IBM COS FA Portal

GLOBAL ADMINISTRATOR GUIDE

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:

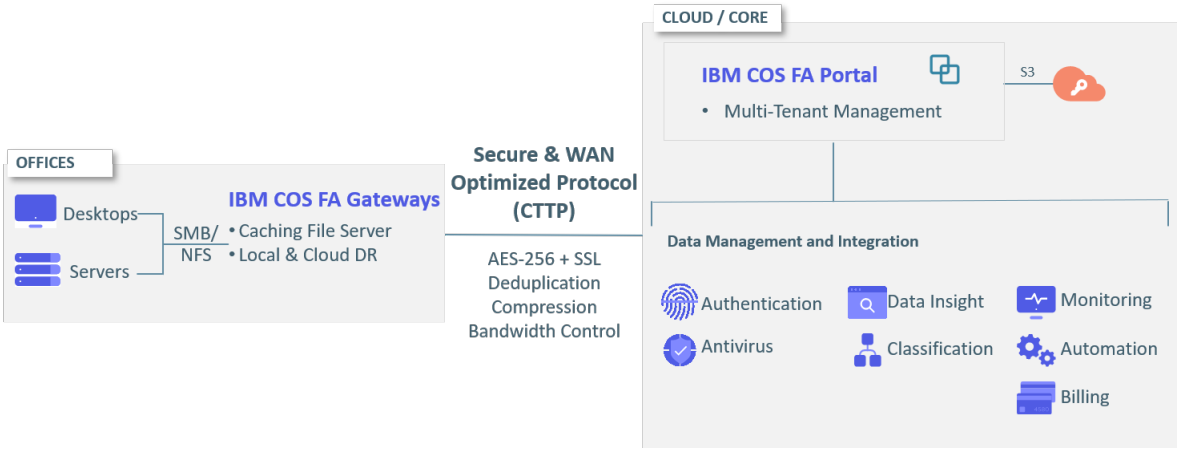
- IBM COS FA Portal
- IBM COS FA Gateway

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.



In this chapter

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. View the device status in detail, including logged events, network status, and 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.

VIRTUAL PORTALS: TENANTS

As the IBM COS FA Portal owner, you can create one or more virtual, team, IBM COS FA Portals on a single set of physical servers.

When multiple team portals are created, the IBM COS FA Portal owner can assign each team portal to a different organizational unit within the company or team. Each organizational unit can log in to their own virtual portal and manage their settings.

The IBM COS FA Portal owner can access and manage the contents of any team portal, as well as manage global settings across all virtual portals. This guide describes the global administration tasks. For information about administering each team IBM COS FA Portal, see the *IBM COS FA Portal Team Administrator Guide*.

IBM COS FA PORTAL PROVISIONING

Provisioning is the process of assigning services and quotas to team IBM COS FA Portals. The IBM COS FA Portal owner provisions each virtual portal owner with services and quotas. In order to obtain services, virtual team IBM COS FA Portals are assigned to a *global plan* which defines a set of services that the portal will receive. The plan can also specify a maximum snapshot retention policy for the portal. For example, it is possible to limit a virtual portal to use a total of up to 100GB of storage spaces.

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 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

In order to use the IBM COS FA Portal, you need an Internet 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 portal
- Managing the servers on which IBM COS FA Portal is installed
- Creating and configuring virtual portals
- Provisioning the virtual portals

Each virtual portal also has its own administration interface. As a global administrator, you can access the global administration interface and each virtual portal's administration interface.

For information about administering each virtual portal, see the *IBM COS FA Portal Team Administrator Guide*.

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 all virtual portals and also enables you to perform specific administration tasks for a specific portal.

The interface includes the following views:

Administration view – Enables you to perform administration tasks that are global, affecting all virtual portals. The tasks described in this guide are performed in this view.

Virtual portal view – Enables you to perform administration tasks for each virtual portal. Administrators of a virtual portal can perform the same tasks via their portal administration interface, which is almost identical to this view. For information about administering each virtual portal, see the *IBM COS FA Portal Team Administrator Guide*.

