IBM COS FA Portal

TEAM ADMINISTRATOR GUIDE

This edition applies to IBM COS FA Portal Team Administrator Guide and is valid until replaced by new editions.

CONTENTS

CHAPTER 1. ABOUT IBM COS FA PORTAL

Note: Features and functionality in the user interface that are not covered in this documentation are not supported.

IBM Cloud Object Storage File Access (COS FA) is a software defined offering that provides SMB and NFS protocol interfaces to applications to store, archive and retrieve infrequently accessed files on IBM Cloud Object Storage.

The IBM COS FA Solution includes the following components:

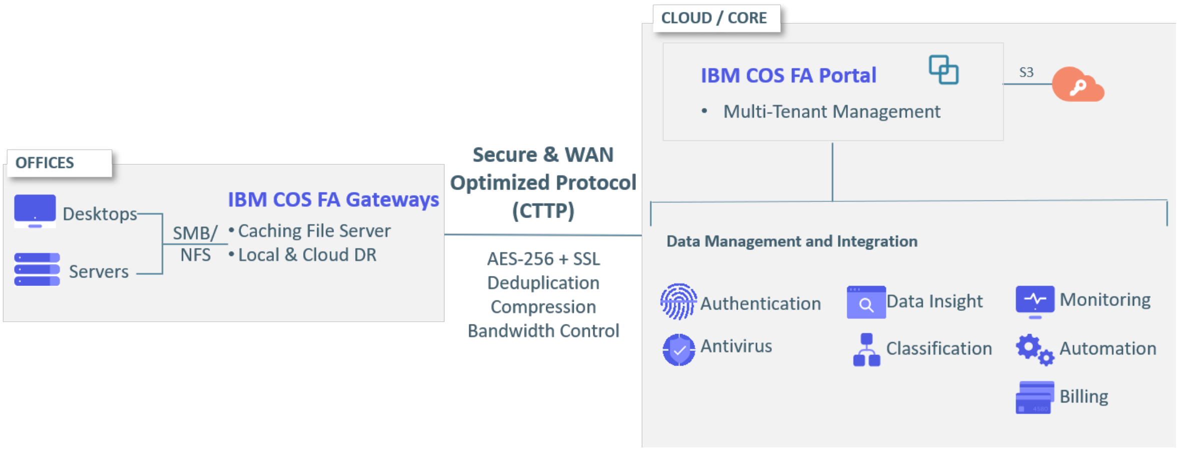
- IBM COS FA Portal
- IBM COS FA Gateway

The IBM COS FA Portal is the management component of the offering. The IBM COS FA Portal interacts with IBM COS FA Gateways and efficiently handles file data exchange between these applications and users and the private/public IBM Cloud Object Storage side. A centralized management console makes it possible to effectively manage a very large number of connected IBM COS FA Gateways.

The IBM COS FA Portal was designed to scale from tens to hundreds and thousands of connected IBM COS FA Gateways and to support an easy to scale file system with PBs of data and more. The IBM COS FA Portal it is capable of supporting both *scale-up* and *scale-out* deployment schemes: administrators may deploy the IBM COS FA Portal software on increasingly more powerful compute platforms, thus scaling the deployment up. Alternatively, they can distribute the IBM COS FA Portal processes on multiple concurrent compute platforms, thus scaling the deployment out. In addition, the file system is fully scalable by enlarging the database to accommodate data capacity growth.

The IBM COS FA Gateway is the component that the application and other data sources are connected to, and allows LAN speed writes via SMB and NFS protocols, and is in charge of onboarding the data to IBM Cloud Object Storage instantly and seamlessly.

Note: The IBM COS FA Gateway works in caching mode, which means that it has a dedicated local disk space to allow local LAN speed ingestion.



MANAGEMENT FEATURES

With the IBM COS FA Portal, you control all aspects of cloud storage, including:

- **Remote Device Management and Monitoring**
  Manage IBM COS FA Gateways remotely. This enables you to view the device status in detail, including logged events, network status, ands storage volumes, as well as to set firmware upgrades, and more.
- **Real-Time Event Monitoring**
  Centrally monitor and audit all events pertaining to the cloud service.
- **Reporting**
  Run and export detailed reports on a variety of usage parameters, including storage usage, bad files, snapshot status, and more. Generate user reports that are automatically emailed as PDF attachments.

SECURITY

IBM COS FA Portal incorporates multiple layered security features to ensure that your data is protected whether in transit or at rest:

- You can deploy the IBM COS FA Portal either on-premise or in a virtual private cloud (VPC) to keep your data within your network and 100% behind your firewall.
- IBM COS FA Portal uses cryptographic libraries certified with FIPS 140-2.
- All data is encrypted before it is sent to the cloud using AES-256 encryption and remains encrypted as it is stored.
- All WAN transfers use Transport Level Security (TLS) protocol over the WAN, preventing unauthorized interception of data transfers.
- Manage your own encryption keys or use personal passphrases per user to prevent privileged administrators from accessing data. Password policy enforcement ensures that passwords have a minimum length and complexity, and that the password is changed frequently.
- IBM COS FA Portal provides role-based access control, using Active Directory or LDAP roles and groups to control access to data and set up administrator roles.
- IBM COS FA Portal integrates with leading antivirus tools.

CHAPTER 2. GETTING STARTED

This chapter describes how to get started with the IBM COS FA Portal.

In this chapter

BROWSER REQUIREMENTS

You log on to your IBM COS FA Portal in a browser. You can use any of the latest two releases of Google Chrome, Apple Safari and Microsoft Edge.

THE ADMINISTRATION INTERFACE

IBM COS FA Portal provides an administration web interface for:

- Configuring and monitoring the IBM COS FA Portal
- Provisioning the virtual IBM COS FA Portal

LOGGING IN TO THE ADMINISTRATION INTERFACE

As an administrator, you have access to the administration Web interface. This interface lets you perform administration tasks for the IBM COS FA Portal.

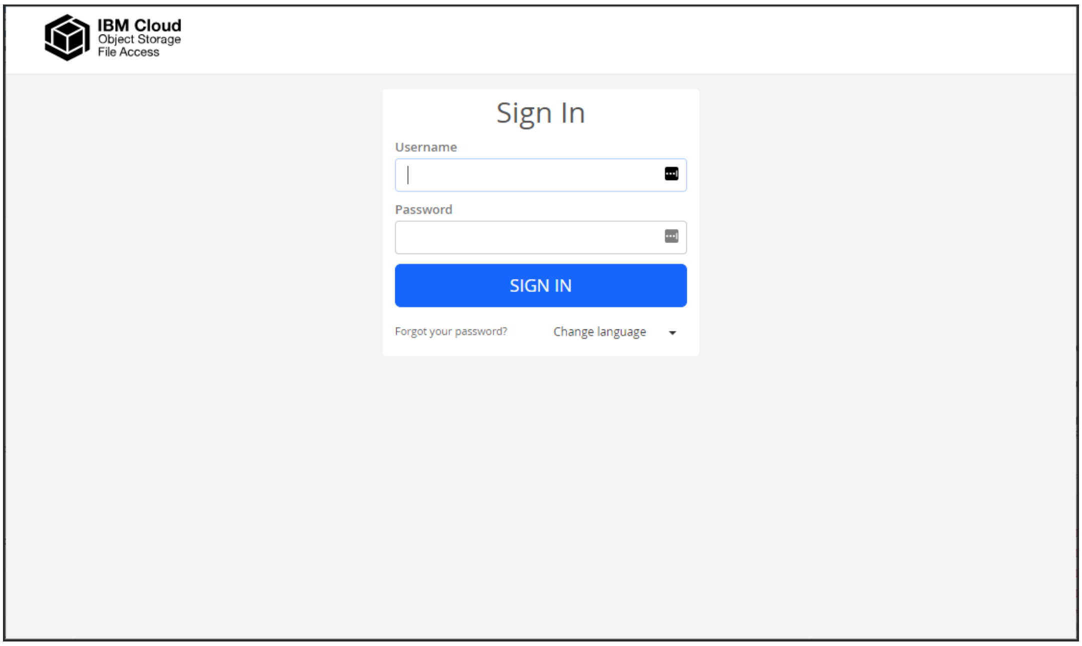
To log in to the administration interface you use the IP address of the IBM COS FA Portal server the DNS service is set up, you can use it with the IBM COS FA Portal's DNS suffix and, if changed from the default, the HTTPS access port number.

To log in to the administration interface:

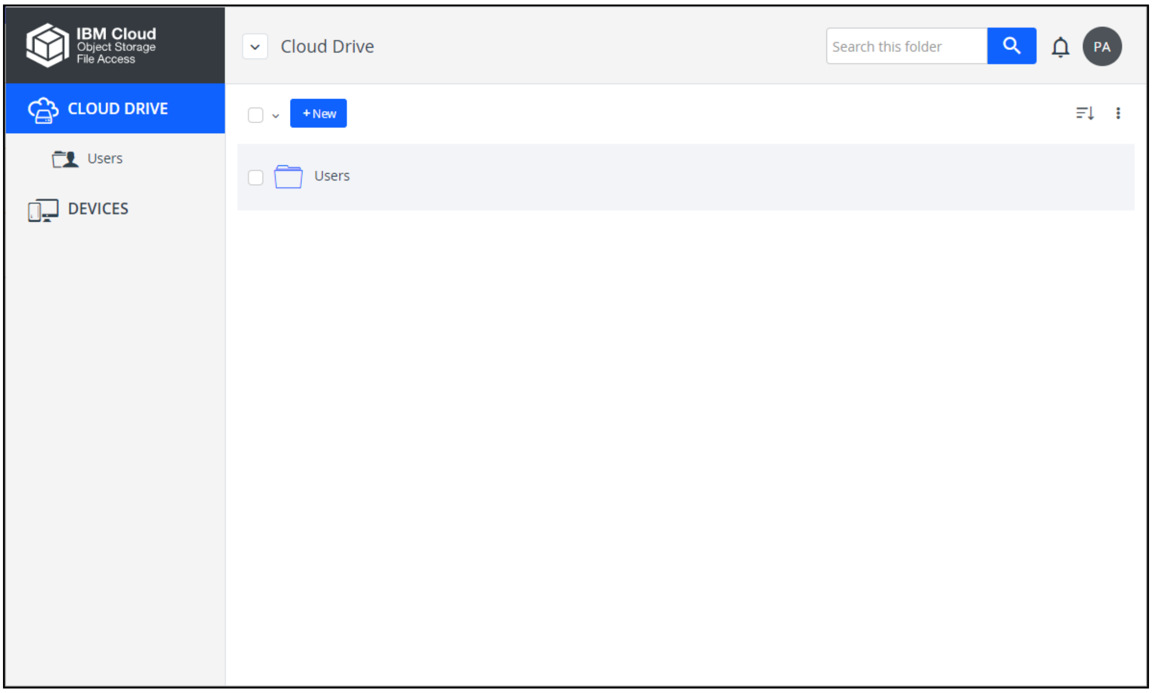
1 In a Web browser open
`http://<virtualportal_name>.<DNS_Suffix>/ServicesPortal`.
where, `<virtualportal_name>` is the name of any one of the virtual IBM COS FA Portals defined in IBM COS FA Portal, and `<DNS_Suffix>` is the DNS suffix for the whole IBM COS FA Portal installation.
This opens the interface to the specific IBM COS FA Portal's view.

Note: If the IBM COS FA Portal is set to redirect HTTP requests to HTTPS, IBM COS FA Portal redirects the browser to the HTTPS page. It is also possible to set the HTTPS access port to be different from the standard 443. In this case, the address is:
`https://<virtualportal_name>.<DNS_Suffix>:<HTTPS_port>/ServicesPortal`, where `<HTTPS_port>` is a customized port.
For example, to connect to Acme's administration IBM COS FA Portal using HTTPS port 2222, use the following address: `https://acme.ibm.com:2222/ServicesPortal`.

The IBM COS FA Portal opens, displaying the login page.

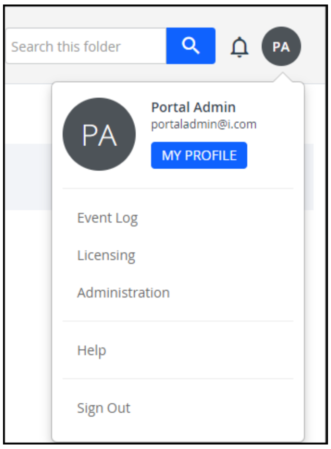


2 Enter your administrator user name and password and click **SIGN IN**.
The end user interface opens.

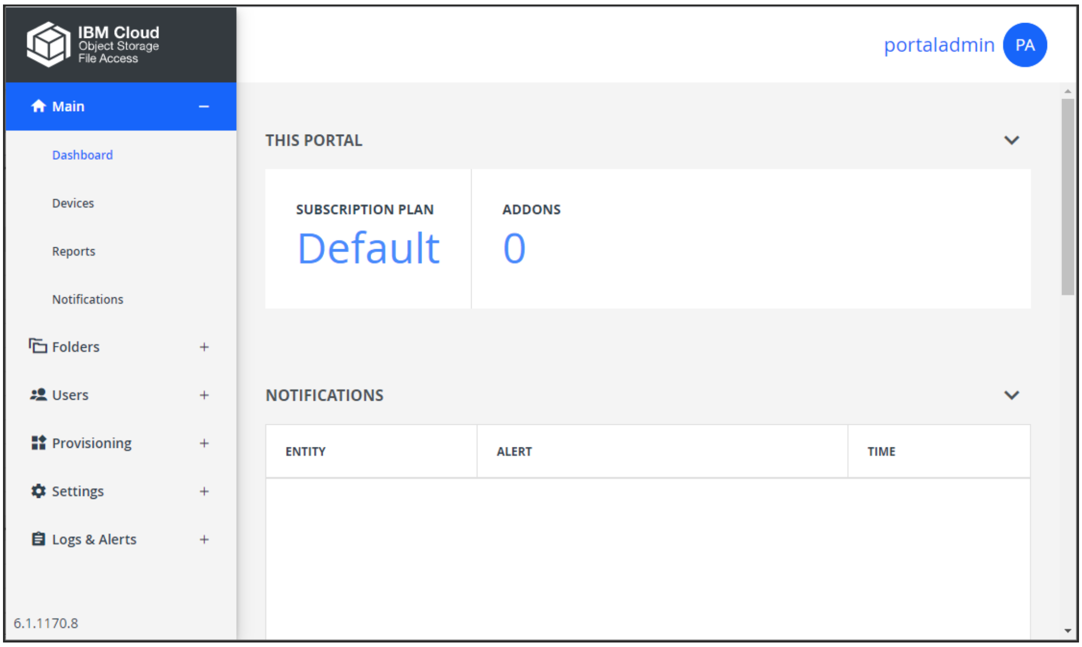


An administrator has options to manage the end users in this view, as described in Administrator Options In the End User Interface.

3 To access the full administrator interface, click the avatar at the top right, or your initials, if you have not yet configured an avatar, as described in Changing Your Personal Details, and select **Administration**.



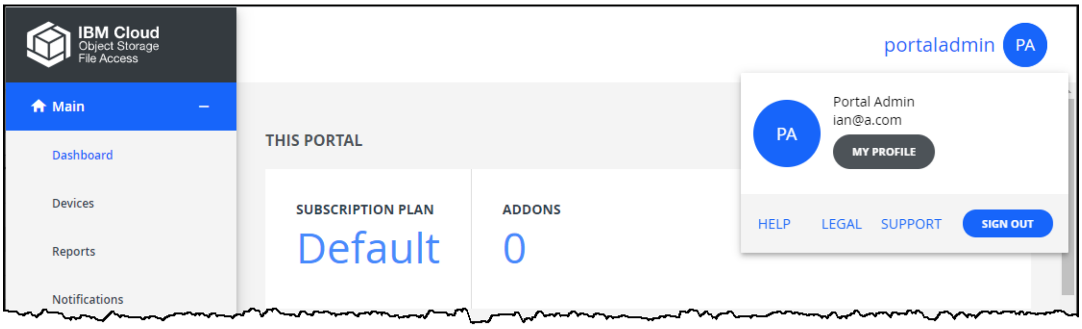
The administration interface opens in a new tab, displaying the **Main > Dashboard** page of the IBM COS FA Portal.



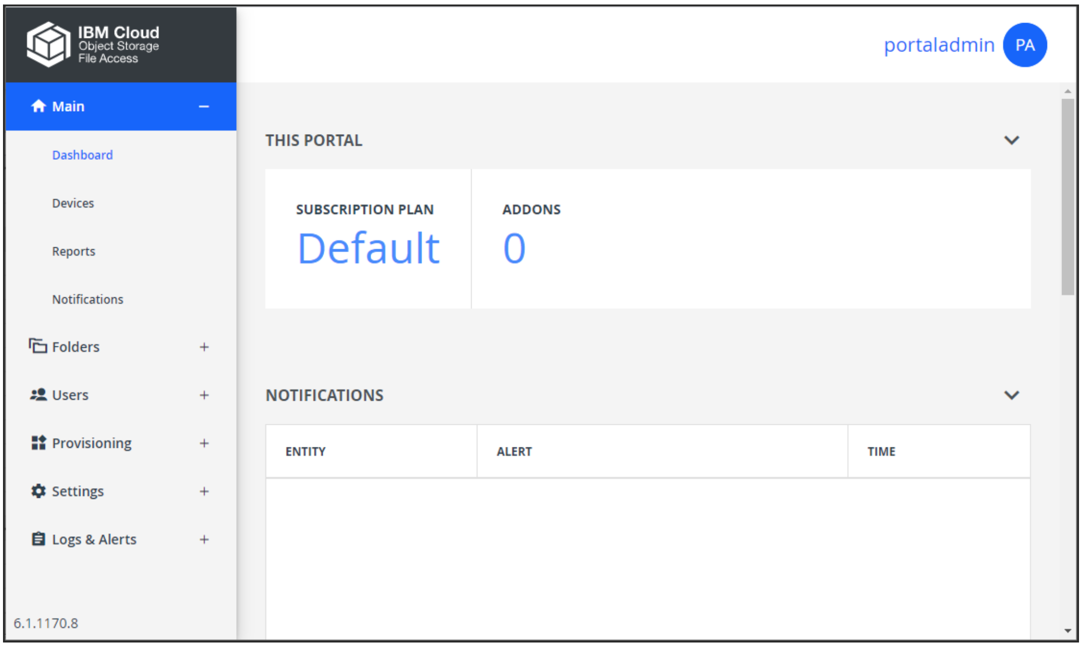
USING THE IBM COS FA PORTAL ADMINISTRATION INTERFACE

The IBM COS FA Portal interface consist of the following elements:

Top bar – The user name at the top right. Clicking the graphic next to the name displays additional controls, such as access to the online help.



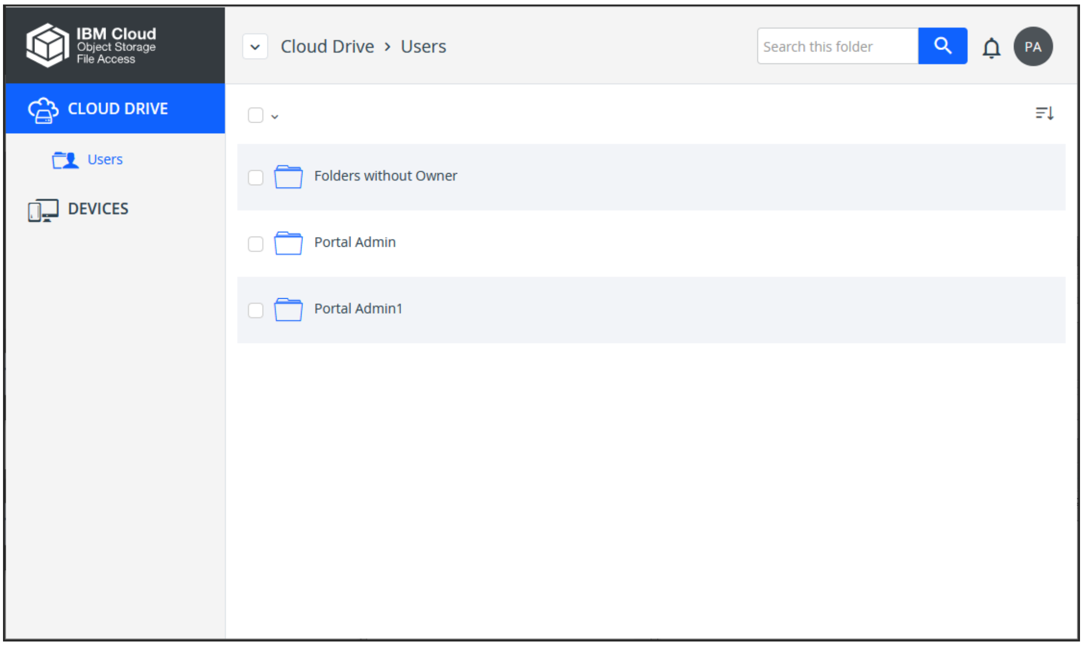
Navigation Pane – To navigate between pages in the IBM COS FA Portal.
Content – Displays the IBM COS FA Portal pages.



ADMINISTRATOR OPTIONS IN THE END USER INTERFACE

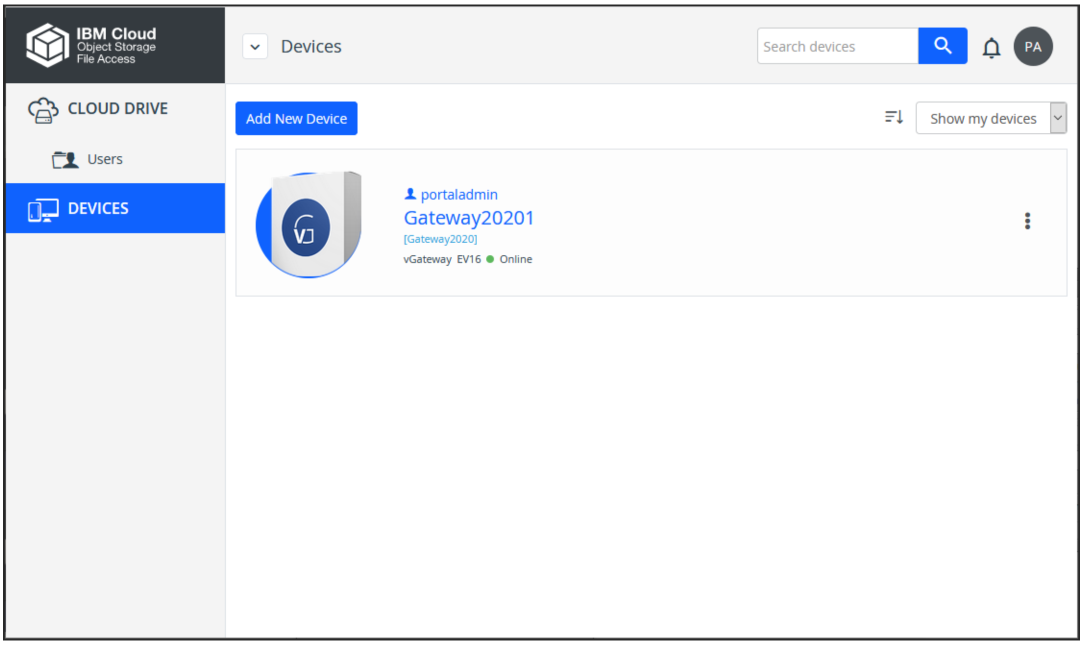
When you connect to an end user IBM COS FA Portal as an administrator you have the **Users** and DEVICE options.

Users Option



An administrator with the **Read Only Administrator** role can see the users and the folders for each user. An administrator with the **Read/Write Administrator** role can also manage the user folders and files as if he was that user.

DEVICES Option



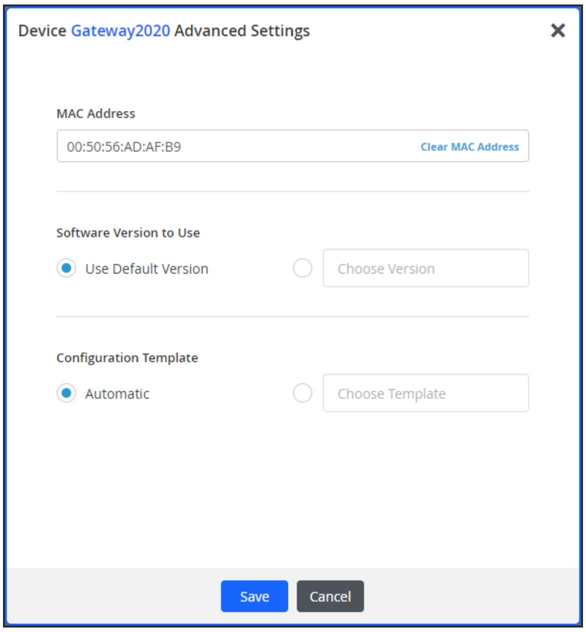
The end user IBM COS FA Portal displays all devices connected to the IBM COS FA Portal that you are managing.

To manage a device as an administrator:

1 Click the **DEVICES** option in the navigation pane.
This page displays all of the devices connected to the IBM COS FA Portal.

2 Click the ⋮ icon to the right of the device you want to manage. Options are displayed in a popup menu.
Rename Device – Rename the device.
Set Description – Provide a description of the device.
Restart Device – If, the device is running, this option is displayed enabling the administrator to remotely restart the device.

Advanced Settings – Advanced settings for the device.



Device Gateway2020 Advanced Settings

MAC Address

00:50:56:AD:AF:B9

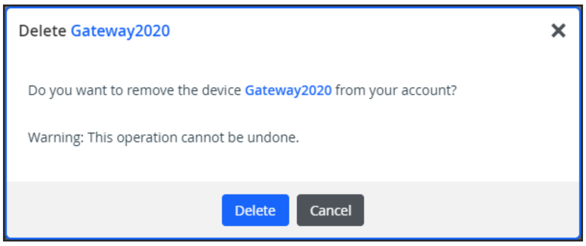
Software Version to Use

● Use Default Version ○ Choose Version

Configuration Template

● Automatic ○ Choose Template

Delete Device – Remove the device from the IBM COS FA Portal. This does not delete the actual device.



Delete Gateway2020

Do you want to remove the device Gateway2020 from your account?

Warning: This operation cannot be undone.

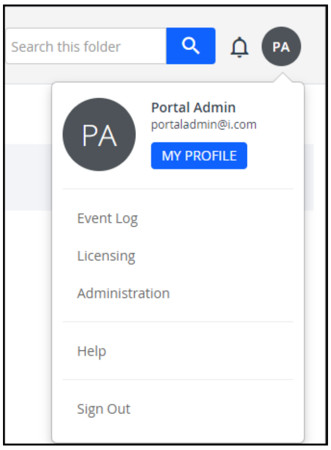
Changing Your Personal Details

You can configure the following personal details:

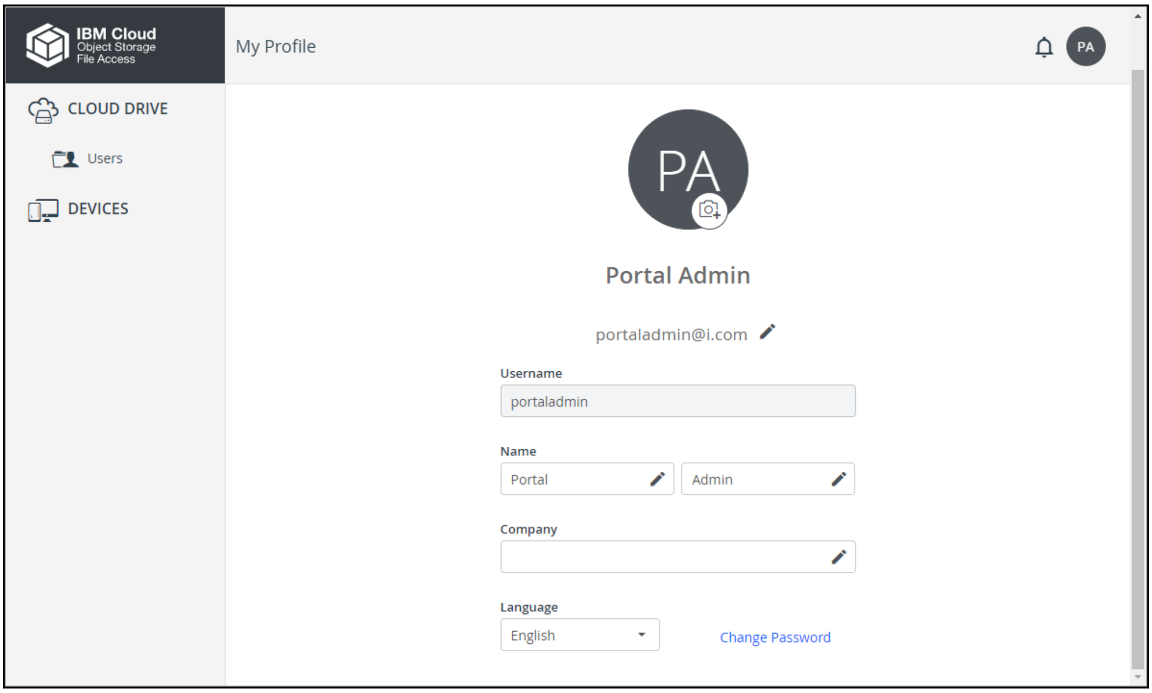
- Add or change the avatar used to identify you. If an avatar is not used, your initials are used.
- Your email address.
- Your first and last name. If you do not have an avatar, the initials of the first and last name displayed here are used.
- Your company.

To configure your user profile:

1 Click your avatar or initials in the upper-right corner and in the menu, click **MY PROFILE**.



The **My Profile** page is displayed.



2 You can upload an avatar by clicking and selecting your picture. The picture must be a JPEG or PNG file.
The avatar is displayed instead of your initials.

3 To change information, click ✎ by the item to change, enter the change and click ☑ to confirm the change.

Note: To change your email address you have to enter the and user password to the IBM COS FA Portal and then confirm the email change after receiving a verification email to the new email address.

To exit your profile, click on one of the options in the navigation bar.

Changing the Interface Language

You can change the user interface language from the **My Profile** page.

- You can also change the language in the sign in page

To change the user interface language:

1. Click your avatar or initials in the upper-right corner and then in the menu click **MY PROFILE**.
2. Select the desired language in the **Language** drop-down list.

After a few seconds, the interface is refreshed with the chosen language.

Changing Your Password

If access to the IBM COS FA Portal is by a local user, You can change your password from the **My Profile** page.

A user accessing the IBM COS FA Portal using Active Directory, cannot change the password form this page, but must contact the system administrator.

To change the password used to access the IBM COS FA Portal:

1. Click the avatar in the upper-right corner, and then in the menu click **MY PROFILE**.
2. Click the **Change Password** link.
3. The **Change Password** window is displayed.
4. Complete the fields, then click **Change Password**.

CHAPTER 3. CONFIGURING IBM COS FA PORTAL SETTINGS

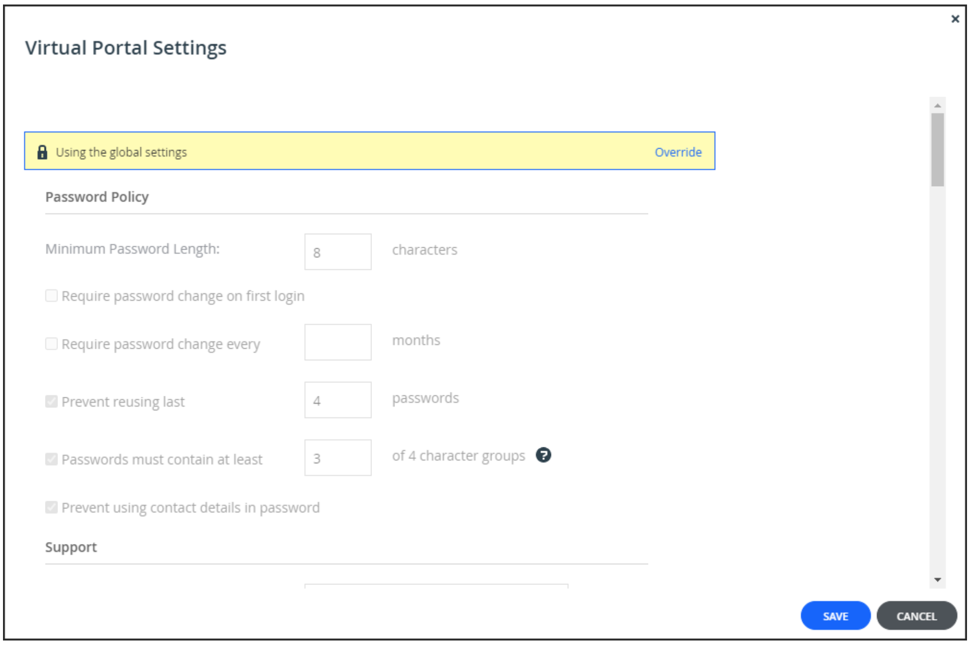
By default, the IBM COS FA Portal inherits its settings from global virtual IBM COS FA Portal settings, which are set for multiple virtual IBM COS FA Portals by a global administrator. You can override the global settings for the IBM COS FA Portal and modify the settings as needed.

In this chapter

To set virtual IBM COS FA Portal settings:

1 Select **Settings** in the navigation pane.

2 Select **Virtual Portal**, under **SETTINGS** in the **Control Panel** content page.
The **Virtual Portal Settings** window is displayed.



Virtual Portal Settings

🔒 Using the global settings — Override

Password Policy

Minimum Password Length: 8 characters

☐ Require password change on first login

☐ Require password change every months

☑ Prevent reusing last 4 passwords

☑ Passwords must contain at least 3 of 4 character groups

☑ Prevent using contact details in password

Support

3 Click **Override** to enable changing the default settings for the virtual IBM COS FA Portal.

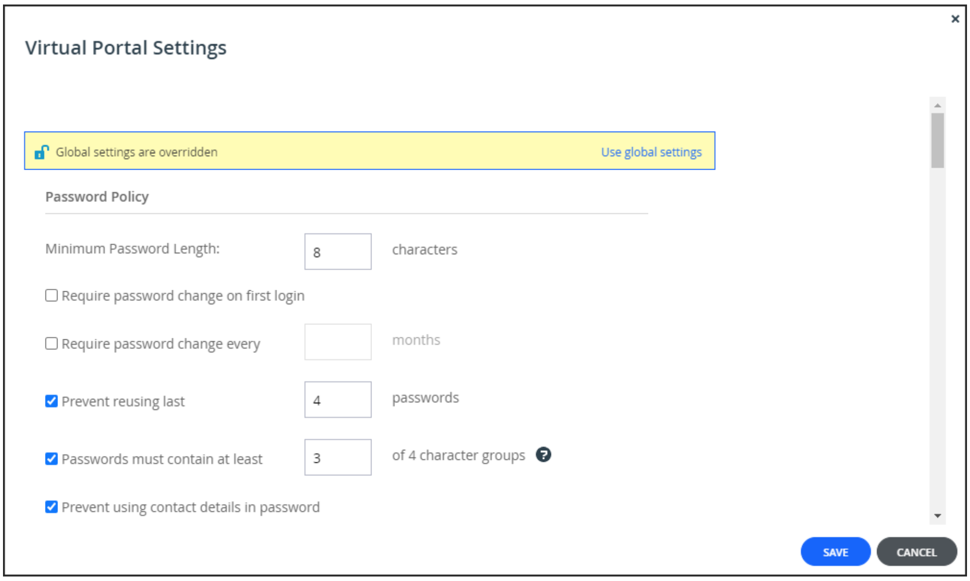
4 Change settings as required, as described below.

5 Click **SAVE**.

PASSWORD POLICY

IBM COS FA Portal features a password strength policy to comply with security standards. You can:

- Configure a password rotation cycle (in months)
- Prevent the re-use of the last X passwords
- Determine the number of character groups required in a user's password. The available character group values are:
  - Lowercase characters
  - Uppercase characters
  - Numerical characters
  - Special characters such as "!@#$"
- Prevent users from using their personal details in their password, including first name, last name, email, username, and company name.



Virtual Portal Settings

Global settings are overridden — Use global settings

Password Policy

Minimum Password Length: 8 characters

□ Require password change on first login

□ Require password change every [ ] months

☑ Prevent reusing last 4 passwords

☑ Passwords must contain at least 3 of 4 character groups

☑ Prevent using contact details in password

Minimum Password Length – The minimum number of characters that must be used in a IBM COS FA Portal account password. The default value is 8 characters.

Require password change on first login – Force users to change their password on their first login.

Require password change every – Force users to change their password after a certain number of months: Specify the number of months. When the specified number of months has elapsed, the user's password expires, and a new password must be provided on their next login.

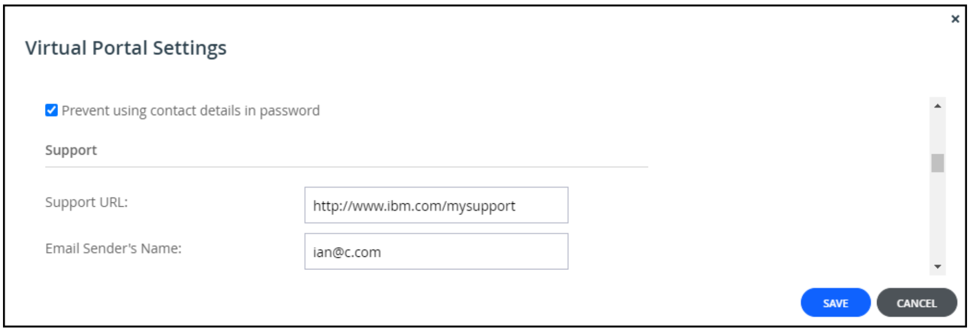
Prevent reusing last... passwords – Prevent users from reusing a specified number of their previous passwords when they change their password. Specify the number of previous passwords you want this to apply to.

Passwords must contain at least.... of 4 character groups – Require users to choose passwords that contain at least a specified number of the following character groups:

- Lowercase characters
- Uppercase characters
- Numerical characters
- Special characters such as "!@#$"

Prevent using contact details in password – Prevent users from using their personal details in their password, including first name, last name, email, username, and company name.

SUPPORT SETTINGS


Virtual Portal Settings

☑ Prevent using contact details in password

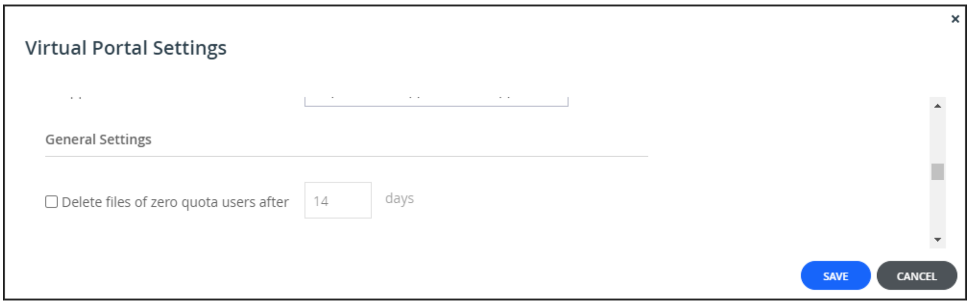
Support

Support URL: http://www.ibm.com/mysupport

Email Sender's Name: ian@c.com

Support URL – The URL to which IBM COS FA Portal users browse for customer support.
Email Sender's Name – The email address that is displayed in the **From** field of notifications sent to users by the virtual IBM COS FA Portal.

GENERAL SETTINGS

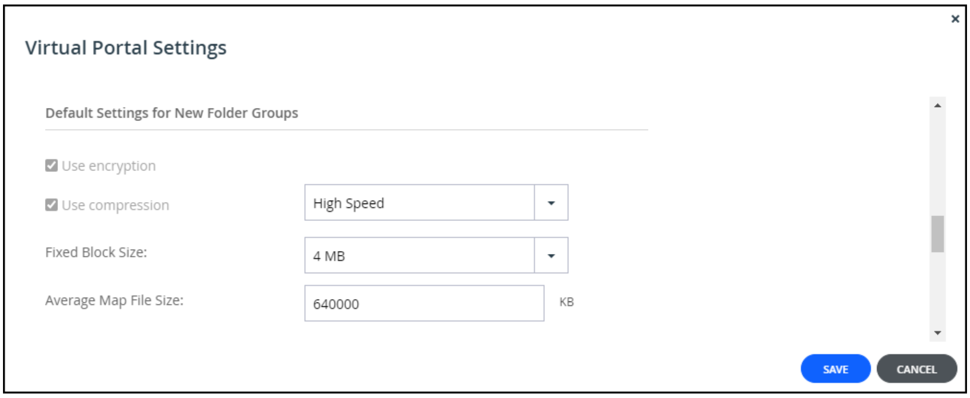

Virtual Portal Settings

General Settings

☐ Delete files of zero quota users after 14 days

Delete files of zero quota users after – The storage folders of customers who have no quota (for example, customers with expired trial accounts) are deleted automatically after a certain number of days. Enabling this option helps free storage space. A notification is sent to the customer prior to deletion, prompting the customer to purchase cloud storage in order to avoid the scheduled deletion of their files. Storage folders of over-quota users with a non-zero quota are not deleted. The default value is 14 days.

DEFAULT SETTINGS FOR NEW FOLDER GROUPS


Virtual Portal Settings

Default Settings for New Folder Groups

☑ Use encryption

☑ Use compression: High Speed

Fixed Block Size: 4 MB

Average Map File Size: 640000 KB

Note: Changes to these values do not affect existing folder groups.

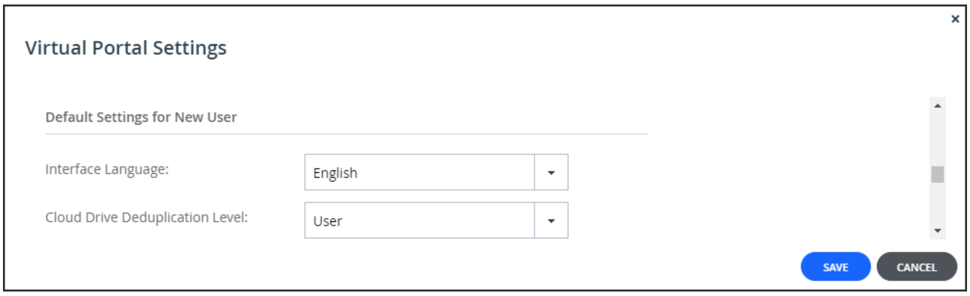
Use encryption – Data in newly created folder groups is stored in encrypted format by default.
Use compression – Specify which data compression method is selected by default for newly created folder groups:

- High Compression
- High Speed (default)

Fixed Block Size – The fixed block size used by the folder group. IBM COS FA Portal deduplication splits each stored file into blocks. Increasing the **Fixed Block Size** causes the files to be split into larger chunks before storage, and results in increased read/write throughput at the cost of a reduced deduplication ratio. Increased block size is useful for workloads that require high performance, as well as for those that do not gain greatly from deduplication. For example, where the stored files consist mostly of videos, images, and music files that are not frequently modified. IBM recommends keeping the default 4MB fixed block size.

Average Map File Size – The average map file size used by new folder groups. IBM COS FA Portal uses file maps to keep track of the blocks each file is made of. The Average Map File Size represents the maximum size of file that will be represented using a single file map object. For example, if the average map file size is set to 100MB, files of up to approximately 100MB will have one file map, files of up to approximately 200MB will have two file maps, and so on. Reducing the average map file size causes more file maps to be created per file. This may result in smoother streaming of files; however, it will also result in some extra overhead for creating, indexing, and fetching the additional file maps. The default value is 640,000KB. This value applies to new folder groups only and cannot be changed for existing folder groups.

DEFAULT SETTINGS FOR NEW USER


Virtual Portal Settings

Default Settings for New User

Interface Language: English

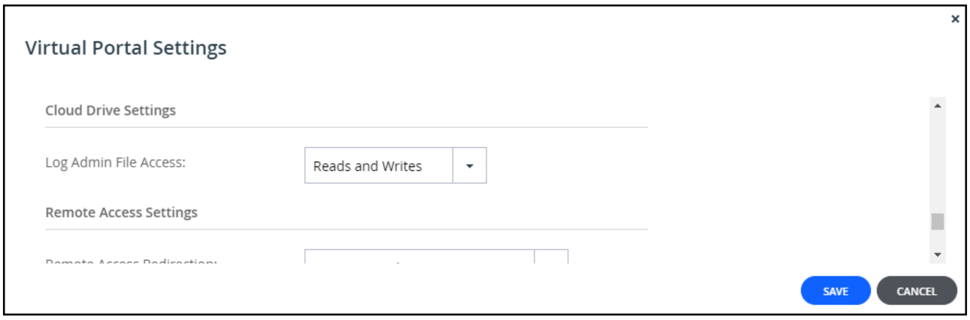
Cloud Drive Deduplication Level: User

Interface Language – The default language for new administrators.

