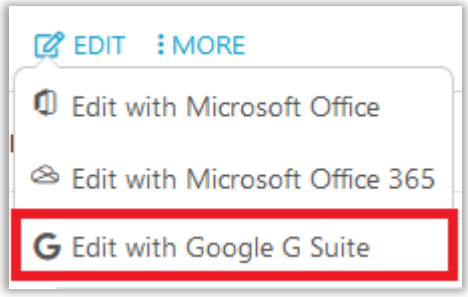


The integration for automatic account linking with Google Drive is now complete.

When a user logs into Foldr using the web, mobile or desktop apps, they will now see Google Drive under My Files.

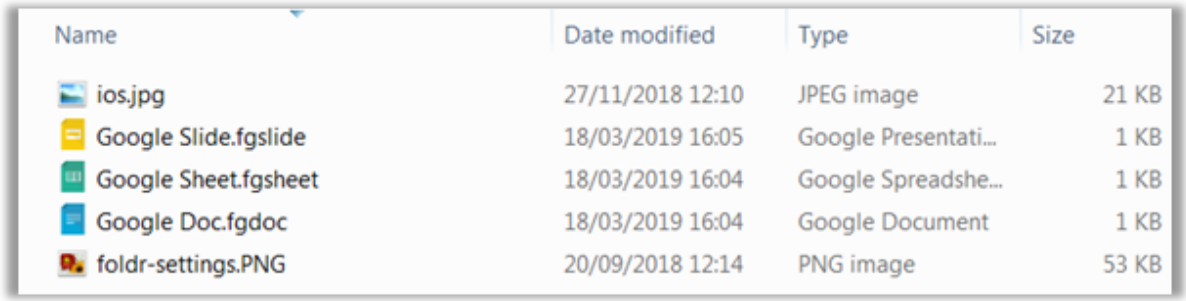
Microsoft Office documents that are hosted on-premise or in Google Drive may be edited in place using G-Suite/Workplace cloud-based editing tools/web apps (Docs, Sheets and Slides) will save back to their original location once the user has finished editing. As part of enabling the Google integration the user will now see a 'Edit with Google G-Suite' button in the Foldr web app for Office and G-Suite files.

Edit with Google Docs button (web app using the web file viewer)



Edit with Google Docs button (web file viewer disabled)

The Windows and macOS desktop apps will allow users to edit G Suite files (Docs, Slides and Sheets) straight from Explorer / Finder – double click a native Google file and the system default browser will launch and load the Google web app and document ready for editing.



Searching Google Drive in Foldr

Providing Search capabilities through Foldr (web, desktop or mobile apps) for files in Google Drive can be enabled by following the steps 1-4 on the following online KB article (see section titled ***Using the cloud provider's search API (no indexing required)***)

Google Integration 2 – Manual account linking

IMPORTANT - This integration method is not typically recommended for an organisation with a managed Google G Suite / Workspace environment. Auto account linking should be used above (Google Integration 1)

Pre-requisite: To use this feature, the Foldr appliance must be accessible externally and have a signed SSL certificate installed.

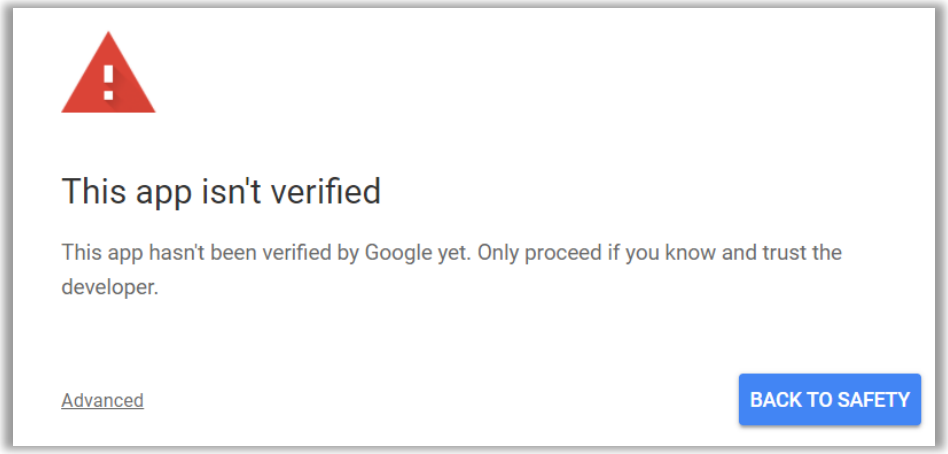
The steps to configure manual account linking for Google G Suite/Workspace are available in the online KB article here

NOTE - Linking Personal Google Accounts

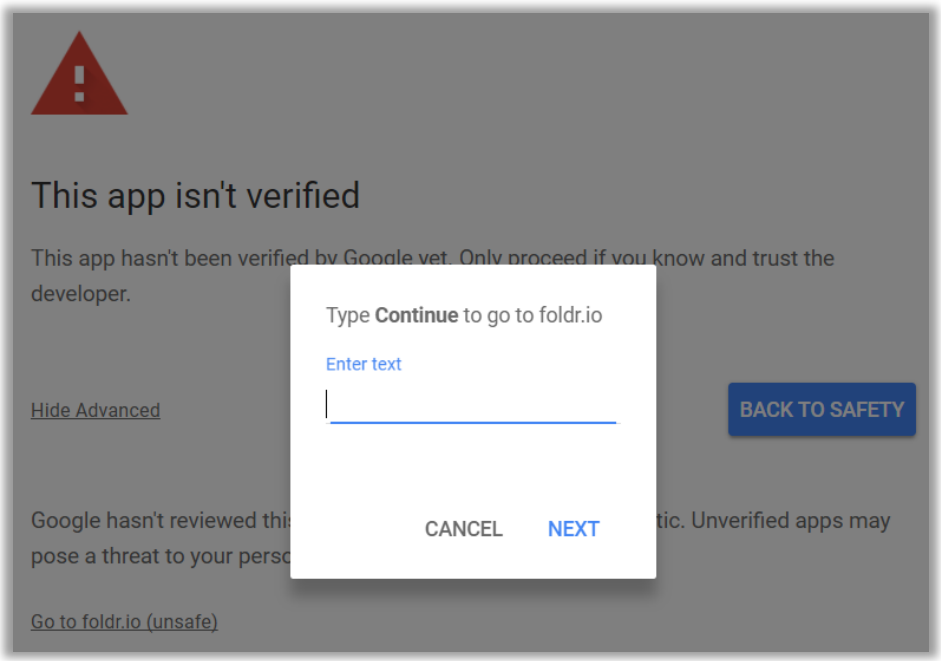
Security changes that were made to Google G Suite / Workplace, mean that it while it is possible to link a personal Google account in Foldr, users now receive an additional security warning that the Foldr installation hasn't been verified.

This prompt is shown once, when the user links their account and does not affect any other functionality. To proceed through this, the user must click **Advanced > Go to *domain-name***

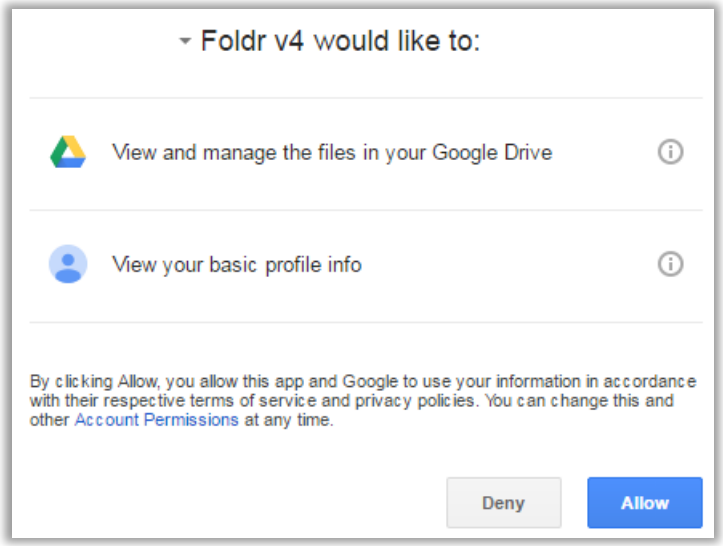
As Foldr is a self-hosted solution, each installation would need to be verified on an individual basis with Google to remove this warning. This includes completing an app Oauth review form and includes making available a privacy policy for Foldr hosted on a server in the same domain as your Foldr installation.



Type *Continue* and click NEXT



Accept the permission dialog



If you would like to submit your Foldr installation for review with Google to remove the warning shown about it is recommended that you firstly validate ownership of your domain and complete the Oauth review form.

Google Domain Verification

https://www.google.com/webmasters/tools/home

Google Oauth App Review Form

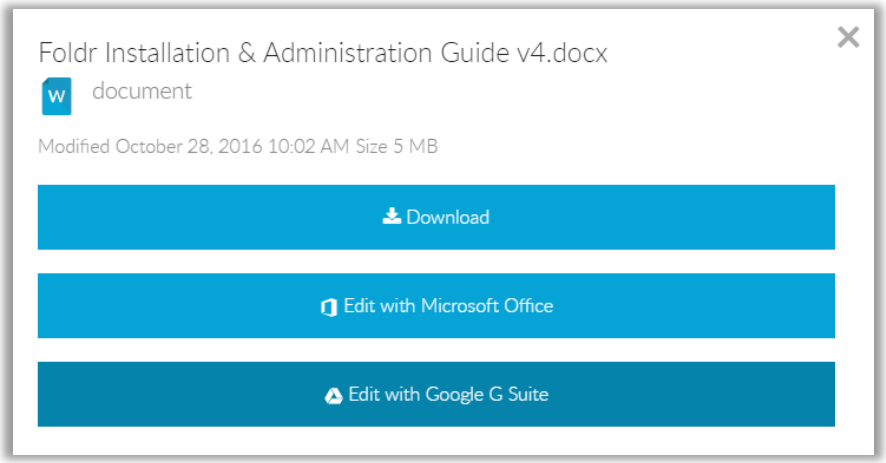
https://support.google.com/code/contact/oauth_app_verification

Providing the API has been enabled correctly, and a user's account has been linked, Google Drive should now be accessible in the main Shares list within My Files. The ability to edit Office documents through the **Edit in Google G Suite** but will now be available in the web app when users click on local or cloud-based Office documents.

Document Editing – Google G-Suite (Docs, Slides or Sheets)

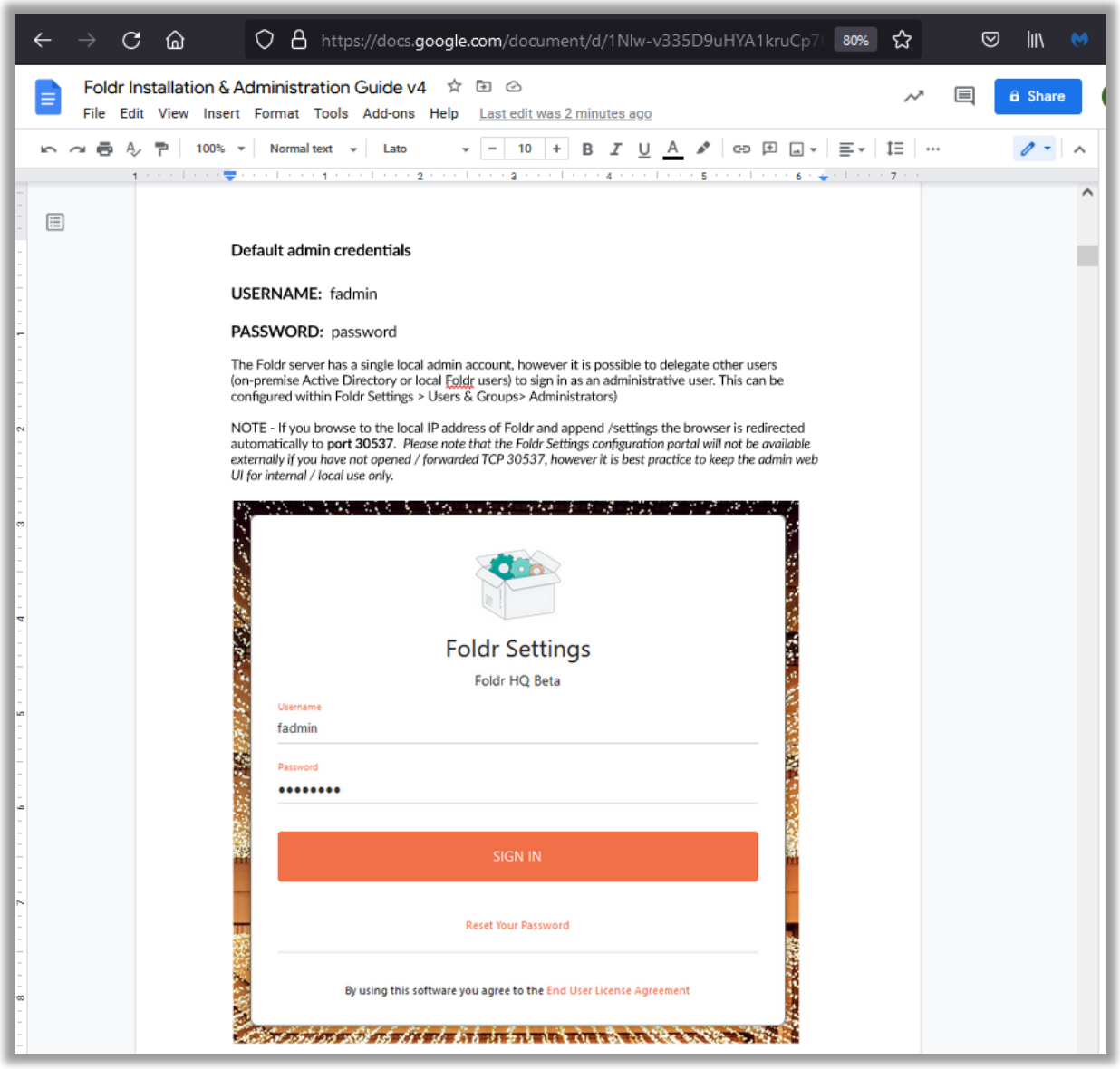
When the Google integration is complete (option 1 or 2) users can select, and edit on-premise or cloud-based Microsoft Office files, or native Google Docs, Slides or Sheets for editing in the G-Suite browser interface using the appropriate Google app.

Example – Edit a word document held on an on-premise SMB share in Google Docs.

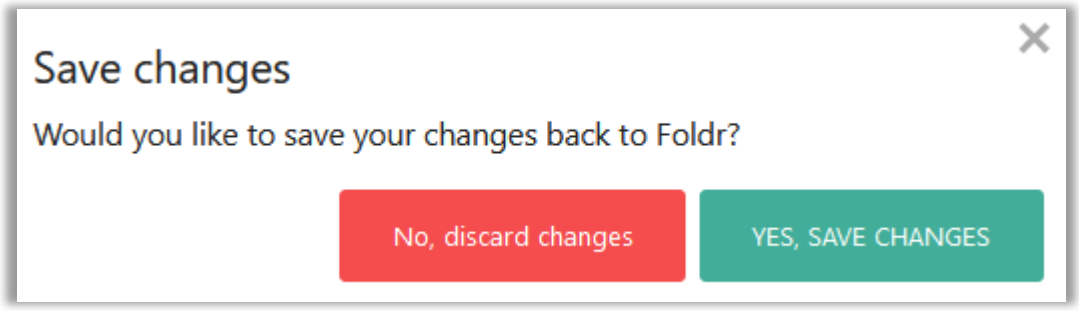


The user selects a document and clicks 'Edit with Google G Suite'. The file is copied to Google Drive temporarily into a staging folder in the root labelled 'Foldr Files' and is then presented in the browser, ready for editing in the relevant G Suite interface.

Word documents in Docs, Excel workbooks in Sheets and PowerPoint presentations in Slides.



If the source document resides on Google Drive, any changes are saved automatically when the browser tab is closed. If the original document was sent to Google Apps from another location, you will be prompted to either or discard or save changes back when the Google Apps tab is closed. See below:



By default Foldr, if the manual account linking integration option is used (option 2), the system will allow users to link *any* Google account to their Foldr account. Google accounts that are outside of the organization's administrative control, such as a personal account, will be shown a Google security warning but users can still proceed past this and link the account successfully.

If it is desirable to only permit organisation-controlled Google accounts to be linked in Foldr you should specify your Google G Suite domain within ***Integrations > Google G Suite > Google G Suite Domain***

Shared Google Drive Accounts

Foldr gives you the ability to present a specific Google Drive with everyone in the organisation or selected users/groups as required. The shared Drive still belongs to a user in the Google Apps / G Suite domain however a Google service account is used to impersonate this account for access by others.

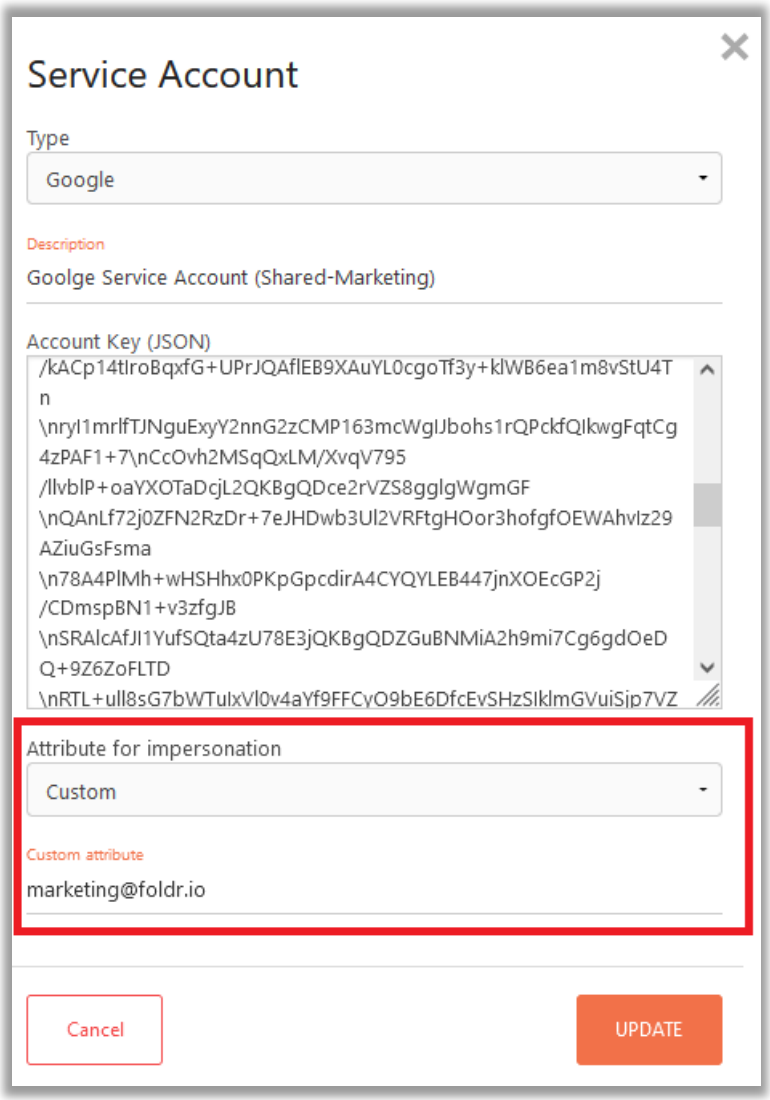
The user being impersonated can be either a new dedicated user account created to facilitate a shared area or an existing user.

Example – Creating a Shared Google Drive for a Department

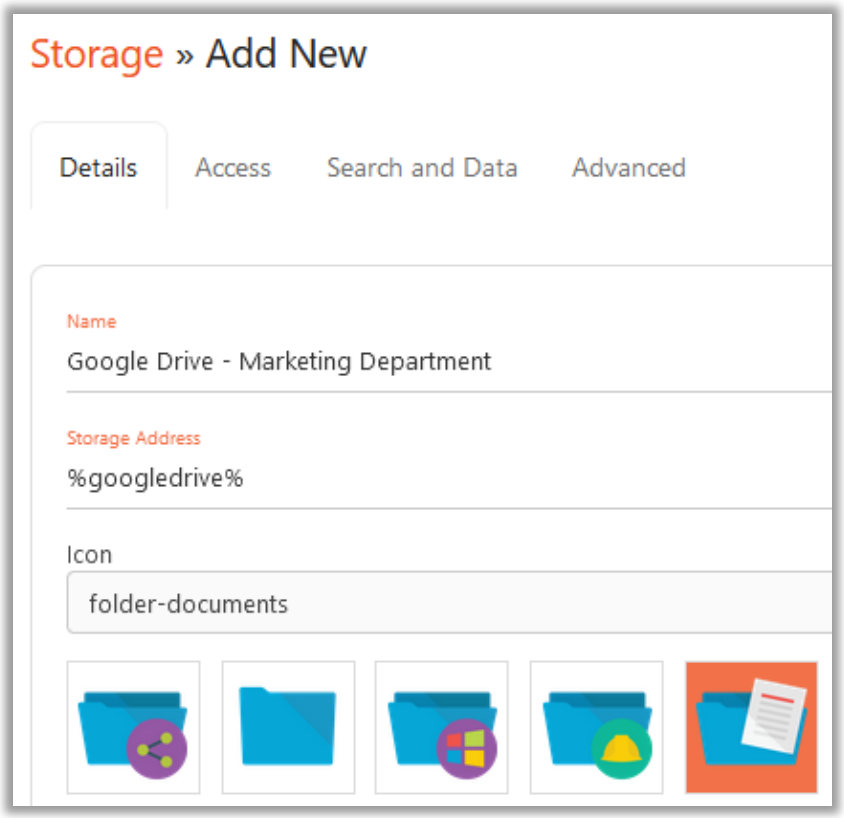
1. If required, create the new user account (to be shared) within the Google Admin Console at admin.google.com for the Mathematics department.

2. Using the same process as above (the same private key JSON file may be used) create another service account within ***Foldr Settings > Integrations > Service Accounts***

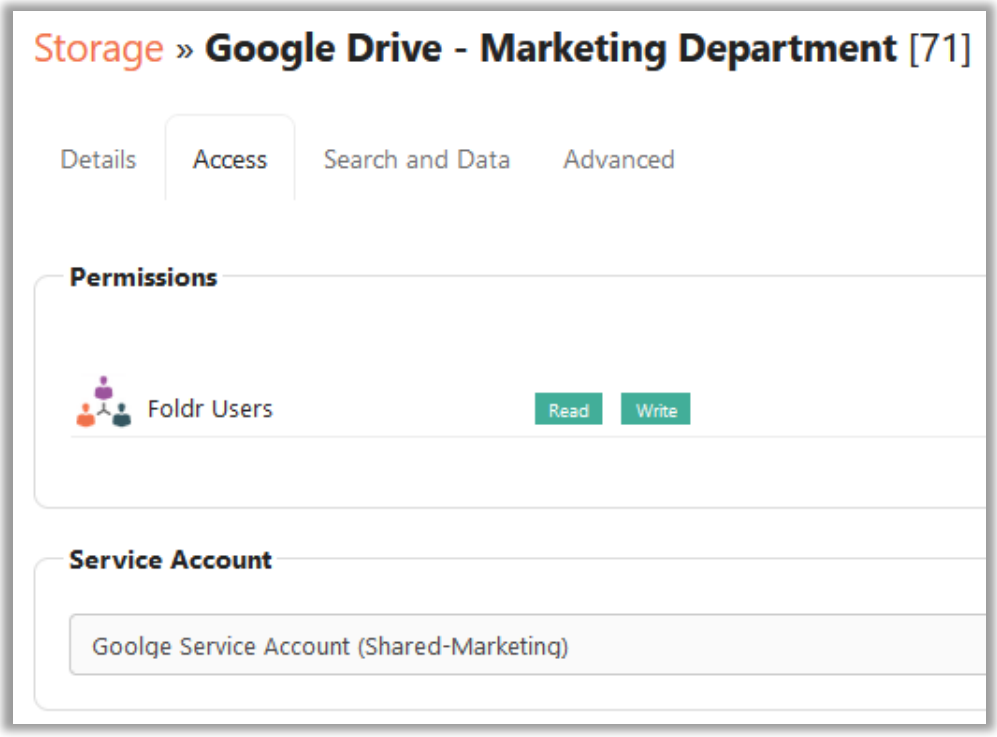
Note the User Attribute selected is **CUSTOM** and we are specifying the email address of the new shared Google user account for impersonation.



3. Create a storage item within ***Foldr Settings > Files & Storage*** and configure it to use the service account (Access tab) created above



In the Access tab, select the Google service account to be used to access the Marketing Drive.



Note – You can control visibility of the Marketing Google Drive using Foldr permissions in the Access tab. Leaving the permissions as default (Foldr Users – read & write allowed) will allow all users full access to the shared Google Drive.

The built-in Foldr Users group can be removed and replaced with specific users and groups that require access to the Marketing Drive as required.

Google Shared Drives (Team Drives)

Google Shared Drives may be presented in the Foldr interface alongside a user's personal Drive and other storage locations. Users working with Google Shared Drives can treat it as any other storage location within Foldr and may individually or collaboratively edit documents in G-Suite from the web app.

The administrator has the option of presenting either the Shared Drive root as a storage item with each Team Drive presented automatically inside this as a sub folder, or individual Shared Drives may be presented as separate items under My Files.

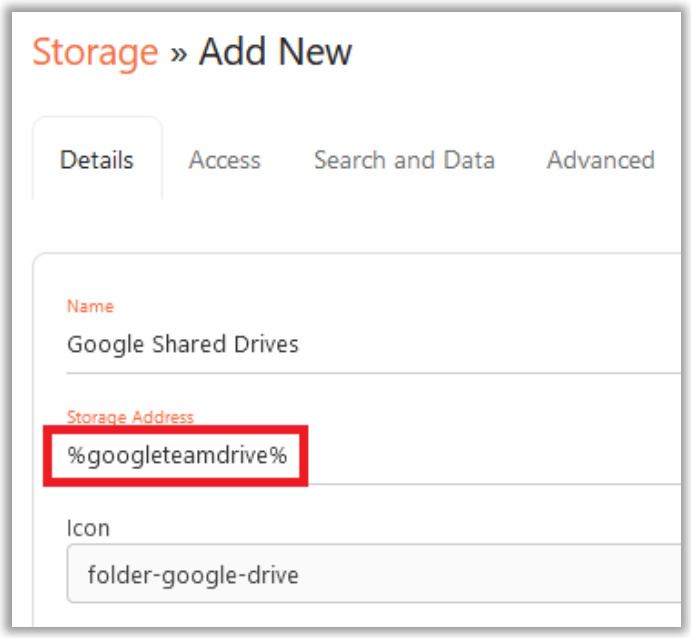
It is recommended that you use the automatic account linking method (Google service account to automate the process of linking the user's Google and Active Directory account) when using Google Shared Drives, however manually linking Google accounts will also work with Google Shared Drive.

Steps to present the organisation Team Drive root to users:

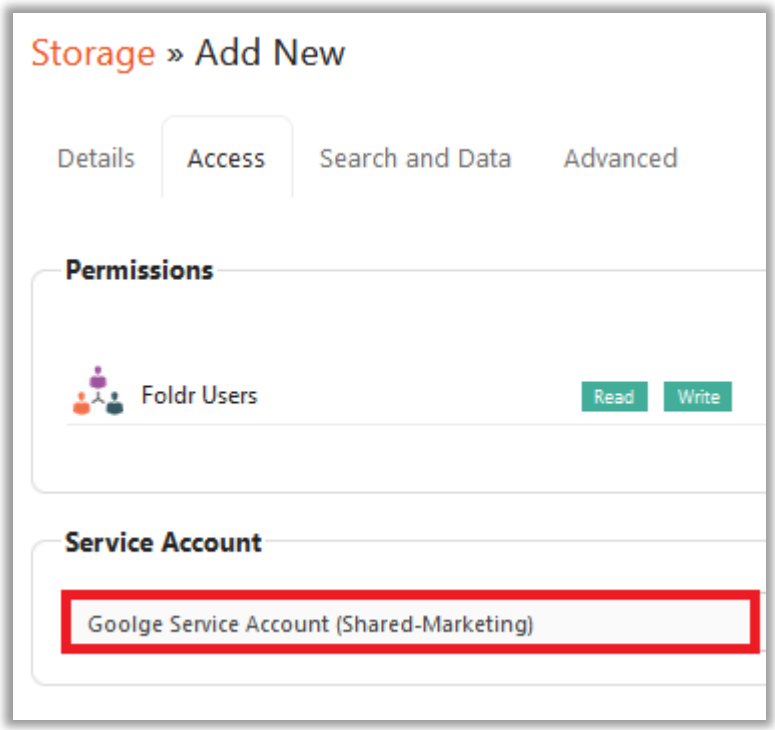
1. Follow the standard Google G-Suite configuration steps here (automatic/service accounts) or here (manual account linking)

2. To present the organisation's Team Drive root, add a new share / storage location under ***Foldr Settings*** > ***Files & Storage*** using a storage address path of:

%googleteamdrive%

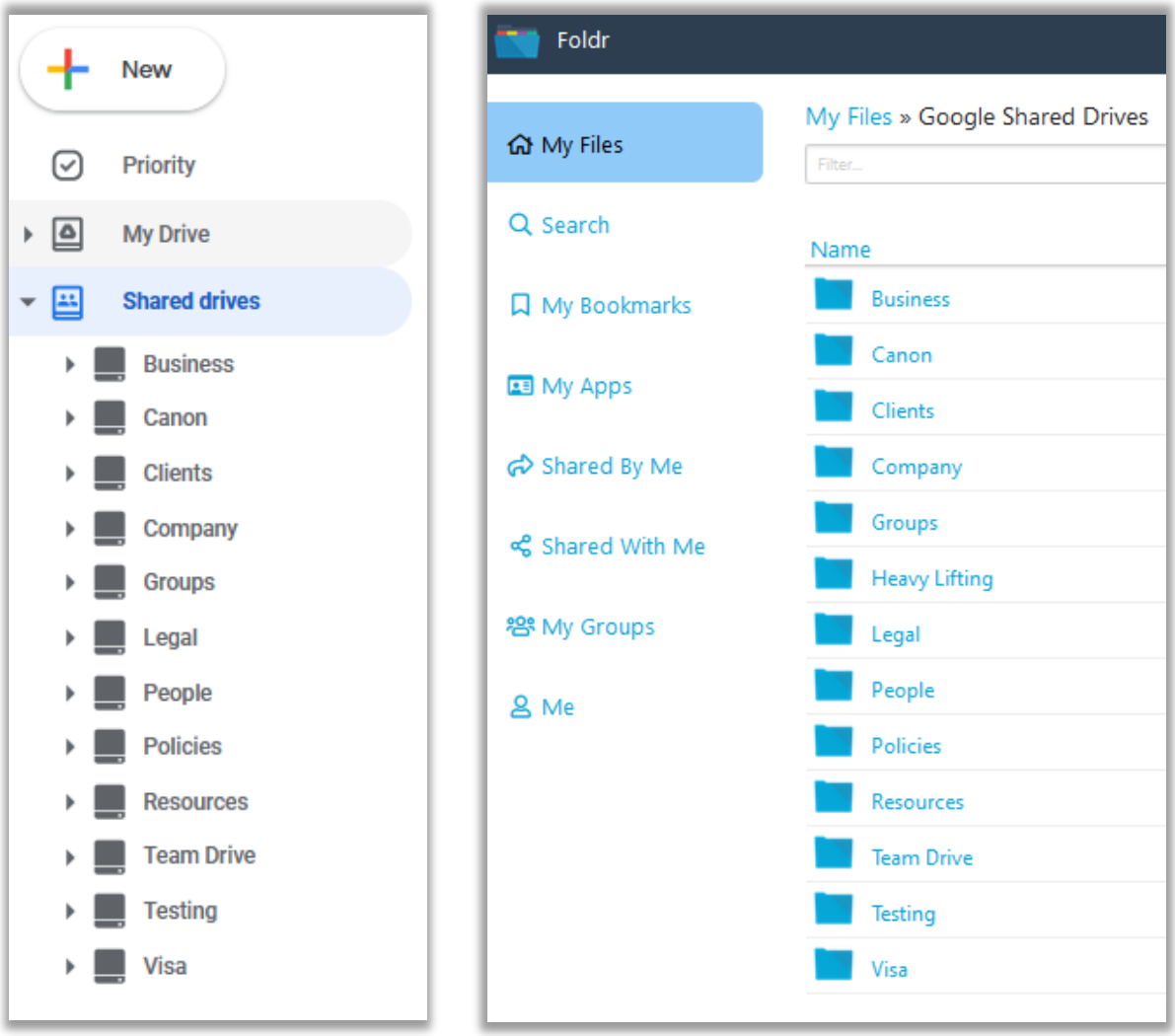


3. Configure other options / permissions as appropriate, if using a Google service account (automated account linking) select this in the Access tab and click **Save**.


Storage » Add New
Details
Access
Search and Data
Advanced
Permissions
Foldr Users
Read
Write
Service Account
Goolge Service Account (Shared-Marketing)

Google Shared Drives in the Foldr interface:

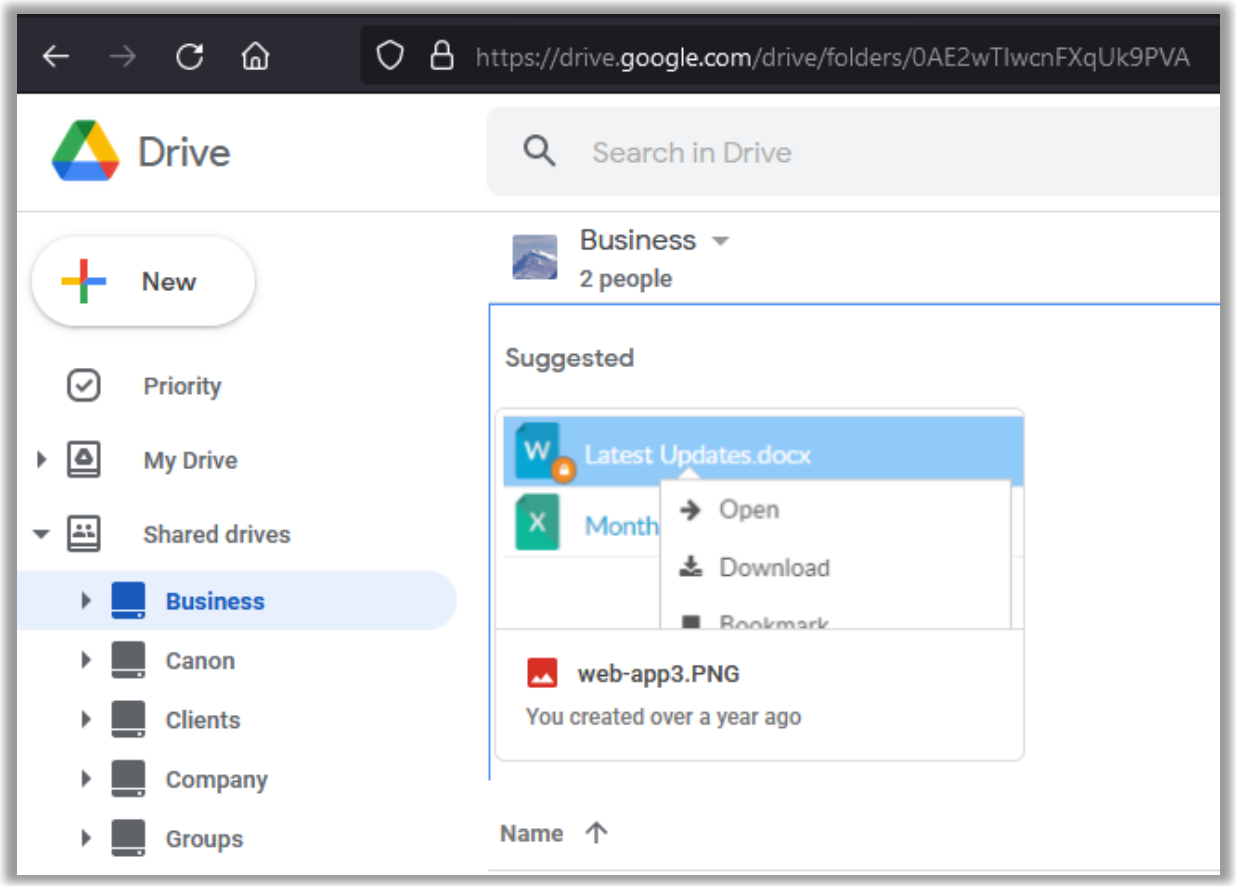
Native Google UI *Foldr*



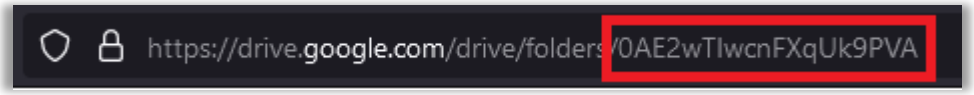
Presenting **a specific Google Team Drive to users:**

1. Follow the standard Google G-Suite configuration steps here (automatic/service accounts) or here (manual account linking)

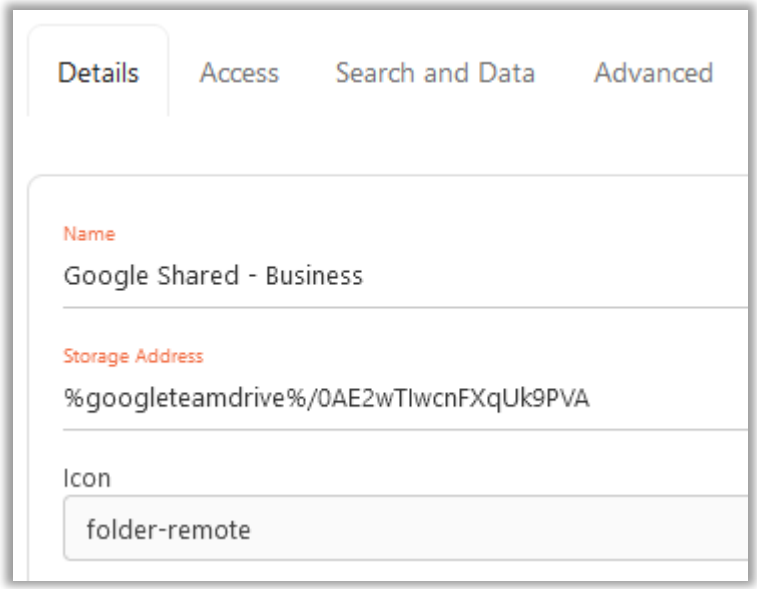
2. Find the Team Drive ID for the Drive that you would like to present to users by logging into Google directly > Drive > Expand Google Team Drive and Select the Team Drive.



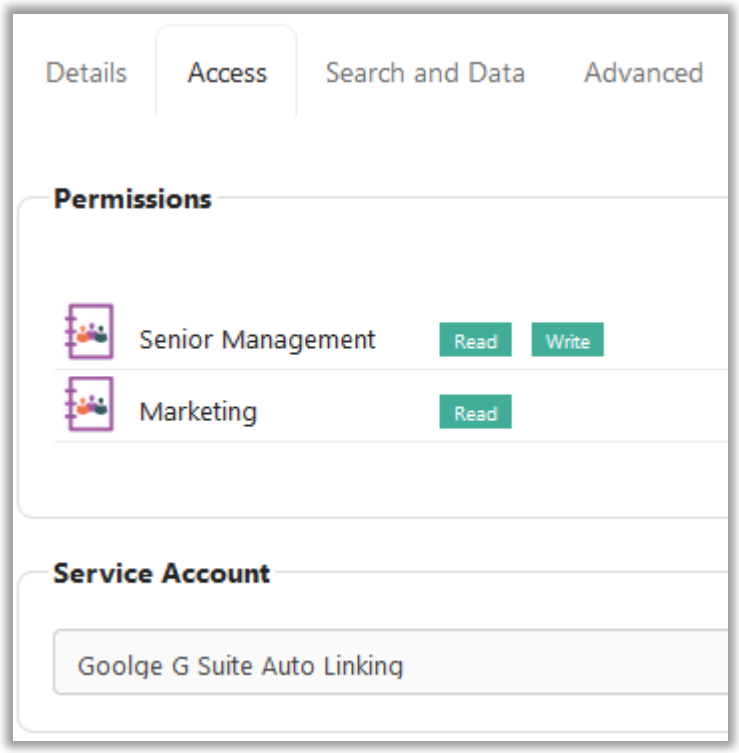
3. Copy the **Shared Drive ID**



4. Add a new share / storage location under ***Foldr Settings*** **>** ***Files & Storage*** using storage address / path of **%googleteamdrive%/*Shared-Drive-ID***



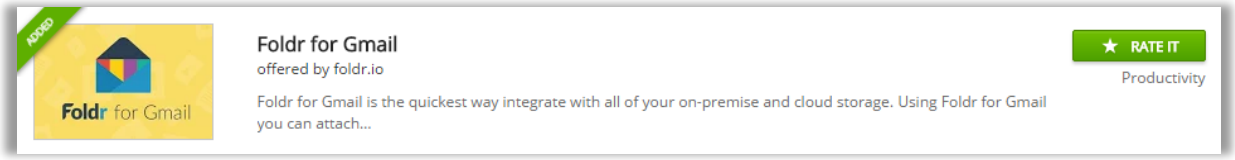
5. Finally, configure other share options / permissions as appropriate. Example below:



If using a Google service account (automated account linking), select this as the service account to be used on the **Access** tab and click **Save**.

Google Chrome Extension (Foldr for Gmail)

If the organisation uses Google Mail for corporate email, a Chrome browser extension is available to allow for quick and easy upload and download of mail attachments to / from the network or cloud storage areas via the Foldr appliance(s)

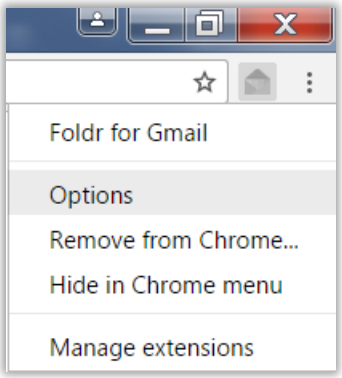


The extension is available here on the Chrome Store.

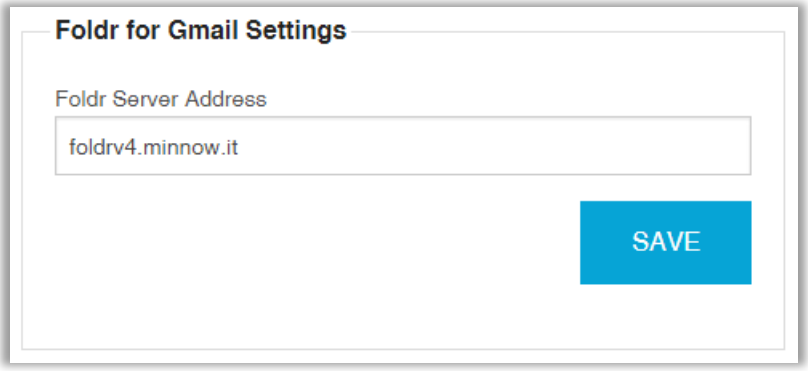
Configuring the Chrome Extension

Once installed you will notice an envelope icon next to the address bar. To start using the extension you must first configure the address of your Foldr system

Select OPTIONS from the pop-up menu

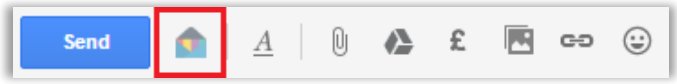


Enter the address of your Foldr appliance and click Save

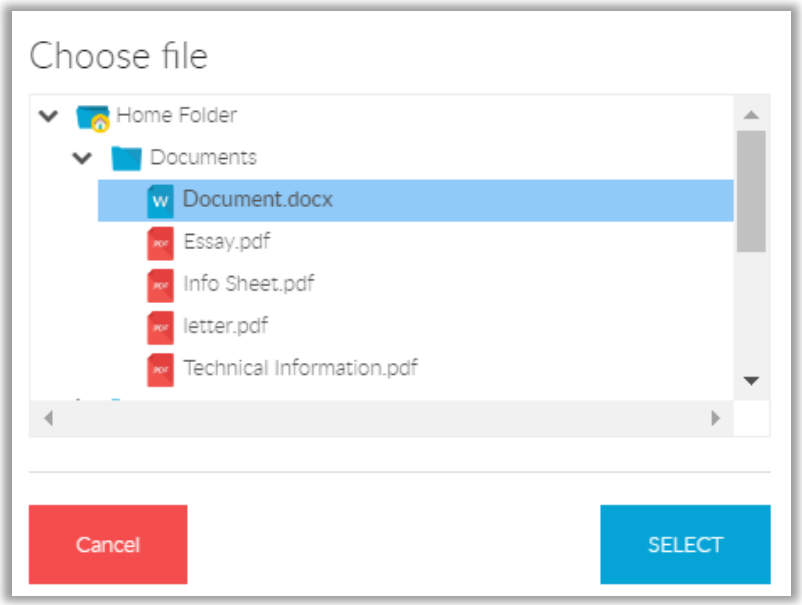


Uploading an attachment from Gmail to Foldr

Now when composing an email in Google Mail (in Chrome) upload attachments by selecting the envelope icon as shown:



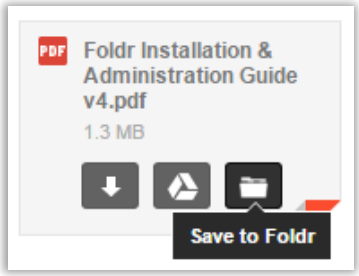
Choose a file to attach and click SELECT



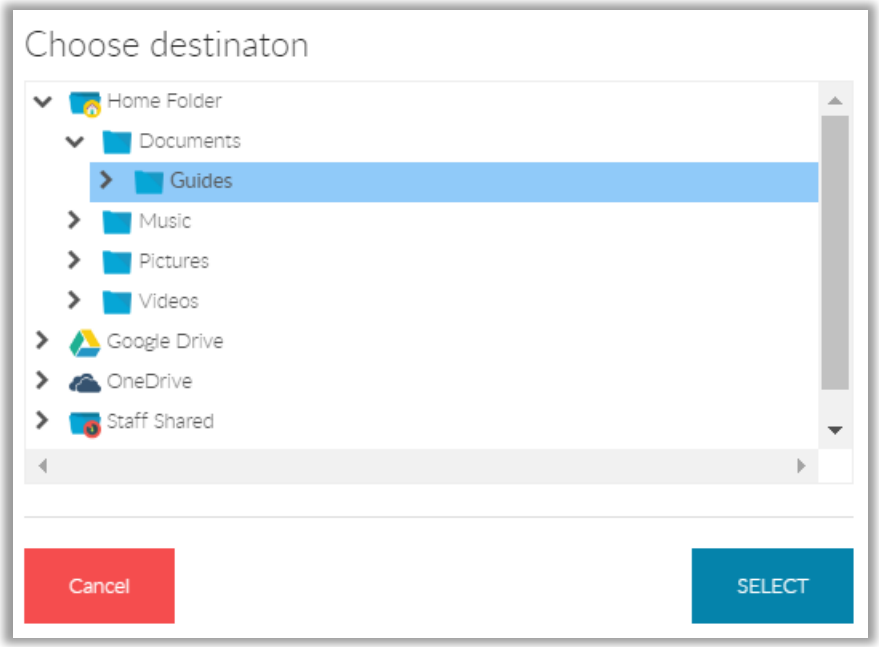
The file will be automatically downloaded from the network share and then attached to the email message.

Downloading an attachment from Gmail to Foldr

Select the envelope icon in the attachment



Choose a destination and click SELECT



The file is now uploaded to the share and folder selected.

Office 365 Integration (OneDrive, SharePoint Online & Teams)

Foldr provides integration with Office 365 to allow OneDrive for Business and SharePoint Online sites to be presented in the Foldr interface. Foldr can also provide access to the document storage locations that are available to users through Office 365 Teams.

Active Directory accounts may be automatically linked to Office 365 accounts and the corresponding OneDrive, Teams and SharePoint sites can be presented in the Foldr interface. Users can alternatively link a Microsoft Office 365 accounts manually. Manual linking will present a pop-up dialog requesting the user's Microsoft account credentials the first time they try to access OneDrive, SharePoint Online or a Teams share in Foldr.

Once an Office 365 account is linked in Foldr, a user can edit any on-premise or cloud hosted Office files in Office Online (web-based versions of Word, Excel & PowerPoint). Collaborative editing is also possible through Office Online with SharePoint Online.

Manual or Automatic Account Linking?

The administrator should decide which method of account linking is to be used in the deployment as there are benefits to both methods. Automated account linking uses a service account to provide immediate access to user's OneDrive and SharePoint sites with no additional effort from the user. However, the connection always uses service account credentials, rather than those of the individual user. Only the manual account linking method can respect the granular Office 365 user's permissions for sites and nested sub-folders.

Essentially, if only OneDrive is being presented to users through Foldr, then automated linking would provide a smoother user experience and remove the need to enter the Office 365 credentials the first time it was accessed. If you intend you present SharePoint sites, then it would be recommended to use manual linking, unless the security permissions in place in Office 365 are flat across the organisation, with no granular access permissions.

Regardless of the account linking method used, the administrator can still control visibility of all storage locations (OneDrive, SharePoint libraries, Teams) using permissions in ***Foldr Settings > Files & Storage***, specifying read/write access by user or group.

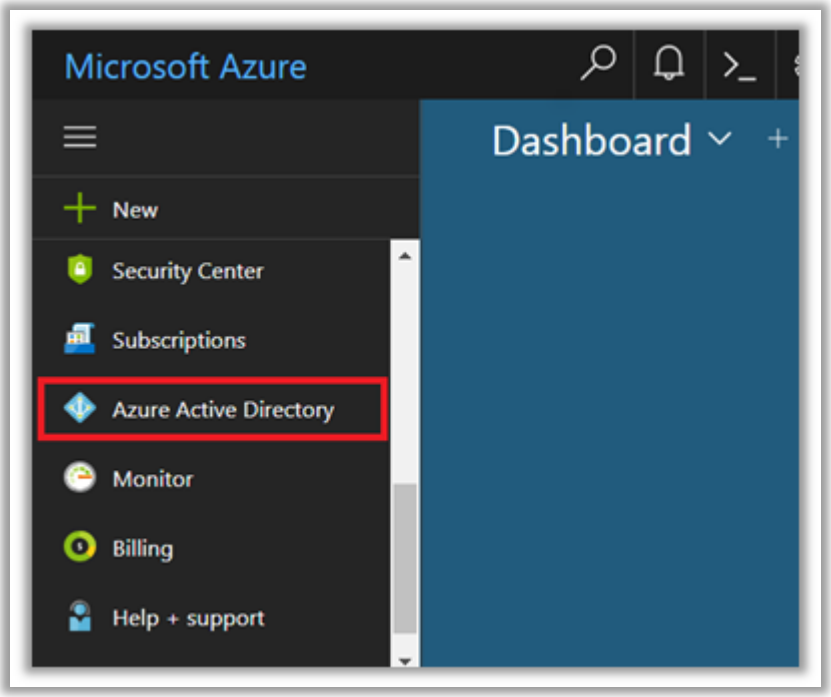
Finally, it should be noted that if MANUAL linking is being used, the Foldr system must be accessible externally and a signed SSL certificate installed.

Office 365 Integration 1 – Manual Account Linking

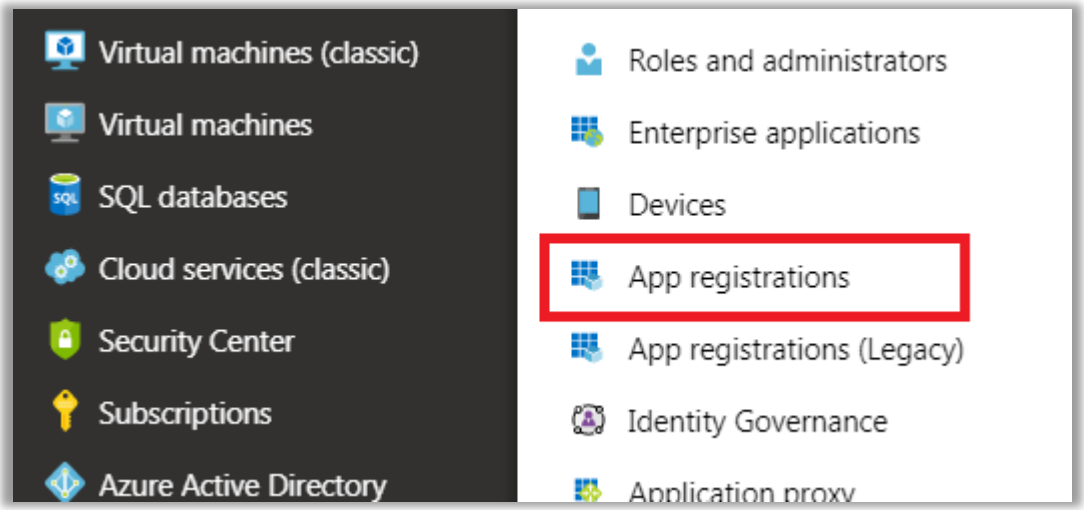
Creating the App Registration in Azure

1. Log into the Microsoft Azure Portal at https://portal.azure.com using your administrative Microsoft account.

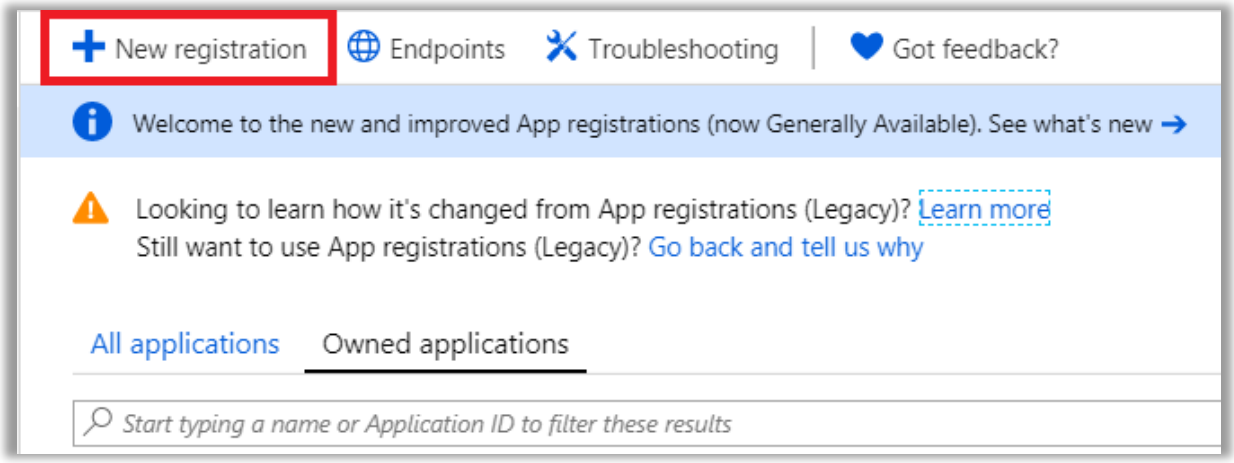
2. Select Azure Active Directory from the left-hand panel.