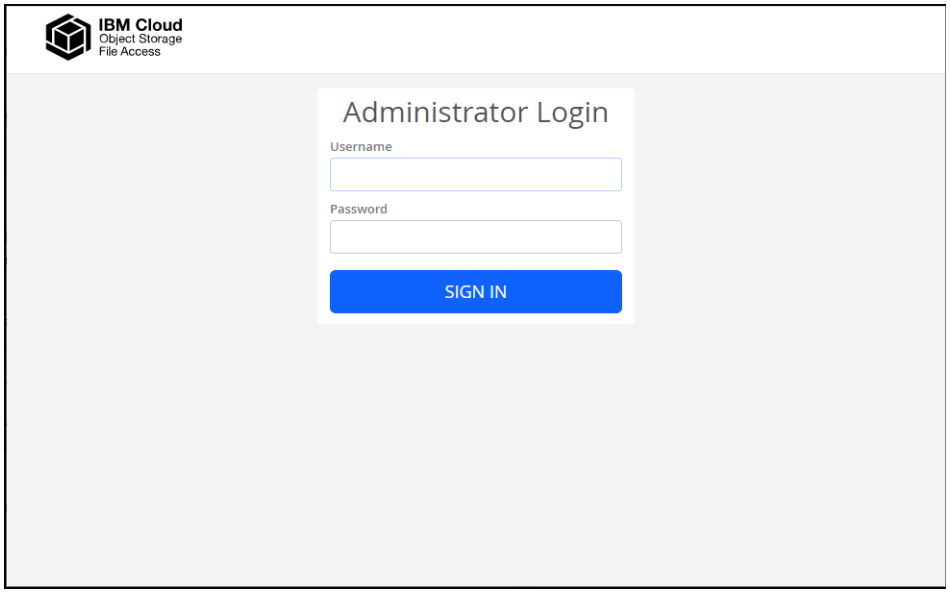
To log in to the administration interface you use the IP address of one of the IBM COS FA Portal servers or, after the DNS service is set up, you can use it with the portal's DNS suffix and, if changed from the default, the HTTPS access port number.

To log in to the administration interface:

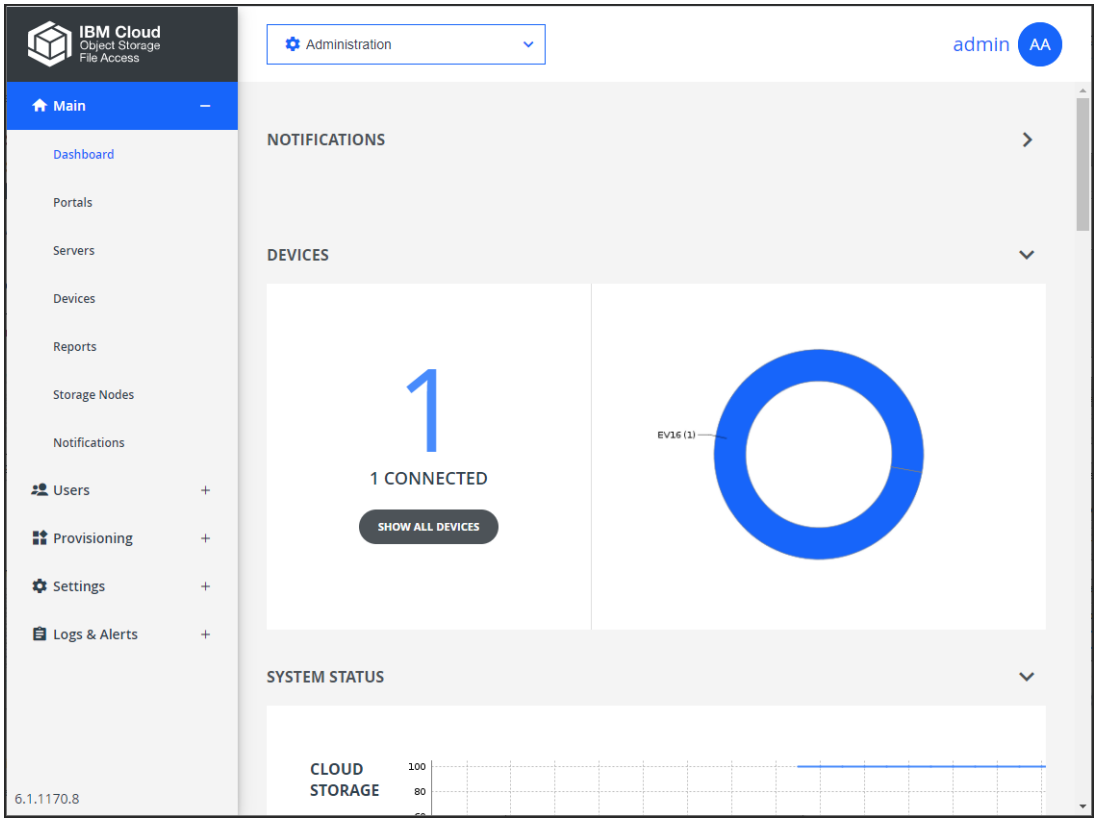
1 In a Web browser open `http://<virtualportal_name>.<DNS_Suffix>/admin`.
where, `<virtualportal_name>` is the name of any one of the virtual portals defined in IBM COS FA Portal, and `<DNS_Suffix>` is the DNS suffix for the whole IBM COS FA Portal installation.
This opens the interface to the specific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