Cloud Drive Deduplication Level – The default deduplication level to use for cloud folders, for all new users in team IBM COS FA Portals:

User – Create a single folder group for each user account, containing all of the user account's cloud folders. Deduplication is performed for the user account's folder group.
Portal – Create a single folder group for each virtual IBM COS FA Portal, containing all of the cloud folders in the team IBM COS FA Portal. Deduplication is increased but performance impacted and this setting is not recommended for large IBM COS FA Portals.
Folder – Create a folder group for each of a user account's devices, containing all of the device's cloud folders. Deduplication is performed separately for each of the user account's folder groups, decreasing the benefits of deduplication.

CLOUD DRIVE SETTINGS



Virtual Portal Settings

Cloud Drive Settings

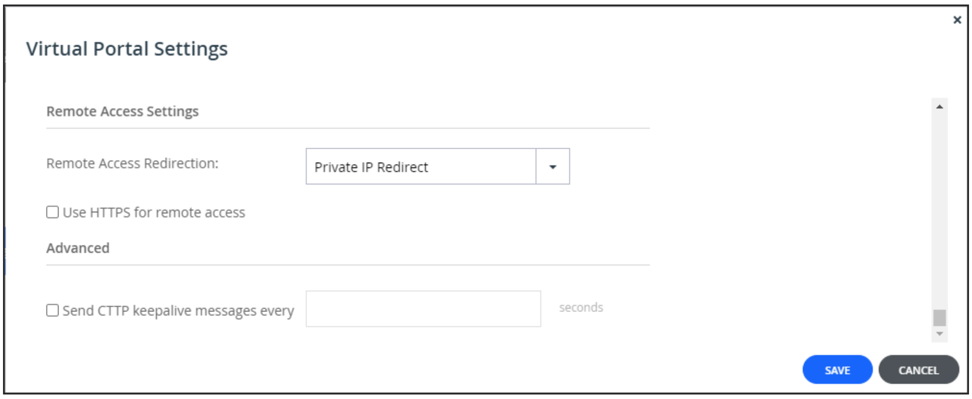
Log Admin File Access: Reads and Writes

Remote Access Settings

Log Admin File Access– The logging level for the Cloud Drive:

- **None**
- **Writes Only** – The access log only includes what files were uploaded or deleted.
- **Reads and Writes** – The access log includes what files were uploaded, deleted, copied and moved.

REMOTE ACCESS SETTINGS



Virtual Portal Settings

Remote Access Settings

Remote Access Redirection: Private IP Redirect

☐ Use HTTPS for remote access

Advanced

☐ Send CTTP keepalive messages every ____ seconds

Remote access must be configured **On** in the IBM COS FA Gateway in **Cloud Services > Remote Access**, in the **CONFIGURATION** tab. If it is configured **Off**, when trying to access the IBM COS FA Gateway from the IBM COS FA Portal, the following message is displayed:

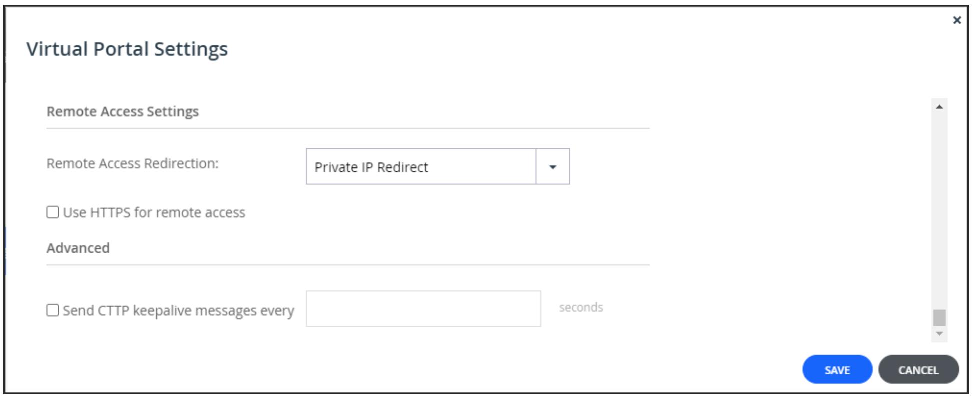
```
Remote Access is disabled Remote Access is disabled
Remote access is currently not available for this device.
```

Remote Access Redirection – Whether Web clients attempting to remotely access a IBM COS FA Gateway are redirected to communicate directly with the IBM COS FA Gateway, instead of relaying communications through the IBM COS FA Portal:

- **Public IP Redirect** – Redirect Web clients to the device's public NAT IP. The inbound port 80 or 443 towards the endpoint device must be open.
- **Private IP Redirect** – Redirect Web clients to the device's private IP address. The same network is used by both device and end user, who can reach the IP address. If the device is in the same network/network subnet, the redirection works.
- **No Redirect** – Do not redirect communications between Web clients and the device. Relay all communications through the IBM COS FA Portal. No special ports are required. The IBM COS FA Portal acts as a mediator and the HTTP is tunneled to the device through the open 995 connection to the IBM COS FA Portal.

Use HTTPS for remote access – Use HTTPS for remotely accessing devices, using the remote access service. For example, if a device is named *dev1* and the IBM COS FA Portal is named *portal.mycompany.com*, then enabling this option will cause the client's browser to be automatically redirected from the HTTP URL http://dev1.portal.mycompany.com to the HTTPS-secured URL https://portal.mycompany.com/devices/dev1.

ADVANCED



Virtual Portal Settings

Remote Access Settings

Remote Access Redirection: Private IP Redirect

□ Use HTTPS for remote access

Advanced

□ Send CTTP keepalive messages every seconds

Send CTTP keepalive messages every – Prevent proxy or load balancer servers from preemptively terminating connection between a device and the IBM COS FA Portal. In the field provided, specify an interval, in seconds, smaller than the timeout value configured on the proxy or load balancer server.

CHAPTER 4. MANAGING IBM COS FA PORTAL SNAPSHOTS

The IBM COS FA Portal retains previous file versions for each user, by using snapshots. *Snapshots* are read-only copies of files as they were at a particular point-in-time.

The IBM COS FA Portal creates snapshots automatically and retains them according to a configurable *snapshot retention policy*. So long as a snapshot is retained by IBM COS FA Portal, the relevant version of the user data can be retrieved.

In this chapter

- The Snapshot Retention Policy Options
- Configuring a Snapshot Retention Policy
- Applying a Snapshot Retention Policy
- Snapshot Retention for the Cloud Drive Service
- Snapshot Consolidation

THE SNAPSHOT RETENTION POLICY OPTIONS

A retention policy specifies the following:

- **The number of hours to retain all snapshots**
  Every snapshot is retained for this amount of time. After this time has passed for any given snapshot, the snapshot may be retained or deleted depending on the other settings.
- **The number of hourly snapshots to retain**
  For example, if hourly snapshots are set to 10, then the last 10 hourly snapshots are retained. If daily snapshots are set to 0, then the hourly snapshot are deleted when the next hour starts.
- **The number of daily snapshots to retain**
  For example, if daily snapshots are set to 10, then the last 10 daily snapshots are retained. If daily snapshots are set to 0, then the daily snapshot are deleted when the next day starts.

  Note: A day is defined as starting at 00:00:00 and ending at 23:59:59.
- **The number of weekly snapshots to retain**
  A weekly snapshot is the latest snapshot taken during the week.

  Note: A week is defined as starting on Monday and ending on Sunday.
  Example 1: Snapshots were successfully taken every day until the current day, which is Sunday. The weekly snapshot is the one taken on Sunday, as it is the latest snapshot taken this week.
  Example 2: Snapshots were successfully taken every day until the current day, except the Saturday and Sunday snapshots, which were not taken because the device was turned off. The weekly snapshot is the one taken on Friday, as it is the latest snapshot taken this week.
- **The number of monthly snapshots to retain**
  A monthly snapshot is the latest snapshot taken during the month.
  Example 1: Snapshots were successfully taken every day until the current date, which is April 30th. The monthly snapshot is the one taken on the 30th, as it is the latest snapshot taken this month.
  Example 2: Snapshots were successfully taken every day until the current date, except snapshots for the 25th through the 30th, which were not taken because the device was turned off. The monthly snapshot is the one taken on the 24th, as it is the latest snapshot taken this month.
- **The number of quarterly snapshots to retain**
  A quarterly snapshot is the latest snapshot taken during the quarter.
  Example 1: Snapshots were successfully taken every day until the current date, which is the March 31. The quarterly snapshot is the one taken on March 31st, as it is the latest snapshot taken this

quarter.
Example 2: Snapshots were successfully taken every day until the current date, except snapshots for March 25 through 31 were not taken because the device was turned off. The quarterly snapshot is the one taken on March 24th, as it is the latest snapshot taken this quarter.

- **The number of yearly snapshots to retain**
  A yearly snapshot is the latest snapshot taken during the year.
  Example 1: Snapshots were successfully taken every day until the current date, which is the December 31st. The yearly snapshot is the one taken on the 31st, as it is the latest snapshot taken this year.
  Example 2: Snapshots were successfully taken every day until the current date, except snapshots for the 25nd through the 31st were not taken because the device was turned off. The yearly snapshot is the one taken on the 24th, as it is the latest snapshot taken this year.
- **The numbers of days to keep deleted files**
  The retention period for deleted files.
  When portal users delete a file or a folder, either via the Web interface or via the local synchronization folder, the deleted data is moved to a recycle bin. It is then retained in the recycle bin for a number of days, defined in the retention policy of the user's assigned subscription plan. As long as files are retained, users can recover their deleted data from their Cloud Drive using a Recycle Bin feature in the end user portal interface.
  The minimum value is 7 days.

CONFIGURING A SNAPSHOT RETENTION POLICY

The snapshot retention policy is configured as part of the subscription plan described in Provisioning and specifically in step **4** of the procedure To add or edit a subscription plan:, in the **Snapshot Retention Policy** window.

APPLYING A SNAPSHOT RETENTION POLICY

Snapshot retention policies can be applied as part of the subscription plan at the following levels:

At the portal level – The snapshot retention policy defined in the subscription plan applies to all users in the IBM COS FA Portal, as described in Provisioning.

At the user level – A subscription plan including the snapshot retention policy can be applied to individual users in the IBM COS FA Portal. See Provisioning User Accounts for details about assigning a subscription plan to an individual user account.

Applying a Snapshot Retention Policy at Both the Virtual Portal and User Levels

When a snapshot retention policy is assigned to a IBM COS FA Portal, the policy is globally enforced as a set of maximum values for all users in the IBM COS FA Portal. Individual users in that IBM COS FA Portal can be assigned user-level snapshot retention policies, so long as the values in the user-level policy do not exceed those of the portal-level policy.

For example, a IBM COS FA Portal called *example* is assigned a subscription plan, *example-plan*, which includes the following snapshot retention policy.

- Retain 7 daily snapshots
- Retain 4 weekly snapshots
- Retain 12 monthly snapshots

Users in the *example* IBM COS FA Portal cannot be assigned a snapshot retention policy that exceeds the values specified in *example-plan*. Therefore, users in this IBM COS FA Portal cannot be assigned the following snapshot retention policy:

- Retain 10 daily snapshots
- Retain 15 weekly snapshots
- Retain 17 monthly snapshots

However, they can be assigned the following snapshot retention policy:

- Retain 6 daily snapshots
- Retain 2 weekly snapshots
- Retain 9 monthly snapshots

SNAPSHOT RETENTION FOR THE CLOUD DRIVE SERVICE

Each user account using the Cloud Drive service is assigned a *home folder* in the IBM COS FA Portal, when the user account is created. This Cloud Drive home folder serves as the block destination for IBM COS FA Gateway sync operations. Snapshots of Cloud Drive folders are taken for each folder once every five minutes, if there were any changes in the folder during that five minutes.

For example, assume a file is synced to the IBM COS FA Portal at 09:10am. The IBM COS FA Portal opens a snapshot which will close after 5 minutes, at 09:15am. At 09:24am a new file is synced to the IBM COS FA Portal and a new snapshot is opened that will close at 09:29am. Between 09:15am and 09:24am no snapshot is open, since there are no changes between the user local files and the files synced to the IBM COS FA Portal. The snapshot that closed at 09:15am is registered as a previous version, with the opening time for the snapshot, 9:10am.

SNAPSHOT CONSOLIDATION

The *snapshot consolidator* is a scheduled job that runs every hour. It is responsible for deleting all the snapshots that should not be retained, according to the retention policy.

CHAPTER 5. PROVISIONING

Users in the team IBM COS FA Portal obtain services through subscription plans for an open-ended period of time without payment.

A IBM COS FA Portal is subscribed to a global plan that determines the maximum licenses and snapshot retention policies for the whole IBM COS FA Portal. A default user subscription plan is created automatically and contains the licenses specified in the global plan. All user accounts are assigned to this default plan.

You can create alternate subscription plans and assign those to individual user accounts. You can change the default plan that is assigned to users. You can also define conditions for automatically assigning plans to users based on user attributes.

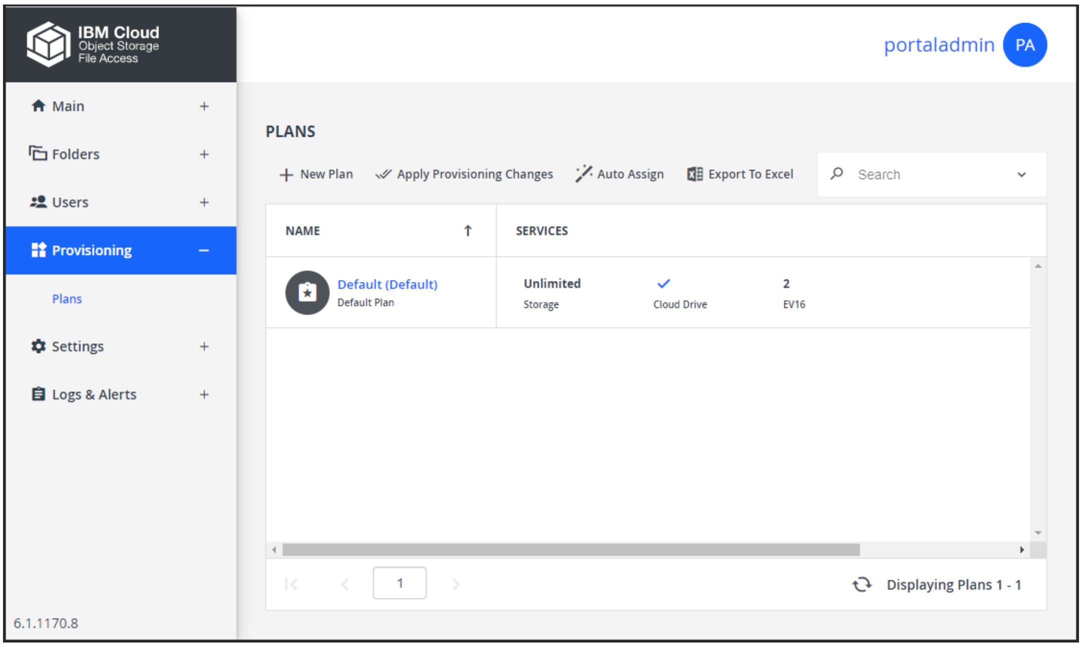
In this chapter

See Provisioning User Accounts for details about assigning a subscription plan to an individual user account.

VIEWING SUBSCRIPTION PLANS

To view all plans:

- Select **Provisioning > Plans** in the navigation pane.
  The **PLANS** page is displayed.



NAME	SERVICES		
Default (Default) Default Plan	Unlimited Storage	✓ Cloud Drive	2 EV16

The page includes the following:

NAME – The subscription plan's name. `Default Plan` is displayed under the plan name for the default plan.

SERVICES – The services provisioned in the plan.

Storage – The amount of storage allocated for the plan.

Cloud Drive – The IBM COS FA Portal can be accessed by users up to the number of licenses in the plan.

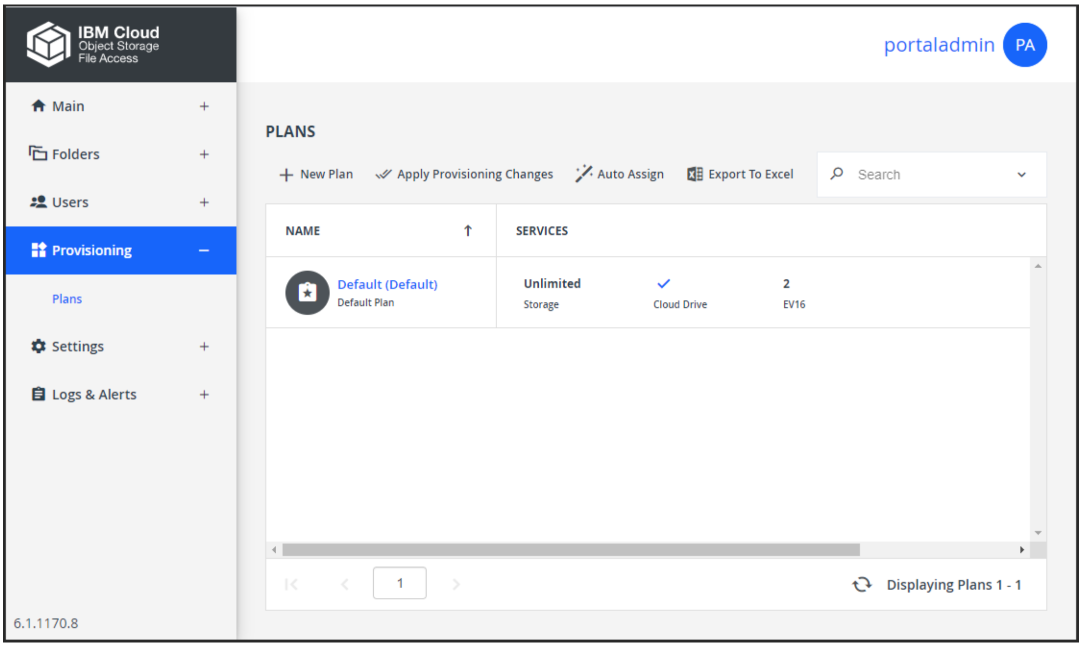
EV16 – The number of IBM COS FA Gateways included in the plan.

TRIAL – If the plan includes a free trial period, this column displays the number of days included in the free trial period.

ADDING AND EDITING SUBSCRIPTION PLANS

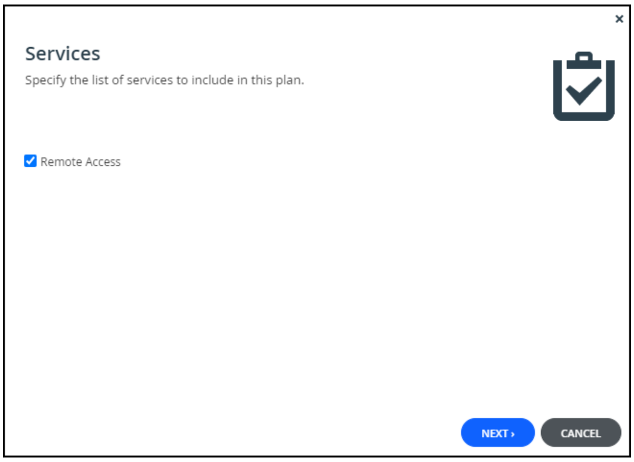
To add or edit a subscription plan:

1 Select **Provisioning > Plans** in the navigation pane.
The **PLANS** page is displayed.



NAME	SERVICES		
Default (Default) Default Plan	Unlimited Storage	✓ Cloud Drive	2 EV16

2 To add a new plan, click **New Plan**.
Or,
To edit an existing plan, click the plan's name**.**
The plan wizard opens, displaying the **Services** window.


Services

Specify the list of services to include in this plan.

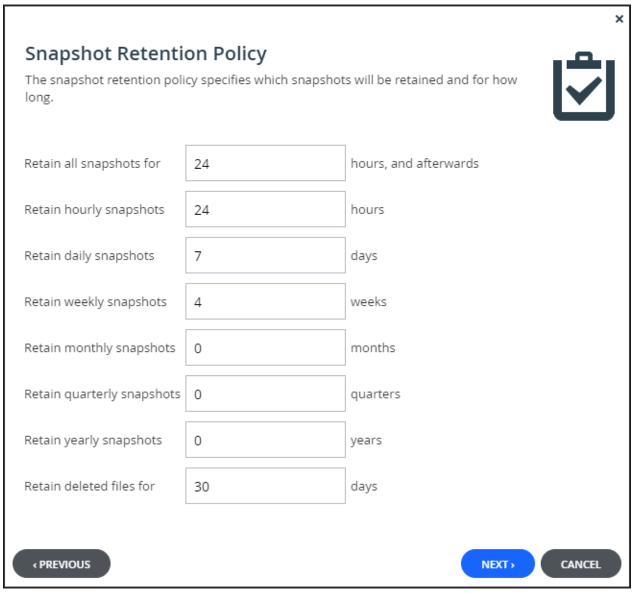
☑ Remote Access

Remote Access – Include remote access in the subscription plan. Remote access includes both access to the device's management interface via the IBM COS FA Portal and a dedicated URL, access to the user's files via the IBM COS FA Portal and a dedicated URL.

Note: Device owners can disable remote access via the device's management interface.

3 Click **NEXT**.

The **Snapshot Retention Policy** window is displayed.



Snapshot Retention Policy

The snapshot retention policy specifies which snapshots will be retained and for how long.

Retain all snapshots for 24 hours, and afterwards

Retain hourly snapshots 24 hours

Retain daily snapshots 7 days

Retain weekly snapshots 4 weeks

Retain monthly snapshots 0 months

Retain quarterly snapshots 0 quarters

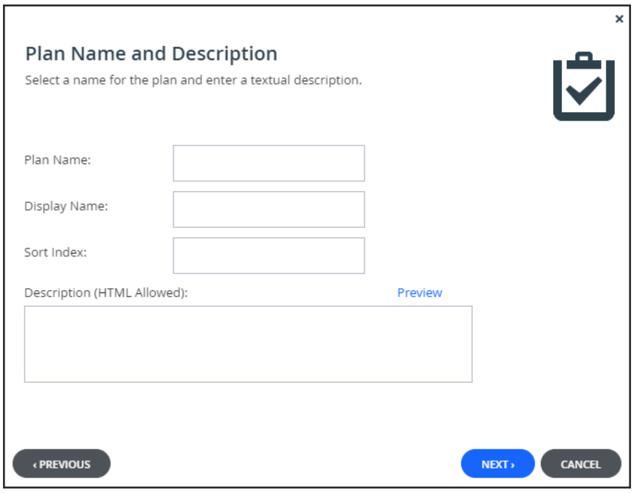
Retain yearly snapshots 0 years

Retain deleted files for 30 days

4 Set the snapshot retention policy.
Retain all snapshots for – The number of hours after creation that all snapshots are retained.
Retain hourly snapshots – The number of hourly snapshots that are retained.
Retain daily snapshots – The number of daily snapshots that are retained.
Retain weekly snapshots – The number of weekly snapshots that are retained.
Retain monthly snapshots – The number of monthly snapshots that are retained.
Retain quarterly snapshots – The number of quarterly snapshots that are retained.
Retain yearly snapshots – The number of yearly snapshots that are retained.
Retain deleted files for – The number of days to retain deleted files. The minimum is 7 days.

Note: For an explanation of each policy, see Managing IBM COS FA Portal Snapshots.

5 Click **NEXT**.
The **Plan Name and Description** window is displayed.



Plan Name and Description

Select a name for the plan and enter a textual description.

Plan Name:

Display Name:

Sort Index:

Description (HTML Allowed):

6 Specify the plan name and provide a description.
Plan Name – A name for the plan. Only letters and numbers can be used for the name.
Display Name – The name to use when displaying this plan in the end user IBM COS FA Portal and

notifications.

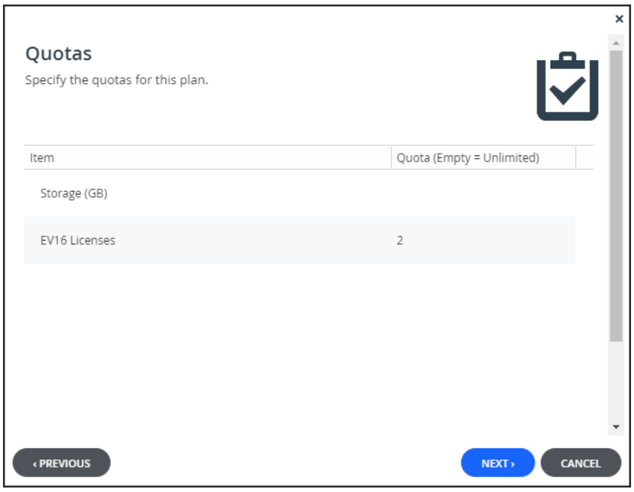
Sort Index – Optionally, an index number to assign the plan, to enable custom sorting of the plans displayed to end users in the Subscribe to Plan wizard.

Description – A description of the plan. HTML tags can be used in the description.

Click **Preview** to open a new page in the browser displaying the plan description.

7 Click **NEXT**.

The **Quotas** window is displayed.



Quotas

Specify the quotas for this plan.

Item	Quota (Empty = Unlimited)
Storage (GB)	
EV16 Licenses	2

8 For each item, click in the quota field and enter the number to include in the plan.

For example, to include 100GB of storage space, click in the Storage (GB) item's quota field and enter 100.

Note: The quotas must not exceed the number specified in the license. An error message is displayed when you attempt to assign a user to a plan with a quota that exceeds the number specified in the license.

9 Click **NEXT**.

The **Wizard Completed** screen is displayed.

10 Click **FINISH**.

If you edited an existing plan, IBM COS FA Portal applies changed plans to all users every day at midnight.

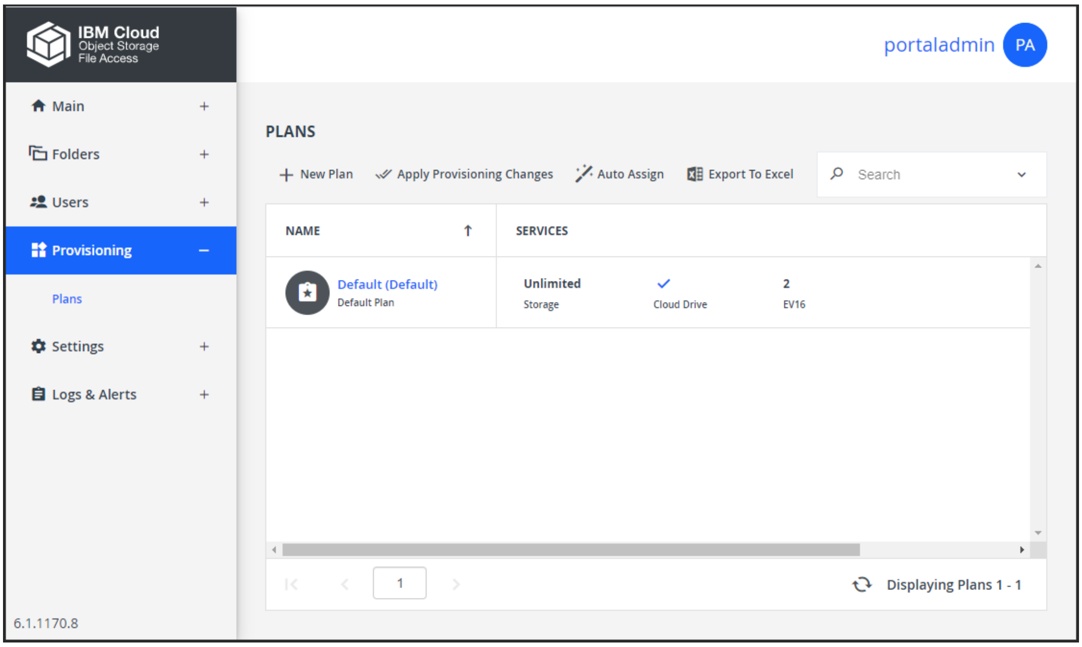
You can use apply the plan changes immediately by clicking **Apply Provisioning Changes**. The **Apply Provisioning Changes** window is displayed and the changes are applied. Either click **CONTINUE IN BACKGROUND** or wait for the update to complete and click **CLOSE**.

SETTING OR REMOVING THE DEFAULT PLAN

The default plan is automatically assigned to all new user accounts.

To set a plan as the default:

1 Select **Provisioning > Plans** in the navigation pane.
The **PLANS** page is displayed.



2 Select the desired plan's row.

3 Click **Set Default.**
The selected plan becomes the default subscription plan. `Default Plan` is displayed under the plan name.

To remove a subscription plan from being the default:

1 Select **Provisioning > Plans** in the navigation pane.
The **PLANS** page is displayed.

2 Select the default subscription plan's row.

3 Click **Remove Default.**
The subscription plan is no longer the default.

AUTOMATICALLY ASSIGNING PLANS

Automatic plan assignment allows you to define a policy that determines which subscription plans will be assigned to which users.

You can automatically assign subscription plans based on the following user attributes:

- Username
- User Groups
- Role
- First Name
- Last Name
- Company
- Billing ID
- Comment

The policy rules are processed in ascending order. The first rule that matches applies. You can change the rules' order by using the Move Down/Move Up buttons. You can also choose to apply a default plan in the event that no rule applies.

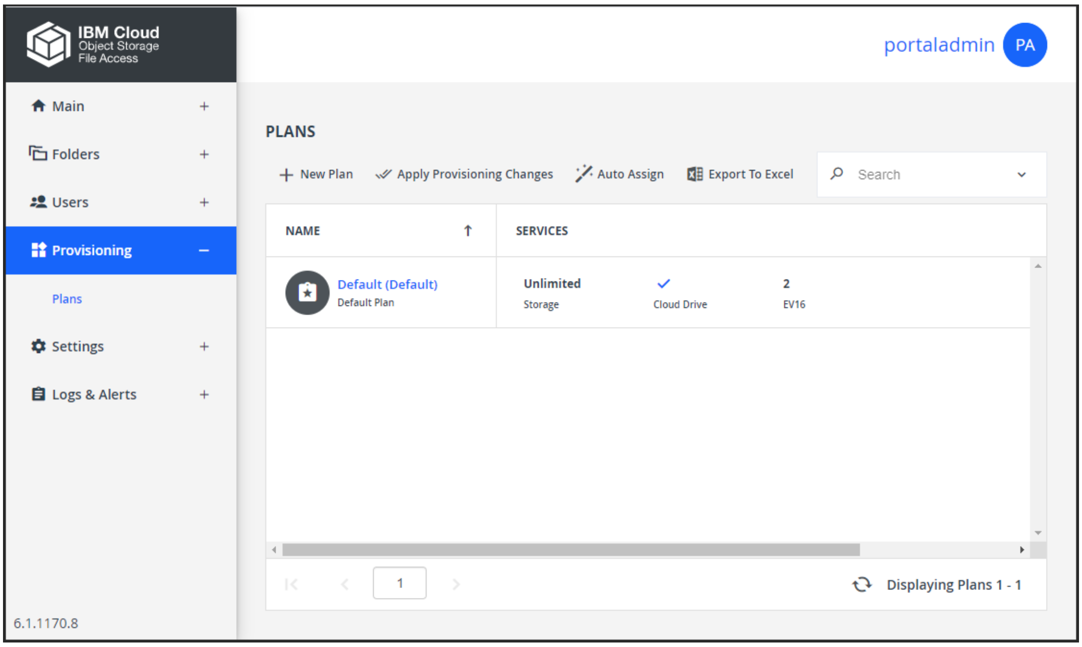
If the IBM COS FA Portal is integrated with a Directory Service, such as Active Directory you can define a policy even before users have joined the service, so that when users join, they are automatically assigned the appropriate plan to get the correct quota and licenses.

Note: In order that new users in an Active Directory group are automatically assigned to a plan, the Active Directory group must have been fetched or already in the Active Directory groups under the IBM COS FA Portal.

For details about using directory services, see Using Directory Services For the Users.

To configure automatic plan assignment:

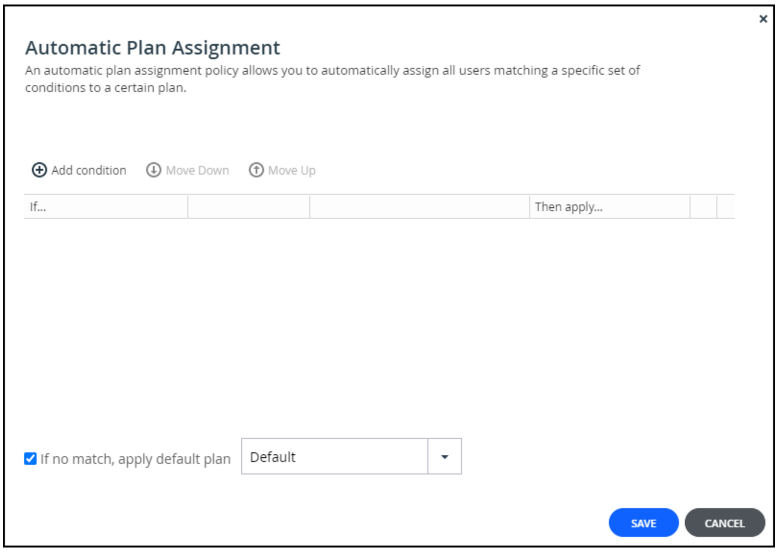
1 Select **Provisioning > Plans** in the navigation pane.
The **PLANS** page is displayed.



NAME	SERVICES		
Default (Default) Default Plan	Unlimited Storage	✓ Cloud Drive	2 EV16

2 Click **Auto Assign**.

The **Automatic Plan Assignment** window is displayed.



Automatic Plan Assignment

An automatic plan assignment policy allows you to automatically assign all users matching a specific set of conditions to a certain plan.

3 Click **Add condition** to define a condition.

  a In the **If** column select a user attribute.

  b Select an operator, such as *is one of*.

  c Enter a value to apply on the operator.
  When adding a condition for *User Groups*, the only operator is *includes one of*. You have to put the exact name of the group to apply the plan and not part of the name, even if that part is unique.

  d In the **Then apply** column select a plan to apply if a user satisfies the condition.

  e Order the conditions by selecting a condition and using the **Move Down** and **Move Up** options to move the condition to the required place in the list.
  The order of the conditions is critical to applying the correct plan. For example, if a user is a member of two different groups in the auto plan assignment, whichever condition applies to the group the user is in first in the list of conditions is the plan that user gets. Therefore, order the list of conditions with the least restrictive conditions at the top of the list.

4 To delete a condition, click 🗑 in its row.

5 Click **SAVE**.

EXPORTING PLAN DETAILS TO EXCEL

You can export a list of plans and their details to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export a list of plans to Microsoft Excel:

1 Select **Provisioning > Plans** in the navigation pane.
The **PLANS** page opens, displaying all the plans.

2 Click **Export to Excel**.

The list of plans is exported to your computer.

DELETING A PLAN

To delete a plan:

1. Select **Provisioning > Plans** in the navigation pane.
   The **PLANS** page is displayed.
2. Select the plan's row.
3. Click **Delete Plan.**
   A confirmation window is displayed.
4. Click **DELETE** to confirm.

The subscription plan is deleted.

CHAPTER 6. USING DIRECTORY SERVICES FOR THE USERS

In this chapter

- How Directory Service Synchronization Works
- Integrating IBM COS FA Portal with a Directory Service
- Manually Fetching User Data

IBM COS FA Portal can be integrated with the following directory services:

- Microsoft Active Directory – If you are integrating the IBM COS FA Portal with Active Directory, make sure the ports described in the planning part of the IBM COS FA Portal setup guide are opened.
- LDAP directory services:
  - OpenDS
  - Oracle Unified Directory
  - Oracle Directory Server Enterprise Edition
  - Sun Java System Directory Server
- Apple Open Directory

User accounts are automatically fetched and refreshed from the directory, and user authentication is performed using the directory.

IBM COS FA Portal administrators can define an access control list specifying which directory service groups and individual users are permitted to access the IBM COS FA Portal, and which user roles they are assigned in the IBM COS FA Portal.

Note: Users must have an email address, as well as a first and last name, defined in the directory service. Users without one of these attributes cannot log in to the IBM COS FA Portal and will cause synchronization to fail.
Nested groups are not supported by default since supporting nested groups has a performance impact. If you need support for nested groups, contact IBM COS FA Portal support.

After users are fetched, they can be viewed in the IBM COS FA Portal. For details, see Managing Administrator Users.

HOW DIRECTORY SERVICE SYNCHRONIZATION WORKS

When integrated with a directory service, the IBM COS FA Portal fetches user data from the directory upon the following events:

- An administrator can manually fetch specific users from the directory. See Manually Fetching User Data.
- If a user attempts to sign in, but does not yet have a local IBM COS FA Portal account, their user account is automatically fetched from the directory.
- The directory services settings are configured to automatically create a local IBM COS FA Portal account, without the user having to sign in to the IBM COS FA Portal.
- The IBM COS FA Portal automatically re-fetches all previously fetched directory users, every day at midnight, as part of the daily *Apply provisioning changes* task.
- An administrator can force a re-synchronization of all previously fetched directory users, by running the **Apply Provisioning Changes Wizard**. See Applying Provisioning Changes.

IBM COS FA Portal handles special cases as follows:

- If during the fetch it is determined that a user exists in the local user database but not in the directory, then the user is assumed to have been deleted, and IBM COS FA Portal deletes the user from the local user database. The user's folders are not deleted.
- If the access control list specifies that the user is no longer allowed to access IBM COS FA Portal, then IBM COS FA Portal changes the user account's role to "Disabled". The user account is not deleted.

Note: Each virtual IBM COS FA Portal can optionally be integrated with a different Active Directory or LDAP directory.

INTEGRATING IBM COS FA PORTAL WITH A DIRECTORY SERVICE

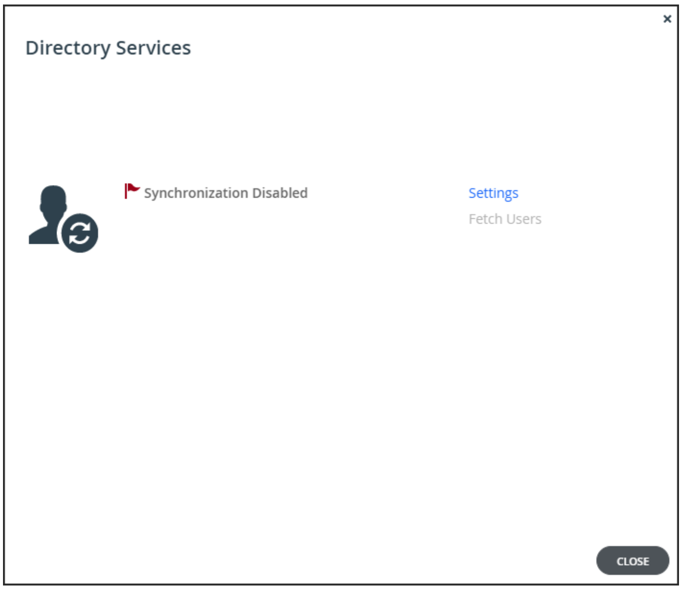
Before integrating the IBM COS FA Portal to an active directory, to set up integration with SSL:

- LDAPS (TCP port 636) and Global Catalog SSL (TCP port 3269) ports must be opened.
- Domain controllers must have a domain controller certificate with the EKU (Enhanced Key Usage) Client Authentication/ ServerAuthentication.
  - a On the domain controller, open the Certificates MMC and export the domain controller certificate into **`.cer`** format.
  - b Import the certificate on each IBM COS FA Portal application server:
    - i Log in to each IBM COS FA Portal application server using SSH.
    - ii Run the command: `portal-cert.sh import -f` *`certificate`*`.cer` *`Alias Name`*
  - c After importing the certificate to each IBM COS FA Portal application server, run the command to start the IBM COS FA Portal: `portal-manage.sh restart`
  - d Follow the instructions in Active Directory, checking **Use SSL**.
  - e Remove access to ports TCP 389 and TCP 3268.

To integrate a virtual IBM COS FA Portal with a directory service:

1 Select **Settings** in the navigation pane.

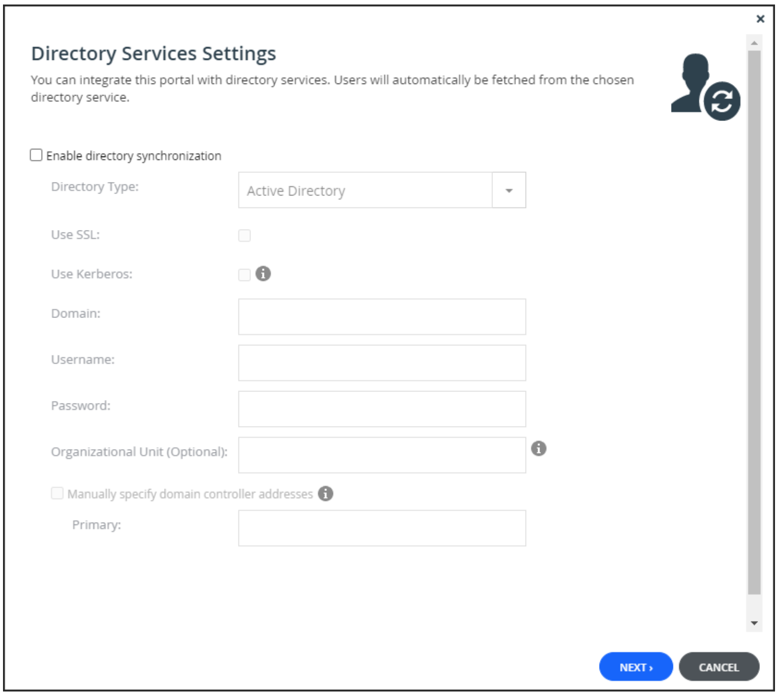
2 Select **Directory Services** under **USERS** in the **Control Panel** page.
The **Directory Services** window is displayed.



Directory Services

Synchronization Disabled

3 Click **Settings** to set directory settings, including enabling connecting to a directory service. If you have already connected to a directory service, you can fetch all the users from the domain by clicking **Fetch Users**, as described in Manually Fetching User Data.
After clicking **Settings**, the Directory Services Settings window is displayed.



Directory Services Settings

You can integrate this portal with directory services. Users will automatically be fetched from the chosen directory service.

□ Enable directory synchronization

Directory Type: Active Directory

Use SSL: □

Use Kerberos: □

Domain:

Username:

Password:

Organizational Unit (Optional):

□ Manually specify domain controller addresses

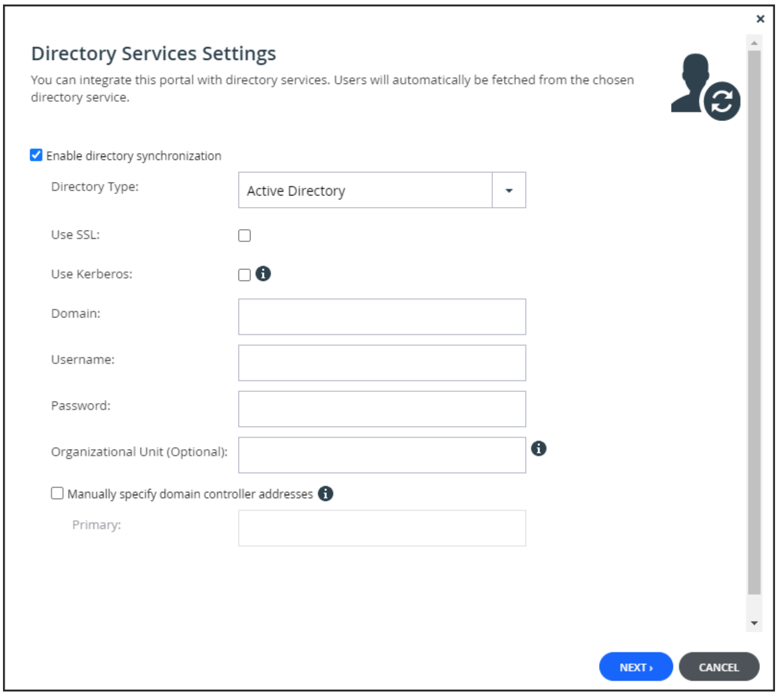
Primary:

Enable Directory Synchronization – Enable integration with a directory domain.
Directory Type – The type of directory with which to integrate IBM COS FA Portal:

- Active Directory
- LDAP
- Apple Open Directory

After selecting the directory type the fields are enabled and match the type selected:

Active Directory



Directory Services Settings

You can integrate this portal with directory services. Users will automatically be fetched from the chosen directory service.