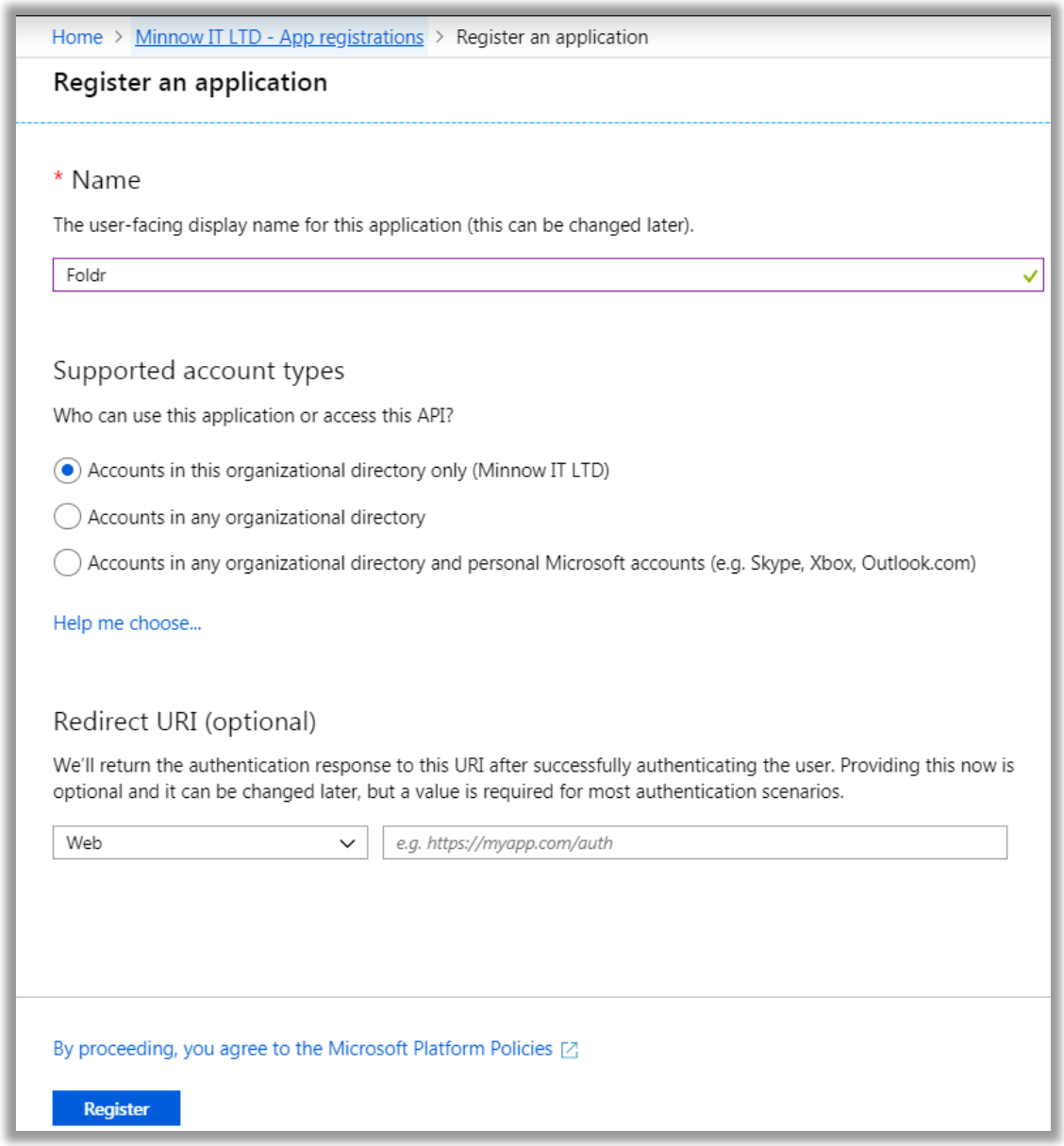
3. Click **App Registrations.**



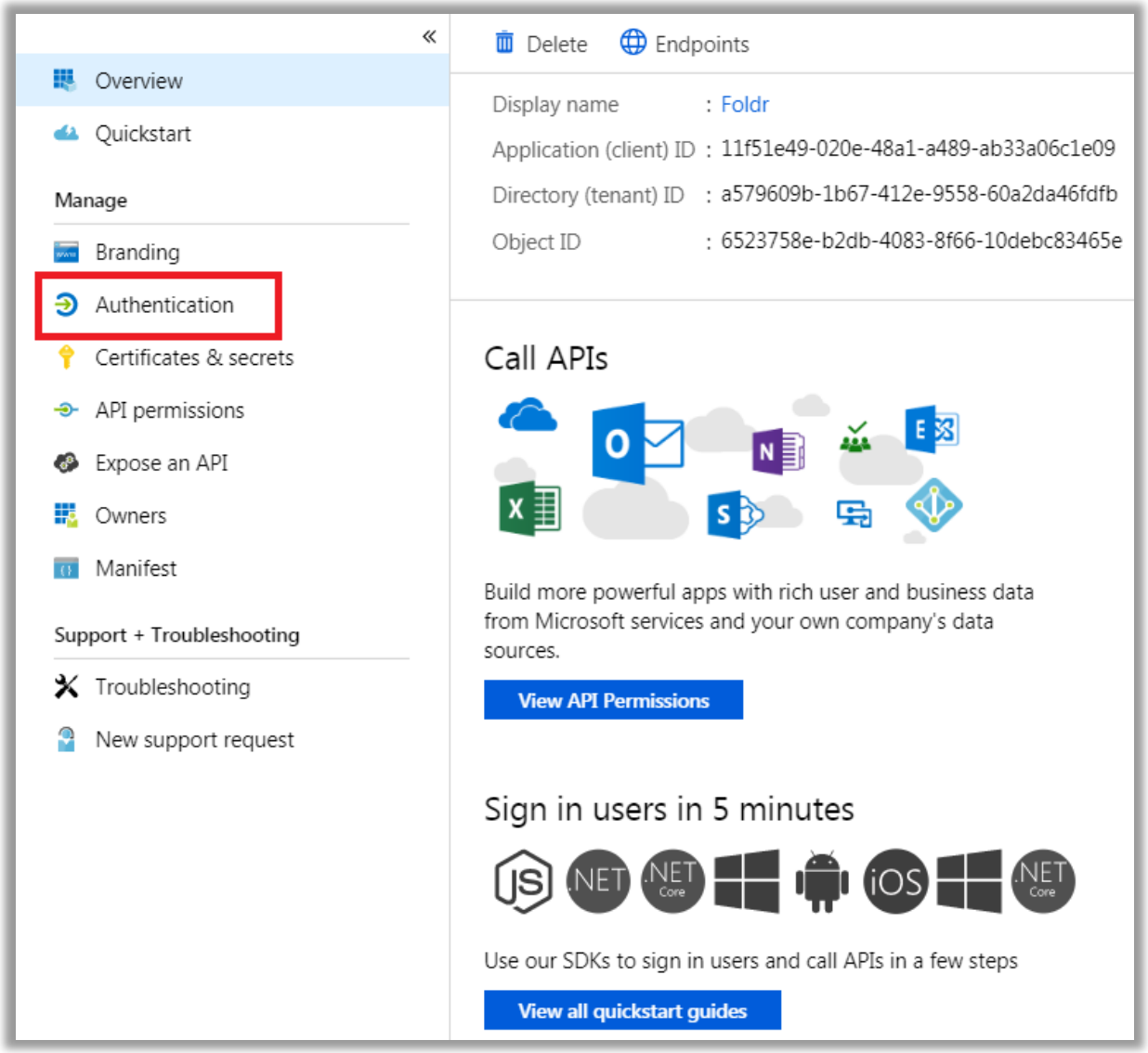
4. Click **New registration.**



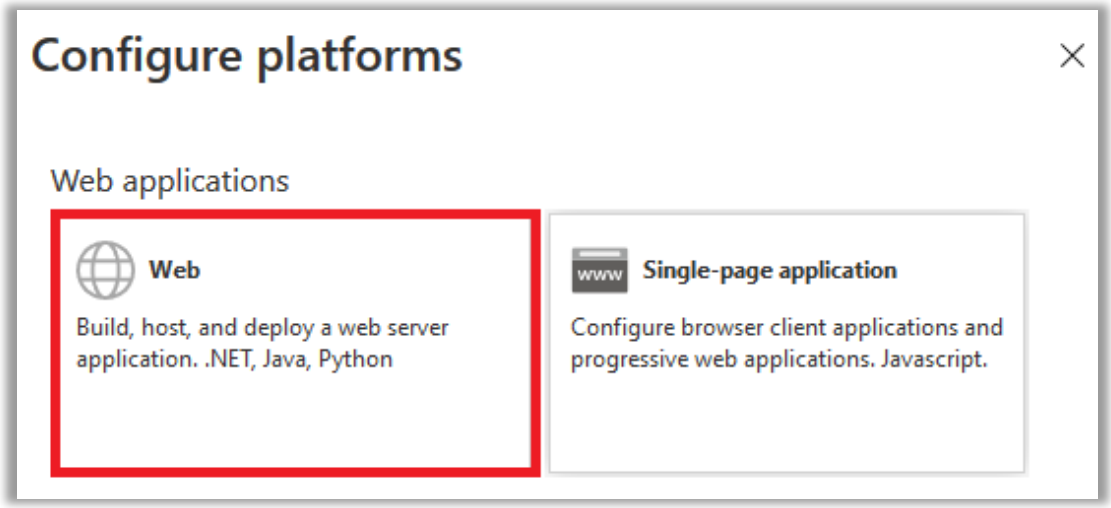
5. Give the application a suitable name, and click **REGISTER.** In most cases the supported account type can be left as default (top radio button)



6. The app summary / configuration screen will be show. Click **Authentication.**



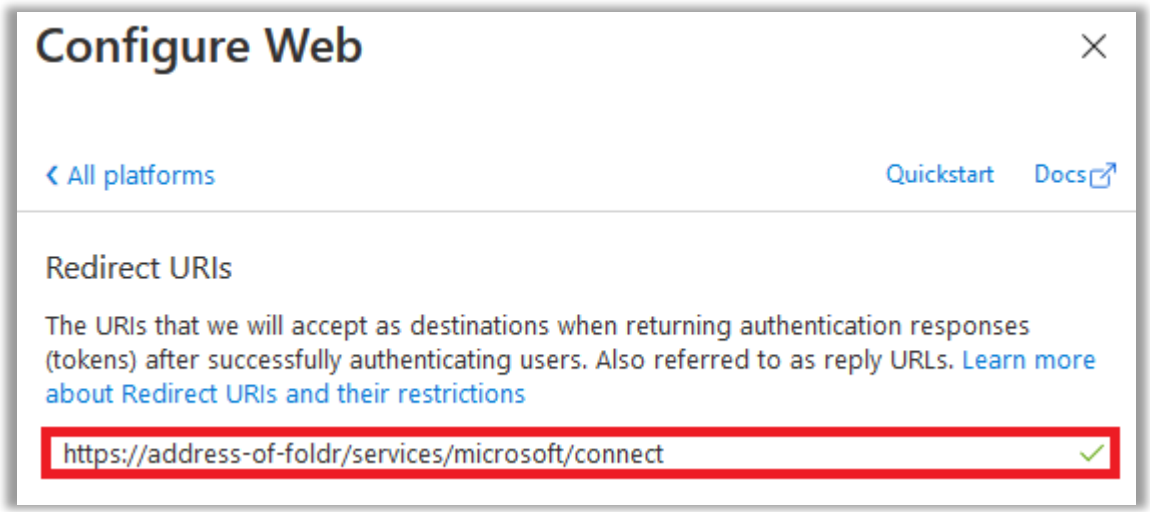
7. Click **+ Add a platform** and select **Web**.



Add a Redirect URI (Reply URL) using the format:

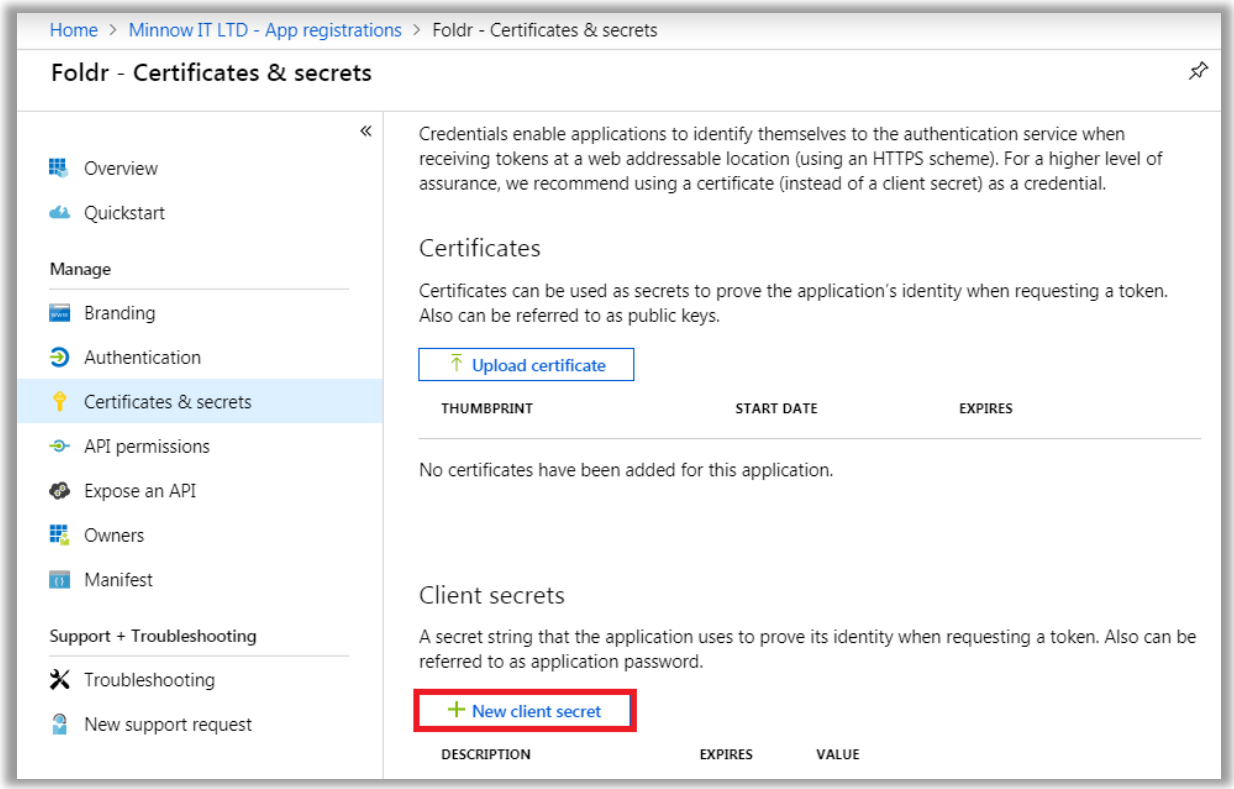
https://address-of-foldr/services/microsoft/connect

The Redirect URI / Reply URL must be the **public address** of the Foldr installation appended with */services/microsoft/connect* as shown in the example below

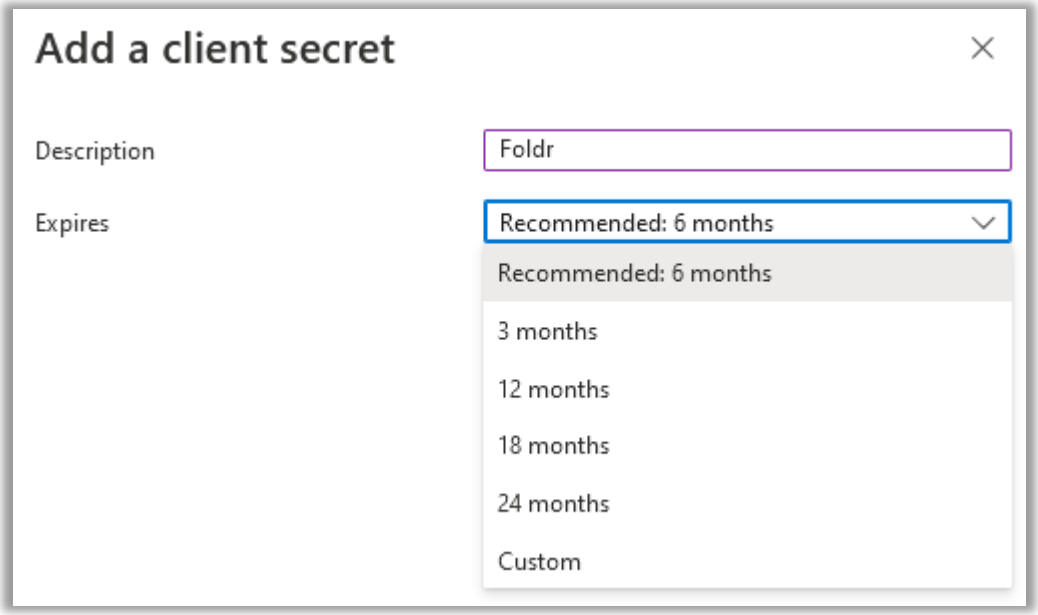


8. Click **CONFIGURE.**

9. Click Certificates & secrets > **New client secret.**

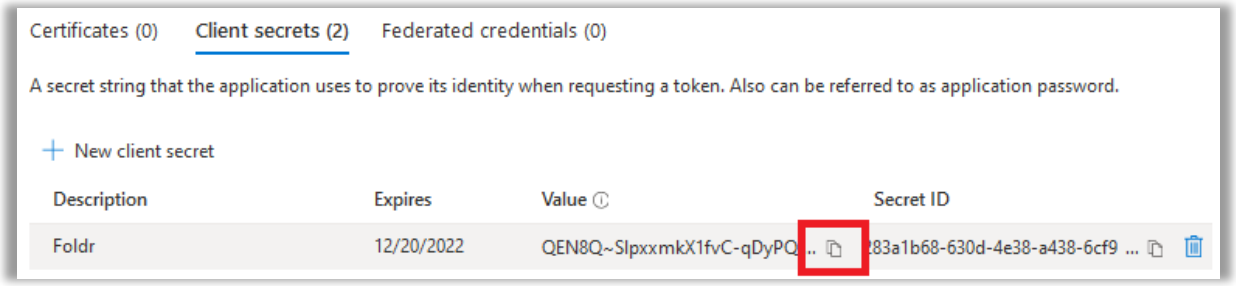


10. Enter a description, select a suitable expiration, and finally click **ADD.**

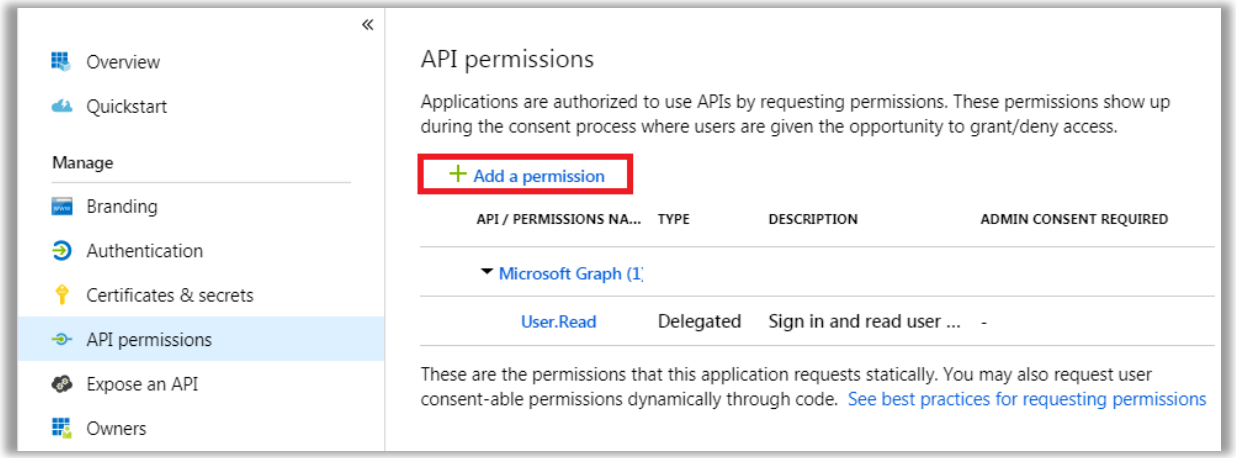


11. The new client secret will be displayed.

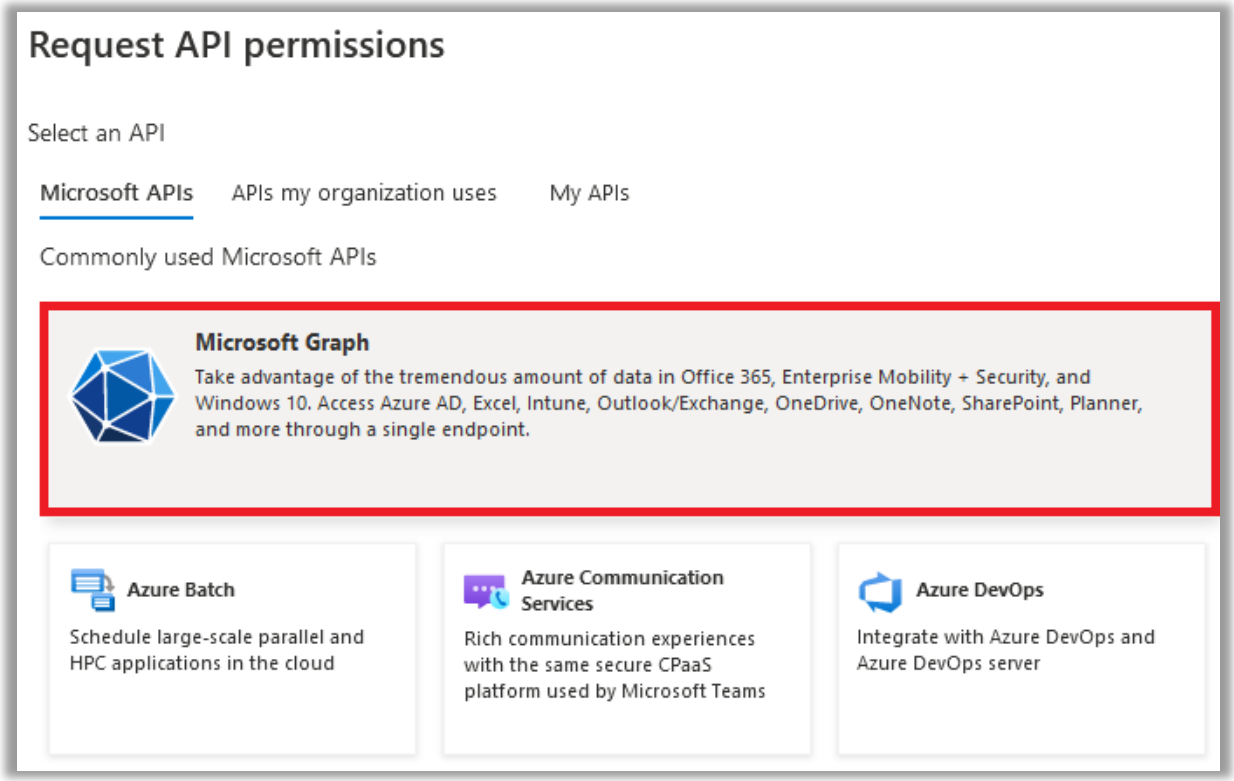
IMPORTANT – You should take a copy of the key at this point as you cannot retrieve it again later, however new keys can be generated later, if required.



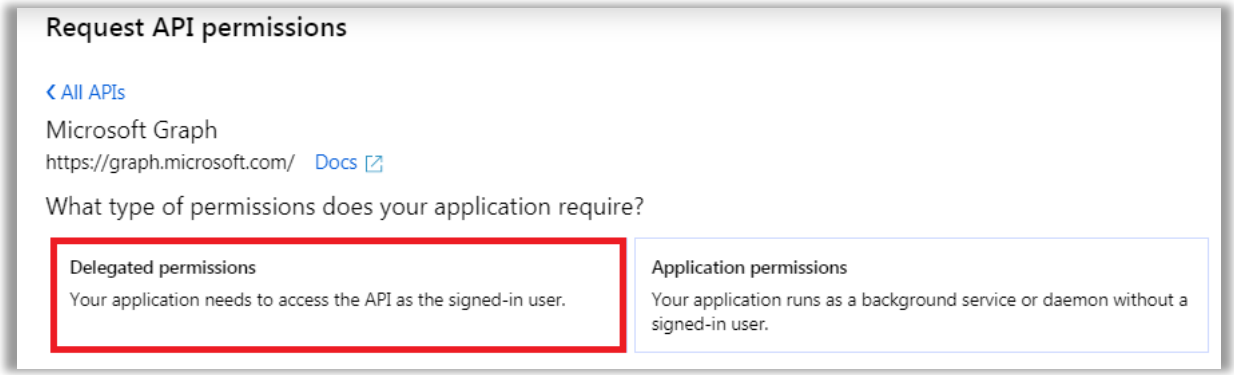
12. Click API Permissions > **Add a permission**



13. Select **Microsoft Graph**

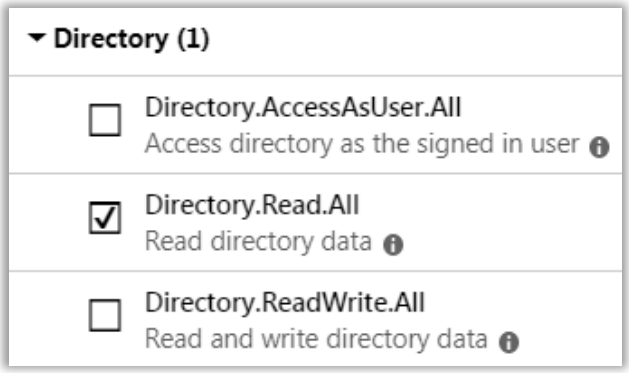


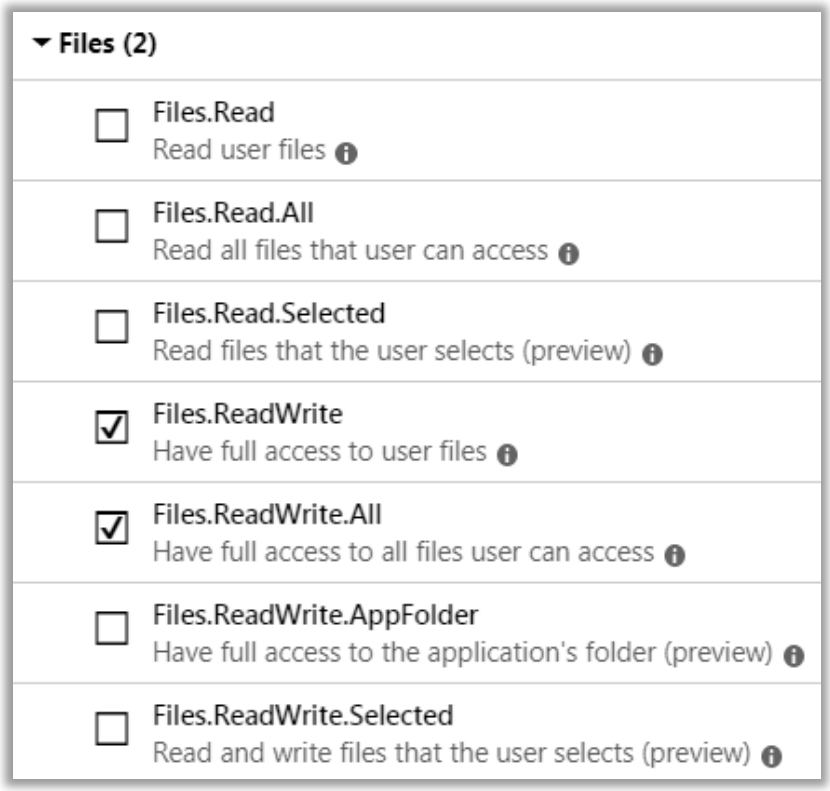
14. Click **Delegated Permissions.**



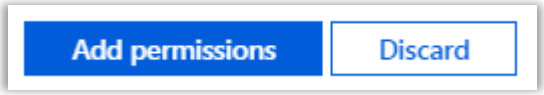
15. Select the following permissions from the Directory and Files sections:

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

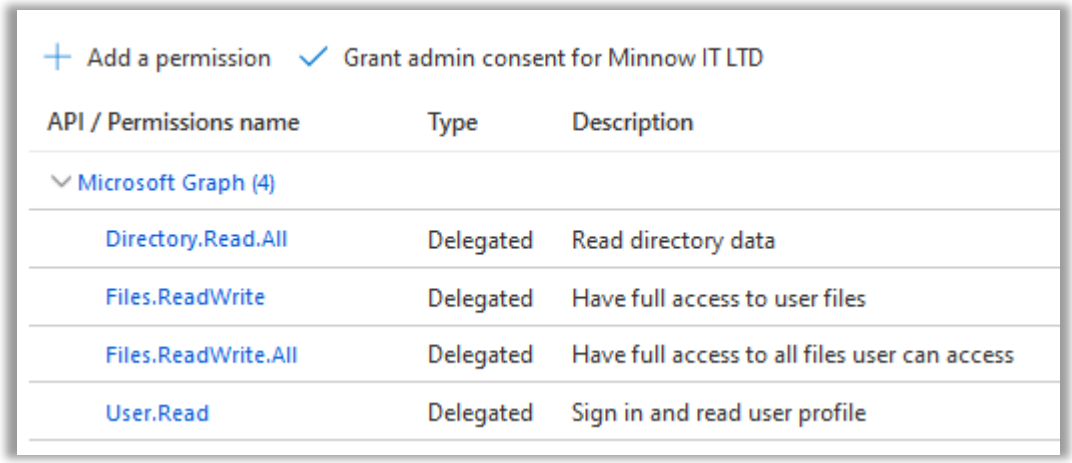




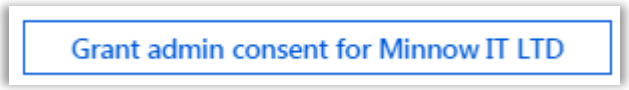
16. Click **Add Permissions** at the bottom of the screen.



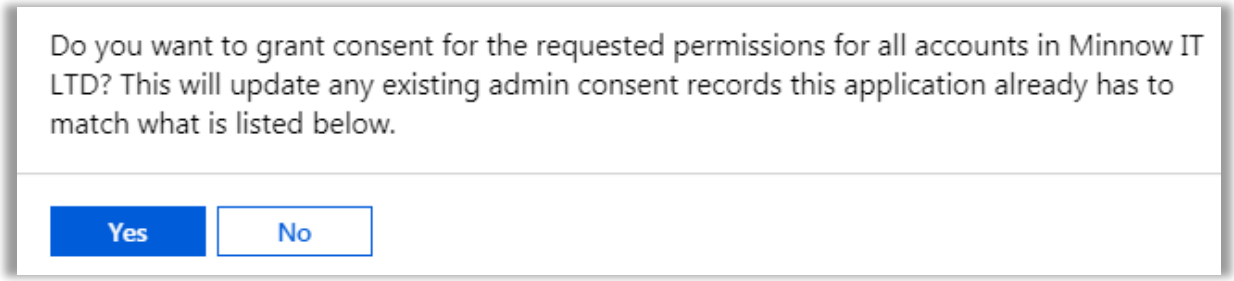
17. The permission summary will now be shown showing the new delegated permissions.



18. Click the **GRANT ADMIN CONSENT** button.

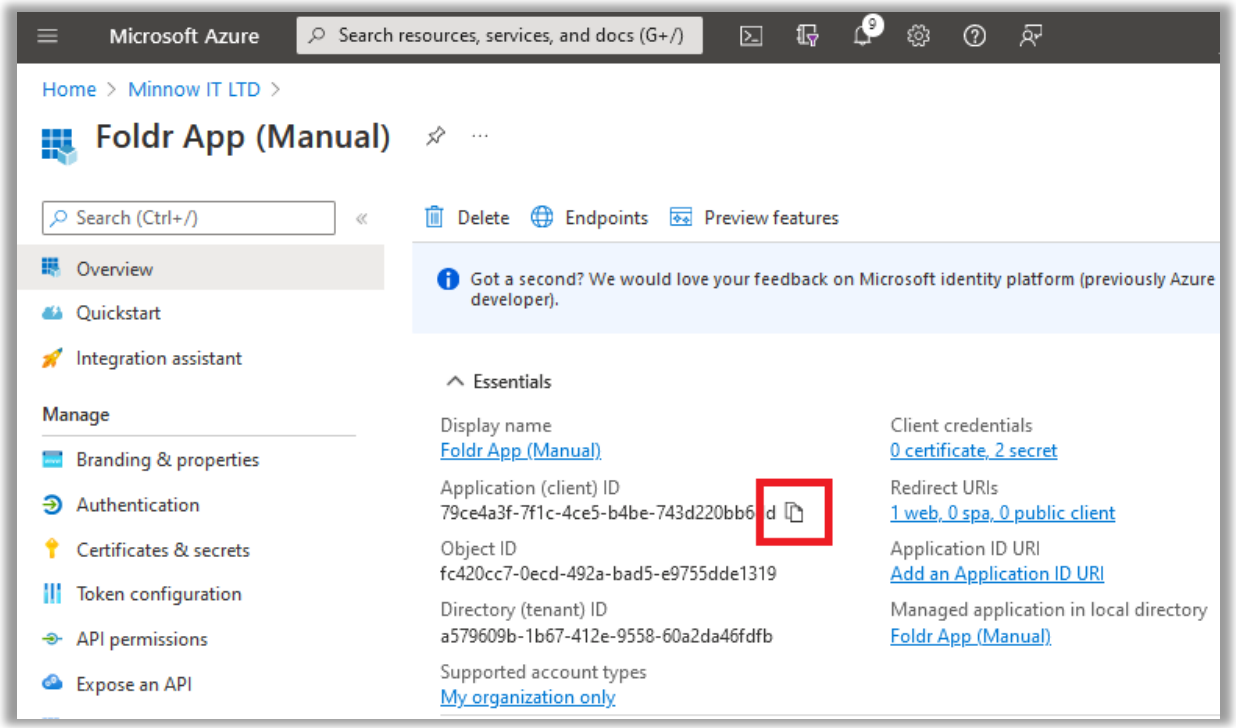


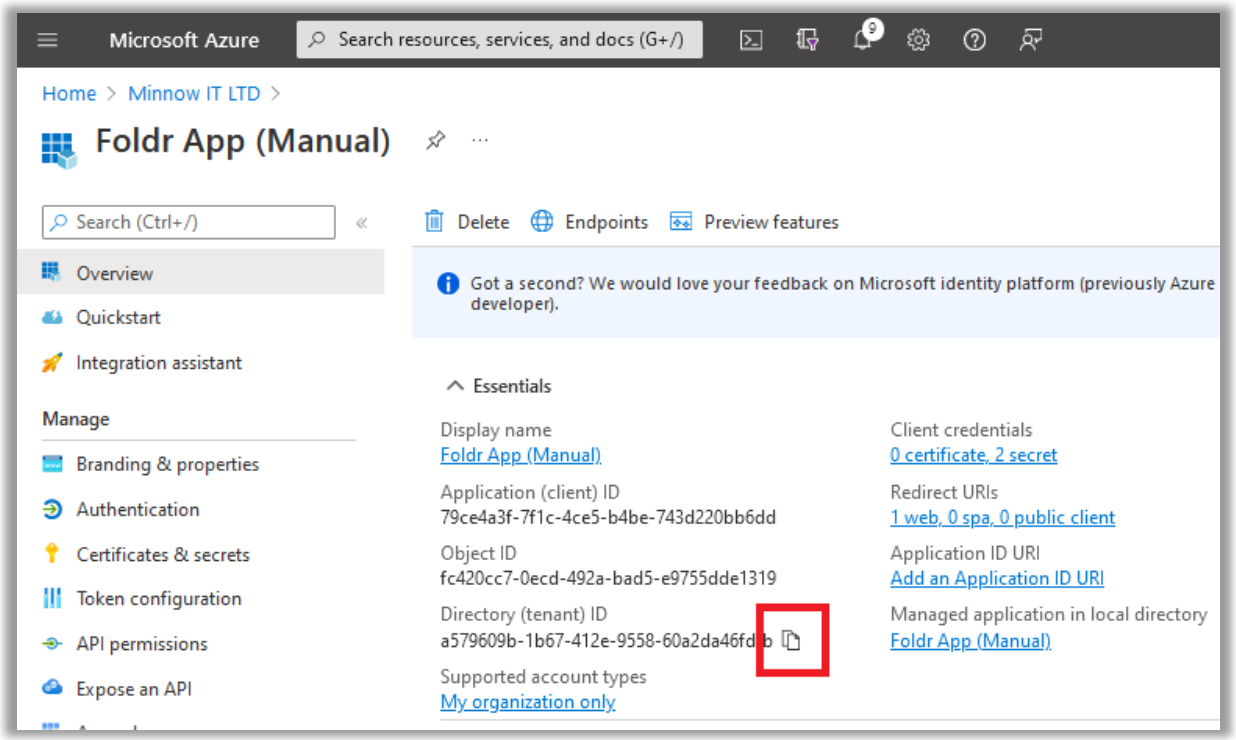
19. Click **Yes** on the confirmation prompt.



20. A success message will then be shown

21. Click on Overview and take a copy of the **Application (client) ID** and **Directory (tenant) ID**. These will be required later when enabling the integration on the Foldr appliance.





Enabling the Office 365 integration in Foldr

The Office 365 integration should now be enabled and the Application ID, Client secret and Directory ID, should be pasted into the relevant the fields within:

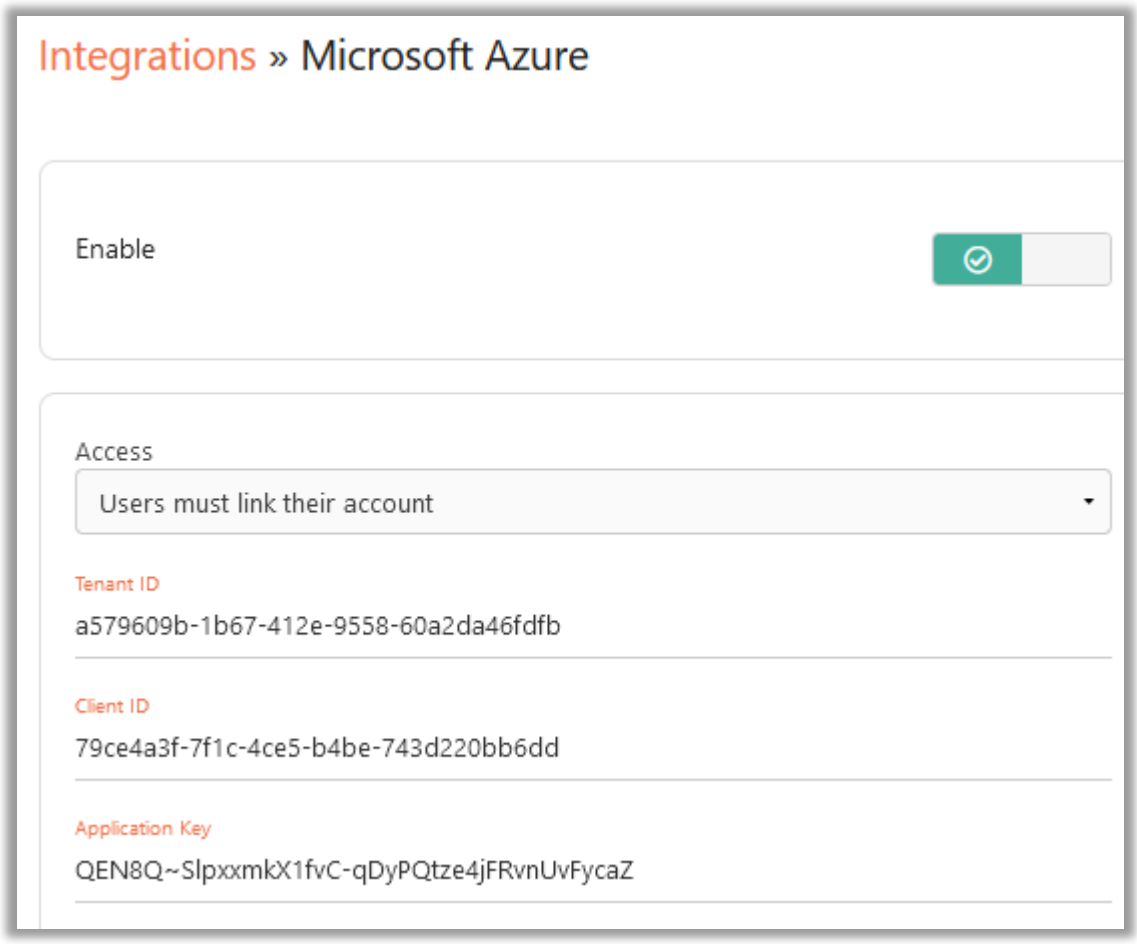
Foldr Settings > Integrations > Microsoft Azure

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

Application Key = ***Client secret*** in Azure

Tenant ID = ***Directory (tenant) ID*** in Azure

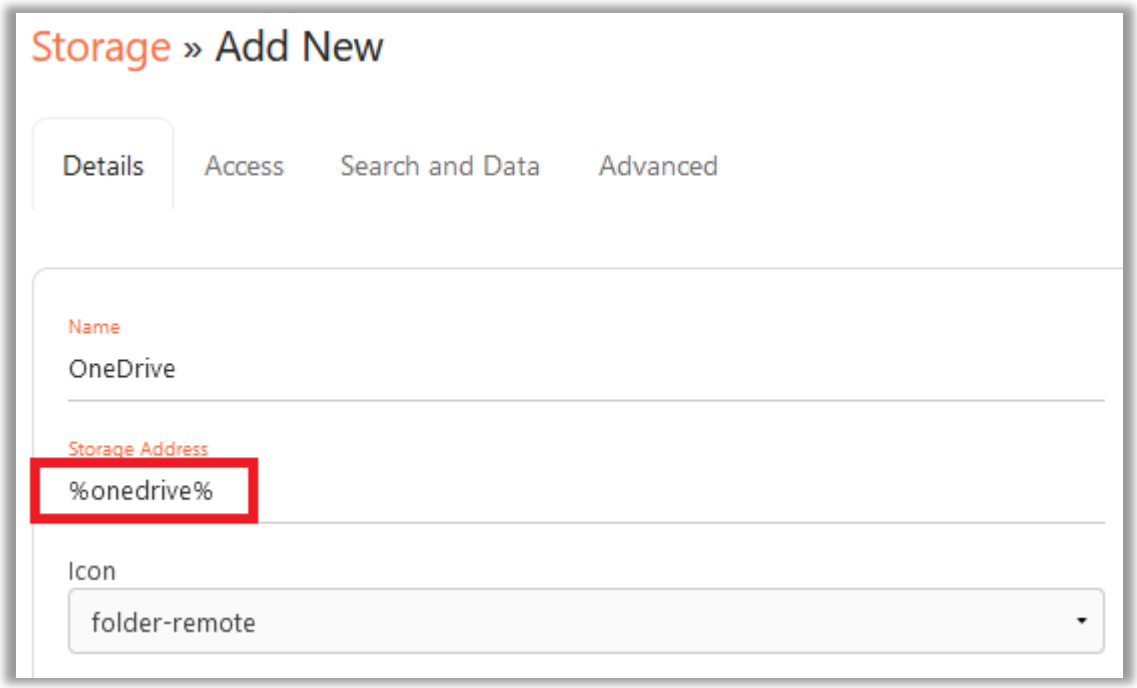
Example settings shown below for Office 365 Manual Account linking.



Finally, Click **SAVE CHANGES**.

Adding the Storage Item for OneDrive

A new storage item should be created for OneDrive under ***Foldr Settings > Files & Storage*** using the Share URI **%onedrive%**



Select a suitable icon and click **SAVE.**

Presenting SharePoint sites to Users

A new share should be created for each SharePoint site under ***Foldr Settings > Files & Storage*** using the Share URI:

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

Note if **/sites/** is not in the SharePoint URL when viewed through O365 directly, it can be removed from the Share URI

To present the organisation's root/default SharePoint site, using the Share URI **%sharepoint%**

Presenting Teams storage to Users

A new share can be created for Teams under ***Foldr Settings > Files & Storage*** using the Share URI **%teams%**

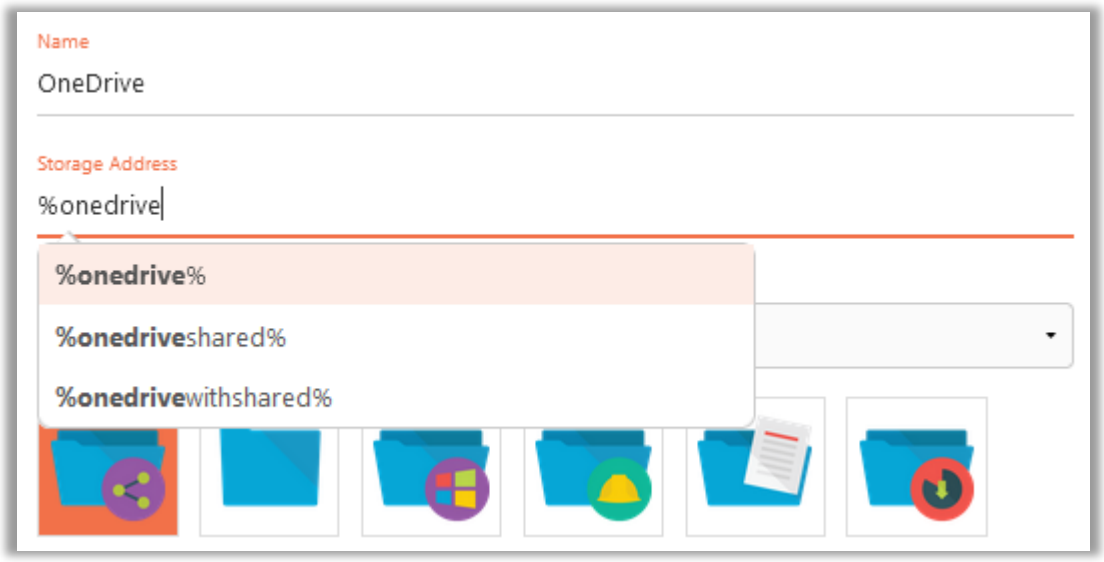
Presenting Shared Office 365 items to Users

Foldr can present items that have been shared with them using the native sharing tools in Office 365.

Shared items can be displayed in a dedicated share/storage item within My Files or alternatively a 'Shared with Me' directory can be displayed inside a user's OneDrive and all shared items will be available inside.

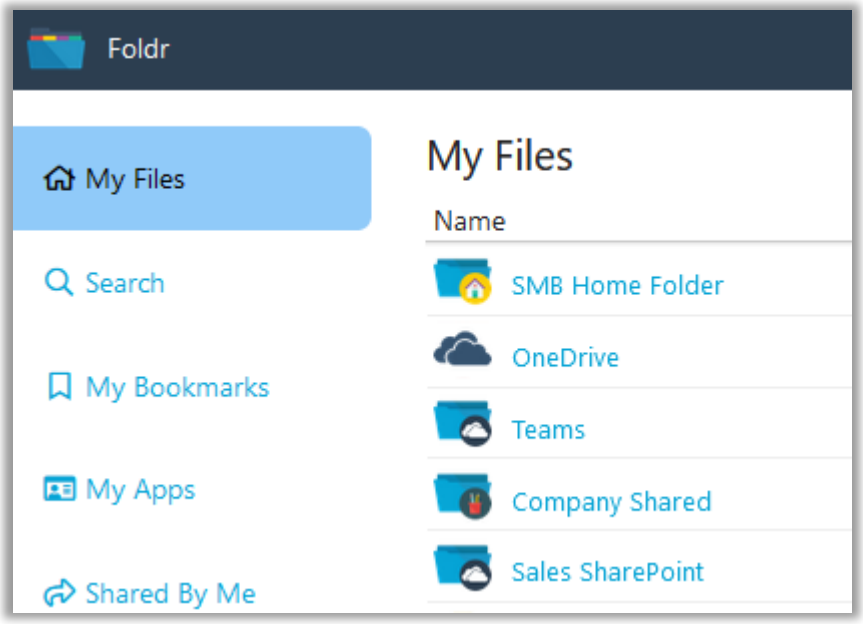
To create a dedicated share for Office 365 shared items, create a new share within ***Foldr Settings > Files & Storage*** and set the Share URI to **%onedriveshared%**

To present a user's OneDrive with a 'Shared with Me' folder in the root of OneDrive, create a share and set the Share URI to **%onedrivewithshared%**

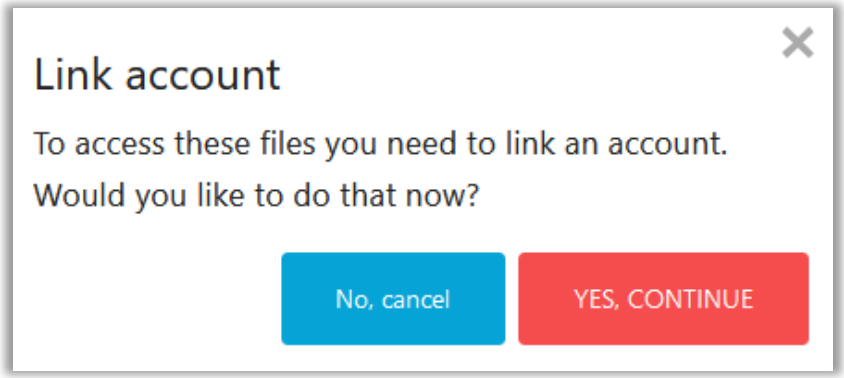


User Experience - Linking the Office 365 account (Web app)

OneDrive, SharePoint & Teams storage icons will be visible to users immediately in the web app before they link their account. Once they click one of the Office 365 storage locations, they will be prompted to link their account and enter their Office 365 credentials.

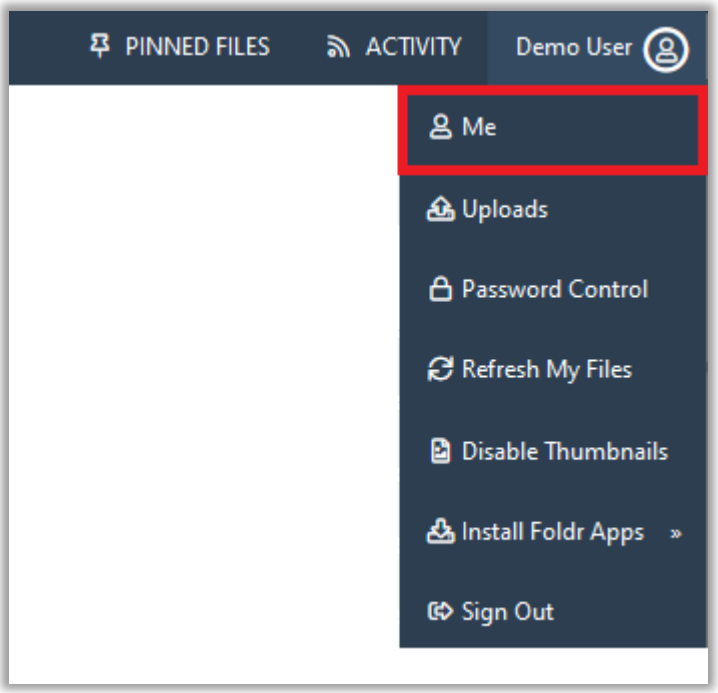


i.e. The user clicks the OneDrive item and is prompted as below to authenticate with Office 365 in a new tab.

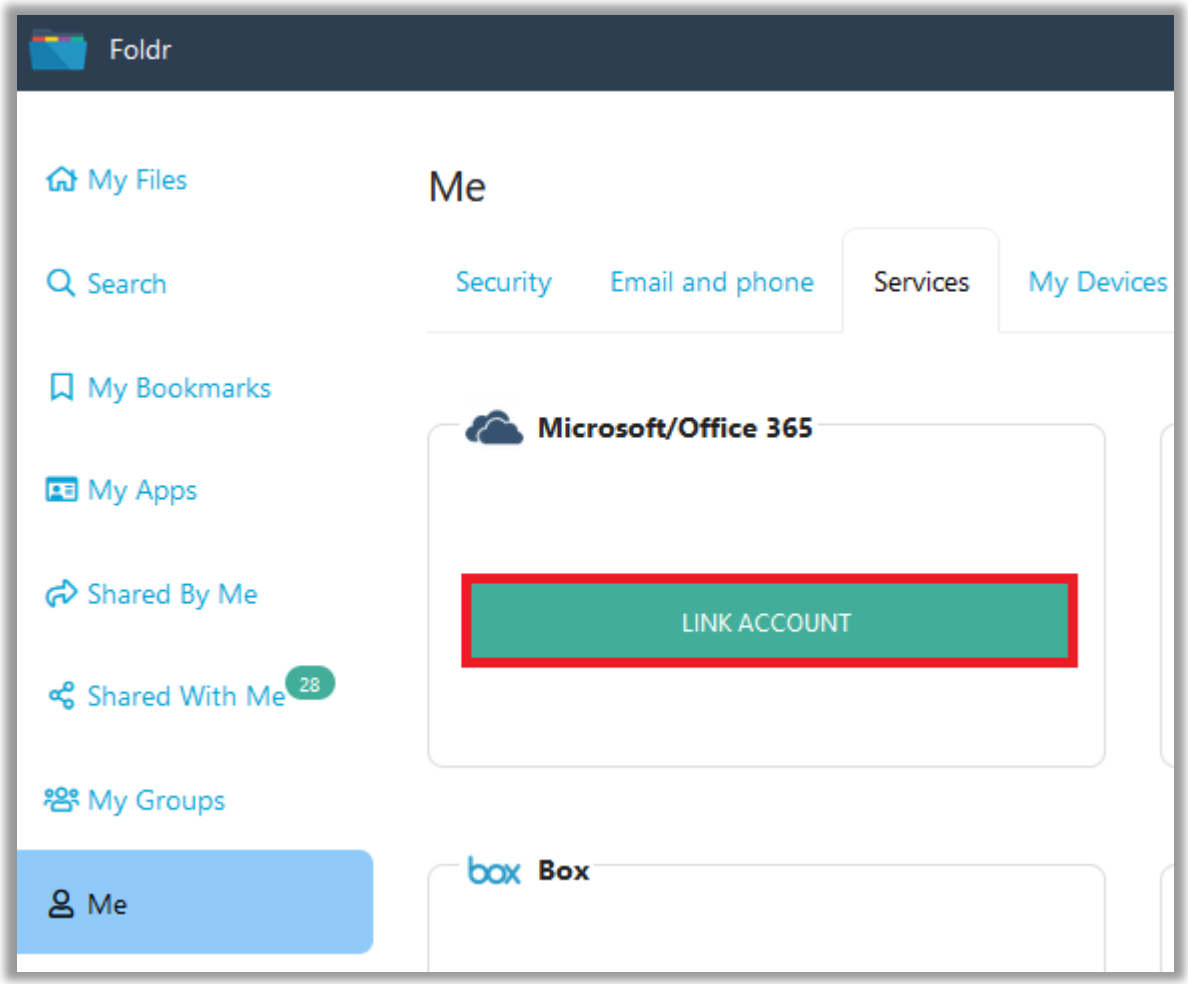


The account is then linked, and OneDrive storage should be browsable in any of the Foldr apps and all Office documents can be edited in Office Online.

Alternatively, a user can link and unlink their Microsoft accounts when logged into the Foldr web app using the menu item '**Me' > Services**. This is available top right menu of the interface or the left-hand panel.



Click **Services > OneDrive/Office 365**



Click '**LINK ACCOUNT**' and you will be prompted to sign in at Microsoft Online.

The account is then linked, and OneDrive storage should be available in any of the Foldr apps and Office documents can be edited in Office Online from on-premise shares or OneDrive / SharePoint. Users can unlink their Microsoft Account at any time from the Services menu shown above.

The integration for Office 365 (manual linking) is now complete.

Office 365 Integration 2 – Automatic Office 365 Account Linking

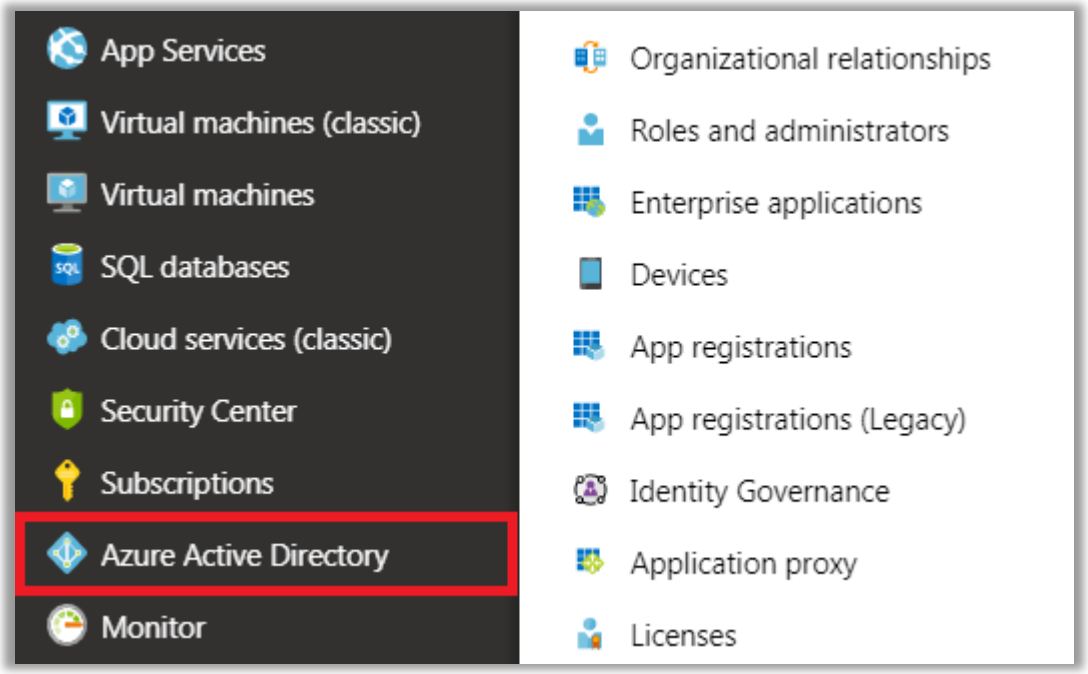
The steps involved for automatic account linking are very similar to manual linking, but you are required to enter the application ID, client secret and tenant ID to create a Microsoft service account on the Foldr appliance. The service account also needs to be selected on any Office 365 storage items in ***Foldr Settings > Files & Storage***.

Automatic account linking is generally recommended when only OneDrive is being presented to users in Foldr (SharePoint sites and Teams are not being presented via Foldr) – It is possible to present all Office 365 locations using automatic account linking, but the user in Foldr will not receive their 'own' permissions in 365, but instead will be accessing all data using the permissions that apply to the **service account**. For this reason, Manual linking (integration method 1) is recommended to access SharePoint or Teams via Foldr.

Creating the App Registration in Azure

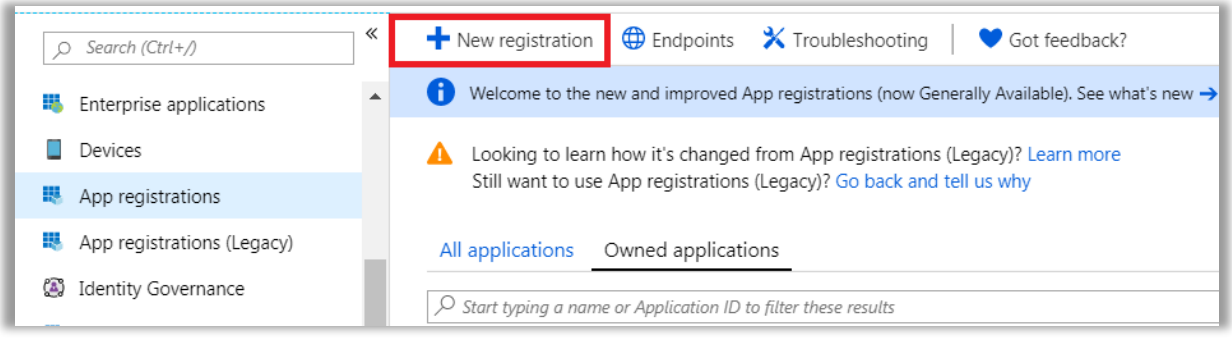
1. Log into the Microsoft Azure Portal at https://portal.azure.com using your administrative Microsoft account.