Note: If the 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>/admin`, where `<HTTPS_port>` is a customized port. See The HTTPS Access Port.
For example, to connect to Example's administration portal using HTTPS port 2222, use the following address: `https://CompanyPortal.example.com:2222/admin`.

Or,
Open `http://<Portal_Server_IP>/admin`.
where <Portal Server IP> is the IP address of one of the IBM COS FA Portal servers. For example, to connect to the global administration view of a portal whose server IP address is 192.168.10.10, open `http://192.168.10.10`. This method enables you to gain access to the administration view, if the DNS service is not set up.
After connecting, you can switch to any specific virtual portal view or back to the administration view, as described in Navigating Between Views.
The IBM COS FA Portal opens, displaying the login page.



2 Enter your administrator user name and password and click **SIGN IN**. If you are redirected to an identity provider's login page, enter your credentials there. The identity provider processes your authentication.
The administration interface opens displaying the **Main > Dashboard** page of the administration view, shown below, or a specific portal.



NAVIGATING BETWEEN VIEWS

To navigate between the administration view and a specific virtual portal view:

1. Open the portal drop-down list in the top bar.
2. Select **Administration** or the virtual portal you want to manage. You can start typing the name of the portal in the drop-down to filter the names displayed in the drop-down.

Note: If there are too many portals to list in the drop-down, you can also choose **Main > Portals** in the navigation pane of the administration view and scroll to the portal you want.

Click the icon in the **NAME** column to open the administration view for the portal.

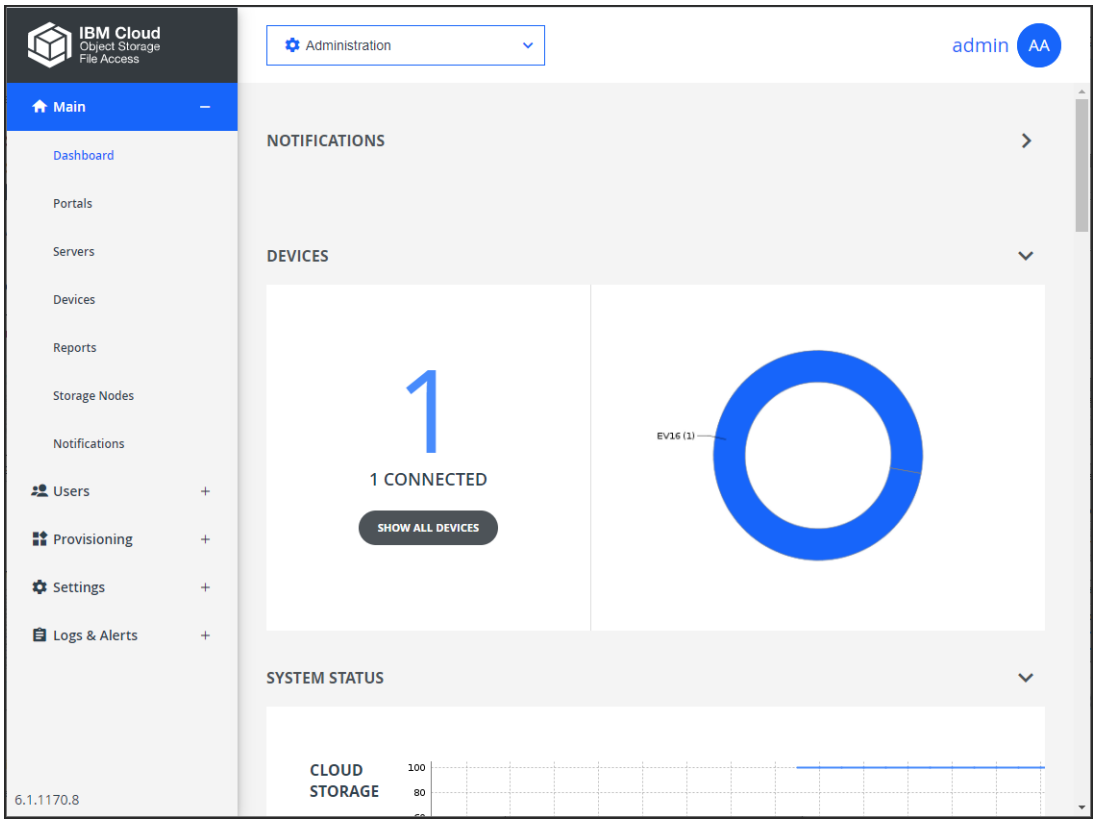
For information about administering each virtual portal, see the *IBM COS FA Portal Team Administrator Guide*.