☑ Enable directory synchronization

Directory Type: Active Directory

Use SSL: □

Use Kerberos: □

Domain:

Username:

Password:

Organizational Unit (Optional):

□ Manually specify domain controller addresses

Primary:

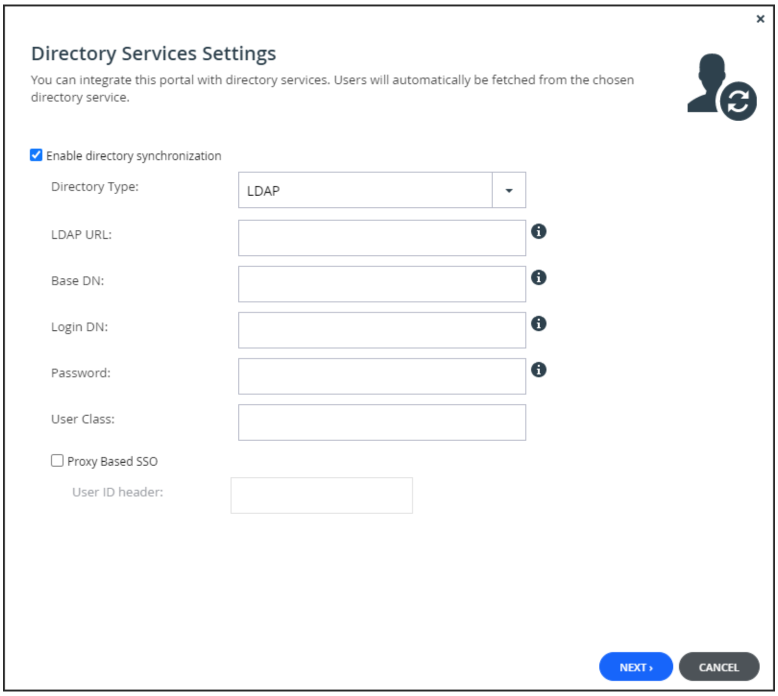
Use SSL – Connect to the Active Directory domain using SSL.
Use Kerberos – Use the Kerberos protocol for authentication when communicating with the Active Directory domain.

Note: Only one virtual IBM COS FA Portal, per system, can use Kerberos.

Domain – The name of Active Directory domain with which you want to synchronize users.
Username – The name to use for authenticating to Active Directory.
Password – The password for authenticating to Active Directory.
Organizational Unit (optional) – The name of the organizational unit within the Active Directory domain.
Manually specify domain controller addresses – The IP address of the Active Directory domain controllers. If unchecked, DNS is used to automatically find the domain controllers.

Primary – The address of the primary domain controller.
Secondary – The address of the secondary domain controller.

LDAP Directory Server



Directory Services Settings

You can integrate this portal with directory services. Users will automatically be fetched from the chosen directory service.

☑ Enable directory synchronization

Directory Type: LDAP

LDAP URL:

Base DN:

Login DN:

Password:

User Class:

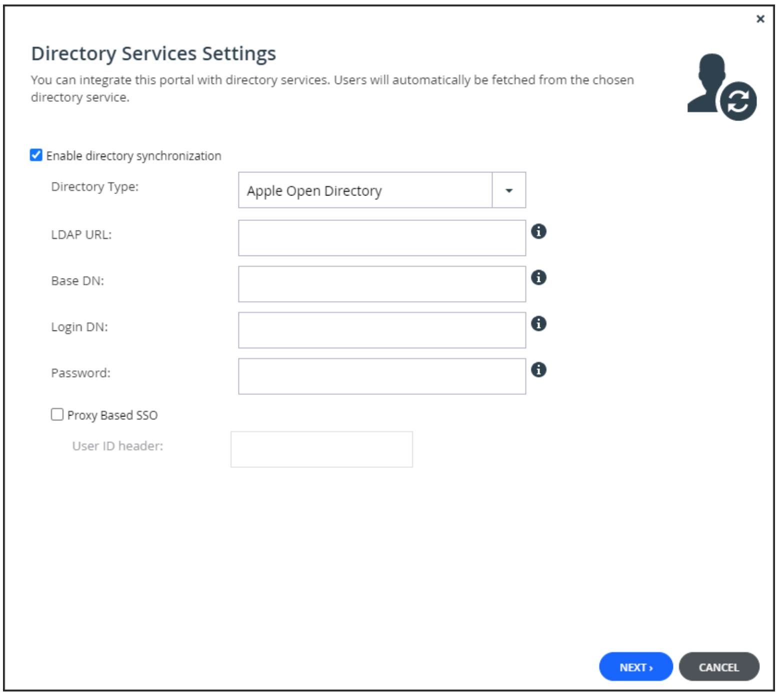
□ Proxy Based SSO

User ID header:

LDAP URL – The URL to connect to the LDAP server. Both ldap and ldaps are supported. The default port is 389 for *ldap* and 636 for *ldaps*.
Base DN – Optional: The base DN of the LDAP server.
Login DN – The bind DN: The distinguished name of a user with full user read rights, used for binding to the directory. For example, `cn=Manager,dc=company,dc=com`
Password – The password to use for binding to the LDAP server.
User Class – The LDAP object class for user objects in the LDAP directory.
Proxy Based SSO – To configure an access manager that supports proxy-based SSO, also known as reverse proxy-based SSO:

User ID Header – The attribute that your access manager adds to each incoming HTTP request.

Apple Open Directory Server



Directory Services Settings

You can integrate this portal with directory services. Users will automatically be fetched from the chosen directory service.

☑ Enable directory synchronization

Directory Type: Apple Open Directory

LDAP URL:

Base DN:

Login DN:

Password:

□ Proxy Based SSO

User ID header:

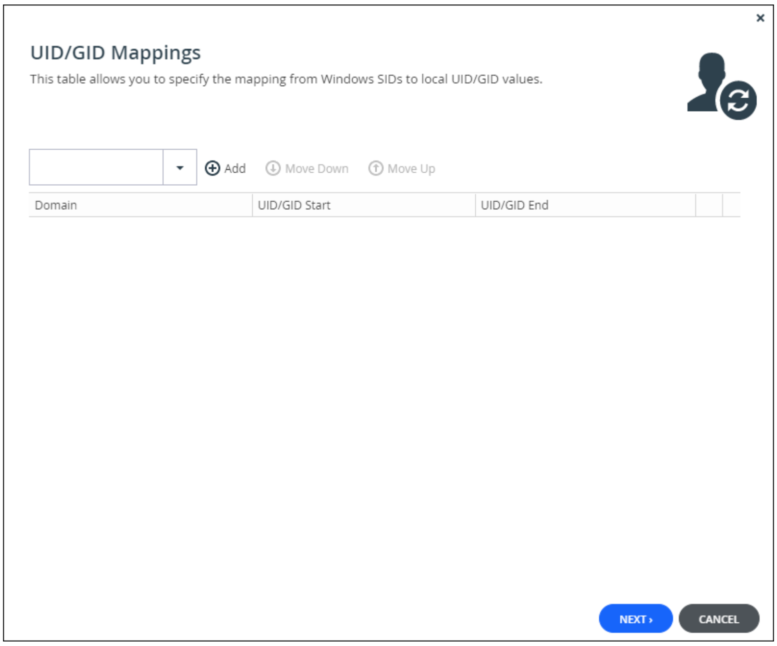
LDAP URL – The URL to connect to the Apple Open Directory server.
Base DN – Optional: The base DN of the Apple Open Directory server.
Login DN – The distinguished name of a user with full user read rights, used for binding, authenticating, to the LDAP server, also known as bind DN.
Password – The password to use for binding to the Apple Open Directory server.
Proxy Based SSO – To configure an access manager that supports proxy-based SSO, also known as reverse proxy-based SSO:

User ID Header – The attribute that your access manager adds to each incoming HTTP request.

4 Click **NEXT**.

Active Directory

The IBM COS FA Portal connects to the domain and the **UID/GID Mappings** window is displayed.



UID/GID Mappings

This table allows you to specify the mapping from Windows SIDs to local UID/GID values.

a To add the other Active Directory domains in the tree/forest, do the following for each one:

b Select the user to add to the group and click **Add**.

  i In the **Add domain** field, enter the Active Directory domain name, or select it from the drop-down list.

  ii Click **Add**.
  The domain is added.

  iii In the **UID/GID Start** field enter the starting number in the range of IBM COS FA Portal user and group IDs (UID/GID) to assign to users and user groups from this Active Directory domain.

  iv In the **UID/GID End** field enter the ending number in the range of IBM COS FA Portal user and group IDs (UID/GID) to assign to users and user groups from this Active Directory domain.

c You can re-order the list of added domains by selecting a domain and clicking **Move Up** or **Move Down**.
The order in which domains are displayed represents the order in which the domains are displayed in lists throughout the IBM COS FA Portal interface.

d To remove a Active Directory domain, select the domain row and click 🗑.
The domain is removed.

e Click **NEXT**.

The **Access Control** window is displayed.

LDAP

The IBM COS FA Portal connects to the LDAP server and the **Advanced LDAP Mappings** window is displayed. To configure the IBM COS FA Portal to match a custom LDAP schema:

a Edit the LDAP mappings: Click each attribute that maps to the corresponding user properties.
The following user properties must be mapped to LDAP attributes:
username – The user name in the IBM COS FA Portal to uniquely identify the user. This can map to any LDAP attribute that uniquely identifies the user, such as **userPrincipalName**.

password – The user password. The corresponding LDAP attribute is **userPassword**.
email – The user email. The corresponding LDAP attribute is **mail**.
firstName – The user first name. The corresponding LDAP attribute is **givenName**.
lastName – The user family name. The corresponding LDAP attribute is **sn**.
memberOf – The group the user is a member of. The corresponding LDAP attribute is **memberOf**.

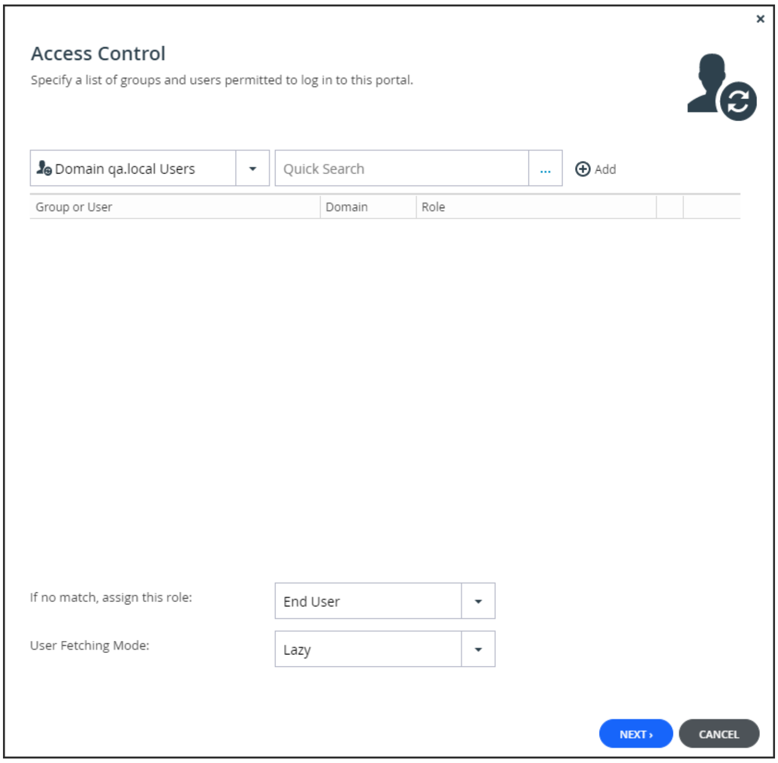
b Click **NEXT**.

Apple Open Directory

The IBM COS FA Portal connects to the Apple Open Directory server.

Active Directory, LDAP and Apple Open Directory

The **Access Control** window is displayed.



Access Control

Specify a list of groups and users permitted to log in to this portal.

If no match, assign this role: End User

User Fetching Mode: Lazy

5 Add each directory user and user group allowed to access the IBM COS FA Portal:

a In the drop-down list, select one of the following:
Domain Users – Search the users defined in directory service.
Domain Groups – Search the user groups defined in directory service.

b Select the user or user group from the dropdown list or in the **Quick Search** field, enter a string that is displayed anywhere within the name of the user or user group you want to add.

c Select the user or group and click **Add**.
The user or user group is added to the list of users and user groups with access to the IBM COS FA Portal.

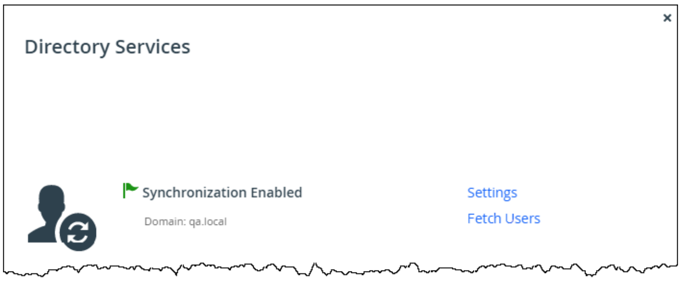
6 To remove a user or group, select the row and click 🗑.
The user or user group is removed.

7 In each user and user group's row, click in the **Role** column, then select the user role from the drop-down list.

Disabled – The user account is disabled. The user cannot access the IBM COS FA Portal.

  - **End User** – The user can access the IBM COS FA Portal.
  - **Read/Write Administrator** – The user can access the IBM COS FA Portal as an administrator with read-write permissions.
  - **Read Only Administrator** – The user can access the IBM COS FA Portal as an administrator with read-only permissions.
  - **Support** – The user can access the IBM COS FA Portal as an administrator and has read/write access to devices, user accounts, folders, and folder groups, and read-only access to all other settings in the IBM COS FA Portal.

8. To assign a role for a directory user or user group with no match in the access control list, select the user role from the **If no match, assign this role** drop-down list: **Disabled**, **End User**, **Read/Write Administrator**, **Read Only Administrator**, **Support**.
9. To automatically fetch new users and create home folders for them, without the need to perform a manual fetch for them or to require them to sign in to the IBM COS FA Portal, select the **Eager** fetch mode from the **User Fetch Mode** drop-down list.
   - **Lazy** – Users are created and data associated with them after either the user signs in to the IBM COS FA Portal or a manual fetch is performed for the users.
   - **Eager** – Users in groups in the access control list are immediately created and home folders created for them.
10. Click **NEXT**.
    The **Wizard Completed** window is displayed.
11. Click **FINISH**. The **Apply Changes** window is displayed.
    While the changes are being applied you can either stop the process, by clicking **STOP** or close the window while the process continues to run in the background by clicking **CONTINUE IN BACKGROUND**.
12. Click **CLOSE**.
    Synchronization with the directory server is enabled.
    You can now fetch the users from the directory to use in the IBM COS FA Portal.



Directory Services

Synchronization Enabled

Domain: qa.local

13. Click **CLOSE**.

The users in the IBM COS FA Portal are automatically updated at midnight of every night with the users in the directory. To immediately fetch the users, see Manually Fetching User Data.

MANUALLY FETCHING USER DATA

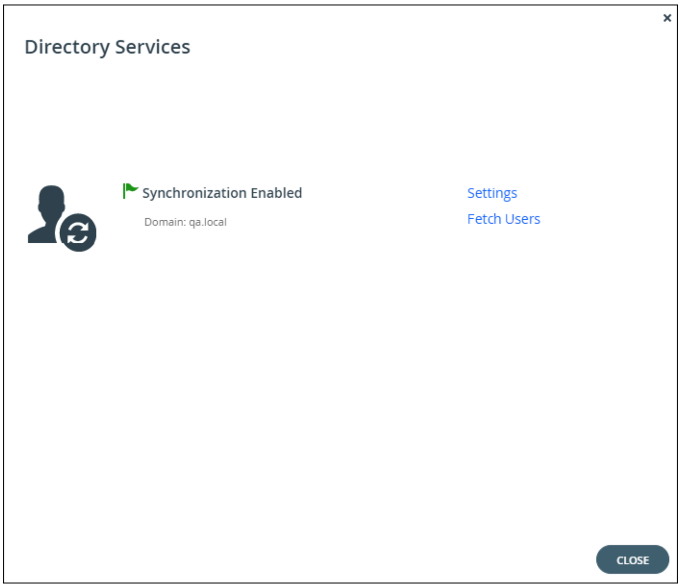
You can manually fetch user data from an integrated directory, after the connection with the directory service is established, as described in Integrating IBM COS FA Portal with a Directory Service:

- To immediately update data in the local user database, instead of waiting for IBM COS FA Portal to automatically fetch data at midnight.
- To create an account for a user that does not yet exist in the local user database, before their first login.

To manually fetch user data:

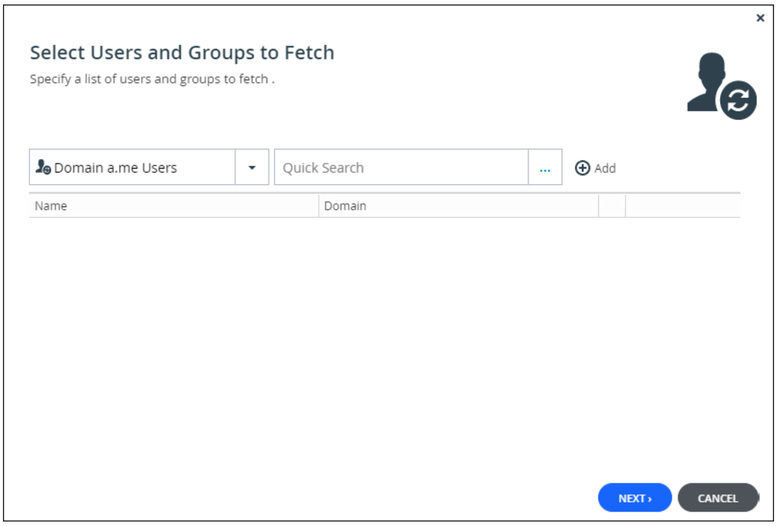
1 Select **Settings** in the navigation pane.

2 Select **Directory Services** under **USERS** in the **Control Panel** page.
The **Directory Services** window is displayed.



Directory Services

3 Click **Fetch Users**.
The **Select Users and Groups to Fetch** window is displayed.



Select Users and Groups to Fetch

Specify a list of users and groups to fetch .

4 Add each directory user and user group allowed to access the IBM COS FA Portal:

a In the drop-down list, select one of the following:
Domain Users – Search the users defined in directory service.
Domain Groups – Search the user groups defined in directory service.

b Select the user or user group from the dropdown list or in the **Quick Search** field, enter a string that is displayed anywhere within the name of the user or user group you want to add.

c Select the user or group and click **Add**.
The user or user group is added to the list of users and user groups to fetch.

5. To remove a user or group, select the row and click 🗑.
   The user or user group is removed from the list.
6. Click **FINISH**. The User data is fetched from the directory, and the **Apply Changes** window is displayed and the changes are applied.
   While the changes are being applied you can either stop the process, by clicking **STOP** or close the window while the process continues to run in the background by clicking **CONTINUE IN BACKGROUND**.
7. Click **CLOSE**.

CHAPTER 7. MANAGING ADMINISTRATOR USERS

Administrators are registered with the IBM COS FA Portal and have access to the IBM COS FA Portal. Each administrator is represented in the IBM COS FA Portal by a *user account*.

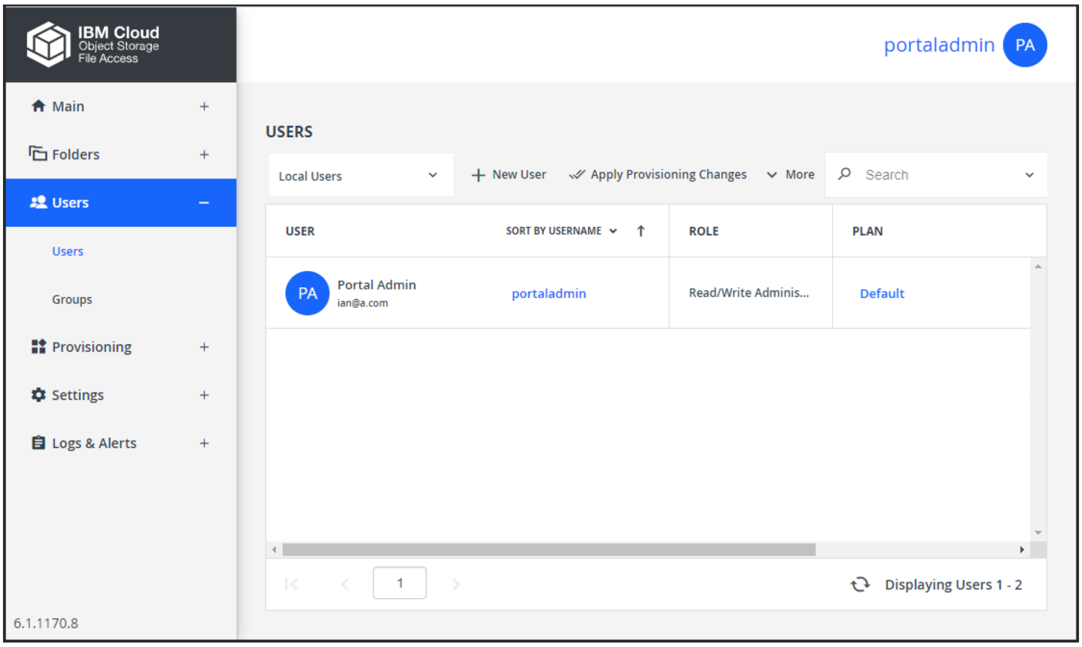
Administrators and groups of administrators should be added directly in the IBM COS FA Portal or by using directory services, such as Active Directory. You can attach a directory service and fetch users and groups from the directory service. For information about using a directory service, see Using Directory Services For the Users.

In this chapter

VIEWING USERS

To view all users in the IBM COS FA Portal:

- Select **Users > Users** in the navigation pane.
  The **USERS** page opens, displaying the users for the IBM COS FA Portal.



USER – The user’s first and last names.

Email (under the user name) – The administrator's email address.

Username – The username.

Company (under the user name) – The name of the user's company.

Disabled – Displayed if the user is defined as disabled and cannot access the IBM COS FA Portal.

ROLE – The user role: Disabled, Read/Write Administrator, Read Only Administrator, Support.

PLAN – The plan assigned to the user. You can access the plan details directly by clicking the plan. For details, see Provisioning.

RESOURCES – The resources allocated to the user. The information can be different per user. Expanding the column or clicking **more >** displays more information:

- The number and type of IBM COS FA Gateway licenses used.
- The amount of storage the user has consumed out of the total number provisioned.
- Whether or not the user has the Cloud Drive service.

To view only a specific type of user:

1. In the navigation pane, click **Users > Users**.
   The **USERS** page opens, displaying the users for the IBM COS FA Portal.
2. Click the filter drop-down to filter the users either by the default **Local Users** or by a domain.

ADDING USERS

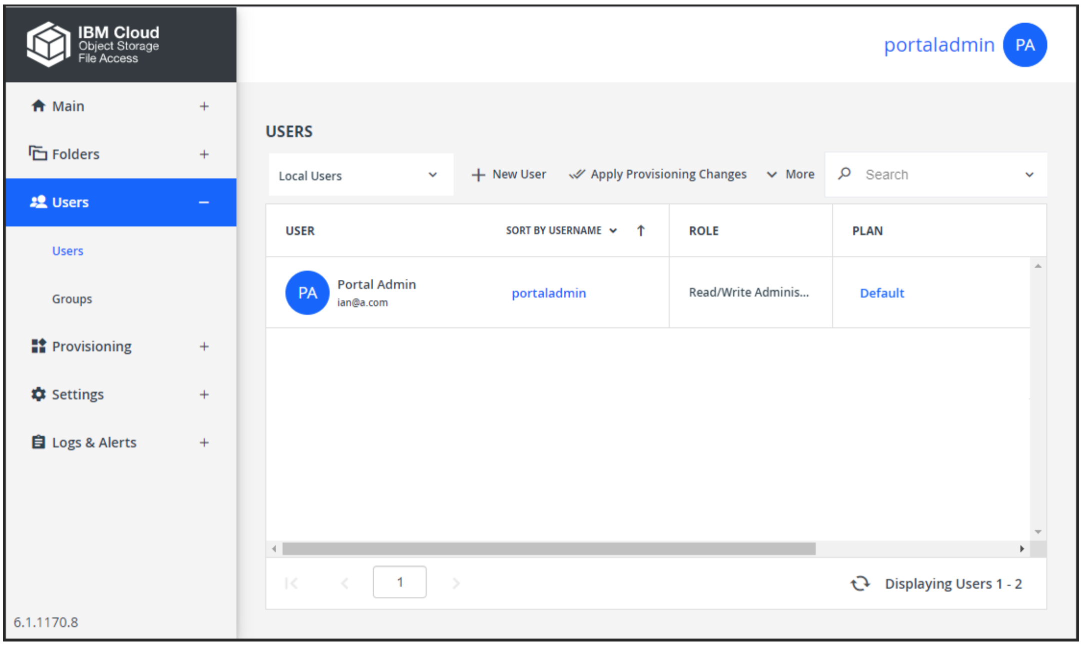
You can add users to the IBM COS FA Portal in the following ways:

- Adding Users In the IBM COS FA Portal Interface
- Importing Users from a File
- Using directory services, such as Active Directory. For information about using a directory service, see Using Directory Services For the Users

Adding Users In the IBM COS FA Portal Interface

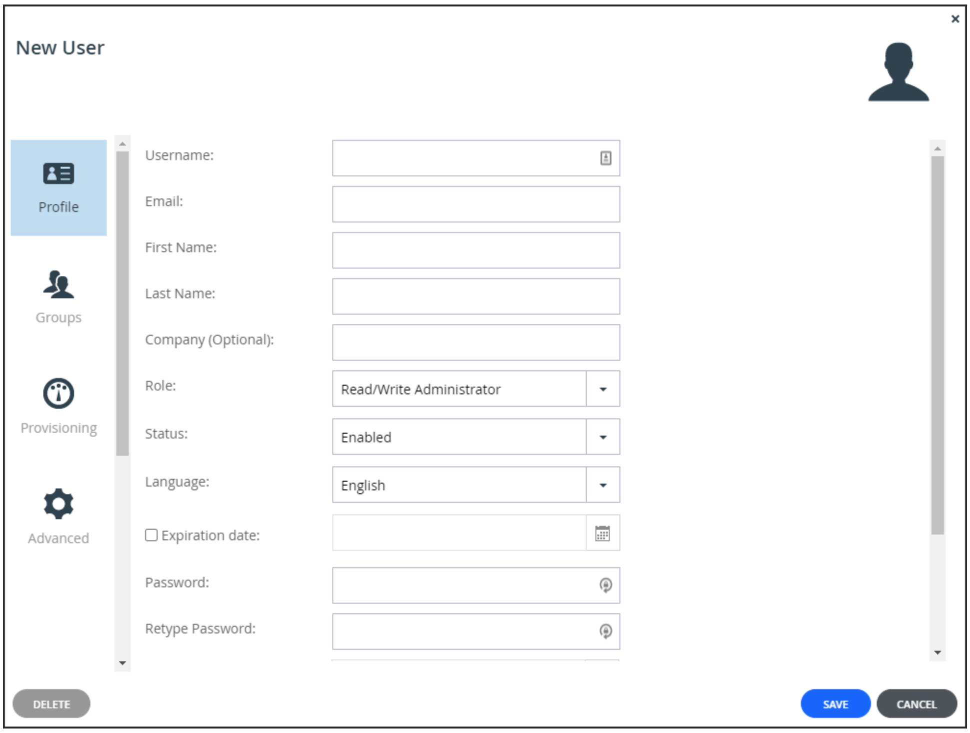
To add a user or edit an existing user in the IBM COS FA Portal:

1 Select **Users > Users** in the navigation pane.
The **USERS** page opens, displaying the users for the IBM COS FA Portal.



USER		ROLE	PLAN
PA Portal Admin ian@a.com	portaladmin	Read/Write Adminis...	Default

2 Click **New User**.
The **New User** window is displayed.



New User

Username:

Email:

First Name:

Last Name:

Company (Optional):

Role: Read/Write Administrator

Status: Enabled

Language: English

☐ Expiration date:

Password:

Retype Password:

3 Complete the fields in the **Profile** option:

Username – A name for the user's IBM COS FA Portal account.
Email – The user's email address.
First Name – The user's first name.
Last Name – The user's last name.
Company (Optional) – The name of the user's company.
Role – The user's role:

> **Disabled** – The user account is disabled. The user cannot access the IBM COS FA Portal.
> **Read/Write Administrator** – The user can access the IBM COS FA Portal as an administrator with read-write permissions.
> **Read Only Administrator** – The user can access the IBM COS FA Portal as an administrator with read-only permissions.
> **Support** – The user can access the IBM COS FA Portalas an administrator and has read/write access to devices, user accounts, folders, and folder groups, and read-only access to all other settings in the IBM COS FA Portal.

Status. Select the account status:

> **Enabled** – The account is enabled, and the user can access the IBM COS FA Portal.
> **Disabled** – The account is disabled, and the user cannot access the IBM COS FA Portal.
> The default value for new users is *Enabled*.
> The default value for invited users is *Disabled*. The status changes to *Enabled* when the invited user activates the account.
> **Note:** In order to access the EIBM COS FA Portal, the user must have a role other than Disabled, and the status must be enabled.

Language – The language used for the user interface.
Expiration date – The expiration date of the user account.
Password / Retype Password – A password for the user's account. Password requirements depend on the password policy, which can be overridden and modified in the **Virtual Portal Settings**.
Force Password Change – An expiration date for the user account password. When the password has expired, the user must configure a new password on the next login.

Numeric UID (Optional) – A numeric user ID to assign the user's account.
Comment – A description of the user account.

4 Click **SAVE**.

After a user is added, the options available to the administrator, such as the user devices and cloud drive folders. Some of these options, such as devices and folder groups are shortcuts to the relevant setting.

The user receives an email and can access the IBM COS FA Portal using the username and password from the administrator. By default, the email does not include the user password, for added security, and the user must contact the IBM COS FA Portal administrator for the password. Inviting users from the **USERS** page, with the **More > Invite** option, enables the user to choose a password on initial logon without needing to contact the administrator.

Importing Users from a File

You can import users and their details from a comma separated values (*.csv) file.

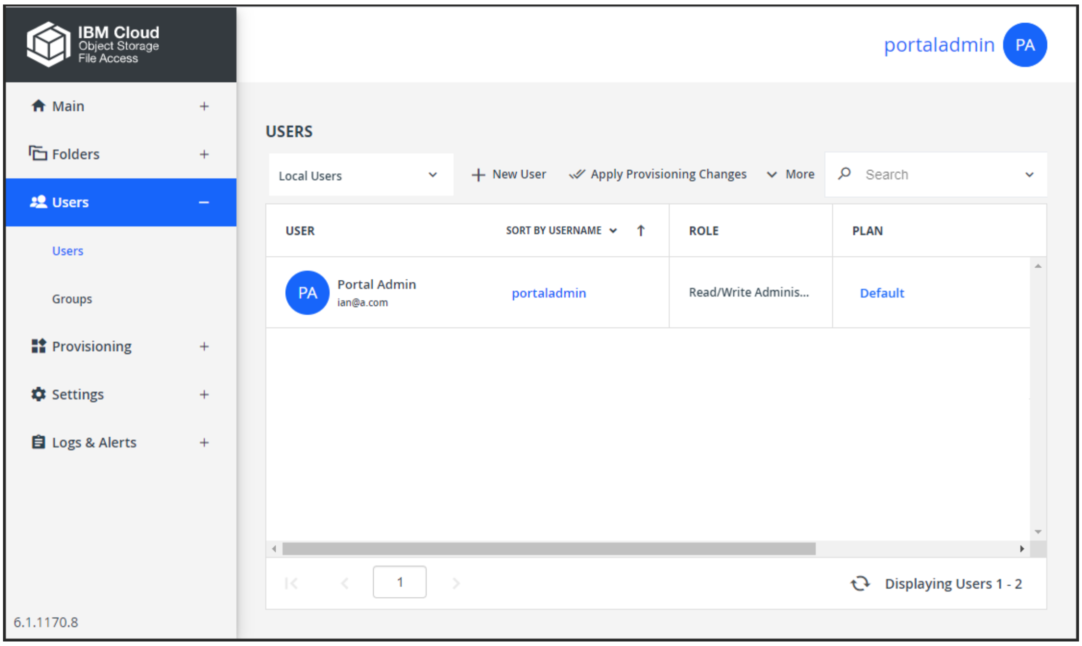
The *.csv file's columns must be in the following order:

1 Username
2 First name
3 Last name
4 Email address
5 Company (Optional)
6 Password
7 Role
8 Plan (Optional)
9 Numeric UID (Optional)
10 External Account ID (Optional)
11 Comment (Optional)
12 Status (Optional)

Optional fields can be left blank.

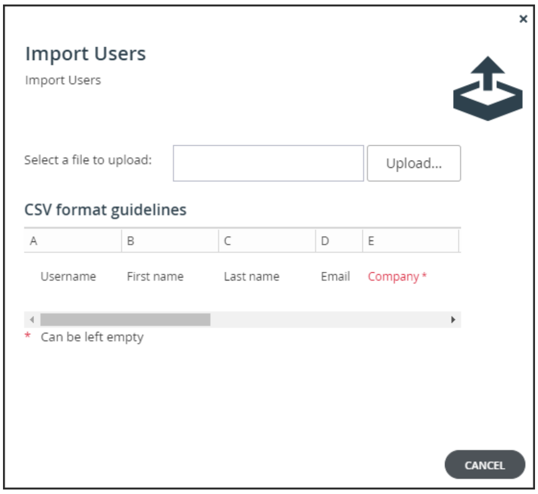
To import users from a *.csv file:

1 Select **Users > Users** in the navigation pane.
The **USERS** page opens, displaying the users for the IBM COS FA Portal.



USER	SORT BY USERNAME	ROLE	PLAN
PA Portal Admin ian@a.com	portaladmin	Read/Write Adminis...	Default

2 Click **More > Import CSV File**.
The **Import Users** window is displayed.



A	B	C	D	E
Username	First name	Last name	Email	Company *

* Can be left empty

3 Click **Upload** and select the file with the users to upload.

4 Click **Open**.
The file is uploaded and the **Import Completed** window is displayed.

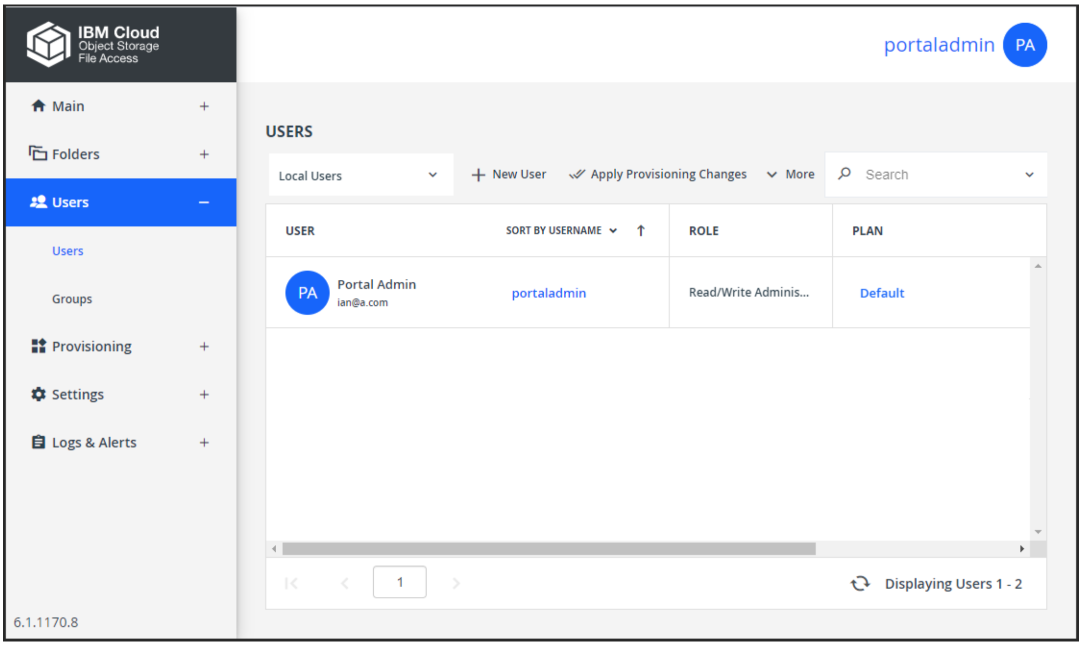
5 Click **FINISH**.

EDITING USERS

You can edit user details, including the devices with which the user has connected to the IBM COS FA Portal and the user's cloud drive.users to the IBM COS FA Portal in the following ways:

To edit an existing user:

1 Select **Users > Users** in the navigation pane.
The **USERS** page opens, displaying the users for the IBM COS FA Portal.



USER	SORT BY USERNAME	ROLE	PLAN
PA Portal Admin ian@a.com	portaladmin	Read/Write Adminis...	Default

2 Click the user's name**.**
The user window is displayed with the user name as the window title and more options, such as the user devices and cloud drive folders.

3 Edit the fields in the **Profile** option:
Username – A name for the user's IBM COS FA Portal account.
Email – The user's email address.
First Name – The user's first name.
Last Name – The user's last name.
Company (Optional) – The name of the user's company.
Role – The user's role:
Disabled – The user account is disabled. The user cannot access the IBM COS FA Portal.
End User – The user can access the IBM COS FA Portal.
Read/Write Administrator – The user can access the IBM COS FA Portal as an administrator with read-write permissions.
Read Only Administrator – The user can access the IBM COS FA Portal as an administrator with read-only permissions.
Support – The user can access the IBM COS FA Portal as an administrator and has read/write access to devices, user accounts, folders, and folder groups, and read-only access to all other settings in the IBM COS FA Portal.
Status. Select the account status:
Enabled – The account is enabled, and the user can access the IBM COS FA Portal.
Disabled – The account is disabled, and the user cannot access the IBM COS FA Portal.
The default value for new users is *Enabled*.

The default value for invited users is *Disabled*. The status changes to *Enabled* when the invited user activates the account.

Note: In order to access the IBM COS FA Portal, the user must have a role other than Disabled, and the status must be enabled.

Language – The language used for the user interface.

Expiration date – The expiration date of the user account.

Password / Retype Password – A password for the user's account. Password requirements depend on the password policy, which can be overridden and modified in the **Virtual Portal Settings**.

Force Password Change – An expiration date for the user account password. When the password has expired, the user must configure a new password on the next login.

Numeric UID (Optional) – A numeric user ID to assign the user's account.

Comment – A description of the user account.

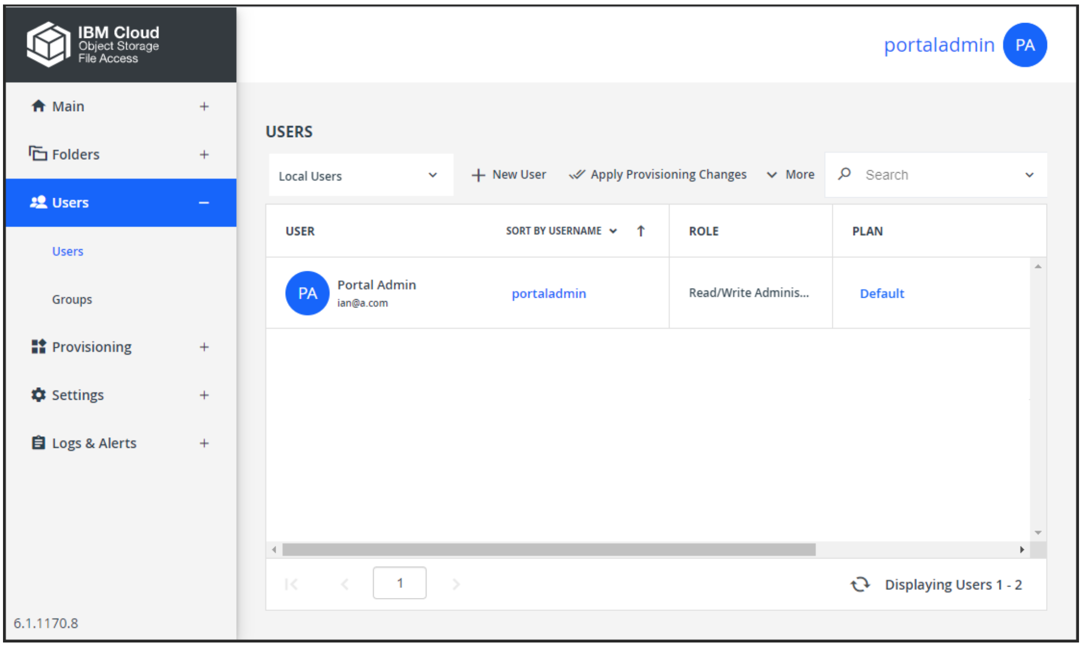
4 Click **SAVE**.

ENABLING/DISABLING USER ACCOUNTS

You can disable or enable a user account. Disabling the account prevents the user from accessing the IBM COS FA Portal, without removing the user or associated folders and files from the IBM COS FA Portal.

To enable a user account:

1 Select **Users > Users** in the navigation pane.
The **USERS** page opens, displaying the users for the IBM COS FA Portal.



USER		ROLE	PLAN
PA Portal Admin ian@a.com	portaladmin	Read/Write Adminis...	Default

2 Click the user to disable or enable.
The user window is displayed.

3 In the **Status** field, select **Enabled** or **Disabled** as required.

4 Click **SAVE**.

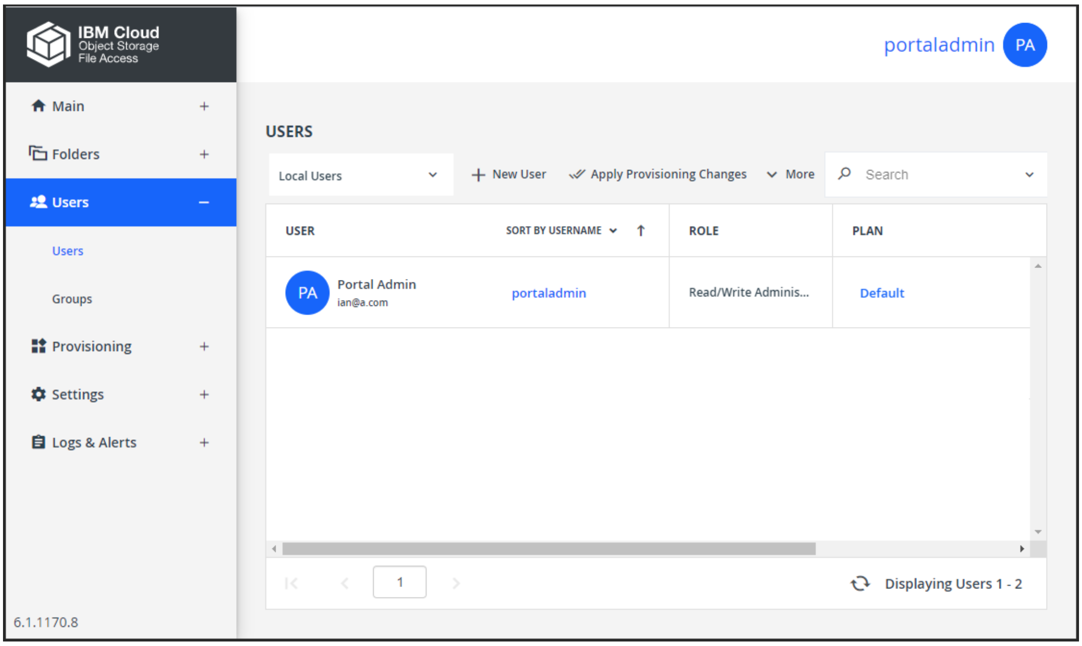
PROVISIONING USER ACCOUNTS

Users may be assigned to a default subscription plan or assigned automatically to another plan based on automatic template assignment settings. For details, see Provisioning. If desired, you can subscribe an individual user to a different subscription plan. You can also unsubscribe the user account, which deletes all files stored in the account and terminates the account.

Assigning Users to Plans

To assign a user to a plan:

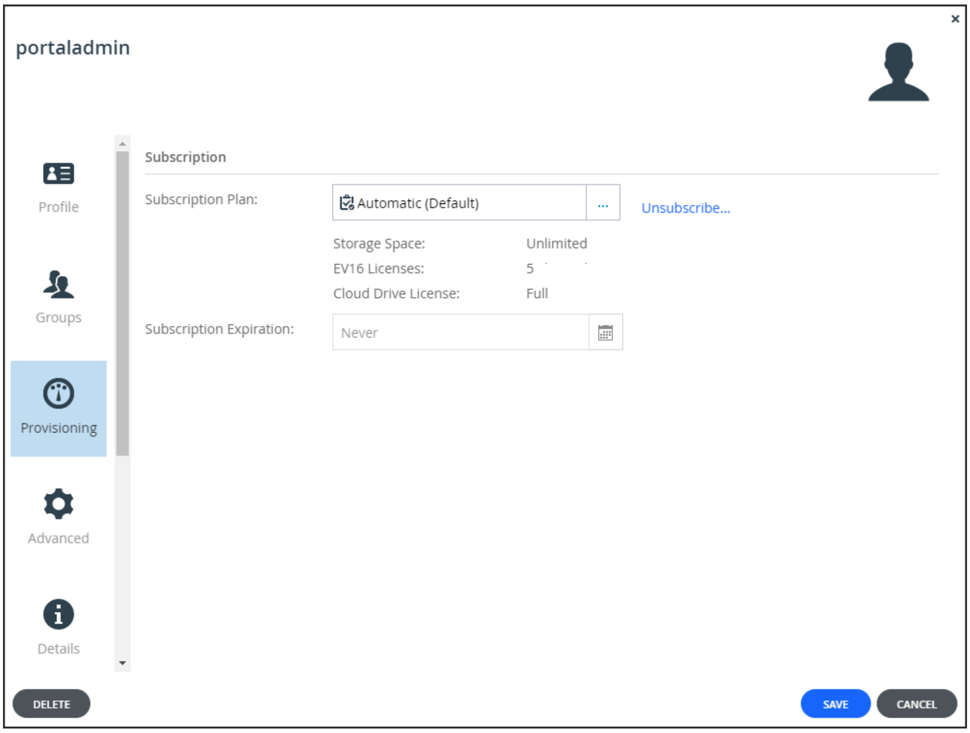
1 Select **Users > Users** in the navigation pane.
The **USERS** page opens, displaying the users for the IBM COS FA Portal.