2. Select Azure Active Directory from the left-hand panel.

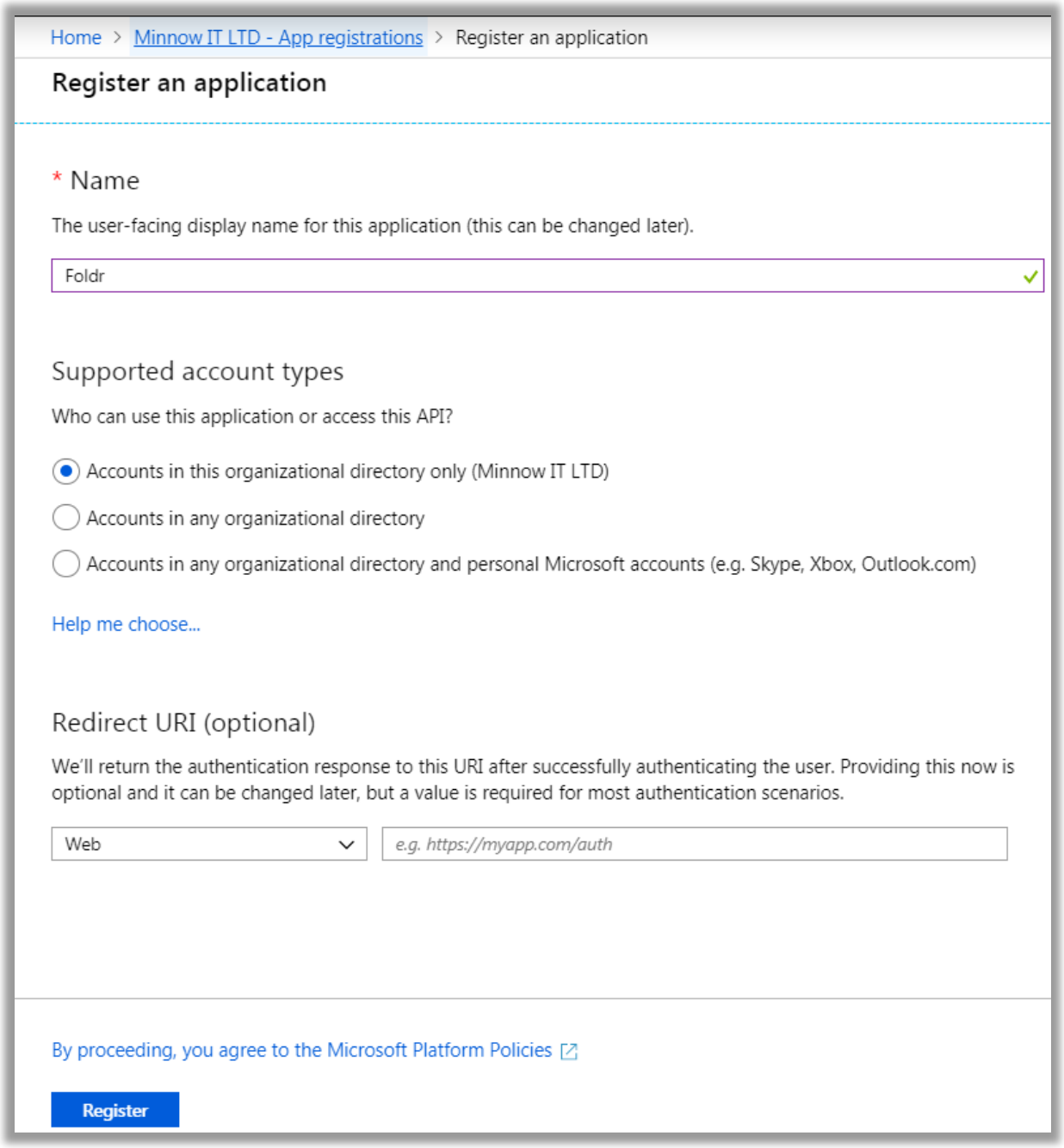


3. Click **Application Registrations > New Application**

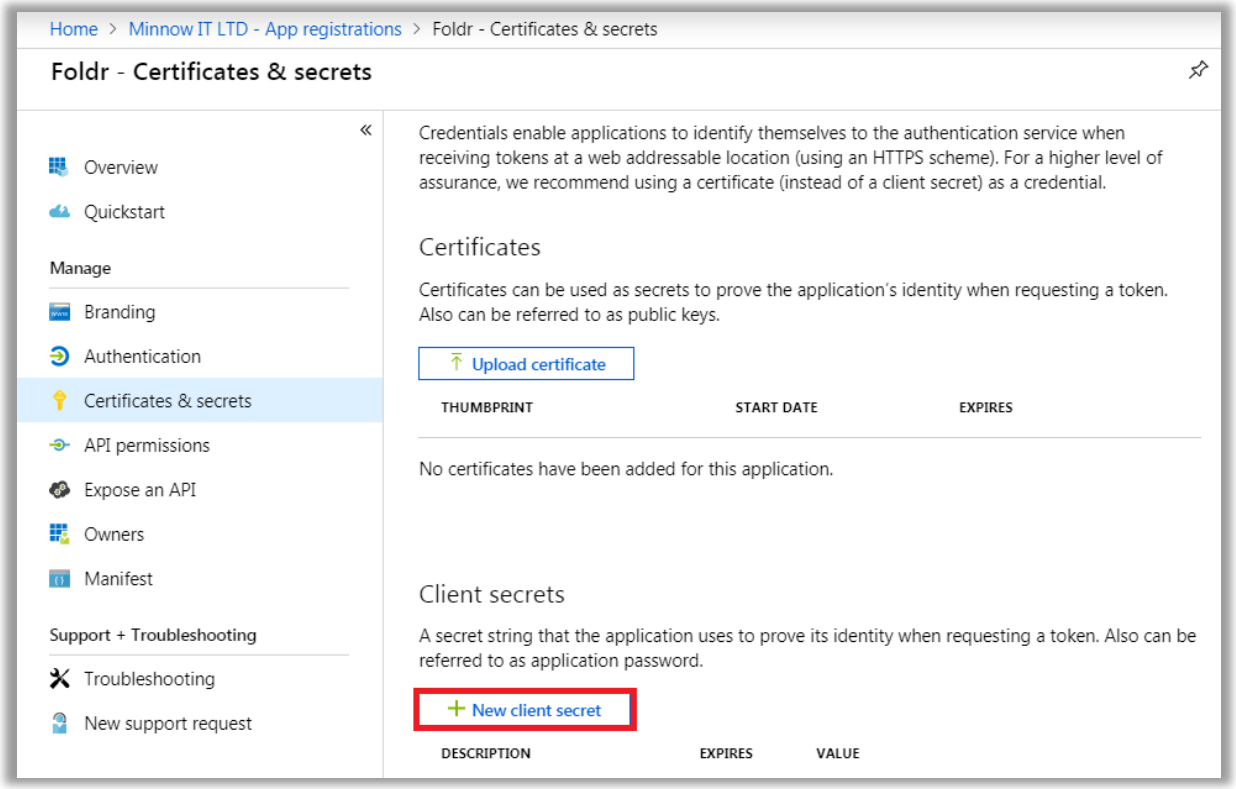
w



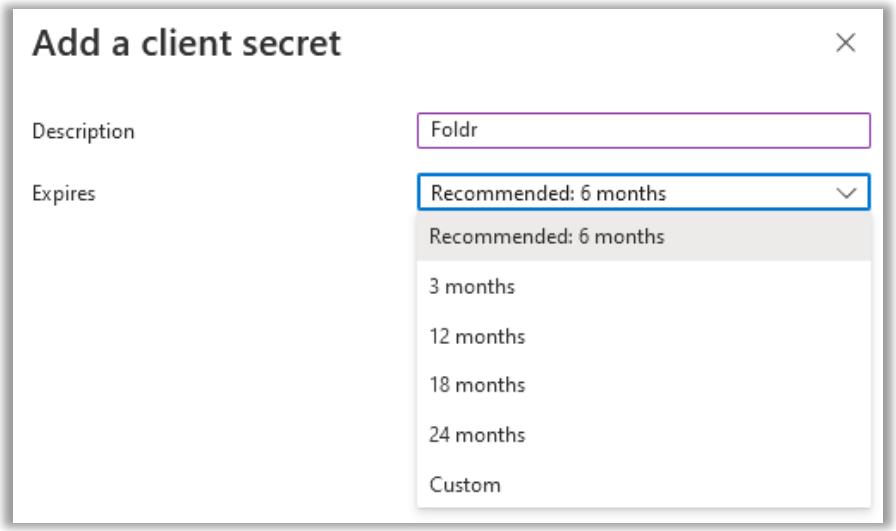
4. Give the application a suitable name, and click **REGISTER.** In most cases the supported account type can be left as default (top radio button)



5. Click Certificates & secrets > **New client secret.**

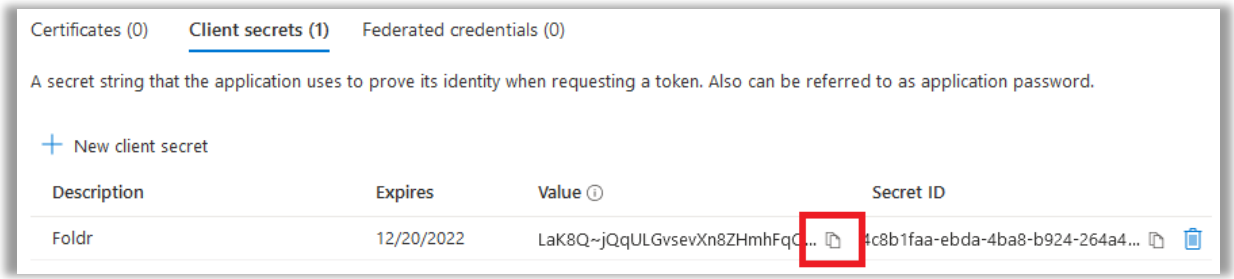


6. Enter a description, select a suitable expiration lifetime, and finally click **ADD.** Note a long client secret lifetime is recommended, otherwise the Foldr integration will stop working.

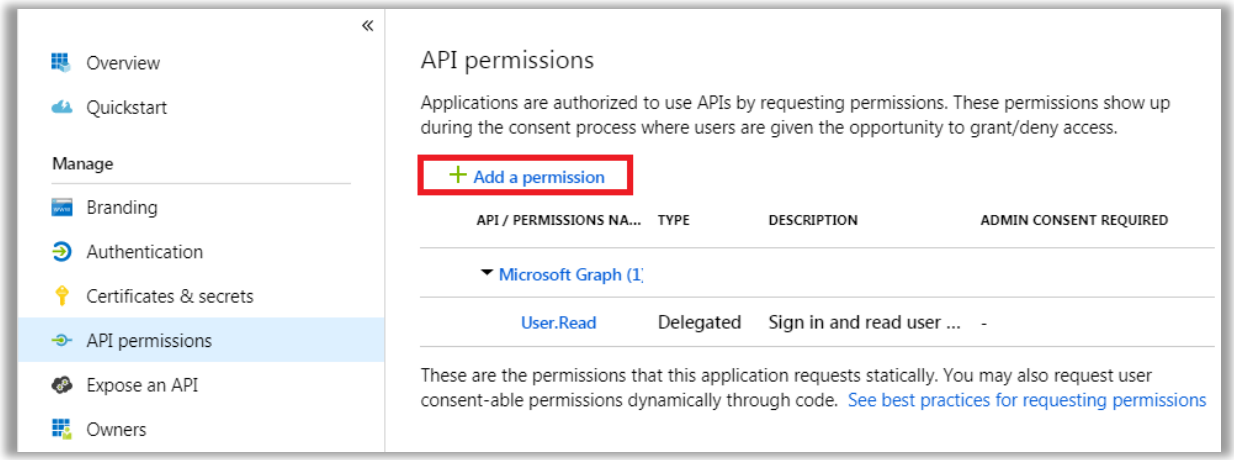


7. The new client secret will be displayed.

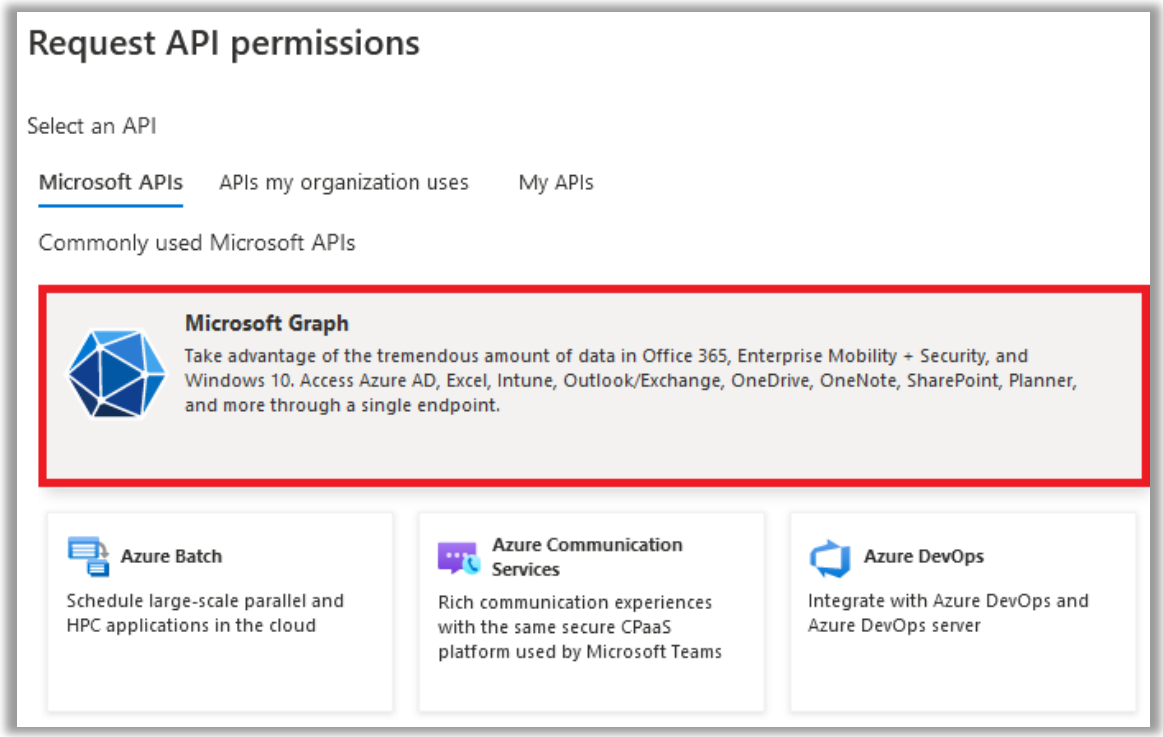
IMPORTANT – You should take a copy of the key at this point as you cannot retrieve it again later, however new keys can be generated later, if required.



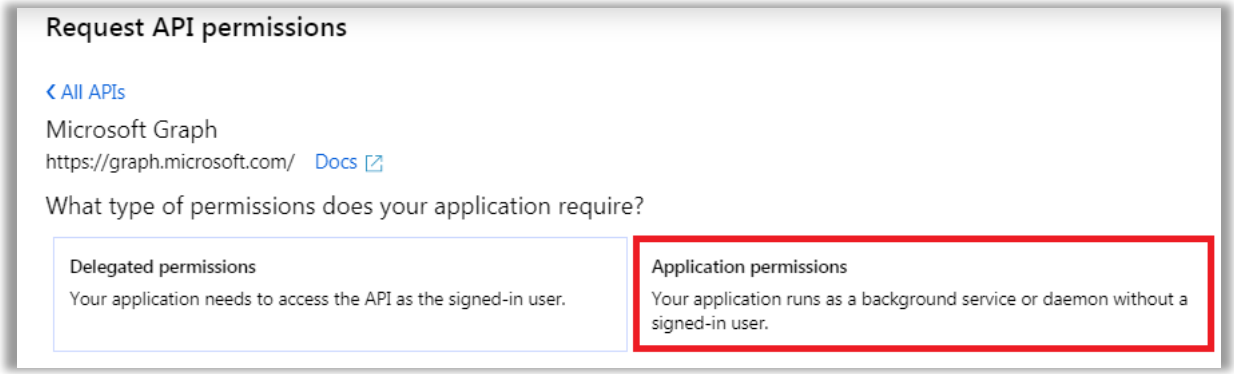
8. Click API Permissions > **Add a permission**



9. Select **Microsoft Graph**

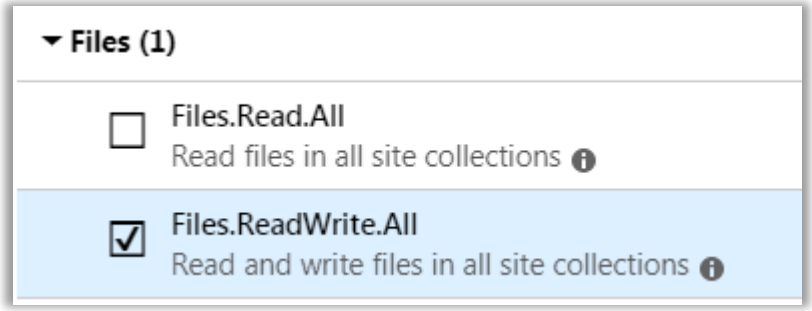


10. Click **Application Permissions.**



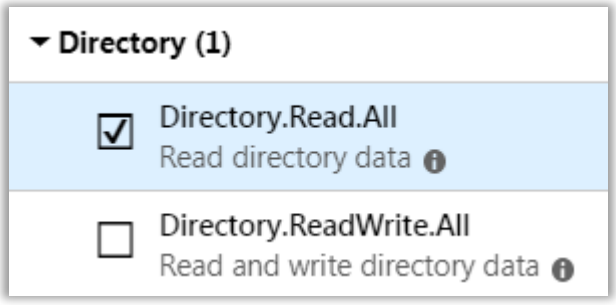
11. Select the following permission from the Files section:

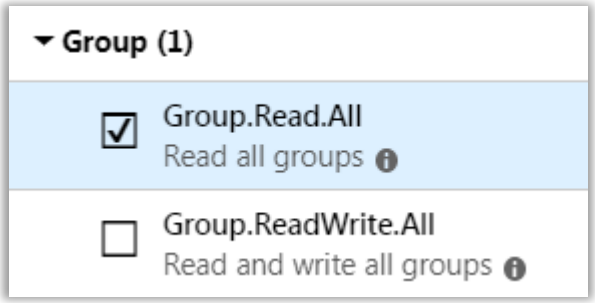
Files.ReadWrite.All



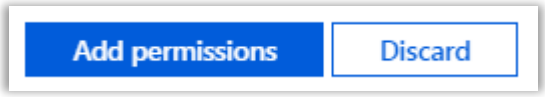
If presenting Teams storage to users, also enable the following additional permissions from the Group and Directory sections:

Directory.Read.All
Group.Read.All

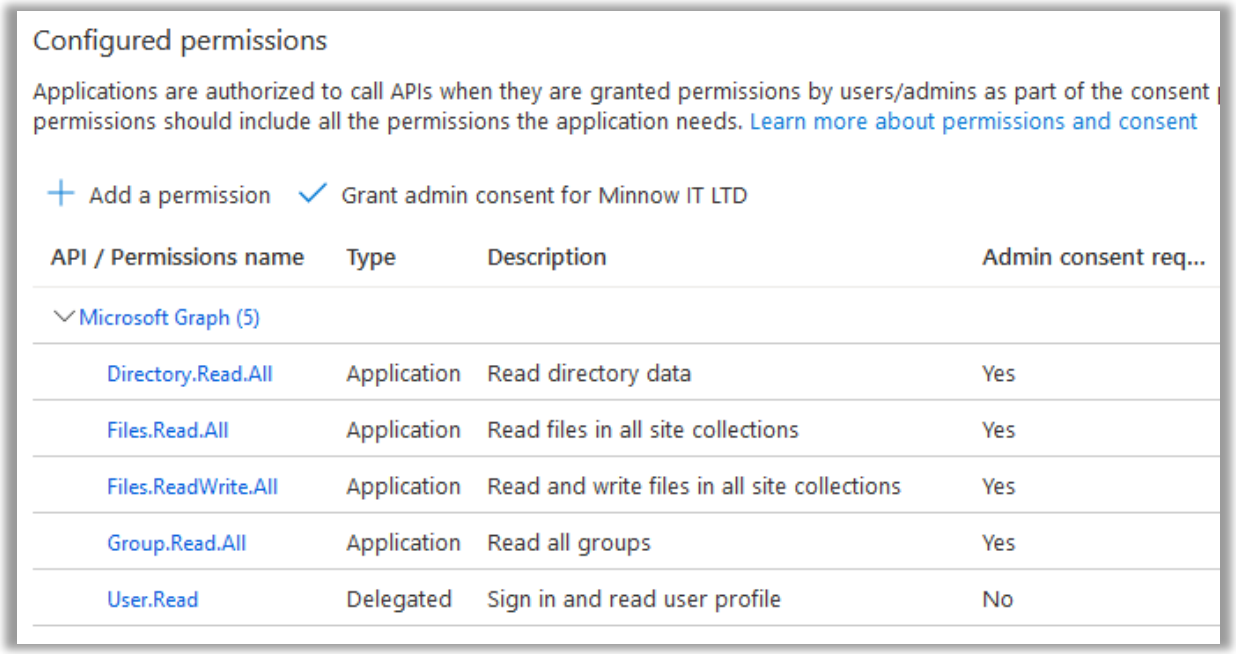




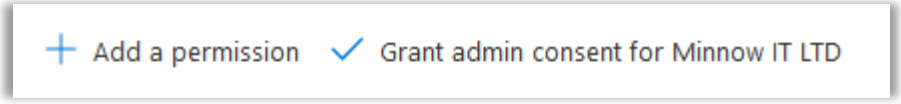
12. Click **Add Permissions** at the bottom of the screen.



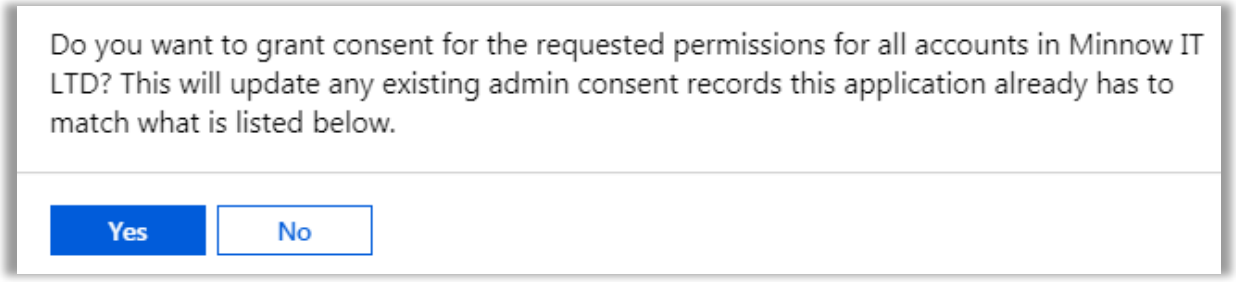
13. The permission summary will now be shown showing the new Application permissions.



14. Click the **GRANT ADMIN CONSENT** for … button at the bottom of the screen.

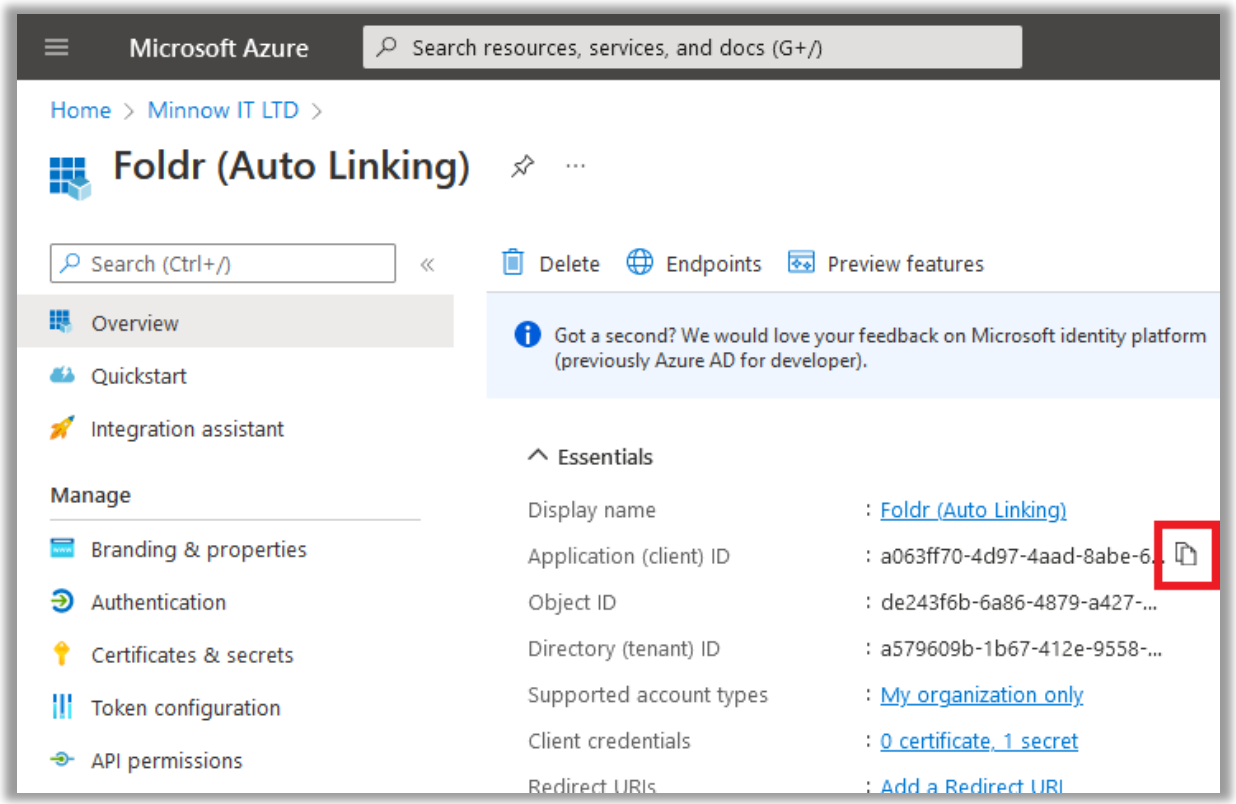


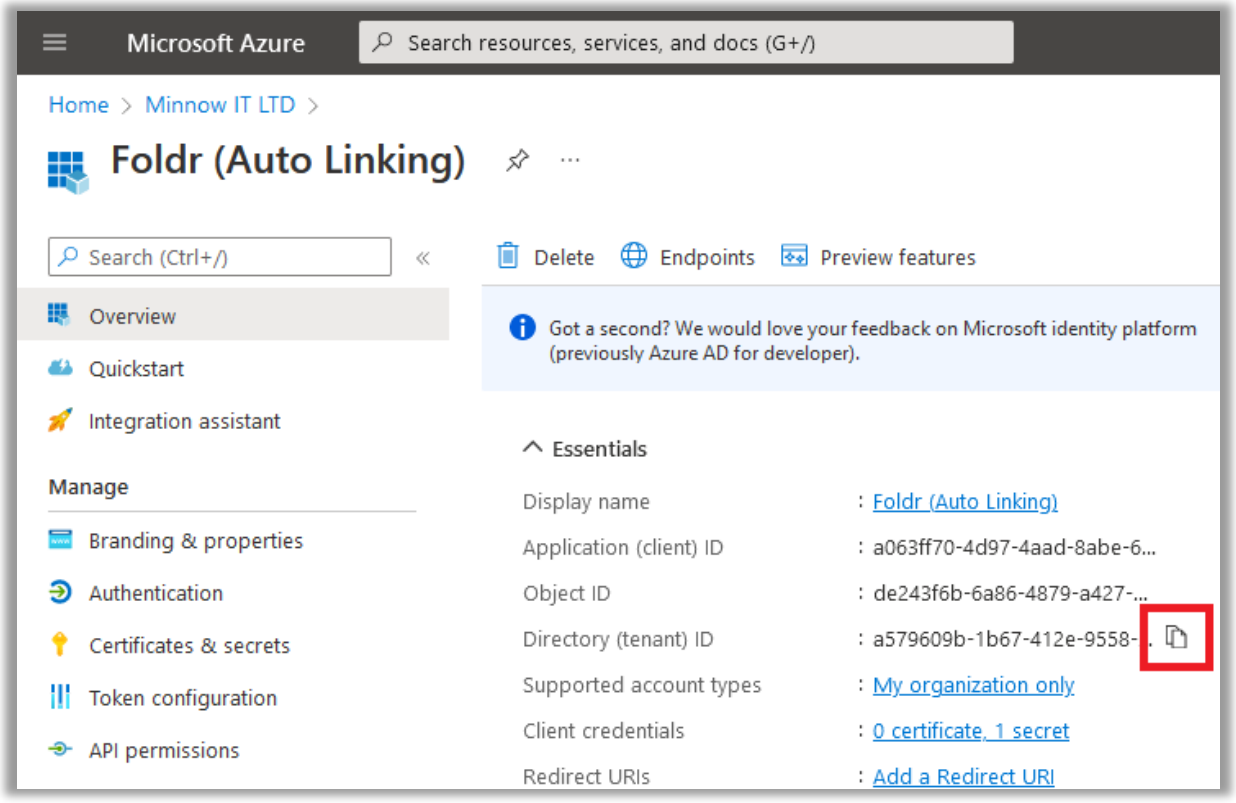
15. Click **Yes** on the confirmation prompt.



16. A success message will then be shown

17. Click on Overview and take a copy of the **Application (client) ID** and **Directory (tenant) ID** – these will be required later.





Creating the Microsoft Service Account

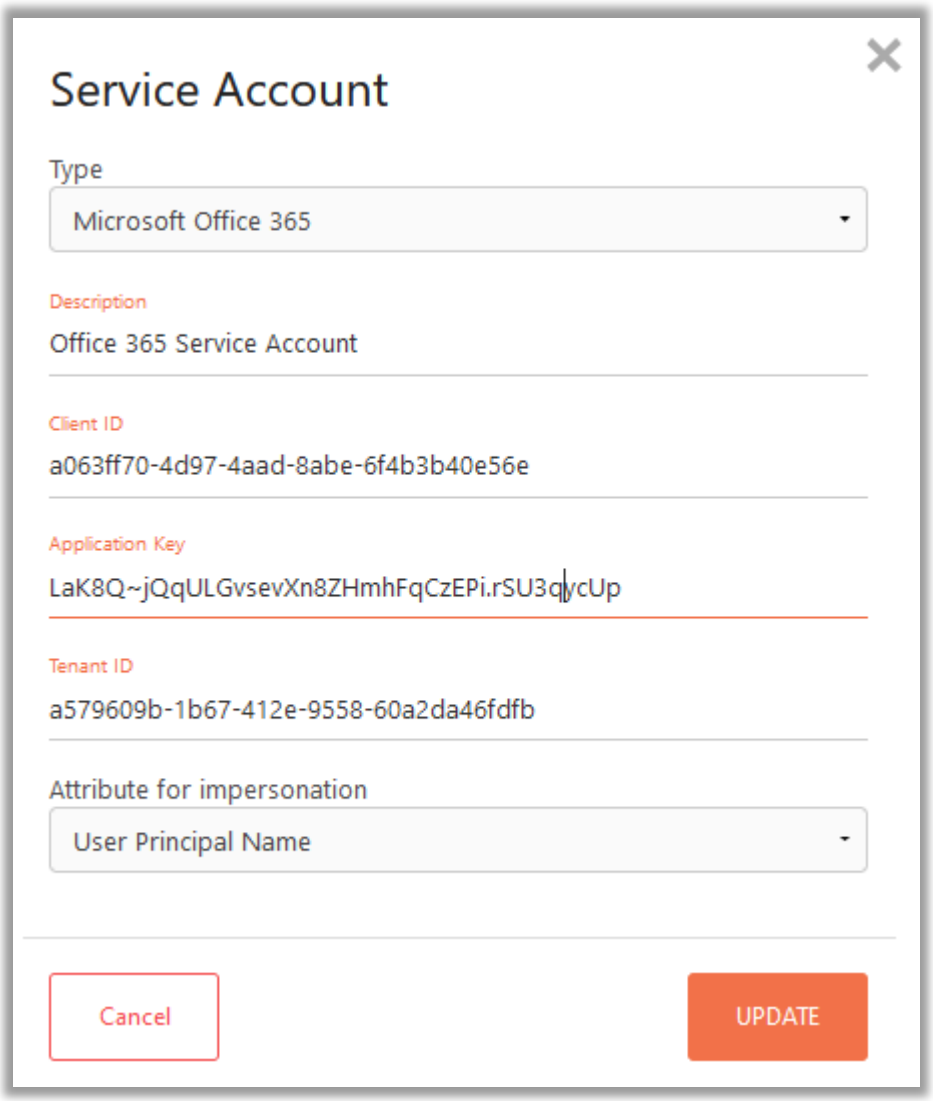
A **Microsoft** service account must now be created within ***Foldr Settings > Integrations > Service Accounts***

The **Application (client) ID** as shown in Overview panel should be copied into the *Client ID* ***field***.

The **Client secret** as created in at step 5 above should be copied into *Application Key* field

The **Directory (tenant) ID** as shown in the Overview panel should be copied into ***Tenant ID*** field

Creating the Microsoft Office 365 service account



Attribute for impersonation

You must finally select the Active Directory Attribute that is going to be used to match against the corresponding Office 365 account.

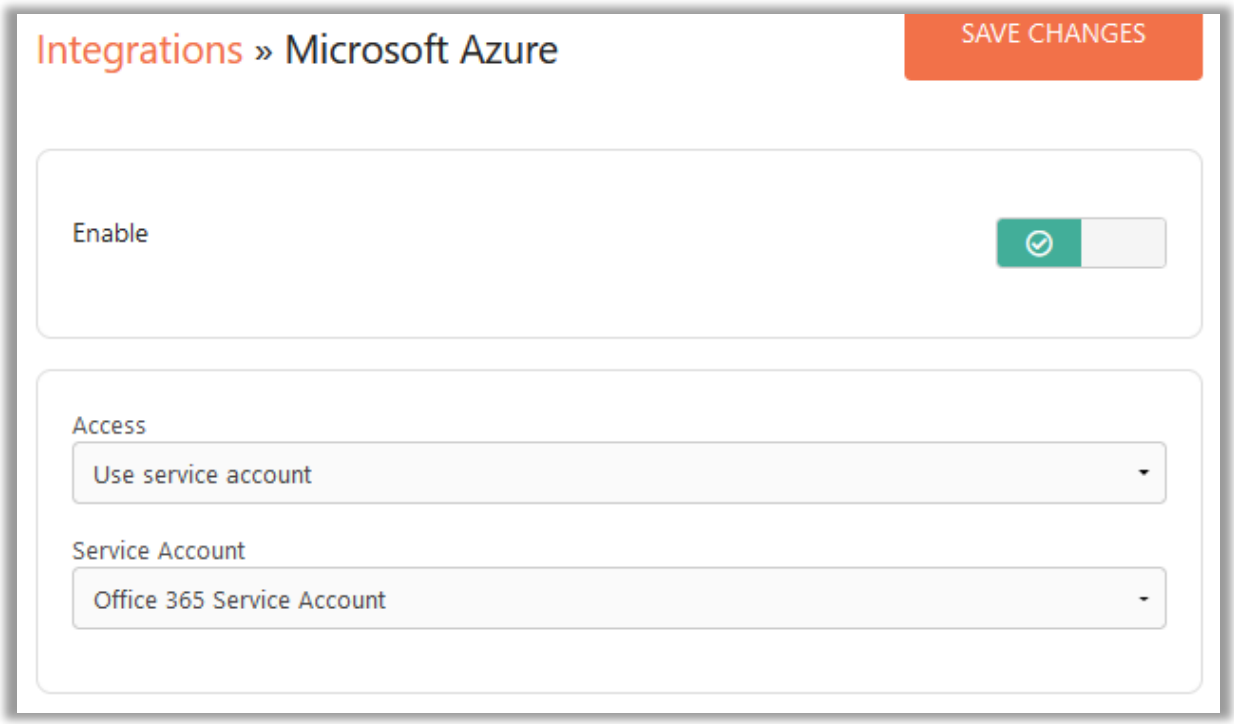
Typically, either the user's User Principle Name (UPN) or email address will match the Office 365 email address used to identify their account. If neither of these attributes match, you can select the 'custom' option to build your own matching rule, such as %username%@office-365-domain.com

Click **SAVE**

Enable the OneDrive integration & Change Background Account Access

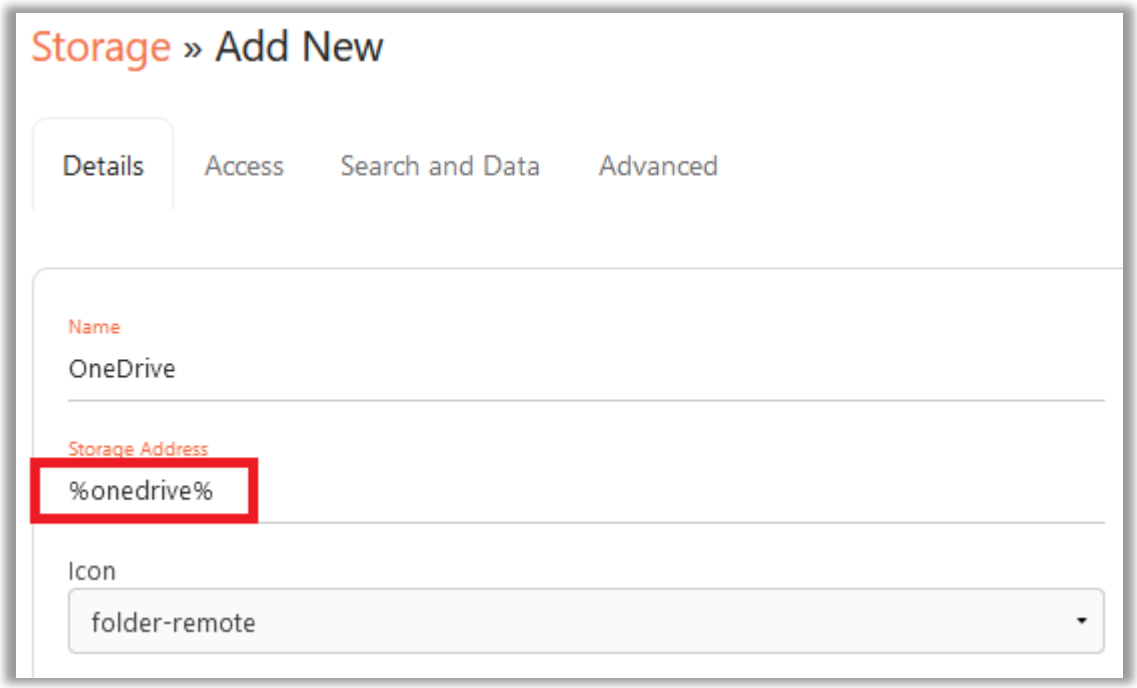
Navigate to ***Foldr Settings > Integrations > Microsoft Azure***

Enable the integration and select '**Use service account'** under the Access section and select the service account.

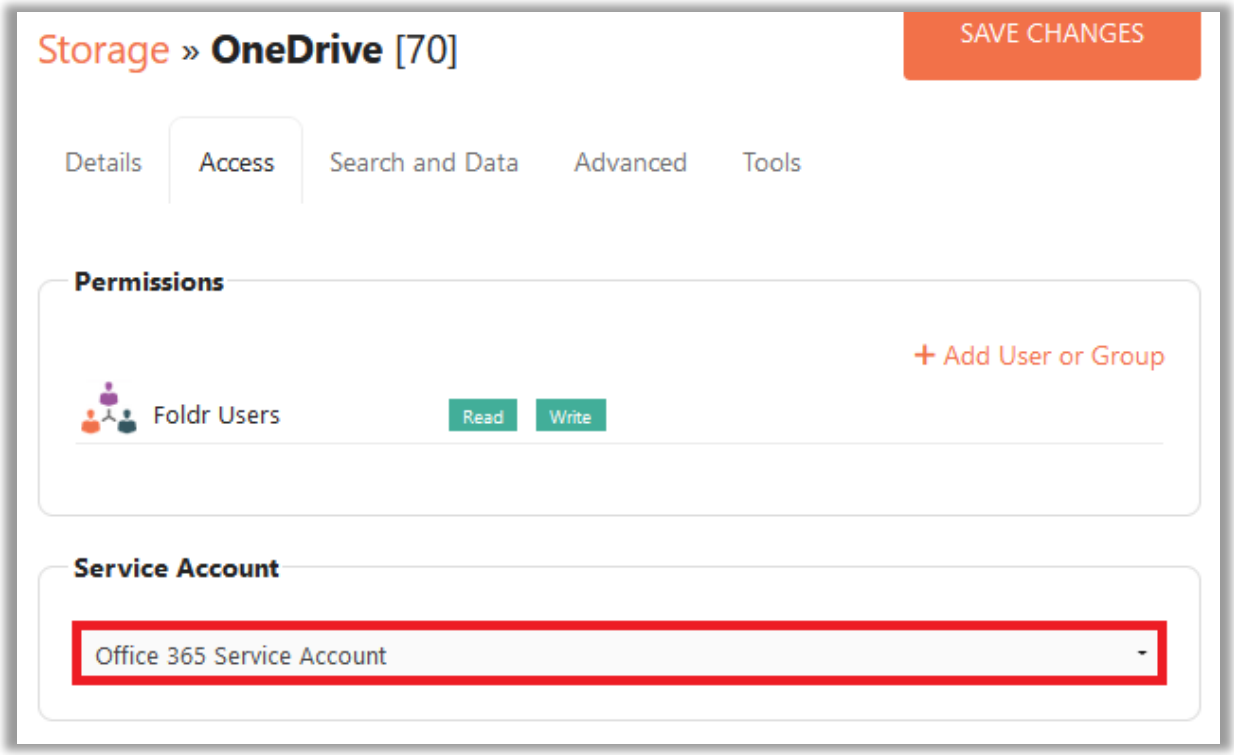


Add the Storage Item for OneDrive

A new Share should now be created for OneDrive under ***Foldr Settings > Files & Storage*** the storage address **%onedrive%** to present the users OneDrive storage within the Foldr interface. Give the share a suitable name, icon and any other options that are required.

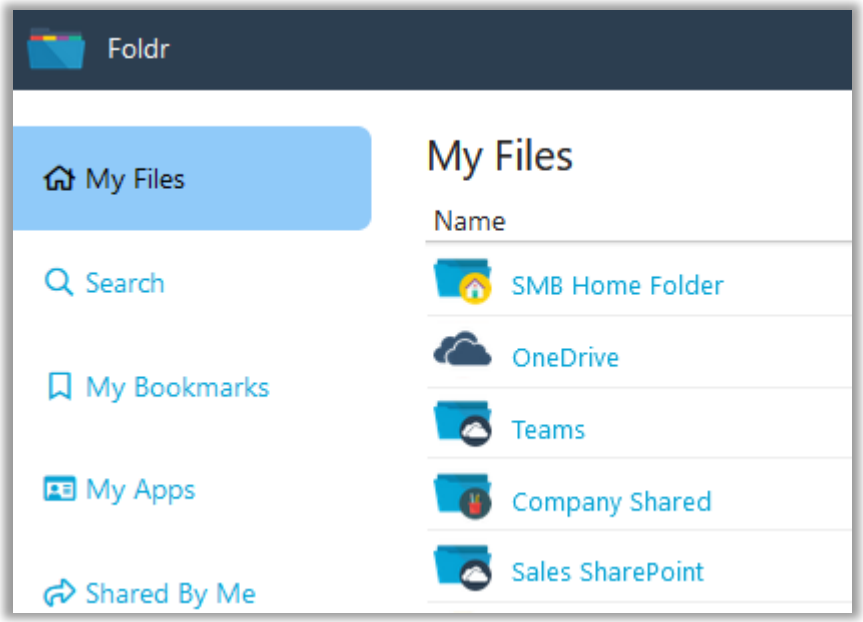


Click the **Access** tab and select the **Microsoft service account** on the OneDrive share configuration screen



Finally, Click **SAVE CHANGES**.

The integration steps for automatic account linking and presenting OneDrive to users is now complete. When a user signs into Foldr, their corresponding OneDrive storage should be presented to the user automatically.



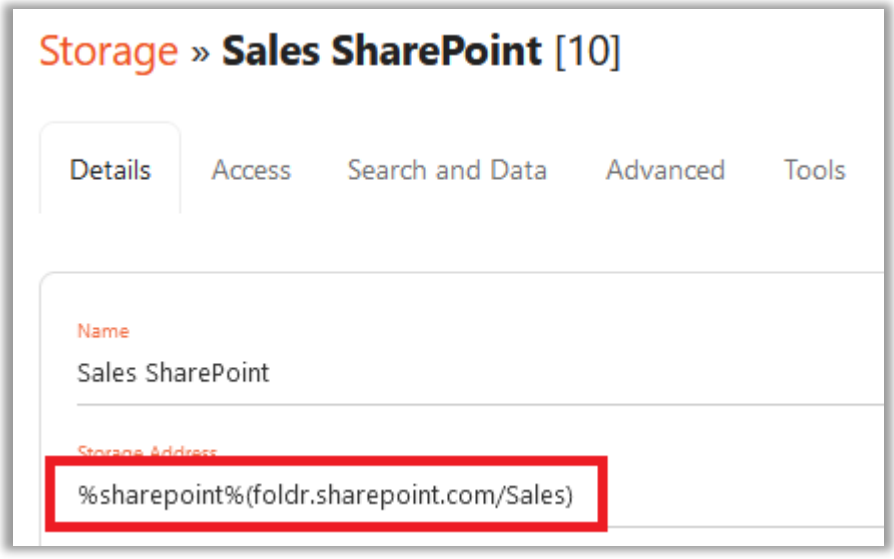
Presenting SharePoint sites to Users

A dedicated KB article to configure SharePoint sites is available here

The basic steps to present a SharePoint site are:

Create a new storage item should be created for each SharePoint site (or Document Library) under ***Foldr Settings > Files & Storage*** using the storage path:

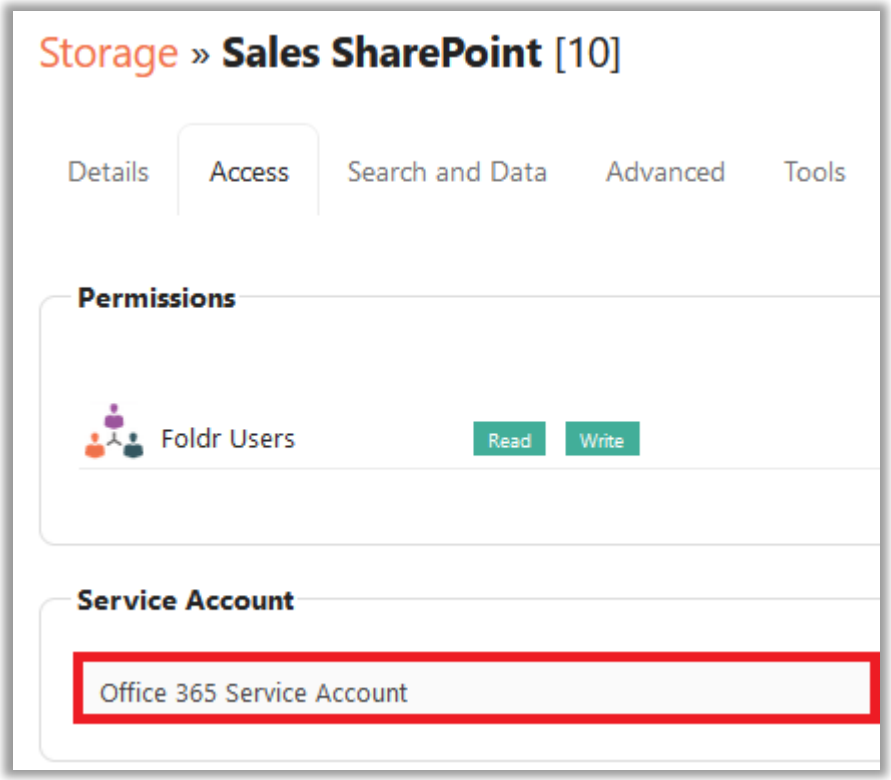
%sharepoint%(tenant.sharepoint.com/sites/site-name)



Note if /sites/ is not in the SharePoint URL when viewed through O365 directly, it can be removed from the Share URI

The administrator can present the root SharePoint site for an organisation using the Share URI **%sharepoint%**

On the Access tab, select the **Microsoft service account** on the SharePoint share configuration screen.



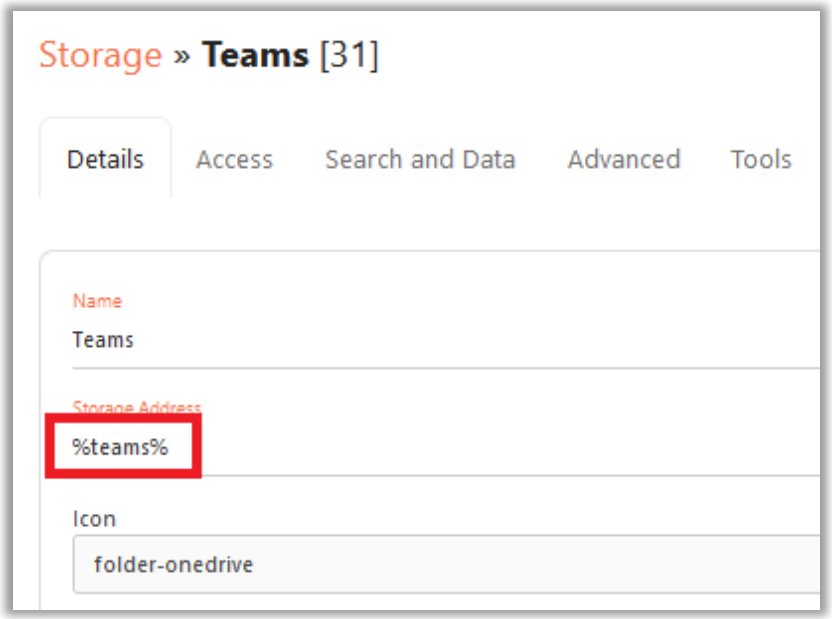
Click **SAVE CHANGES**.

Presenting Teams storage to Users

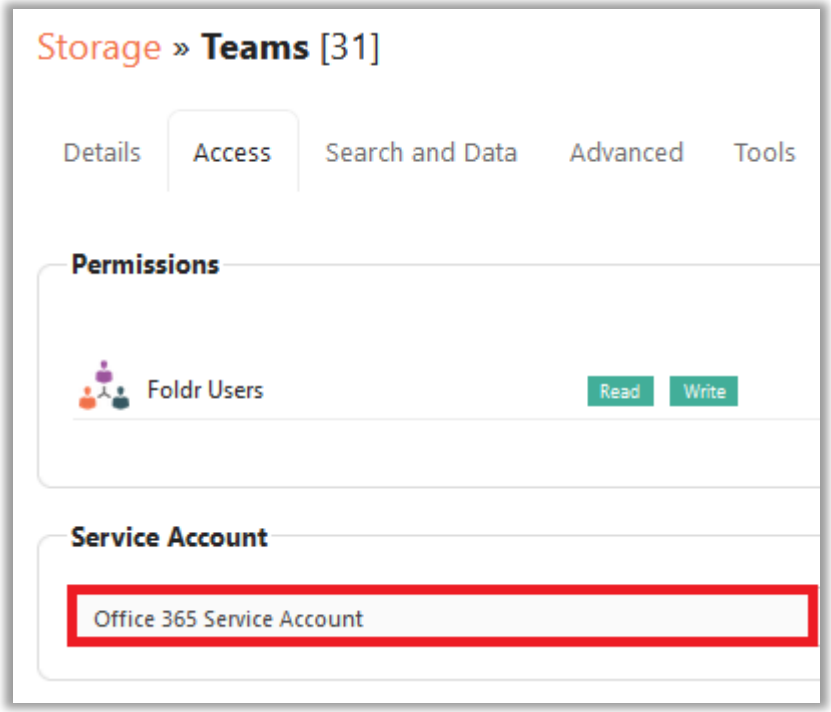
A new share should be created for Teams under ***Foldr Settings > Files & Storage*** using the storage address **%teams%.**

There is an alternative **%teamedu%** storage connector for education Office 365 customers which will support additional features that are exclusive to education institutions.

note the additional Application permissions for Teams are required (Read directory data and read all groups). All Teams storage will be displayed within this one storage location in Foldr.



Select the **Microsoft service account** on the Teams configuration screen **Access** tab.

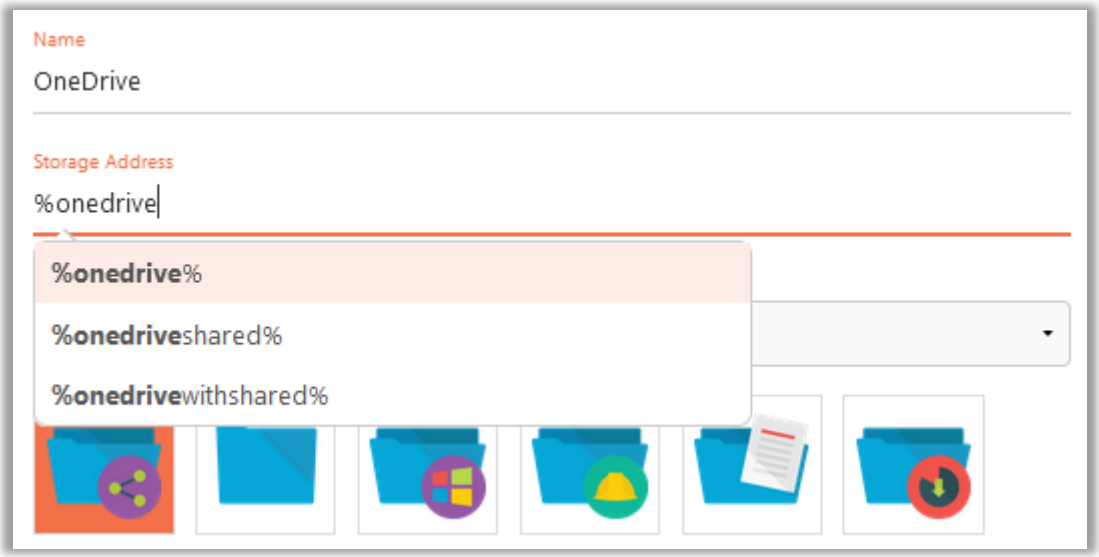


Presenting Shared Office 365 items to Users

Foldr can present files/folders that have been shared from within Office 365. Shared items can be displayed in a dedicated share/storage item within My Files or alternatively a 'Shared with Me' directory can be displayed inside a user's OneDrive and all shared items will be available inside.

To create a dedicated share for Office 365 shared items, create a new item within ***Foldr Settings > Files & Storage*** using path **%onedriveshared%.** To present a user's OneDrive with a 'Shared with Me' folder

in the root of OneDrive, create a share and set the path **%onedrivewithshared%** If automatic linking is being used, select the Microsoft service account on the Access tab.