USING THE PORTAL ADMINISTRATION INTERFACE

The portal interface consist of the following elements:

Top bar – The list of portals in a drop-down and the user name at the top right. Clicking the graphic next to the name displays additional controls, such as access to help.

Navigation Pane – To navigate between pages in the portal.
Content – Displays the portal pages.



ACCESS URLS FOR ADMINISTRATORS

The global administration interface is accessible via the IP address of any of the IBM COS FA Portal servers. IBM recommends using IP address access for testing environments. For production environments, IBM recommends configuring the DNS service.

The URL for accessing a virtual portal as an end user or as an administrator, or for accessing the global administration interface of the IBM COS FA Portal may depend on:

- The Access Protocol
- The HTTPS Access Port

Note: A DNS suffix, used to create a virtual portal's DNS name, to access the portal, was set when the portal was installed, as described in the installation guide for the environment and in Configuring Global Settings.

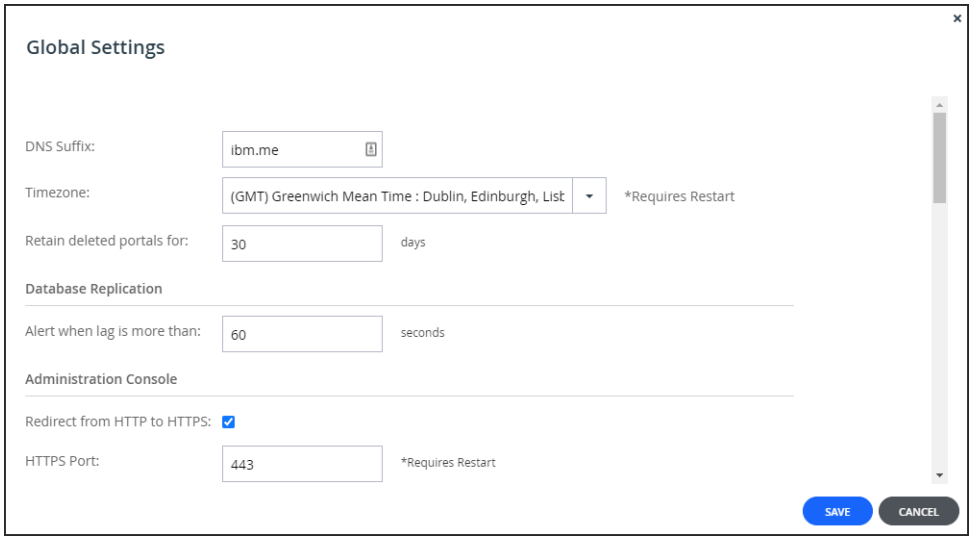
The Access Protocol

The global administration interface is accessible only via HTTPS.

The end user interface for team administrators is accessible via HTTP or HTTPS. You can enable automatic redirection of users from HTTP to HTTPS.

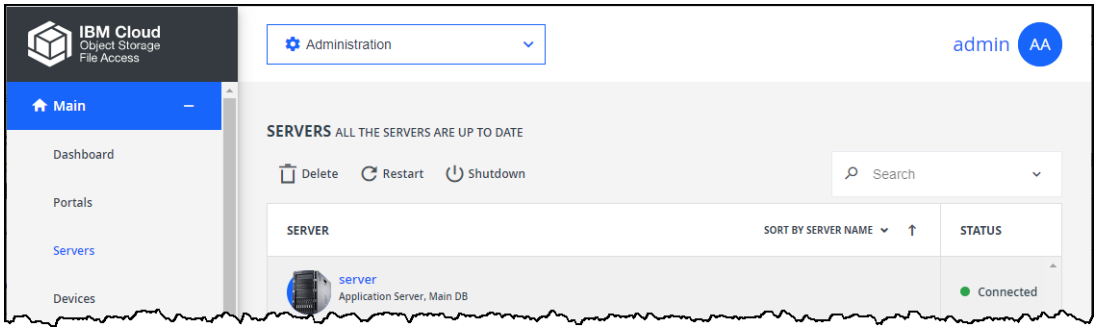
To enable automatic redirection from HTTP to HTTPS

1. In the global administration view, select **Settings** in the navigation pane.
2. Select **Global Settings** in the **Control Panel** content page.
   The **Global Settings** window is displayed.