USER	SORT BY USERNAME	ROLE	PLAN
PA Portal Admin ian@a.com	portaladmin	Read/Write Adminis...	Default

2 Click the user's name.
The user window is displayed with the user name as the window title.

3 Select the **Provisioning** option.



portaladmin

Subscription

Subscription Plan: Automatic (Default) ... Unsubscribe...

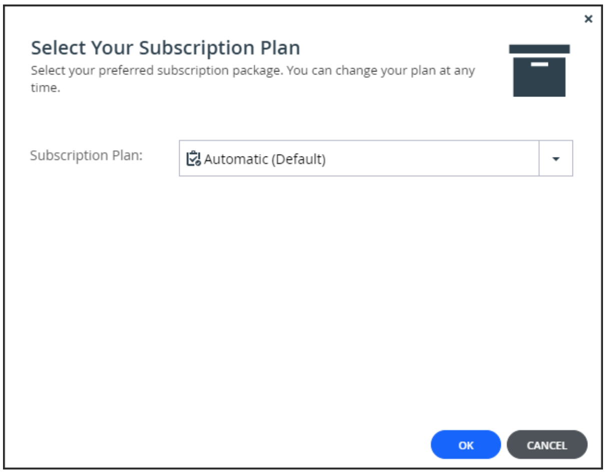
Storage Space: Unlimited

EV16 Licenses: 5

Cloud Drive License: Full

Subscription Expiration: Never

4 Click the **Subscription Plan.**
The **Select Your Subscription Plan** window is displayed.



Select Your Subscription Plan

Select your preferred subscription package. You can change your plan at any time.

Subscription Plan: Automatic (Default)

5 In the **Subscription Plan** drop-down list, select the subscription plan to assign the user.

6 Click **OK**.

7 Click **SAVE**.

Terminating User Accounts

Unsubscribing a user from a plan terminates the account and removes all the files stored in the account.

To terminate a user account:

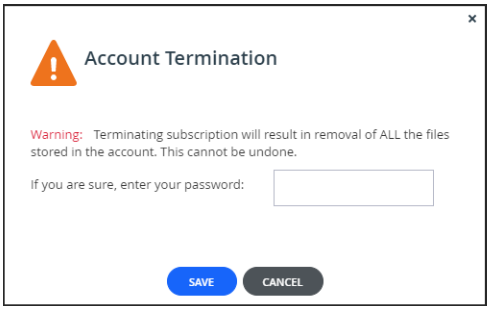
1 Select **Users > Users** in the navigation pane.
The **USERS** page opens, displaying the users for the IBM COS FA Portal.

2 Click the user's name.

The user window is displayed with the user name as the window title.

3 Select the **Provisioning** option.

4 Click **Unsubscribe**.
The **Account Termination** window is displayed.



Account Termination

Warning: Terminating subscription will result in removal of ALL the files stored in the account. This cannot be undone.

If you are sure, enter your password:

5 If you are sure you want to proceed, enter your password.

6 Click **SAVE**.

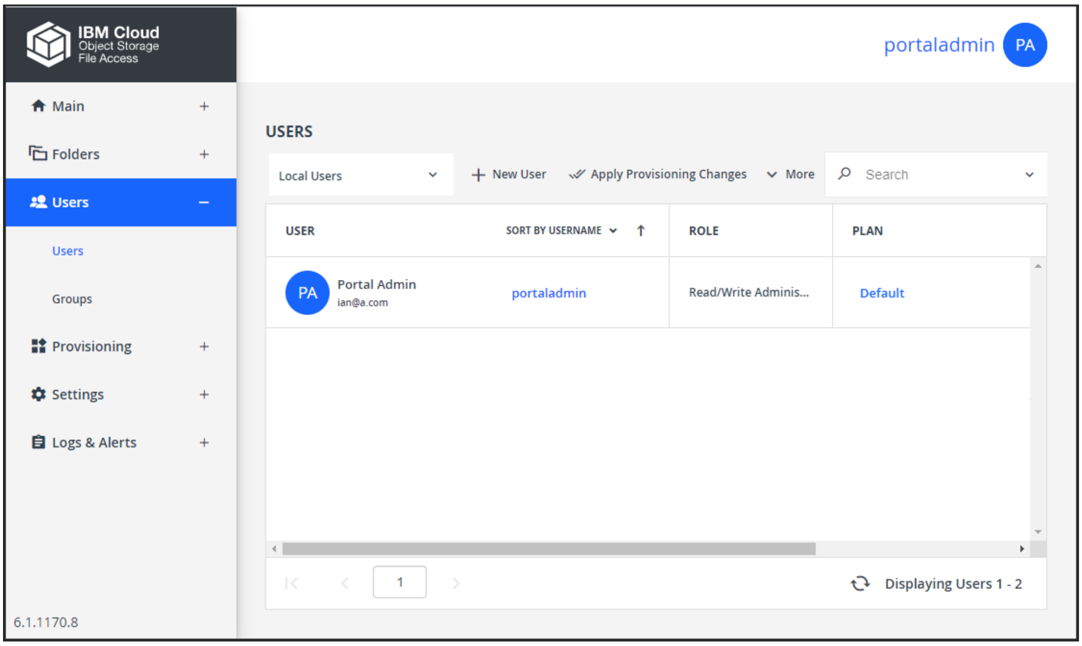
Applying Provisioning Changes

IBM COS FA Portal applies changed plan settings to all users every day at midnight. You can also apply all changes immediately.

Note: If the IBM COS FA Portal is integrated with a directory service, applying provisioning changes will also cause the IBM COS FA Portal to synchronize all the users with the directory.

To apply provisioning changes:

1 Select **Users > Users** in the navigation pane.
The **USERS** page opens, displaying the users for the IBM COS FA Portal.



USER	SORT BY USERNAME	ROLE	PLAN
PA Portal Admin ian@a.com	portaladmin	Read/Write Adminis...	Default

2 Click **Apply Provisioning Changes**.
The **Apply Provisioning Changes** window is displayed and the changes are applied.
While the changes are being applied you can either stop the process, by clicking **STOP** or close the window while the process continues to run in the background by clicking **CONTINUE IN**

BACKGROUND.

3 Click **CLOSE**.

MANAGING USER GROUPS

User groups are groups of users that you can define and then use to simplify assigning user permissions. Groups are useful when setting several types of policies and permissions, such as:

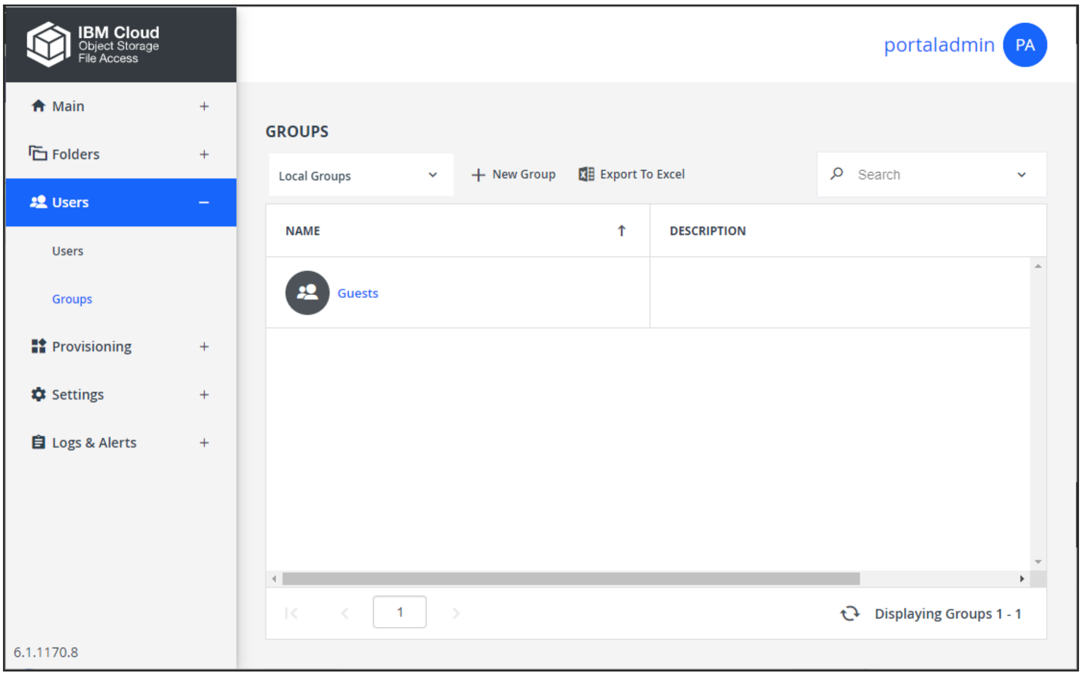
- Automatic template assignment policy. See Configuring the Automatic Template Assignment Policy.
- Setting permissions for accessing folders. See Managing Folders and Folder Groups.

Note: You can create groups manually, as described below, or you can fetch groups from a directory service, as described in Using Directory Services For the Users.

Viewing Groups

To view all user groups:

- Select **Users > Groups** in the navigation pane.
  The **GROUPS** page opens, displaying the users for the IBM COS FA Portal.



NAME	DESCRIPTION
Guests	

Displaying Groups 1 - 1

NAME – The user group's name.
DESCRIPTION – A description of the user group.

To view only a specific type of group:

1 In the navigation pane, click **Users > Groups**.
The **GROUPS** page opens, displaying the users for the IBM COS FA Portal.

2 Click the filter drop-down to filter the users either by the default **Local Users** or by an Active Directory or LDAP directory name.

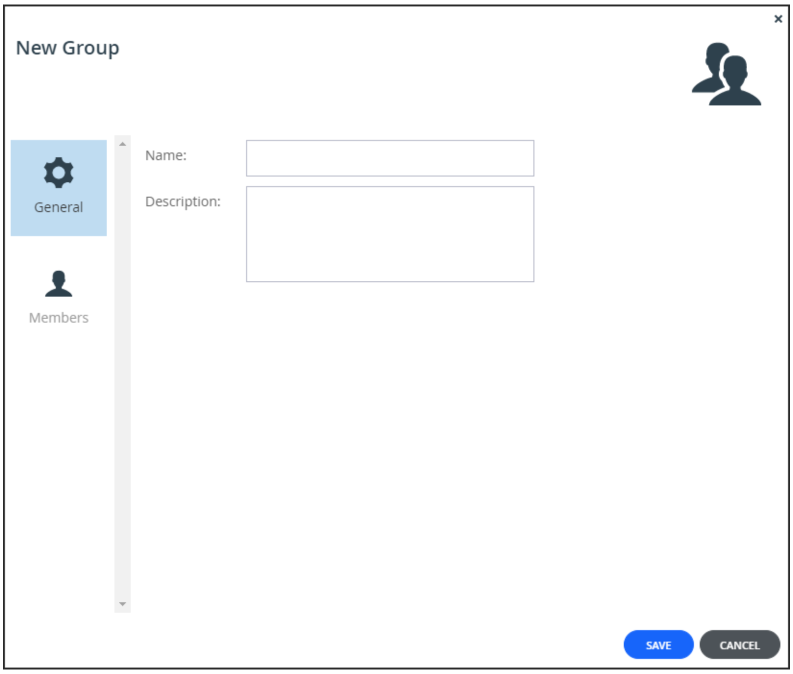
Adding or Editing Groups

To add or edit a user group:

1 Select **Users > Groups** in the navigation pane.
The **GROUPS** page opens, displaying the users for the IBM COS FA Portal.

2 Either,

- Add a group, click **New Group**.
  The **New Group** window is displayed.



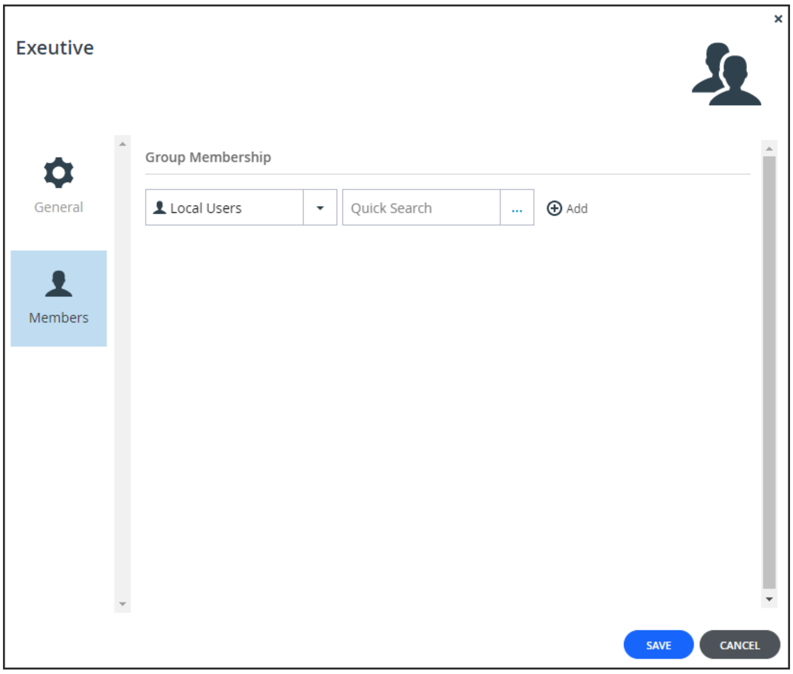
New Group

Or,

- Edit an existing group, click the group's name**.** The group window is displayed with the username of the group as the window title.

3 Complete the fields in the **Profile** option:
Name – A name for the group.
Description – A description of the group.

4 Select the **Members** option.



5 Select either **Local Users** or the Active Directory or LDAP directory name.

6 In the **Quick Search** field, enter a string that is displayed anywhere within the name of the user. A list of users matching the search string is displayed.

7 Select the user to add to the group and click **Add**.

Note: Users can belong to multiple user groups.
A User can be added to an existing group from the **Users > Users** option, described in Adding a User to an Existing Groups.

8 To remove a user from the group, select the user row and click 🗑. The user is removed from the group.

9 Click **SAVE**.

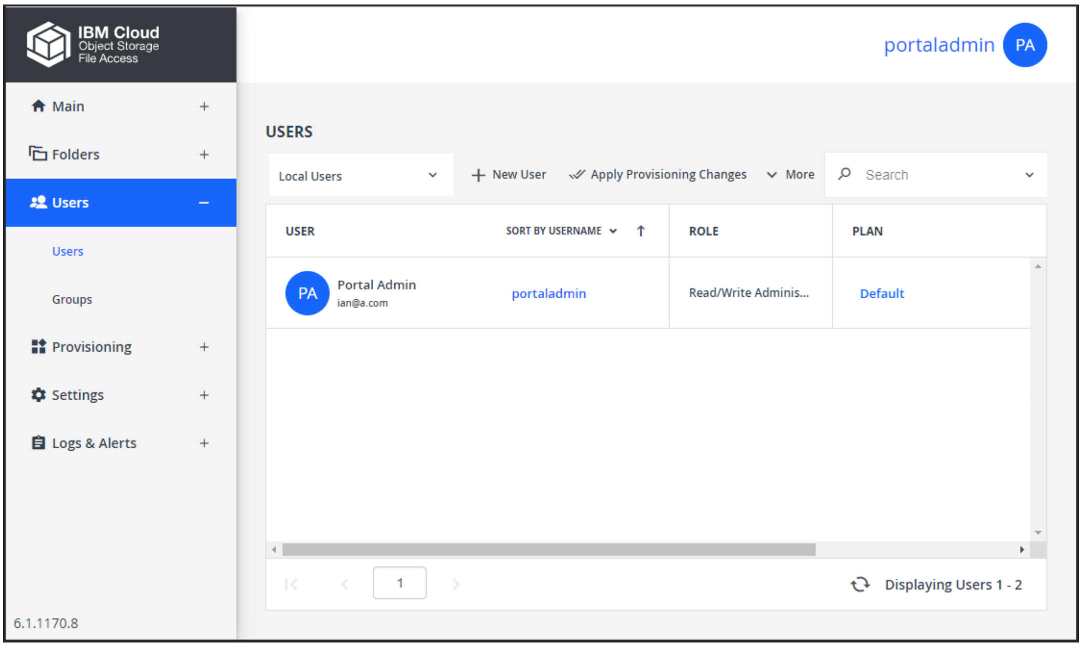
The user is added to the list of group members.

Adding a User to an Existing Groups

A User can be added to an existing group from the **Users > Users** option.

To add a user to an existing group:

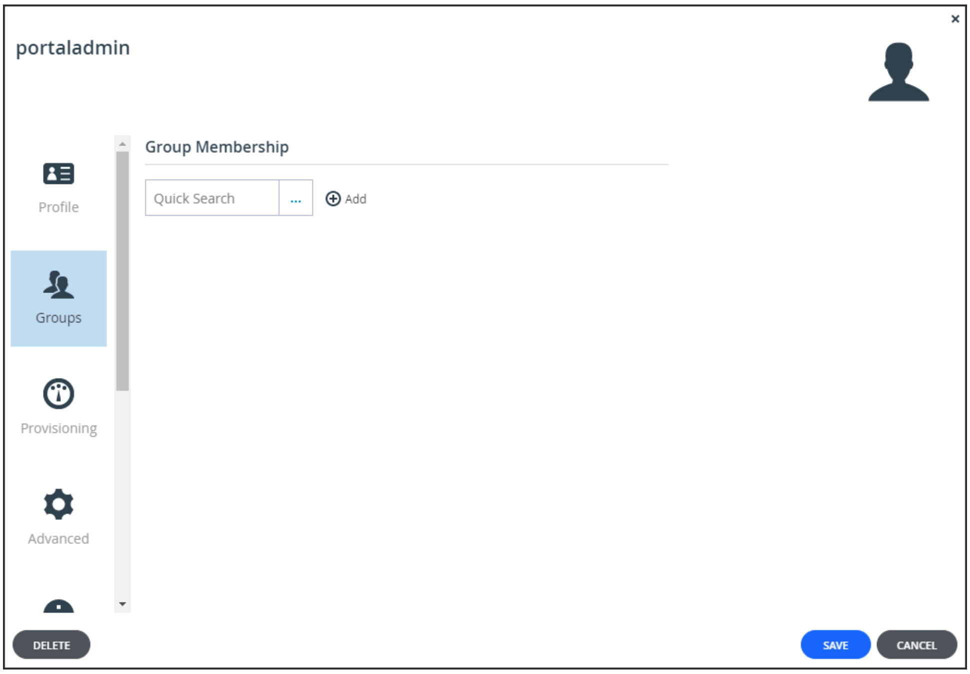
1 Select **Users > Users** in the navigation pane.
The **USERS** page opens, displaying the users for the IBM COS FA Portal.



USER	SORT BY USERNAME	ROLE	PLAN
PA Portal Admin ian@a.com	portaladmin	Read/Write Adminis...	Default

2 Click the user's name.
The user window is displayed with the user name as the window title.

3 Select the **Groups** option.



4 In the **Quick Search** field, enter a string that is displayed anywhere within the name of the group.
A list of groups matching the search string is displayed.

5 Select the group and click **Add**.

Note: Users can belong to more than one user group.

6 Click **SAVE**.

Exporting Group Information to Excel

You can export a list of groups and their details to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export a list of groups to Microsoft Excel:

1 Select **Users > Groups** in the navigation pane.
The **GROUPS** page opens, displaying all the users accounts.

2 Click **Export to Excel**.

The group list is downloaded to your computer.

Deleting Groups

To delete a user group:

Note: Deleting a user group does not delete the users.

1 Select **Users > Groups** in the navigation pane.
The **GROUPS** page opens, displaying all the users accounts.

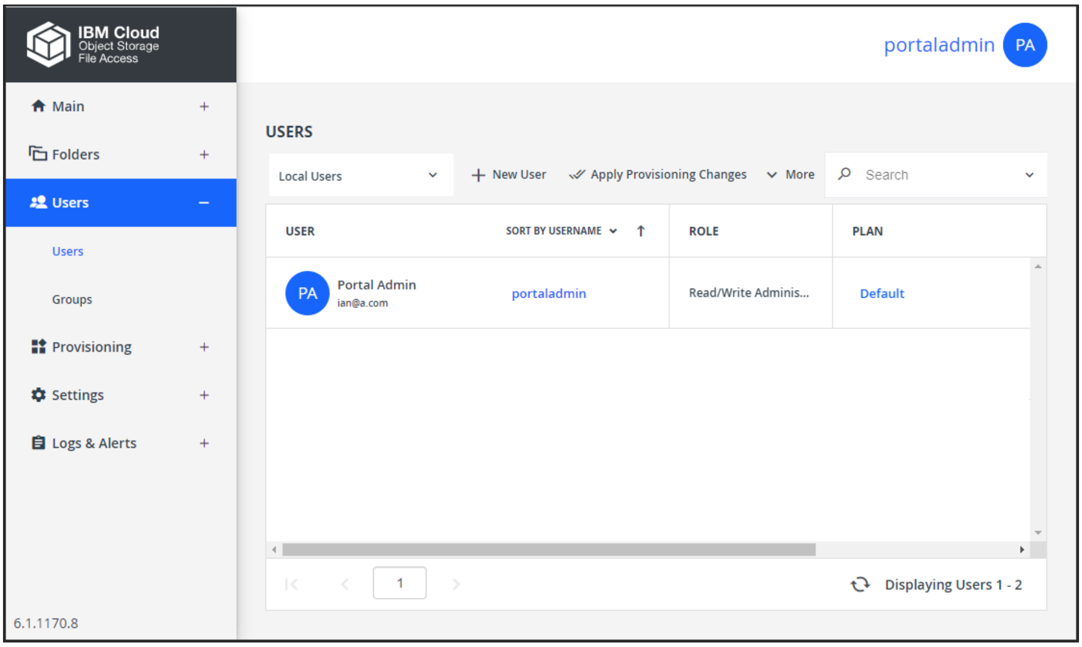
2 Select the group's row to delete and click **Delete Group**.
A confirmation window is displayed.

3 Click **DELETE GROUP** to confirm.

The group is deleted.

CONFIGURING A USER'S DEDUPLICATION SETTINGS

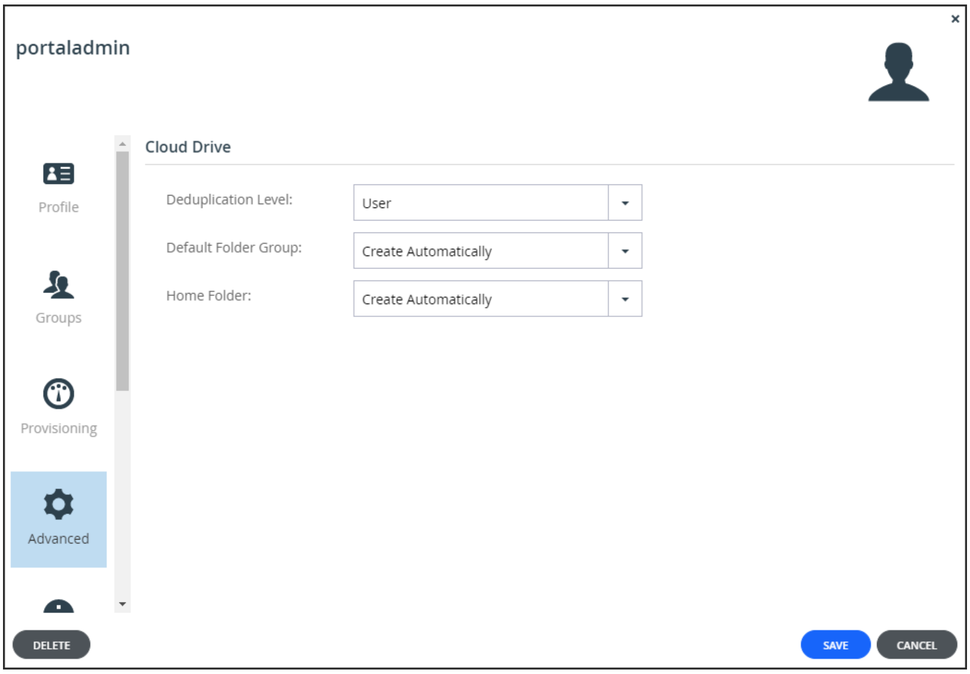
1 Select **Users > Users** in the navigation pane.
The **USERS** page opens, displaying the users for the IBM COS FA Portal.



USER	SORT BY USERNAME	ROLE	PLAN
PA Portal Admin ian@a.com	portaladmin	Read/Write Adminis...	Default

2 Click the user's name.
The user window is displayed with the user name as the window title.

3 Select the **Advanced** option.



Cloud Drive

Deduplication Level: User

Default Folder Group: Create Automatically

Home Folder: Create Automatically

Cloud Drive

Deduplication Level – The default deduplication level to use for new cloud folders:

User – Create a single folder group for the user account, containing all of the user account's cloud folders. Deduplication is performed for the user account's folder group.

Portal – Use a single folder group that is shared by the entire virtual IBM COS FA Portal, containing all of the cloud folders in the IBM COS FA Portal.

Folder – Create a folder group for each of the user account's devices, containing all of the device's cloud folders. Deduplication is performed separately for each of the user account's folder groups. IBM COS FA Portal recommends this option.

Default Folder Group – Displayed only if **User** is selected as the *Deduplication Level*. Select the default folder group to use for all of the user account's cloud folder:

- An existing folder group
- **Create Automatically**. Automatically create a new folder group.

Home Folder – One of the user's personal folders to act as the user's home folder. The home folder is a personal folder that is linked to the user account and cannot be deleted.

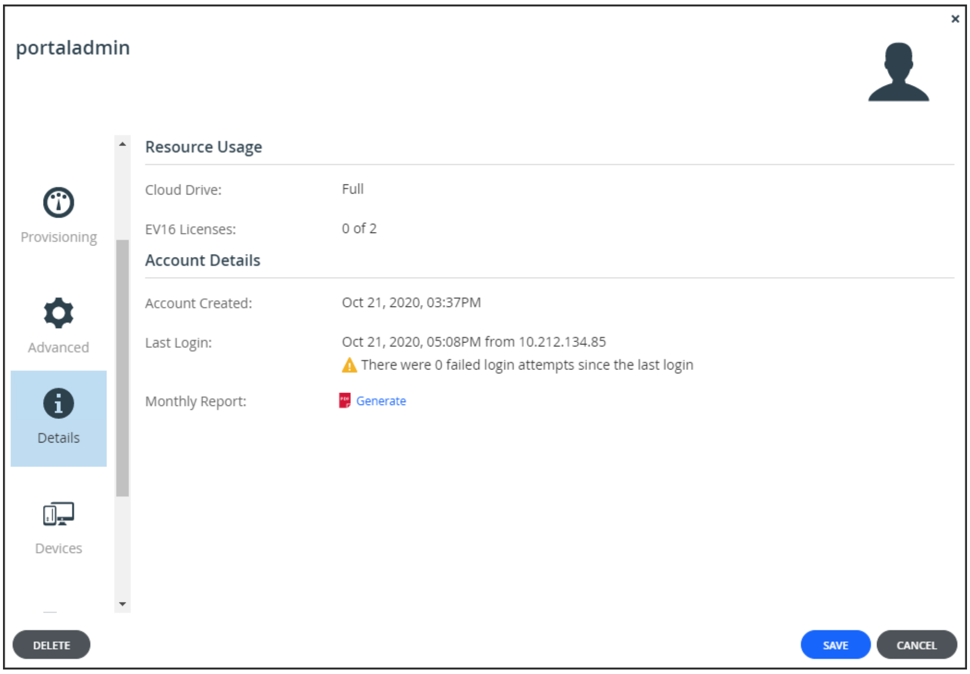
4 Click **SAVE**.

VIEWING USER DETAILS

1 Select **Users > Users** in the navigation pane.
The **USERS** page opens, displaying the users for the IBM COS FA Portal.

2 Click the user's name.
The user window is displayed with the user name as the window title.

3 Select the **Details** option.



portaladmin

Resource Usage

Cloud Drive: Full

EV16 Licenses: 0 of 2

Account Details

Account Created: Oct 21, 2020, 03:37PM

Last Login: Oct 21, 2020, 05:08PM from 10.212.134.85

⚠ There were 0 failed login attempts since the last login

Monthly Report: Generate

Storage Quota – The amount of storage the user has consumed out of the total amount available in their subscription plan.

Cloud Drive – Whether the user is provisioned to have the Cloud Drive service.

EV*nn* Licenses – The number of IBM COS FA Gateway licenses associated with the user account. If the user's subscription plan includes IBM COS FA Gateways, this number is expressed as a number of the total number of IBM COS FA Gateways available in the user account's subscription plan.

Account Created – The date and time when the user account was created.
Last Login – The date and time when the user last signed on to the IBM COS FA Portal as well as details about how many successful and failed times the user attempted to sign on and the IP addresses used to sign-on.
Monthly Report – A link for generating and downloading a monthly report of events in the user account in PDF format.

Generating Monthly Reports

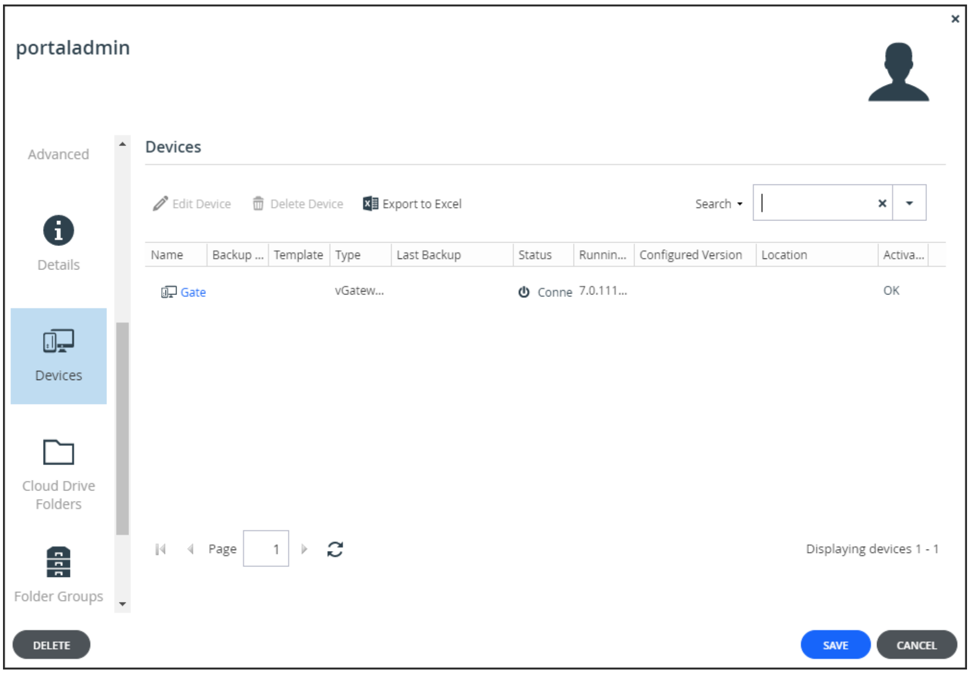
You can trigger the immediate generation and sending of the monthly report for a specific user account.

To generate a monthly report for the user:

- In the **Details** option, click **Generate**.
  A report is generated and sent to the user by email.

MANAGING A USER'S DEVICES

1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the IBM COS FA Portal.
2. Click the user's name.
   The user window is displayed with the user name as the window title.
3. Select the **Devices** option.



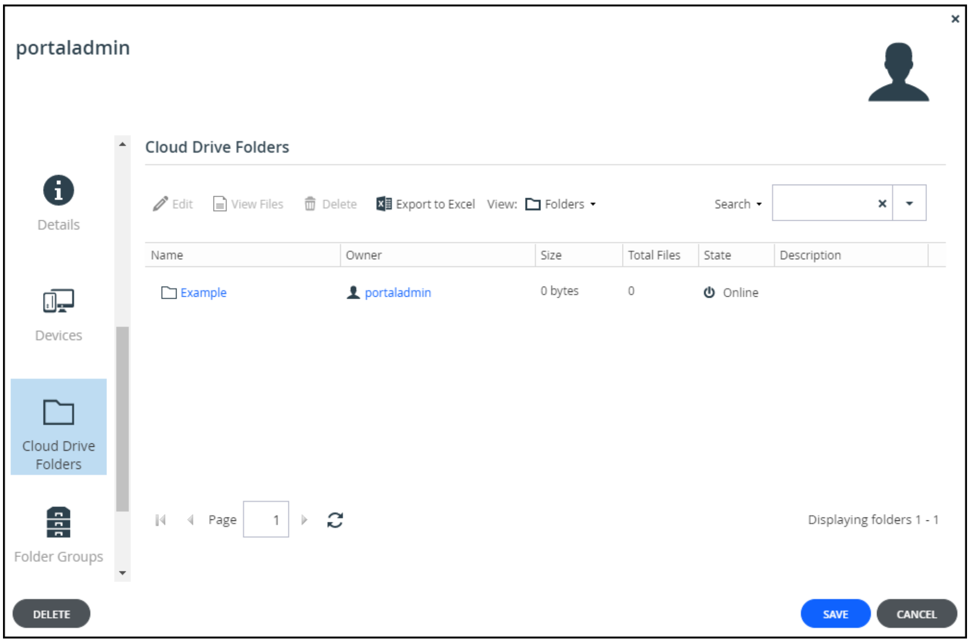
Name	Backup ...	Template	Type	Last Backup	Status	Runnin...	Configured Version	Location	Activa...
Gate			vGatew...		Conne	7.0.111...			OK

You can perform any of the device management tasks described in Managing Devices.

MANAGING A USER'S CLOUD DRIVE FOLDERS

1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the IBM COS FA Portal.
2. Click the user's name.
   The user window is displayed with the user name as the window title.

3 Select the **Cloud Drive Folders** option.
The **Cloud Drive Folders** option displays all cloud drive folders owned by the user.



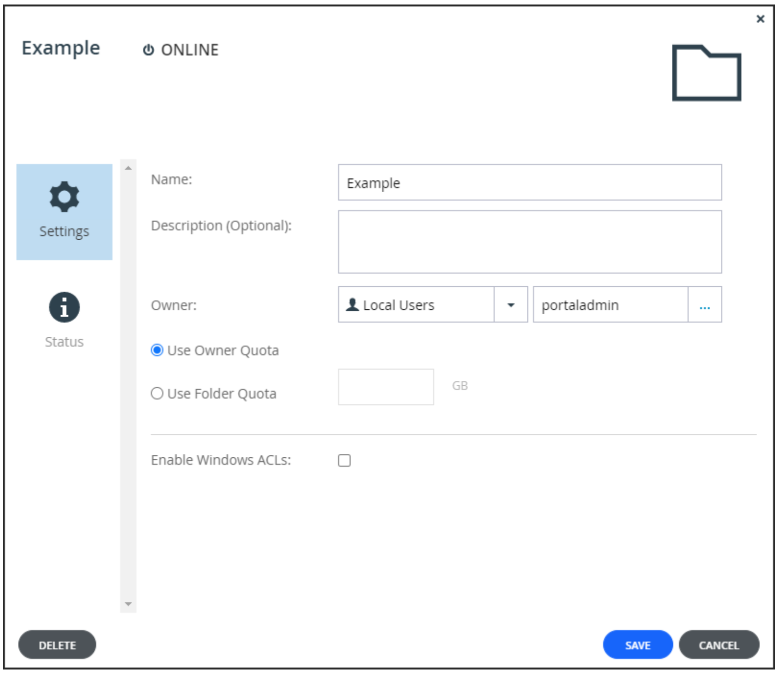
Name	Owner	Size	Total Files	State	Description
Example	portaladmin	0 bytes	0	Online	

4 Click **Export to Excel** to export the folder details of all the cloud drive folders to a comma separated values (*.csv) Microsoft Excel file on your computer.

5 Select a row and click **View Files** to open the IBM COS FA Portal view with the files from the folder displayed.

6 Select a row and click **Delete** to delete the folder from the cloud drive after confirming this is what is wanted.

7 Click a folder to configure its settings and review its status: The number of files and the storage used by these files.



Example ONLINE

Name: Example

Description (Optional):

Owner: Local Users portaladmin

● Use Owner Quota

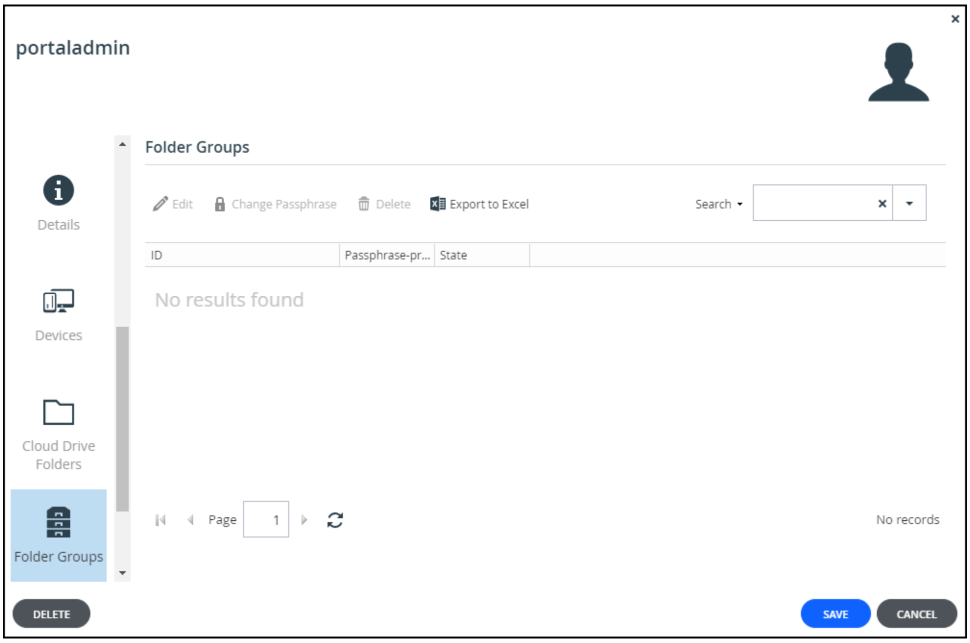
○ Use Folder Quota GB

Enable Windows ACLs: □

- You can add a description for the folder as well as changing the folder and owners names. You can also set the folder to inherit the Windows ACLs from the local PC settings.

MANAGING A USER'S FOLDER GROUPS

1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the IBM COS FA Portal.
2. Click the user's name.
   The user window is displayed with the user name as the window title.
3. Select the **Folder Groups** option.
   The **Folder Groups** option displays all folder groups associated with the user.



You can perform any of the folder group management tasks described in Managing Folders and Folder Groups.

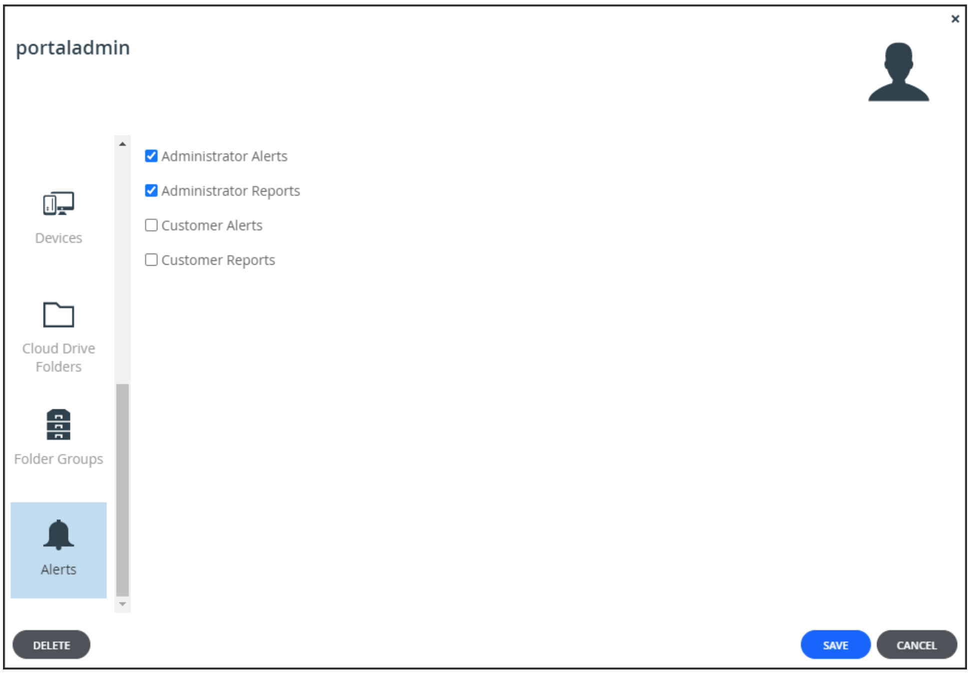
CONFIGURING ALERTS FOR TEAM ADMINISTRATORS

You can specify alerts that team administrators receive.

1 Select **Users > Users** in the navigation pane.
The **USERS** page opens, displaying the users for the IBM COS FA Portal.

2 Click the user's name for an administrator user.
The user window is displayed with the user name as the window title.

3 Select the **Alerts** option.



☑ Administrator Alerts
☑ Administrator Reports
☐ Customer Alerts
☐ Customer Reports

4 Check the types of alerts to receive:
Administrator Alerts – Notifications about IBM COS FA Portal-level problems.
Administrator Reports – Notifications reporting IBM COS FA Portal-level activity.
Customer Alerts – Notifications about device-level problems.
Customer Reports – Notifications about customer activity.

5 Click **SAVE**.

CUSTOMIZING ADMINISTRATOR ROLES

By default, IBM COS FA Portal includes built-in administrator roles for administrators:

Read/Write Administrator – The administrator has read/write permissions throughout the IBM COS FA Portal.
Read Only Administrator – The administrator has read-only permissions throughout the IBM COS FA Portal.
Support – The administrator has read/write access to devices, user accounts, folders, and folder groups, and read-only access to all other settings in the IBM COS FA Portal.

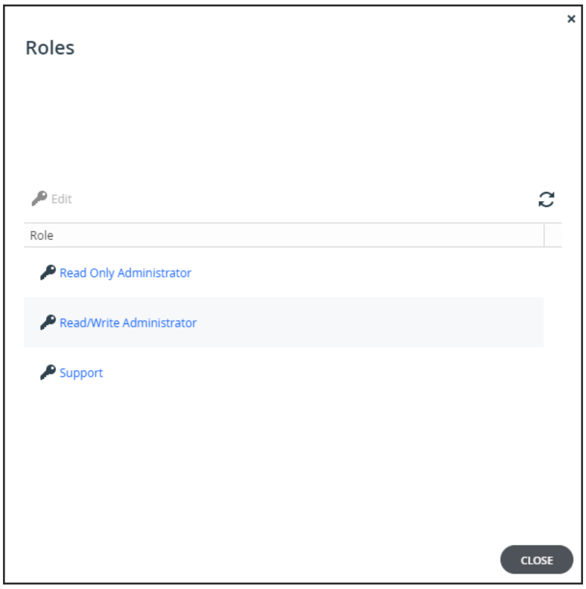
You can customize these roles, adding or removing permissions.

To customize an administrator role:

1 Select **Settings** in the navigation pane.
The **Control Panel** page is displayed.

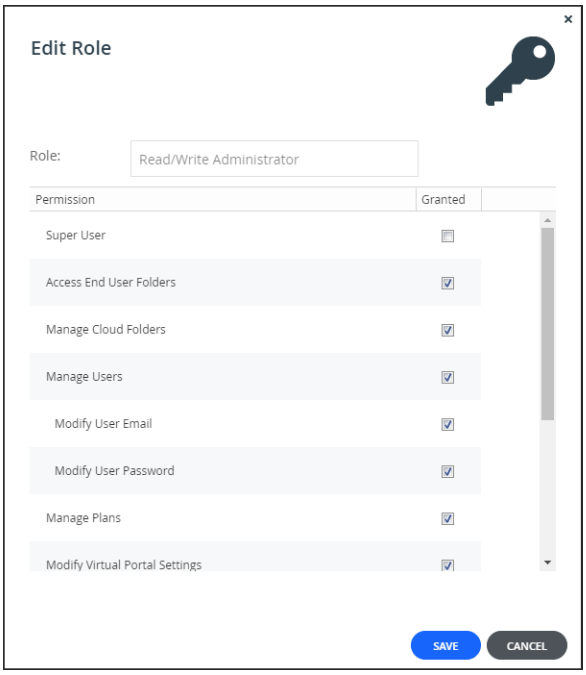
2 Select **User Roles**, under **USERS** in the **Control Panel** page.