Troubleshooting – HTTPS / SSL inspection

Please ensure the following domains are excluded from HTTPS / SSL man-in-the-middle inspection on your firewall / web filter, as this will cause issues between the Foldr and OneDrive / SharePoint Online:

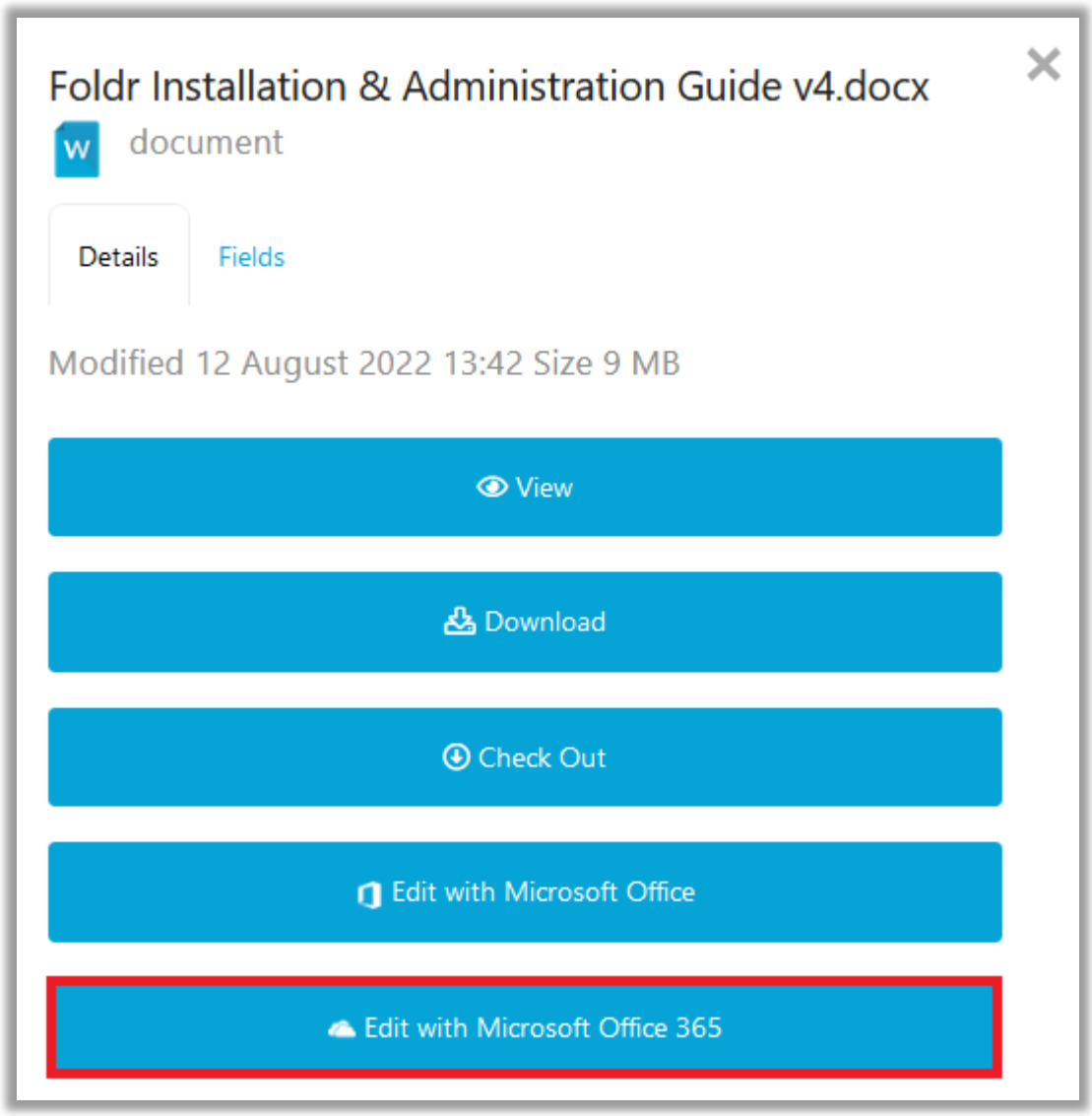
graph.microsoft.com
api.office.com
login.microsoftonline.com
{office365-tenant}-my.sharepoint.com

i.e. company-my.sharepoint.com

Document Editing in Office Online

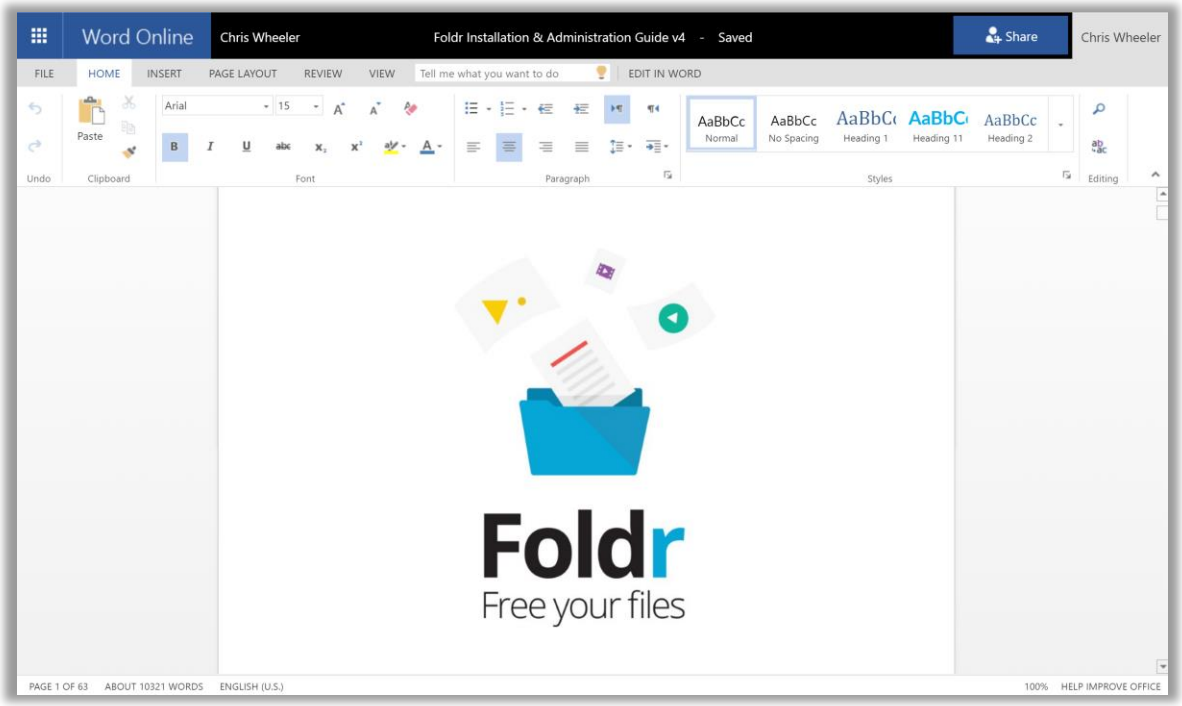
Now that the Office 365 integration has been configured, users are able to utilize the web-based Office apps to edit either on-premise or cloud-based documents from the Foldr web app.

Example – Edit a word document held on on-premise / local SMB share in Office (Word) Online.



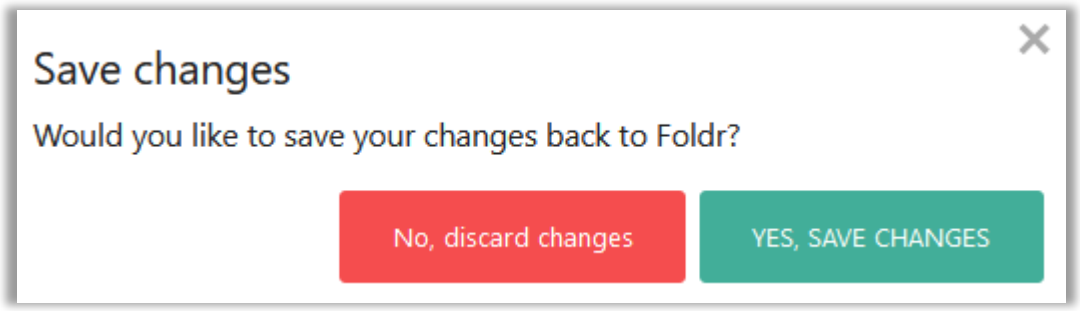
The user selects the document in the Foldr web app, clicks **Edit with Office Online**. A new browser tab will open and the document will open within the relevant web-based Office 365 web app ready for editing.

Web based version of Word (Word Online):



If the source document resides on OneDrive, the user is working natively/directly as if they were signed into Office 365 natively. Any changes are saved automatically when the browser tab is closed and other features in 365 such as collaborative editing will function as normal.

If the original document was hosted elsewhere, such as an on-premise SMB share, the user will be prompted to either or discard or save changes when the Office Online tab is closed. When the user clicks Yes in this prompt the file is downloaded back from Office 365 and saved into its original location, overwriting this original file.

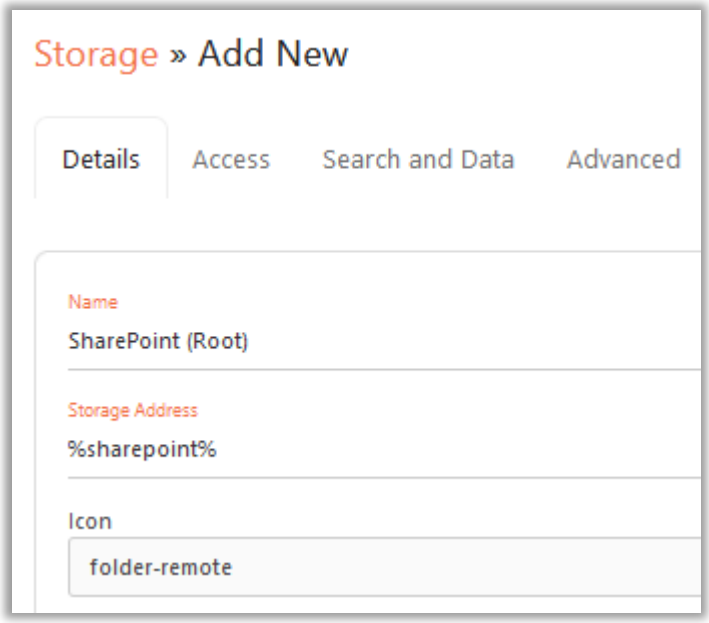


SharePoint Online (Office 365 SharePoint) Integration

Individual SharePoint Online sites may be presented to users in addition to OneDrive storage. The initial integration steps are identical for OneDrive. i.e. An application key and secret are generated in Azure in the same way, and no additional permissions are required when using MS Graph API to access SharePoint Online.

Adding the Share for the Root SharePoint Site

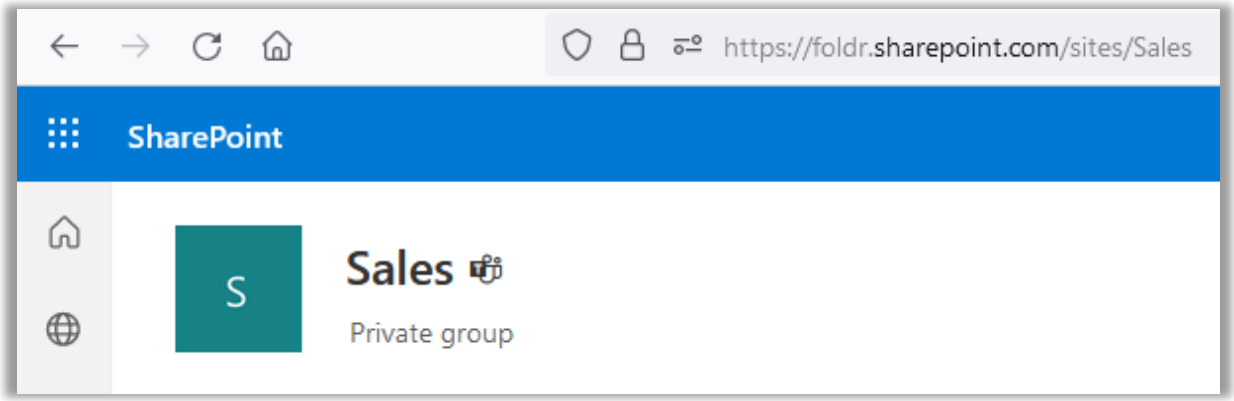
Add a new Share under ***Foldr Settings > Files & Storage*** using the share URI **%sharepoint%** to present the root of the organisation's SharePoint structure.

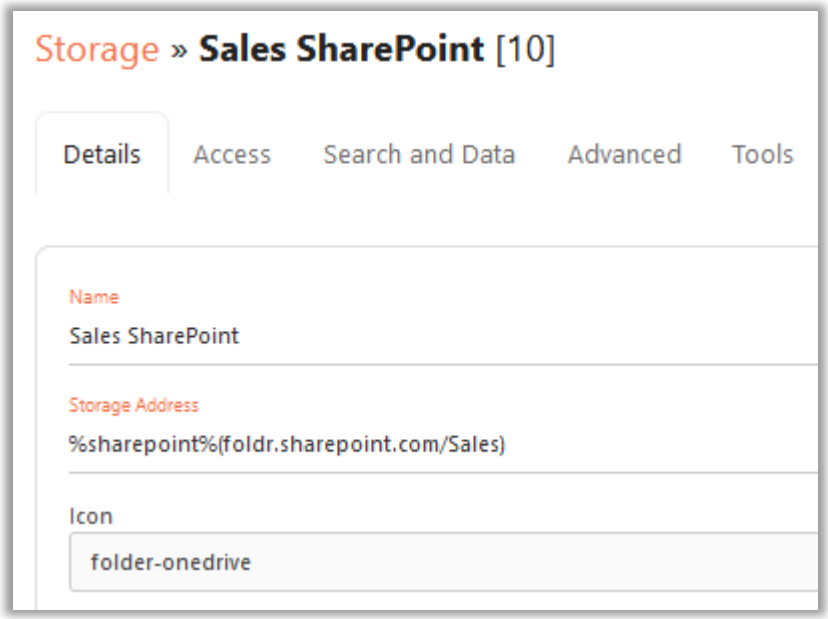


Important – If automatic account linking is being used, ensure that the Microsoft service account is selected on the Share configuration screen.

Adding a Share for Specific SharePoint Sites

To present the Documents folder from a SharePoint Team site called 'Sales', the storage path requires the **tenant address in parentheses, followed by the site name** as shown below. SharePoint sites are usually prefixed with **/sites/** so the URI is formatted as shown below.

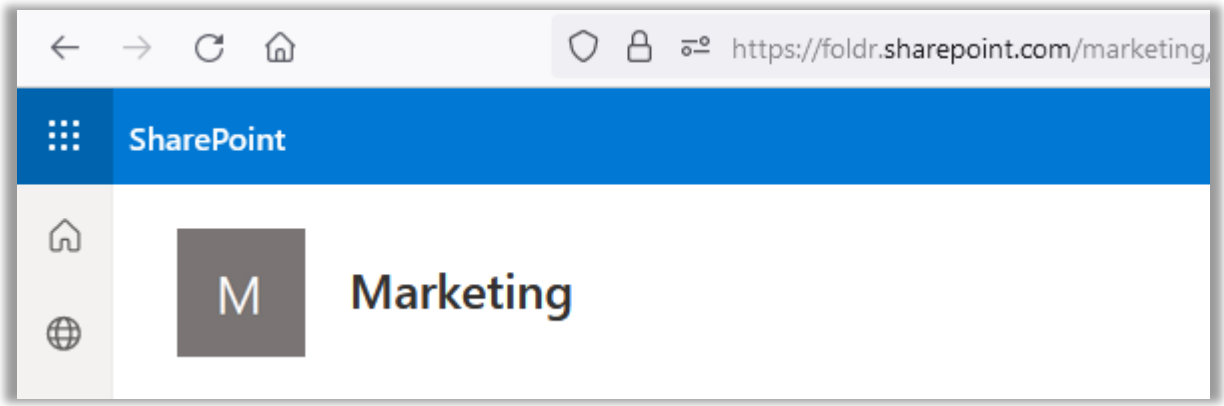




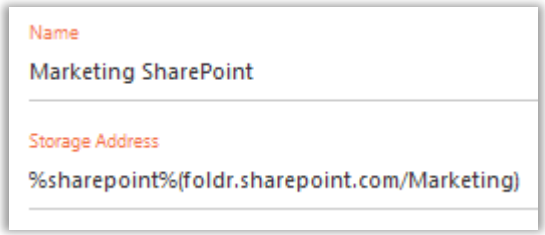
The Office 365 tenant name, can be found by signing into portal.office.com, launching SharePoint from the dashboard and obtaining it from the browser address bar.

Some SharePoint sites may not contain /sites/ in their URL, if this is the case you can be present these to users using the Share URI as shown:

Example tenant name as seen in Office 365:



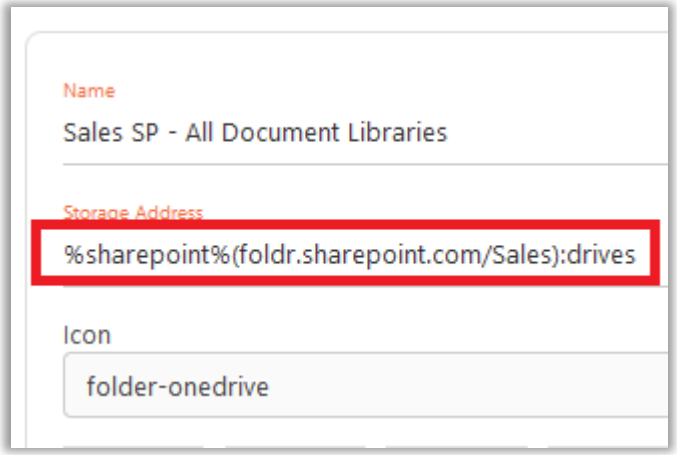
Storage path in Foldr to support this type of site (note that /sites is missing in this example):



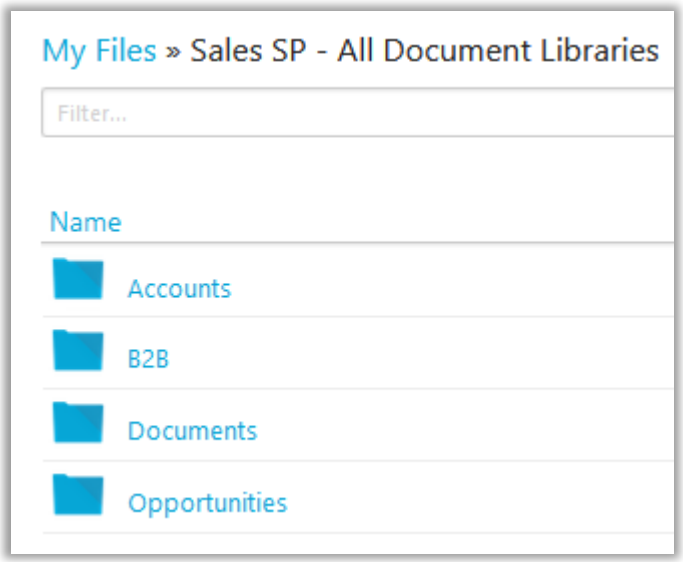
Important – If automatic account linking is being used, ensure that the Microsoft Office 365 service account is selected on the Access tab.

The above Share URI will show the user only the content of the default '**Documents**' folder / library in the configured SharePoint site.

To list all document libraries inside a site, the URI should be appended with **:drives** as shown below.



The user would then be presented all document libraries inside the site – example below:



Teams Integration

Teams is the chat-based collaboration tool in Office 365. Each 'Team' has a document area for file storage and Foldr is able to present all Teams storage that a user has permission to access within a single share / storage item in the Foldr interface.
Teams storage is available for both **manual** and **automated** account linking scenarios.

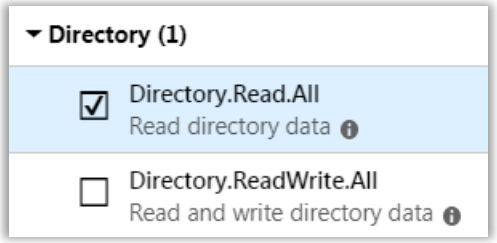
Additional Graph API Permissions

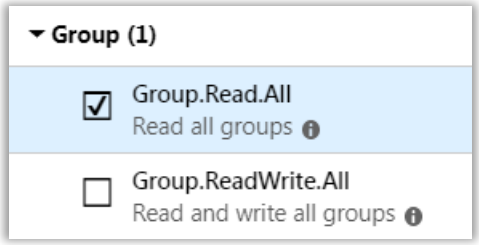
Manual account linking does not require any additional permission.

Automated linking using service accounts requires the following additional **application** permissions to be able to access Teams storage that applies to the user in question:

Group and Directory sections:

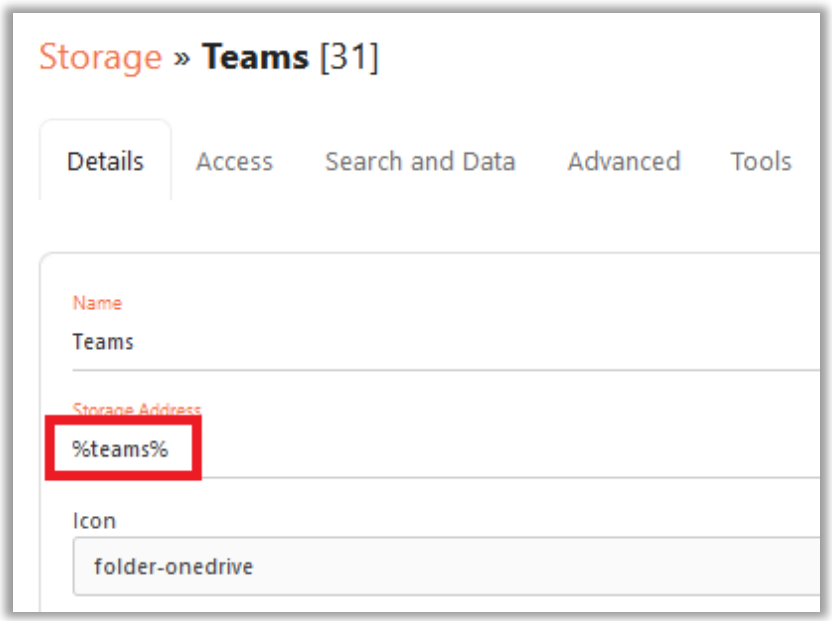
Directory.Read.All
Group.Read.All





Creating the Teams Share

1. Navigate to ***Foldr Settings > Files & Storage*** and click + Add New Share
2. Give the item a suitable name and use storage address **%teams%**



3. If automatic account linking is being used, select the Microsoft service account on the Access tab.
4. Click **SAVE CHANGES**.

Permissions and Controlling Visibility of the Teams Share

With both account linking methods, Foldr will respect the permissions in Office 365 automatically and only show the Teams storage folders that a user should have access to.

Should you wish to hide the main ‘Office 365 Teams’ share from the interface from selected users or groups, modify the Permissions section on the share configuration screen (shown above) – removing Foldr Users and create allow / deny rules as required.

Microsoft Outlook Add-In

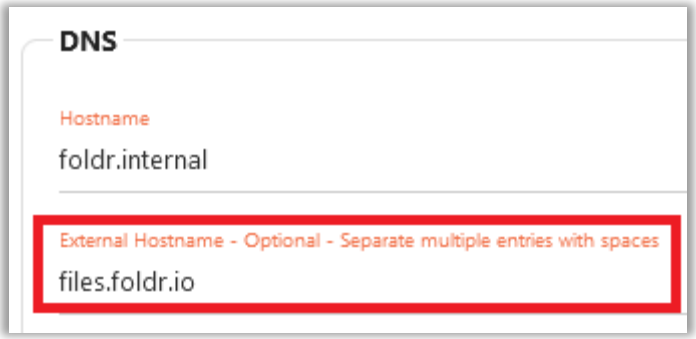
Foldr includes an Outlook Add-In feature that allows Outlook users to include files/folders from Foldr storage either as a link or individual files as an attachment. The add-in is compatible with both desktop and web-based versions of the Outlook client on Windows and macOS. The add-in must be added as a one-time operation via either the web or desktop Outlook app. Once it is added, it will be available in both apps (web and desktop).

Requirements:

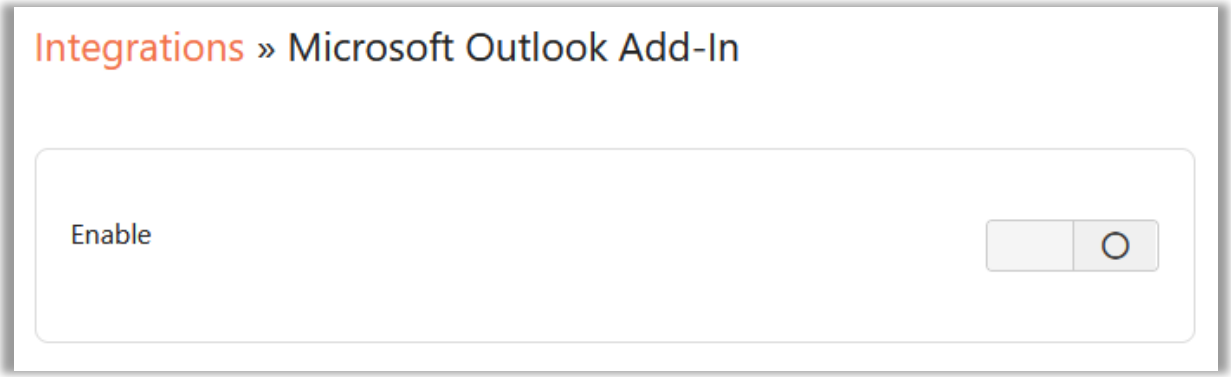
– The Foldr server must be available externally
– A valid signed SSL certificate must be installed on the Foldr server.
– Sharing features must be enabled on the server to allow users to insert public or secure links
– The File Picker is enabled in Foldr Settings > Integration > File Picker (enter the server's public URL/external hostname)

Enabling the Outlook Add-In on the Foldr Server

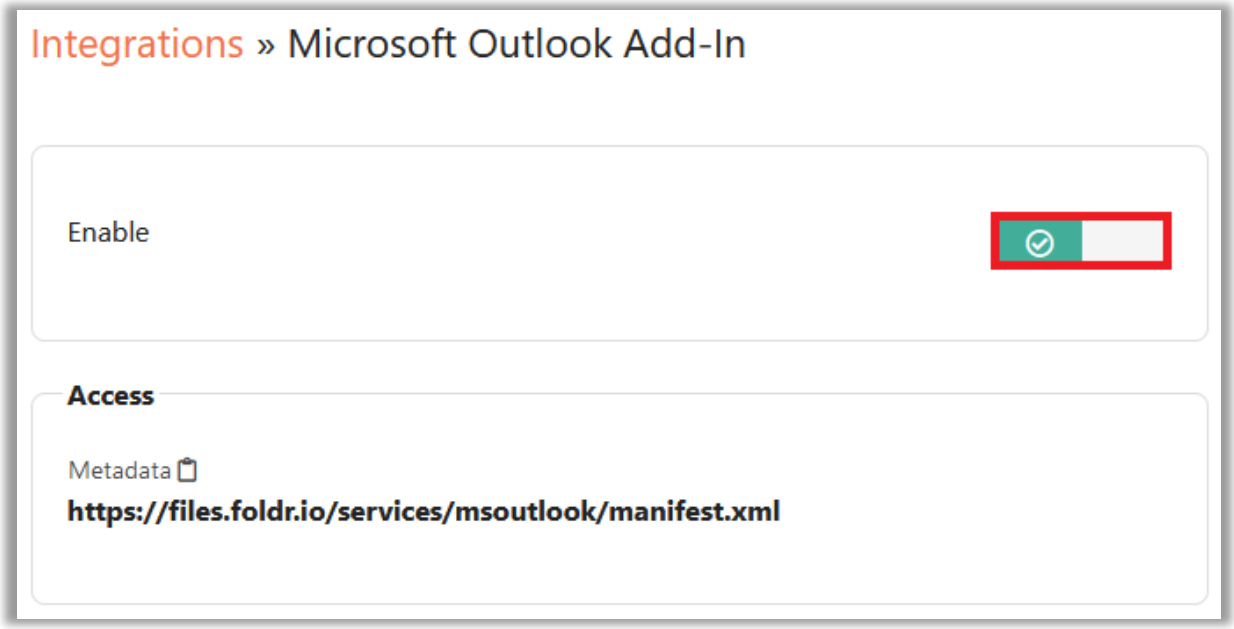
1. Ensure the Foldr server's public/external address is configured within ***Foldr Settings > Appliance > Network > Configuration > External Hostname***. (https://files.foldr.io is to be used as an example in this KB article)



2. Enable the Outlook Add-In, by browsing to ***Foldr Settings > Integrations > Microsoft Outlook Add-in***



3. Enable the **toggle** and click **Save Changes**



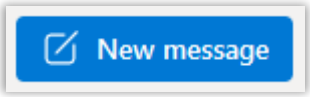
4. Copy the **metadata address** shown in the format:

https://address-of-foldr/services/msoutlook/manifest.xml

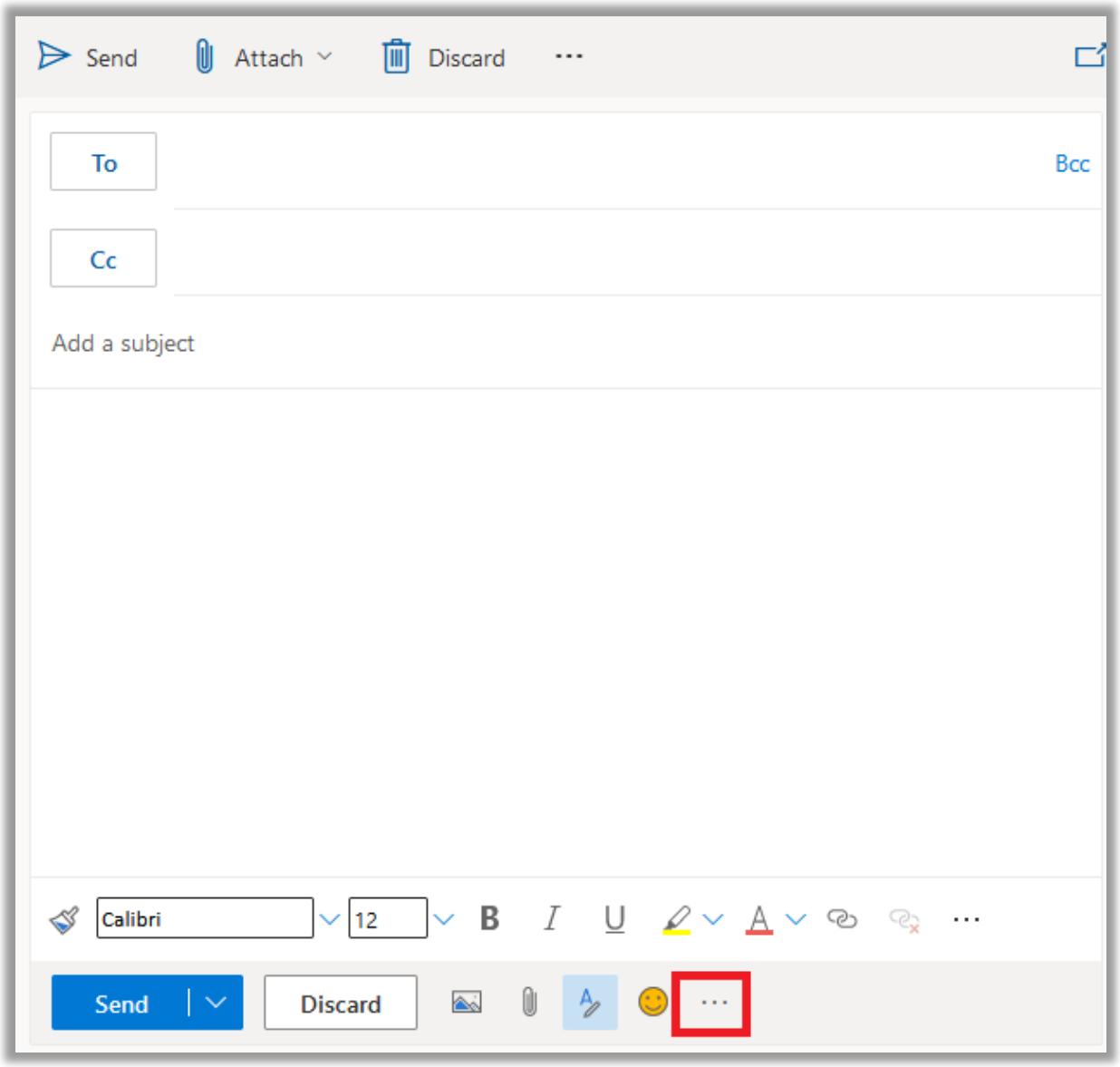
Adding the Foldr Add-In to a single Outlook account (Web app)

Open the browser and sign into Outlook at https://outlook.office.com/mail

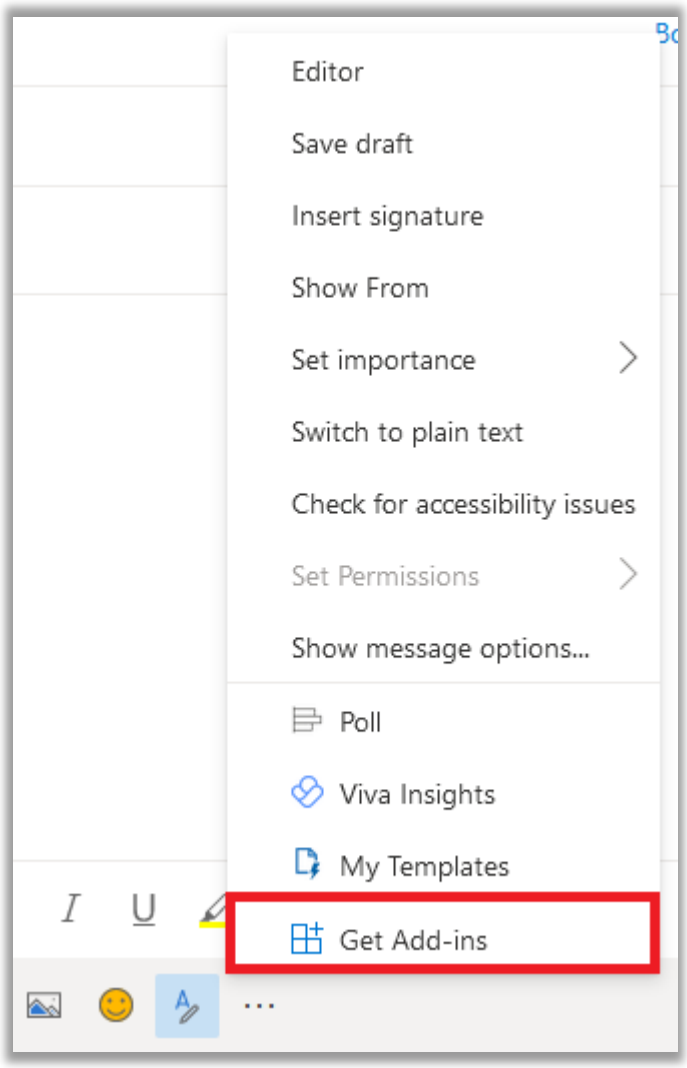
To add the Foldr Add-In, click New message to compose a new email



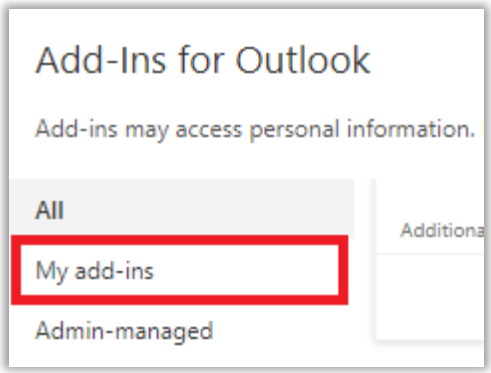
Click the **Ellipsis** [...] button highlighted below.



Click **Get Add-Ins**

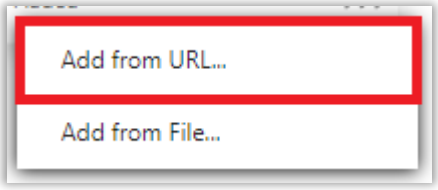


The Add-ins for Outlook dialog will display. Click **My add-ins** on the left panel.

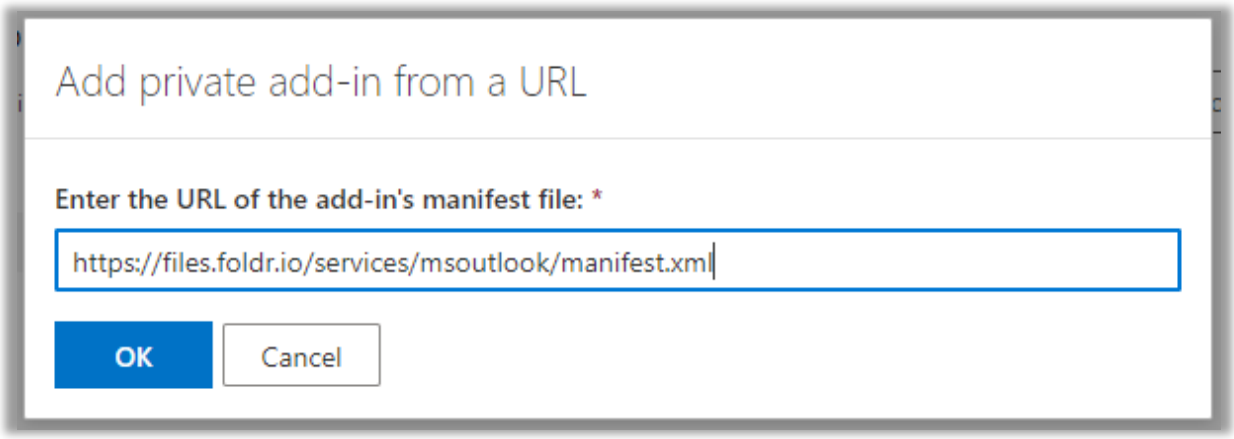


Under ***My add-ins***, scroll down to the Custom Add-Ins section.

In the pop-up menu, select **Add from URL**

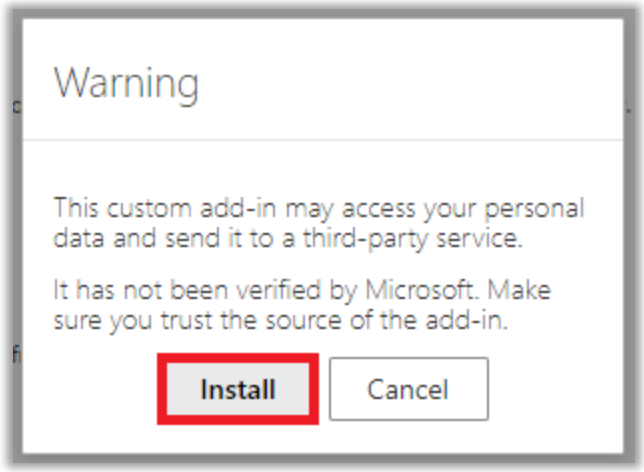


Paste in the metadata address copied earlier in ***Foldr Settings > Integrations > Microsoft Outlook Add-In***

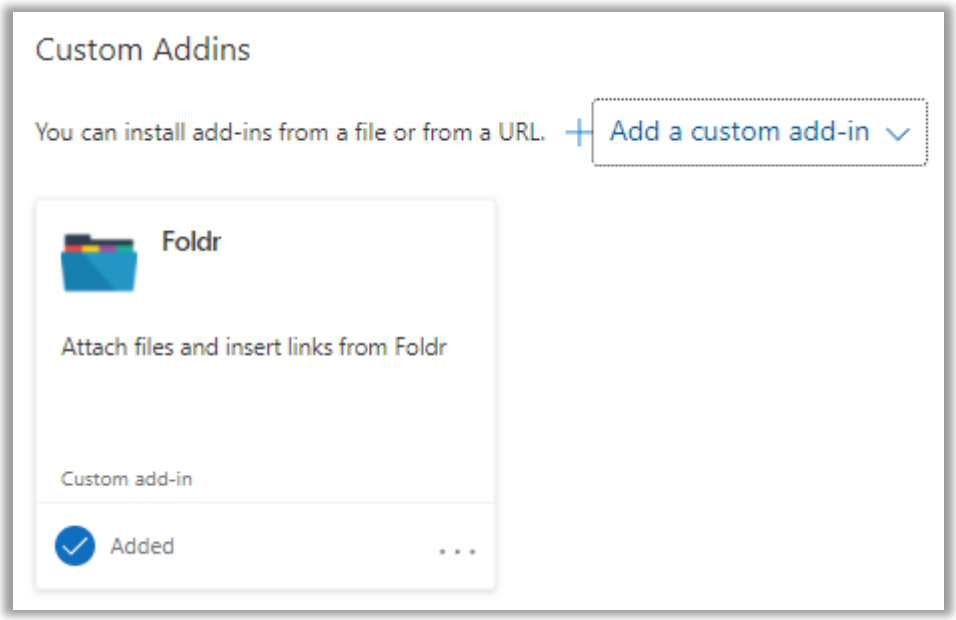


Click **OK**

Click **Install** on the following prompt.



Foldr will now be shown as a custom add-in.

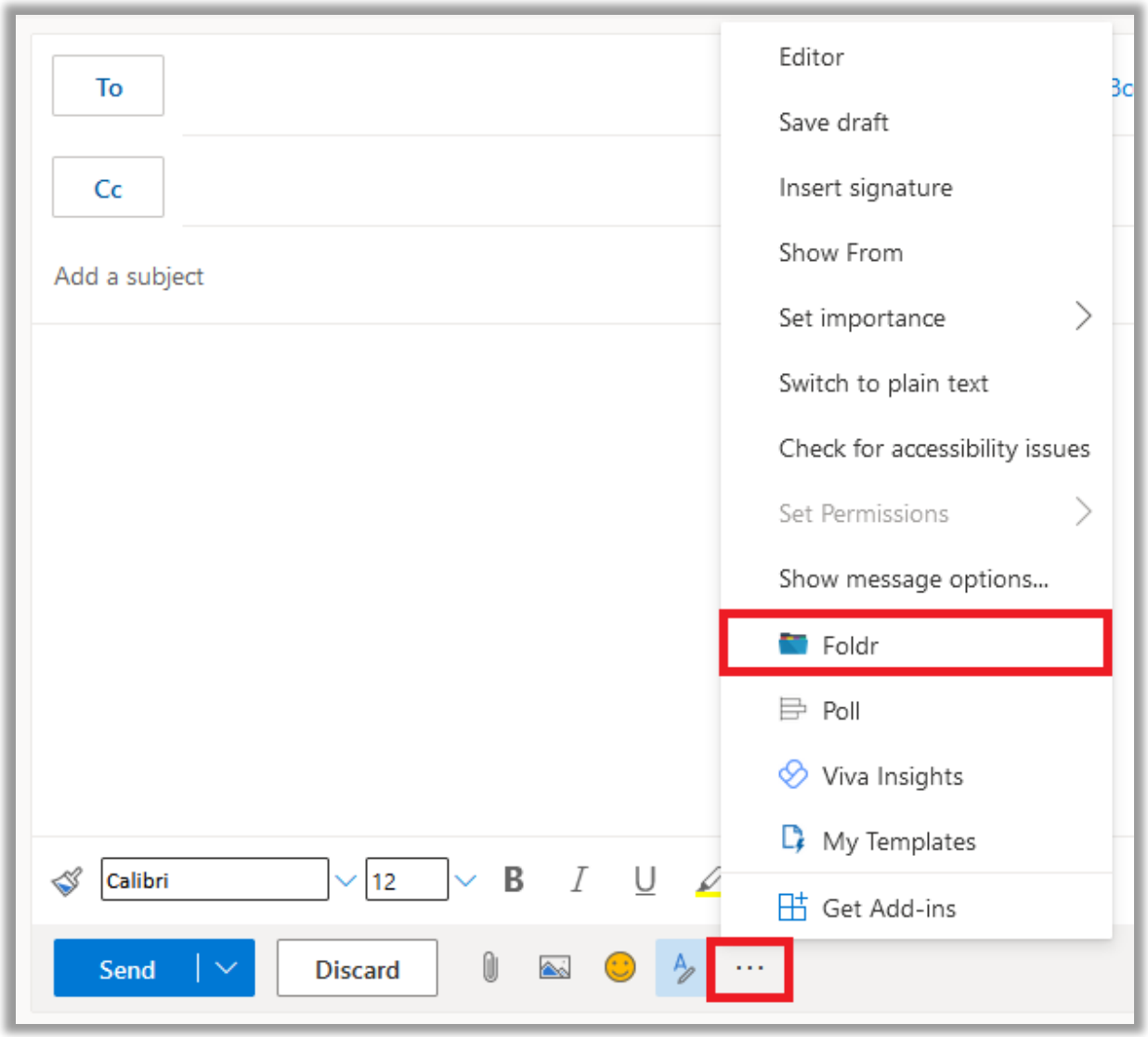


Close the Add-Ins for Outlook dialog.

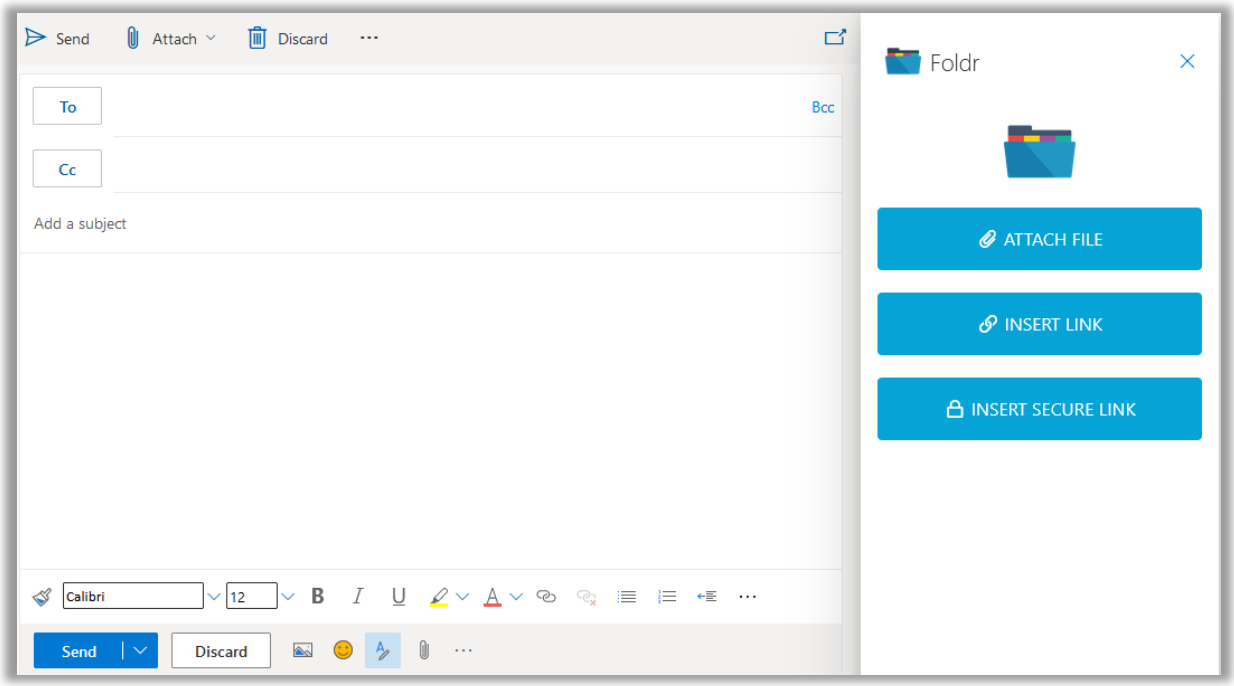
The add-in is now ready to use and will be available in both web and desktop versions of Microsoft Outlook.

User Experience - Using the Outlook Add-In (web)

When composing an email, the Foldr add-in can be opened using the **ellipsis [...] > Foldr**



The Foldr panel will appear on the right of the interface. Where the user can select to Attach a file, create a link to a file or folder (public link) or a secure link. A secure link allows the user to specify recipients allowed to use the link by email address.

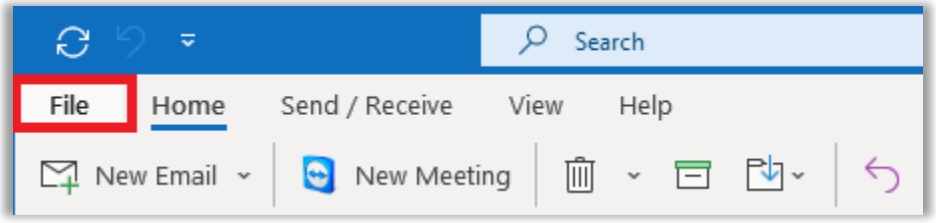


Selecting one of the buttons in the Foldr add-in will open the Foldr web sign-in UI where the user can sign in and view the storage available to them through the Foldr file picket. The user can browse to individual files to attach to emails or files and folders to create basic or secure links.

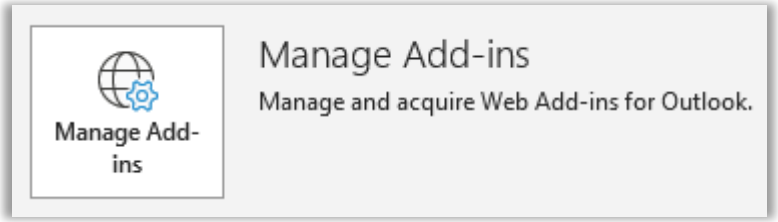
When creating secure links, providing the user has already populated the TO: field in the email, these will be automatically added to the External users field in the sharing UI.

Adding the Foldr Add-In to a single Outlook account (Windows desktop app)

To enable the Foldr add-in in the Outlook desktop, the process is the same as above for the web app, but the user must first click **File**

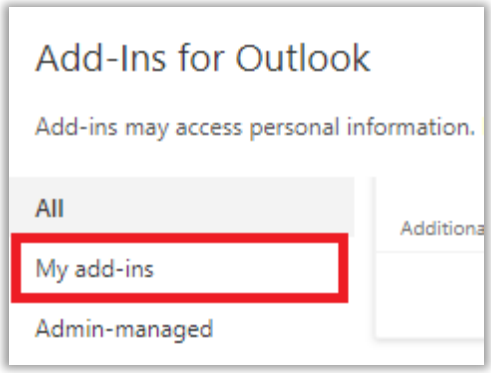


Then, click **Manage Add-ins** (bottom option)

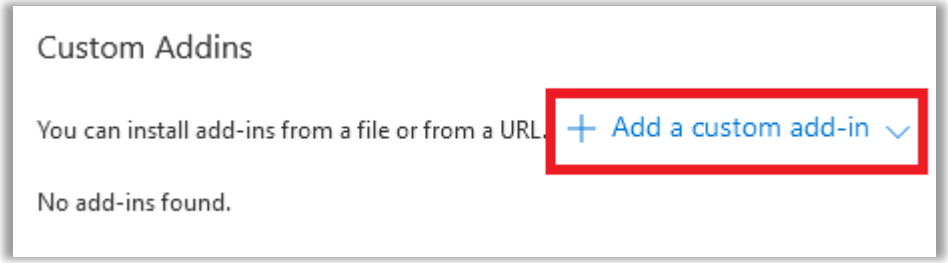


The system default web browser will launch and the user will be prompted to sign into Office 365 if not already signed in. After sign in, the Outlook Add-ins page will be displayed and the process is the same as the Outlook web app.

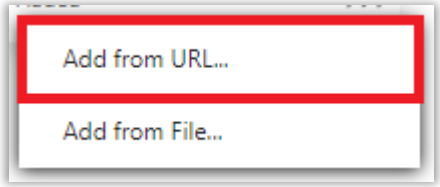
Click **My add-ins**



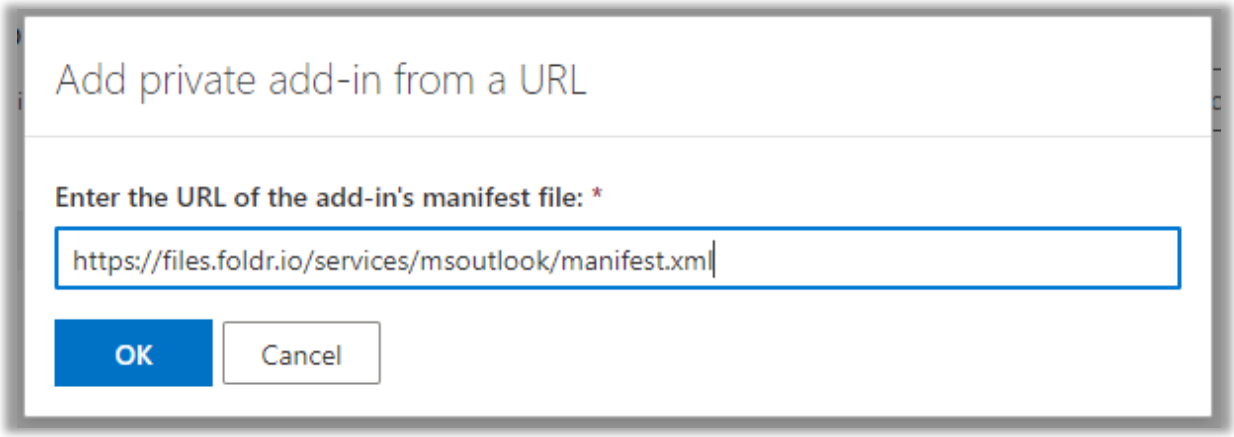
Under ***My add-ins***, scroll down to the Custom Add-Ins section



In the pop-up menu, select **Add from URL**

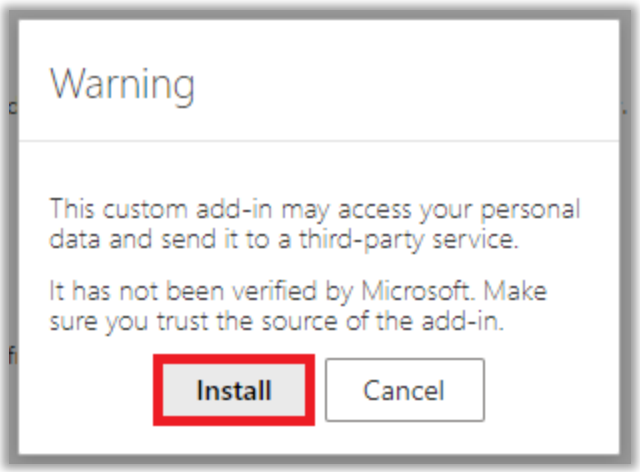


Paste in the metadata address (https://***address-of-foldr***/services/msoutlook/manifest.xml) copied earlier in ***Foldr Settings > Integrations > Microsoft Outlook Add-In***

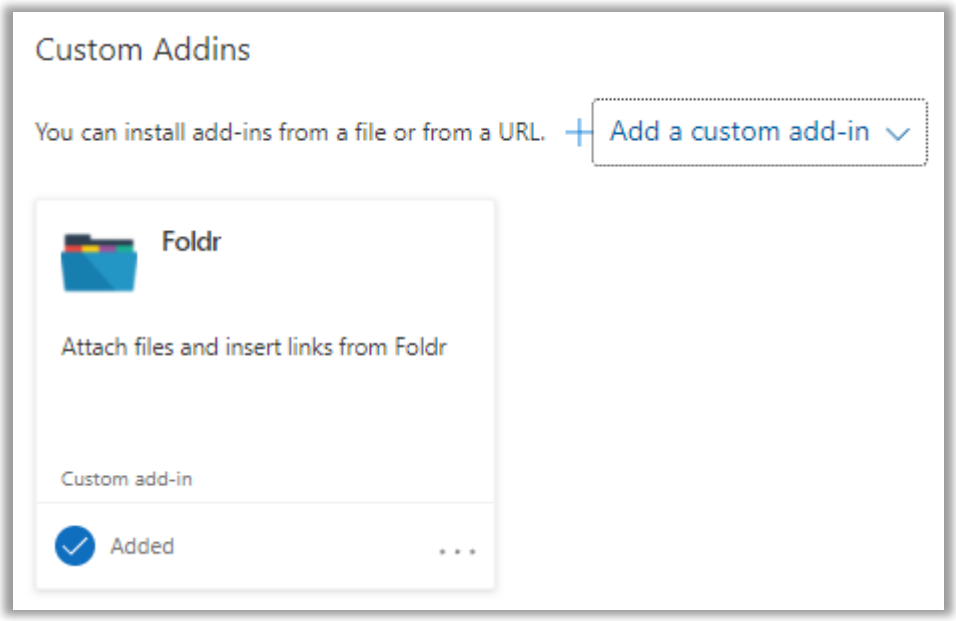


Click **OK**

Click **Install** on the following prompt



Foldr will now be shown as a custom add-in

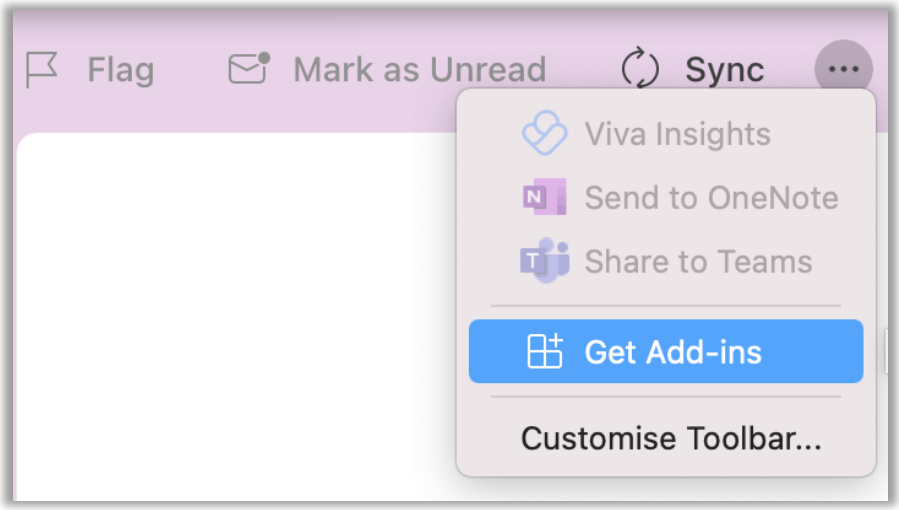


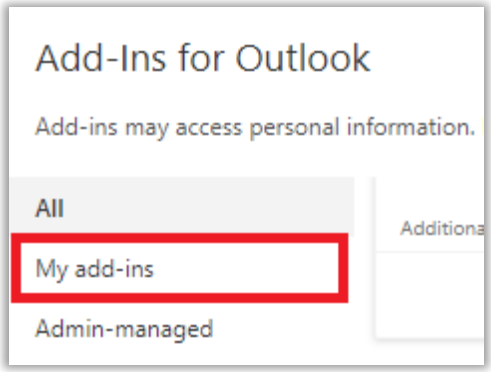
Close the Add-Ins for Outlook dialog.

The add-in is now ready to use and will be available in both web and desktop versions of Microsoft Outlook.