3. For administrators, make sure **Redirect from HTTP to HTTPS** is checked under **Administration Console**.
4. For the end user interface for team administrators, check **Redirect from HTTP to HTTPS** under **End-User Portal**.
5. Click **SAVE**.
6. Restart the IBM COS FA Portal servers in the following order.
   a. Main database server.
   b. Replication database server.
   c. All application servers.

Select each server in turn and click **Restart** on the **Main > Servers** page.



The change is implemented after the restart.

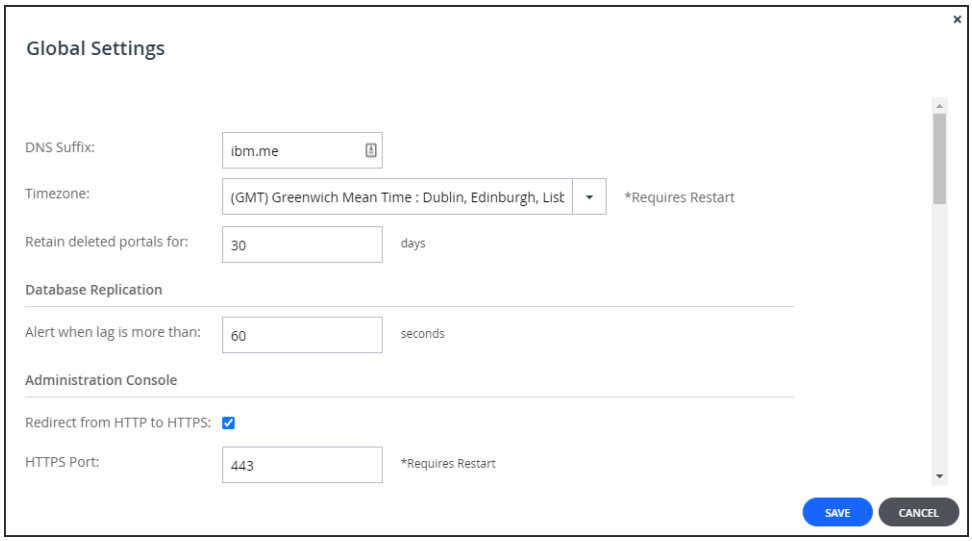
The HTTPS Access Port

By default, the administration portal is accessible via the standard HTTPS port, 443. However, you can change the HTTPS port. Changing the administration portal's HTTPS access port can block undesired access to the portal. Once the HTTPS port is changed, the non standard port must be specified in the URL in order for the browser to access the portal.

To connect to the administration portal after changing the administration access port, append the port number to the FQDN of your portal. For example, to connect to *Example's* administration portal using HTTPS port 2222, use the following address: `https://example.ibm.me:2222/admin`

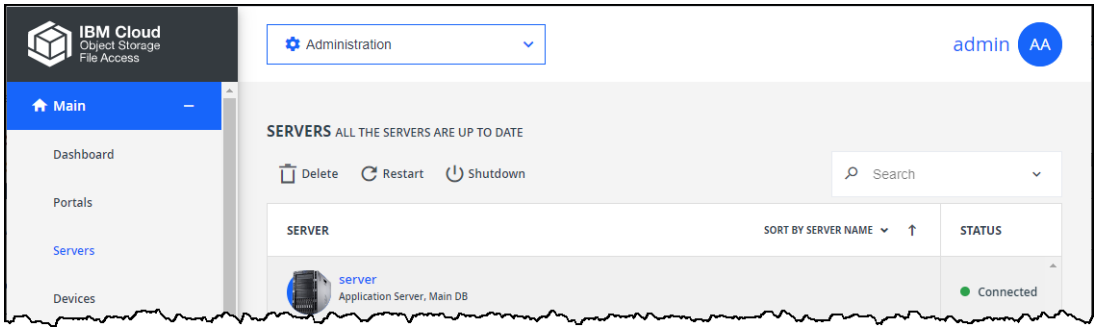
To customize the administration portal HTTPS access port:

1. In the global administration view, select **Settings** in the navigation pane.
2. Select **Global Settings**, under **SETTINGS** in the **Control Panel** content page.
   The **Global Settings** window is displayed.