The **Roles** window is displayed.



Role
Read Only Administrator
Read/Write Administrator
Support

3 Either click a role or select a role's row and click **Edit**.
The **Edit Role** window is displayed.



Role: Read/Write Administrator

Permission	Granted
Super User	□
Access End User Folders	☑
Manage Cloud Folders	☑
Manage Users	☑
Modify User Email	☑
Modify User Password	☑
Manage Plans	☑
Modify Virtual Portal Settings	☑

4 Check the permissions you want to include in the role, and uncheck those that you don't want to include.
Access End User Folders – Allow administrators to access end users' folders. If this option is not selected, and an administrator with this role attempts to access an end user's folder, the administrator will be prompted to enter the folder owner’s password.
Manage Cloud Folders – Allow administrators to manage cloud folders. Without this permission, an administrator only has read-only access to the projects and personal folder objects.

Note: A Read/Write Administrator with both **Access End User Folders** rand **Manage Cloud Folders** roles can also share the end user cloud folders.

Manage Users – Allow administrators to edit user emails and passwords and add, edit, and delete users.

Modify User Email – Allow administrators to modify the email addresses associated with user accounts.

Modify User Password – Allow administrators to modify the passwords associated with user accounts.

Manage Plans – Allow administrators to add, edit, delete, assign, set defaults, and remove default plans.

Modify Virtual Portal Settings – Allow administrators to modify virtual IBM COS FA Portal settings. This option is selected by default and cannot be modified.

Modify Roles – Allow administrators to modify administrator roles.

Allow Single Sign On to Devices – Allow administrators to remotely manage devices for which Remote Access with single sign on (SSO) is enabled, without entering the username and password for accessing the device.

5 Click **SAVE**.

Permissions Per Administrator Role

The different administrator roles have different permissions.

Permission	Read/Write Administrator	Read Only Administrator	Support
Access End User Folders	Yes	Yes	Yes (Default is No)
Manage All Folders	Yes	No	Yes
Manage Users	Yes	No	Yes
Modify User Email	Yes	No	Yes
Modify User Password	Yes	No	Yes
Manage Plans	Yes	No	Yes
Modify Virtual Portal Settings	Yes	No	Yes (Default is No)
Modify Roles	Yes	No	Yes (Default is No)

EXPORTING USER DETAILS TO EXCEL

You can export a list of user accounts and their details to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export a user details to Microsoft Excel:

1 Select **Users > Users** in the navigation pane.
The **USERS** page opens, displaying all the users accounts.

2 Click **More > Export to Excel**.

The user list is downloaded to your computer. For each user, the report includes user details such as names and email address, role, subscription plan for the user, and the available licenses.

DELETING USER ACCOUNTS

Deleting a user account from the IBM COS FA Portal cancels the user's subscriptions to plans, and deletes all of the user's folders and folder groups.

To delete a user account:

1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying all the users accounts.
2. Either,
   a. Select the user’s row to delete and click **Delete**.
      A confirmation window is displayed.
   b. Click **DELETE USER INCLUDING ASSOCIATED FOLDERS** to confirm.

   Or,

   a. Click the user.
   b. Click **DELETE**.
      A confirmation window is displayed.
   c. Click **DELETE USER INCLUDING ASSOCIATED FOLDERS** to confirm.

The user is deleted.

CHAPTER 8. MANAGING FOLDERS AND FOLDER GROUPS

Folders

Cloud Drive folders are folders created by the Cloud Drive service for personal and shared use. The IBM COS FA Portal automatically creates a personal folder for each user account's private files when the user account is created in the IBM COS FA Portal. The folder is displayed to the user as `My Files` and is the user's home folder. The folder contains files that can only be viewed and edited by the user. The home folder name and the automatic creation of the home folder can be changed in the General Settings of the IBM COS FA Portal, accessed via **Settings > Virtual Portal Settings**.

Note: You can migrate your Windows file system to an IBM COS FA Gateway, maintaining the same file structure and ACLs after the migration. Every share on the IBM COS FA Gateway, must be first created as a Cloud Folder in the IBM COS FA Portal.

By default, when folders are created in a IBM COS FA Portal, they are assigned a name based on the device's name. For example, if a device is named JohnS, then this device's files will be backed up to a folder called JohnS, and its cloud files will be stored in a folder called JohnS-CloudFiles followed by a number. You can add new folders manually and can edit their properties.

Folder Groups

IBM COS FA Portal organizes cloud folders in *folder groups*. Each folder group acts as a deduplication realm. Deduplication means that when files are written to a folder in a folder group, the files' content is compared to data already stored in *other* files in the same folder group. Only the data that *differs* from existing data in the other files is stored in the folder group so that data is only stored once.

Folder groups are organized according to each user's deduplication level for Cloud Drive folders.

For Cloud Drive folders, you can set the deduplication level to any of the following:

- **User**
  A single folder group is created for each user account, containing all of the user account's cloud folders. Deduplication is performed for the user account's folder group.
- **Folder**
  A folder group is created for each of a user account's devices, containing all of the device's cloud folders. Deduplication is performed separately for each of the user account's folder groups.
- **Portal**
  A single folder group is shared by *all* user accounts in the IBM COS FA Portal. The folder group acts as a deduplication realm that spans the entire IBM COS FA Portal. In other words, if different users' devices back up similar data, the similar data will only be stored once.

You can change the default deduplication levels for any user created in the IBM COS FA Portal, and you can change any user's deduplication levels. You can choose a different level for folders and for Cloud Drive folders.

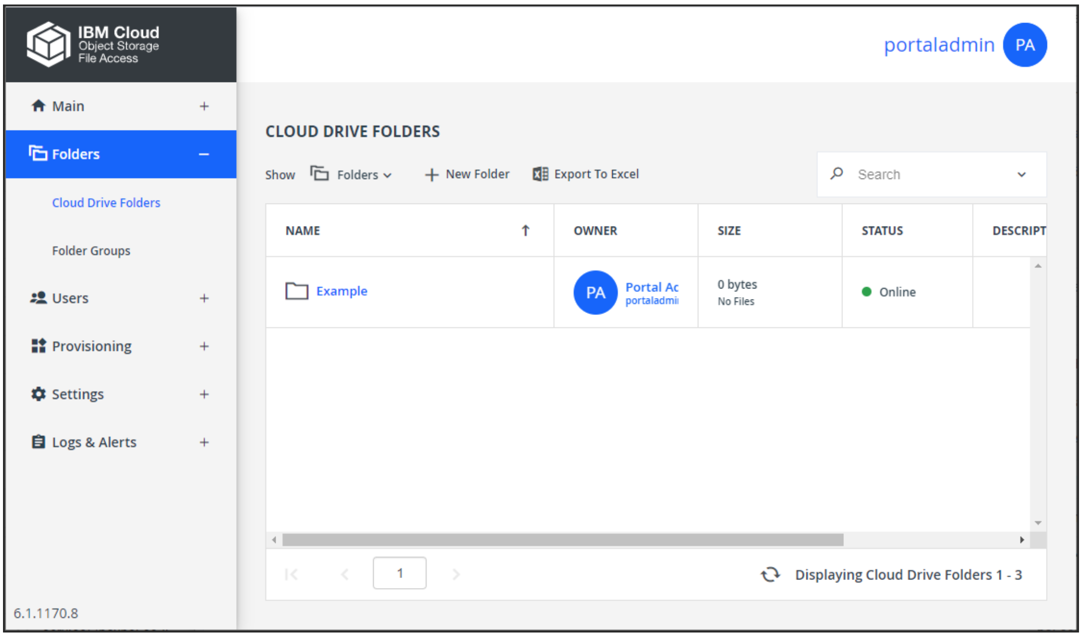
Note: All folders in a folder group must use the same encryption key and passphrase.

In this chapter

VIEWING CLOUD DRIVE FOLDERS

To view all cloud drive folders:

- Select **Folders > Cloud Drive Folders** in the navigation pane.
  The **CLOUD DRIVE FOLDERS** page opens, displaying all cloud drive folders.



NAME	OWNER	SIZE	STATUS	DESCRIPT
Example	PA Portal Ac portaladmi	0 bytes No Files	● Online	

NAME – The folder's name.
OWNER – The user name of the folder's owner.
SIZE – The current size of the folder. The total number of files in the folder is displayed under the size.
STATUS – The folder's status:

Online – The folder is online, and it is possible to view and modify, and sync files to it.
Offline – The folder is offline, and it is not possible to view, modify, or sync files to it. Folders may be taken offline during some maintenance operations, such as when repairing a folder.

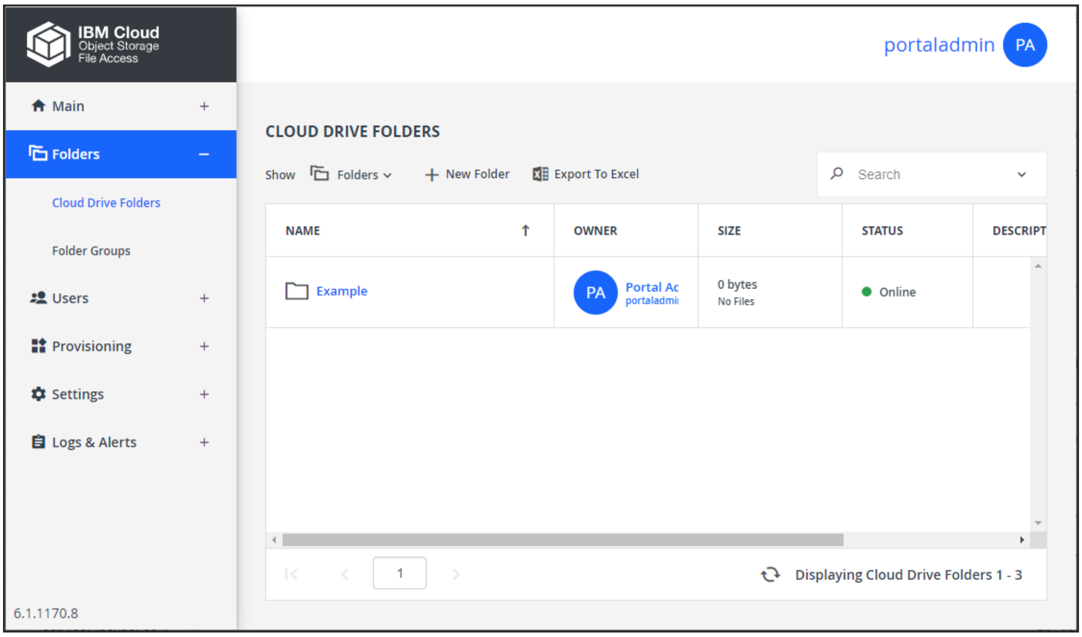
DESCRIPTION – An optional description of the folder.

CREATING OR EDITING CLOUD DRIVE FOLDERS

You can create a folder in the cloud drive for a user, or edit an existing folder.

To create or edit a cloud drive folder:

1 Select **Folders > Cloud Drive Folders** in the navigation pane.
The **CLOUD DRIVE FOLDERS** page opens, displaying all cloud drive folders.

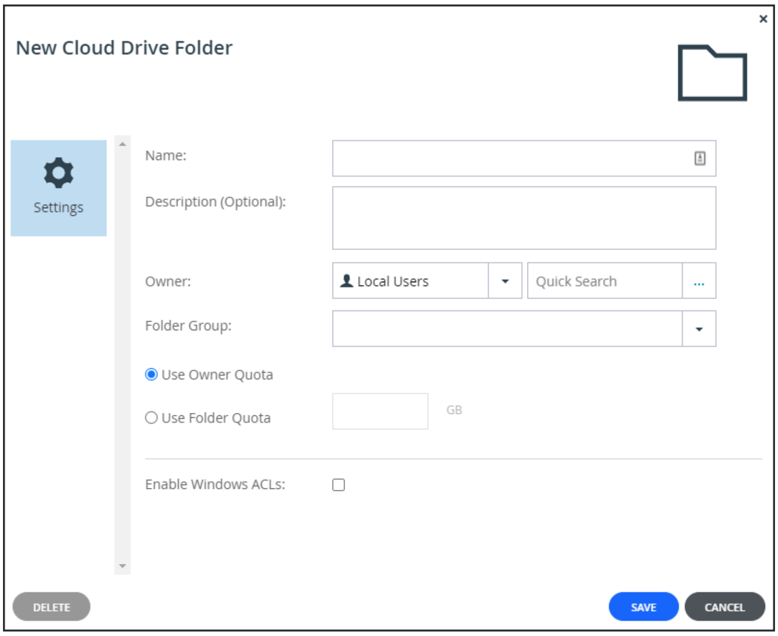


NAME	OWNER	SIZE	STATUS	DESCRIPT
Example	PA Portal Ac portaladmi	0 bytes No Files	Online	

Displaying Cloud Drive Folders 1 - 3

2 Either,

- Create a new folder, click **New Folder**.
  The **New Cloud Drive Folder** window is displayed.



New Cloud Drive Folder

Settings

Name:

Description (Optional):

Owner: Local Users | Quick Search

Folder Group:

● Use Owner Quota

○ Use Folder Quota GB

Enable Windows ACLs: □

Or,

- Edit an existing folder, click the folder's name**.**
  The folder window is displayed with the folder name as the window title.

3. Complete the fields:
   Name – A name for the folder.
   > **Note:** Renaming a nested cloud drive folder makes the folder inaccessible to every IBM COS FA Gateway that includes this share.

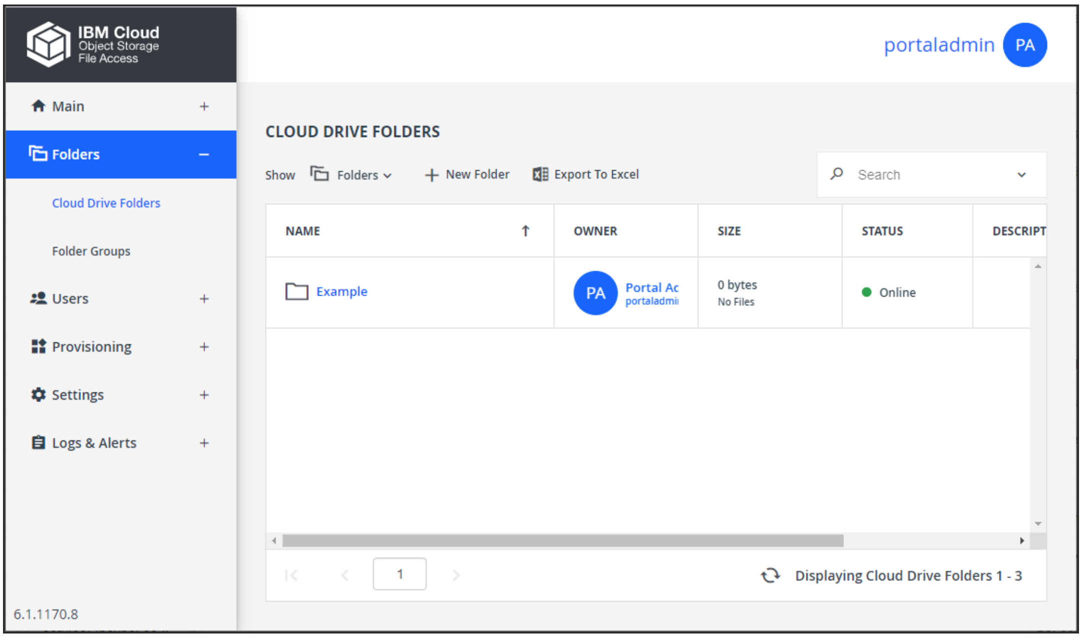
   Description – A description for the folder.
   Owner – The user to own the folder. The owner controls access to the folder.
   Folder Group – A folder group for the folder. The drop-down list only displays the folders for the selected owner.
   Use Owner Quota – The storage for this folder is taken from the storage quota of the folder owner.
   Use Folder Quota – The amount of storage for this folder which is taken from the storage quota of the team IBM COS FA Portal. The value must be an integer value.
   Enable Windows ACLs – Select this option if you are syncing an IBM COS FA Gateway share to a IBM COS FA Portal including the NT ACLs and extended attributes on the IBM COS FA Gateway. The files are saved in the IBM COS FA Portal using the NT ACL settings defined on the files. For more information, see Maintaining Windows File Server Structure and ACLs in IBM COS FA Portal Folders.
4. Click **SAVE**.

The cloud drive folder is created or updated.

MONITORING FOLDER USAGE

To monitor folder usage:

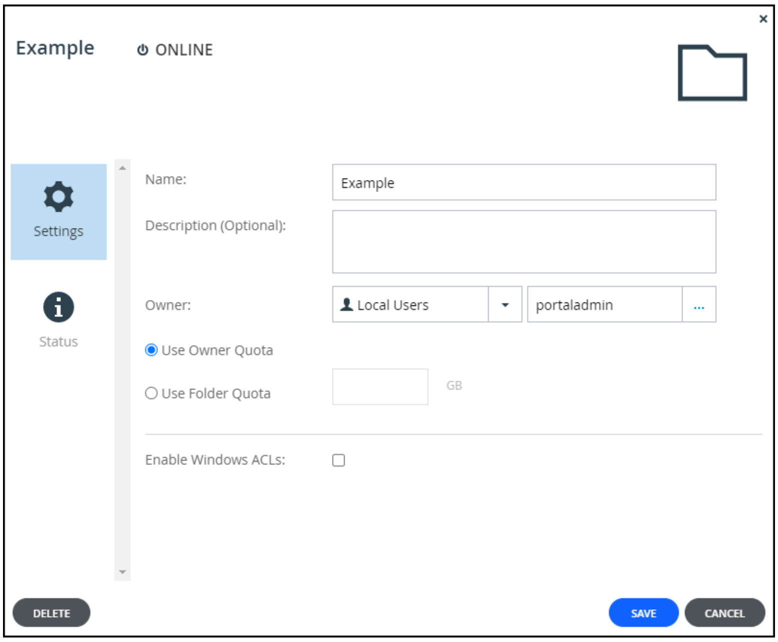
1 Select **Folders > Cloud Drive Folders** in the navigation pane.
The **CLOUD DRIVE FOLDERS** page opens, displaying all cloud drive folders.



CLOUD DRIVE FOLDERS

NAME	OWNER	SIZE	STATUS	DESCRIPT
Example	PA Portal Ac portaladmi	0 bytes No Files	● Online	

2 Click the folder's name.
The folder window is displayed with the folder name as the window title.



Name: Example

Description (Optional):

Owner: Local Users portaladmin

● Use Owner Quota

○ Use Folder Quota GB

Enable Windows ACLs: □

3 Click **Status**.
The folder status is displayed.You can see the following information about the folder:

- The number of files in the team project. Click **View Files** to open the IBM COS FA Portal displaying the team project folder. You are prompted for the user password to gain access to the files.

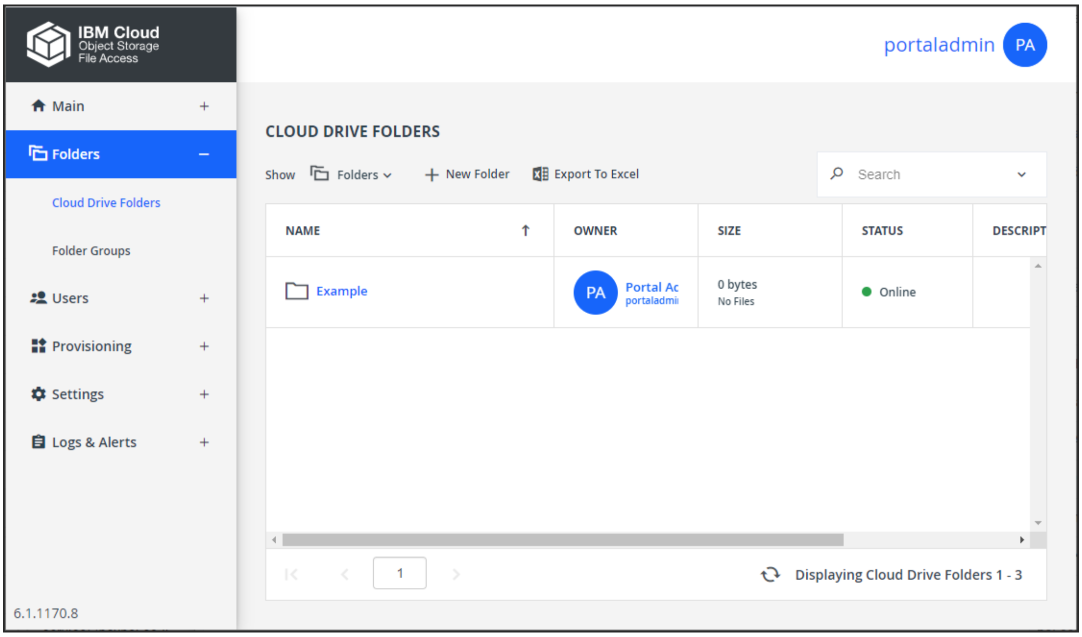
- The amount of storage that has been used. If the folder is a team project folder, the amount of storage used is shown as the percentage of storage allocated to the team project folder.
- The folder group the of the folder.
- When antivirus protection is configured, the number of files found to contain malware. Click **View Files** to view the list of infected files.
- When data loss prevention is configured, The number of files that have sensitive content. Click **View Files** to view the list of sensitive files.

VIEWING FOLDER CONTENTS

Note: Viewing folder content can be managed by the *Access End User Folders* administrator role attribute. See Customizing Administrator Roles for details.

To view a folder's content:

1 Select **Folders > Cloud Drive Folders** in the navigation pane.
The **CLOUD DRIVE FOLDERS** page is displayed.



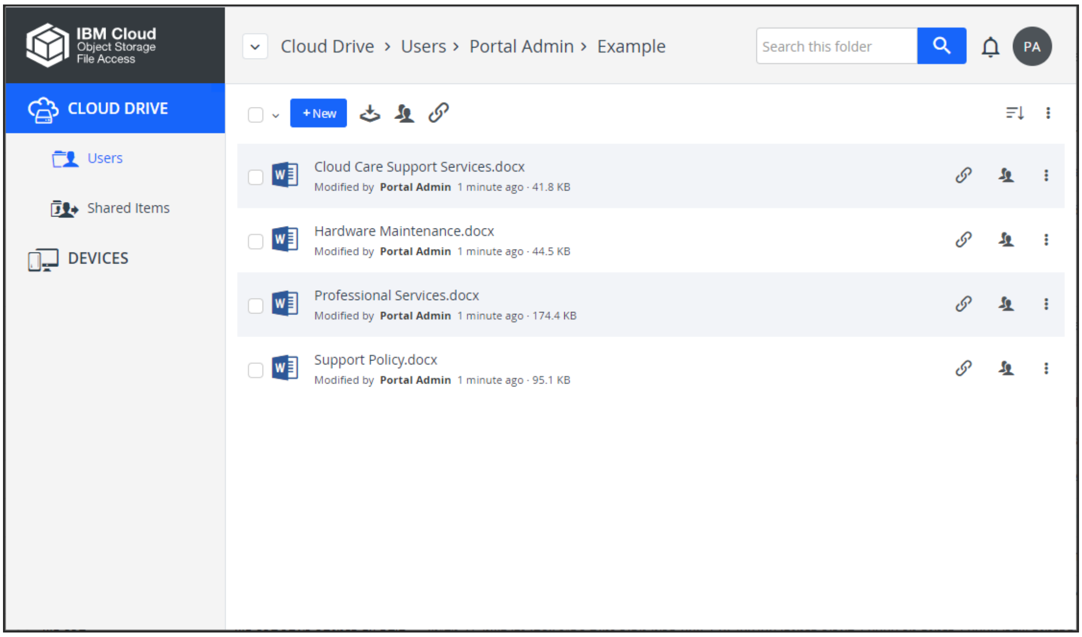
CLOUD DRIVE FOLDERS

NAME	OWNER	SIZE	STATUS	DESCRIPT
Example	PA Portal Ac portaladmi	0 bytes No Files	● Online	

2 Mouse over the folder you want to view.

The folder icon is displayed.

3 Click next to the folder you want to view.
If you don't have permission to access the folder, you are prompted for the folder owner's password. Enter the password and click **OK**.
The IBM COS FA Portal view opens, showing the folder you selected.



Cloud Care Support Services.docx
Modified by **Portal Admin** 1 minute ago · 41.8 KB

Hardware Maintenance.docx
Modified by **Portal Admin** 1 minute ago · 44.5 KB

Professional Services.docx
Modified by **Portal Admin** 1 minute ago · 174.4 KB

Support Policy.docx
Modified by **Portal Admin** 1 minute ago · 95.1 KB

You can manage the files in this view, as if you are the end user.

MAINTAINING WINDOWS FILE SERVER STRUCTURE AND ACLS IN IBM COS FA PORTAL FOLDERS

If you have your Windows file server structure and ACLs defined in a shared system on your IBM COS FA Gateway, as described in the *IBM COS FA Gateway Administrator Guide,* and you want to implement this structure on the IBM COS FA Portal, use the following procedure.

To maintain your Windows file server structure and ACLs in the IBM COS FA Portal**:**

1 Create a new cloud drive folder. You cannot edit an existing folder to emulate Windows ACLs.

2 Create the cloud share root folders in the IBM COS FA Portal, as described in To create or edit a cloud drive folder:, checking **Enable Windows ACLs** in step 3.

3 Set up the cloud share with Windows ACL emulation in the IBM COS FA Gateway, as described in the *IBM COS FA Gateway Administrator Guide*.

4 Migrate the file system from the old share in the IBM COS FA Gateway to the new share, as described in the *IBM COS FA Gateway Administrator Guide.*

Since you can have many users and root folders to migrate, IBM COS FA Portal recommends writing scripts to perform these tasks. The following procedure, shows how to set up the file server in the IBM COS FA Portal.

EXPORTING FOLDER DETAILS TO EXCEL

You can export a list of folders and their details to a Comma Separated Values (*.csv) Microsoft Excel file on your computer.

To export a folder details to Microsoft Excel:

1. Select **Folders > Cloud Drive Folders** in the navigation pane.
   The **CLOUD DRIVE FOLDERS** page is displayed.
2. Click **Export to Excel**.

The folder list is downloaded to your computer.

DELETING FOLDERS

To delete a folder:

1. Select **Folders > Cloud Drive Folders** in the navigation pane.
   The **CLOUD DRIVE FOLDERS** page is displayed.
2. Either,
   a. Select the folder’s row to delete and click **Delete**.
      A confirmation window is displayed.
   b. Click **DELETE** to confirm.

   Or,
   a. Click the folder.
   b. Click **DELETE**.
      A confirmation window is displayed.
   c. Click **YES** to confirm.

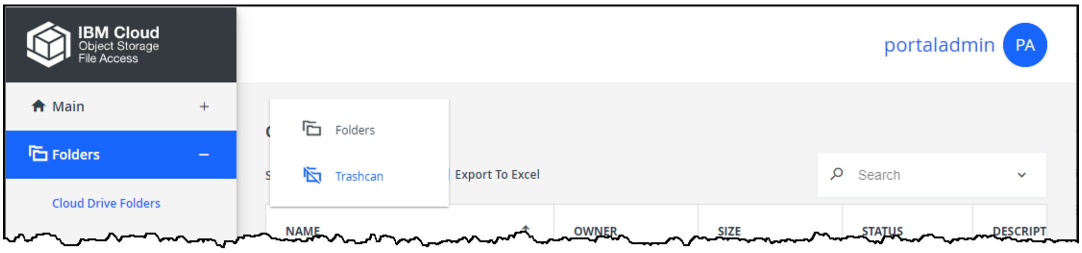
The folder is deleted.

MANAGING DELETED FOLDERS

You can review folders that have been deleted and either undelete them or permanently delete them.

To view deleted folders:

1. Select **Folders > Cloud Drive Folders** in the navigation pane.
   The **CLOUD DRIVE FOLDERS** page is displayed.
2. In the **Show** option, from the drop-down list select **Trashcan**, to display all the deleted cloud folders.

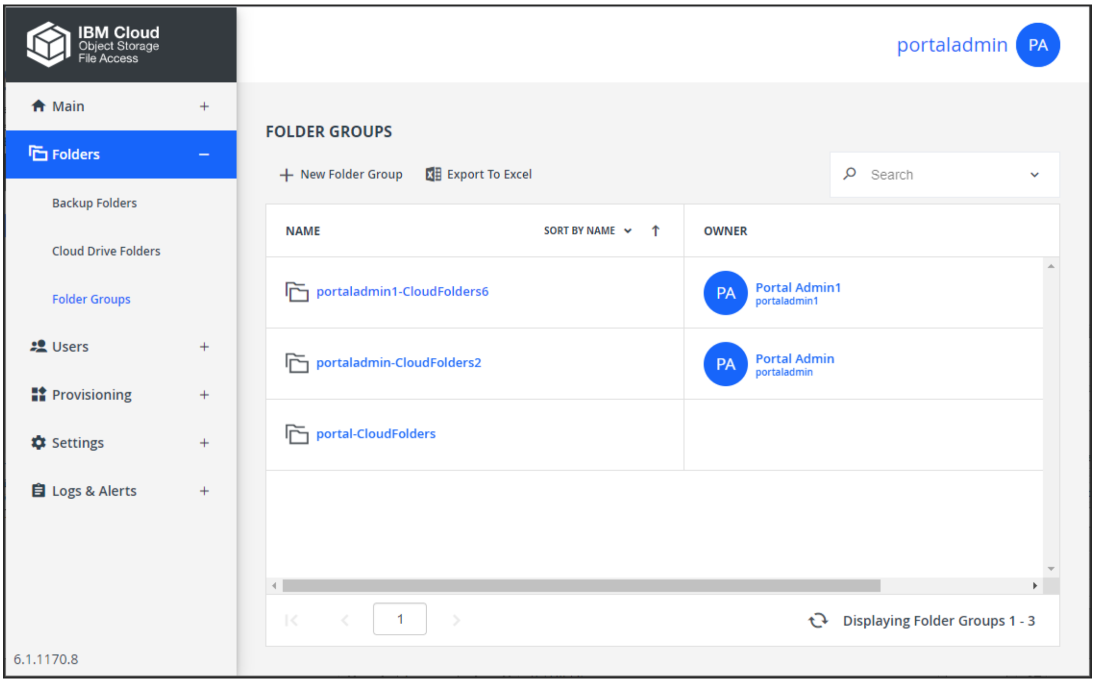


3. You can select one folder row to review the files in that folder that were deleted, as described in Viewing Folder Contents or select one or more rows to either undelete the folders, by clicking **Undelete**, or permanently delete the folders and their contents, by clicking **Delete Permanently**.

VIEWING FOLDER GROUPS

To view all folders groups in the IBM COS FA Portal:

- Select **Folders > Folder Groups** in the navigation pane.
  The **FOLDER GROUPS** page opens, displaying all folder groups.



NAME	OWNER
portaladmin1-CloudFolders6	Portal Admin1 portaladmin1
portaladmin-CloudFolders2	Portal Admin portaladmin
portal-CloudFolders	

NAME – The folder group's name. If the folder is passphrase-protected, this information is displayed.

OWNER – The user name of the folder group's owner.

STATUS – The folder's status:

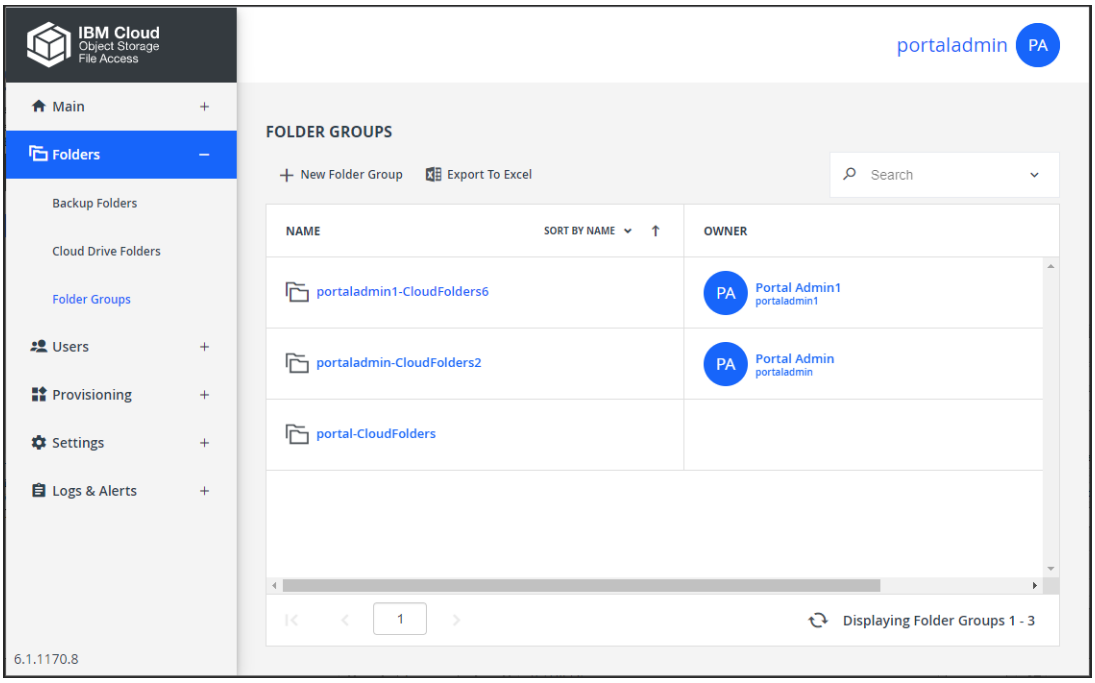
> **Online** – The folder group is online, and it is possible to view and modify, and sync files to it.
>
> **Offline** – The folder group is offline, and it is not possible to view, modify, or sync files to it. Folders may be taken offline during some maintenance operations, such as when repairing a folder.

ADDING A FOLDER GROUP

When a device first backs up files to a IBM COS FA Portal, and cooperative deduplication is enabled for the device's owner, a folder group is automatically created. By default, the folder group is assigned a name based on the device's name. You can add new folder groups manually.

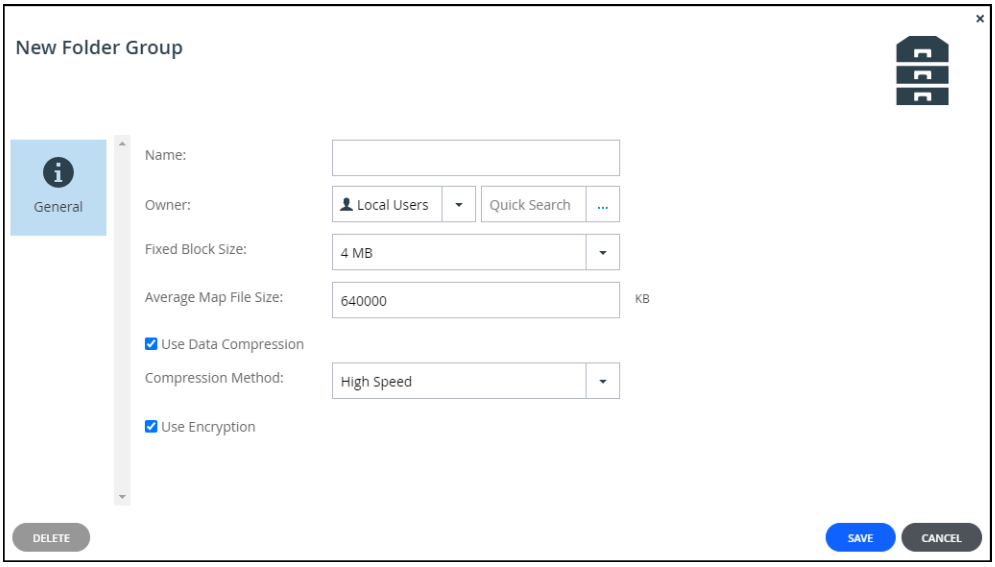
To add a folder group:

1 Select **Folders > Folder Groups** in the navigation pane.
The **FOLDER GROUPS** page opens, displaying all folder groups.



NAME	OWNER
portaladmin1-CloudFolders6	PA Portal Admin1 portaladmin1
portaladmin-CloudFolders2	PA Portal Admin portaladmin
portal-CloudFolders	

2 Click **New Folder Group**.
The **New Folder Group** window is displayed.



Name:

Owner: Local Users Quick Search ...

Fixed Block Size: 4 MB

Average Map File Size: 640000 KB

☑ Use Data Compression

Compression Method: High Speed

☑ Use Encryption

3 Complete the fields in the **General** option.

Name – A name for the folder group.
Owner – An owner for the folder group. When editing a folder group, you can click on the owner's name to open the User Account Manager and manage the owner's user account. For information on managing user accounts, see Managing Administrator Users.
Fixed Block Size – The fixed block size used by the folder group. IBM COS FA Portal deduplication splits each stored file into blocks. Increasing the **Fixed Block Size** causes the files to be split into larger chunks before storage, and results in increased read/write throughput at the cost of a reduced deduplication ratio. Increased block size is useful for workloads that require high performance, as well as for those that do not gain greatly from deduplication. For example, where the stored files consist mostly of videos, images, and music files that are not frequently modified. IBM recommends keeping the default 4MB fixed block size.
Average Map File Size – The average map file size used by new folder groups. IBM COS FA Portal uses file maps to keep track of the blocks each file is made of. The Average Map File Size represents the maximum size of file that will be represented using a single file map object. For example, if the average map file size is set to 100MB, files of up to approximately 100MB will have one file map, files of up to approximately 200MB will have two file maps, and so on. Reducing the average map file size causes more file maps to be created per file. This may result in smoother streaming of files; however, it will also result in some extra overhead for creating, indexing, and fetching the additional file maps.
Use Data Compression – Data in this folder group will be stored in compressed format. IBM recommends only unchecking this option after consulting with IBM support.

> **Compression Method** – The compression method to use for file storage: **High Compression** or **High Speed**.

Use Encryption – The data in this folder group is stored in encrypted format.

Note: Only the **Name** and **State** settings can be changed after creating the folder group.

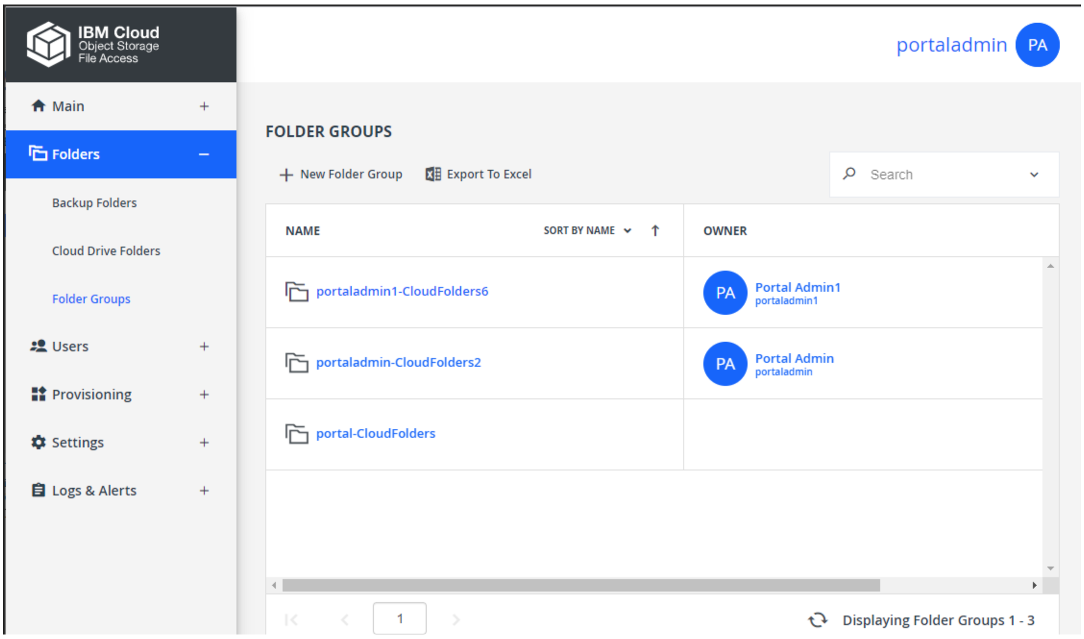
4 Click **SAVE**.

EDITING A FOLDER GROUP

You can edit folder group properties.

To edit a folder group:

- Select **Folders > Folder Groups** in the navigation pane.
  The **FOLDER GROUPS** page opens, displaying all folder groups.

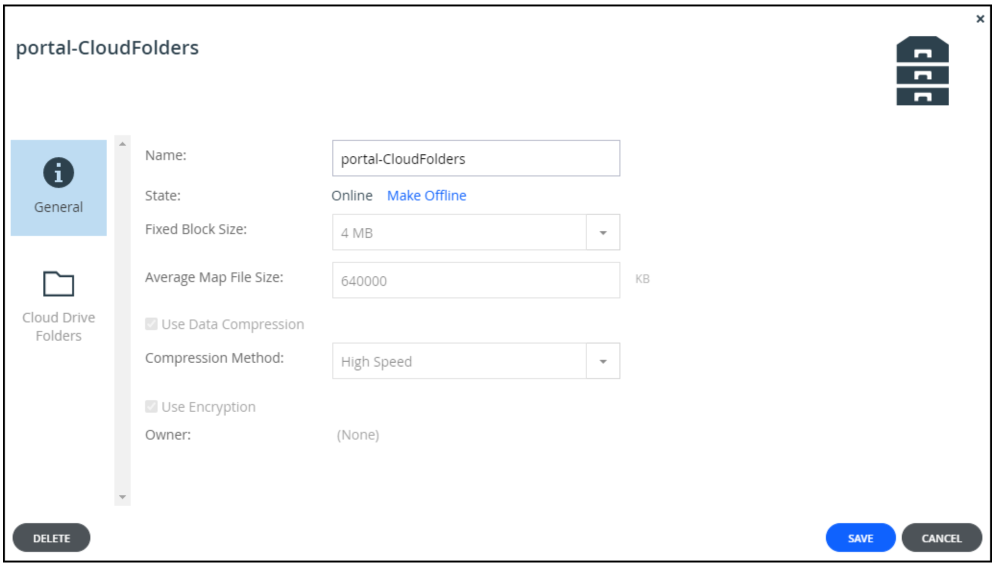


FOLDER GROUPS

NAME	OWNER
portaladmin1-CloudFolders6	PA Portal Admin1 portaladmin1
portaladmin-CloudFolders2	PA Portal Admin portaladmin
portal-CloudFolders	

Displaying Folder Groups 1 - 3

5 Click the folder group’s name.
The folder group window is displayed with the folder group name as the window title and options for **Cloud Drive Folders**.



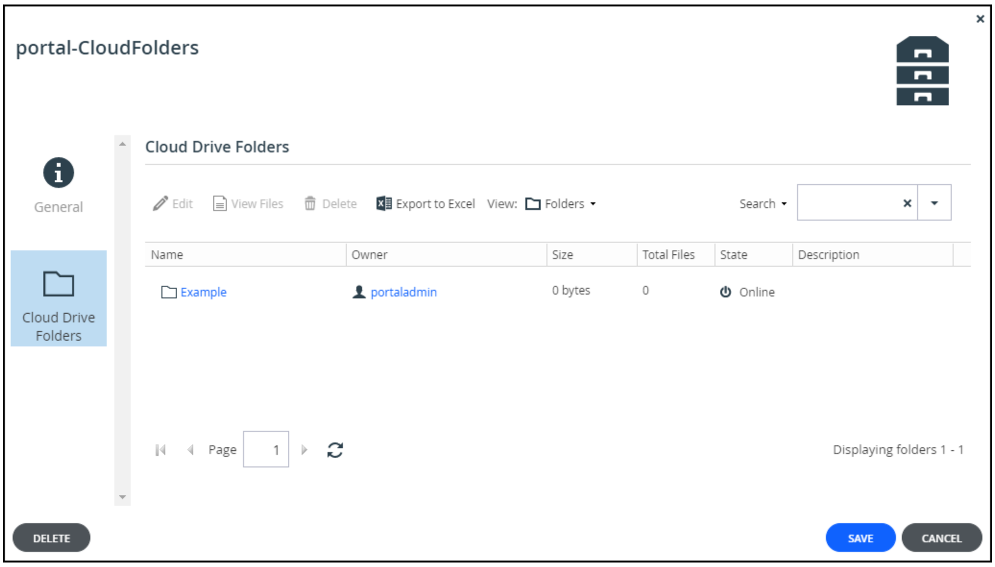
portal-CloudFolders

Name: portal-CloudFolders
State: Online Make Offline
Fixed Block Size: 4 MB
Average Map File Size: 640000 KB
☐ Use Data Compression
Compression Method: High Speed
☐ Use Encryption
Owner: (None)

6 Edit enabled fields in the **General** option.
Name – The name for the folder group.
State – The folder group's state:

Online – The folder group is online. Click **Make Offline** to change the state to offline.
Offline – The folder group is offline. Click **Make Online** to change the state to online.
All member folders will inherit the folder group's state.