Adding the Foldr Add-In to Outlook (macOS desktop app)

The steps to add the Outlook Add-in on macOS is the same as for Windows (above), but the Get Add-Ins menu is available on the Outlook home screen using the Ellipsis menu below. Click **Get Add-ins**

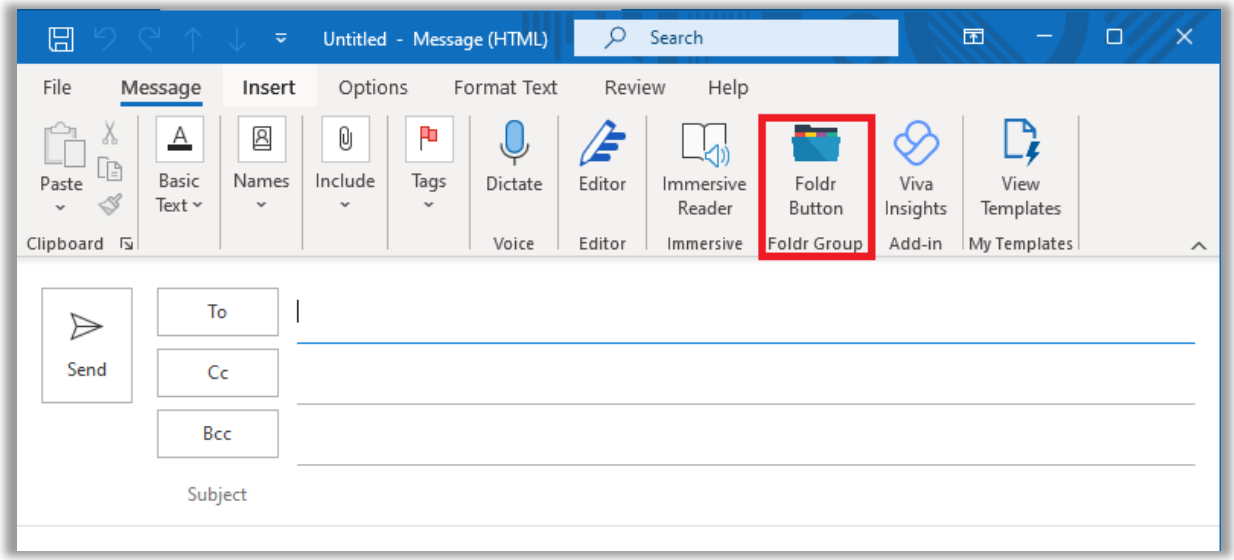




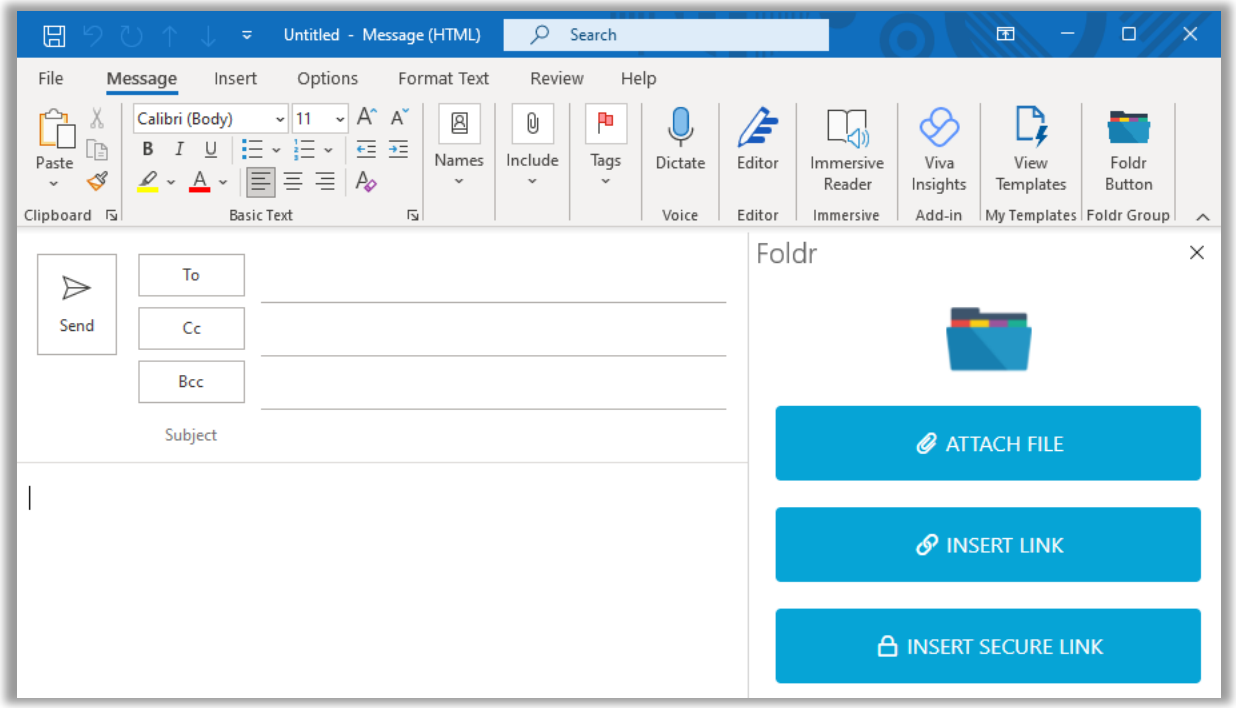
The 'Add-Ins for Outlooks' web dialog will be displayed, and the steps are then identical to Windows.

Using the Outlook Add-in (desktop)

Now the add-in is available in the desktop client, the Foldr button will be visible when composing new email messages



Clicking the button will open the Foldr add-in panel on the right of the Outlook interface.



Selecting one of the buttons in the Foldr add-in will open the web sign-in UI where the user can sign in and view the storage available to them through Foldr. The user can browse to individual files to attach to emails or files and folders to create basic or secure links.

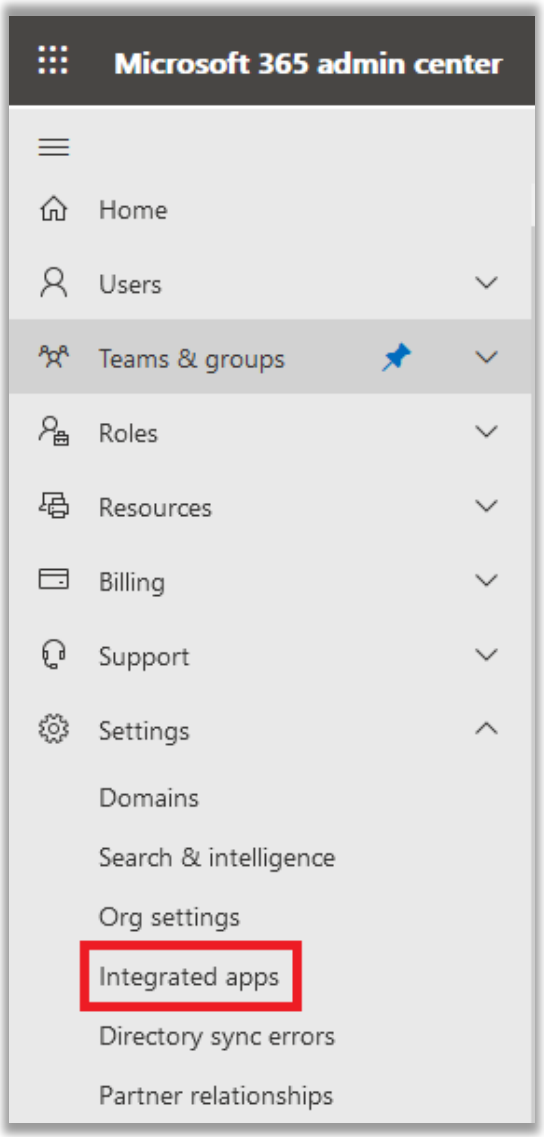
When creating secure links, providing the user has already populated the TO: field in the email, these will be automatically added to the External users field in the sharing UI.

Adding the Outlook app for all users (Office 365 Admin)

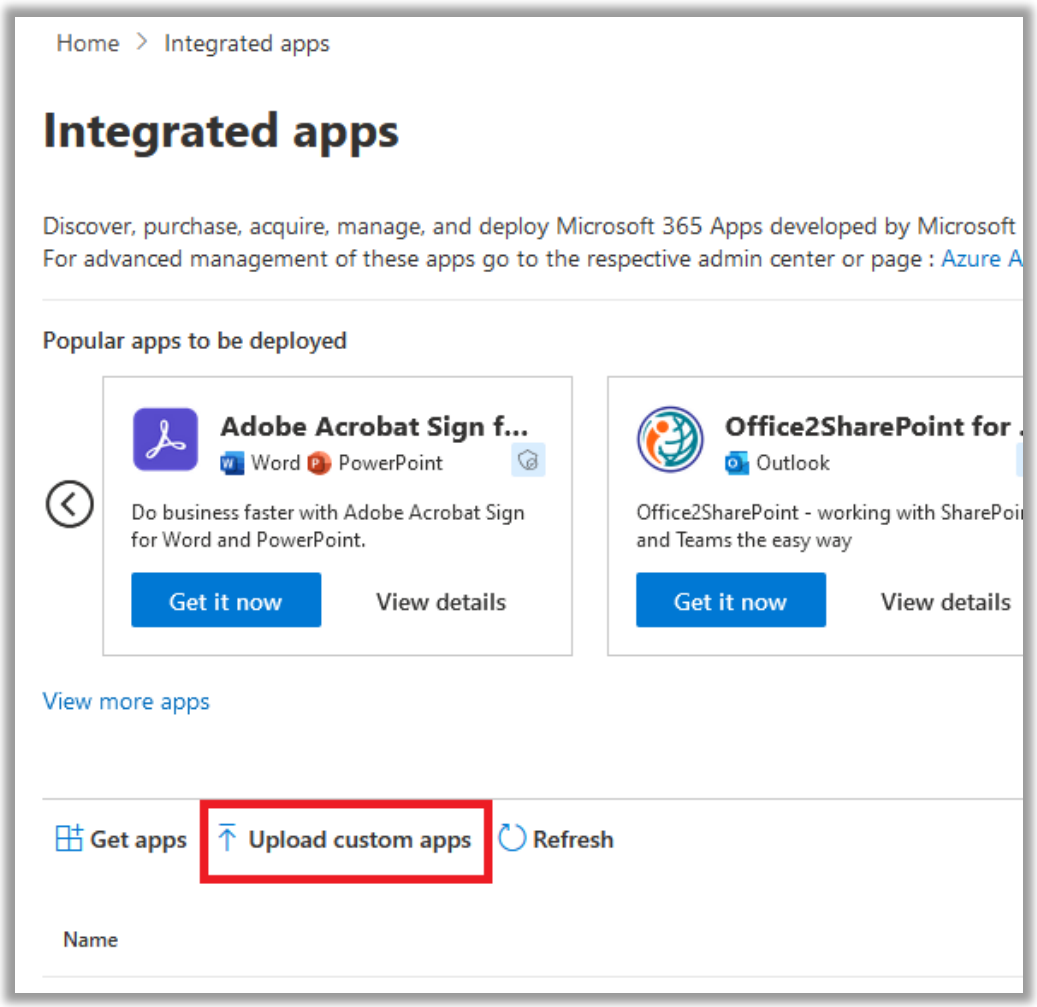
It is possible to add the Outlook add-in for all or selected users/groups in Office 365 so it will be available immediately without the user having to manually add it themselves.

To do this, browse to https://admin.microsoft.com and sign in with the administrative account.

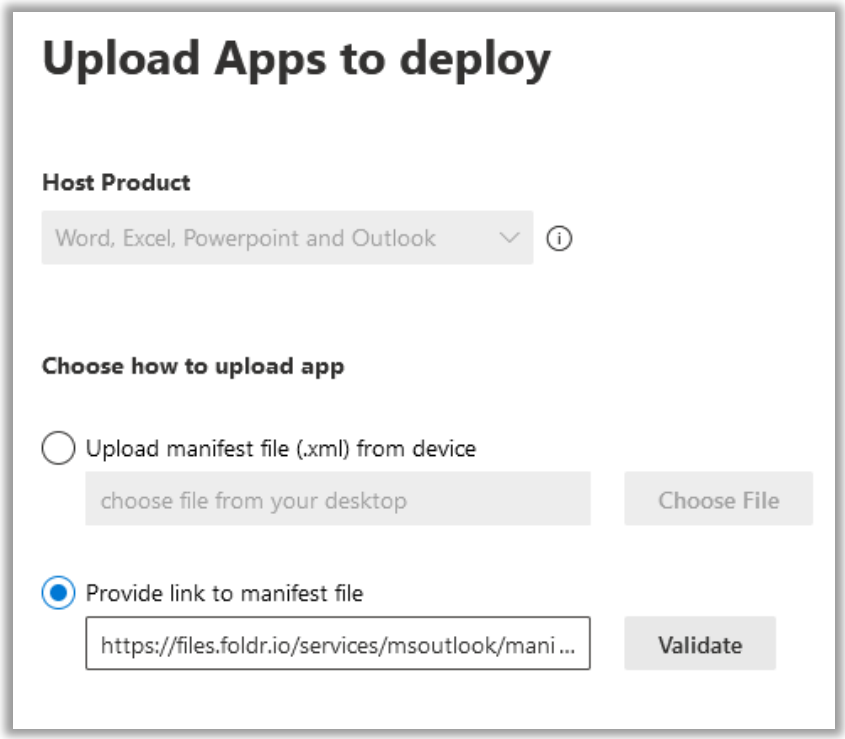
Click **Show All** > **Settings** > **Integrated Apps**



Click **Upload Custom Apps**

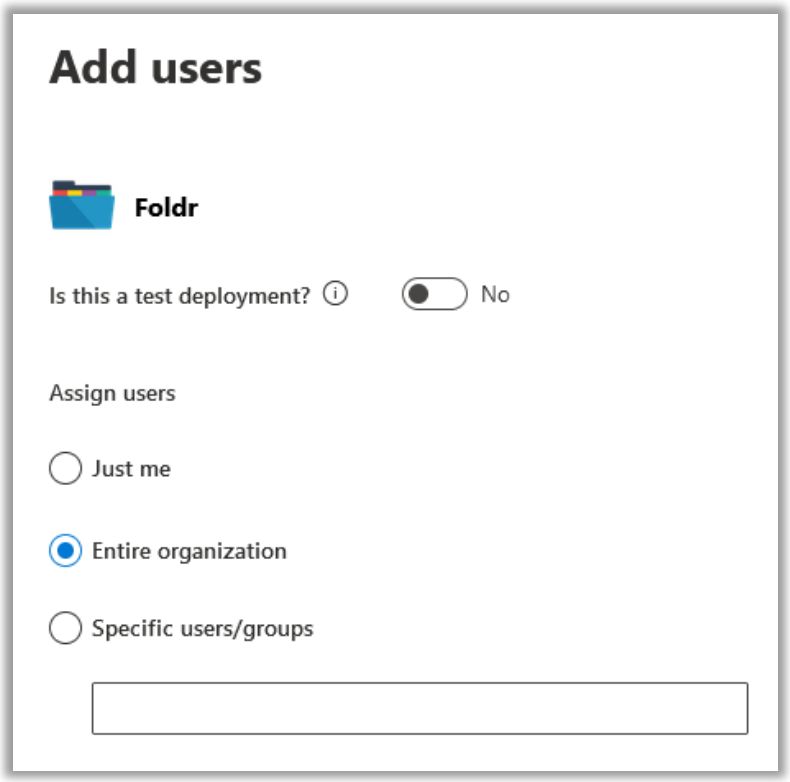


Select '**Provide a link to manifest file**' and enter the URL shown in ***Foldr Settings > Integrations > Microsoft Outlook Add-in***



Click **Validate** and a success message should be shown

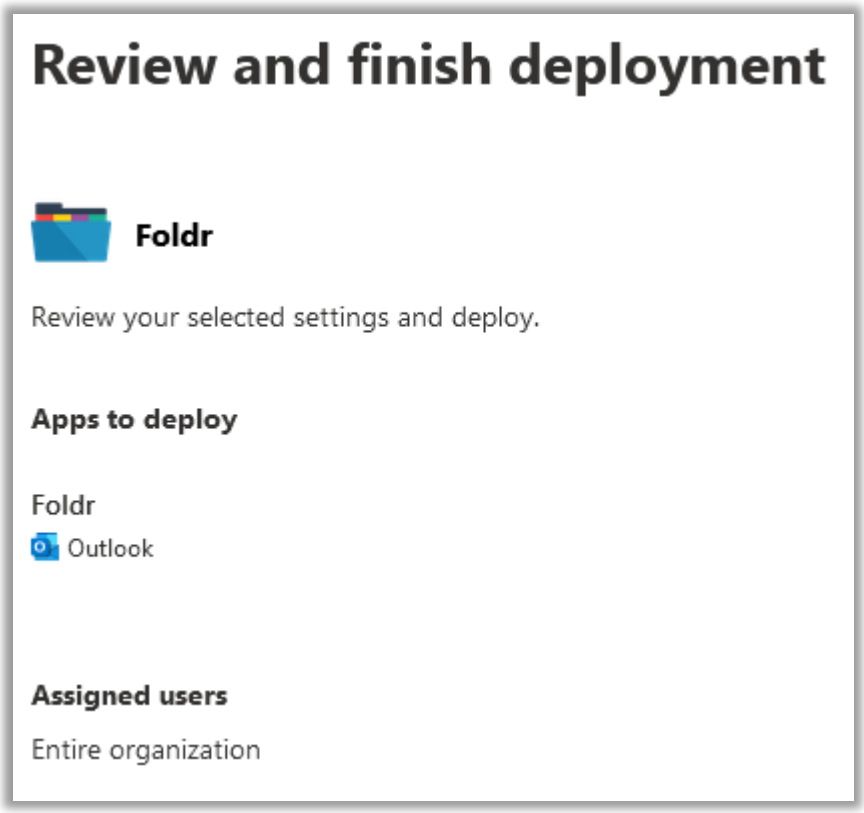
On the next screen, choose which users/groups the app should be made available to, or select the 'Entire organization'



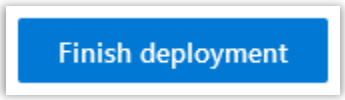
A permission request summary will be shown

Click **Next**

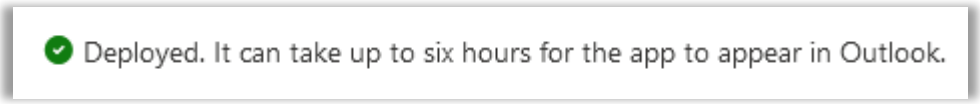
A Review and finish deployment summary will be shown.



Click **Finish deployment**



A message will be shown informing the admin that it may take up to six hours for the Foldr app to be available in the selected users Outlook application. Note that it may take some time to appear in Outlook.



Foldr will now be visible under the Outlook Add-in screen, under Managed apps and should appear automatically for users. Users can initiate and use the Outlook Add-in as shown in the sections above titled 'Using the Outlook Add-in for desktop | web'

Other Cloud Platforms (S3, Dropbox, Box etc)

Dedicated knowledge base articles for integrating other cloud platforms are available on the Foldr online knowledgebase at https//kb.foldr.io

19. Single Sign-On (SSO)

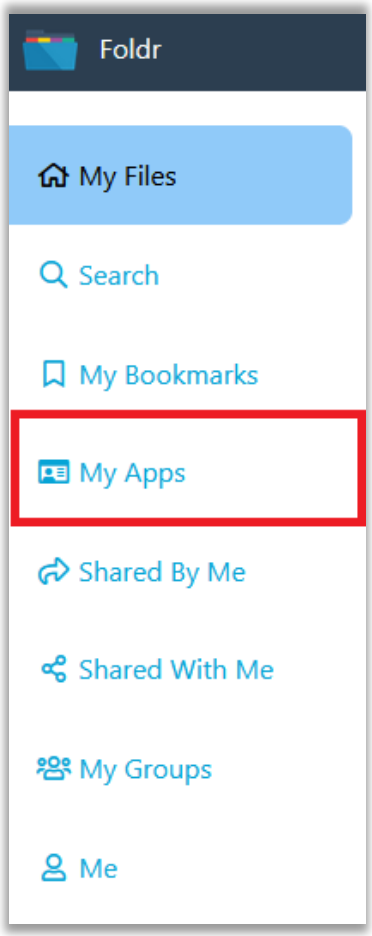
Identity Provider (IdP)

The Foldr server can act as a SAML v2.0 compliant SSO Identity Provider (IdP) or Service Provider (SP). When operating as the IdP, the server can sign Foldr users into other SAML compatible web services, such as Office 365 and Google. If Kerberos SSO is also enabled, domain users can automatically sign into these third-party web services as they are automatically signed into Foldr by default.

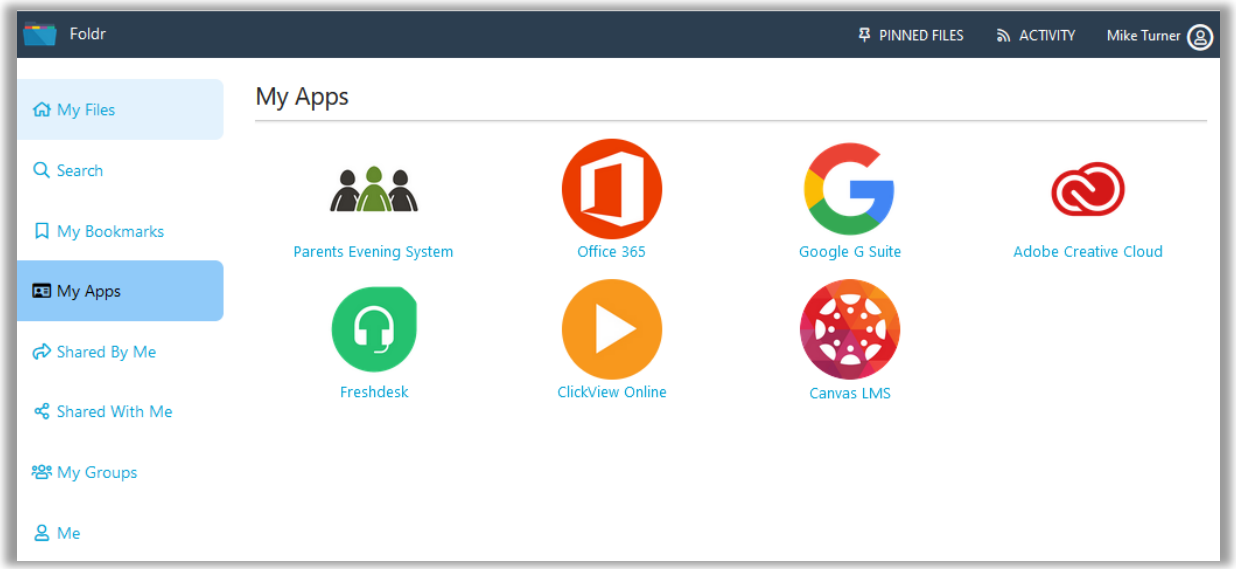
Templates are available for commonly used SPs or new SPs can be configured from scratch.

Once the IdP role has been enabled and configured, the Foldr administrator can enable each configured service to appear in the new 'My Apps' panel in the web interface to provide convenient links to pre-configured SSO services as shown below. If the user clicks the Service Provider (i.e. ClickView) they will be signed in automatically to that web-based service.

My Apps panel



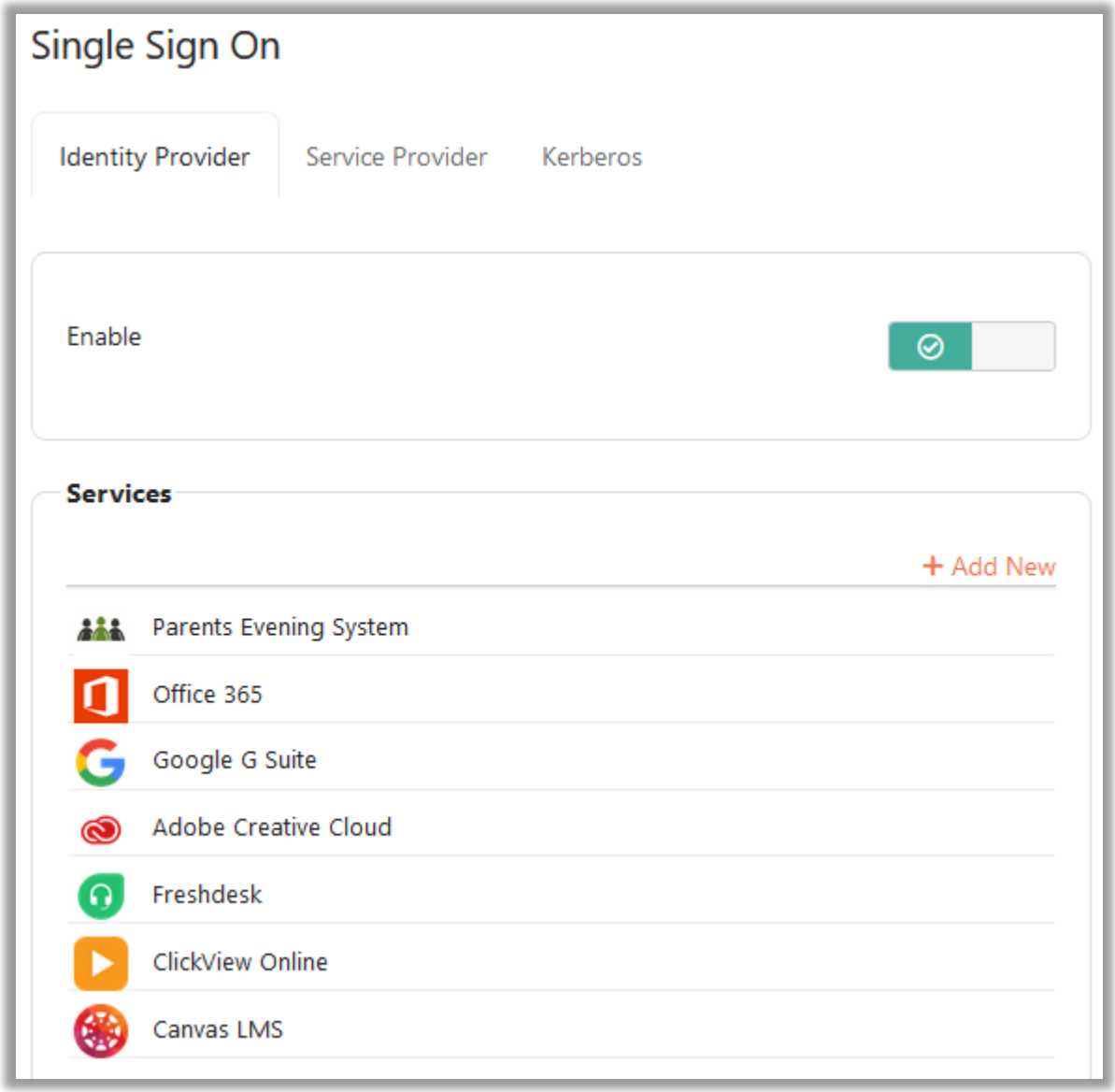
Service Providers in the Web Interface



You can enable the IdP service from within ***Foldr Settings > Single Sign-On > Identity Provider***

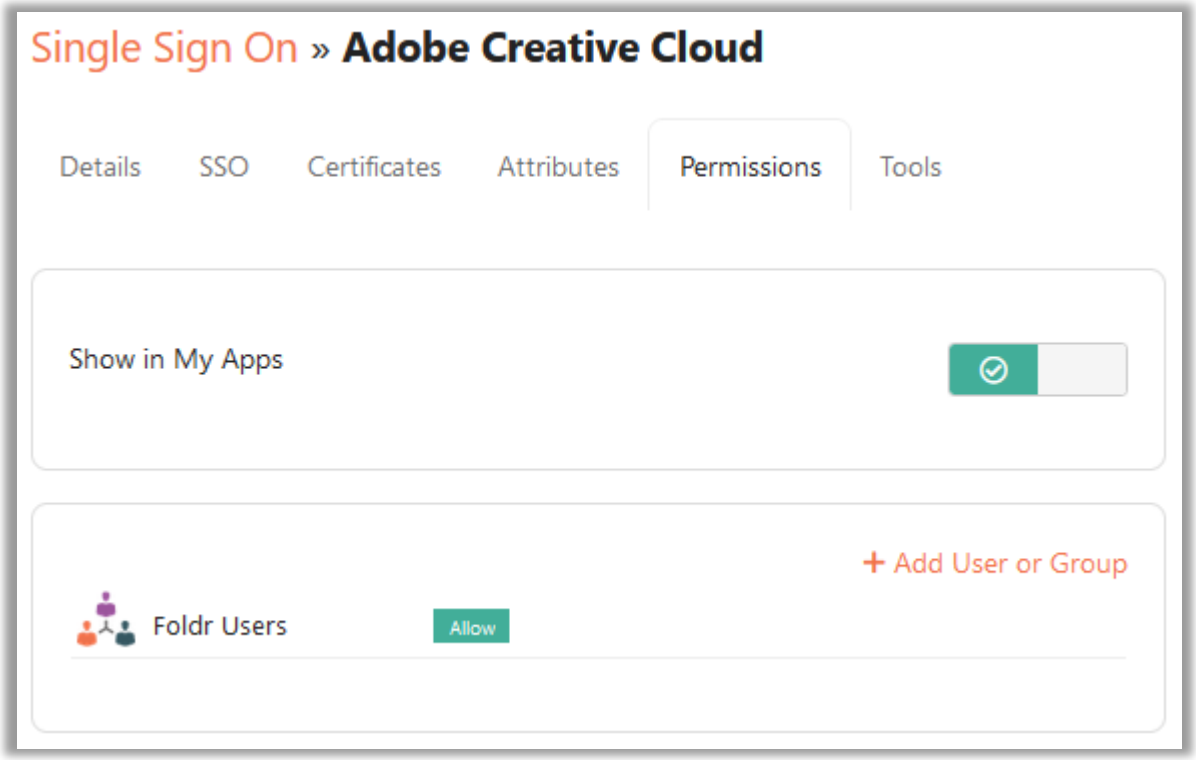
To add a Service Provider (SP), firstly ensure you are browsing Foldr Settings via the URL that the service provider will be connecting to, this is typically the external URI (i.e. do not browse using the internal IP address or internal DNS hostname) and click **+ Add New Service Provider**

Single Sign-On IdP Configuration Screen

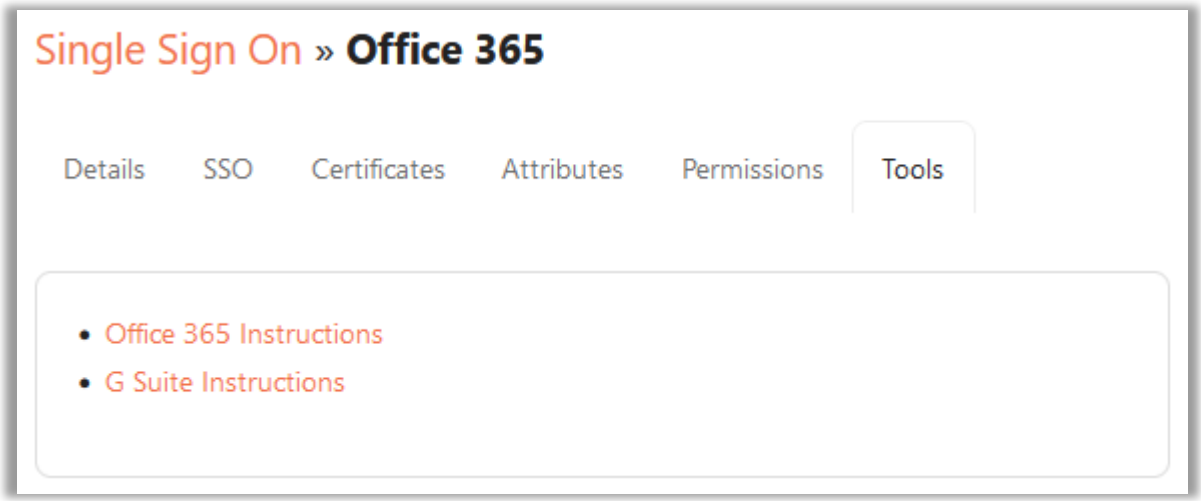


Select the appropriate SP template as required or select NONE if you wish to configure a different third-party SP that is not listed.

Once you have configured your new Service Provider, the administrator can present it to users by using the '**Show in users' My Apps**' toggle within ***Foldr Settings > Single Sign-On*** > Add a Service > Permissions tab



Instructions for Office 365 & G Suite are available under the Tools tab when you are configuring either service.



Any other SAML compatible service can be added to the Foldr IdP, please consult the service providers documentation regarding the required configuration and attributes required to integrate with an IdP such as Foldr.

Service Provider (SP)

When acting as the Service Provider, Foldr provides the ability for users to log in automatically to the Foldr web app without being prompted for their network credentials. In this scenario, the user is signed into another compatible IdP service such as Active Directory Federation Services.

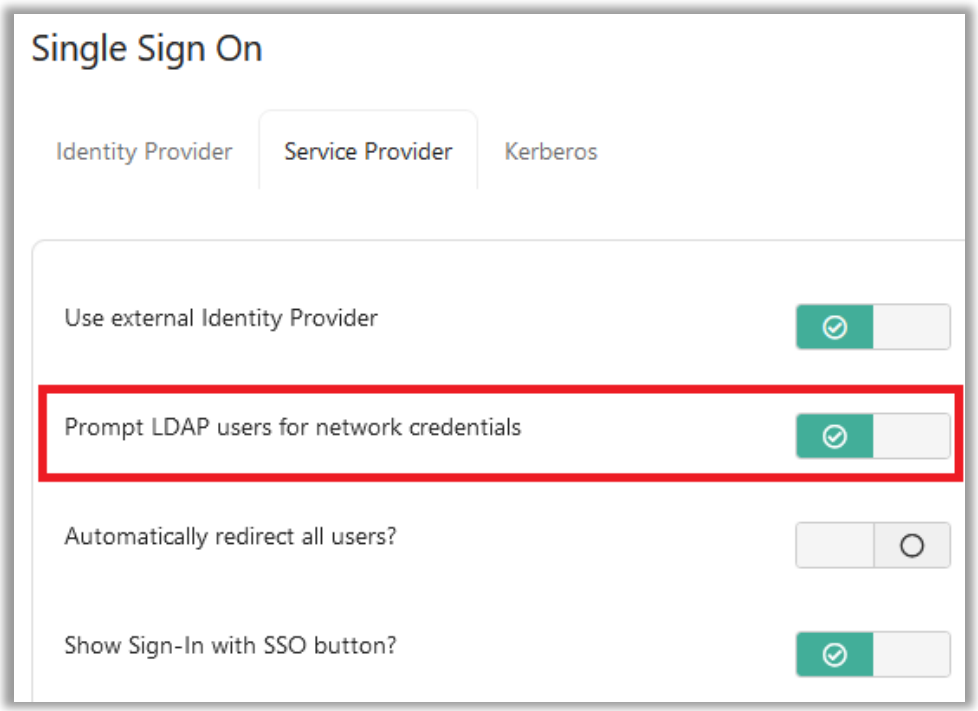
Security Considerations – Service Accounts and Users' Passwords

Active Directory and traditional Windows file services have no concept of SAML or SSO access tokens. As such, when users are signing into the Foldr appliance without directly providing their password to the system, it is not possible for Foldr to provide the usual granular ACL / security permission access to the shares for that user. The administrator has two different options to this problem:

1. Use pre-defined service accounts in the Foldr Settings backend and connect to each configured share with a master service account, ensuring they select 'Use service account for all access' on the share configuration screen. This approach does not allow Foldr to respect a users' actual security permissions and will respect the permissions that apply to the service account user. The administrator can still control read or write access to each share for the service account using the share permissions in ***Foldr Settings > Files & Storage***.

2. (***Recommended)*** – Prompt users for their password the first time they access the system by SSO. Once the Foldr appliance has the user's password, it is encrypted and stored within the configuration database and can then be used for future sessions.

A benefit of this approach is that service accounts are not required for access to SMB shares and Foldr can operate in the normal manner of respecting all existing security ACLs on the file servers providing access to the shares / data. You can enable the prompt for network credentials feature when enabling the SSO service within ***Foldr Settings > Single Sign-On > Service Provider***.



SSO Configuration (Azure/Microsoft Online)

A dedicated KB article for integrating Foldr as a service provider against Azure's IdP is available here.

SSO Configuration (Google)

A dedicated KB article for integrating Foldr as a service provider against Google's IdP is available here.

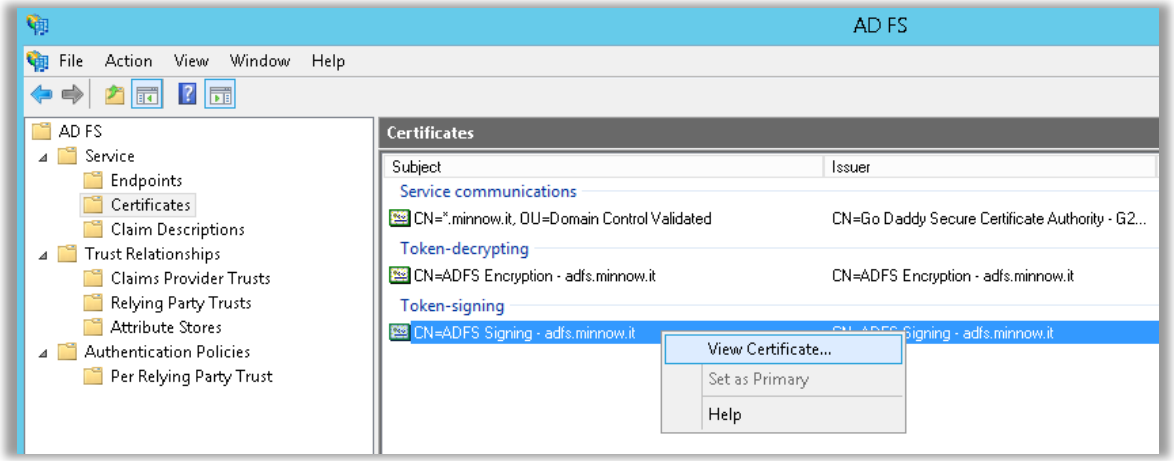
SSO Configuration (AD FS)

The Foldr appliance must have a signed SSL certificate installed before attempting to integrate Foldr as a service provider with AD FS. If the appliance is using the default self-signed certificate, the integration will fail. Should you need to obtain a signed SSL certificate for your Foldr appliance, consider using the free Let's Encrypt SSL option available under ***Foldr Settings > Certificates***. More information is available here

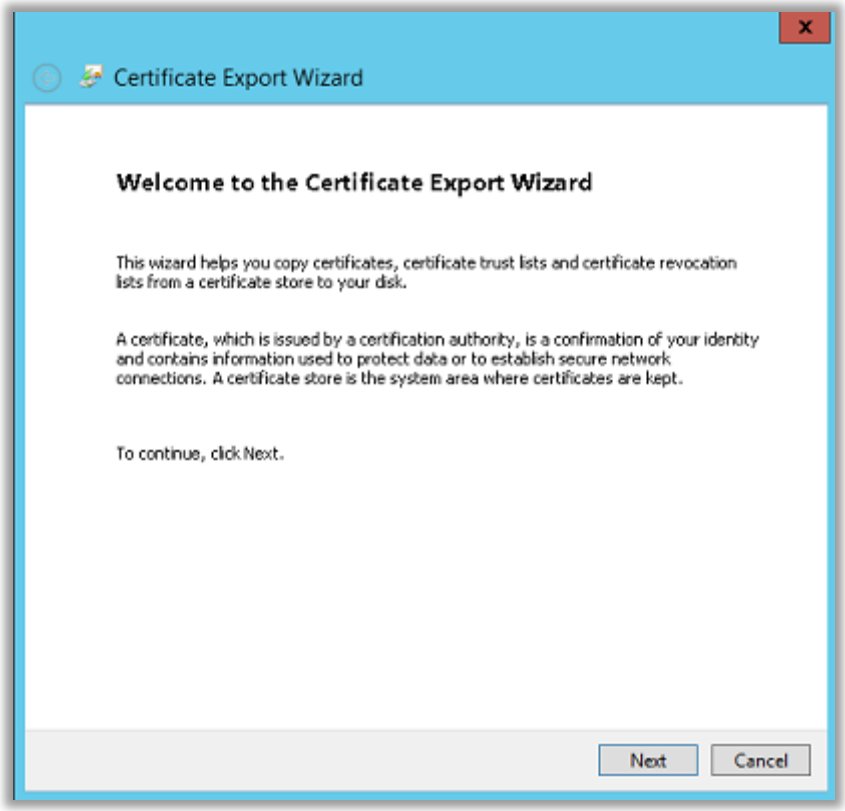
1. **Export the Token-Signing Certificate**

The public certificate used for token-signing in AD FS needs to be installed on the Foldr appliance. To extract a copy of the certificate, open the AD FS management console and navigate to Service > Certificates.

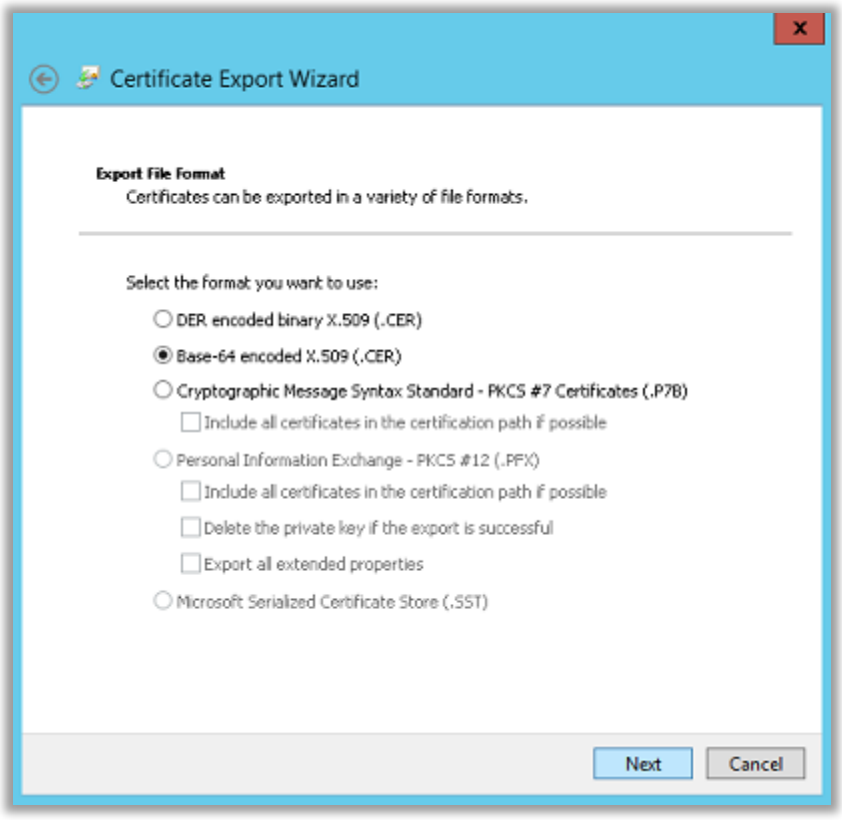
Right click on the Token-signing certificate > View Certificate



Click Next > Details tab > Copy to File and proceed through the export wizard.



Select **Base-64 encoded X.509 (.CER)** and click Next



Select an export destination and file name > click Save to save the certificate

2. **Enable SSO on the Foldr appliance and import the token-signing certificate**

Enable Foldr as a Service Provider within ***Foldr Settings > Single Sign-On > Service Provider*** (Example settings for AD FS are shown below)

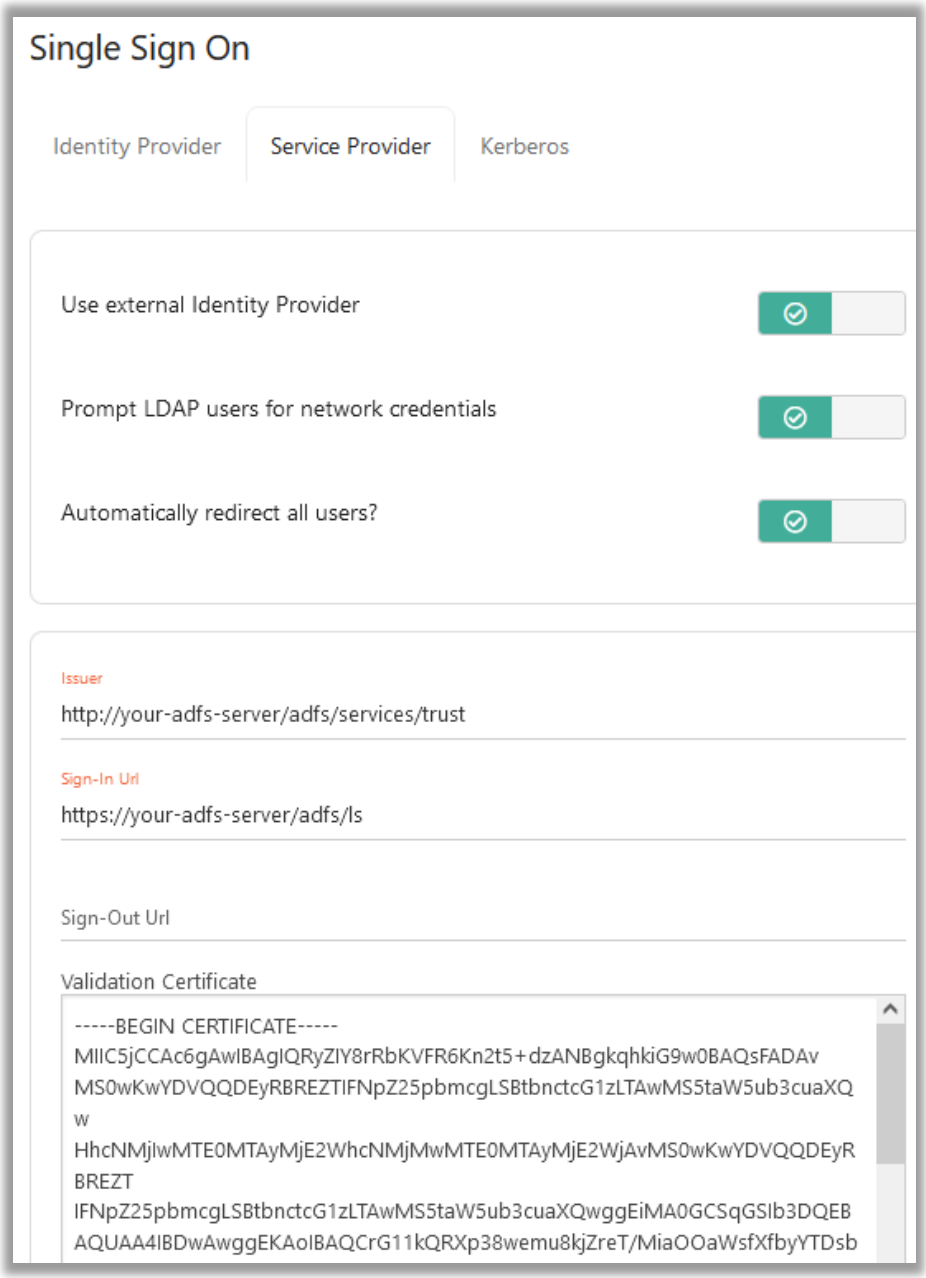
Issuer = http://your-adfs-server/adfs/services/trust

Sign-In URL = https://your-adfs-server/adfs/ls

Validation Certificate

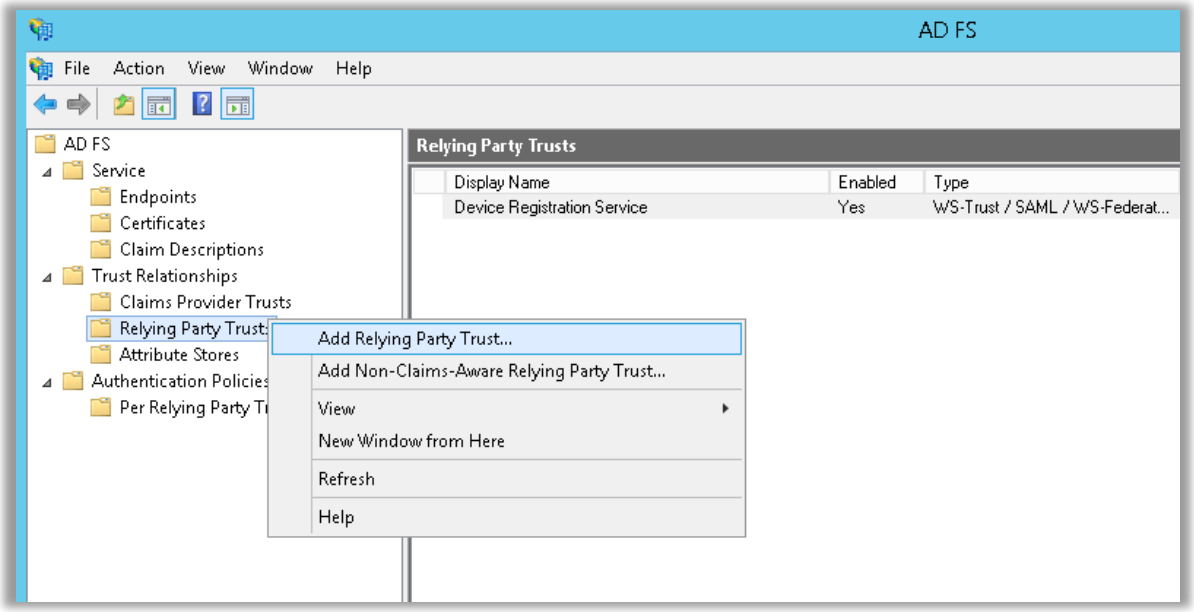
The token-signing certificate used by AD FS that was extracted above must be opened in a text editor and entered here.

Foldr Settings SSO Service Provider Configuration Screen



3. Add the Relying Party Trust to AD FS

Within the AD FS management console, go to Trust Relationships > Relying Party Trusts > Right click > Add Relying Party Trust



Select 'Import data about the relying party published online or on a local network' and enter the Federation metadata address as below and click Next – (replace ***address-of-foldr*** with the URL to your installation)

https://address-of-foldr/sso/sp/metadata

Note 1 – A signed SSL certificate must be installed on the Foldr appliance otherwise this step will fail.

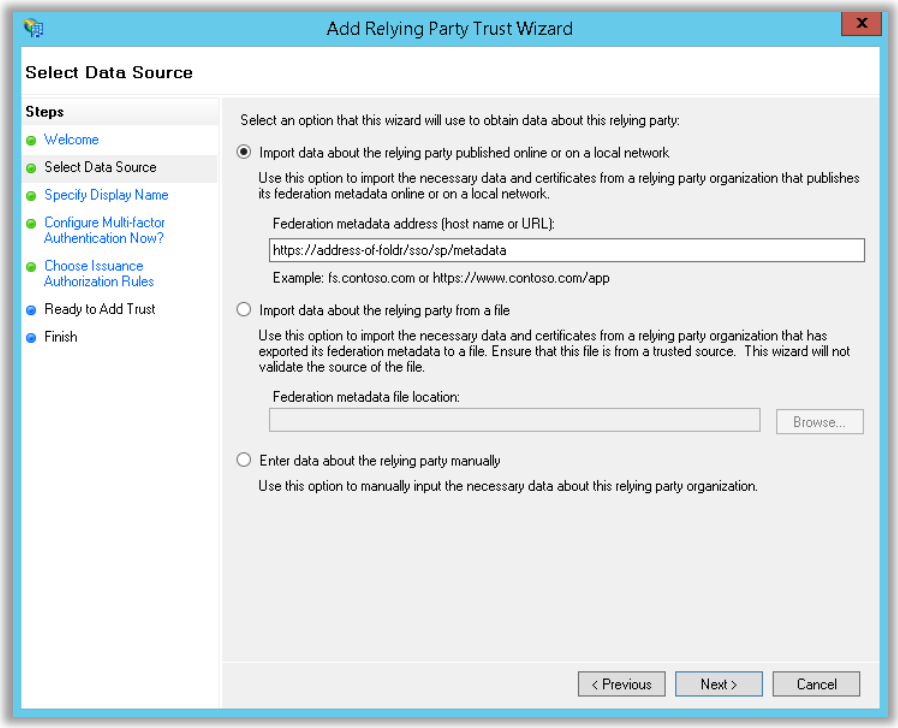
Note 2 – Foldr uses TLS 1.2 exclusively and the Microsoft AD FS Wizard attempts to connect using TLS 1.0 to retrieve metadata. There are various ways of resolving this on the AD FS end, so it connects using TLS 1.2 however these are outside the scope of this guide. A workaround is to simply re-enable the legacy TLS protocols in Foldr, import the metadata and then disable them again.

To re-enable TLS 1.0, 1.1 (1.2 will remain enabled) run the appliance console command:

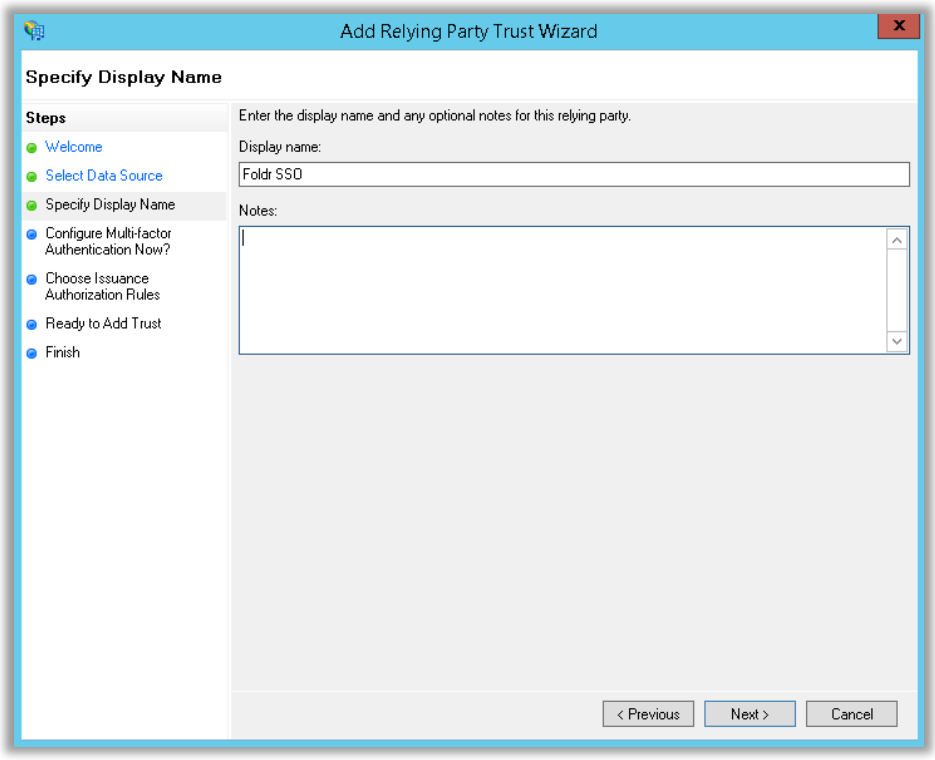
```
set-ciphers legacy
```

To disable TLS 1.0 and 1.1 and put Foldr back into its default SSL configuration run the command:

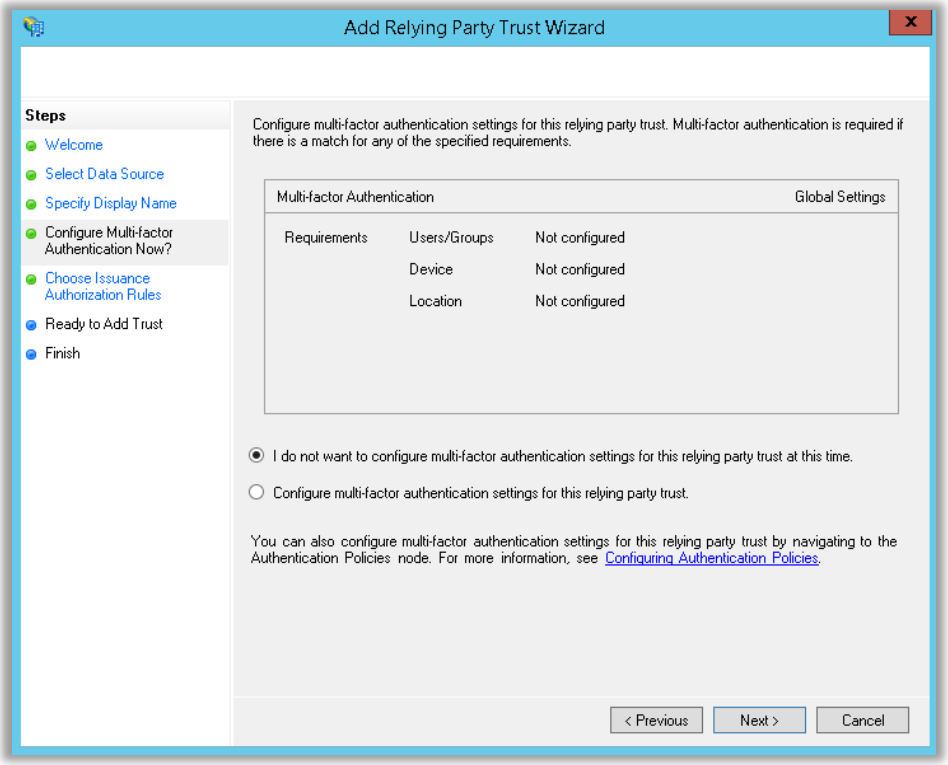
```
set-ciphers modern
```



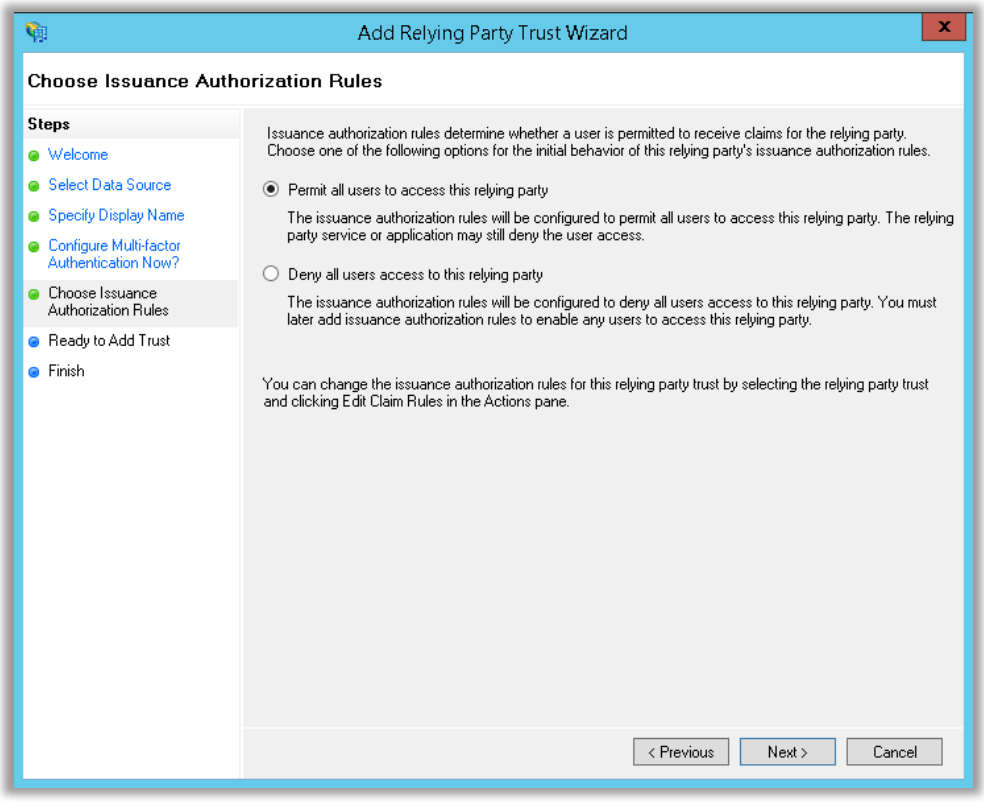
Enter a Display name and click Next.