7 To manage cloud drive folders in a folder group, click the **Cloud Drive Folders** option.



Name	Owner	Size	Total Files	State	Description
Example	portaladmin	0 bytes	0	Online	

8 Perform any folder task.

9 Click **SAVE**.

EXPORTING FOLDER GROUP DETAILS TO EXCEL

You can export a list of folder groups and their details to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export a list of folder groups to Microsoft Excel:

1 Select **Folders > Folder Groups** in the navigation pane.
The **FOLDER GROUPS** page is displayed.

2 Click **Export to Excel**.

The folder group list is downloaded to your computer.

DELETING FOLDER GROUPS

To delete a folder group:

1 Select **Folders > Folder Groups** in the navigation pane.
The **FOLDER GROUPS** page is displayed.

2 Either,

a Select the folder group row to delete and click **Delete Folder Group**.
A confirmation window is displayed.

b Click **DELETE FOLDER GROUP** to confirm.

Or,

a Click the folder group.

b Click **DELETE**.
A confirmation window is displayed.

c Click **YES** to confirm.

The folder group is deleted.

CHAPTER 9. CONTENT PROTECTION

In this chapter

- Cloud Drive Policy
- Virus Protection

CLOUD DRIVE POLICY

Cloud Drive policy determines the type of data that can be synchronized through IBM COS FA Gateways or uploaded to the IBM COS FA Portal.

To set Cloud Drive policy, you create *Allow* and *Deny* rules based on the following attributes:

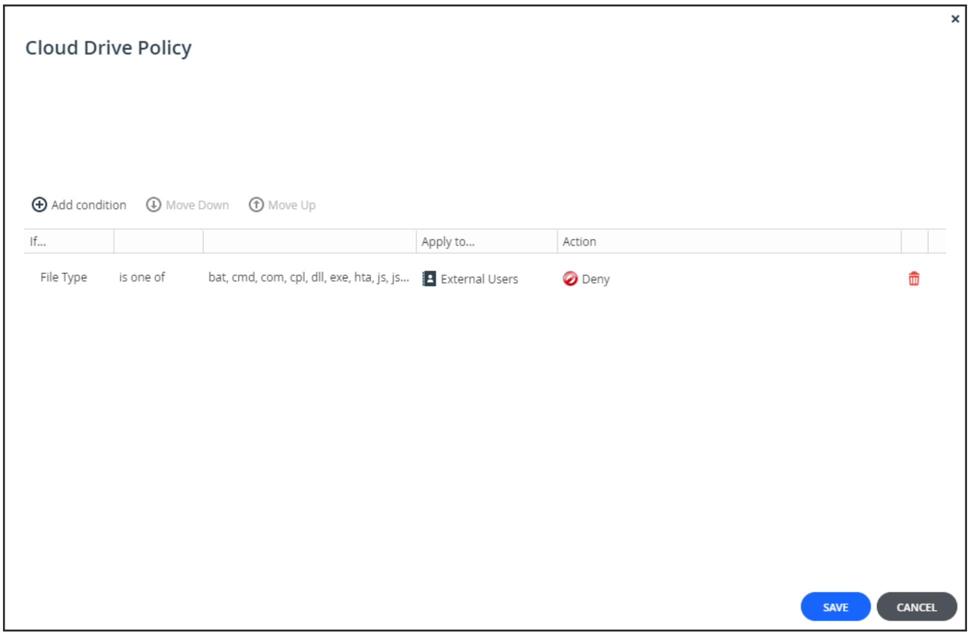
- File Name
- File Size
- File Type

Each rule can be applied to everyone or to a specific user or group, whether they are users and groups from an integrated directory service or local users and groups defined in the IBM COS FA Portal.

To configure Cloud Drive policy:

1 Select **Settings** in the navigation pane.

2 Select **Cloud Drive Policy** under **CLOUD DRIVE** in the **Control Panel** page.
The **Cloud Drive Policy** window is displayed.



If...			Apply to...	Action
File Type	is one of	bat, cmd, com, cpl, dll, exe, hta, js, js...	External Users	Deny

3 Click **Add condition** to define a condition.

a In the **If** column select a file attribute.

b Select an operator, such as *is one of*.

c Enter a value to apply on the operator.

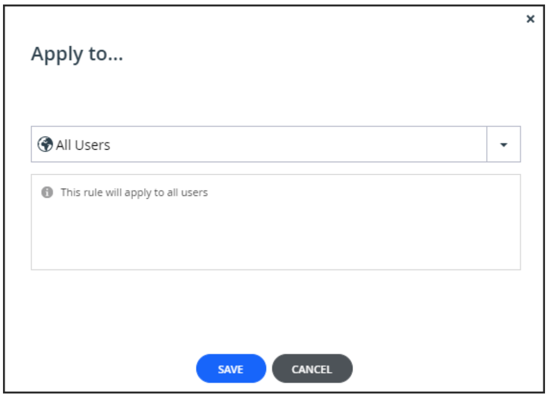
d In the **Then apply** column select a plan to apply if a user satisfies the condition.

e In the **Apply to** column select to whom the policy applies.

i Unless the user is **All Users**, select the type of user or group.

ii In the **Quick Search** field, enter a string that is displayed anywhere within the name of the user.
A list of users and groups matching the search string is displayed.

iii Select the user or group and click **SAVE**.



All Users

This rule will apply to all users

f In the **Action** column select **Allow** or **Deny** to allow or deny the specified condition.

4 To delete a condition, click 🗑 in its row.

5 Click **SAVE**.

VIRUS PROTECTION

When antivirus scanning is implemented, files are scanned for malware automatically and transparently, before they are downloaded from the IBM COS FA Portal. Background scanning checks for files that were not previously scanned, for example, when the antivirus was disabled or not running on a server. Background scanning scans the following:

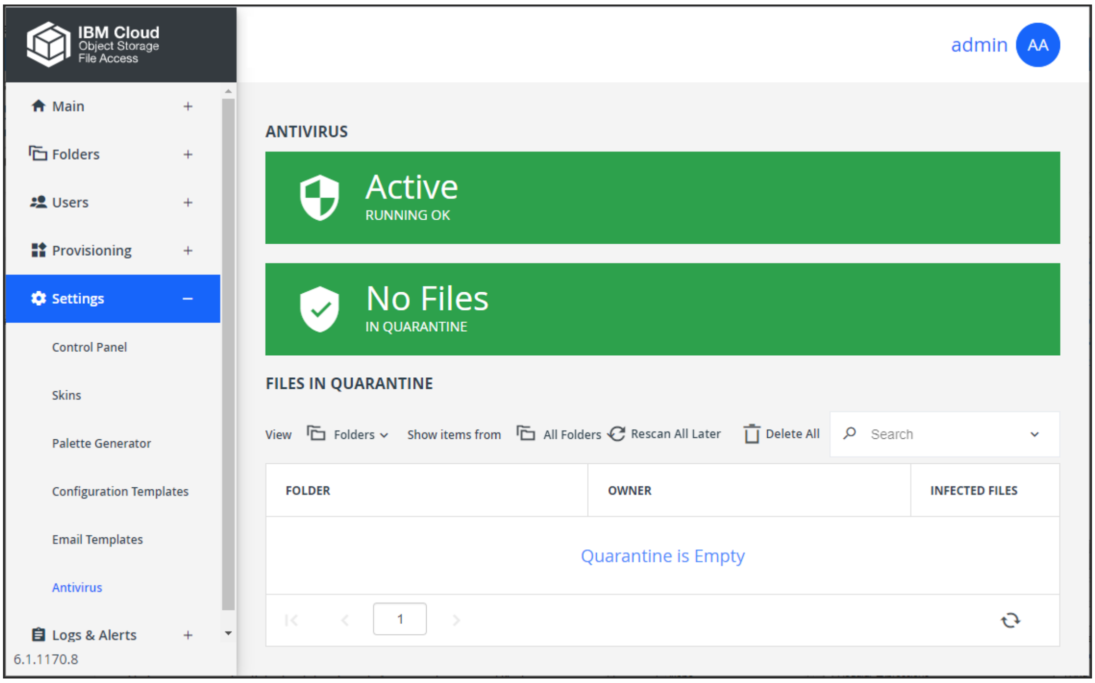
- Files that were not previously scanned.
- Cloud drive folders.

If an infected file is found, the user who owns the file receives an email notification indicating that malware was blocked and specifying the file name. A copy of the infected file is quarantined so that the administrator can determine if any action is necessary.

Virtual IBM COS FA Portal administrators can view files that are quarantined by the antivirus servers, the Cloud Drive location and the user who owns the files.

To manage quarantined files:

1 Select **Settings > Antivirus** in the navigation pane.
The **ANTIVIRUS** page is displayed.



FOLDER	OWNER	INFECTED FILES
Quarantine is Empty		

If no quarantined files were scanned, a block is displayed specifying that no files are in quarantine. Any folder that includes one or more files with malware is listed with the number of quarantined files.
You can also view change the few to displays the quarantined files:

- Choose either **Folders** or **Files** from the **View** drop-down options.
In the **Folders** view, you can select what type of folder to inspect, **All Folders or Cloud Folders**. The number of infected files displayed is for all the folders. In the **Files** view the list of infected files displayed is from cloud folders. In in the **Files** view you can search the list by file name.

2 Click on an owner to see details of the user who owns the infected file.

3 In the **Folders** view, click on a link in the **INFECTED FILES** column to display the details of the infected files.
Clicking on the file link displays the **Quarantined Files** window, with the infected files in that folder.
The infected files in the folder are displayed as well as the owner of the folder.

You can remove all the files from the list by clicking **Rescan All Later** in the **ANTIVIRUS** page or **Quarantined Files** window or select a quarantined file from the list in the **Quarantined Files** window and click **Rescan Later** to remove that file from the list. These files will be rescanned and access blocked the next time an external user attempts to view or download them, as long as DLP scanning is defined.

You can delete all the files from the list by clicking **Delete All** in the **ANTIVIRUS** page or **Quarantined Files** window or select a quarantined file from the list in the **Quarantined Files** window and click **Delete** to delete that file.

CHAPTER 10. MANAGING DEVICES

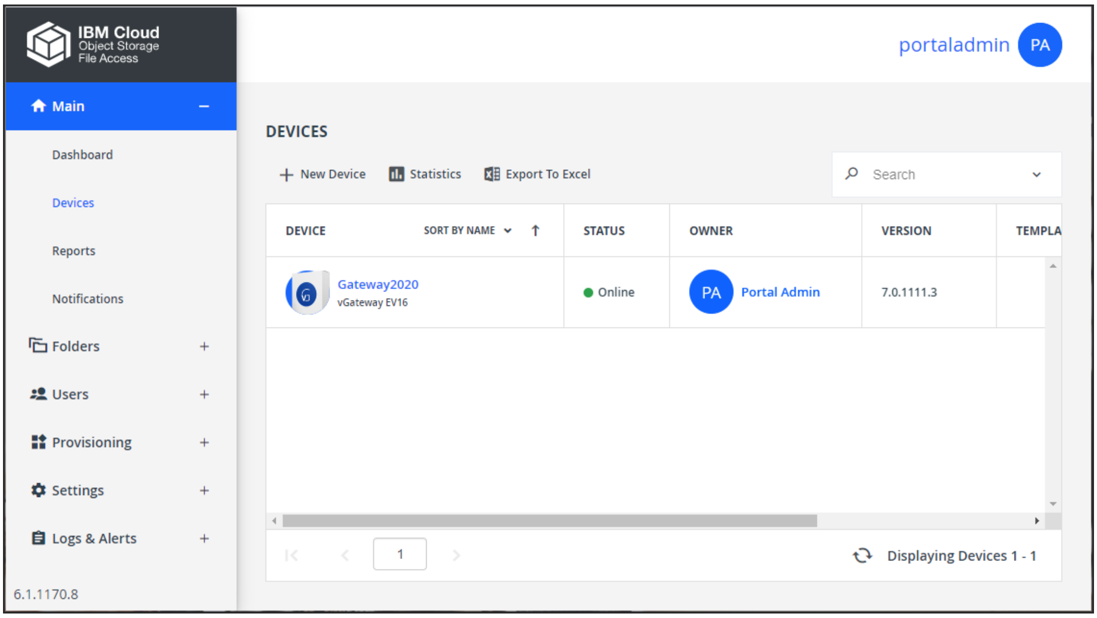
A *device* refers to an IBM COS FA Gateway connected to the IBM COS FA Portal. Devices are automatically added to the IBM COS FA Portal, when their owners connect the device to the IBM COS FA Portal.

In this chapter

VIEWING ALL DEVICES

To view all devices connected to the virtual IBM COS FA Portal:

- Select **Main > Devices** in the navigation pane.
  The **DEVICES** page opens, displaying all the devices connected to the IBM COS FA Portal.



DEVICE	STATUS	OWNER	VERSION	TEMPLA
Gateway2020 vGateway EV16	● Online	PA Portal Admin	7.0.1111.3	

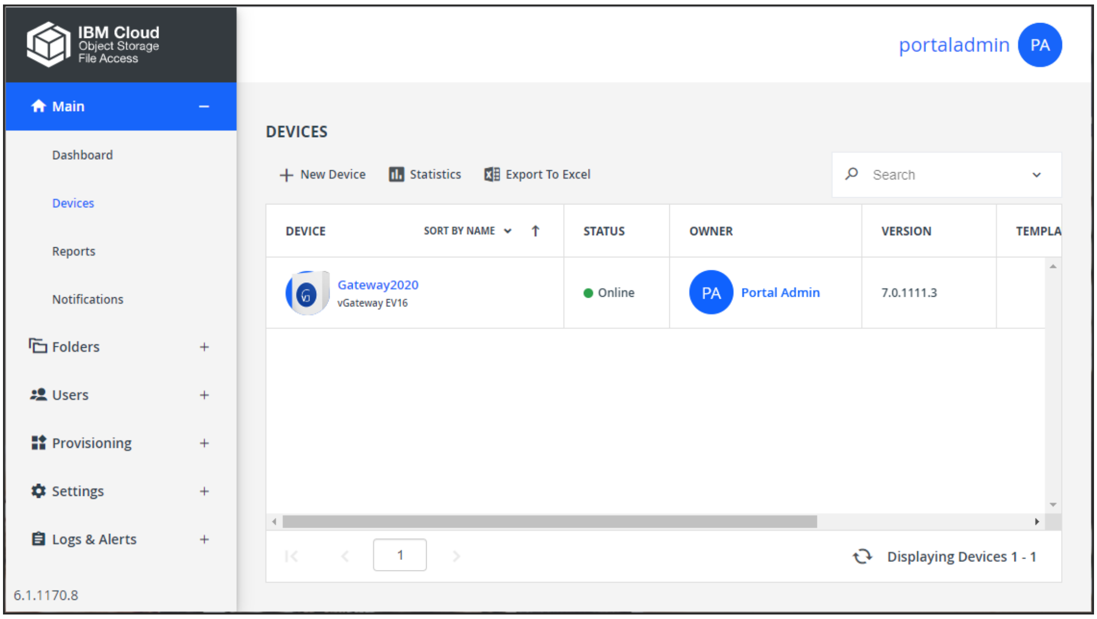
The page includes the following columns:

Column	Display
DEVICE	The device's name. To edit the device, click the device name. The type of device is displayed under the name.
STATUS	The device's connection status: **Online** or **Offline**.
OWNER	The user account name of the device's owner. To edit the user account, click the user account name.
VERSION	The firmware version currently installed on the device.
TEMPLATE	The template assigned to the device.

VIEWING INDIVIDUAL DEVICE DETAILS

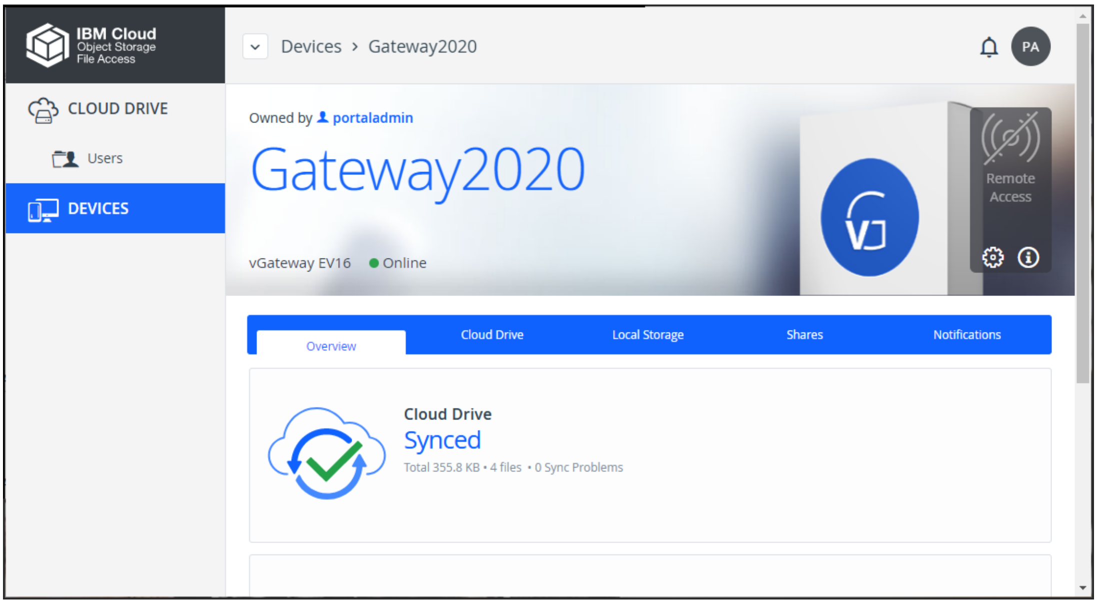
To view individual device details:

1 Select **Main > Devices** in the navigation pane.
The **DEVICES** page opens, displaying all the devices connected to IBM COS FA Portal.



DEVICE	STATUS	OWNER	VERSION	TEMPLA
Gateway2020 vGateway EV16	● Online	PA Portal Admin	7.0.1111.3	

2 Click the device name.
The device details are displayed in a new browser window. The details are different whether the device is online or not.



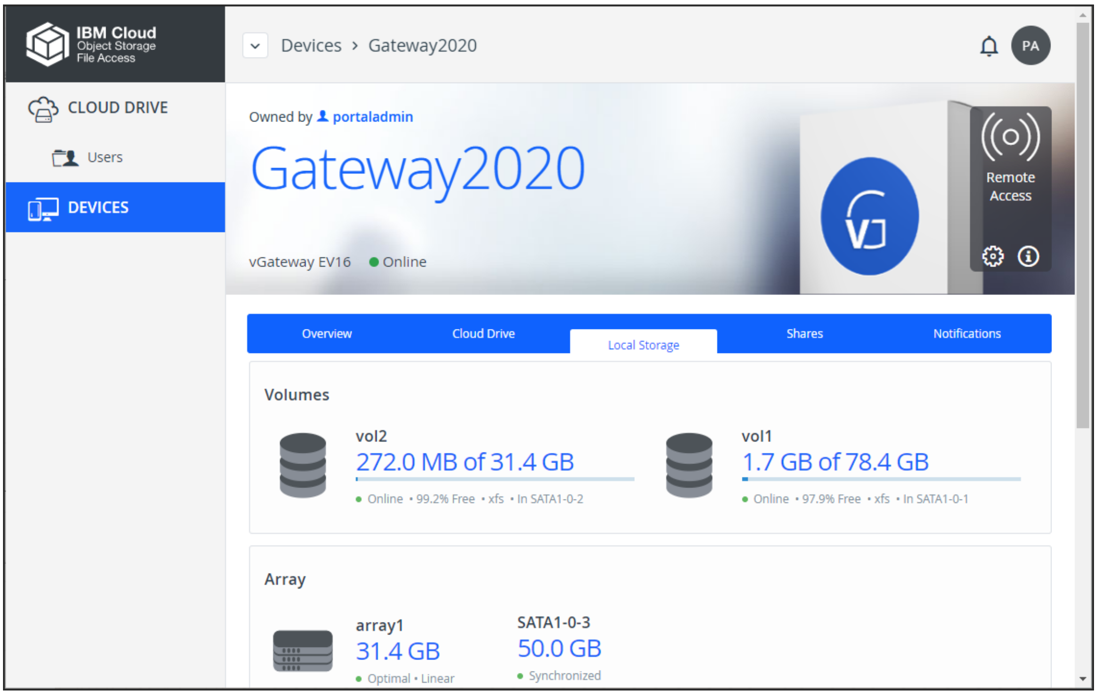
Cloud Drive
Synced
Total 355.8 KB • 4 files • 0 Sync Problems

From this window:

- Click **Remote Access** to access the device over the Internet for administration or to access files. The IBM COS FA Portal administrator must enable **Remote Access**.
- Click the ⚙ icon to edit the device settings, rename or delete the device and add text to describe a device.
- Click the ⓘ icon to view information about the device: The IP address, software version, serial number, MAC address, firmware version and physical location. For an IBM COS FA Gateway, the license is also displayed and if required and enabled, can be changed.

The device details are divided over a number of tabs.

- The IBM COS FA Gateway details include the following tabs:
  Overview – Details of the device, including an overview of the following:
    The cloud drive status
    Local storage
  Cloud Drive – File sync details. You can also sync a folder, as described in Syncing Content to the IBM COS FA Portal and view IBM COS FA Gateway statistics, by clicking **Statistics**.
  Local Storage – Details about the IBM COS FA Gateway volumes and arrays storage utilization.



Notifications – A list of notifications for this device.
The color of the exclamation mark to the left of each notification indicates the severity.

Blue – Information
Orange – Warning

MANAGING INDIVIDUAL DEVICE DETAILS

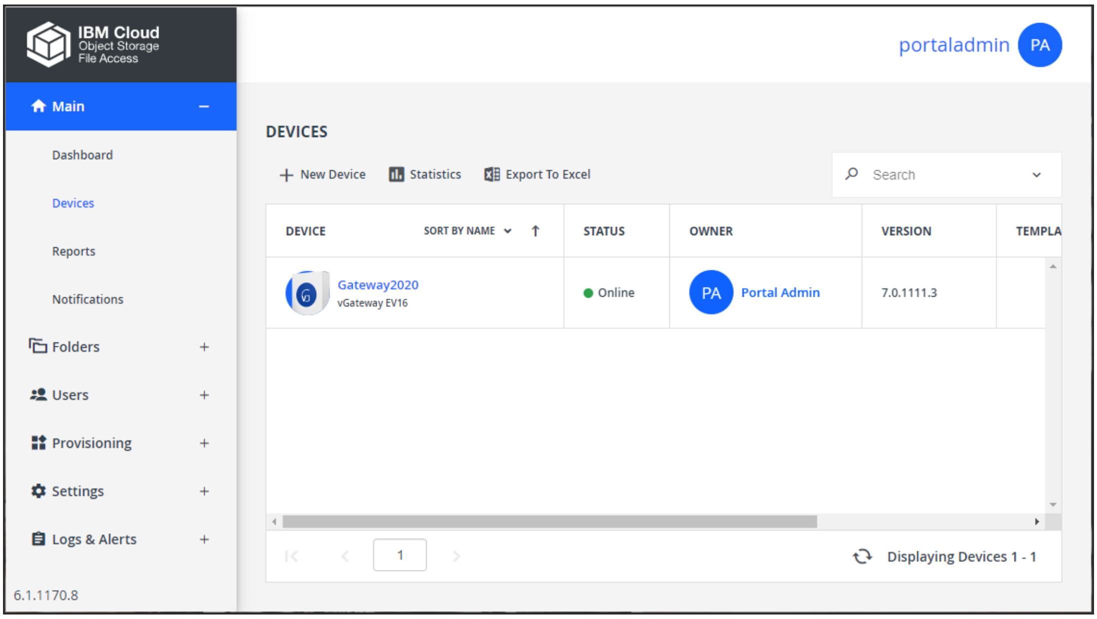
You can manage the following details for a device:

- The device name.
- A description of the device. You can use this to add comments about the device.
- Advanced settings, including:
  - The MAC address
  - The software version.
  - The configuration template, either the default template or another templates defined in the IBM COS FA Portal.

In addition, administrators can restart devices and delete devices from the IBM COS FA Portal, for example inactive devices that are using a license can be deleted to free up a license.

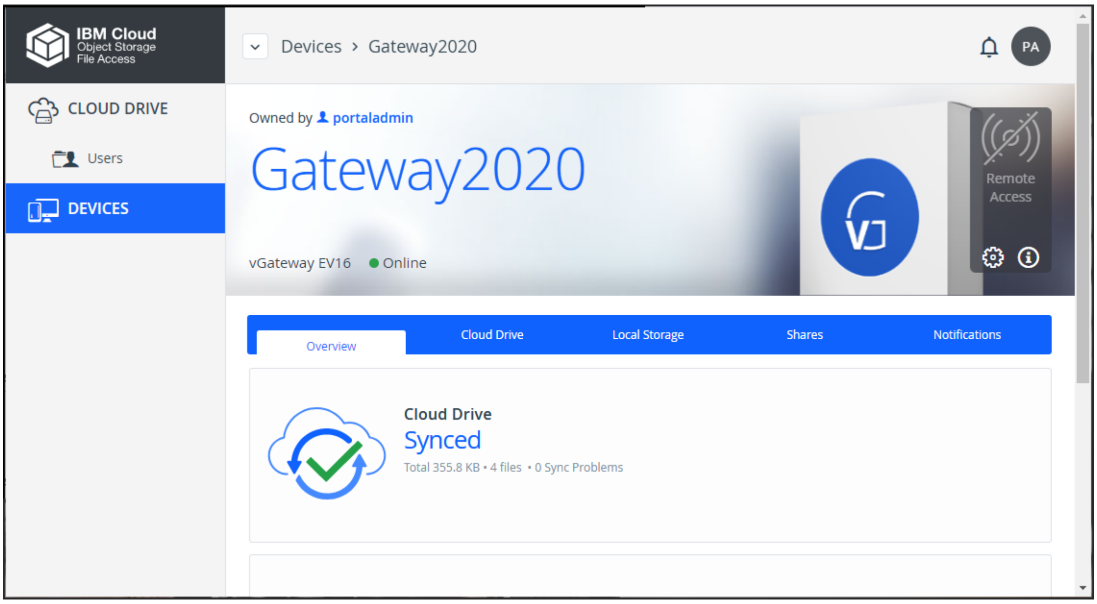
To manage individual device details:

1 Select **Main > Devices** in the navigation pane.
The **DEVICES** page opens, displaying all the devices connected to IBM COS FA Portal.



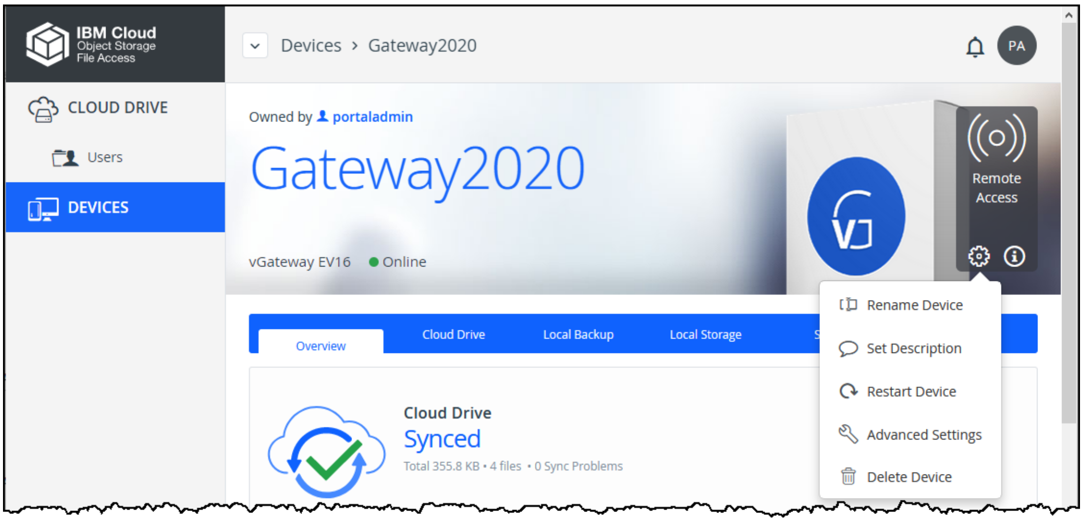
DEVICE	STATUS	OWNER	VERSION	TEMPLA
Gateway2020 vGateway EV16	Online	Portal Admin	7.0.1111.3	

2 Click the device name.
The device details are displayed in a new browser window.



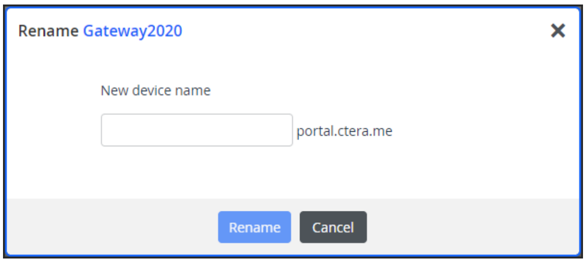
The details are different for each type of device and whether the device is currently connected to IBM COS FA Portal.

3 Click the ⚙ icon and select the option required for the device.



Note: The list of available options is dependent on the device. For example, mobile devices do not have the devices do not have the **Advanced Settings** option and only connected devices have a **Restart Device** option.

When **Rename Device** is selected, the **Rename** window is displayed.


Rename Gateway2020

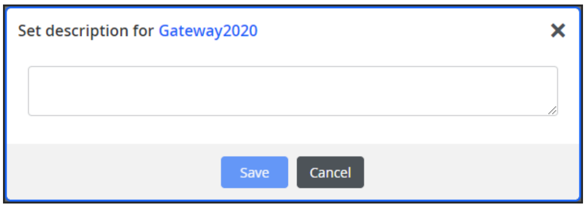
New device name

portal.ctera.me

Enter the new device name and click **Rename**. The device is offline for a few seconds as the name change is applied.

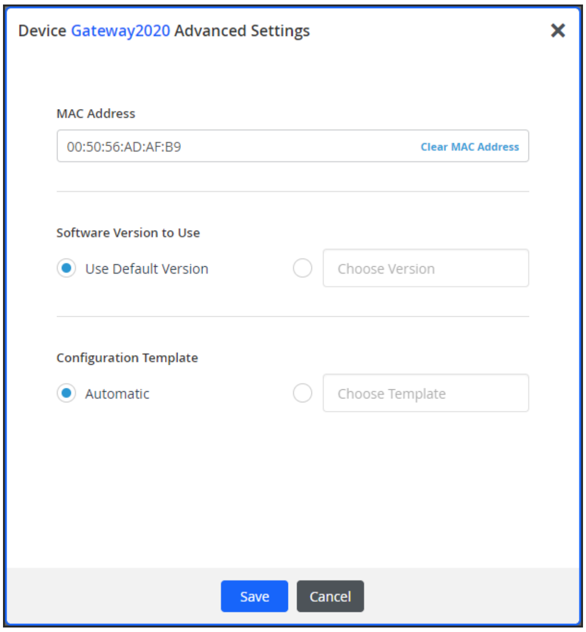
When **Restart Device** is selected, the **Restart Device** window is displayed prompting the restart. Click **Restart** to restart the device.

When **Set Description** is selected, the **Set Description** window is displayed.


Set description for Gateway2020

Enter any information you want to describe the device and click **Save**.

When **Advanced Settings** is selected, the **Device Advanced Settings** window is displayed.



Device Gateway2020 Advanced Settings

MAC Address

00:50:56:AD:AF:B9

Software Version to Use

● Use Default Version ○ Choose Version

Configuration Template

● Automatic ○ Choose Template

Enter the configuration you want for the device and click **Save**.

To delete a device, see Deleting Devices.

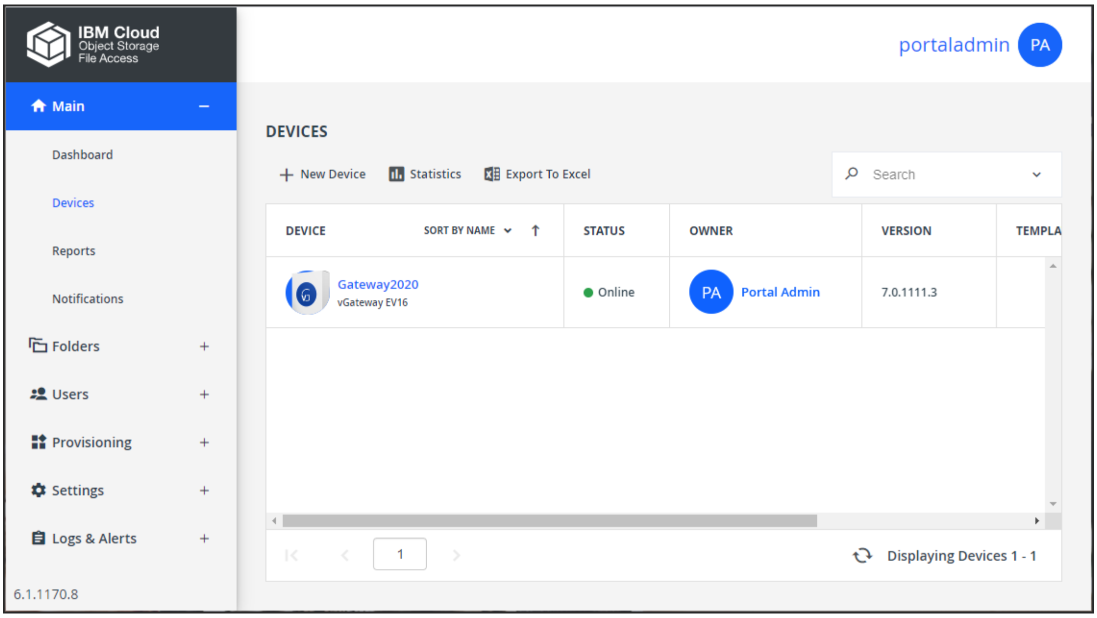
SYNCING CONTENT TO THE IBM COS FA PORTAL

When an IBM COS FA Gateway is connected to the IBM COS FA Portal, files are synced between the device and the IBM COS FA Portal. You sync content with the IBM COS FA Portal from the device and configure what content should be synced. You can also throttle the sync data from the device, for example, to free up bandwidth from other tasks at certain times of the day.

You can also sync content from the IBM COS FA Portal.

To sync content from the IBM COS FA Portal:

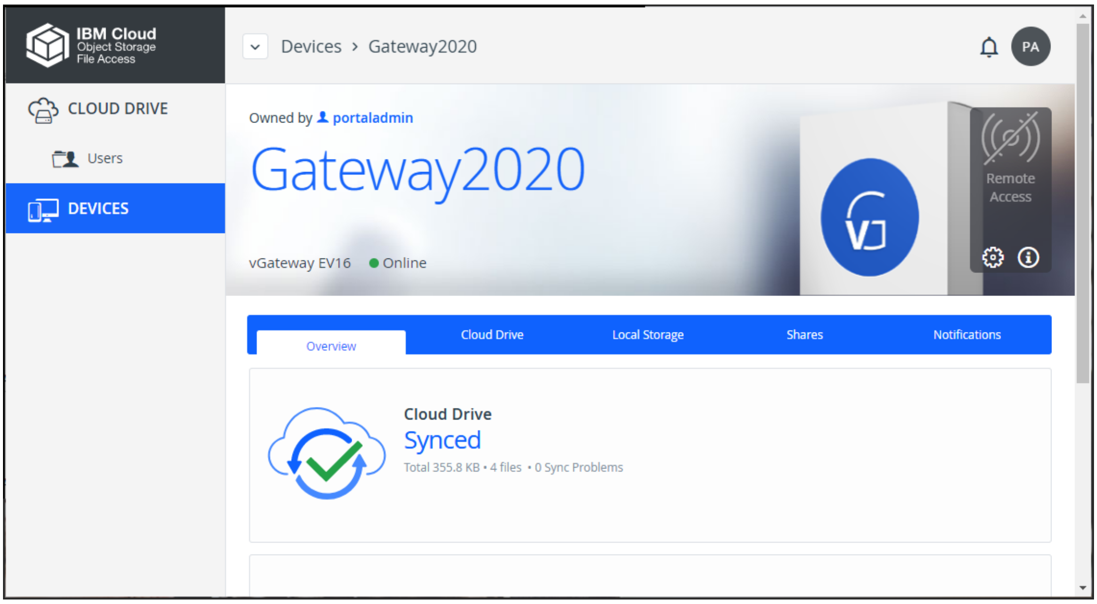
1 Select **Main > Devices** in the navigation pane.
The **DEVICES** page opens, displaying all the devices connected to IBM COS FA Portal.



DEVICE	STATUS	OWNER	VERSION	TEMPLA
Gateway2020 vGateway EV16	Online	PA Portal Admin	7.0.1111.3	

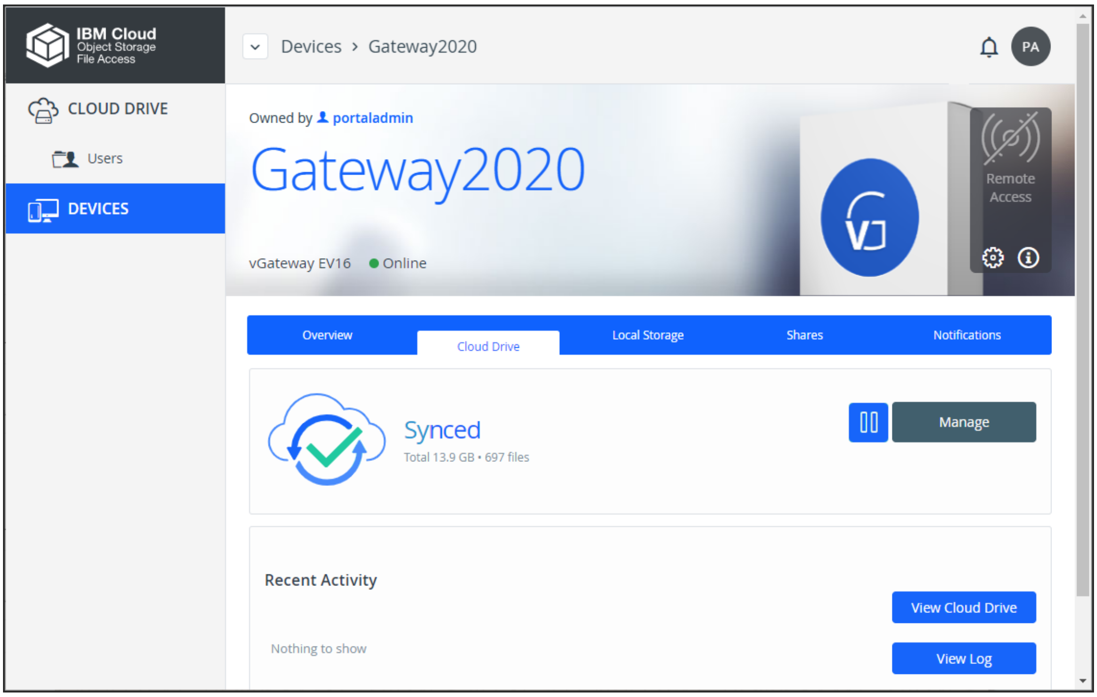
2 Click the device name.

The device details are displayed in a new browser window.



Note: In this example you can see that the cloud drive is fully synced with the device.

3 Click the **Cloud Drive** tab.
The cloud drive details for the device are displayed.

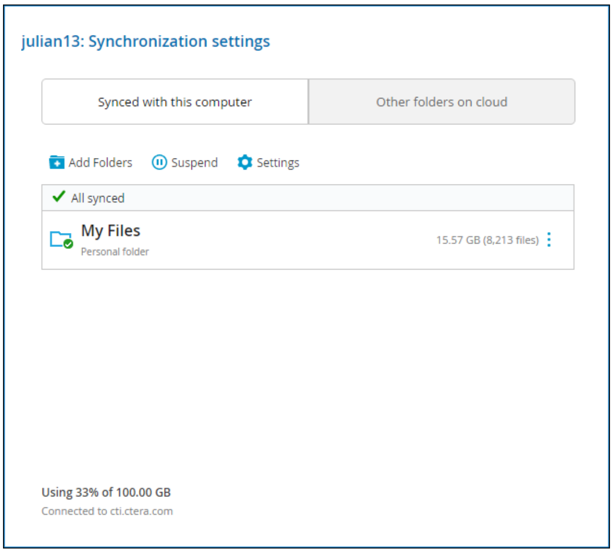


4 Click ▷ to sync a folder.

To suspend a sync that is currently running, click ⏸.

To resume a sync that is suspended running, click ▷.

5 Click Manage to configure the folders to be synced.
The folders that are synced are displayed.



julian13: Synchronization settings

Synced with this computer	Other folders on cloud

Add Folders · Suspend · Settings

✓ All synced

My Files
Personal folder — 15.57 GB (8,213 files)

Using 33% of 100.00 GB
Connected to cti.ctera.com

You can view device statistics by clicking Statistics.

You can view the cloud drive by clicking View Cloud Drive.

You can view a log of all file activity on the cloud drive by clicking View Log.

MANAGING DEVICES FROM THE END USER IBM COS FA PORTAL

An administrator can also remotely manage devices from the end user IBM COS FA Portal. The **DEVICES** option displays all devices connected to the IBM COS FA Portal that you are managing.

For each device a read only administrator can do the following:

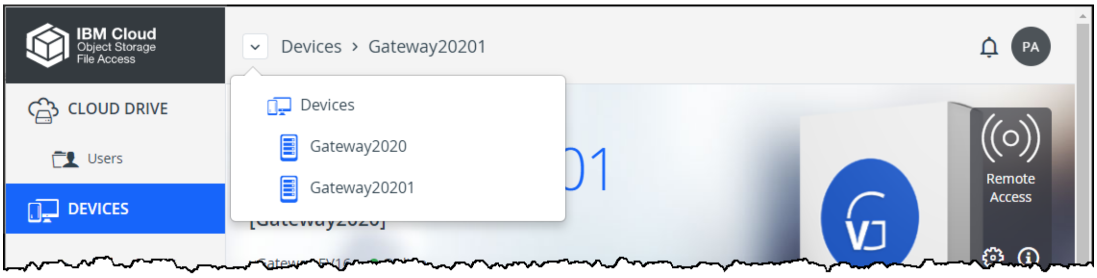
- Rename the device.
- Edit device settings, such as the configuration template used and clear the MAC address.
- Delete a device.

In addition, a read/write administrator can also edit device settings, such as the configuration template to apply to the device.

To edit device settings:

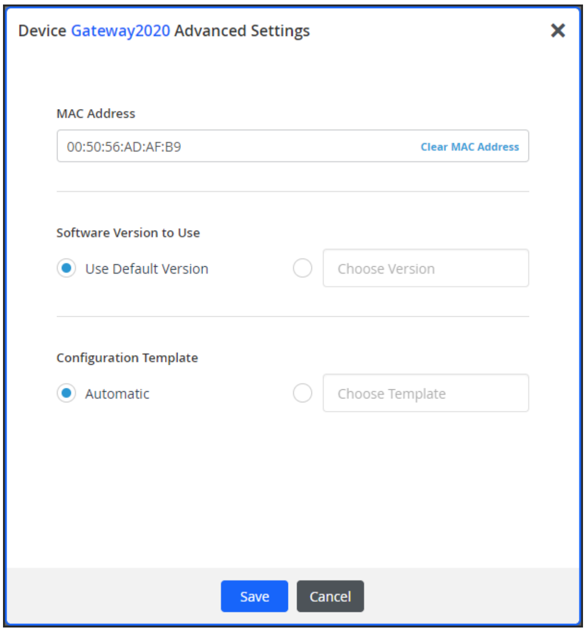
1 Click the **DEVICES** option in the navigation pane.
This page displays all of the administrator's devices connected to the IBM COS FA Portal.

2 Click the down arrow in the heading to list all the devices for the IBM COS FA Portal.



3 Select a device from the list to display device details.

4 Click the ⚙ icon and select **Advanced Settings**.
The device configuration is displayed.



Device Gateway2020 Advanced Settings ✕

MAC Address

00:50:56:AD:AF:B9 Clear MAC Address

Software Version to Use

● Use Default Version ○ Choose Version

Configuration Template

● Automatic ○ Choose Template

Save Cancel

Administrators can change the following:

- The MAC address
- The software version.
- The configuration template, either the default template or to one of the other templates defined in the IBM COS FA Portal.

To remotely restart an IBM COS FA Gateway **(read/write administrator):**

1 Click the **DEVICES** option in the navigation pane.
This page displays all of the devices connected to the IBM COS FA Portal.

2 Click the ⋮ icon to the right of the IBM COS FA Gateway you want to restart and select **Restart Device**.
The page changes to the page with the device details and a confirmation message is displayed.

3 Click **Restart** to restart the device.

The device restarts.