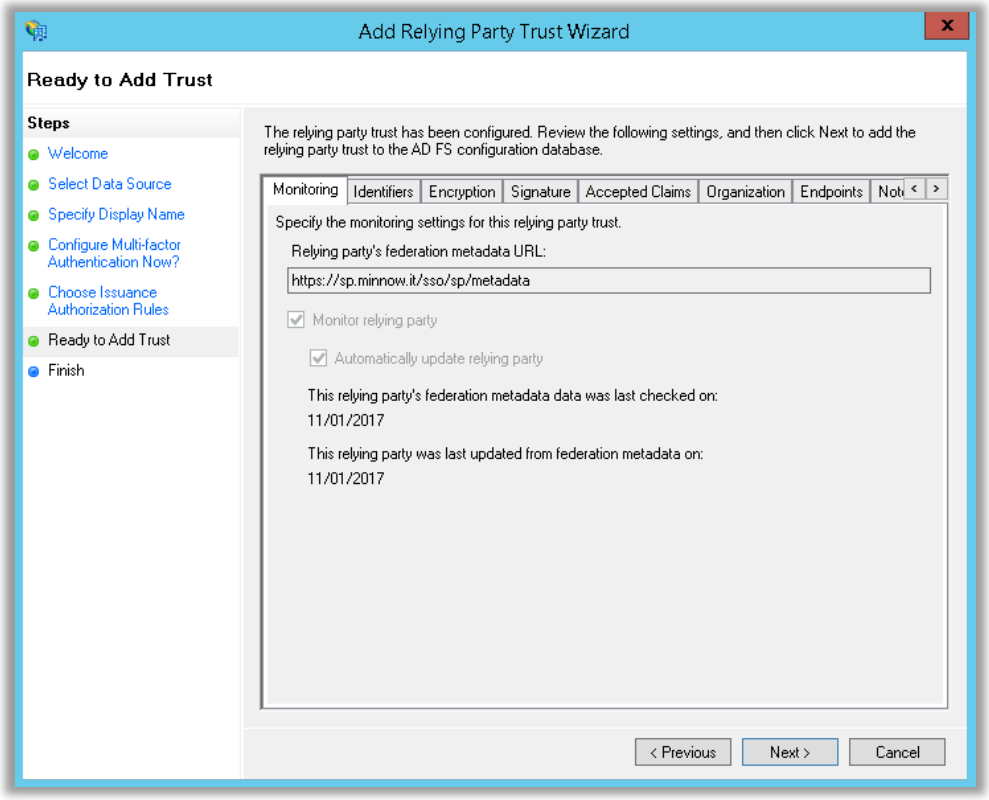
Configure Multi-Factor Authentication options if used, otherwise leave as default (shown below) and click Next.



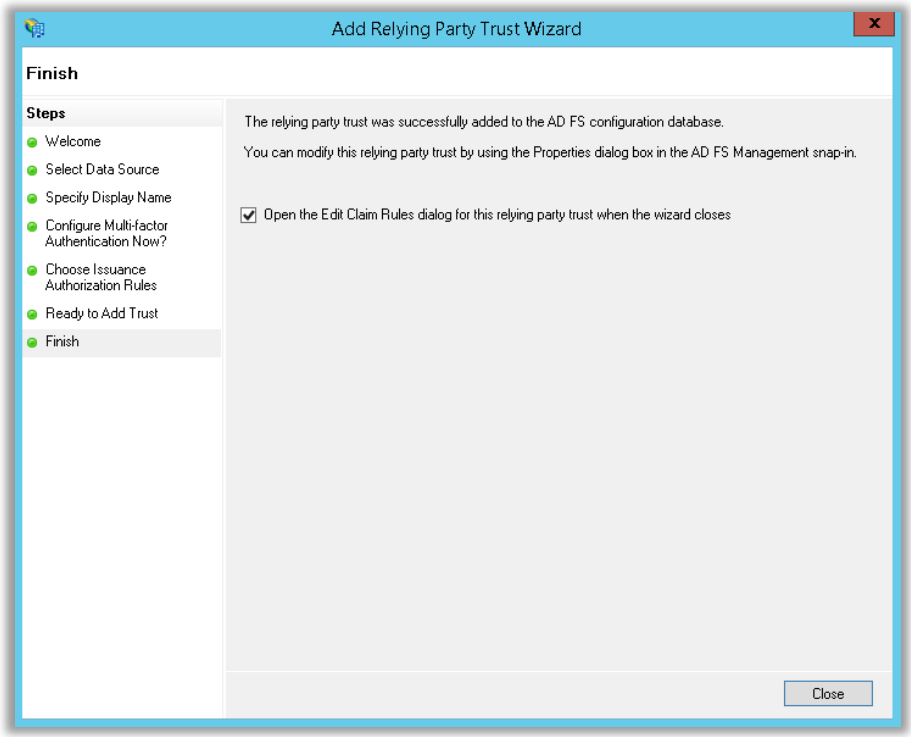
Configure Issuance Authorization Rules as required. Generally, this would be left as 'Permit all users to access this relying party' > Click Next



You can confirm the configuration that has been obtained from the metadata URL by using the tabs in the Ready to Add Trust dialog. When you are ready to proceed, click Next

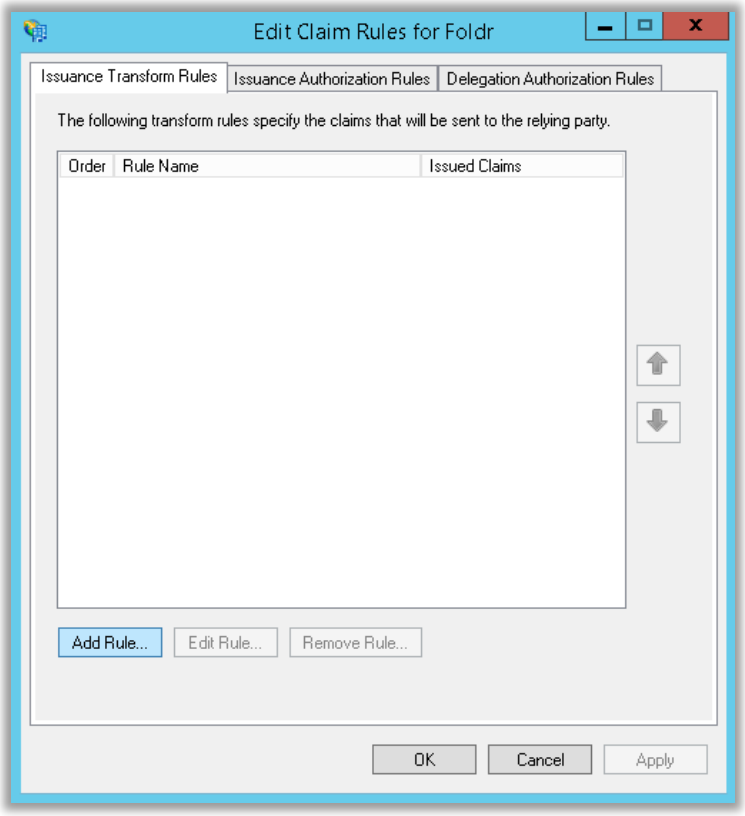


Leave '**Open the Edit Claim Rules**' checkbox ticked and click Close.

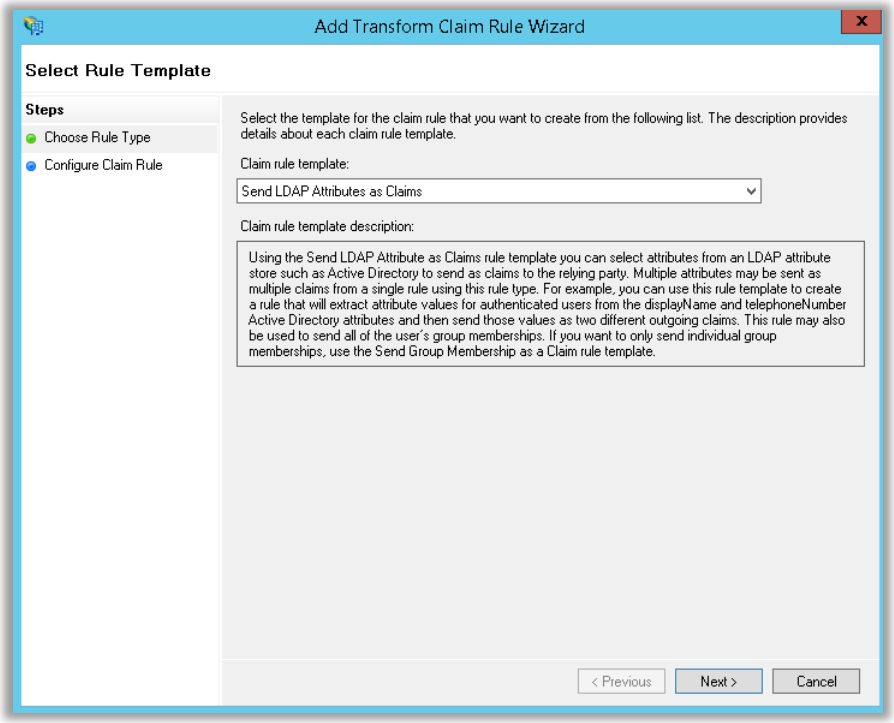


4. **Configure the Claim Rules for Foldr**

Click '**Add Rule**' on the Issuance Transform Rules tab

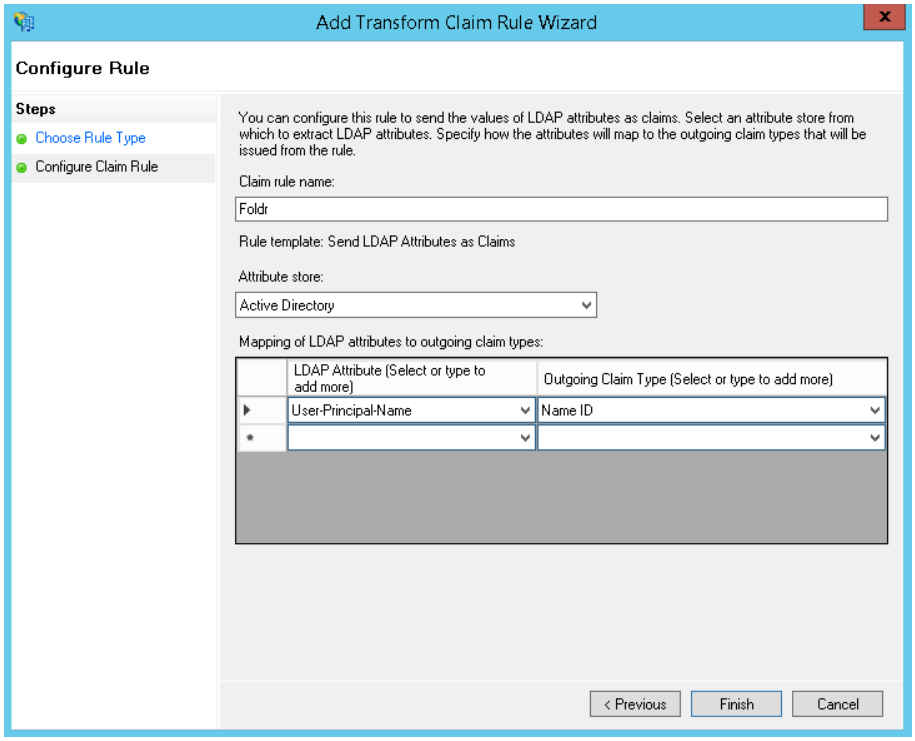


Select '**Send LDAP Attributes as Claims**' from the template drop-down menu



- Enter a suitable Claim rule name
- Select '**Active Directory**' from the Attribute store

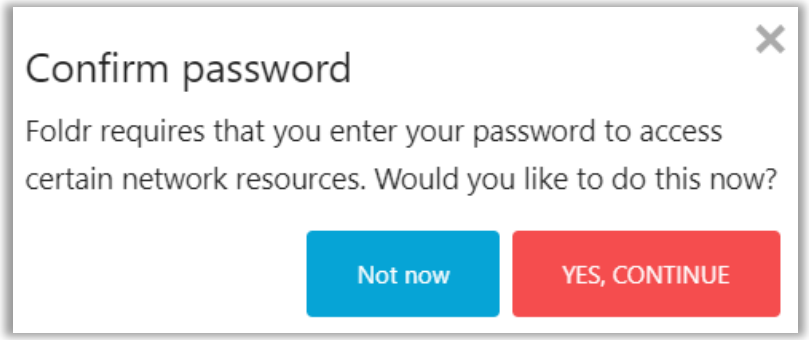
Finally, from the **drop-down menu** map the LDAP Attribute '**User-Principle-Name**' to Outgoing Claim Type of '**Name ID**' > Click Finish.



Single sign-on configuration should now be complete. If a user visits the Foldr appliance URL and they are not signed into AD FS they will be redirected to the AD FS sign-in page. If the user is already signed into AD FS, they should automatically log into Foldr and be presented with their shares.

If the administrator has enabled '***Prompt users for network credentials***' in the Foldr Single Sign-On > Service Provider configuration screen, the user will see the following prompt the first time that they sign in automatically by SSO. It is important that the user supply their password at this time if any SMB shares are being presented to users (where service accounts and 'use for all access' isn't being used). Failure to supply the password will result in SMB shares being missing from the My Files storage list.

Confirm password dialog for SMB share access:



When the user clicks Yes, Continue an update password prompt will be displayed.

Should the user cancel the dialog and not provide the password, they will be prompted to provide it the next time they sign in. A user can change or update their Active Directory password at any time using the ME menu in the Foldr web app.

Kerberos SSO

Foldr can be configured to authenticate users using Kerberos authentication. This provides a convenient way to automatically sign users into Foldr if they are using a PC or Mac that is bound to Active Directory. With Kerberos SSO, a user can sign in automatically to either the Foldr web app or Windows / macOS drive mapping clients. Kerberos SSO is not supported in the iOS or Android apps.

To use Kerberos authentication, the Foldr appliance must have accurate system time – i.e. it must be in sync with the Active Directory domain. You can check the appliance time from within Foldr Settings (show top right of the UI) or by running the date command from the console when signed in as fadmin. Should you need to correct the appliance time, this can either be done by correcting the host clock (VMware ESXi etc) or if using NTP in ***Foldr Settings > Appliance > Date & Time*** and obtain time from a local domain controller.

You can force the appliance's clock to be synchronised with an NTP time source using the console command:

time-sync x.x.x.x

SSL Certificate Requirements

A signed SSL certificate must be installed on the Foldr server for Kerberos authentication to work successfully. You can install a purchased signed certificate from a recognised provider or make use of the free SSL service offered via the Let's Encrypt CA. The default, self-signed or other 'untrusted' certificate cannot be used.

Internal DNS changes should be made to allow clients using Kerberos to connect to the Foldr server using the URI protected by the SSL certificate. This is covered later in this section.

Enabling Kerberos authentication and binding the appliance to the domain.

1. Log onto the Foldr appliance console and issue the command:

   krb5-enable <Active Directory FQDN> <Domain Controller FQDN> <Foldr Appliance FQDN> <Foldr Appliance Hostname> <AD Account to join Foldr to domain>

Example:

```
krb5-enable minnow.it dc-01.minnow.it foldr-v4.minnow.it foldr-v4
administrator
```

2. Enter the Active Directory account password
3. The Foldr appliance will bind to the domain and a computer account object will be created in the default Computers container in Active Directory.

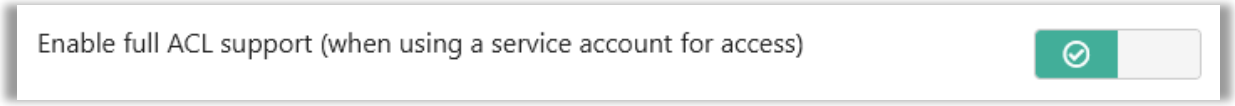
Security Considerations – Service Accounts and User Passwords

When a user signs into Foldr using Kerberos, the appliance still needs user credentials to connect to the backend SMB storage such as those hosted on Windows file servers. The administrator has two different options to this problem:

1. Use pre-defined service accounts in the Foldr Settings backend and connect to each configured share with a master service account. To use this option this administrator must select a suitable service account in ***Foldr Settings > Files & Storage*** and then enable 'Use service

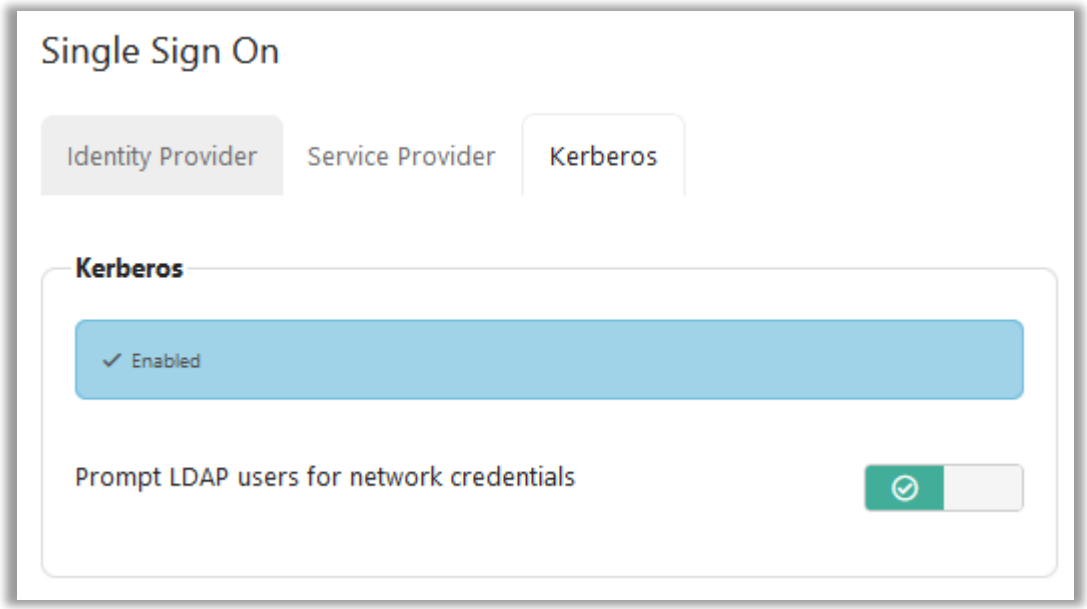
account for all access' on the advanced tab in the share configuration screen

If the administrator also enables 'Full ACL support' on the advanced tab, the appliance will connect to the storage using the service account credentials, but then parse the Windows ACLs to provide the correct permissions for the user signed into Foldr.



If full ACL support is not enabled, Foldr will not respect the users' actual security permissions but instead provide the level of permission that applies to the service account user. The administrator can still control read or write access to each share for the service account using the permissions section in ***Foldr Settings > Files & Storage***.

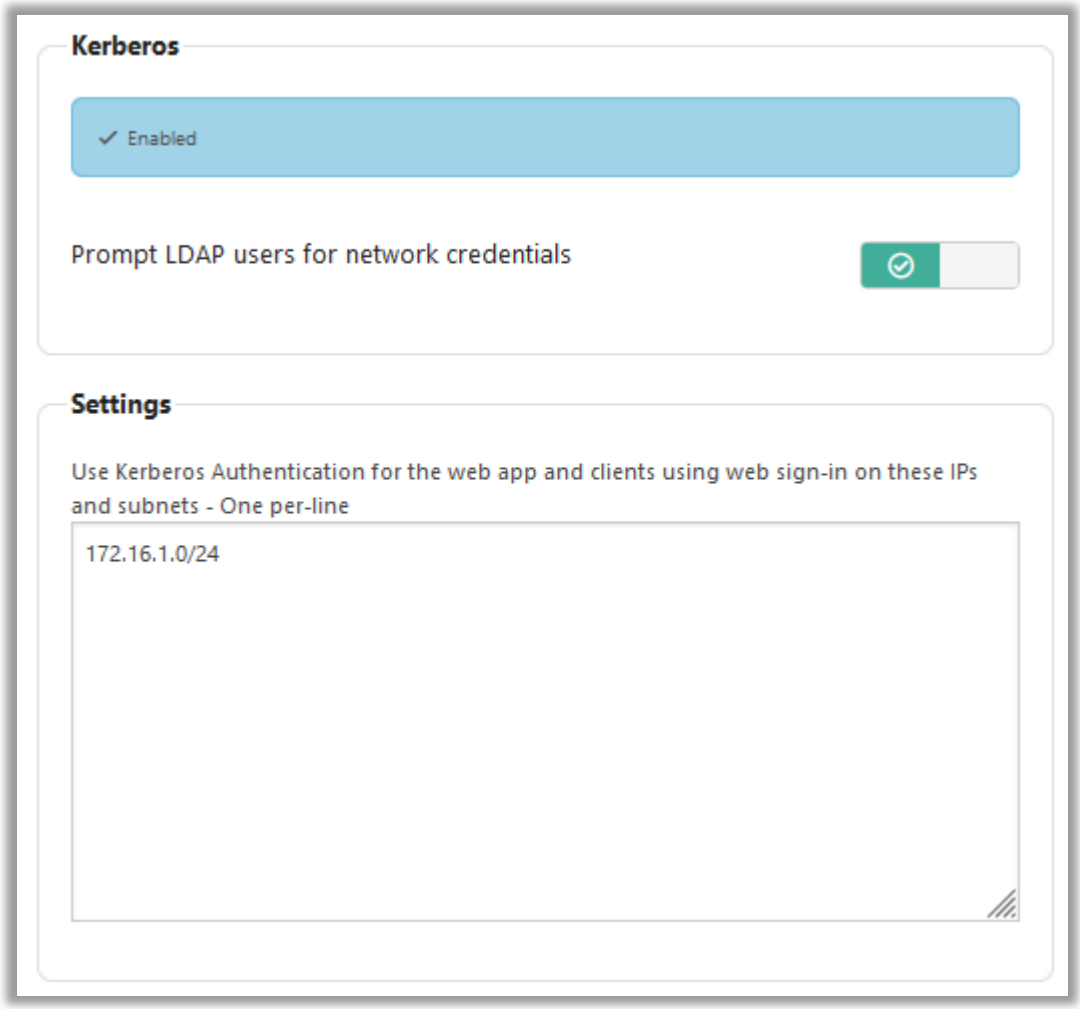
2. Prompt users for their password the first time they access the system by Kerberos SSO. Once the Foldr appliance has the user's password, it is encrypted and stored within the configuration database and can then be used for future sessions. A benefit of this approach is that service accounts are not required for access to SMB shares and Foldr can operate in the normal manner of respecting all existing security ACLs on the file servers providing access to the shares / data. You can enable the **prompt for network credentials** feature when enabling the SSO service within ***Foldr Settings > Single Sign-On > Kerberos***.



Specify the subnets to be used for Kerberos SSO

IMPORTANT – The IP addresses or subnets configured here applies to the web app and desktop apps using **web sign-in.**

Within ***Foldr Settings > Single Sign-on > Kerberos*** you should now configure the subnets (or even individual IP addresses) that clients will be connecting that should use Kerberos SSO. Configure one subnet / IP address per line.

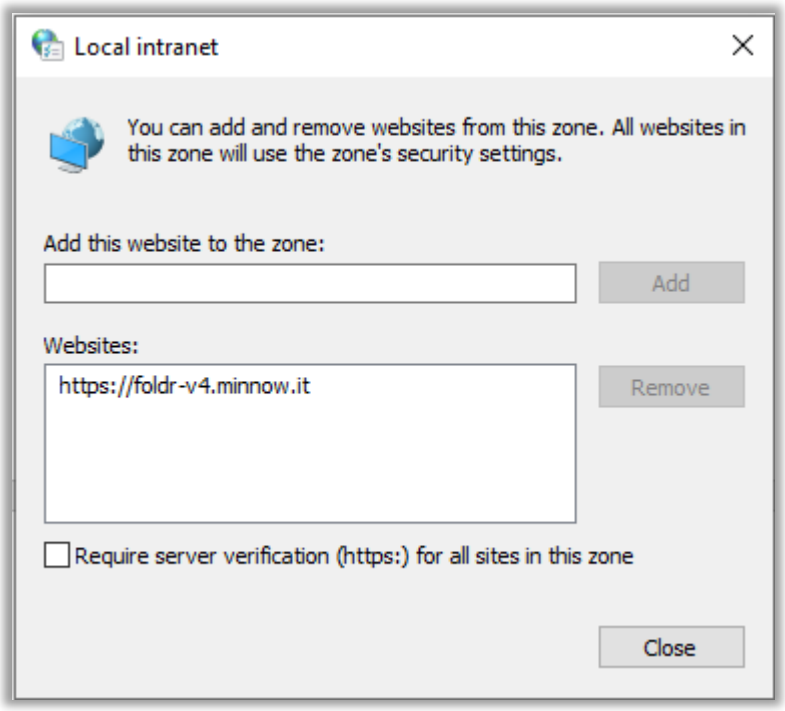


Click **Save**.

Windows Client Configuration (Applies to web app and apps using 'web sign-in')

The Foldr appliance URI must be added to the workstations **LOCAL INTRANET** zone before they are able to use Kerberos SSO in the web browser interface.

Control Panel > Network and Internet > Internet Options > Security tab > Local Intranet > Sites > Advanced



Once this change has been made Internet Explorer, Edge, Google Chrome and Firefox and their variants should sign into the Foldr web app automatically. Other browsers may not be compatible.

These settings can be controlled in a domain environment through Group Policy.

macOS Client Configuration

No client configuration is required on a domain bound macOS computer when using SSO in the Safari browser.

To use Google Chrome browser with Kerberos based SSO, you must run the following commands from the macOS terminal, replacing “foldr-server.fqdn” with the URL of the Foldr appliance.

```
defaults write com.google.Chrome AuthServerWhitelist “foldr-server.fqdn”
```

defaults write com.google.Chrome AuthNegotiateDelegateWhitelist “foldr-server.fqdn”

Authentication Fallback

Should you attempt to connect to web app from within a Kerberos SSO specified subnet, but the machine is not domain bound, you will be presented with a standard authentication prompt. If valid credentials are entered into the prompt, the web app will sign in as usual.

SSL Certificates and Domains

It is common to use different domain names inside an organisation (Active Directory) and externally (for the public website, email etc). Due to the way Kerberos works, accessing Foldr via the internal FQDN will work by default, however it will also present the user with unwanted SSL trust warnings in the browser that must be accepted before signing in.

In order to do this, assuming that one does not already exist, you must create a forward lookup zone on the internal DNS service (typically a Windows domain controller) for the EXTERNAL / PUBLIC domain and create a CNAME record pointing at the internal FQDN of the Foldr system. A CNAME in DNS is an alias and as such does not break Kerberos authentication in the same way that a simple A record would.

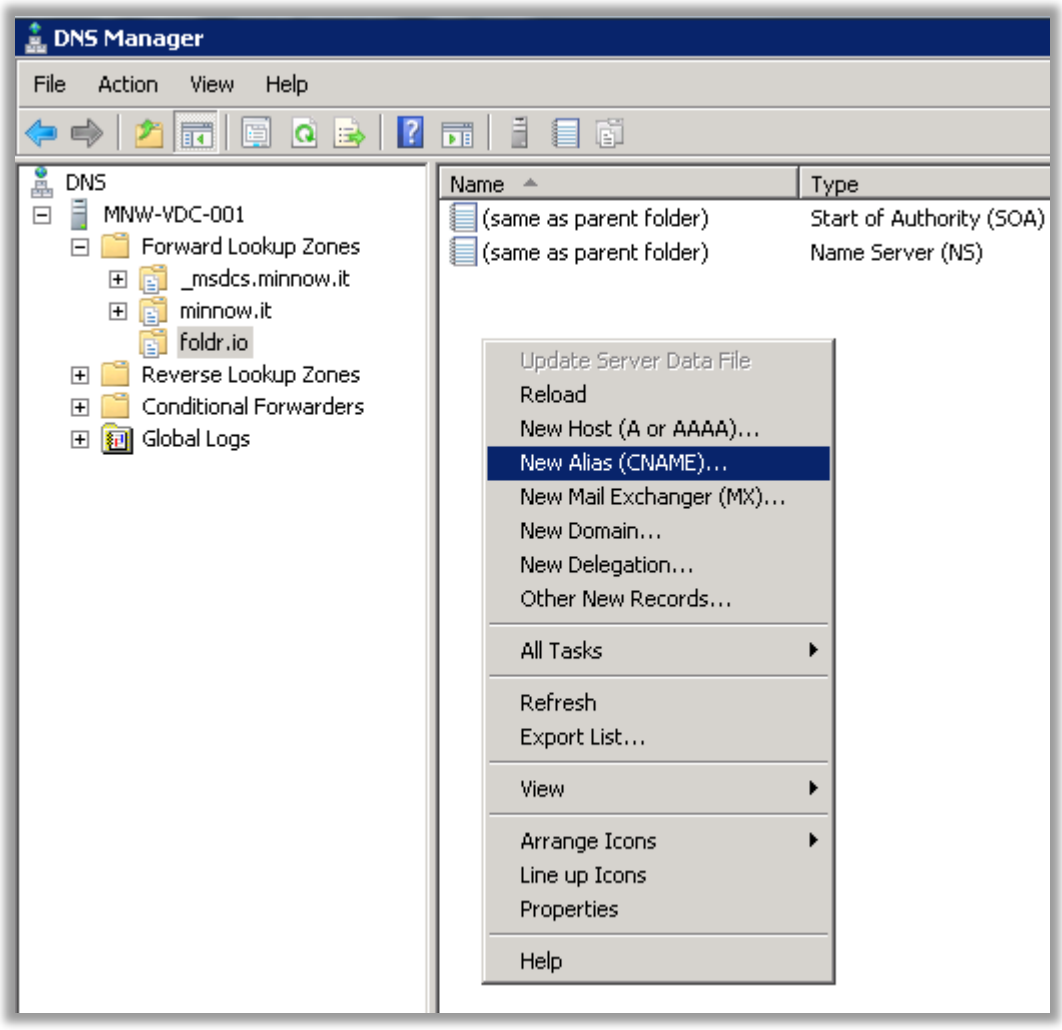
Creating the CNAME record

In the example below, the domains are as follows:

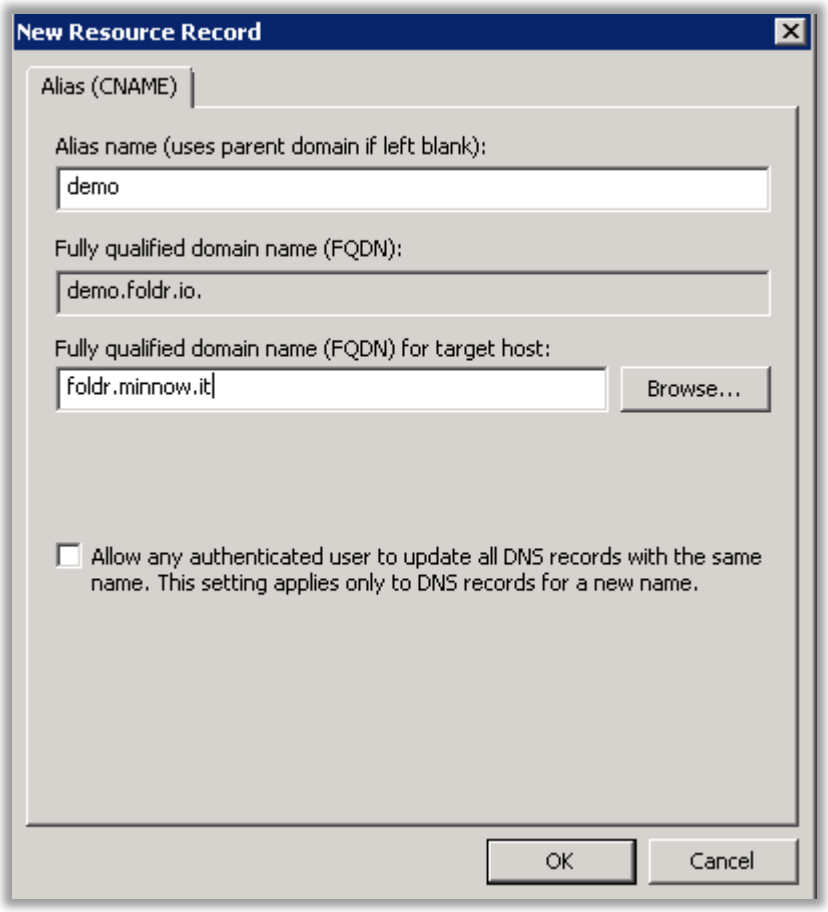
minnow.it = The internal Active Directory domain with a Foldr appliance accessible at foldr.minnow.it. An A record already exists in this zone for 'foldr' pointing at the virtual appliance.

Foldr.io = The organisation's public domain.

After creating a new lookup zone for foldr.io, right click in the zone and select 'New Alias (CNAME)

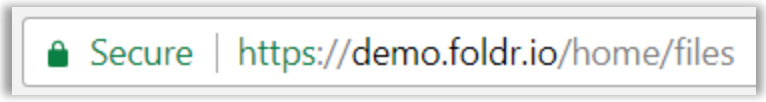


Enter the public FQDN of the appliance (i.e. that is covered by the SSL certificate installed on the appliance) and point this at the internal FQDN (foldr.minnow.it)



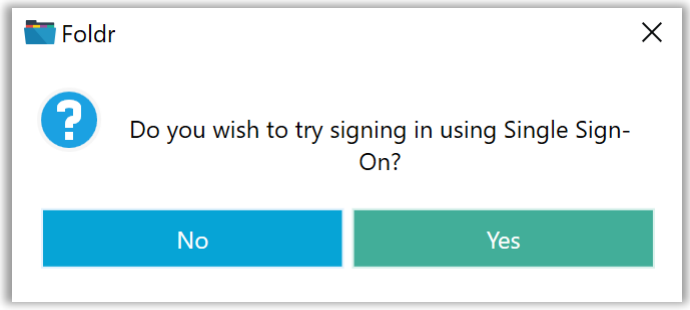
IMPORTANT – When creating the new lookup zone on the internal DNS service for the organisation's public domain, you must also consider any other records that need to be created. Typical examples are the public website, webmail servers and so on. Create records for each as required and point them at the relevant public IP address.

If you now browse to the Foldr server at https://demo.foldr.io on a domain bound workstation, the SSL certificate will validate, and it will sign in automatically with Kerberos authentication.



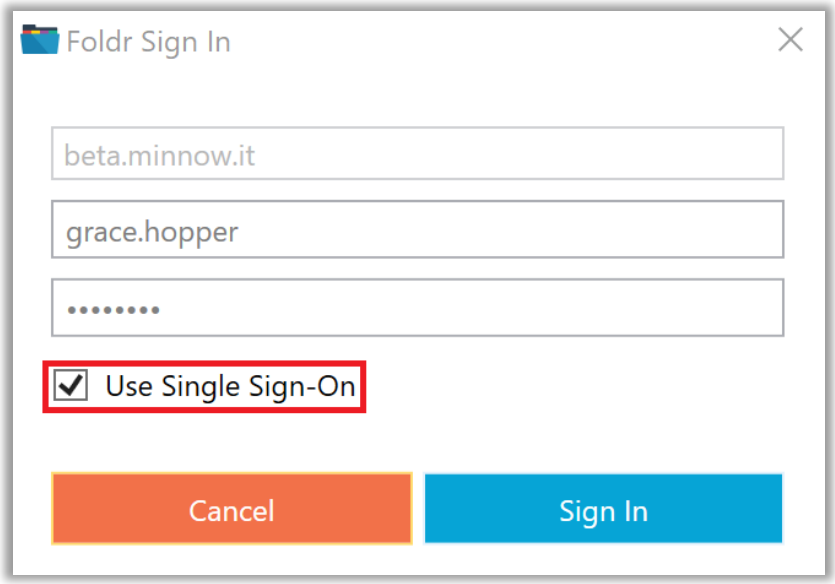
Windows App Configuration (Drive Mapping Client)

The Windows app will automatically detect if Kerberos SSO is available (i.e. is it enabled on the server and does the client have a valid Kerberos ticket) and prompt the user:



If the user selects No, they can still authenticate by manually entering their credentials.

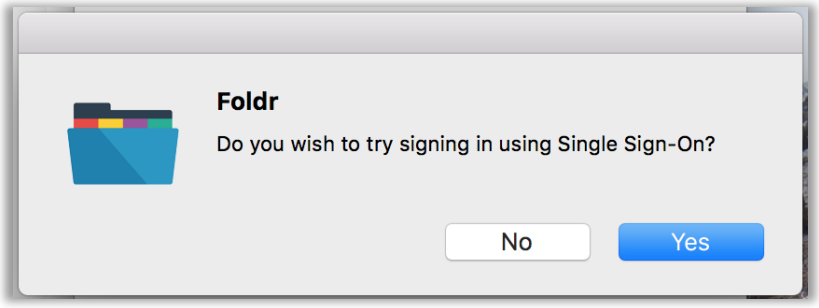
If Web Sign-In is disabled on the server, the app will display the legacy / alternative login dialog and the user can enable the checkbox as shown to attempt SSO sign-in.



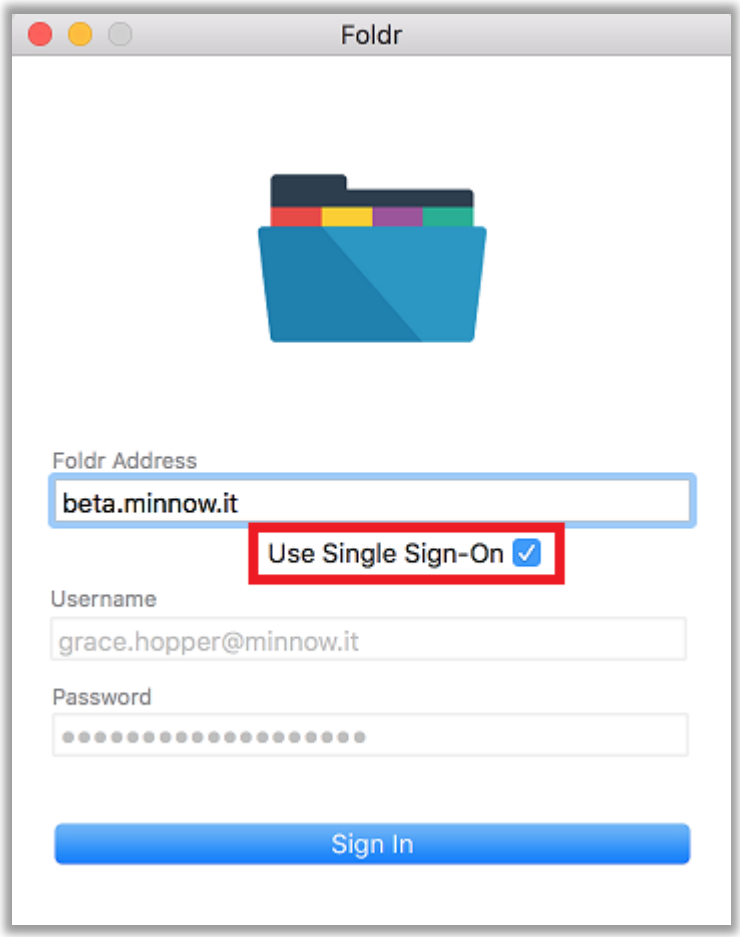
Kerberos SSO can set as the default authentication method through an MSI option when deploying the client (SSO_LOGIN_BY_DEFAULT=1) – More information on deploying the Windows application and the available MSI options can be found in the following KB article

macOS App Configuration (Drive Mapping Client)

The macOS app will automatically detect if Kerberos SSO is available and prompt the user (i.e. is it enabled on the server and the client has a valid Kerberos ticket by being signed into the domain)



If the user selects No, they can still authenticate by manually entering their credentials. If Web Sign-In is disabled on the server, the app will display the legacy / alternative login dialog and the user can enable the checkbox as shown to attempt SSO sign-in.



Troubleshooting Kerberos using macOS

Mac clients provide some useful command line utilities to help troubleshoot Kerberos issues. If you are having issues with the app signing in, please follow these steps and raise a support ticket through the support email address.

Firstly, double check that the user in question has no issues with their account in Active Directory. A blank UPN attribute (User Principle Name / username@domain) from a misconfigured bulk user import script can be the root cause of some Kerberos issues that only become apparent on non-Windows clients.

Check DNS, and if required in your environment, create a CNAME record as described above. Ensure the client is connecting to Foldr so the (signed) SSL certificate is valid on the client.

1. Open Terminal
2. Check for the existence of a Kerberos ticket using the command:

```
klist
```

Note – if you need to request a new ticket, or are testing on a standalone Mac, issue the command:

```
kinit username@DOMAIN.COM
```

Note – the DOMAIN section must be uppercase

```
curl -v –negotiate -u : https://FOLDR/sso/krb5
```

Replacing FOLDR with the FQDN of the Foldr appliance

4. If Kerberos authentication is working as expected, towards the end of the output you should see a HTTP 302 redirect pointing to /home

20. Custom Branding

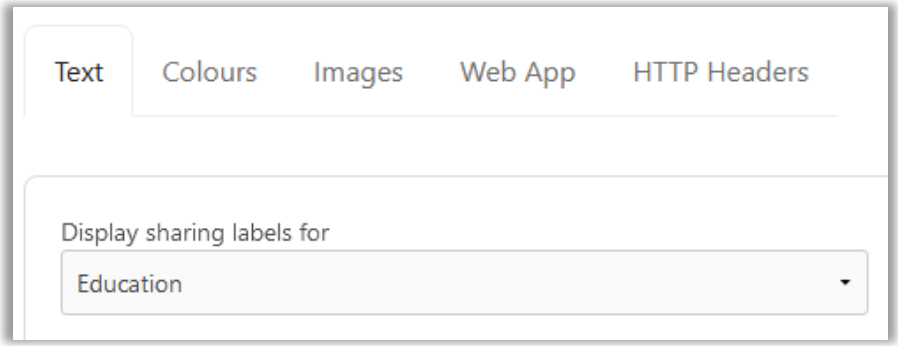
Within ***Foldr Settings > Customise***, the administrator can change numerous visual aspects of the web app interface.

On the log in screen, the administrator can change the full-page background wallpaper, welcome text, title text and upload a custom icon image file that will replace the default Foldr icon. Once a user has signed in the top banner and text within the banner can use specific custom colours. Custom colours and logos will also be reflected in the iOS app (Android custom branding support coming late 2019)

The administrator can alter the wording of sharing types/modes in Foldr between education and business focused use cases and finally you can provide custom headers for appliance for allowing interoperability with other systems.

Display Sharing Labels

This option will change the text labels used in the Sharing features in Foldr.



Education

Hand Out = Read Only
Hand In = Read source files and write files into dedicated subfolders
Manage = Read / Write

Business

Duplicate = Read Only
Submit = Read source files and write files into dedicated subfolders
Manage = Read / Write

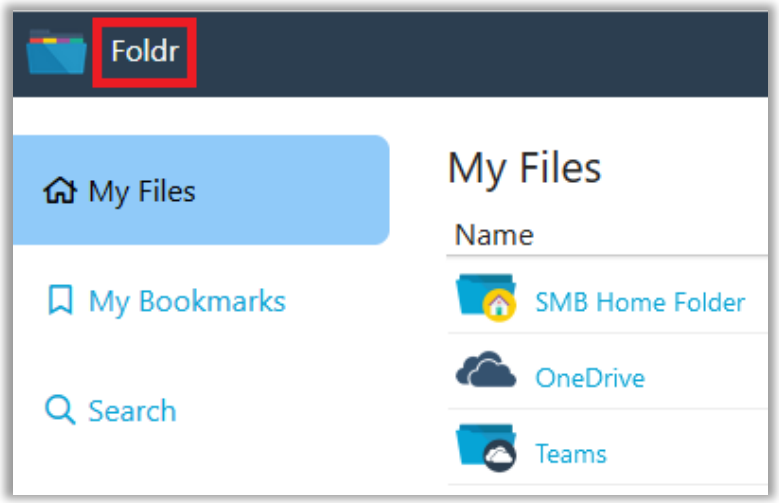
Custom Text (Sign-in Screen)

Sign In

Text entered into this field will replace the default '**Welcome to Foldr'** message on the web app sign in dialog

Title

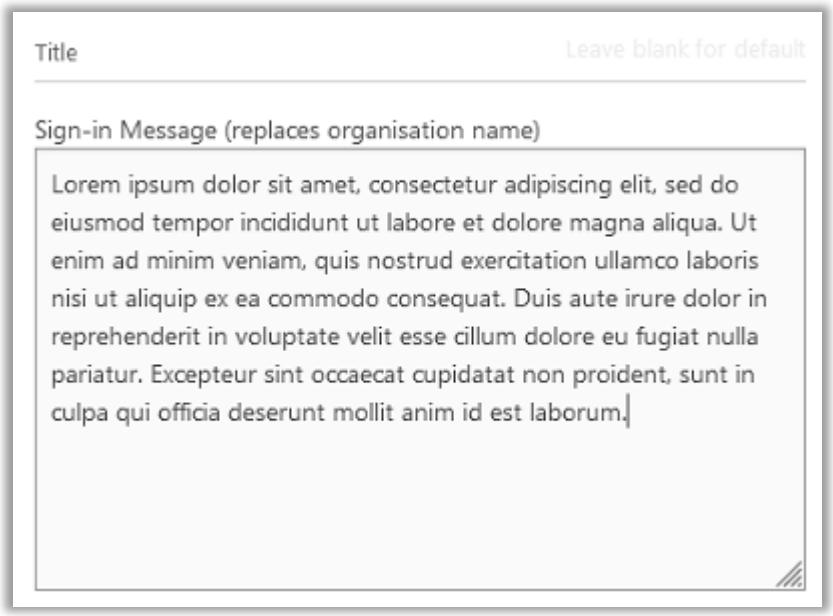
Text entered into this field will affect both the
browser tab title and also the default 'Foldr' text when a user is signed into the web app (shown below)



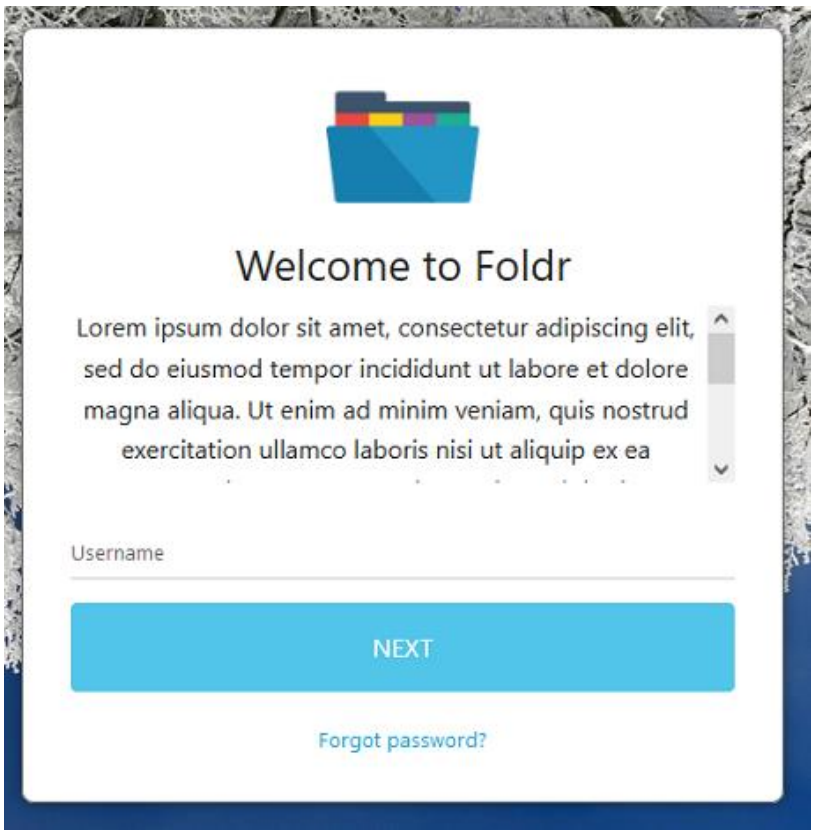
Sign-In Message

Text entered into the Sign-In Message will replace the organisation name, which is taken from the

licence key. The text will be displayed on the web app and mobile/desktop app sign on dialogs (web sign in required).

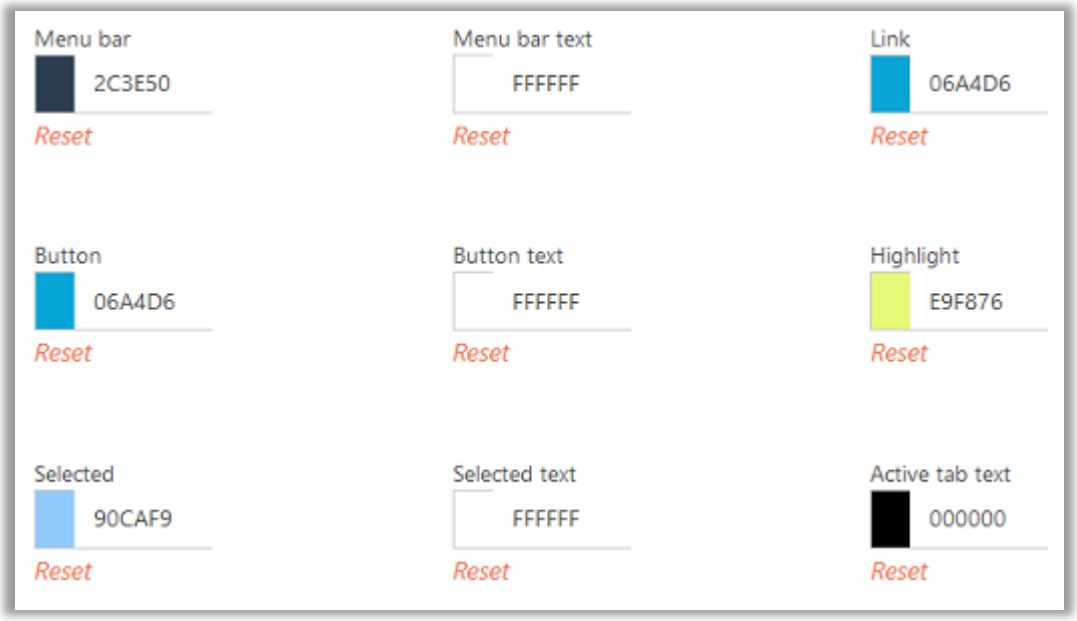


Web app showing a custom Sign-in Message – note this is scrollable.

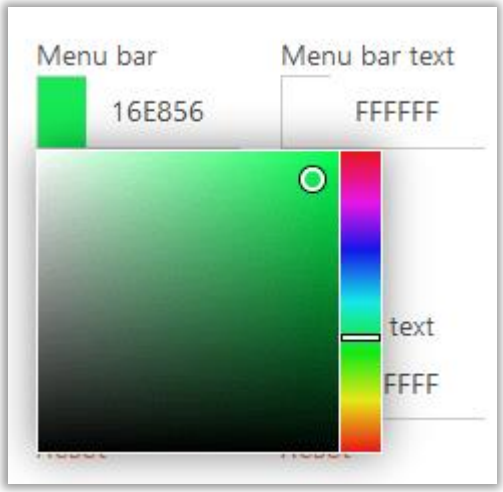


Custom Colours

The web app may be customised using custom colours for highlighted elements, buttons, text and menu bars

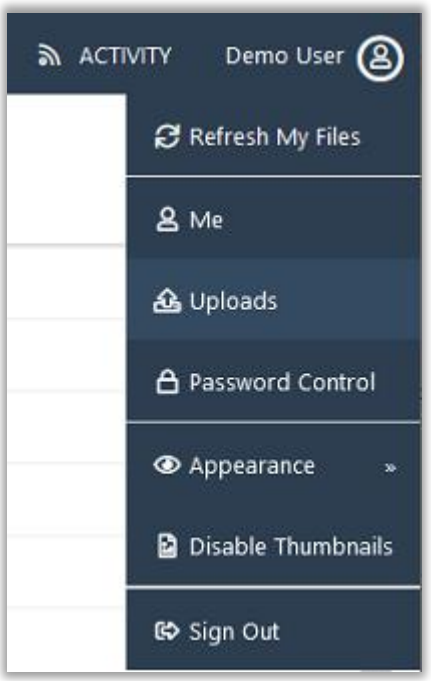


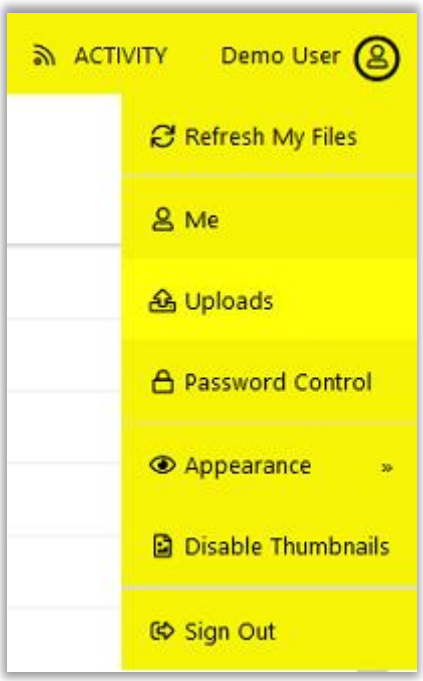
Using the Colour Picker



An example of changing the menu bar and menu bar text colour

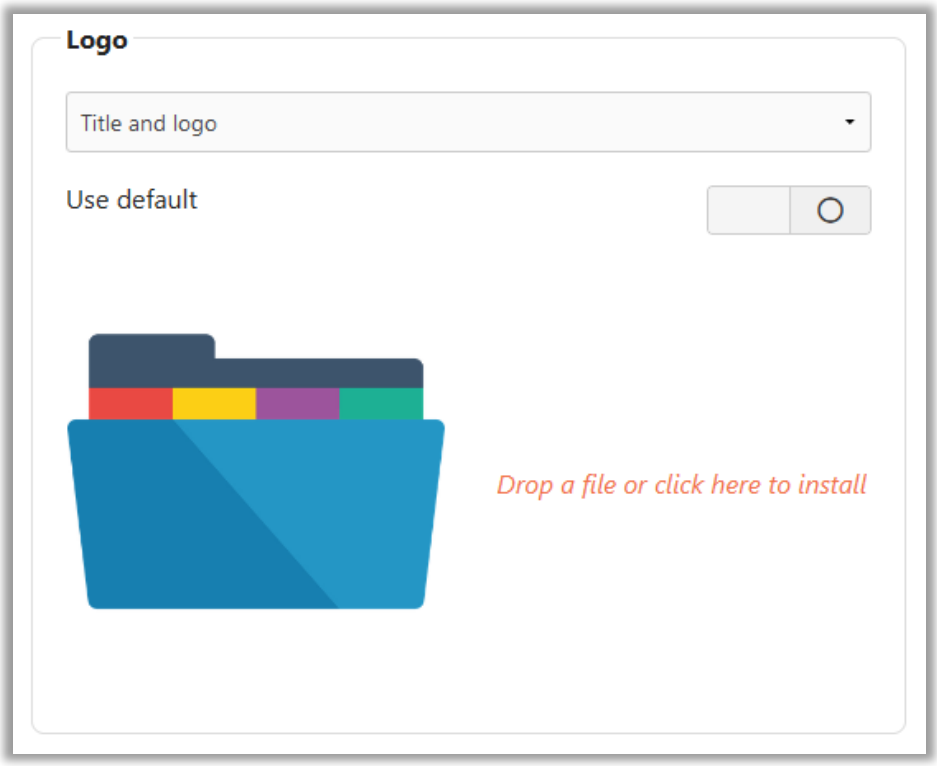
Default banner colour **Custom banner example**





Configuring a custom logo

To replace the default Foldr logo shown on the sign in screen, turn '**Use default**' off and drag / drop a new logo into the space provided.



The image will be scaled automatically and should be supplied in JPG, PNG or GIF format.

Configuring a custom background image

To replace the default Foldr wallpaper shown on the sign in screen, turn '**Use default**' toggle off and drag / drop a new image into the space provided.

The image will be sized to fill the user's web browser window, so an appropriately sized image should be provided. Please note that the file must be provided in PNG, JPEG or GIF format and should be 1.5MB size or less. For reference the sample background provided with the appliance is 2400x1600

Custom HTTP Headers

The Custom Headers field is an advanced option and should only be configured if you require this functionality. One of the main use cases for custom headers would be to enable Cross-Origin Resource Sharing (CORS), this allows the administrator to allow another system to make requests to the Foldr appliance. This could be used to allow a third-party service to make calls to the sharing features in the appliance, such as public links, to display shared files on other platforms.

Example shown below:


One per-line **HEADER: VALUE**
Access-Control-Allow-Origin: https://foldr.io
Vary: Origin

21. Miscellaneous System Settings

HSTS (HTTP Strict Transport Security)

HSTS is a security feature and is **automatically enabled** on the Foldr appliance, it cannot be disabled. More information on HSTS can be found here.

It is important to understand the implications of HSTS when installing a signed SSL certificate. Once installed, a user's web browser will expect all future HTTPS connection from the Foldr URL to use a valid, signed certificate. In the event of the certificate expiring or being revoked user access will be unavailable (from that client browser) until the SSL configuration is restored, or they switch to an alternative web browser.

In this scenario Foldr will always be available as a last resort via the (public or private) IP address.

The Appliance Console – Command List

The following commands are available from the console.

Command	Function
`dig`	DNS information & diagnostics
`netconfig`	Presents a simple to use console menu where you can configure the virtual appliance's network settings.
`netstat`	Displays network connections and statistics
`nslookup`	DNS troubleshooting
`passwd`	To change password for the fadmin account use 'passwd fadmin'
`ping`	Network connectivity & troubleshooting
`traceroute`	Determines the route taken by packets to reach a destination
`tenant-enable`	Enables multi-tenancy mode
`tenant-disable`	Disables multi-tenancy mode
`tenant-add "tenant-name" subdomain`	Adds a tenant, specify a friendly tenant name first in quotes followed by the required subdomain that will be used
`tenant-list`	Shows all tenants and the status of the encryption keys for each
`tenant-sync ip-1 ip-2 -p password`	Synchronises tenants across multiple appliances. Optionally specify the fadmin password for all appliances with the -p option.
`Tenant-reset-password subdomain`	Reset the tenant admin (tadmin) account for the given subdomain. The password will be reset to 'password' without quotes.
`Install-xen-guest-utils`	Installs the Citrix XenTools guest drivers for improved system performance. Requires the xs-tools ISO to be mounted in XenCenter.
`support-enable`	Enables fsupport mode. This can be used a technical support representative to log in for troubleshooting purposes or performing a password reset for the fadmin account.
`iptables`	Modifies the built-in firewall. All rules should be commented *-m comment –comment "foldr-admin"* to enable the rules to persist after a system update
`iptables-save`	Commits all firewall rules so they are permanently saved.
`add-interface ethx`	Creates an additional network interface. This must be used before you can configure these NICs with the netconfig menu. The appliance supports a maximum of 4 virtual NICs (eth0 – eth3)

`remove-interface ethx`	Removes additional network interface.
`set-routes ethx`	Set static routes for additional network interfaces
`ethtool -P ethx`	Displays the MAC address for interface ethx in the example. Useful if you have attached multiple interfaces to the appliance for identification purposes
`certificate-reset`	Resets the SSL certificate installation back to the self-signed (default) certificate
`time-sync ntp-server`	Forces the appliance system clock to sync with an NTP server. NTP must be selected within Foldr Settings > Appliance > Time Settings for this command to work successfully.
`ocsp-enable | disable`	Enables or disables OCSP stapling (default = disabled)
`flush-cache`	Flushes cached database entries on the server
`set-ciphers modern | default`	Configures the appliance web server SSL configuration. 'Modern' disables TLS 1.0, 1.1 and also disables the weaker (3DES) cipher suites.
`smb-mode legacy|default|modern|edge`	Configures SMB protocol on the appliance. The different modes are explained below: legacy = sets max client protocol to SMB1 default = sets max client protocol to SMB2 modern = sets min client protocol to SMB2 & max client protocol to SMB3 edge = set max client protocol to SMB3
`http-test <URL>`	Performs HTTP(S) connectivity tests using cURL. Example command to show verbose output: http-test -v https://letsencrypt.org
`ldap-test <filter>`	Performs LDAP(S) tests using ldapsearch
`install-datto-agent`	Downloads and installs the Datto Linux backup agent
`search-reserve-mem x`	Reserves xGB of RAM for non-search related functions (recommended minimum of 2)
`remove-tc-log`	Removes the transaction co-ordinator log file to aid with database recovery/start
`db-bootstrap`	Marks the local database as 'safe to bootstrap' – Useful to recover a cluster that has not shut down gracefully
`list-checkouts`	Lists all checkouts currently made by users, either manually or via an Edit in Office session in the web app
`remove-checkouts <days>`	Removes all checkouts older than the <days> specified
`remove-devices <days>`	Removes all user devices (including browsers) that were last seen older than the number of <days> specified
`set-inbox-allow-from '<addreses>'`	Configures the Foldr server to only receive email from the hosts specified.
`install-nutanix-guest-tools`	Installs the Nutanix AHV hypervisor tools

22. Connecting Users to Foldr

Users can connect to Foldr server via its web app or from one of the mobile (Android/iOS) or desktop (Windows/macOS) client apps. Note that the web app provides access to all Foldr features, some features (such as sharing) may not be available in specific apps.

Users connect to the appliance from any app / browser using the same address.

https://foldr.yourdomain.com

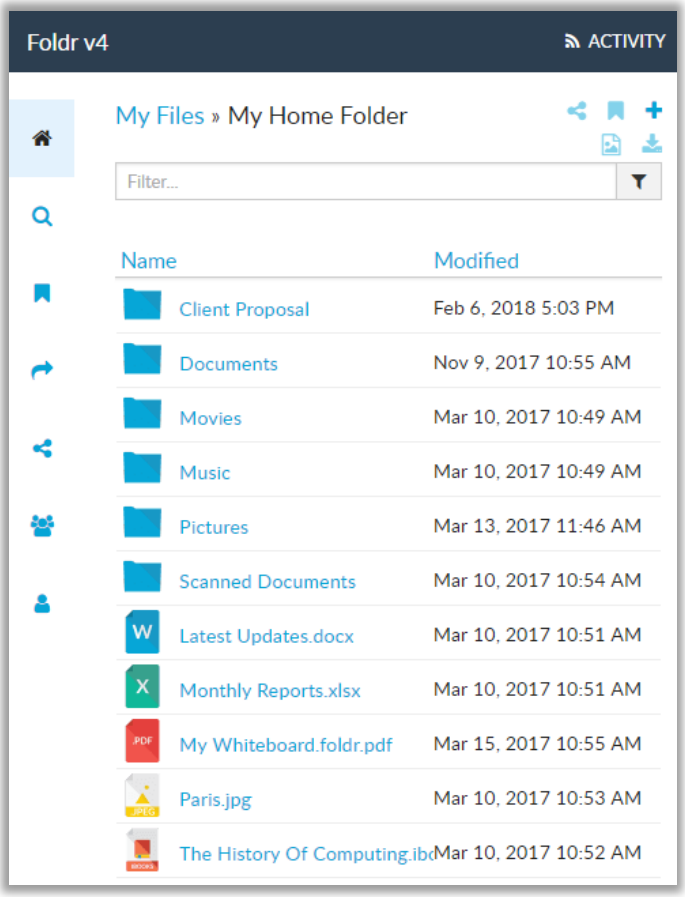
Desktop apps (drive mapping)

Windows app is available here - The macOS app is available here

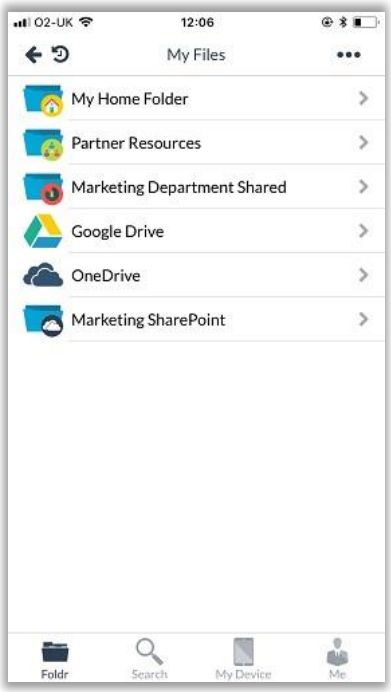
Mobile apps:

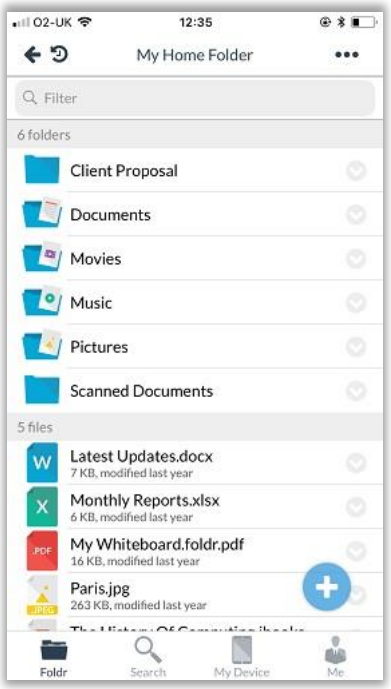
Foldr for iOS and Android is available in the App Store and Google Play

Web app

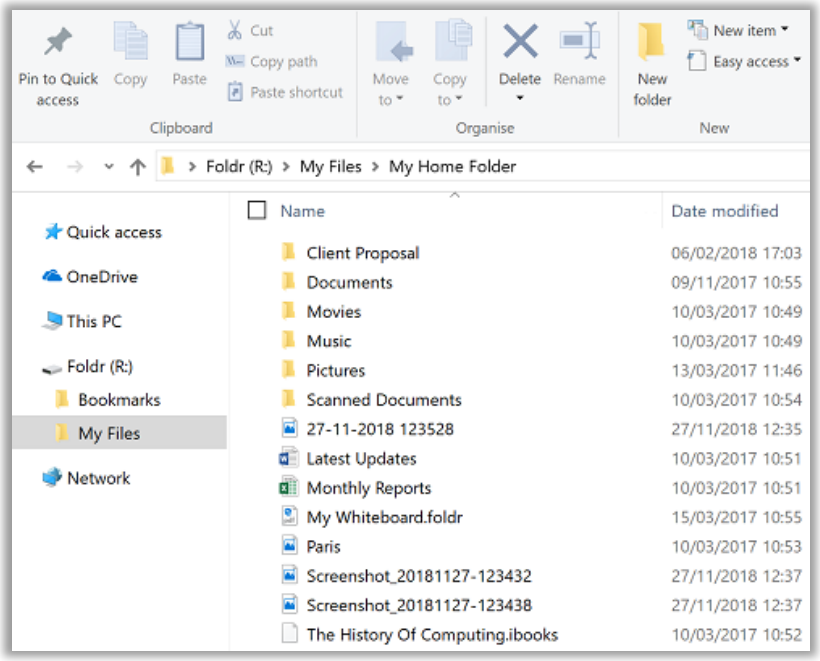


Mobile app (iPhone/iOS shown):

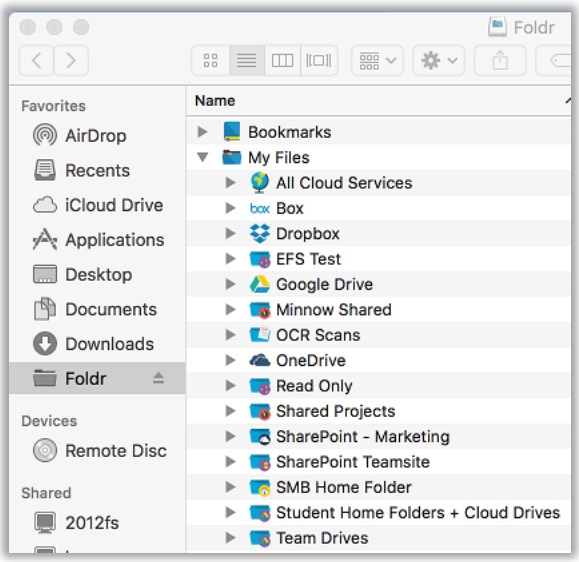




Foldr for Windows



Foldr for macOS

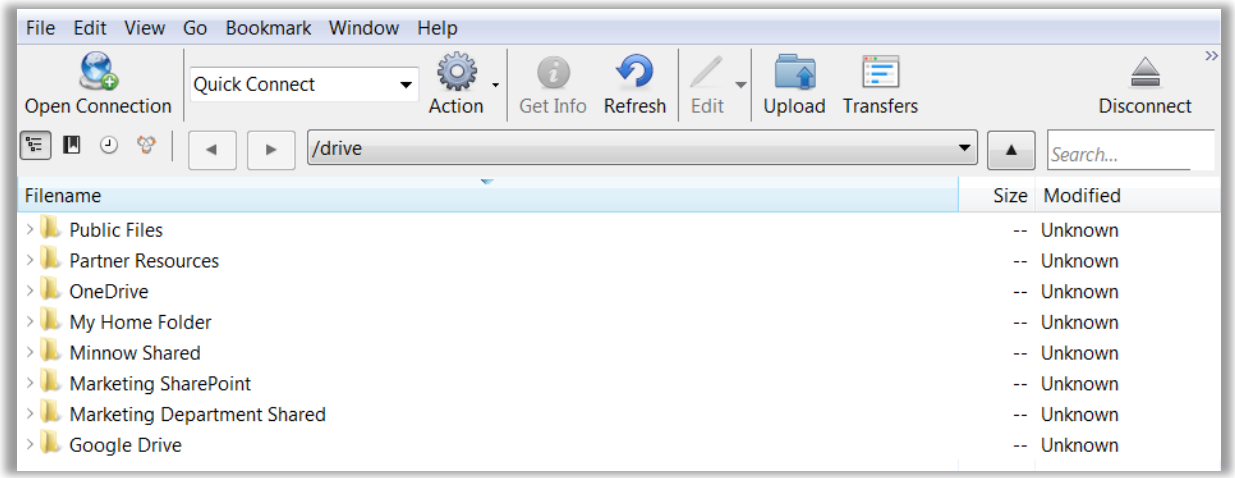


WebDAV clients:

The native Foldr apps do **not** use WebDAV, however the server does provide WebDAV support for users connecting with a third-party client, such as Cyberduck.

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

Third party WebDAV app (Cyberduck shown)



23. Controlling Client App Access

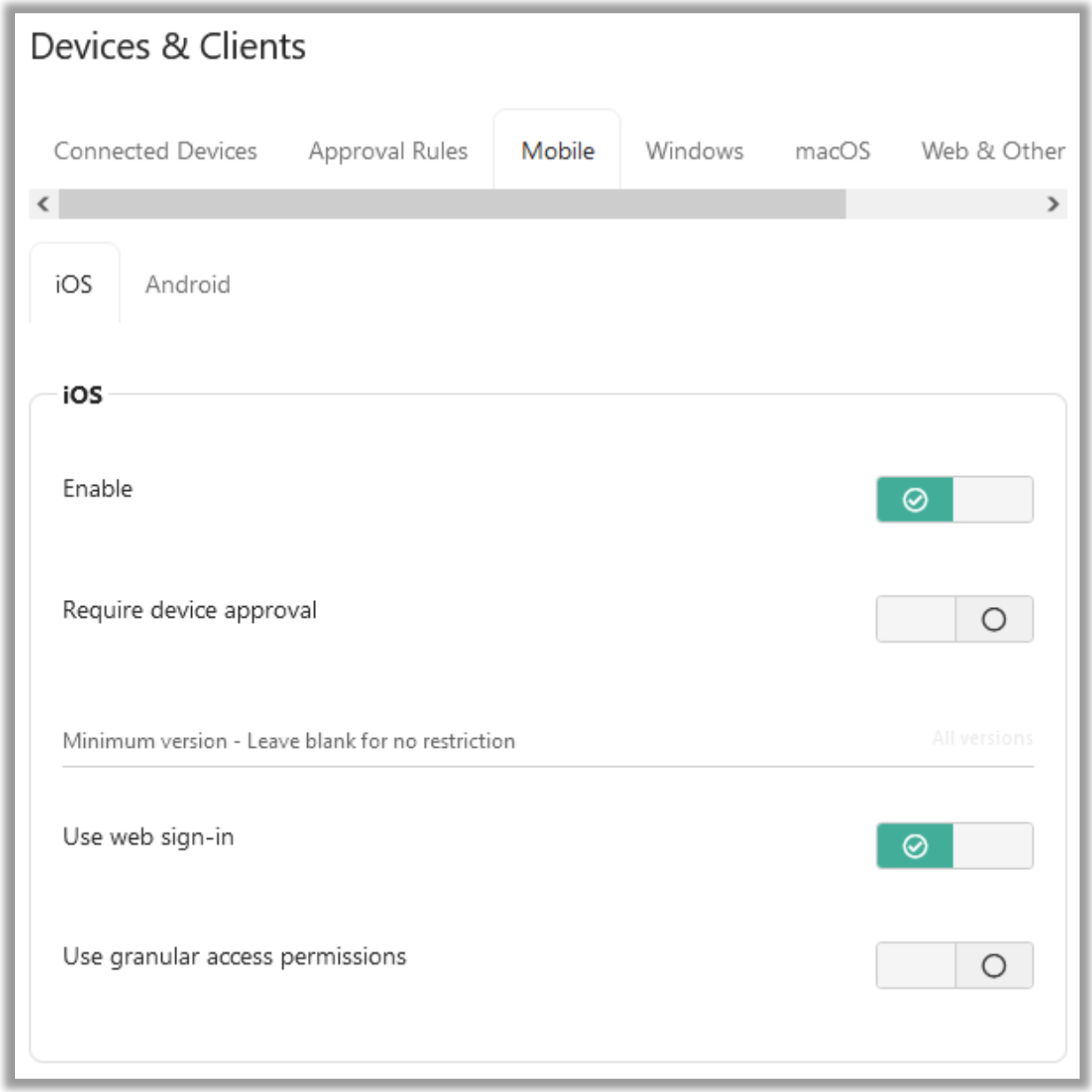
By default, Foldr will allow users to sign in from any location and from any client (web, desktop or mobile apps)

You can disable client access from each client type individually, specify version requirements or apply granular permissions and IP subnet rules for each. IP access rules can apply to individual users or groups as required. This could be used for example to allow specific users to connect from the iOS app, but only on the internal / organisation wireless network.

Device Configuration

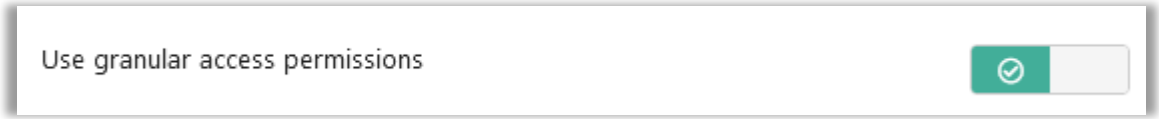
Devices and applications can be configured within ***Foldr Settings > Devices & Clients***.

iOS app configuration screen is shown below.



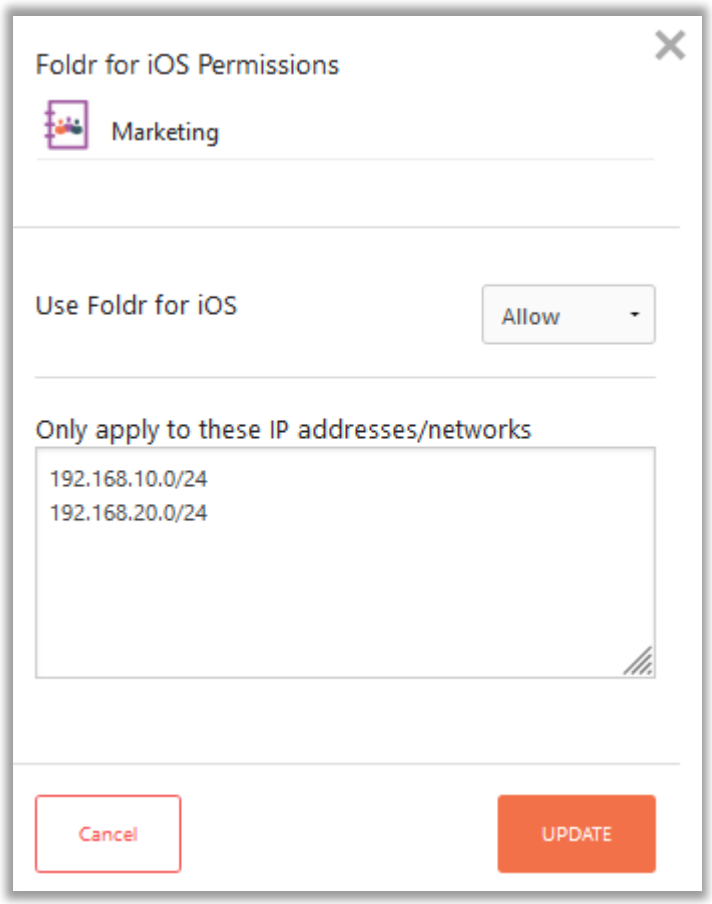
Separate configuration tabs are available for iOS, Android, Windows, macOS, Non-Foldr clients (curl for example) and the web app.

To enable granular access permissions on a specific app type, enable the toggle shown at the bottom of the dialog and configure as required. You can search for individual users or security groups and create separate rules for each.



The example below shows the iOS app configured for the Marketing security group. Users that are in this group will only be allowed to sign in using the iOS app if their client device is within either the 192.168.10.0/24 or 192.168.20.0/24 subnets. Foldr access from the iOS app will be denied automatically to Marketing users from any other location.

Applying granular access permissions to an app (iOS shown)



24. Managing & configuring the Foldr for Windows & macOS apps

Desktop apps are available for both Windows and macOS. These apps will present all storage locations available via the Foldr server under a single mounted drive Web in Explorer or Finder. The apps support search (via a web-based UI), and security features such 2FA, WebAuthn and SSO.

Foldr for Windows

The Foldr for Windows drive mapping client provides access to all storage locations presented through Foldr directly from Windows Explorer using a single mapped drive.

Limitations:

The app currently does not provide sharing features (sharing with others or public links etc). Users should use the Foldr web app if they need to use the sharing features.

System Requirements

Windows 8 – 11 (32bit or 64bit)
Visual C++ 2015 runtime – 14.0.24215 is required or higher

The Foldr for Windows app can be downloaded from the website:

https://foldr.io/products/foldr-for-files/microsoft-windows

The Foldr-setup.exe download for x86 and x64 systems will attempt to install the pre-requisite Visual C++ runtime if it isn't already installed. The app may be deployed using Group Policy, SCCM, Intune, scripts or open-source deployment tools such as WPKG using the .MSI version, which is available here:

x64 MSI - https://foldr.io/downloads/clients/win/x64/latest.zip

x86 MSI - https://foldr.io/downloads/clients/win/x86/latest.zip

It is recommended to install the latest C++ runtime bundle. This must be installed before attempting to deploy the .MSI version. The latest Microsoft C++ runtime package can be downloaded here:

x86 and x64 - https://docs.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170

When deploying Foldr using the MSI, it is recommended that the MSI remains accessible to the client, whether over a local or network connection, if deployed centrally.

The administrator can optionally pass various options to the installer to configure the application as required.

Antivirus Recommendations

Antivirus software can interfere with the running of the application and severely impact the performance / user experience when using the Foldr drive. It is recommended that antivirus software is modified so that both the mounted Foldr drive, and the local cache location is excluded for both real-time and on-demand scanning. If antivirus software is not modified, it may scan the drive and crawl through the shares/directories available resulting in many files to be downloaded to the local cache which is undesirable.

The application cache is stored at within the users local AppData directory which by default is available at:

%localappdata%\foldr\cache

This is in turn points to *C:\Users\<username>\AppData\Local\Foldr\cache*

App configuration and Registry Settings

By using any of the following msiexec installer options, registry keys are created automatically for each under:

HKEY_LOCAL_MACHINE\SOFTWARE\Foldr\Default

These registry keys apply to all users of the system and as such an administrator can configure the Foldr app by pushing these registry values to workstations, instead of using the msiexec options. This is typically done via Group Policy Preferences or via a script.

MSIEXEC Option	Value	Registry Key
FOLDR_SERVER	foldr.server.fqdn	FoldrServer
REQUIRES_ANTIVIRUS	1 or 0	RequiresAntivirus
AV_UPDATE_GRACE_MINUTES	Any numeric value	AVUpdateGraceMinutes
AV_GRACE_MINUTES	Any numeric value	AVGraceMinutes
DETECT_RENAME_THREAT	1 or 0	DetectRenameThreat
DETECT_EXTENSIONS_THREAT	1 or 0	DetectExtensionsThreat
FOLDR_DRIVE	e.g. "Z:"	FoldrDrive
DRIVE_TYPE_REMOVABLE	1 or 0	DriveTypeRemovable
USER_CAN_CHANGE_DRIVE_TYPE	1 or 0	UserCanChangeDriveType
USER_CAN_CHANGE_DRIVE_LETTER	1 or 0	UserCanChangeDriveLetter
SHARES	e.g. "1,2,10"	EnabledShares
UPDATES_ENABLED	1 or 0	UpdatesEnabled
SIGN_OUT_ON_EXIT	1 or 0	SignOutOnExit
SSO_LOGIN_BY_DEFAULT	1 or 0	SSOLoginByDefault
SERVER_OS_USING_DRIVE	e.g. "Z:"	*See details below*
CACHE_EXPIRY_DAYS	1, 5, 7, 14 or 28	CacheExpiryDays
CERTIFICATE_PROMPTS	1 or 0	CertificatePrompts
UPLOAD_NOTIFICATIONS	1 or 0	UploadNotifications
SHOW_WINDOWS_SHORTCUTS	1 or 0	ShowWindowsShortcuts
USE_MY_FILES	1 or 0	UseMyFiles
OPEN_DRIVE_AT_STARTUP	1 or 0	OpenDriveAtStartup
CLEAR_CACHE_ON_EXIT	1 or 0	ClearCacheOnExit
SSO_AUTO_SIGN_IN	1 or 0	SSOAutoSignIn
PROMPT_AT_STARTUP	1 or 0	PromptAtStartup
MAX_UPLOADS	1,2,3,4or 5	MaxUploads
NO_CACHE_MSI	1 or 0	Not stored in registry
EXCESSIVE_DOWNLOAD_ALERTS	1 or 0	ExcessiveDownloadAlerts
OFFICE_AUTO_CHECKOUTS	1 or 0	OfficeAutoCheckouts
OFFICE_ASSIST	1 or 0	OfficeAssist
OFFICE_ASSIST_ALLOW_OPEN	1 or 0	OfficeAssistAllowOpen
PRESERVE_WFR_ON_SIGN_OUT	1 or 0	PreserveWFROnSignOut
ADMIN_UPDATES	1 or 0	AdminUpdates
PROXY	http://proxy-address:port	Proxy
USER_CAN_CHANGE_PROXY	1 or 0 This option must be set to 0 for the 'Proxy' option to be used	UserCanChangeProxy
USE_OFFLINE_FILES	1 or 0	UseOfflineFiles

Example MSIEXEC installation command

msiexec /i FoldrSetup.msi /quiet /log install.log FOLDR_SERVER=https://demo.foldr.io REQUIRES_ANTIVIRUS=1 DETECT_RENAME_THREAT=1 DETECT_EXTENSIONS_THREAT=1 FOLDR_DRIVE="R:" SHARES="1,3"

Installation Option Details

FOLDR_SERVER=<SERVER ADDRESS>

Sets the default Foldr server address and will pre-populate the server address in the sign-in dialog.

Registry Setting
Name = FoldrServer
Type = REG_SZ (String)
Value = https://foldr.yourdomain.com

REQUIRES_ANTIVIRUS=1|0

Determines whether Antivirus is required to be enabled and up to date on the client machine. If set to =0 during installation, users will be able to change this option under Settings > Advanced tab; NOTE that on the client this setting will enabled by default.

Note: This can be overridden by the Foldr appliance.

Registry Setting
Name = RequiresAntivirus
Type = REG_SZ (String)
Value = 1|0

AV_UPDATE_GRACE_MINUTES=1|0

When Foldr detects that the client's antivirus is out-of-date, this option will allow the client machine the configured amount of time to update its AV definitions. If the AV is not updated before the timer expires, the drive will be disconnected.

A value of 0 disables any grace period whatsoever, regardless of the value of AV_GRACE_MINUTES, below.

Note that the client itself must still be within AV_GRACE_MINUTES for this setting to apply.

Note: This can be controlled / overridden by the Foldr appliance within ***Foldr Settings > Devices & Clients > Windows***

Registry Setting
Name = AVGraceMinutes
Type = REG_SZ (String)
Value = 1|0

AV_GRACE_MINUTES=1|0

The number of minutes allowed to elapse before an out-of-date Antivirus product causes the Foldr drive to go offline.

Note: This can be controlled / overridden by the Foldr appliance within ***Foldr Settings > Devices & Clients > Windows***

Registry Setting
Name = AVGraceMinutes
Type = REG_SZ (String)
Value = 1|0

DETECT_RENAME_THREAT=1|0

Configures a value in the Windows Registry that determines whether we detect ransomware rename threats on the client machine.

Note: This can be overridden by the Foldr appliance.

Registry Setting
Name = DetectRenameThreat
Type = REG_SZ (String)
Value = 1 or 0

DETECT_EXTENSIONS_THREAT=1|0

Configures a value in the Windows Registry that determines whether we detect ransomware extension threats on the client machine.

Note: This can be overridden by the Foldr appliance.

Registry Setting
Name = DetectExtensionsThreat
Type = REG_SZ (String)
Value = 1 or 0

FOLDR_DRIVE=<DRIVE LETTER>

Configures the drive letter to be used when mounting the Foldr drive.

Registry Setting
Name = FoldrDrive
Type = REG_SZ (String)
Value = R: (as an example)

DRIVE_TYPE_REMOVABLE=1|0

Configures the drive type to be used when mounting the Foldr drive (1 configures a Removable Drive, 0 configures a Network Drive).

Removable Drive is the default drive type and is recommended in typical installations. This mode provides improved support for Office files and saving back to the Foldr drive when the document is still open.

For compatibility reasons, the drive should be configured in Network mode in remote desktop sessions.

Registry Setting
Name = DriveTypeRemovable
Type = REG_SZ (String)
Value = 1|0

USER_CAN_CHANGE_DRIVE_TYPE=1|0

Configures whether the user can override the drive type used when mounting the Foldr drive.

Registry Setting
Name = UserCanChangeDriveType
Type = REG_SZ (String)
Value = 1|0

USER_CAN_CHANGE_DRIVE_LETTER=1|0

Configures whether the user can change the drive letter assigned to the Foldr drive. Note that this setting only takes affect if FOLDR_DRIVE=<DRIVE LETTER> has been set.

Registry Setting
Name = UserCanChangeDriveLetter
Type = REG_SZ (String)
Value = 1|0

SHARES=<LIST OF ENABLED SHARES>

Determines which shares are available to the user through the Windows application. If the option is not configured or an empty value is set, all shares will be available.

Otherwise, use a comma separated list of share IDs to specify which shares should be available, all others will be hidden from the drive. The share ID can be found in the ***Foldr Settings > Files & Storage*** area (shown in the browser address bar)

Registry Setting
Name = EnabledShares
Type = REG_SZ (String)
Value = 1,2,3,4 (example comma separated values for the share ID)

UPDATES_ENABLED=1|0

Determines whether the update mechanism is enabled.

If disabled, then no checking for updates will be made and the option to check for an update in the system tray context menu will be hidden.

Registry Setting
Name = UpdatesEnabled
Type = REG_SZ (String)
Value = 1|0

SIGN_OUT_ON_EXIT=1|0

Determines whether the user is signed-out when they exit the app. This would be useful in an environment where more than one user will need to sign into Foldr using the same Windows desktop session. If this option is enabled, the user is prompted to enter their credentials when the app is next launched. If enabled, the upload queue is wiped when the app is closed. As such, users must ensure all uploads have completed before exiting the app or logging out of Windows.

Registry Setting
Name = SignOutOnExit
Type = REG_SZ (String)
Value = 1|0

SSO_LOGIN_BY_DEFAULT=1|0

Determines if the 'Use Single Sign-On' checkbox is always checked. The user may still uncheck the control and sign-on with a username and password if they wish.

If disabled, then when the login dialog is shown, the 'Use Single Sign-On' is only checked when the user has previously enabled SSO.

Registry Setting
Name = SSOLoginByDefault
Type = REG_SZ (String)
Value = 1|0

SERVER_OS_USING_DRIVE=<DRIVE LETTER>

A convenience option (recommended for deployments to a Windows Server O/S) which overrides the following options with:

FOLDR_DRIVE=<DRIVE LETTER>
DRIVE_TYPE_REMOVABLE=0
USER_CAN_CHANGE_DRIVE_LETTER=0
USER_CAN_CHANGE_DRIVE_TYPE=0

CACHE_EXPIRY_DAYS=1|0

Sets the number of days that files are cached on the user's local filesystem.

When a value is assigned to this setting, the user will be unable to override the configured value.

Registry Setting
Name = CacheExpiryDays
Type = REG_SZ (String)
Value = 1, 5, 7, 14 or 28

CERTIFICATE_PROMPTS=1|0

Determines whether the user is prompted if the server they are connecting has an untrusted / expired SSL certificate.

When a value is assigned to this setting, the user will be unable to override the configured value.

Registry Setting
Name = CertificatePrompts
Type = REG_SZ (String)
Value = 1|0

UPLOAD_NOTIFICATIONS=1|0

Determines whether a pop-up notification is displayed when a file is queued for upload.

When a value is assigned to this setting, the user will be unable to override the configured value.

Registry Setting
Name = UploadNotifications
Type = REG_SZ (String)
Value = 1|0

SHOW_WINDOWS_SHORTCUTS=1|0

Determines whether the Windows Shortcuts are shown on the Foldr drive.

When a value is assigned to this setting, the user will be unable to override the configured value.

Registry Setting
Name = ShowWindowsShortcuts
Type = REG_SZ (String)
Value = 1|0

USE_MY_FILES=1|0

Determines whether 'my files' and 'bookmarks' are shown in the root of the Foldr drive. When enabled, the shares available to the user will be contained within the 'my files' directory. When disabled, the shares will be shown in the root of the Foldr drive.

When a value is assigned to this setting, the user will be unable to override the configured value.

Registry Setting
Name = UseMyFiles
Type = REG_SZ (String)
Value = 1|0

OPEN_DRIVE_AT_STARTUP=1|0

Determines whether the Foldr drive is opened in an Explorer window when mounted at start up.

Note:

When a value is assigned to this setting, then the user will be unable to override the configured value.

Registry Setting
Name = OpenDriveAtStartup
Type = REG_SZ (String)
Value = 1|0

CLEAR_CACHE_ON_EXIT=1|0

Determines whether the cache is cleared when Foldr exits.

When a value is assigned to this setting, the user will be unable to override the configured value.

Registry Setting
Name = ClearCacheOnExit
Type = REG_SZ (String)
Value = 1|0

SSO_AUTO_SIGN_IN=1|0

When Foldr is started up, and single-sign-on is available, Foldr will attempt to sign in automatically using SSO.

When a value is assigned to this setting, the user will be unable to override the configured value.

Registry Setting
Name = SSOAutoSignIn
Type = REG_SZ (String)
Value = 1|0

PROMPT_AT_STARTUP=1|0

This setting configures whether Foldr prompts the user to sign-in (when no account is setup, or when the user is signed-out) when Foldr starts.

There is no user configuration for this option. When no value is assigned to this setting, Foldr will prompt the user to sign-in.

Registry Setting
Name = PromptAtStartup
Type = REG_SZ (String)
Value = 1|0

MAX_UPLOADS=1,2,3,4 or 5

This setting determines the number of uploads Foldr uses when uploading a batch of files to the Appliance.

When no value is assigned to this setting, Foldr will prompt the user to sign-in.

Registry Setting
Name = MaxUploads
Type = REG_SZ (String)
Value = 1|0

NO_CACHE_MSI=1|0

Use to inform the installer whether to preserve a cached copy of the FoldrSetup.msi installer. This means that when Windows needs the installer (after a major Windows update for example) there will be a copy available, and Windows will not prompt the user for its location.

If the argument is not supplied, or is set to '0', then the installer caches the MSI in a directory named '%COMMONPROGRAMFILES%/Foldr'

If the argument is set to '1', then installer does not cache the MSI.

This argument to the installer is not stored in the Windows Registry.

EXCESSIVE_DOWNLOAD_ALERTS=1|0

This setting configures whether Foldr notifies a user when it detects excessive download activity for a particular process (for example, an Antivirus product scanning files on the Foldr drive).

If the argument is set to 1, then Foldr will issue alerts. The user will be unable to configure the setting.

If the argument is set to 0, then Foldr will not issue alerts. The user will be unable to configure the setting.

When unset, the user will be able to configure the setting, The default value is 1.

Registry Setting
Name = ExcessiveDownloadAlerts
Type = REG_SZ (String)
Value = 1|0

ADMIN_UPDATES=1|0

This setting configures whether users are allowed to install app updates without administrative privileges.

If the argument is set to 1, AdminUpdates are enabled. The user will be unable to configure the setting in the App Settings UI (Advanced tab).

If the argument is set to 0, AdminUpdates is disabled. The user will be unable to configure the setting.

When unset, the user will be able to configure the setting in the App Settings UI (Advanced tab). They will need to satisfy a UAC prompt in order to do so.

Registry Setting
Name = AdminUpdates
Type = REG_SZ (String)
Value = 1|0

OFFICE_AUTO_CHECKOUTS=1|0

Determines whether the Microsoft Office files are automatically checked-out when they are opened. This feature requires that the drive is mounted as a Network Drive.

When a value is assigned to this setting, the user will be unable to override the configured value

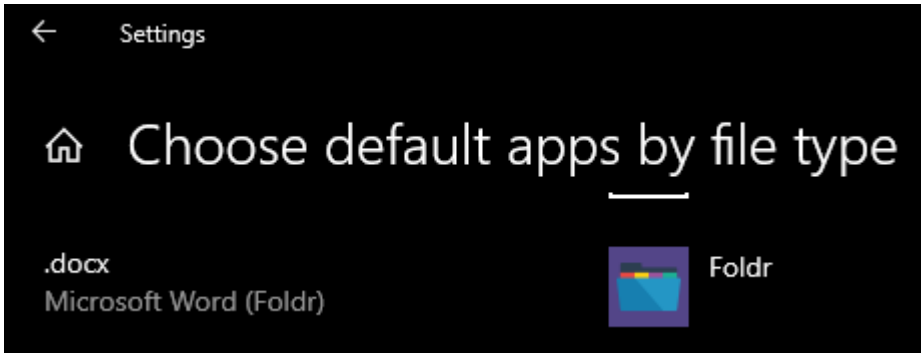
Registry Setting
Name = OfficeAutoCheckouts
Type = REG_SZ (String)
Value = 1|0

OFFICE_ASSIST=1|0

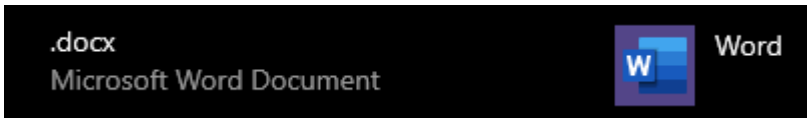
This setting configures whether Office documents are associated with the Foldr app (when the app is running).

When Office Assist is enabled, double-clicking Word, Excel or PowerPoint files that are hosted in Office 365 locations will open documents directly via the files online URL and use the Office apps native/built-in saving mechanism to save back to OneDrive, SharePoint and Teams. Saving files with Office Assist enabled, bypass the Foldr server, local upload queue, results in no temporary files being created (~$ prefix Office owner files), enables the autosave feature in the Office apps and allows for native collaborative editing.

The local file association is modified on the Windows client when the Foldr is running for .docx, .xlsx and .pptx files.



When the app is quit, the file association will automatically revert to default, as shown below.

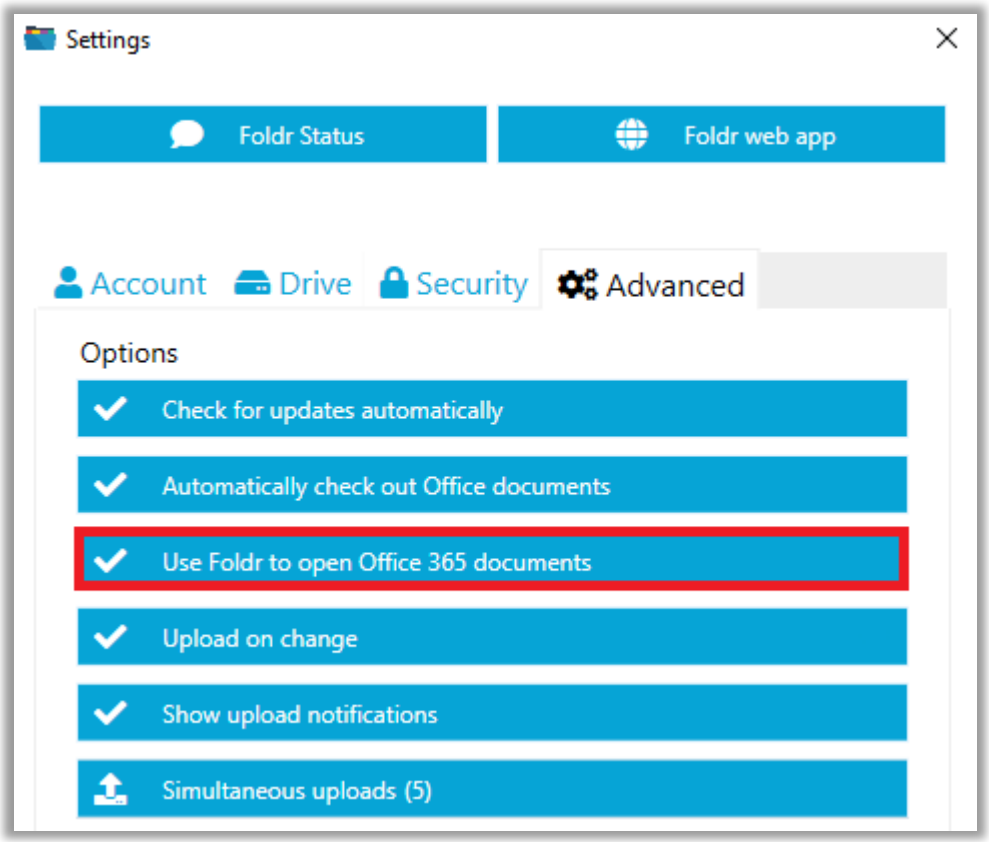


If the argument is set to 1, then OfficeAssist is enabled. The user will be unable to configure the setting in the app.

If the argument is set to 0, OfficeAssist is disabled. The user will be unable to configure the setting in the app.

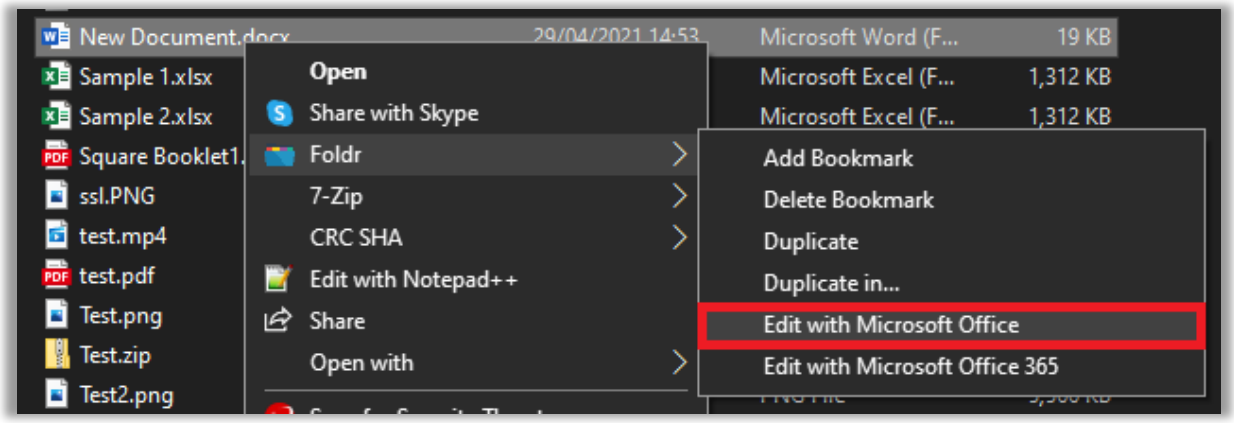
When unset, the user will be able to configure the setting, The user is prompted, at start up, for its initial value.

If the user is allowed to enable Office Assist manually in the app, this can be done in the app settings > Advanced tab as shown below:



The functionality to edit 'online' can be used **without** 'OfficeAssist' being enabled by using the context menu in Explorer > Foldr > Edit in Microsoft Office. As with OfficeAssist, the context menu will open

the file directly using its online URL, autosave is enabled automatically and native collaborative editing is supported.

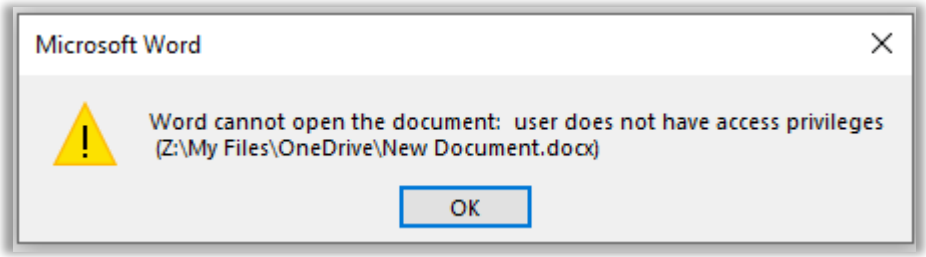


Registry Setting
Name = OfficeAssist
Type = REG_SZ (String)
Value = 1|0

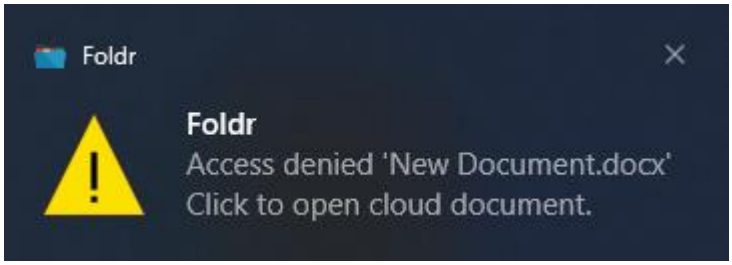
NOTE 1 – When Office Assist is enabled, users will be able to open Office documents from Explorer that are stored outside of Foldr providing the path has a drive letter. For example, local disks, external storage and mapped network drives will open documents as expected when a user double clicks a file in Explorer. Users will be unable to open files using UNC paths in Explorer.

NOTE 2 – It is recommended that users open Office files hosted in Office 365 locations by double-clicking the files to open in their File browser (Windows Explorer). This ensures the online version is opened rather than using File > Open inside the Office app – see below.

When Office Assist is enabled, the app will block the File > Open route of opening Office files hosted in Office 365 locations from the Foldr drive. This is to prevent a local / offline version of the file being opened. If a user tries to use File > Open with Office Assist open, they will see the following error:



A Windows notification will appear (bottom right) and if the user clicks this, the online document will be opened in the local Office app.



The user can then continue working on the file 'live' using the online version – autosave, collaborative editing and any other native Office 365 features available in Office will function as usual.

OFFICE_ASSIST_ALLOW_OPEN

When Office Assist is enabled, the feature, by design (as of app release 1.5.23) will prevent users from directly opening Office documents from inside an Office app hosted in any Office 365 location using FILE > OPEN > Z: (i.e. the Foldr Drive letter) – Office Assist users should instead browse through Explorer, via the Foldr drive and double click files to open.

The Foldr app blocks File > Open as a route to open Office 365 files as it is unable to open the 'online' document version at Office365 using this route. If the user attempts this they will receive an error that the Office app was unable to open the file (as the app is blocking the action) and a Windows notification will appear to allow the user to open the cloud version by clicking upon the notification.

1 – OfficeAssistAllowOpen is enabled. The user will be unable to configure the setting.
0 – OfficeAssistAllowOpen is disabled. The user will be unable to configure the setting.

When unset, the user will be able to configure the setting.

Registry Setting
Name = OfficeAssistAllowOpen
Type = REG_SZ (String)
Value = 1|0

PRESERVE_WFR_ON_SIGN_OUT
Working File Recovery (WFR) is a feature that provides an in-app recycle bin for files that have been worked on from the Foldr drive. The app and it will keep a copy of each document/file in the WFR location for every save action.

By default files in the WFR location (%localappdata%\Foldr\cache\restore) will remain if the app is quit (or machine is shutdown). However, if the user **signs out** of the app, the default behaviour is for files in the WFR store to be **deleted**. Foldr will automatically manage files in the WFR store in-line with the setting to manage the cache (Clear cached files after x days). Manually clearing the cache will not affect files in the WFR store.

The admin option *PRESERVE_WFR_ON_SIGN_OUT* allows the administrator to change the app behaviour so files in the WFR store are not deleted if the user signs out of the app.

If the argument is set to 1 – Working files in the filesystem cache\restore folder are preserved on sign-out. The user will be unable to configure the setting.

If the argument is set to 0 – Working files in the filesystem cache\restore folder are removed on sign-out. The user will be unable to configure the setting.

When unset, the user will be able to configure the related user-setting in the app settings > Advanced tab > Working File Recovery > Preserve files on sign-out button. Shown below:

Registry Setting
Name = PreserveWFROnSignOut
Type = REG_SZ (String)
Value = 1|0

PROXY

By default Foldr will use the device configured proxy. This option allows the administrator to configure the Foldr app to use an alternative proxy for app communications.

The proxy should be specified using the proxy address appended by the port. For following examples are valid:

10.1.1.1:8080
myproxy.com:8080
http://myproxy:8080

Note: This setting ONLY applies when USER_CAN_CHANGE_PROXY / UserCanChangeProxy is also set to 0

Registry Setting
Name = Proxy
Type = REG_SZ (String)
Value = address:port

USER_CAN_CHANGE_PROXY

This configures whether the user may configure a manual HTTP proxy in the app settings.

1 – the user may configure a proxy the setting.
0 – The user will be unable to configure a proxy, the option is greyed out and the admin configured proxy (set using the Proxy registry key above will be used)

When unset, the user will be able to configure a proxy

Registry Setting
Name = UserCanChangeProxy
Type = REG_SZ (String)
Value = 1|0

USE_OFFLINE_FILES

Used in conjunction with **USE_MY_FILES** to determine whether the 'Offline Files' directory is shown in the root of the Foldr drive.

Note:
When a value is assigned to this setting, then the user will be unable to override the configured value.

Registry Setting
Name = UseOfflineFiles
Type = REG_SZ (String)
Value = 1|0

User Default Settings:

Option	Default Value
FOLDR_SERVER	Empty
REQUIRES_ANTIVIRUS	1
AV_UPDATE_GRACE_MINUTES	0 (Disabled) – Can no longer be modified by the user
AV_GRACE_MINUTES	0 (Unlimited) – Can no longer be modified by the user
DETECT_RENAME_THREAT	1
DETECT_EXTENSIONS_THREAT	1
FOLDR_DRIVE	The first available drive letter working in reverse from Z:
DRIVE_TYPE_REMOVABLE	1
USER_CAN_CHANGE_DRIVE_TYPE	1
USER_CAN_CHANGE_DRIVE_LETTER	1
SHARES	Empty (all shares available)
UPDATES_ENABLED	1
SIGN_OUT_ON_EXIT	0
SSO_LOGIN_BY_DEFAULT	0
SERVER_OS_USING_DRIVE	Not applicable (see individual settings)
CACHE_EXPIRY_DAYS	7
CERTIFICATE_PROMPTS	1
UPLOAD_NOTIFICATIONS	1
SHOW_WINDOWS_SHORTCUTS	0
USE_MY_FILES	1
OPEN_DRIVE_AT_STARTUP	1
CLEAR_CACHE_ON_EXIT	0
SSO_AUTO_SIGN_IN	0
PROMPT_AT_STARTUP	Not applicable (enabled by default)
MAX_UPLOADS	5
EXCESSIVE_DOWNLOAD_ALERTS	1
OFFICE_AUTO_CHECKOUTS	0
OFFICE_ASSIST	Empty
OFFICE_ASSIST_ALLOW_OPEN	Empty
PRESERVE_WFR_ON_SIGN_OUT	0
PROXY	Empty
USER_CAN_CHANGE_PROXY	1
USE_OFFLINE_FILES	1

Using Group Policy to deploy the Foldr app

The recommended method of deploying the app with Group Policy is given below:

1. Download the latest Foldr setup .MSI using the .zip links below:

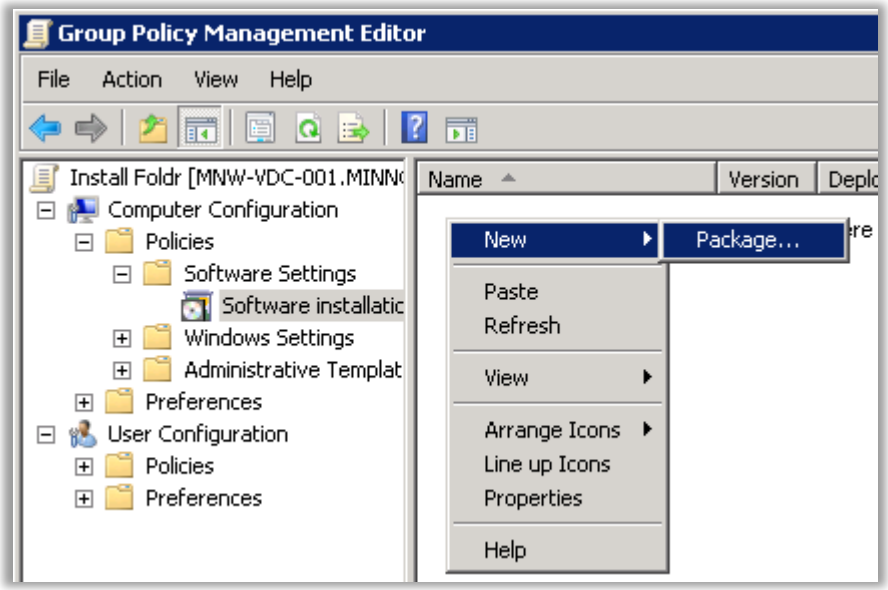
x86 - https://foldr.io/downloads/clients/win/x86/latest.zip

x64 - https://foldr.io/downloads/clients/win/x64/latest.zip

2. Extract the zip file. If you are attempting to install app version 1.2.0 rename the FoldrSetup.msi to 'setup.1.2.0.msi' and place it into a suitable SMB share on the network.

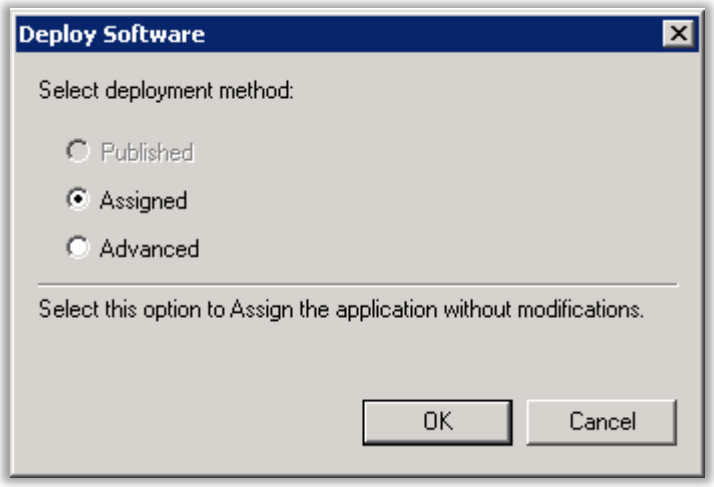
3. Open the Group Policy Management Console (GPMC). Create and link a new GPO on the Organisational Unit that contains the Windows clients that are to receive the Foldr app; or edit an existing policy if one for software installs. Edit the policy.

4. Browse to ***Computer Configuration > Policies > Software settings > Software installation***. Add a new item by right clicking on the main pane > New > Package.

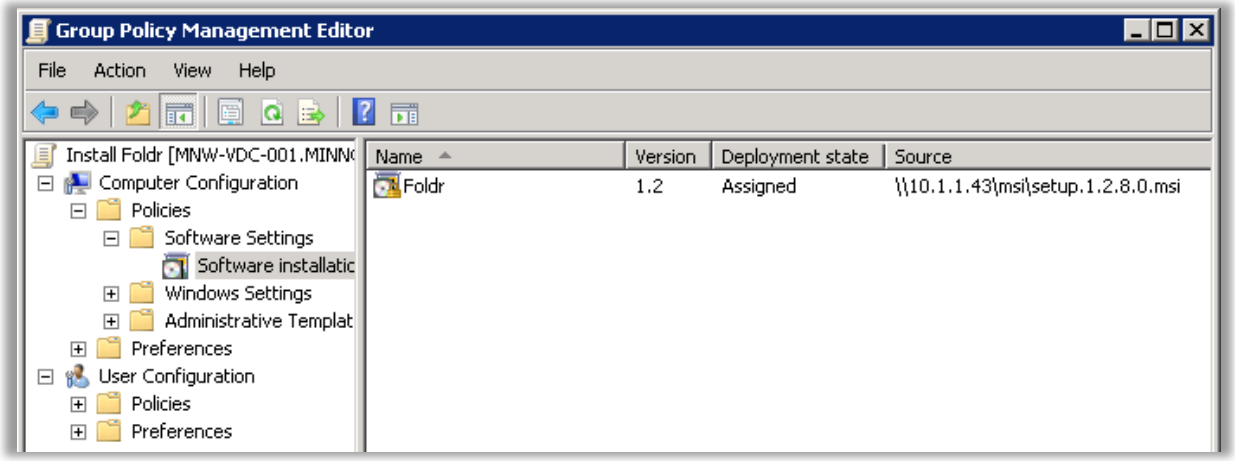


5. Browse to the location of the .MSI file using the network **UNC path** (for example \\server\share\setup.1.2.0.msi) and select the .MSI to be installed on the clients.

6. Use the default 'Assigned' deployment type and click OK to confirm.



7. The app will appear in the main panel showing the application name, version and path.



The basic deployment steps are now complete. When the Windows clients next reboot and they are connected to the network the Foldr app will be installed automatically.