EXPORTING A LIST OF DEVICES TO EXCEL

You can export the list of devices and their details to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export a list of devices to Microsoft Excel:

1. Select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices connected to the IBM COS FA Portal.
2. Click **Export to Excel**.
   The list of devices is exported to your computer. The report includes the type of device, version and any description set for the device.

CHANGING A IBM COS FA GATEWAY LICENSE

An IBM COS FA Gateway receives a license from IBM COS FA Portal. You can change the license level to another license level.

For details about activating this feature, contact IBM.

DELETING DEVICES

To delete a device:

1. Select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices connected to the IBM COS FA Portal.
2. Select the row of the device to delete and click **Delete**.
   A confirmation window is displayed.
3. Click **DELETE DEVICE**.

The device is disconnected and deleted from the IBM COS FA Portal.

CHAPTER 11. MANAGING DEVICE CONFIGURATION TEMPLATES

IBM COS FA Portal enables you to centrally manage device settings, by assigning devices to *device configuration templates*: When a device is assigned to a template, it inherits the following settings from that template:

- Installed software and firmware versions
- Automatic firmware updates

In this chapter

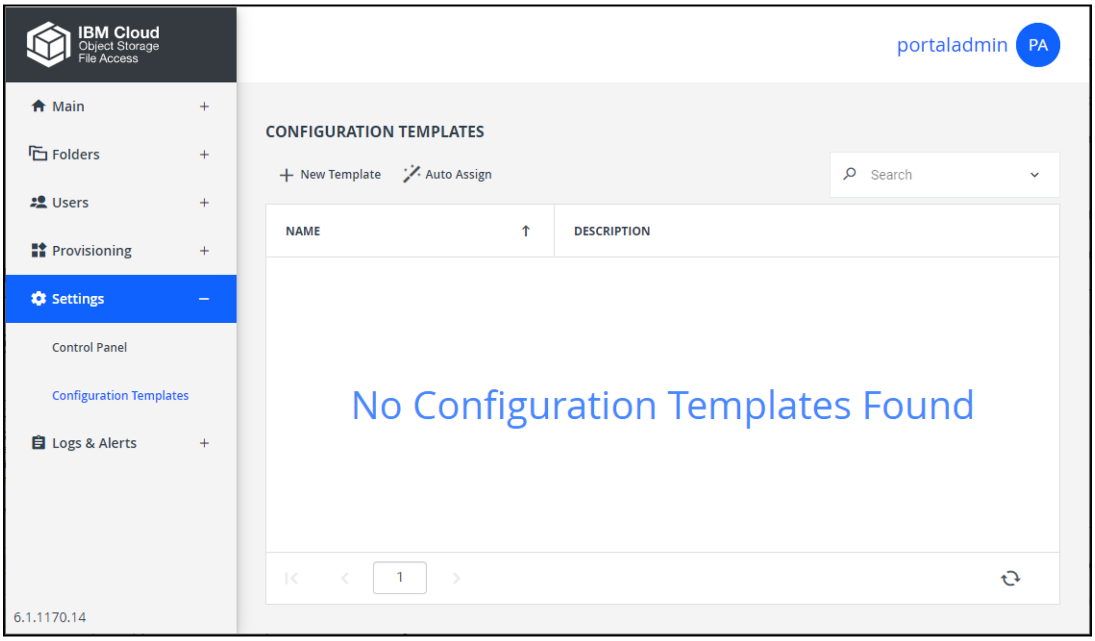
Devices can be assigned to templates in the following ways:

- Automatic template assignment.
  Devices can be assigned to templates based on the *automatic template assignment policy*, which specifies a set of criteria for assigning a template such as device type and operating system, as well as an optional default template that is assigned when none of the criteria are met.
  See Configuring the Automatic Template Assignment Policy.
- Manually, by editing the device settings.
  See Managing Devices From the End User IBM COS FA Portal.

VIEWING DEVICE CONFIGURATION TEMPLATES

To view all device configuration templates in the IBM COS FA Portal:

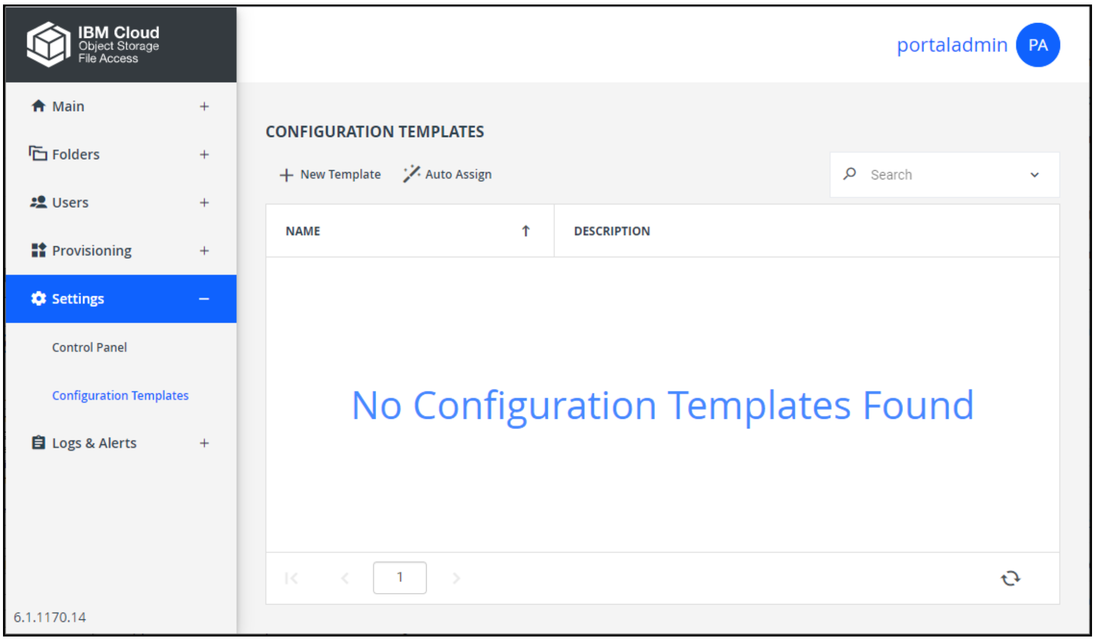
- Select **Settings > Configuration Template** in the navigation pane.
  The **CONFIGURATION TEMPLATES** page is displayed.



ADDING AND EDITING DEVICE CONFIGURATION TEMPLATES

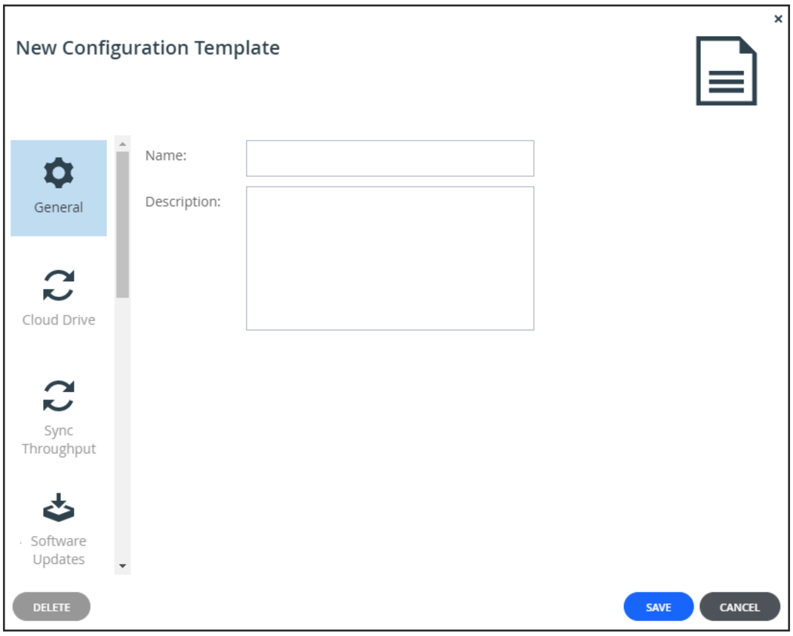
To add or edit a device configuration template:

1 Select **Settings > Configuration Template** in the navigation pane.
The **CONFIGURATION TEMPLATES** page is displayed.



2 Either,

- Add a new template, click **New Template**.
The **New Configuration Template** window is displayed.



Or,

- Edit an existing configuration template, click the template's name.

The configuration template window is displayed with the configuration template name as the window title.

3 Enter the general details for the template:
Name – A unique name for the template. Spaces and special characters cannot be used in the name.
Description – A description of the template.

4 Access the following options to complete configuring the template:
Cloud Drive – Which IBM COS FA Portal cloud folders are be synchronized with the device, and with which folder each cloud drive folder is synced.
Sync Throughput – Restrict bandwidth for specific hours in a day or on specific days.
Software Updates – A firmware image for all relevant devices.
Update schedule – Configure how and when to install updates.

5 Click **SAVE**.

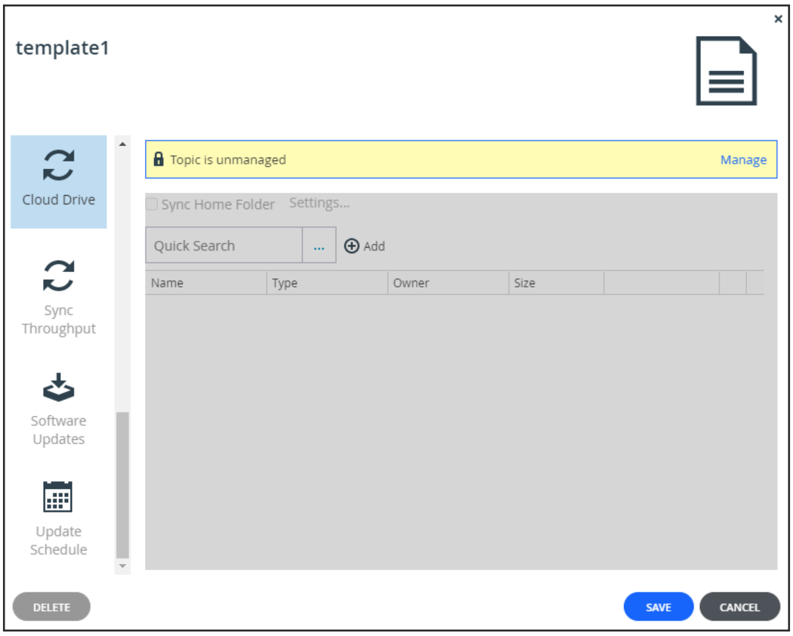
The configuration is saved and, after a few minutes, applied to devices to which the template is assigned.

Cloud Drive

Specify which IBM COS FA Portal cloud folders are be synchronized with the device, and with which folder each cloud drive folder is synced.

To manage cloud drive sync in the device template:

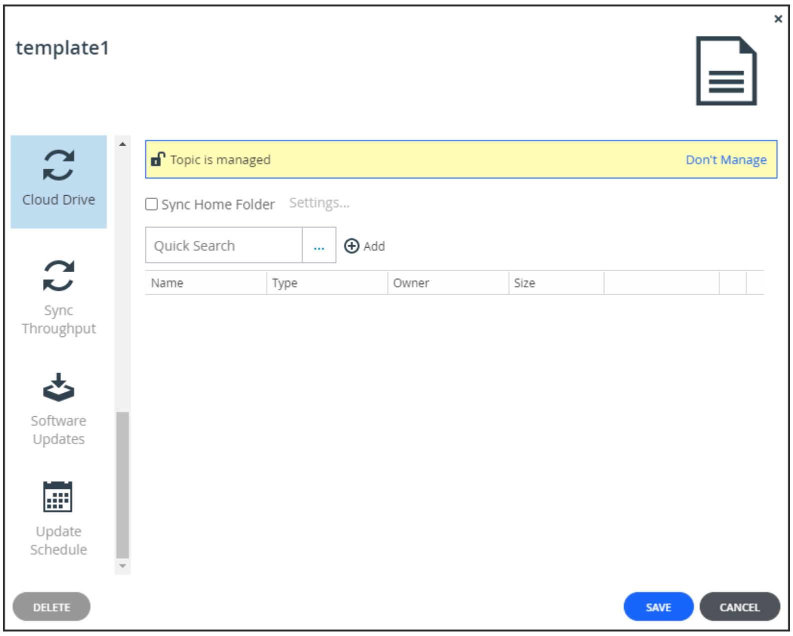
1 In the configuration template window, select the **Cloud Drive** option**.**



template1

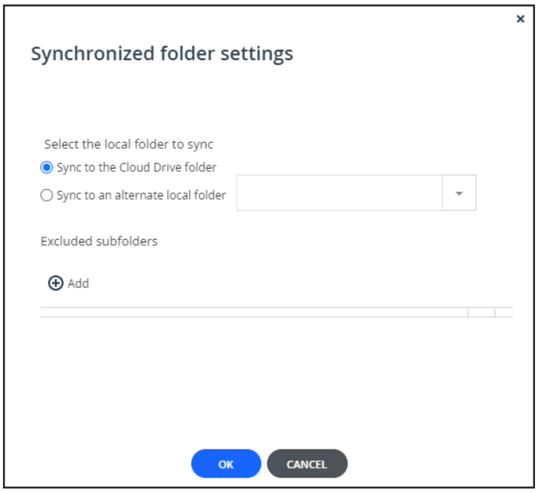
Topic is unmanaged

2 Click **Manage**, if the cloud drive is unmanaged. The device template will manage the cloud drive folders sync for devices using this template.



If you do not want managed cloud drive folder syncs, click **Don't Manage**.

3 To sync the home folder, select **Sync Home Folder** and click **Settings**.


Synchronized folder settings
Select the local folder to sync
● Sync to the Cloud Drive folder
○ Sync to an alternate local folder
Excluded subfolders
Add
OK
CANCEL

4 Set which local folder on the device the cloud drive home folder should be synced:

- Sync the folder to cloud drive folder on the IBM COS FA Gateway.
- Sync the folder to an alternative local folder on the IBM COS FA Gateway, using one of the environment variables.

5 Exclude sub-folders: Click **Add** in the **Excluded sub-folders** section.
A row is added to the table.

6 Click in the row and enter the name of a subfolder to exclude from syncing.

7 Click **OK**.

8 To add more cloud drive folders to sync with the device:

a Click in the **Quick Search** field and type a search string to search for the name of a cloud drive folder you want to add.
All the folders that include the search string in their names are displayed.

b Select the folder you want to add.

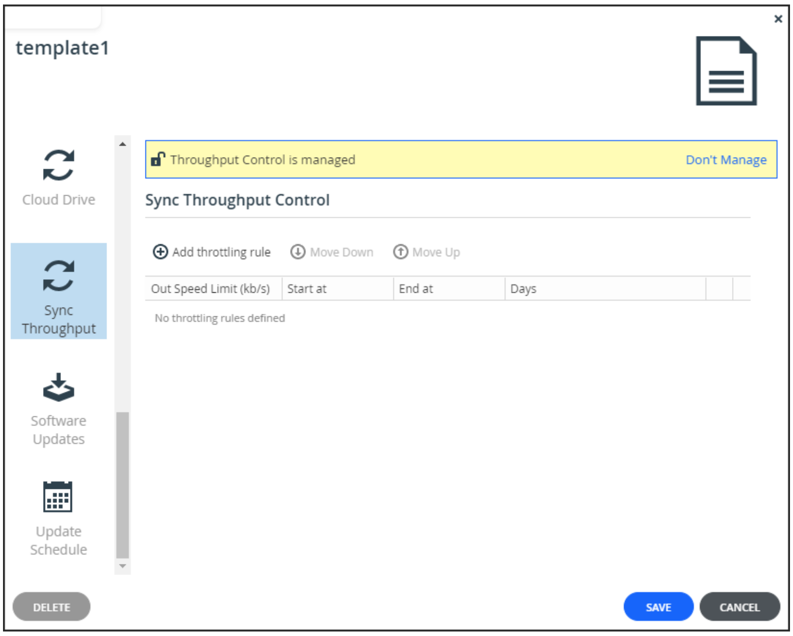
c Click **Add**.
The folder is added to the list.

d To set which folder on the device the folder should sync with, click the **Settings** button in the row and set the folder as described in steps 3 to 7.

Sync Throughput

To control the cloud sync upload speed:

1 In the configuration template window, select the **Sync Throughput** option **and** click **Manage**, if the sync throughput is unmanaged. The device template will manage the cloud drive sync throughput for devices using this template.



Throughput Control is managed

Sync Throughput Control

Out Speed Limit (kb/s)	Start at	End at	Days

No throttling rules defined

If you do not want managed cloud drive sync throughput, click **Don't Manage**.

2 Set the controls for sync throughput: Click **Add throttling rule**.

Note: When no throttling rules are defined, there is no speed restriction for uploading files to the Cloud Drive for syncing.

3 Define the following for the throttling rule:

Out Speed Limit (kb/s) – The maximum speed to use for cloud drive sync upload in Kbits per second.
Start at – Specify the time when the bandwidth limit used for cloud drive sync upload starts.
End at – Specify the time when the bandwidth limit used for cloud drive sync upload ends. When the end time is before the start time, the end time is the next day.
Days – Specify that the bandwidth used for cloud drive sync upload should be restricted every day (the default) or only on specified days.

Note: A maximum of 50 rules can be defined.
When the start and end times for more than one rule overlap, the order of the rules in the list determines how they are implemented with the rule ate the top of the list implemented first. Use **Move Down** and **Move Up** to change the order the rules are listed.

4 To remove a rule, select the rule row and click 🗑.
The rule is removed.

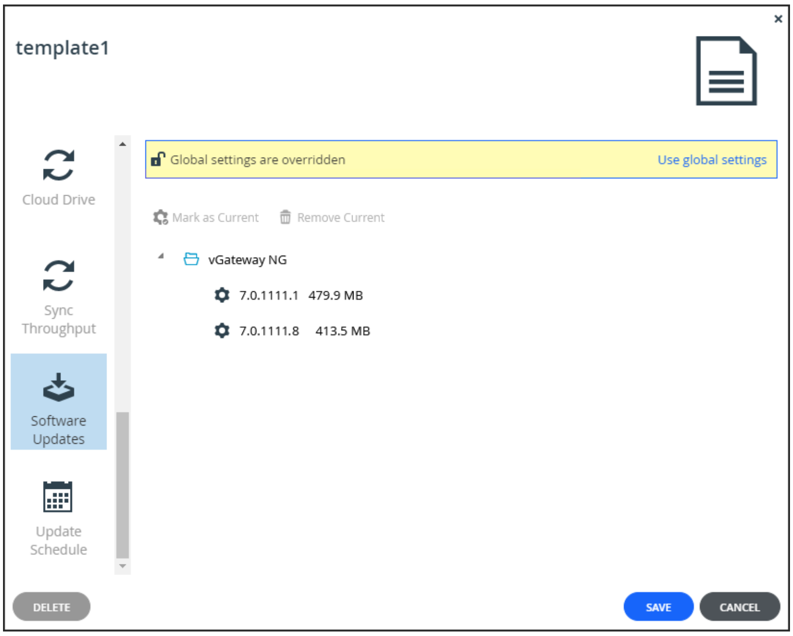
Software Updates

When you mark a firmware image as the current firmware image, all devices that are of the relevant device platform, assigned to this template, and set to automatically download firmware images will download this firmware image.

There can only be one current firmware image per device platform.

To mark a firmware image as the current firmware image:

1 In the configuration template window, select the **Software Updates** option and click **Override** if you want to override global settings.



vGateway NG

7.0.1111.1 479.9 MB

7.0.1111.8 413.5 MB

When global settings are overridden, you can revert to global settings, by clicking **Use global settings**.

2 Select the desired firmware image's row.

3 Click **Mark as Current**.

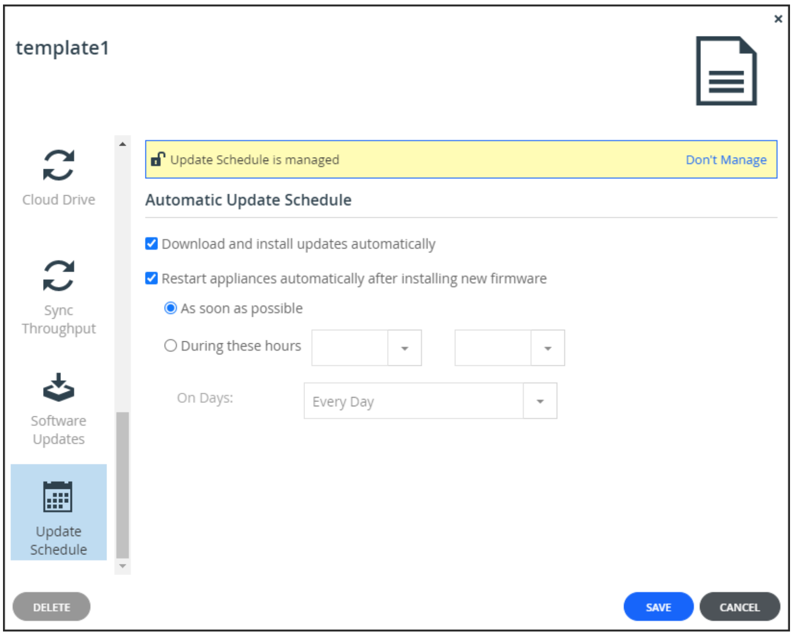
The selected firmware image becomes the current firmware image and is marked with ⚙.

Update schedule

You can configure your devices to automatically download and install firmware updates.

To configure automatic firmware updates:

1 In the configuration template window, select the **Update Schedule** option and click **Manage**, if the update schedule is unmanaged. The device template will manage the update schedule for devices using this template.



template1

Update Schedule is managed

Automatic Update Schedule

☑ Download and install updates automatically

☑ Restart appliances automatically after installing new firmware

● As soon as possible

○ During these hours

On Days: Every Day

If you do not want a managed update schedule, click **Don't Manage**.

2 Configure the firmware update schedule:

Download and install updates automatically – The IBM COS FA Portal downloads and installs firmware updates automatically. If you do not select this option, device owners must perform firmware updates manually.

Restart automatically after installing new firmware – The IBM COS FA Portal automatically reboots after installing new firmware updates:

As soon as possible – To reboot as soon as possible after a firmware update. In this case, the IBM COS FA Portal reboots as soon as it is recommended to do so. For example, the automatic reboot might be deferred, if the IBM COS FA Portal is undergoing system maintenance that should not be interrupted.

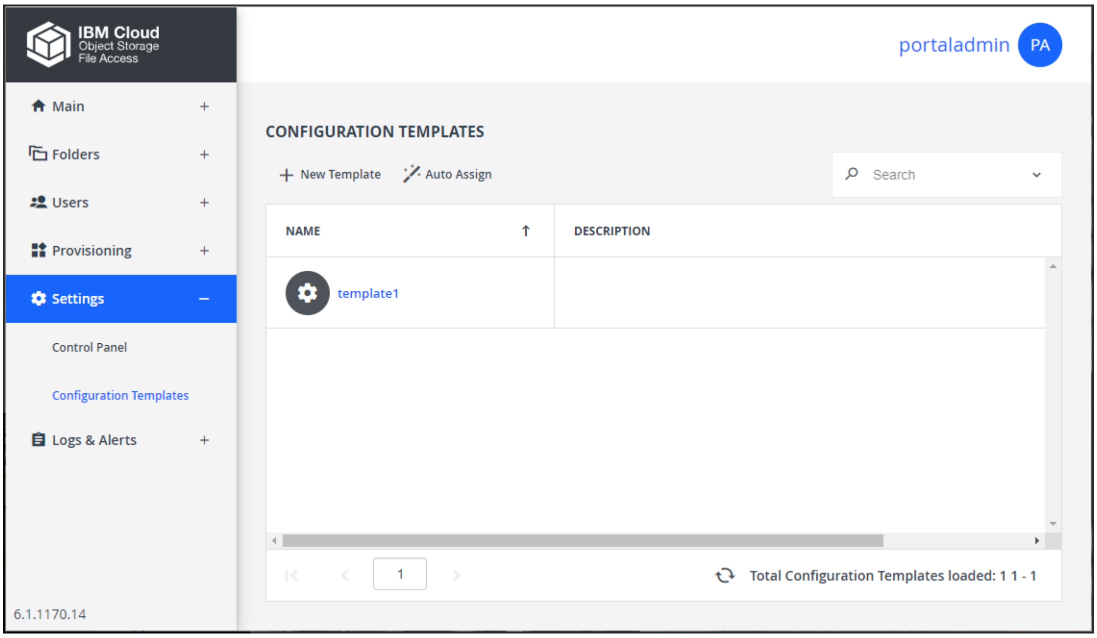
During these hours – To reboot only during specific hours.

On Days – To reboot on automatically on specified days.

CONFIGURING THE AUTOMATIC TEMPLATE ASSIGNMENT POLICY

To configure the automatic template assignment policy:

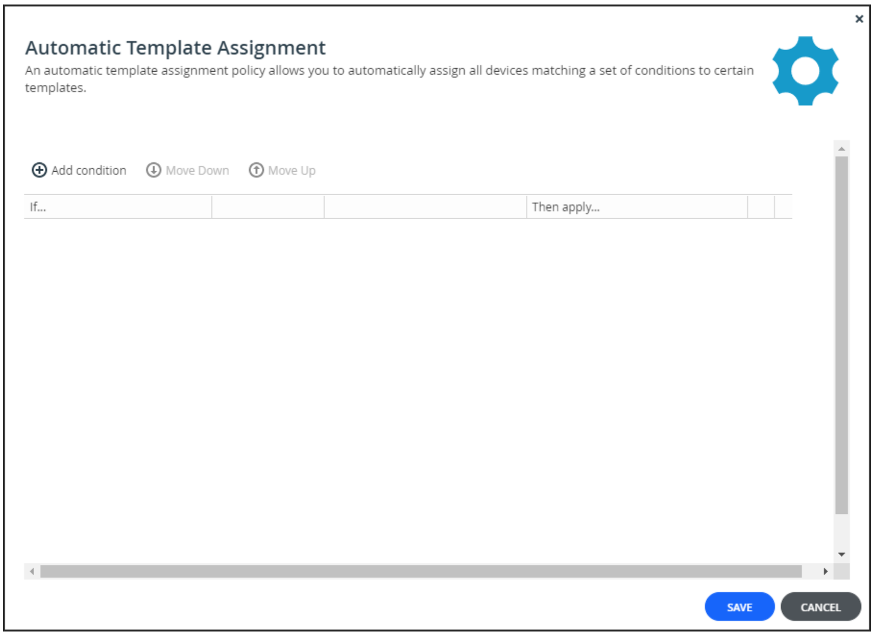
1 Select **Settings > Configuration Template** in the navigation pane.
The **CONFIGURATION TEMPLATES** page is displayed.



NAME	DESCRIPTION
template1	

Total Configuration Templates loaded: 1 1 - 1

2 Click **Auto Assign**.
The Automatic Template Assignment dialog box is displayed.



An automatic template assignment policy allows you to automatically assign all devices matching a set of conditions to certain templates.

3 Define the conditions for a device to be assigned to a template, by doing the following for each condition:

- a Click **Add condition**.
  A row is displayed in the table.
- b Click the cell in the first column and select the condition parameter from the drop-down list.
- c Click in the second column and select the condition operator from the drop-down list.
- d Click in the third column, and complete the condition, by selecting values or entering the free-text value.
  Multiple values must be separated by commas.
  For example, if you select **Owner Groups** as the condition parameter in the first column, **is one of** as the condition operator in the second column, and enter `groupA, groupB` in the third column, then the condition is met when the device owner's user account belongs to user group *groupA* or user group *groupB*.
- e Click in the **Then apply** column, and select the template that is assigned when the condition is met.

4 To delete a condition, click 🗑 in its row.

5 To specify that the policy should include a default device configuration template:

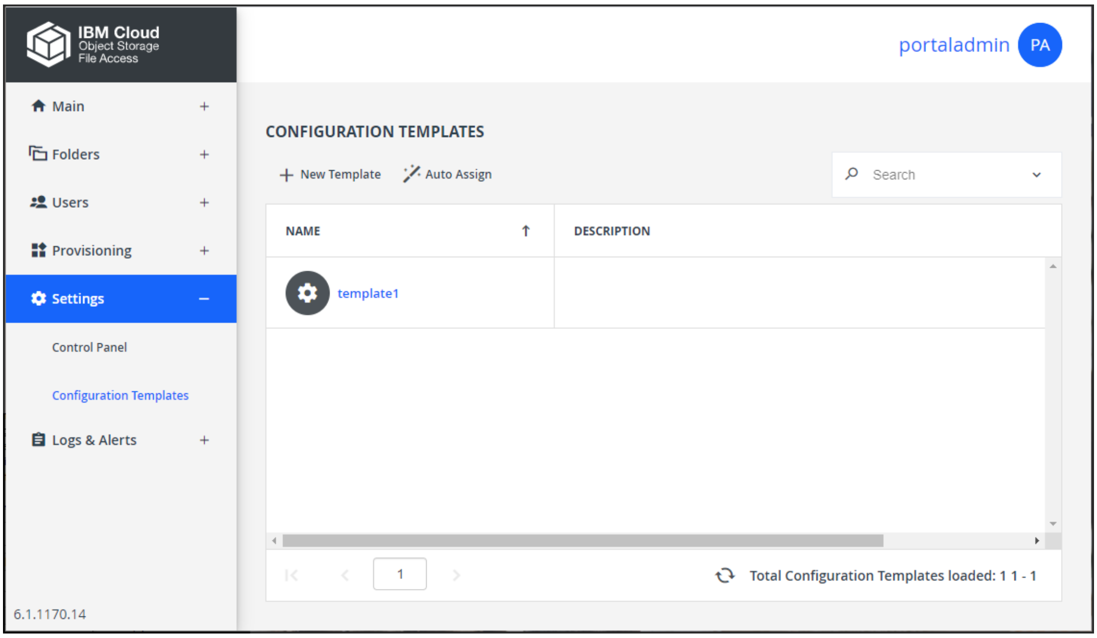
- a Check **If no match, apply default template**.
- b In the drop-down list, select the template to apply when none of the conditions are met.

6 Click **SAVE**.

SETTING THE DEFAULT DEVICE CONFIGURATION TEMPLATE

To set a device configuration template as the default:

1 Select **Settings > Configuration Template** in the navigation pane.
The **CONFIGURATION TEMPLATES** page is displayed.



NAME	DESCRIPTION
template1	

Total Configuration Templates loaded: 1 1 - 1

2 Select the desired template's row.

3 Click **Set Default.**

The selected template becomes the default template.

To stop a default template being the default:

1 In the administration view, select **Settings > Configuration Template** in the navigation pane. The **CONFIGURATION TEMPLATES** page is displayed.

2 Either,

- Select the default template's row and click **Remove Default**. No default template is configured.

Or,

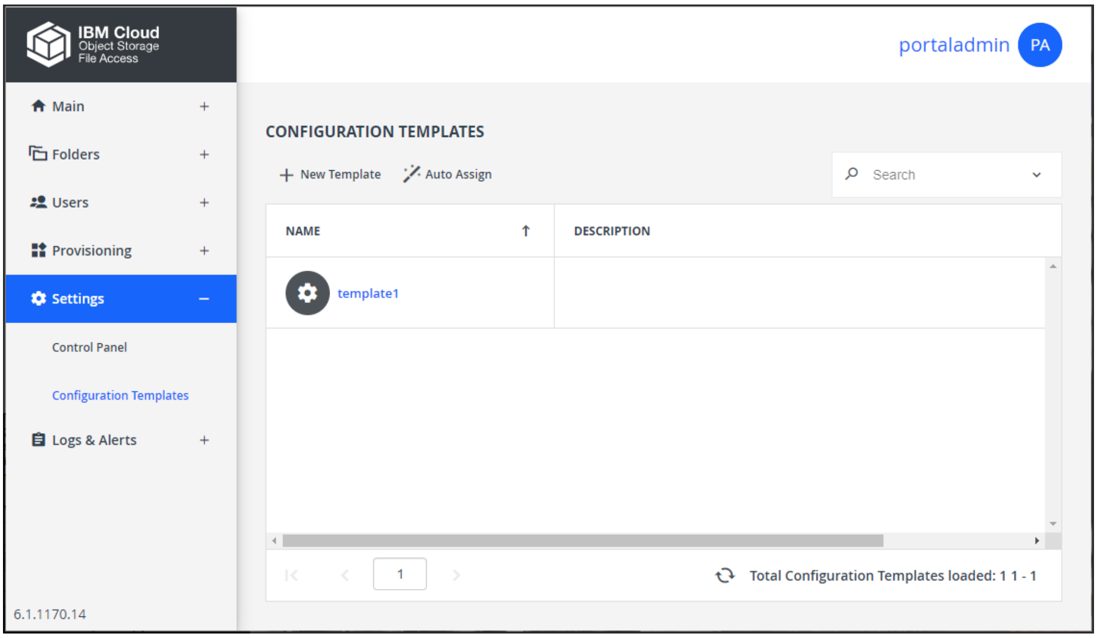
- Select a different template's row to be the default template and click **Set Default.** The newly selected template replaces the original template as the default template.

DUPLICATING CONFIGURATION TEMPLATES

You can create a duplicate of an existing configuration template, then edit it as desired. All settings, except for the template name and description, are copied from the original template.

To duplicate a configuration template:

1 Select **Settings > Configuration Template** in the navigation pane. The **CONFIGURATION TEMPLATES** page is displayed.



2 Select the template's row.

3 Click **Duplicate Template**. A New Configuration Template dialog box is displayed.

4 Enter the **Name** and, optionally, a **Description** of the new template.

5 Click **SAVE**.

The new template is created with the same settings as the original template.

DELETING A CONFIGURATION TEMPLATE

When a device configuration template is deleted from the IBM COS FA Portal, the automatic template assignment policy rules that specify that template are automatically deleted. The policy is then reapplied to all devices that specify automatic template assignment.

Note: When deleting device configuration templates:

- You cannot delete a template that is manually assigned to a device.
- You cannot delete the default template.

To delete a configuration template:

1 In the global administration view, select **Settings > Configuration Template** in the navigation pane.
The **CONFIGURATION TEMPLATES** page is displayed.

2 Either,

a Select the configuration template to delete and click **Delete Template**.
A confirmation window is displayed.

b Click **DELETE TEMPLATE** to confirm.

Or,

a Click the configuration template name.
The configuration template window is displayed with the configuration template name as the window title.

b Click **DELETE**.
A confirmation window is displayed.

c Click **YES** to confirm.

The configuration template is deleted.

CHAPTER 12. MANAGING NOTIFICATIONS

As an administrator, you can receive and view notifications about the IBM COS FA Portal and users as follows:

- On the **Notifications** dashboard of the global administration interface **(Main > Notifications**). Here, you receive all types of notifications that are enabled on the Notification Settings page (**Settings > Notification Settings**).
- In the main Dashboard of the global admin interface. This page displays a summary of the ten highest priority notifications.
- By email. Notifications are sent to administrators by email.

Notifications enable you to track error and warning conditions.

The notification dashboard displays error and warning conditions that are currently in effect, including alerts related to the system, storage nodes, specific virtual IBM COS FA Portals, users and devices.

It is possible to mark specific notifications as hidden, if you do not feel that they require immediate attention. Those notifications can always be unhidden later if desired.

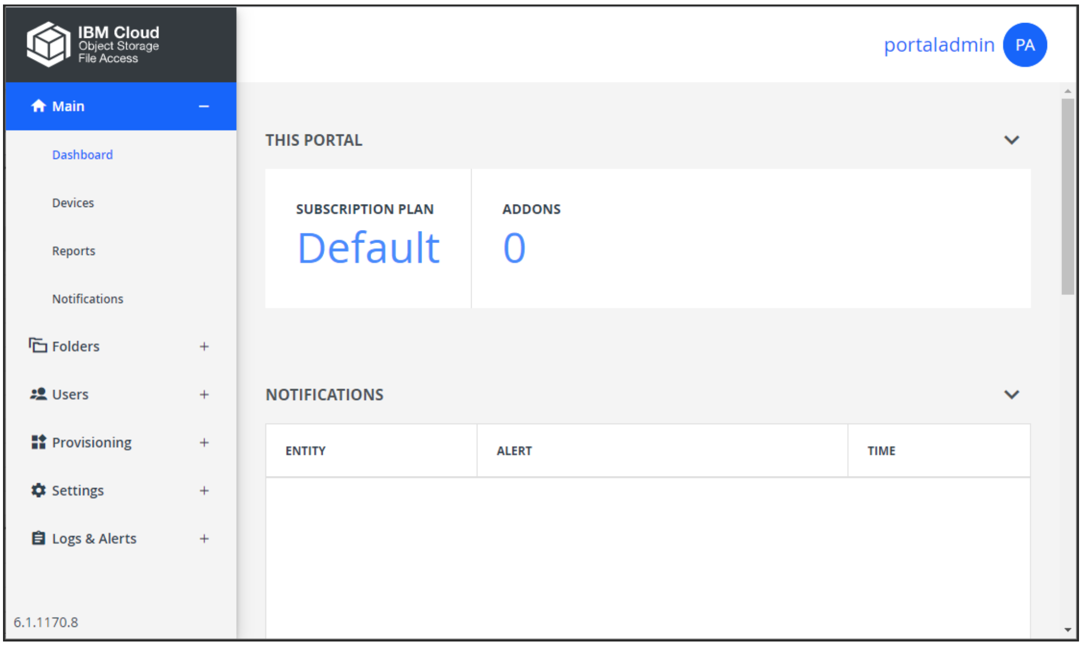
In this chapter

VIEWING NOTIFICATIONS

You can view a summary of the highest priority notifications in the dashboard and all the notifications in the **NOTIFICATIONS** page.

Viewing Notifications in the Main Dashboard

The dashboard displays a summary of the ten highest priority active notifications.



SUBSCRIPTION PLAN
Default

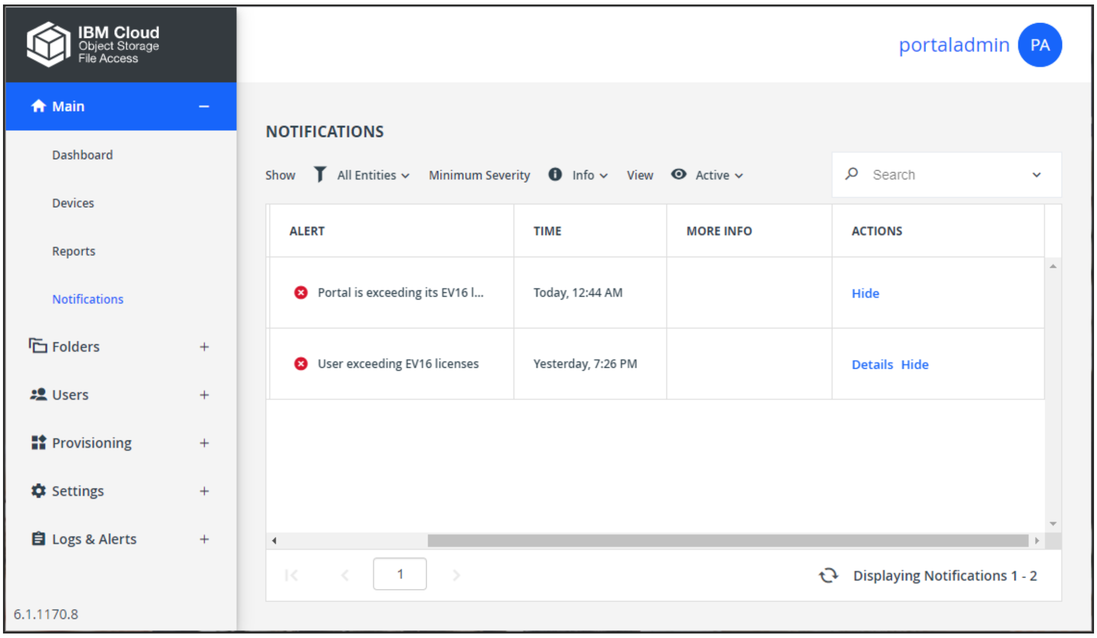
ADDONS
0

If there are notifications, you can go directly to the NOTIFICATIONS page by clicking **SHOW IN NOTIFICATION MANAGER**.

Viewing Notifications in the Notification Page

To view notifications via the notification page:

1 Select **Main > Notifications** in the navigation pane.
The **NOTIFICATIONS** page is displayed.



NOTIFICATIONS

Show All Entities Minimum Severity Info View Active

ALERT	TIME	MORE INFO	ACTIONS
Portal is exceeding its EV16 l...	Today, 12:44 AM		Hide
User exceeding EV16 licenses	Yesterday, 7:26 PM		Details Hide

Displaying Notifications 1 - 2

ALERT – The alert message.
TIME – The time at which the alert was triggered.
MORE INFO – Additional information about the notification.
ACTIONS – Actions you can perform on an alert, for example hiding the alert.

2 You can filter the display.
Show – Filter notifications dependent on the notification source.
All Entities – Notifications from the IBM COS FA Portal, users, and devices.
Portal – Notifications from the IBM COS FA Portal.
Users – User notifications.
Devices – Device Notifications.
Minimum Severity – Filter notifications dependent on the notification severity: **Info**, **Warning**, or **Error**.
View – Filter notifications by whether they are active or not. Non-active notifications are marked as hidden.

3 You can search the list of alerts, searching everything or by entity or by the **MORE INFO** or **ALERT** columns.

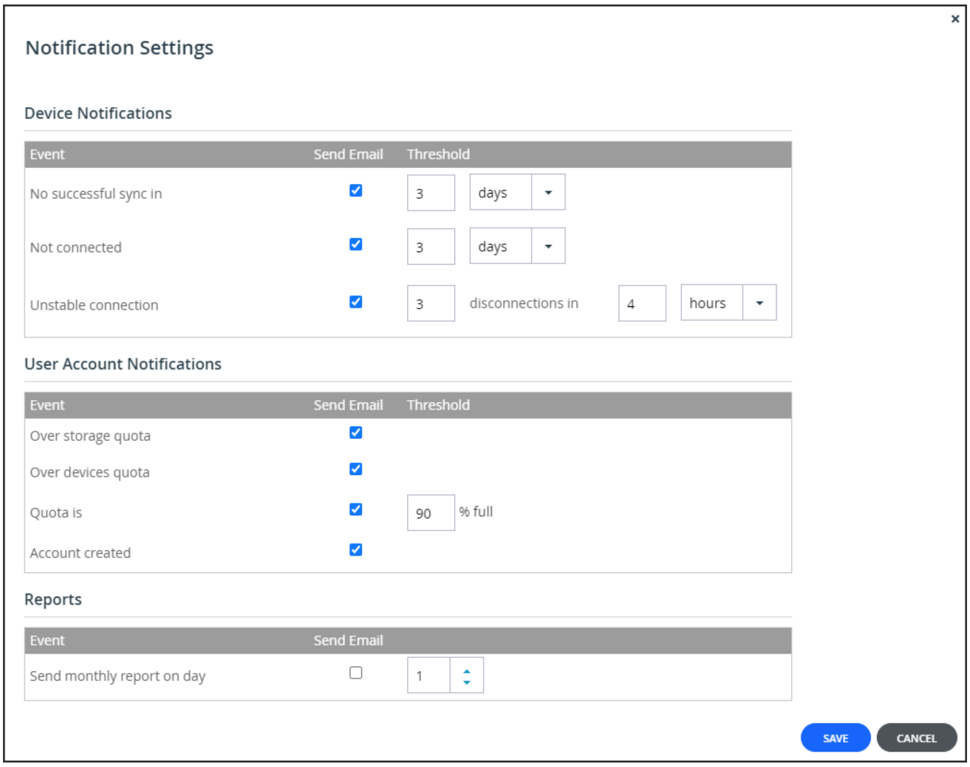
4 You can unhide an notification that you marked as hidden by filtering the display to show hidden notifications and then clicking the **Unhide** link in the **ACTIONS** column for a hidden alert or selecting the notification row and clicking **Unhide**.

CONFIGURING NOTIFICATION SETTINGS

To configure notifications for which emails are sent:

1 Select **Settings** in the navigation pane.

2 Select **Notification Settings**, under **NOTIFICATIONS** in the **Control Panel** content page.
The **Notification Settings** window is displayed.



Notification Settings

Device Notifications

Event	Send Email	Threshold
No successful sync in	☑	3 days
Not connected	☑	3 days
Unstable connection	☑	3 disconnections in 4 hours

User Account Notifications

Event	Send Email	Threshold
Over storage quota	☑	
Over devices quota	☑	
Quota is	☑	90 % full
Account created	☑	

Reports

Event	Send Email	
Send monthly report on day	☐	1

3 Select the notifications which you want to be informed about via email.
The following notifications can be set:

Device Notifications

- A device has not synced with the IBM COS FA Portal for a specified number of hours or days.
- A device has not been connected with the IBM COS FA Portal for a specified number of hours or days.
- A device connection to the IBM COS FA Portal is unstable, having disconnected a specified number of times in a specified number of hours or days.

User Account Notifications

- The amount of storage used exceeds the quota.
- The number of devices used exceeds the quota.
- The amount of storage used is over a specified percentage of the quota.
- An account was created.