Updating the Foldr app with Group Policy

To upgrade the Foldr for Windows app on the Windows clients - In this example we will upgrade from 1.2.8 to 1.3.0:

1. Download the latest Foldr for Windows .MSI file using the download links below:

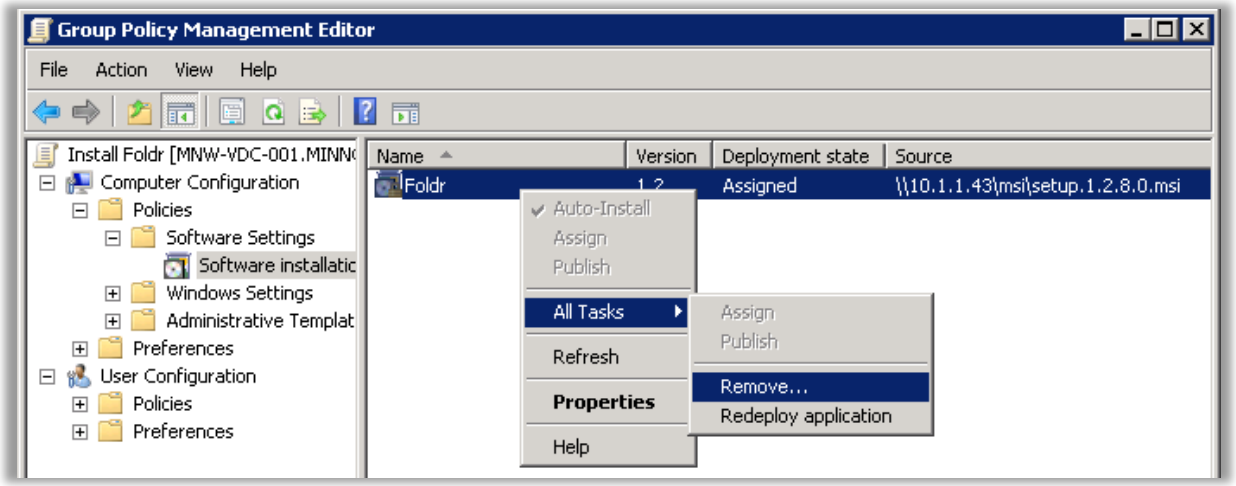
x86 - https://foldr.io/downloads/clients/win/x86/latest.zip

x64 - https://foldr.io/downloads/clients/win/x64/latest.zip

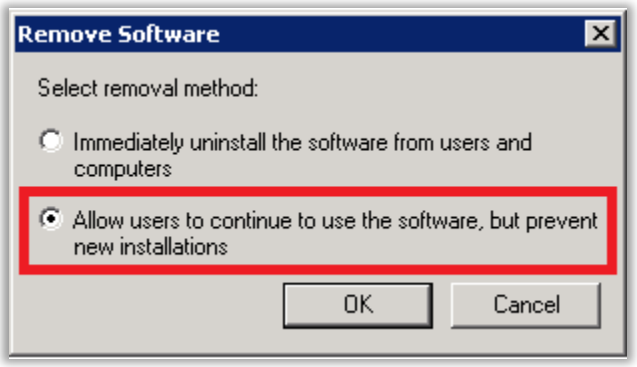
2. Extract the zip file. If you are intending to upgrade to app version 1.3.0 rename the FoldrSetup.msi to 'setup.1.3.0.msi' and place it into a suitable share on the network.

3. Edit the relevant software installation GPO in Group Policy Management and navigate to ***Computer Configuration > Policies > Software settings > Software installation***

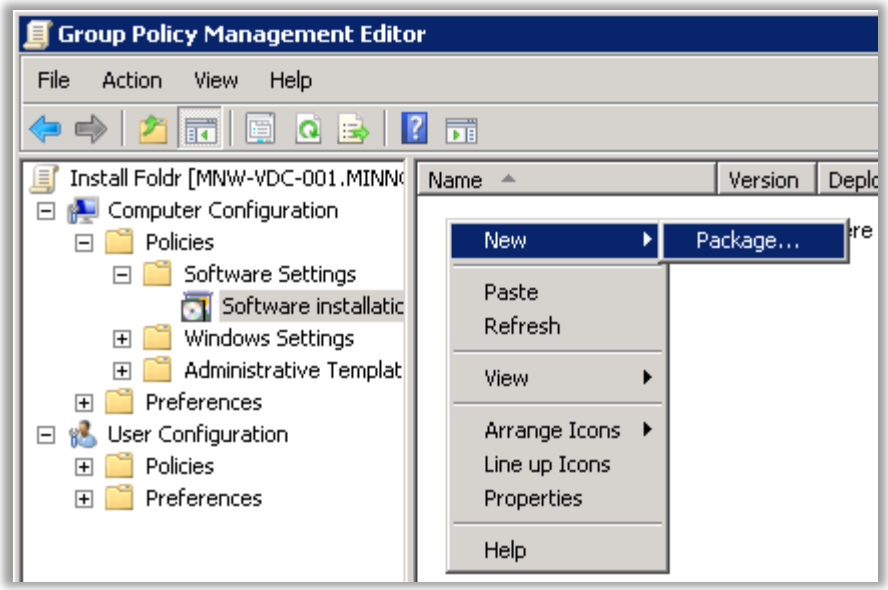
4. Remove the existing v1.2.8 Foldr app listed in the main panel by right clicking > All Tasks > Remove



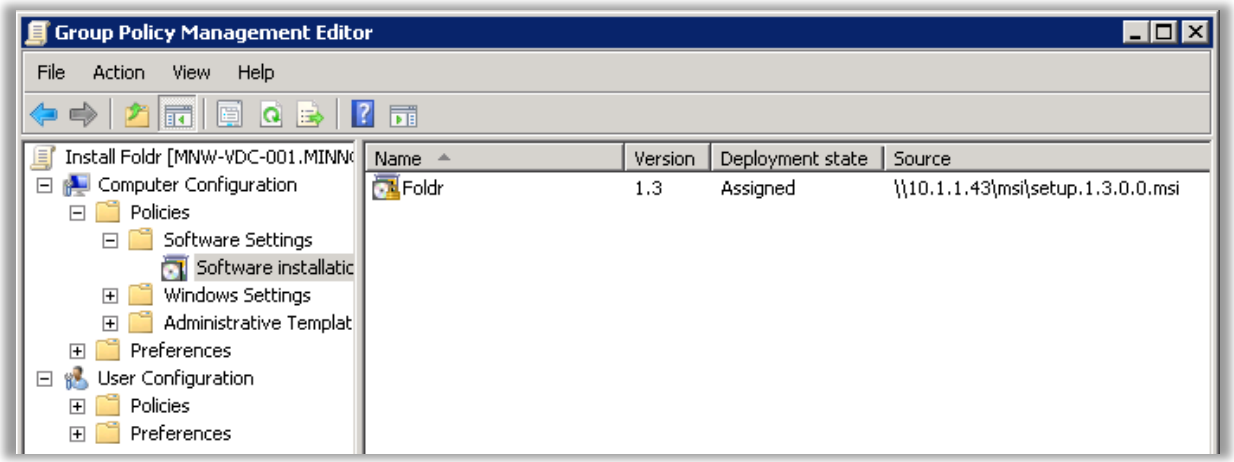
5. Select '**Allow users to continue to use the software, but prevent new installations**' (bottom option) so that the existing Foldr application is not uninstalled from the clients. Click **OK**.



6. The app will be removed from view in the Group Policy Management Console. Add a new application by using the context menu > New > Package.



7. Browse to the location of the .MSI file using its UNC path (\\server\share\setup.1.3.0.msi) and select the upgrade .MSI to be installed on the clients.



The upgrade steps are now complete. When the Windows clients next reboot, and they are connected to the network, the Foldr app will upgraded automatically retaining the installation settings / configuration options that are already in place.

Migrating manually installed clients to centrally managed with Group Policy

If the administrator has manually installed the Foldr client on Windows clients, you can simply migrate/upgrade to a managed installation by following the same installation steps as given above. The installation will overwrite the manually installed version, however any existing app configuration / settings will be retained.

Configuring the Foldr app with Group Policy Preferences

There are various aspects on the Foldr app that can be configured by the administrator such as the Foldr server address, drive mode, cache settings, security options and so on. All registry keys

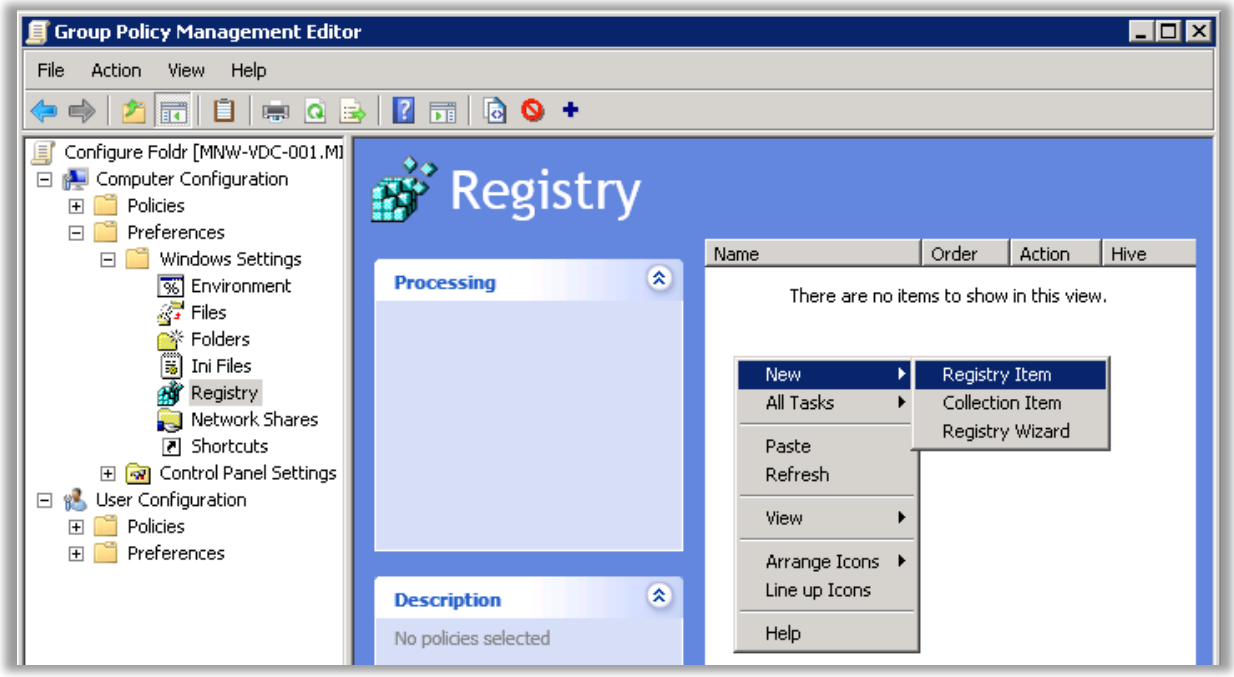
On a manual installation, to configure the app at the time of installation the administrator would typically run the MSI using the msiexec utility and append various options. These options would in turn write registry keys in **HKEY_LOCAL_MACHINE > Software > Foldr > Default** to provide global settings for any user that uses the Foldr app / drive.

The app can be configured in a managed installation easily using Group Policy Preferences (GPP) to write the registry keys and apply these onto client machines. Note - the app doesn't even need to be installed via Group Policy, an administrator could use GPP to modify the configuration of the Foldr app on machines that had the software installed manually.

1. Create a new GPO or edit an existing policy that would apply to the Windows clients in Group Policy Management Console.

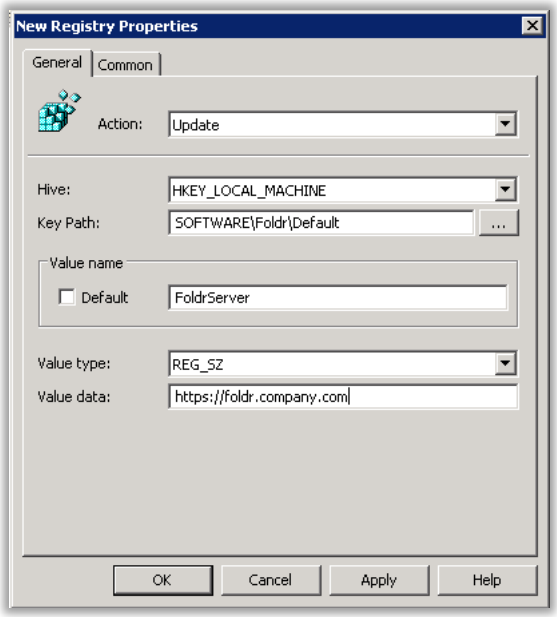
2. Navigate to *Computer Configuration* > *Preferences* > *Windows* > *Registry*

3. Create a new **Registry Item** from the context menu.



4. Configure the item as shown (Example)

Action = Update
Hive = HKEY_LOCAL_MACHINE
Key Path = SOFTWARE\Foldr\Default
Value name = *Registry Key* (see table above)
Value type = REG_SZ
Value data = (1|0 / string etc - see table above)



Click OK and create as many registry items as required to configure the app to your requirements.

Upgrading the Windows App

The app can be upgraded either using the built-in update mechanism

Foldr for macOS

The macOS drive mapping client provides access to any storage presented through Foldr directly from Finder using a single drive. On-premise storage (SMB shares) can be presented alongside Cloud Storage inside the drive.

Limitations:

The app currently does not provide sharing features (share with others or public links etc). Users should use the Foldr web app if they need to use these features.

System Requirements

macOS 10.9 or higher

Antivirus Software

Some antivirus applications can adversely interfere with the Foldr app and mounted drive affecting its usability and performance. Depending on the antivirus client and configuration, the client may also 'trawl' through the mounted drive to scan files and as a result put the server under unnecessary load and at the same time-wasting local storage as the files are downloaded into the local cache. If antivirus software must be used, it is recommended to exclude the local cache location (~/Library/Foldr) and all subfolders.

Installing/Deploying the app

The drive mapping client is provided in standard disk image (.DMG) format can be installed manually or deployed en-masse by enterprise deployment tools, such as JAMF Casper Suite or a compatible MDM solution. Note that we do not provide a .PKG version of the app and Foldr for macOS is not available from the Mac App Store.

The administrator can optionally set various options / preferences to configure the application as required.

Installation Options

– FOLDR_SERVER

– UPDATES_ENABLED

– SIGN_OUT_ON_EXIT

– VOLUME_NAME

– SHARES

– OPEN_DRIVE_DEFAULT

– DETECT_RENAME_THREAT

– DETECT_EXTENSIONS_THREAT

– GATEKEEPER_REQUIRED

– FILEVAULT_REQUIRED

– USE_MY_FILES

– PRESERVE_WRF_ON_SIGN_OUT

– USE_OFFICE_ASSIST

App Options

To set app preferences, you are required to use sudo in the Terminal. This could be automated using a script or using MDM or macOS management solution that supports that functionality:

```
sudo defaults write /Library/Preferences/it.minnow.FoldrAdmin OPTION VALUE
```

Examples:

```
sudo defaults write /Library/Preferences/it.minnow.FoldrAdmin FOLDR_SERVER
"my.foldr-server.address"

sudo defaults write /Library/Preferences/it.minnow.FoldrAdmin
UPDATES_ENABLED 0

sudo defaults write /Library/Preferences/it.minnow.FoldrAdmin
SIGN_OUT_ON_EXIT 1

sudo defaults write /Library/Preferences/it.minnow.FoldrAdmin.plist
VOLUME_NAME "newname"

sudo defaults write /Library/Preferences/it.minnow.FoldrAdmin.plist SHARES
"1,3,5"

sudo defaults write /Library/Preferences/it.minnow.FoldrAdmin.plist
OPEN_DRIVE_DEFAULT 1

sudo defaults write /Library/Preferences/it.minnow.FoldrAdmin.plist
DETECT_RENAME_THREAT 1

sudo defaults write /Library/Preferences/it.minnow.FoldrAdmin.plist
DETECT_EXTENSIONS_THREAT 1

sudo defaults write /Library/Preferences/it.minnow.FoldrAdmin.plist
GATEKEEPER_REQUIRED 1

sudo defaults write /Library/Preferences/it.minnow.FoldrAdmin.plist
FILEVAULT_REQUIRED 1

sudo defaults write /Library/Preferences/it.minnow.FoldrAdmin.plist
USE_MY_FILES 1 or 0

sudo defaults write /Library/Preferences/it.minnow.FoldrAdmin.plist
PRESERVE_WRF_ON_SIGN_OUT 1 or 0

sudo defaults write /Library/Preferences/it.minnow.FoldrAdmin.plist
USE_OFFICE_ASSIST 1 or 0
```

Installation Option Details

FOLDR_SERVER

If the option is absent, then the server address on the sign-in form will be empty until the user configures an account.

If FOLDR_SERVER=”address”, then the specified address will be used on the sign-in form when the user hasn’t yet configured their account.

UPDATES_ENABLED
If the option is absent, then the user can configure whether Foldr checks for updates.

If UPDATES_ENABLED=0, then Foldr will not check for updates. The user will not be able to change the setting.

If UPDATES_ENABLED=1, then Foldr will check for updates, by default. The user will be able to change the setting and may also choose to skip updates.

SIGN_OUT_ON_EXIT

If the option is absent, then the user can configure whether Foldr signs-in automatically.

If SIGN_OUT_ON_EXIT=0, the user does not need to provide login credentials when the app is run. The user will sign-in automatically and will be unable to change the setting.

If SIGN_OUT_ON_EXIT=1, then the user will need to sign-in manually each time the Foldr app starts. They will NOT be able to change the setting.

VOLUME_NAME

Determines the name of the Foldr drive as shown in Finder. If the volume name has not been set by admin, then we allow the user to change the name in the Drive Preferences.

Volume Naming Limitations:

- Length is greater than zero and less than 30 characters.
- Volume name must not contain a colon.

If the VOLUME_NAME contains an error, it will be ignored and the default name “Foldr” will be shown.

SHARES

Determines which shares are available to the user through Finder. If the option is not configured or an empty value is set, all shares will be available.

Otherwise, use a comma separated list of share IDs to specify which shares should be available, all others will be hidden from the drive. The share ID can be found in the ***Foldr Settings > Files & Storage*** area (shown at the end of the URL when editing a share)

OPEN_DRIVE_DEFAULT

Determines whether the drive should be displayed to the user automatically when it is mounted, i.e. after the user signs in.

DETECT_RENAME_THREAT

Determines whether the app detects rename threats and disconnect the drive immediately if detected. This can include multiple rename attempts in quick succession. If enabled, then the user will not be able to override the setting.

DETECT_EXTENSIONS_THREAT

Determines whether the app detects filename/extension threats. This is a pre-defined list of known malicious file extensions. If enabled, then the user will not be able to override the setting.

GATEKEEPER_REQUIRED

Determines whether the app requires macOS Gatekeeper protection to be enabled / running. If enabled, then the user will not be able to override the setting.

FILEVAULT_REQUIRED

Determines whether macOS File Vault full-disk encryption is required on the client to allow the drive to mount. If enabled, then the user will not be able to override the setting.

USE_MY_FILES

Determines whether ‘My Files’ and ‘Bookmarks’ are shown in the root of the Foldr drive. When enabled, the storage locations available to the user will be contained within the ‘My Files’ directory. When disabled, the storage locations will be shown in the root of the Foldr drive.

PRESERVE_WRF_ON_SIGN_OUT

Working File Recovery (WFR) is a feature that provides an in-app recycle bin for files that have been worked on from the Foldr drive. The app and it will keep a copy of each document/file in the WFR location for every save action.

By default files in the WFR location will remain if the app is quit (or machine is shutdown). However, if the user **signs out** of the app, the default behaviour is for files in the WFR store to be **deleted**. Foldr will automatically manage files in the WFR store in-line with the setting to manage the cache (Clear cached files after x days). Manually clearing the cache will not affect files in the WFR store.

The admin option *PRESERVE_WFR_ON_SIGN_OUT* allows the administrator to change the app behaviour so files in the WFR store are not deleted if the user signs out of the app.

If the argument is set to 1 – Working files in the filesystem WFR folder are preserved on sign-out. The user will be unable to configure the setting.

If the argument is set to 0 – Working files in the filesystem WFR folder are removed on sign-out. The user will be unable to configure the setting.

USE_OFFICE_ASSIST

Determines whether locally installed Office apps will open Office documents hosted in Office 365 locations directly via their Online URL. This removes the Foldr server and default save/upload mechanism from the workflow and allows the Office apps to behave natively with 365 documents (from OneDrive, Teams or SharePoint Online). Autosave and will automatically enabled in the Office apps and collaborative editing will function as normal with other Office 365 users.

Reading Configured Options

How to read any options that are currently set:

```
sudo defaults read /Library/Preferences/it.minnow.FoldrAdmin
```

Deleting Options

To unset an option, use the following command:

```
sudo defaults delete /Library/Preferences/it.minnow.FoldrAdmin OPTION
```

Configuring Foldr Desktop Apps from the Server using App Profiles

The Foldr server can apply specific client settings to client apps on a per user/group basis using App Profiles. App Profiles are available for both Windows and macOS Foldr apps.

When using App Profiles, it is important to consider that the server always takes precedence over local client settings.

App Profiles could be useful if you needed to apply a specific change to the app for an individual or a group of users, without having to redeploy the client app or push out other client settings to the registry via Group Policy or script.

An online article for server-based App Profiles and how to configure them is available on the knowledge base.

25. Managing & configuring the Foldr iOS app (MDM)

As well as being available on the App Store, the Foldr iOS app can be 'purchased' via the Apple VPP store and delivered to your iOS devices using a compatible Mobile Device Management (Solution using Managed Distribution. As well as deploying the app en-masse, an administrator is also able to preconfigure the app mode, set various app settings and enforce security settings as appropriate.

The following MDM solutions are a selection of vendors that support Managed App Configuration which is required to configure third party apps, such as Foldr.

AirWatch - instructions
Lightspeed Systems Mobile Manager - instructions
The Casper Suite - instructions

Apple devices use specially formatted XML files, known as Property Lists or 'plists', to store their settings. You can find more information on Property Lists here. Example plist files for configuring the Foldr iOS app are shown below and can be configured / modified as required and imported into your MDM solution.

Example App Config – Shared mode

The example below configures the app in shared mode, sets the Foldr server address and enforces it, shows the shares list automatically when logged in, disables untrusted certificate prompts and finally sets an automatic log out / idle timeout of 5 minutes.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>

<key>appMode</key>
<integer>0</integer>

<key>serverURL</key>
<string>foldr.yourdomain.com</string>

<key>serverFixed</key>
<true />

<key>homeShowShares</key>
<true />

<key>disableCertificatePrompts</key>
<true />

<key>sharedTimeout</key>
<integer>5</integer>
</dict>
</plist>
```

Example App Config – Personal Mode

The example below configures the app in personal mode, sets the Foldr server address, does not present the shares list automatically when logged in (shows My Files & Bookmarks instead), requires the user to set a security PIN, use the PIN each time the app is launched or brought into focus after

being backgrounded and finally sets the app to use a maximum cache value of 500MB.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>

<key>appMode</key>
<integer>1</integer>

<key>serverURL</key>
<string>foldr.yourdomain.com</string>

<key>homeShowShares</key>
<false />

<key>requirePIN</key>
<true />

<key>requireSecurityonWake</key>
<true />

<key> maxCacheSize</key>
<integer>500</integer>
</dict>
</plist>
```

The plist file consists of a list of settings, each followed by a value. Some settings also specify a type for their value. All available settings are shown below:

Setting	Value	Effect
appMode	integer set to either 0 or 1	Specifies whether the app runs in shared or personal mode. **0 = Shared** **1 = Personal** Not specifying this key allows the user to choose a mode to run in.
serverURL	string	The address of your Foldr server i.e. *foldr.yourdomain.com*
disableCertificatePrompts	boolean set to either true or false	Specifies whether the app should suppress invalid / untrusted SSL certificate prompts. By default, the app will present the user with a pop-up warning that the server is unverified when using a self-signed or expired certificate.
requirePIN	boolean set to either true or false	Specifies that the user MUST set a pin code on their Foldr app.
requirePassword	boolean set to either true or false	Specifies that a user MUST set a complex password on their Foldr app. Note that this overrides requirePIN.
requireSecurityOnWake	boolean set to either true or false	Requires that the user enter their pin/password whenever the app is brought to the foreground having been backgrounded. (Lock on Wake)
maxCacheSize	integer	Specifies the amount on local storage on the iOS device that the app consume for caching purposes. Accepted values are: *-1* = no limit *0* = no caching Any other value higher than zero indicates the size in MB to be used for caching. i.e. 123 = 123MB
serverFixed	boolean set to either false or true	Specifies if the Foldr server address is enforced and cannot be changed by the user.
sharedTimeout	integer set to number of minutes required	Automatically logs the app out if there is no activity for a set number of minutes. This option can only be used in Shared mode and the Foldr app must be backgrounded for this to function. Accepted values are: 0=no idle timeout (enforced) Any other value in minutes
homeShowShares	boolean set to either true or false	Automatically shows the shares list when logged in rather than My Files condensed & Bookmarks

webClient	string	Determines how the Foldr app should deal with web shortcuts (.url, .website etc) Accepted values: ***foldr*** = Default behaviour. The Foldr app will present the website using the built-in web client and display it in the standard file preview pane. ***safari*** = Safari will be used to display the web resource **off** = Disable loading web shortcuts Any other value will be treated as off
disableOfflineFiles	boolean set to either true or false	Removes the ability for a user to use the sync offline / make available offline feature in the app. If set to false, a user will still be able to use the feature.
quickAddLocked	boolean set to either true or false	If enabled, removes the ability for the user to configure or change the options that are offered through the Quick Add button.

Note that all fields are optional and may be removed from the plist as necessary.

Bundle ID

If the MDM solution being used requires the app's bundle ID, this is as follows:

it.minnow.foldr

26. External Access (Remote access or BYOD)

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)

It is possible to use a port other than TCP 443 for user sessions. See KB article for more information.

Should you wish to fully administer the system from outside of the network, the following ports should also be opened.

TCP port 5481 (SSL - Custom Update Settings)
TCP port 30537 (SSL - Foldr Settings web UI)
TCP port 2082 (SSH)

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 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:

https://kb.foldr.io/foldr-support/accessing-foldr-remotely-outside-your-organisations-network/

27. Foldr System Updates

Software updates for the Foldr appliance (product and operating system) are delivered over the Internet and can be managed within ***Foldr Settings > Appliance > Updates*** or alternatively https://address_of_Foldr:5481 > Updates.

A typical update takes several minutes to download and install, this may take longer depending on the speed of your Internet connection. Occasionally. larger feature updates are made available which will take longer to install, but it is important to allow the update process to complete gracefully. Under no circumstances should you reboot / reset the appliance mid-update. Please note, the appliance will always automatically restart when the update process completes.

If your network environment uses a proxy server to access the Internet this must be configured within ***Appliance > Network > HTTP Proxy***.

It is recommended that you configure the appliance to automatically download and install updates, however if preferred you can manually update during a routine maintenance window. As we constantly push both OS security updates and product features / fixes, you should always endeavour to keep the system up to date.

NOTE – Foldr will not be able to update over the internet if a HTTPS inspection (web filter / firewall) analyses the update traffic. This will cause the updates to fail a built-in digital signature validation check. Foldr should be excluded from any HTTPS inspection policy and the URL https://updates.minnow.it should also be whitelisted.

If the appliance cannot be excluded from HTTPS inspection, updates can be installed via an ISO file. Contact support@foldr.io for more information.

Updating a Cluster

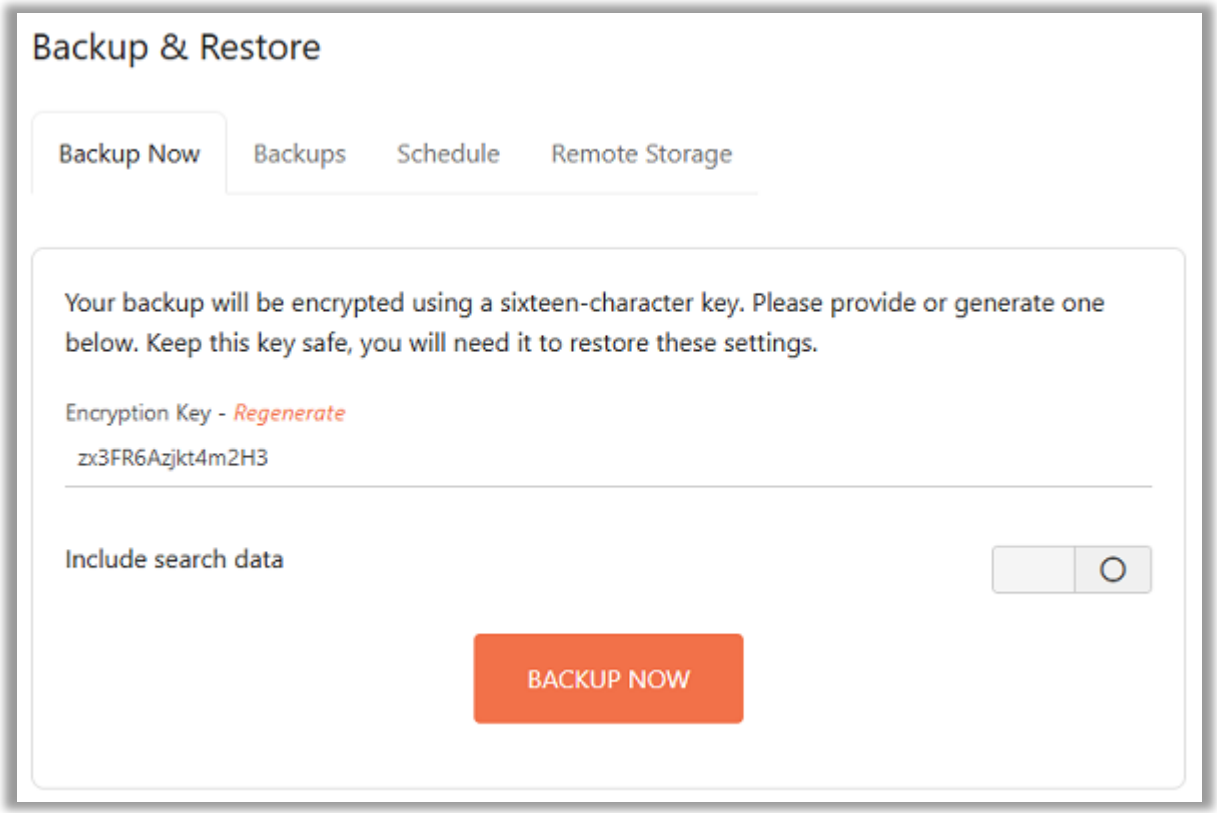
In a multi-appliance cluster installation, the administrator needs to update all appliances in the cluster, including any client access systems so they are running the same release version. It is recommended that you upgrade the infrastructure systems first, followed by the client access appliances. You can confirm that the database cluster is operational but checking **wsrep_cluster_size** returns the expected value within ***Foldr Settings > Infrastructure > Cluster***) – Note – client access VMs are not part of the database cluster itself.

Infrastructure appliances should be updated in a staged manner to allow each cluster node to fully restart and re-join the cluster before moving onto the next cluster member. As such it is recommended that you **avoid** using automatic updates to update all cluster members simultaneously.

28. Backup & Restore

Within ***Foldr Settings > Backup & Restore***, the Foldr administrator can save the appliance configuration settings, user activity logs and search index data to an encrypted file. All configuration settings, licence keys, LDAP Settings, shares, permissions and so on will be included in the backup. Note that SSL certificates and appliance network configuration are not included by design. The backup files may be stored on the appliance itself and optionally copied to a remote SMB share by an automated process. Appliance backups may be scheduled if required.

This feature could be useful to restore a working configuration either to the existing system or another Foldr appliance. They may be used to speed up the recovery in the event of a failure or when migrating the Foldr appliance from one hypervisor platform to another.



It is always recommended to include Foldr in your regular backup routine using the third-party solution of your choice (Veeam B&R, Nakivo B&R, Acronis, Backup Exec etc) – Foldr's own settings backup routine should be considered complimentary to a whole system backup.

Protecting the appliance during updates (Snapshots)

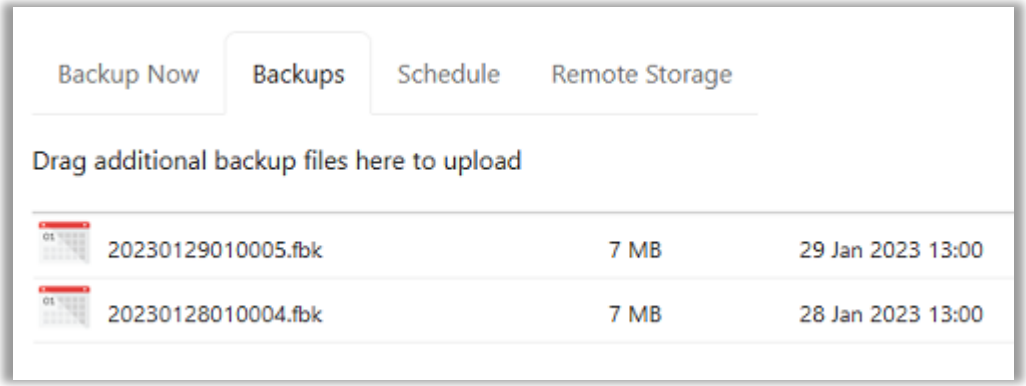
Where Foldr is deployed as a virtual machine, Hypervisor level snapshots should be employed before the system is updated from the online update server and snapshots should always be removed once the update has completed.

Creating a Backup

To create a standalone backup, simply enter a 16-character key (password) and click CREATE BACKUP. Note that the password must be exactly 16 characters in length as this is the encryption key

that will be used to decrypt and restore the backup later. The appliance can create a random 16-character key for you by clicking the text link provided in the dialog.

The backup file will be created and stored upon the appliance itself. The backup size and creation date will be shown as below:

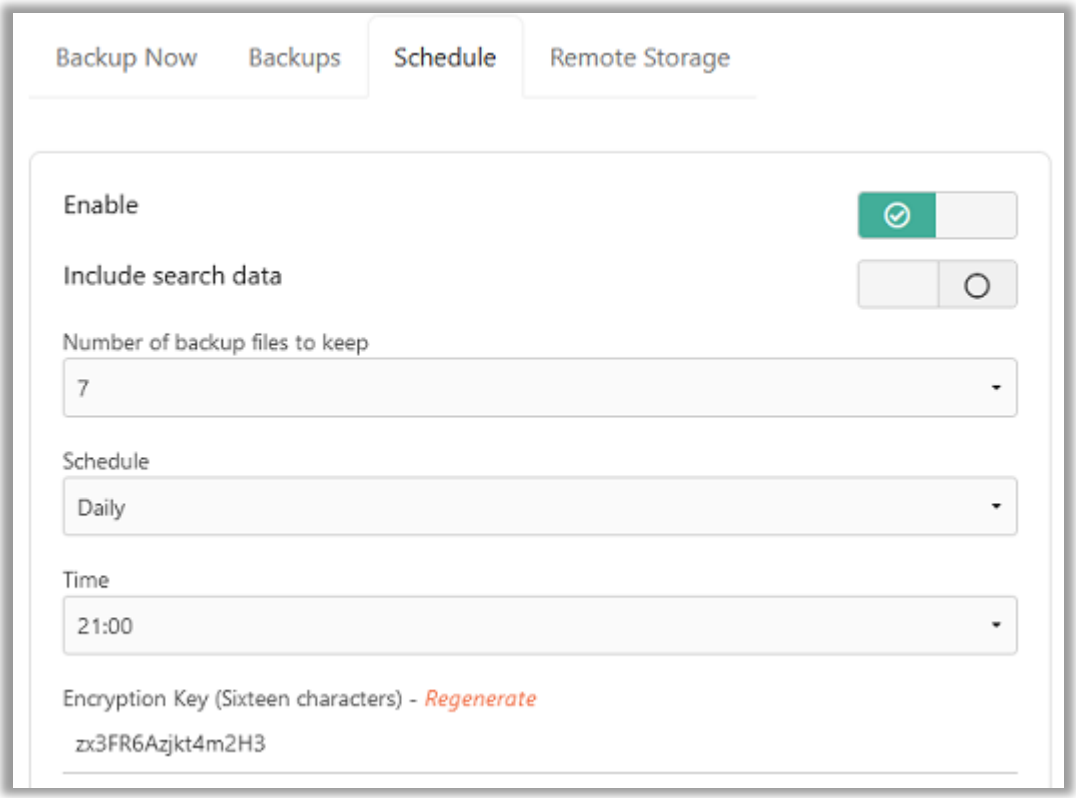


Scheduled / Automatic Backups

The appliance can schedule backups to be taken automatically at a time of your choosing. Within the Schedule tab, you can select the number of backups to store locally on the appliance and the time that the backup should be run, either daily, weekly, or monthly.

Weekly backups are run every Sunday at the time specified.

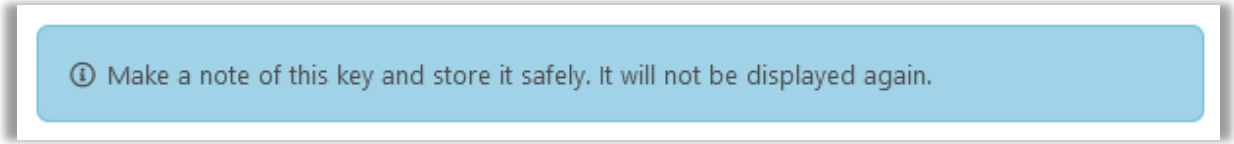
Monthly backups are run on the 1st of the month at the time specified.



To create a scheduled backup, select the configuration required and enter a 16-character key / password and finally click Save Changes. Alternatively, the appliance can create a random 16-character key by clicking the text link shown in the dialog.

Important - Make a note of the encryption key.

It is vital to make a note of the encryption key that is used for both standalone and scheduled backups as it will be required in the event that you need to restore the backup (even to the same system). Note that the key will not be displayed again later.

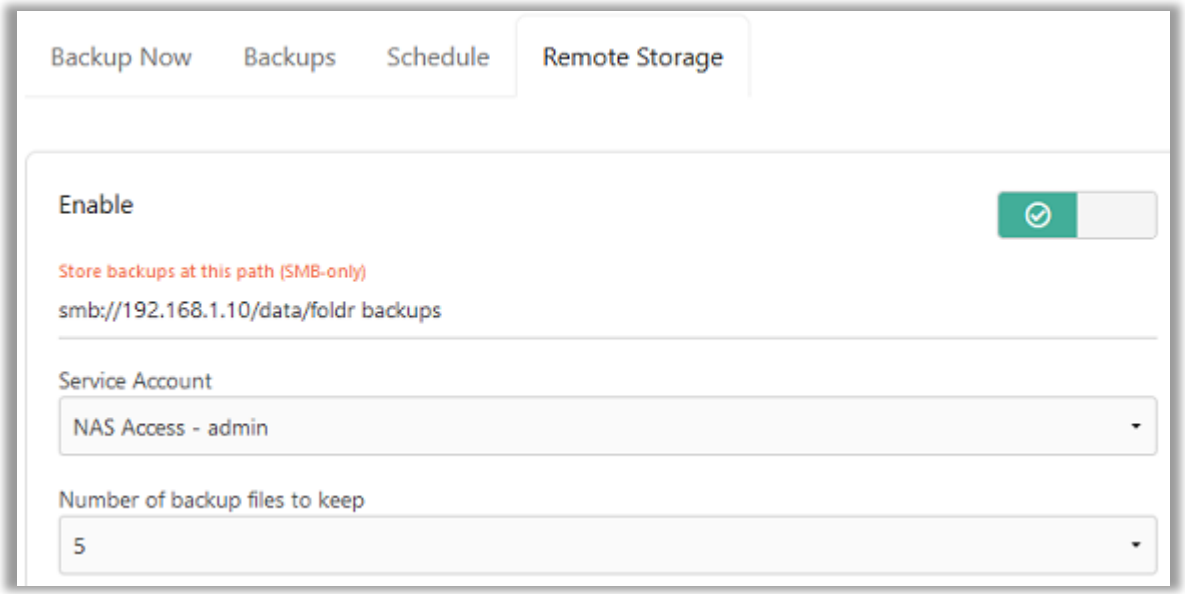


If you fail to make a note of the key, the backups will not be usable.

Copying backups to other storage (SMB)

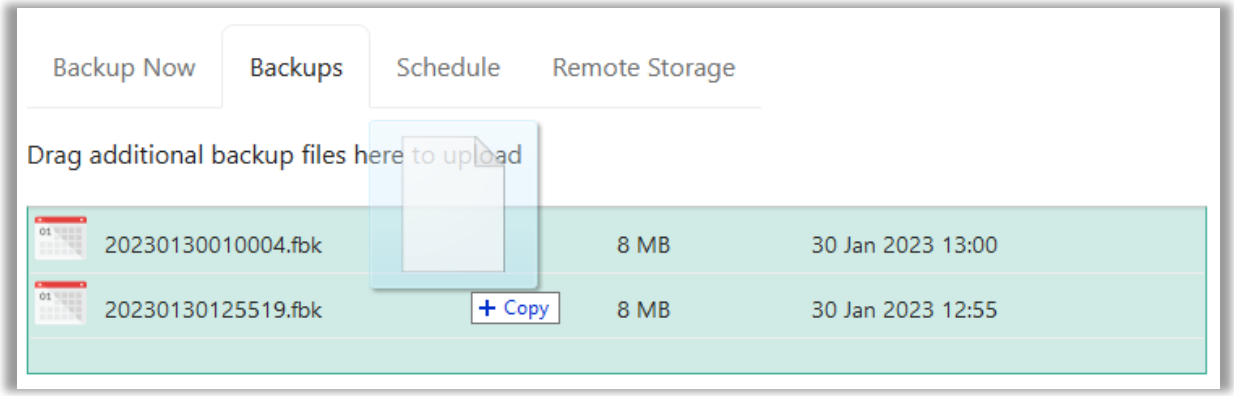
When standalone or scheduled backups are run, the backup file is always firstly created and saved locally on the Foldr appliance, however it can also be copied automatically to a remote SMB share (NAS or Windows file server etc.)

To enable this functionality, navigate to the Remote Storage tab and enter the SMB path to the share and select a suitable service account that has write permission to the share. Note that **all domain-based service accounts should be configured using the UPN** / username@domain.fqdn format.



Importing a Backup

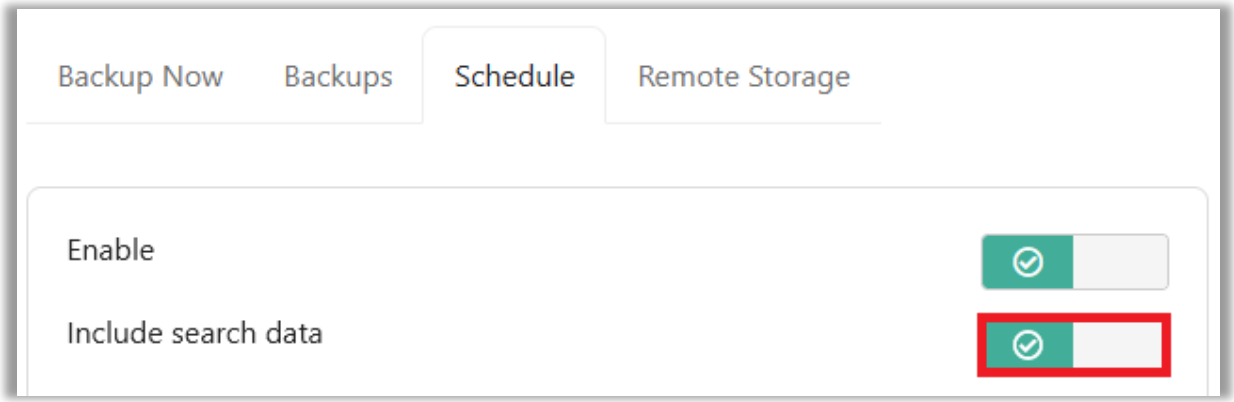
To import a backup file, navigate to ***Foldr Settings > Backup & Restore > Backups*** tab, drag/drop the backup file (.fbk) into the window. When the area goes green you can release the file to upload it to the appliance.



Important - If a large amount of data has been indexed the backup files can be many hundred MBs in size (or more). The administrator should consider limiting the number of backups stored locally on the appliance if using scheduled backups to limit the possibility of filling the virtual disk.

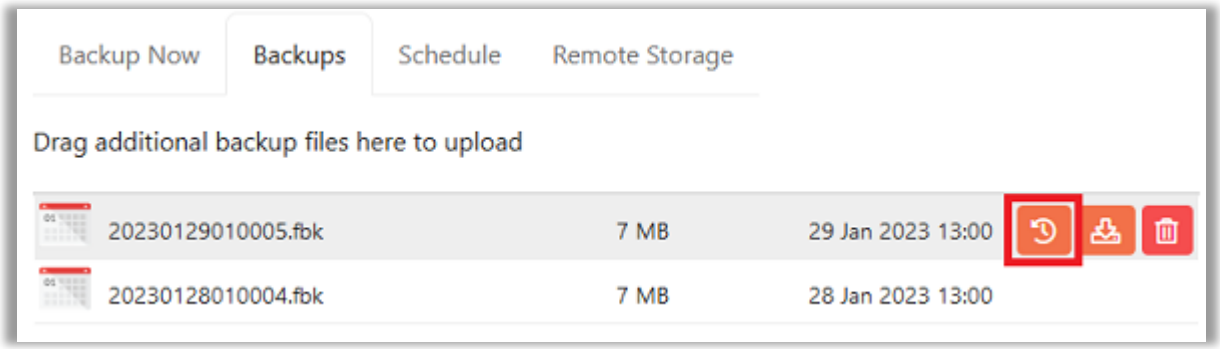
Backing up Search Data

If the server being backed up is running the search index service (indexing SMB shares) this data can be optionally backed up by enabling the 'Include search data' toggle on the **Backup Now** or **Schedule** tabs as required.

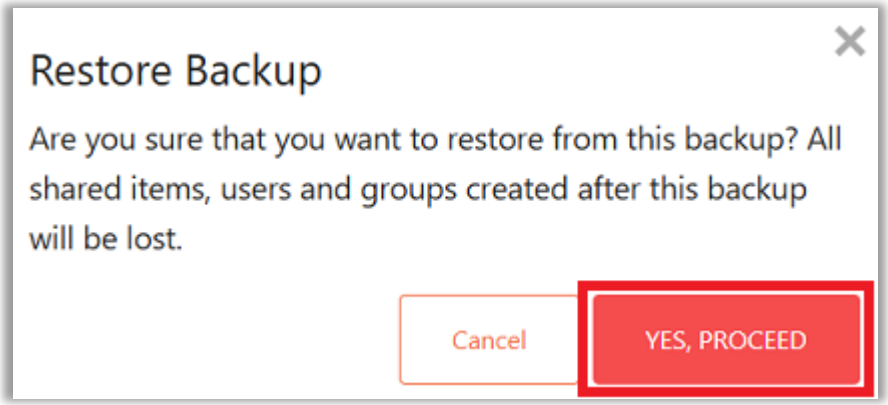


Restoring a Backup

To Restore a backup, mouse over the selected backup file from the list available and select the far left in-line button.



Agree to the prompt - click YES, RESTORE



Provide the backup encryption key and click OK

The backup will be restored, and the appliance configuration will be updated immediately. Where Search data has been restored, the Search index service will need to be manually started within ***Foldr Settings > Appliance > Services*** - restarting the Solr service.

Note that where backups are being restored into a new / unconfigured appliance, it is recommended that the server version is the same as that of the appliance where the backup was originally created.

29. Troubleshooting

Key points to check if Foldr is not authenticating Active Directory users or displaying shares:

1) Ensure the LDAP Server is prefixed ldap:// or ldaps:// as appropriate and that a suitable SERVICE ACCOUNT has been configured and is selected under the Integrations > Active Directory(LDAP).

All Active Directory service accounts must be configured using the account UPN (username@domain.fqdn)- Any other format such as a short username (samaccountname) or domain\username is considered invalid.

Foldr will be unable to authenticate users if a service account is not configured correctly.

2) The appliance hostname is FULLY QUALIFIED and is configured for the INTERNAL Active Directory domain.

This is important for internal short / unqualified DNS lookups. The hostname suffix is used automatically for the appliance Search Domain.

For example, if the Active Directory domain is ***domain.internal*** a suitable hostname for the appliance would be ***foldr.domain.internal***

Please note that the appliance hostname is not linked to the external FQDN that may be used to access Foldr, or any SSL certificates that are installed.

You may find that the mobile Foldr apps are unable to authenticate users if the device has a HTTP proxy configured and you may need to consider implementing a Proxy Auto Configuration file to deliver proxy settings (and exceptions) to these devices so a connection to the Foldr server can be made.

3) Check if the Foldr appliance can resolve server hostnames correctly from the console.

Log into the appliance console using the fadmin account and test DNS resolution using the ping and nslookup utilities.

4) The Search DN is configured correctly.

i.e. if the LDAP domain is domain.internal then the Search DN to encompass the entire domain would be:

DC=domain,DC=internal

5) Check the output of 'Test Settings'

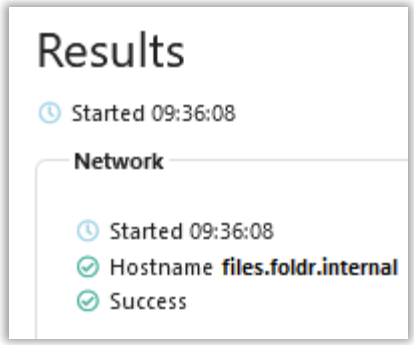
Test Settings is available within ***Foldr Settings > Top Right Menu > Test Settings*** and will indicate if Foldr is unable to authenticate the domain user & connect to the user's home folder, if configured within Active Directory > Profile tab

In this example the LDAP Server is configured as:

ldap://server

The warning is highlighting that the appliance hostname is 'foldr.local (default) and does not fall within the same domain as the configured LDAP (Active Directory) domain. As such any DNS lookup for a short / unqualified hostname will not resolve successfully, i.e. the system will be unable to resolve 'server' and authentication will fail.

After correcting the hostname to *foldr-hostname.internal-domain.fqdn* (files.foldr.internal in this case) the appliance can successfully resolve the unqualified LDAP server hostname and authentication is successful.



Further Troubleshooting & FAQ

What network ports are used by Foldr?

TCP port 25 (SMTP - Inbox feature to receive email if enabled and built-in firewall is modified)
TCP port 80 (HTTP - redirects to HTTPS for user sessions and required by Let's Encrypt as part of the SSL certificate installation process)
TCP port 389 (LDAP)
TCP port 443 (SSL – User sessions)
TCP port 445 (SMB)
TCP port 636 (LDAPS)
TCP port 5481 (SSL – Custom Update settings)
TCP port 30537 (SSL - Foldr Settings)
TCP port 2082 (SSH)
TCP port 22 (SSH – During initial setup only for Headless configuration in Azure / AWS etc)
TCP port 8983 (SSL – Foldr Search – This port is required inbound on the Search appliance)

Can I configure the network settings from the appliance console?

Log onto the console as fadmin (default password = password) and run the '**`netconfig`**' command.

DNS does not seem to be functioning correctly. The Foldr appliance can only resolve fully qualified hostnames.

By default, the Foldr system automatically uses the *hostname suffix* as the DNS Search Domain . As such it is vital that the hostname is configured fully qualified and relevant to the internal domain. Alternatively, configure the Search Domain itself within ***Foldr Settings > Appliance > Network***.

How can I troubleshoot network connectivity issues?

Ping, traceroute, dig, nslookup and netconfig are available for troubleshooting when logged into the virtual appliance console.

Is it possible to access on-premise and cloud storage via Foldr as a regular drive in Windows Explorer and macOS?

Using the Foldr Windows and macOS apps you can connect to Foldr and
access all storage locations within a single mapped drive. This is available for Windows 7-10 for both 32-bit and 64-bit systems. The Foldr Windows client supports two factor authentication, WebAuthn password change control, Google G Suite file support, Kerberos SSO or web sign in for SAML sign in and more.

More information and download links are available here:

https://foldr.io/products/foldr-for-files/microsoft-windows

Is it possible to access Foldr as a regular drive in Mac OS Finder?

A dedicated drive mapping client for macOS is available here:

https://foldr.io/products/foldr-for-files/macos

The macOS client offers the same features as the Windows client.

Is it possible to access Foldr via a WebDAV client?

You can connect to Foldr from a WebDAV client by connecting to https://address-of-foldr/drive (note **/drive**). Using a dedicated standalone WebDAV client, such as Cyberduck is recommended.

While macOS and Windows have built-in WebDAV support, WebDAV performance can vary massively between different versions of Windows and macOS. For the best user experience, it is recommended to avoid using WebDAV and instead use the dedicated Foldr desktop apps for access on these platforms.

Users are unable to connect to Foldr via WebDAV (Foldr Drive)

Ensure you are connecting to the usual Foldr address appending **/drive**. For example: https://address-of-foldr/drive

If using a dedicated WebDAV client, please enter /drive into the 'path' box.

Ensure the user's Active Directory account (or security group) has allow permission set for Connect via WebDAV within ***Foldr Settings > Security***. Note – The default built-in group 'Foldr Users' applies to all users.

Some standalone WebDAV clients will fail to connect unless the external hostname has been correctly configured within **Foldr Settings > Appliance**.

On Windows computers, ensure the 'Web Client' service is running under services.msc

It is recommended to use the dedicated Foldr clients for Windows or macOS instead of WebDAV if a mapped drive is required.

Forgotten fadmin account password?

If you have forgotten the administrative account password, contact Foldr support via *support@foldr.io* for assistance.

No Shares/Storage is available under MY FILES once the user is logged in.

This is most likely caused by either the shares having no permissions listed within ***Foldr Settings > Shares& Storage*** or simply that no additional shares have been configured and users home folders are not configured in Active Directory. This error may also be caused DNS resolution issues or incorrectly configured LDAP settings.

Use the 'Test Settings' tab found in ***Foldr Settings > General*** to troubleshoot where the log in or share mapping process is failing.

SMB file access appears to be slow.

This can be caused due to DNS lookups failing on the file server trying to resolve the Foldr appliance. As such please ensure that an A (host) record has been created on the organisation's *INTERNAL* DNS system (typically a Windows domain controller), matching the appliance hostname exactly as configured within ***Foldr Settings > Appliance > Network > Internal Hostname***. This host record must point at the IP address of the Foldr appliance.

The Foldr appliance is not performing as expected when running on Hyper-V

Please ensure that Virtual Machine Queues are disabled on your physical network adapters on the host server. VMQs can be the cause of network / performance issues on older Microsoft Hyper-V systems, especially where Broadcom NICs are being used.

How can I present Active Directory home folders to users?

Create a new share within *Foldr Settings > Files & Storage* using the storage address of **%homefolder%** -

This will automatically connect a user's home folder if one is configured within the Profile tab in Active Directory Users & Computers.

Home folders are not configured in Active Directory and login scripts or Group Policy Preferences are being used instead. How can these home folders be mapped to users automatically?

Foldr supports the standard environment variable **%username%** when creating share paths. You can add as many shares are required to support your user's home folder paths.

A user has logged into Foldr and can see all configured shares, including those that they shouldn't have access to.

It is important to remember that Foldr will always respect the underlying permissions already in place on the file server. If, for example, a user A logs into Foldr and can access a share that is intended for user B, then the NTFS security permissions / ACLs on the file server are incorrectly configured.

The recommended action in this case would be to correctly configure the backend permissions on the file server itself. However, if for any reason you're unable to amend the configuration on the file server you can use the Permissions feature within ***Foldr Settings > Files & Storage*** to control visibility of shares as required. This can be achieved by removing 'Foldr Users' and replacing with the appropriate users/groups. Deny rules may also be used here if required.

iOS devices are not streaming video content.

Ensure you have a valid, signed certificate installed on the appliance. This is a requirement of iOS to allow streaming over HTTPS.

Windows clients are successfully validating your signed certificate, but other platforms (iOS / Android) are displaying certificate trust warnings.

The Foldr appliance is missing the CA Root and/or Intermediate Chain files for your chosen certificate authority. Please reinstall all 4 files (signed certificate, private key, CA root & intermediate chain).

If your provider issues a bundle certificate instead of individual root and chain certificates, install the entire bundle within the 'Certificate Chain' field, leaving the CA Root field blank.

Providing the Foldr appliance is available externally, you can use one of the many SSL validation tools available such as the following to verify your installation and check the chain is complete:

https://www.sslshopper.com/ssl-checker.html

What are the minimum security permissions required for Foldr to successfully present an SMB share to users?

LIST FOLDER / READ DATA
READ ATTRIBUTES
READ EXTENDED ATTRIBUTES
READ PERMISSIONS

What Service Account permissions are required for 'Hand-Out' / 'Distribute' shared folders & Public Links?

As above.

What Service Account permissions are required for 'Hand-In' shared folders?

LIST FOLDER / READ DATA
READ ATTRIBUTES

READ EXTENDED ATTRIBUTES
READ PERMISSIONS
CREATE FILES / WRITE DATA
CREATE FOLDERS / APPEND DATA

Besides Hand-In permissions, what additional (recommended) Service Account permissions are required when using the shared 'Manage' functionality?

DELETE SUBFOLDERS AND FILES
DELETE

Let's Encrypt SSL certificate installation is failing with an error

Let's Encrypt will not successfully issue the SSL certificate when Foldr is behind a HTTPS inspection / MITM web filtering or firewall product intercepts and re-signs the network traffic between Foldr and the Certificate Authority. If a product of this type is deployed at the site, the Foldr appliance should be excluded from the https filtering policy. The external domain of '*letsencrypt.org*' should also be marked for exclusion from the HTTPS web filtering policy.

The Foldr appliance must be accessible externally over both **TCP port 80 (HTTP) and TCP port 443 (HTTPS)** for Let's Encrypt to successfully complete the certificate request, challenge handshake and installation.

More information on the Let's Encrypt project is available here and on their official website

What URLs should be white-listed and excluded from HTTPS inspection in a web filtering product to allow OneDrive / SharePoint integration to work correctly?

graph.microsoft.com
api.office.com
login.microsoftonline.com
{tenant}-my.sharepoint.com

i.e. foldr-my.sharepoint.com

What URLs should be white-listed and excluded from HTTPS inspection in a web filtering product to allow Google G Suite integration to work correctly?

googleapis.com
accounts.google.com