Reports

- A monthly report is sent on a specified day of the month.

4 Click **SAVE**.

CHAPTER 13. VIEWING LOGS

The IBM COS FA Portal **Log Viewer** includes the following logs:

Log	Content
System	Events that do not belong in other log categories.
Cloud Sync	Cloud drive synchronization operation events.
Access	User access to the IBM COS FA Portal events.
Audit	Changes to the IBM COS FA Portal configuration.

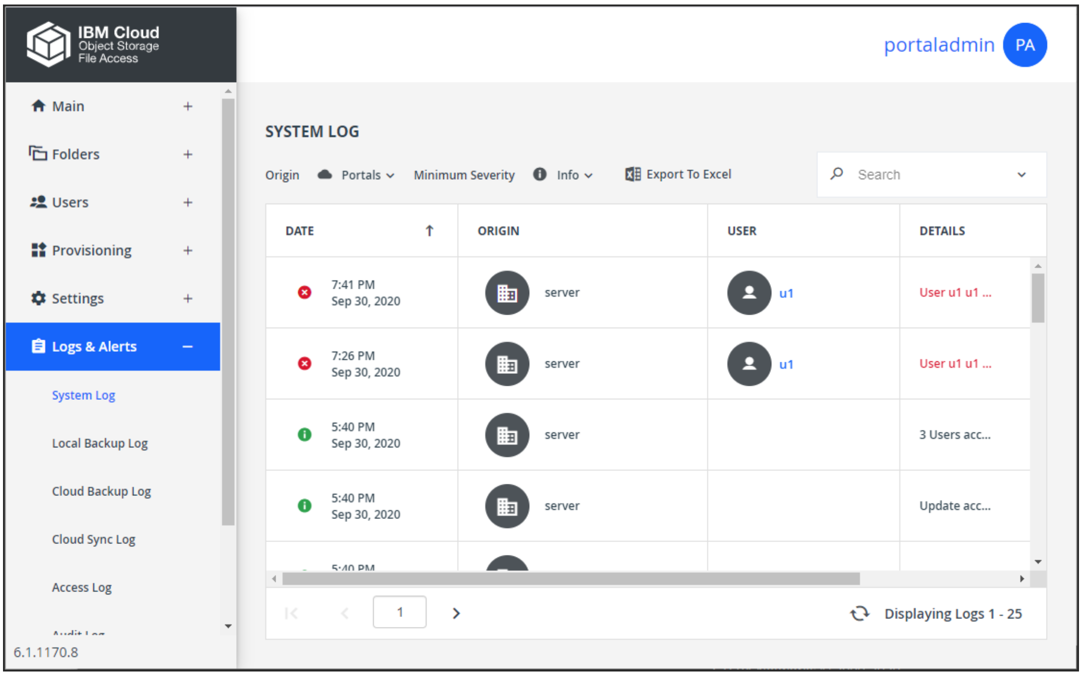
Viewing logs for the IBM COS FA Portal system is available in the Global Administration View. Logs for team IBM COS FA Portals can be viewed in each virtual IBM COS FA Portal's view.

In this chapter

VIEWING SYSTEM LOGS

To view system logs:

- Select **Logs & Alerts > System Log** in the navigation pane.
  The **SYSTEM LOG** page opens, displaying the system log connected to the IBM COS FA Portal.



DATE	ORIGIN	USER	DETAILS
7:41 PM Sep 30, 2020	server	u1	User u1 u1 ...
7:26 PM Sep 30, 2020	server	u1	User u1 u1 ...
5:40 PM Sep 30, 2020	server		3 Users acc...
5:40 PM Sep 30, 2020	server		Update acc...

The information in the System Log can be filtered by:

- The log origin: IBM COS FA Portal, device or both IBM COS FA Portal and device.
- The minimum severity: Debug, Info, Warning, Error.

The page includes the following columns:

Field	Display
DATE	The date and time at which the event occurred. To the left of the date an icon identifies the event severity: ⓘ – Info ⚠ – Warning ⊗ – Error 🐞 – Debug
ORIGIN	The entity that sent the log entry. To view details about the entity, click the entity name.
USER	The user who triggered the event. To view details about the user, click the user name.
DETAILS	A description of the event.
MORE INFO	A possible cause for the entry.

VIEWING CLOUD SYNC LOGS

To view cloud sync logs:

- Select **Logs & Alerts > Cloud Sync Log** in the navigation pane.
  The **CLOUD SYNC LOG** page opens, displaying the cloud syncs to the IBM COS FA Portals.
  The page includes the following columns:

Field	Display
DEVICE	The device name. To view details about the device, click the device name. The device details are displayed in a new browser window.
DATE	The date and time at which the event occurred. To the left of the date an icon identifies the event severity: ⓘ – Info ⚠ – Warning ✖ – Error 🐞 – Debug
RESULT	The result of the cloud sync.
MESSAGE	Additional information in cases where the sync was not successful.

VIEWING ACCESS LOGS

To view access logs:

- Select **Logs & Alerts > Access Log** in the navigation pane.
  The **ACCESS LOG** page opens, displaying the access to the IBM COS FA Portal.
  The page includes the following columns:

Field	Display
DATE	The date and time at which the event occurred. To the left of the date an icon identifies the event severity: ⓘ – Info ⚠ – Warning ✖ – Error 🐞 – Debug
ACTION	The action performed.
ORIGIN	The entity that sent the log entry. To view details about the entity, click the entity name.
USER	The user who triggered the event. To view details about the user, click the user name.
CLIENT IP	The IP address from which the user triggered the event.

Field	Display
TARGET	The entity on which the action was performed.
DETAILS	A description of the event.

VIEWING AUDIT LOGS

To view audit logs

- Select **Logs & Alerts > Audit Log** in the navigation pane.
  The **AUDIT LOG** page opens, displaying the audits to the IBM COS FA Portal.
  The page includes the following columns:

Field	Display
DATE	The date and time at which the event occurred. To the left of the date an icon identifies the event severity: ℹ – Info ⚠ – Warning ✖ – Error 🐞 – Debug
ACTION	The action performed: Added, Modified or Deleted.
ORIGIN	The entity that sent the log entry. To view details about the entity, click the entity name.
USER	The user who triggered the event. To view details about the user, click the user name.
TARGET	The entity that was affected by the action. For example, a folder group or subscription plan, or user. To view details about the entity, click the entity name.
MORE INFO	Additional information about the event.

EXPORTING LOGS TO EXCEL

You can export logs and their details to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export virtual IBM COS FA Portals to Excel:

1. Select the log to export under **Logs & Alerts** in the navigation pane.
   The log page is displayed.
2. Click **Export to Excel**.
   The logs in the current log category are exported to your computer.

MANAGING ALERTS BASED ON LOG EVENTS

You can configure the IBM COS FA Portal to automatically send email alerts to end users and administrators upon certain IBM COS FA Portal log messages.

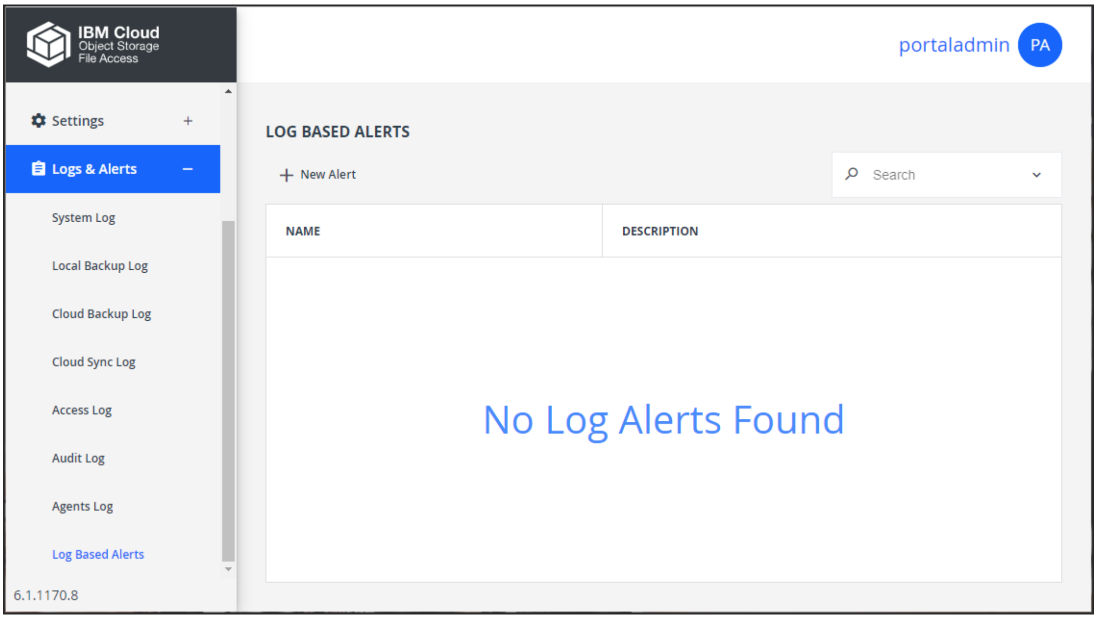
In this section

- Viewing Log Based Alerts
- Adding and Editing Alerts
- Deleting an Alert

Viewing Log Based Alerts

To view all log based alerts:

- Select **Logs & Alerts > Log Based Alerts** in the navigation pane.
  The **LOG BASED ALERTS** page opens, displaying all the Log Based Alerts.



The page includes the following columns:

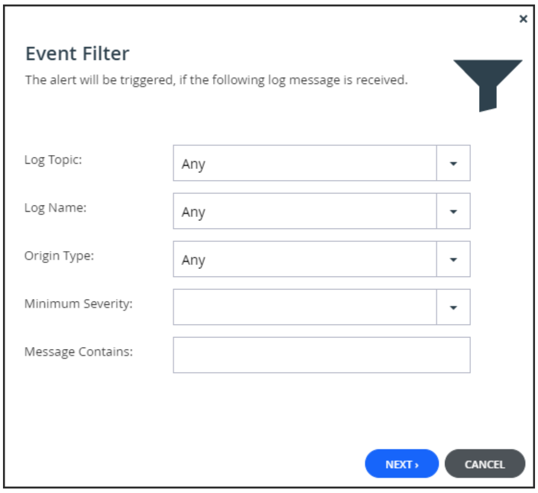
Field	Display
Name	The alert name. To edit the alert, click the alert name.
Description	A description of the alert.

Adding and Editing Alerts

To add or edit an alert:

1. Select **Logs & Alerts > Log Based Alerts** in the navigation pane.
   The **LOG BASED ALERTS** page opens, displaying all the log based alerts.
2. To add a new alert-on, click **New Alert**.
   Or,
   To edit an existing alert, click the alert name**.**

The **Event Filter** window is displayed.



Event Filter

The alert will be triggered, if the following log message is received.

Log Topic: Any

Log Name: Any

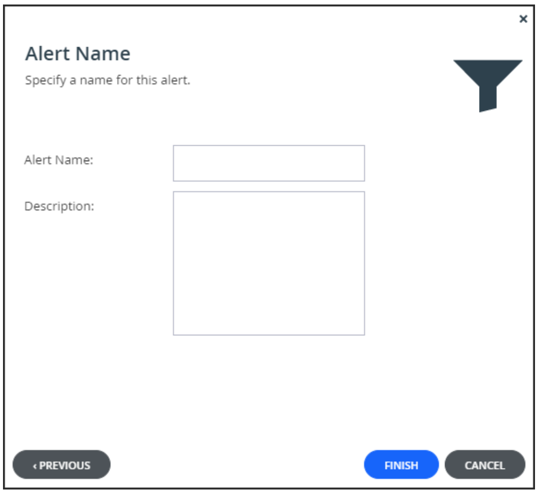
Origin Type: Any

Minimum Severity:

Message Contains:

3 Complete the fields.
Log Topic – The category to trigger the alert. Select **Any** to specify that any log category can trigger the alert.
Log Name – The name of the log event to trigger the alert. Select **Any** to specify that any log event can trigger the email alert.
Origin Type – The entity from which a log must originate to trigger the alert. Select **Any** to specify that any log can originate from any entity in order to trigger the alert.
Minimum Severity – The minimum severity a log must have to trigger the alert.
Message Contains – The text that the log message must contain to trigger the alert.

4 Click **NEXT**.
The **Alert Name** window is displayed.



Alert Name

Specify a name for this alert.

Alert Name:

Description:

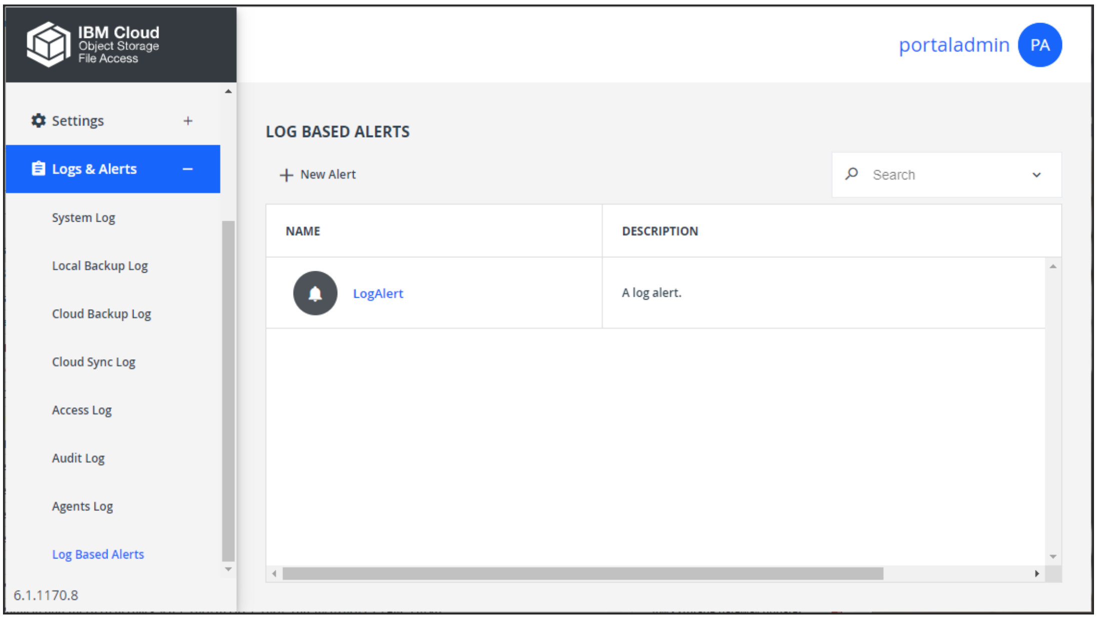
5 Complete the fields.
Alert Name – A name for the alert.
Description – A description of the alert.

6 Click **FINISH**.

Deleting an Alert

To delete an alert:

1 Select **Logs & Alerts > Log Based Alerts** in the navigation pane.
The **LOG BASED ALERTS** page opens, displaying all the Log Based Alerts.



NAME	DESCRIPTION
LogAlert	A log alert.

2 Select the alert row.

3 Click **Delete.**
A confirmation window is displayed.

4 Click **DELETE** to confirm.

The alert is deleted.

UNDERSTANDING IBM COS FA PORTAL LOG MESSAGES

In this section

- Log Message Levels
- Common Log Attributes
- Log Message Topics
- Emergency Messages
- Alert Messages
- Error Messages
- Warning Messages
- Notice Messages
- Info Messages
- Debug Messages

Log Message Levels

IBM COS FA Portal generate log messages upon various events. The log messages are divided into the severity levels.

Level	Required Response
Emergency	System is unusable.
Alert	Action must be taken immediately.
Error	Error condition. Action must be taken as soon as possible.
Warning	Warning messages. An indication that an error may occur if action is not taken.
Notice	Normal but significant condition.
Info	Informational message.
Debug	Debug-level messages, useful for debugging and troubleshooting.

Common Log Attributes

The following attributes are commonly used in Log messages.

Attribute	Type	Description
action	Action	The action (IBM COS FA Portal logs only): • Login • Logout • Create • Download • Update • Delete • Rename • Move • Undelete • Restore • Copy
Action	ChangeAction	The action: • added • deleted • modified • formatted • expanded • disabled • enabled • Additionally for IBM COS FA Gateways: • started • login • logout • command • post_command • get_command • set_command • del_command • put_command
CloudSyncDirection	String	The sync direction: • In • Out
GenericRC	String	The return code: • Ok • PermanentError • TransientError • Warning • NotCompleted

Attribute	Type	Description
id	Integer	The log ID number.
protocol	SessionSource	The protocol for the event: • Administration • Search • FileManager • CLI • CIFS • FTP • NFS • AFP • Rsync • iSCSI • CTTP • webdav • Mobile • WebBrowser • TFTP (only for IBM COS FA Gateways)
RAIDState	String	The RAID state: • optimal • scrubbing • reshaping • recovering • degraded • failed
RepliType	String	The replication type: • Sync • Files • Disk-level
source	String	The entity that sent the event log.
sourceType	LogSourceType	The type of entity that sent the event log: • all • NAS This attribute is optional.
SyncMode	String	The sync mode: • CloudSync
time	dateTime	The date and time at which the event occurred.
username	String	The administrator or user who triggered the event.

Log Message Topics

The log messages are divided in to topics. These topics enable you to understand the source of the message.

Log messages are divided by one of the following topics:

- access
- accounting
- allTopics
- antivirus
- audit
- cloudsync
- files
- sync
- system

Log Message Examples

Example 1

Assume the following IBM COS FA Portal log message is received:

```
info,Login,Portal,,2020-05-06T01:32:05,,CTTP,Administration,Client logged
in to portal,172.21.1.15,,topic: access
```

The first word indicates that this is an info message, and the next two words indicate that it is related to logging into the portal.

UserLoggedInToPortal	Client logged in to portal	Optional: protocol (SessionSource) Optional: clientAddr (String) Optional: action (Action) Optional: host (String) – deprecated

The attributes values are:

Message – `Client logged in to portal`
protocol (SessionSource) – `CTTP`
clientAddr (String) – `172.21.1.15`
action (Action) – Login

The message is also timestamped (`2020-05-06T01:32:05)` with the type of message (`topic: access`).

Example 2

Assume the following IBM COS FA Portal log message is received:

```
error,Login,Portal,,2020-05-06T13:10:00,,,CTTP,Client login to portal
failed,,,failedPortal: portal.myportal.com reason: Login failed: Portal
portal.myportal.com does not exist failedDevice: IT topic: access
```

The first word indicates that this is an error message, and the next two words indicate that it is related to logging into the portal.

UserLoggedInToPortalFailed	Client login to portal failed	Optional: clientAddr (String) Optional: host (String) – deprecated Optional: failedUser (String) Optional: failedDevice (String) Optional: failedPortal (String) Optional: reason (String) Optional: protocol (SessionSource) Optional: action (Action)

The attribute values are:

Message – `Client login to portal failed`
clientAddr (String) – `172.21.1.15`
failedDevice (String) – IT
failedPortal (String) – `portal.myportal.com`
reason – `Login failed: Portal portal.myportal.com does not exist`
protocol (SessionSource) – `CTTP`
action (Action) – Login

The optional field, failedUser (String), does not have a value.

The message is also timestamped (`2020-05-06T13:10:00)` with the type of message (`topic: access`).

Emergency Messages

Class	Message	Additional Attributes
ArrayFailed	RAID array has failed	name (String)

Alert Messages

Class	Message	Additional Attributes
ArrayDegraded	RAID array is running in degraded mode	name (String) Optional: failedDisks (String)
ClocksOutOfSync	Device clock and Portal clock are out of sync. Cloud Drive synchronization disabled	localClock (dateTime) portalClock (dateTime)
CloudConnectFailed	Connection to cloud services has not succeeded for a long time	serverName (String) downSince (dateTime)
CloudSyncFailed	Cloud sync has not succeeded for a long time	—
DeviceClockOutOfSyncError	Device clock and portal clock are out of sync. Cloud Drive synchronization disabled	localClock (dateTime) portalClock (dateTime)
DiskFailedHealthTest	Disk has failed S.M.A.R.T health test	name (String) model (String)

Class	Message	Additional Attributes
DiskNotCompatibleForRAID	Array contains a disk which is unsafe for RAID: SCT Error Recovery Control is unsupported	array (String) disk (String)
FailedToStoreLog	Unable to store logs to log volume	—
SyncFailed	Synchronization task has not succeeded for a long time	name (String) days (Integer)
SyncLinuxAddWatchFailed	Cloud Sync: Add directory watch failed	details (String)
SyncLinuxMaxUserWatchesExceeded	Exceeding the maximum amount of synchronized directories. Some local changes may not be synchronized	details (String)
ThrottlingWritesAlert	Throttling writes due to low space in cache volume.	details (String)
TooMuchDataAsAvaliableOffline	Too much data was marked as available offline. Please increase the cache size in settings	details (String)
TooMuchDataInNonEvictableFolders	Caching Gateway is in critical condition: Too much data in non-evictable folders. Please increase cache size or reduce size of pinned folders.	details (String)
UserQuotaNearFull	User is near quota on volume	user (String) volume (String) usage (String)
UserQuotaOver	User is over quota on volume	user (String) volume (String) usage (String)
VolumeContainErrors	Consistency errors were detected in volume. Run the Volume Repair Wizard	volume (String)
VolumeFull	A storage volume is full	volume (String) usage (String) freeSpace (String)

Error Messages

Class	Message	Additional Attributes
AntivirusErrorLog	Error while scanning a file	Optional: logAction (String) path (String) fileName (String)
AppOperationFailed	Application operation failed	snapshot (String) Optional: filename (String) Optional: path (String) resultCode (GenericRC) resultMsg (String)
AttachFolderGroupFailed	Attempt to access folder with an invalid passphrase	Optional: action (Action)
AutoShareCreationFailed	Automatic share creation process failed	share (String) reason (String)
CatalogDatabaseIsNotResponding	Catalog Database Is Not Responding	serverName (String)
CertificateFailed	No certificate is installed	—
CloudSyncFileTransferFailed	File transfer failed	direction (CloudSyncDirection) Optional: folderID (Integer) Optional: folderName (String) filename (String) Optional: path (String) startTime (dateTime) endTime (dateTime) resultCode (GenericRC) resultMsg (String) totalBlocks (Integer) transferedBlocks (Integer) totalSize (Integer) transferedSize (Integer) Optional: folderOwner (String)
DBNotSaved	Failed to save the configuration file	—
DownloadFailed	Download failed	Optional: protocol (SessionSource) Optional: clientAddr (String) file (String)
Error	Error	details (String)
ErrorLog	Error Message	details (String)
FailedSendingAlertToAll	Failed sending alert. Check your configuration	—
FailedSendingAlertToRecipient	Failed sending alert to specified recipient	recipient (String)
FSCKCompletedWithErrors	File system contains errors that were left unfixed	volume (String)

Class	Message	Additional Attributes
FSCKCompletedWithPersistentErrors	File system contains errors that could not be fixed	volume (String)
InvitationVerificationFailure	Invalid verification code entered	Optional: protocol (SessionSource) Optional: clientAddr (String) mode (String) path (String) Optional: email (String) Optional: phone (String)
MountFailed	Failed mounting the volume. Try enabling snapshots or upgrading your firmware	Optional: volume (String) fsType (String)
RemoteAccessFailedLog	Remote access failed	deviceName (String) errorMsg (String) Optional: action (Action)
RequestFromDeviceFailed	Failed handling device request	device (String) Optional: request (String) Optional: cause (String)
SMTPServerProblem	SMTP server cannot be contacted	description (String)
StorageCommandFailed	Failed running storage command	command (String)
StreamingReplicationFailed	Streaming replication failed	error (String)
TooManyActiveCTTPsessions	User has too many active CTTP sessions	Optional: cause (String)
TooManyFailedLoginAttemps	Too many failed login attempts	Optional: clientAddr (String) Optional: failedPortal (String) Optional: protocol (SessionSource) Optional: action (Action)
TooManyVerificationFailures	Too many verification failures – verification code revoked	Optional: protocol (SessionSource) Optional: clientAddr (String) mode (String) path (String) Optional: email (String) Optional: phone (String)
UnplannedEvent	Unplanned event	details (String)
UserLoggedInToPortalFailed	Client login to portal failed	Optional: clientAddr (String) Optional: host (String) – deprecated Optional: failedUser (String) Optional: failedDevice (String) Optional: failedPortal (String) Optional: reason (String) Optional: protocol (SessionSource) Optional: action (Action)

Class	Message	Additional Attributes
VSSWriterFailed	VSS writer error	mainError (String) writer (String) writerError (String)
XlogArchiveFailed	Xlog archive failed	error (String)

Warning Messages

Class	Message	Additional Attributes
ADConnLocalError	Active Directory connection failed: Domain join operation required	domain (String)
ADConnTransientError	Active Directory connection failed: Network error	domain (String)
AppOperationEndedWithWarnings	Application operation ended with warnings	snapshot (String) Optional: filename (String) Optional: path (String) resultCode (GenericRC) resultMsg (String)
CIFSConnDropped	SMB connection dropped	cause (String)
ConnectionToPortalFailed	Connection to portal failed	name (String) Optional: ip (ipv4) reason (String) retry (Integer) nextRetryDelay (Integer)
DeviceNotificationCacheIsFull	Cache is full but no files could be evicted	Details (String
DeviceUnlicensed	This device is unlicensed	reason (String)
DuplicateArrayName	Found a duplicate array name. Renaming the new array	oldName (String) newName (String)
DuplicateVolumeName	Found a duplicate volume name. Renaming the new volume	oldName (String) newName (String)
DupIPdetectedWarn	Duplicate IP address detected	Optional: MacAddress (String)
FileBlockedDueToSystemErrorLog	Access to file blocked due to system error	Optional: protocol (SessionSource) Optional: clientAddr (String) path (String) Optional: action (Action) Optional: error (String)
FileRejectedLog	File rejected by Cloud Drive policy	Optional: protocol (SessionSource) Optional: clientAddr (String) path (String) Optional: action (Action)

Class	Message	Additional Attributes
FileSyncFailed	File synchronization failed	snapshot (String) filename (String) path (String) resultCode (GenericRC) resultMsg (String) Optional: retry (String)
FileTransferFailed	File transfer failed	snapshot (String) filename (String) Optional: path (String) startTime (dateTime) endTime (dateTime) resultCode (GenericRC) resultMsg (String) totalBlocks (Integer) transferedBlocks (Integer) totalSize (Integer) transferedSize (Integer)
FSCKCompletedFixed	File system contained errors, but they were fixed successfully	volume (String)
FSCKStopped	Repair stopped	volume (String) cause (String)
FTPUserLoginFailedMaxSession	User failed to log in to FTP server: Too many active sessions	maxSessions (Integer)
HomeDirReapplyWarning	Error during home directory reapply process	details (String)
IgnoreVolumeWithDuplicateVolName	Ignoring volume with duplicate volume name	volumeName (String) volumeType (String)
IllegalVolumeName	Found a volume with an invalid name. Renaming the volume	oldName (String) newName (String)
ImportFailed	Import failed	—
KernelLog	Kernel Message	details (String)
LogVolumeNotReady	Log storage location is not available. Storing logs in memory	configuredVolume (String)
LowMemory	System is low on memory	—
MoreThanOnePartition	Detected a disk with more than one partition. Using only the first partition.	port (String)
MultipleConcurrentAdminSessionsDetected	Multiple concurrent sessions detected by an administrator	clientAddr (String) action (Action) hashedSessionID (String)
NetworkGenericError	Network Generic Error	Optional: arg (String)

Class	Message	Additional Attributes
NfsBadPath	Received NFS request for an invalid path	request (String) host (String) path (String)
NfsIllegalPort	Received NFS request on an invalid port	request (String) host (String) path (String) port (String)
NfsNoEntry	Received NFS request for path that is not exported to NFS	request (String) host (String) path (String)
NfsNotExported	Received NFS request for path that is not exported to NFS	request (String) host (String) path (String)
NfsUnknownHost	Received NFS request from unauthorized client	request (String) host (String) path (String)
QuarantinedLog	Infected file found	Optional: logAction (String) path (String) fileName (String) Optional: macAddress (String) Optional: threat (String) Optional: threatAction (String)
RemoveArrayElement	Removing a configuration field that is no longer required from the configuration file	type (String) problem (String)
ResetDB	Resetting the configuration to defaults	—
ResetField	Resetting the configuration field to defaults	field (String) problem (String)
ResourceUsageEvent	Resource Usage Limit Exceeded	eventname (String) description (String)
SendKeepAliveError	Send Keep-Alive alert	details (String)
StreamingReplicationHighLag	Streaming replication is running with latency	error (String)
SyncListenerOverflow	Cloud Sync: Overflow in FS listener	details (String)
UploadRequestDenied	Upload request denied	Optional: protocol (SessionSource) Optional: clientAddr (String) file (String)
UserLoggedInFailed	User failed to log in	Optional: protocol (SessionSource) Optional: clientAddr (String)

Class	Message	Additional Attributes
VirusDetected	Virus detected	filename (String) folder (String) virusname (String)
Warning	Warning	details (String)
WarningLog	Warning Message	details (String)

Notice Messages

Class	Message	Additional Attributes
ArrayStatusChanged	Array status changed	arrayName (String) status (RAIDState)
AuditLog	Configuration Changed	Setting (String) Action (ChangeAction) Optional: Name (String)
CertificateUpdated	Device certificate was updated	SHA1Fingerprint (String)
ConnectedToPortal	Connected to portal	name (String) ip (ipv4)
DeviceStartedUp	Device started up	—
DisconnectedFromPortal	Disconnected from portal	name (String) ip (IPv4)
DiskPlugInLog	Disk plugged in	port (String)
DiskUnPlugLog	Disk unplugged	port (String)
FirmwareChanged	Firmware version changed	previous (String) current (String)
ImportSucceeded	Import succeeded	—
NetworkConnected	Connected to network	port (String) address (IPv4)
NetworkDisconnected	Disconnected from network	port (String) duration (duration)
Notice	Notice	details (String)
NTPTimeUpdate	System time was updated by the NTP server	newTime (String) oldTime (String)
RebootLog	Device restarted	—
ShutdownLog	Device shut down	—
SnapshotAuditLog	Snapshots changed	Setting (String) Action (ChangeAction) Optional: Name (String) Optional: Volume (String) Optional: Comment (String)

Class	Message	Additional Attributes
UserLoggedIn	User logged in	Optional: protocol (SessionSource) Optional: clientAddr (String)
UserLoggedOut	User logged out	Optional: protocol (SessionSource) Optional: clientAddr (String)
VirusDBUpdated	Virus definitions database updated	mainVer (String) dailyVer (String)

Info Messages

Class	Message	Additional Attributes
AccountingLog		Optional: accountName (String)
ADConnOK	Connected to Active Directory domain	domain (String)
AppOperationSuccess	Application operation succeeded	snapshot (String) Optional: filename (String) Optional: path (String) resultCode (GenericRC) resultMsg (String)
ArraySyncFinish	Finished array syncing	Optional: Arr (String)
ArraySyncStart	Starting array syncing	Optional: Arr (String)
ClientActivatedInPortal	Client activated in portal	Optional: protocol (SessionSource) Optional: clientAddr (String) clientMac (String) activationCode (String)
ClientActivatedInPortalFailed	Client failed activation in portal	Optional: protocol (SessionSource) Optional: clientAddr (String) clientMac (String) activationCode (String)
ClientLoggedOutFromPortal	Client logged out of portal	Optional: protocol (SessionSource) Optional: clientAddr (String) Optional: action (Action) Optional: host (String)
CloudDriveAccess	Cloud Drive Access	Optional: protocol (SessionSource) Optional: clientAddr (String) path (String) Optional: newPath (String) Optional: version (String) Optional: action (Action) Optional: upn (String)

Class	Message	Additional Attributes
CloudDriveAccessFailOpen	Cloud Drive Access: DLP service is not available. Download allowed	Optional: protocol (SessionSource) Optional: clientAddr (String) path (String) Optional: newPath (String) Optional: version (String) Optional: action (Action) Optional: upn (String)
CloudSyncFileTransferred	File transferred	direction (CloudSyncDirection) Optional: folderID (Integer) Optional: folderName (String) filename (String) Optional: path (String) startTime (dateTime) endTime (dateTime) resultCode (GenericRC) Optional: resultMsg (String) totalBlocks (Integer) transferedBlocks (Integer) totalSize (Integer) transferedSize (Integer) Optional: folderOwner (String)
DeletedFromQuarantine	File deleted from quarantine	Optional: logAction (String) Optional: path (String) Optional: fileName (String) Optional: threat (String)
DownloadCompleted	Download completed	Optional: protocol (SessionSource) Optional: clientAddr (String) file (String)
FileTransferred	File transferred	snapshot (String) filename (String) Optional: path (String) startTime (dateTime) endTime (dateTime) resultCode (GenericRC) Optional: resultMsg (String) totalBlocks (Integer) transferedBlocks (Integer) totalSize (Integer) transferedSize (Integer)
FSCKCompletedNoErrors	Repair completed successfully without errors	volume (String)
FSCKRecoveryCompleted	File system recovered after unclean shutdown	volume (String)
HomeDirReapplyEnded	Home directory reapply process completed	dirsProcessed (Integer) errors (Integer)
IndexDeleted	Index deleted	Optional: Share (String)

Class	Message	Additional Attributes
Info	Info	details (String)
InfoLog	Informational Message	details (String)
InvitationAccess	User accessed invitation	Optional: protocol (SessionSource) Optional: clientAddr (String) path (String) mode (String) Optional: email (String) Optional: upn (String) code (String) action (Action)
NfsAuth	Received NFS request from authenticated client	request (String) host (String) path (String)
RestoredFromQuarantine	File restored from quarantine	Optional: logAction (String) path (String) Optional: fileName (String)
UserLoggedInToPortal	Client logged in to portal	Optional: protocol (SessionSource) Optional: clientAddr (String) Optional: action (Action) Optional: host (String) – deprecated
UserParkedToPortal	Client connected to portal	Optional: protocol (SessionSource) Optional: clientAddr (String) Optional: host (String) – deprecated Optional: action (Action)
VerifiedPermalinkPincodeLog	External user successfully authenticated by PIN code	clientAddr (String) path (String) email (String) action (Action)
VerifiedPermalinkWithMachineTokenLog	External user successfully authenticated by providing machine token	clientAddr (String) email (String) action (Action)
VolumeTransferred	Volume transferred	snapshot (String) filename (String) volTotalSize (Integer) transferred (Integer) incremental (Integer) resultCode (GenericRC) Optional: resultMsg (String)

Debug Messages

Class	Message	Additional Attributes
AntivirusApprovedLog	File scanned and approved	Optional: logAction (String) path (String) fileName (String)
DebugLog	Debug Message	details (String)
DomainControllerConnFail	Failed connecting to a domain controller	domain (String) Server (String
EvictorNotification	Cloud Cache	Status (String)
LogDropped	Log Dropped	Optional: Class (String) Optional: Field (String)
NotScannedLog	File was not scanned	Optional: logAction (String) path (String) fileName (String)
RemoveField	Removing a deprecated configuration field from the configuration file	field (String)

CHAPTER 14. MANAGING REPORTS

The IBM COS FA Portal provides the following global administration reports:

- Folders
- Folder Groups

In this chapter

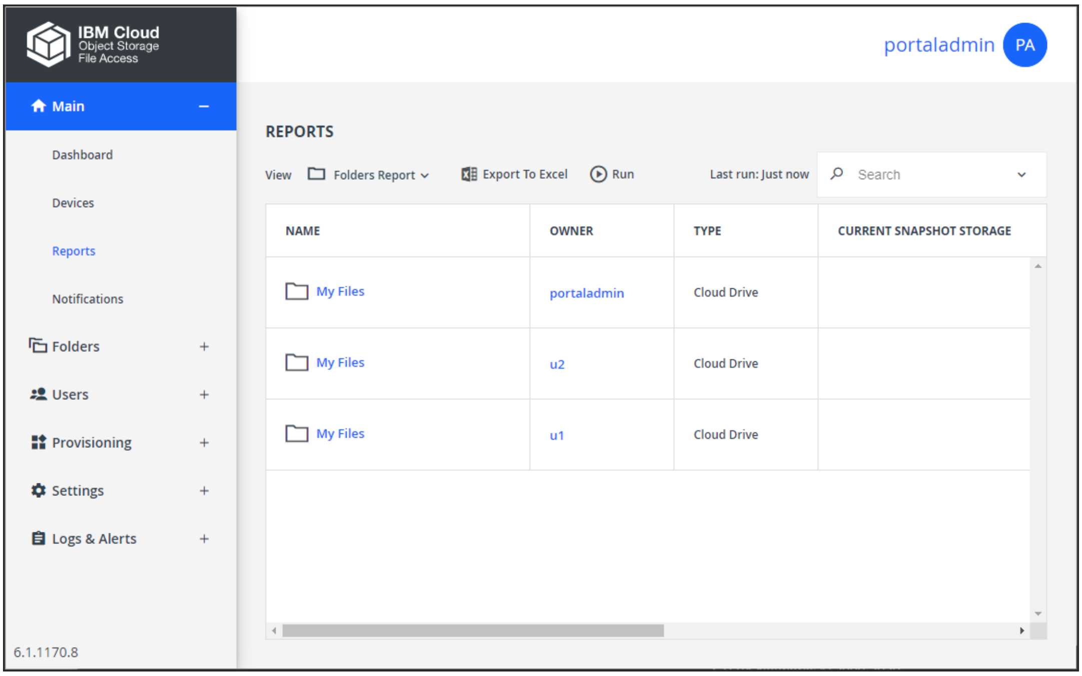
- Viewing the Folders Report
- Viewing the Folder Groups Report
- Generating an Up-To-Date Report
- Exporting Reports to Excel

VIEWING THE FOLDERS REPORT

You can view detailed information about all folders, including deleted ones.

To view the Folders Report:

1 Select **Main > Reports** in the navigation pane.
The **REPORTS** page is displayed.



NAME	OWNER	TYPE	CURRENT SNAPSHOT STORAGE
My Files	portaladmin	Cloud Drive	
My Files	u2	Cloud Drive	
My Files	u1	Cloud Drive	

Note: On first entry to the Reports page, you have to generate the reports.

2 Select **Folders Report** from the **View** drop-down list.

3 If the **Last run on** field displays *Never*, or if you would like to update the displayed report, click **Run**.

The following information is displayed.

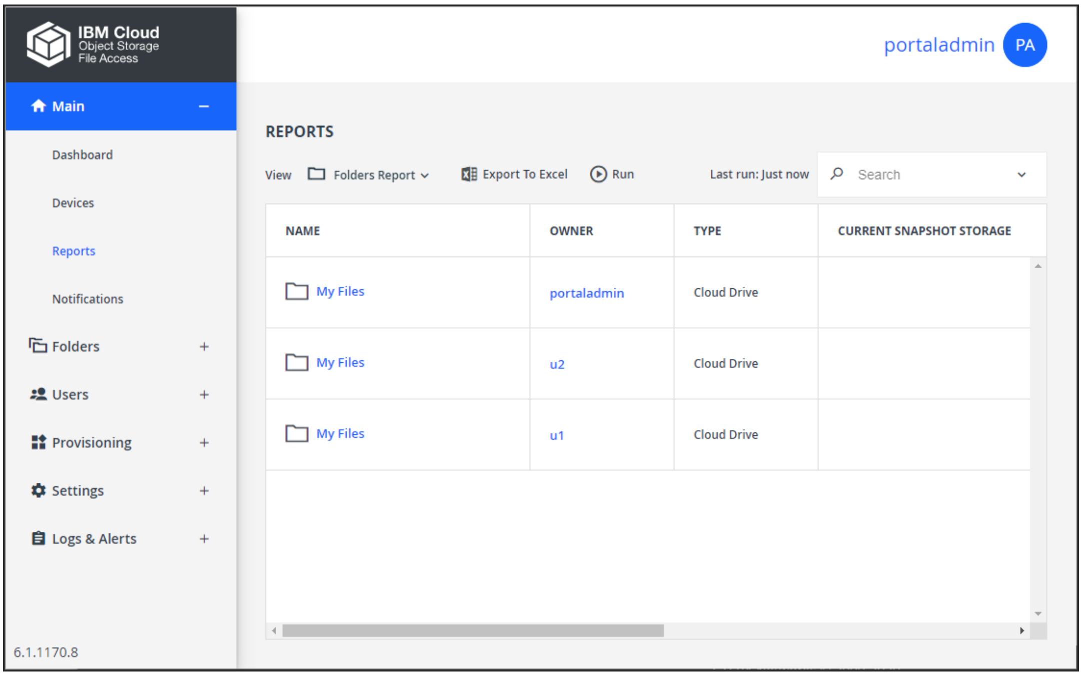
Field	Display
NAME	The folder's name.
OWNER	The folder's owner.
TYPE	The type of folder, cloud drive.
CURRENT SNAPSHOT STORAGE	Details about the latest snapshot: • The storage quota allocated to this folder. If the quota is unlimited, this value is empty, otherwise, it displays the percentage of the storage quota being used. • The amount of storage space used in this folder. • The number of files in the current snapshot and the amount of storage required by these files.
ALL SNAPSHOT STORAGE	Details about all the snapshots: • The total number of snapshots. • Total physical storage required for all the snapshots. • The total number of files in all the snapshots and the amount of storage required by these files. • The number of corrupted files in the virtual IBM COS FA Portal. • The number of files currently being uploaded.

VIEWING THE FOLDER GROUPS REPORT

You can view detailed information about all folder groups, including deleted ones.

To view the Folder Groups Report:

1 Select **Main > Reports** in the navigation pane.
The **REPORTS** page is displayed.



NAME	OWNER	TYPE	CURRENT SNAPSHOT STORAGE
My Files	portaladmin	Cloud Drive	
My Files	u2	Cloud Drive	
My Files	u1	Cloud Drive	

2 Select **Folders Groups Report** from the **View** drop-down list.

3 If the **Last run on** field displays *Never*, or if you would like to update the displayed report, click **Run**.
The following information is displayed.

Field	Display
NAME	The folder's name.
OWNER	The folder's owner.
MAPFILES	Details about the mapfiles: • The amount of storage space consumed by this folder group. • The amount of space consumed by the mapfiles for this folder group. • The number of mapfiles currently being uploaded to folders belonging to this folder group. • The number of missing mapfiles in folders belonging to this folder group. • The total number of mapfiles in folders belonging to this folder group.

Field	Display
BLOCKS	Details about the blocks: • The total number of snapshots. • The number of uploaded blocks in folders belonging to this folder group. • The number of blocks currently being uploaded to folders belonging to this folder group. • The number of missing blocks in folders belonging to this folder group. • The number of files currently being uploaded.
FILES	• The total number of files in folders belonging to this folder group. • The number of folders belonging to this folder group. • The uncompressed size of the files in folders belonging to this folder group. • The number of files that are currently being uploaded to folders belonging to this folder group. • The size of files that are currently being uploaded to folders belonging to this folder group. • The number of corrupted files in folders belonging to this folder group.

GENERATING AN UP-TO-DATE REPORT

The REPORTS page shows the last time the report was generated. You can generate an up-to-date report.

To generate a report:

1. Select **Main > Reports** in the navigation pane.
   The **REPORTS** page is displayed.
2. Select the report to generate from the **View** drop-down list.
3. Click **Run**.

The report is generated.

EXPORTING REPORTS TO EXCEL

You can export the reports to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export a report to Microsoft Excel:

1. View the report to be exported.
2. Click **Export to Excel**.

The report is exported to your computer.

For the **Folders** report the following information is displayed.

Column	Description
Name	The folder's name.
Owner	The folder's owner.
Type	The type of folder, cloud drive.

Column	Description
Quota	The storage quota allocated to this folder in bytes. If the quota is unlimited, this value is zero (0).
Files	The number of files in the current snapshot.
Snapshots	The total number of snapshots.
Physical	Total physical storage required for all the snapshots in bytes.
Files	The total number of files in all the snapshots.
Files in Upload	The number of files currently being uploaded.
Bad Files	The number of corrupted files in the virtual IBM COS FA Portal.

For the **Folder Groups** report the following information is displayed.

Field	Display
name	The folder's name.
Owner	The folder's owner.
Mapfile Overhead	The amount of space consumed by the mapfiles for this folder group in bytes.
Total Mapfiles	The total number of mapfiles in folders belonging to this folder group.
In Upload Mapfiles	The number of mapfiles currently being uploaded to folders belonging to this folder group.
Missing Mapfiles	The number of missing mapfiles in folders belonging to this folder group.
Blocks Storage Space	The amount of block storage space consumed by this folder group in bytes.
Uploaded Blocks	The number of uploaded blocks in folders belonging to this folder group.
In Upload Blocks	The number of blocks currently being uploaded to folders belonging to this folder group.
Total Files	The total number of files in folders belonging to this folder group.
Uncompressed Size	The uncompressed size of the files in folders belonging to this folder group.
Files in Upload	The number of files that are currently being uploaded to folders belonging to this folder group.
Bad Files	The number of corrupted files in folders belonging to this folder group.