3. In the **Administration Console** area, specify the new HTTPS port in the **HTTPS Port** field.
   The allowed HTTPS ports are: 443, and from 1024 to 65535.
4. Click **SAVE**.
5. Restart the IBM COS FA Portal servers.
   a. In the global administration view, select **Main Servers** in the navigation pane.
   The **SERVERS** page is displayed.

b Select each server in turn and click **Restart** for each server.
Restart the servers in the following order:
- Main database server.
- Replication database server.
- All application servers.



The change is implemented after the restart.

6 Configure the firewalls on the IBM COS FA Portal servers to enable TCP traffic between the servers on the customized HTTPS port. This is necessary because the customized HTTPS port is used for IBM COS FA Portal server-to-server communications.

Note: Using *Redirect from HTTP to HTTPS* in addition to a customized HTTPS access port results in a redirect to the address that includes the custom port. For example, a redirect from `http://example.ibm.me/admin` to `https://example.ibm.me:2222/admin`.

CHAPTER 3. MANAGING GLOBAL ADMINISTRATORS

Global administrators have access to the IBM COS FA Portal global administration view, and to the administration view for all team IBM COS FA Portals.

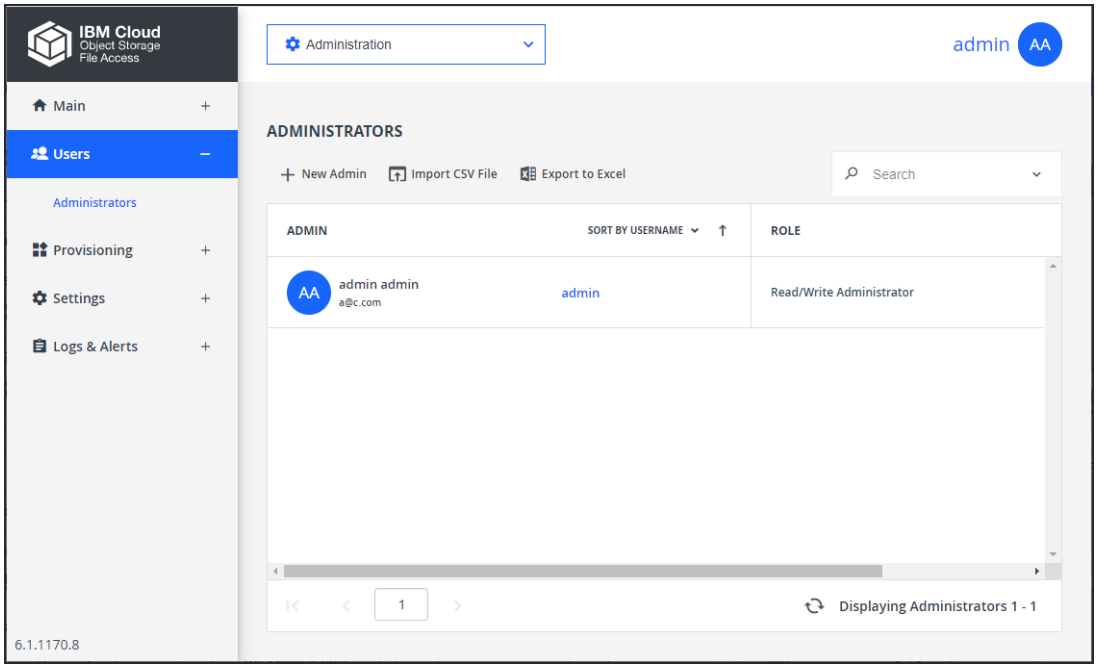
Global administrators must be defined locally.

In this chapter

VIEWING GLOBAL ADMINISTRATORS

To view all global administrators:

1 In the global administration view, select **Users > Administrators** in the navigation pane. The **ADMINISTRATORS** page is displayed.



The following information is displayed for each administrator:

ADMIN – The administrator's first and last names.

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

Username – The administrator's user name.

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

ROLE – The administrator's role: Read/write administrator, read only administrator or support.

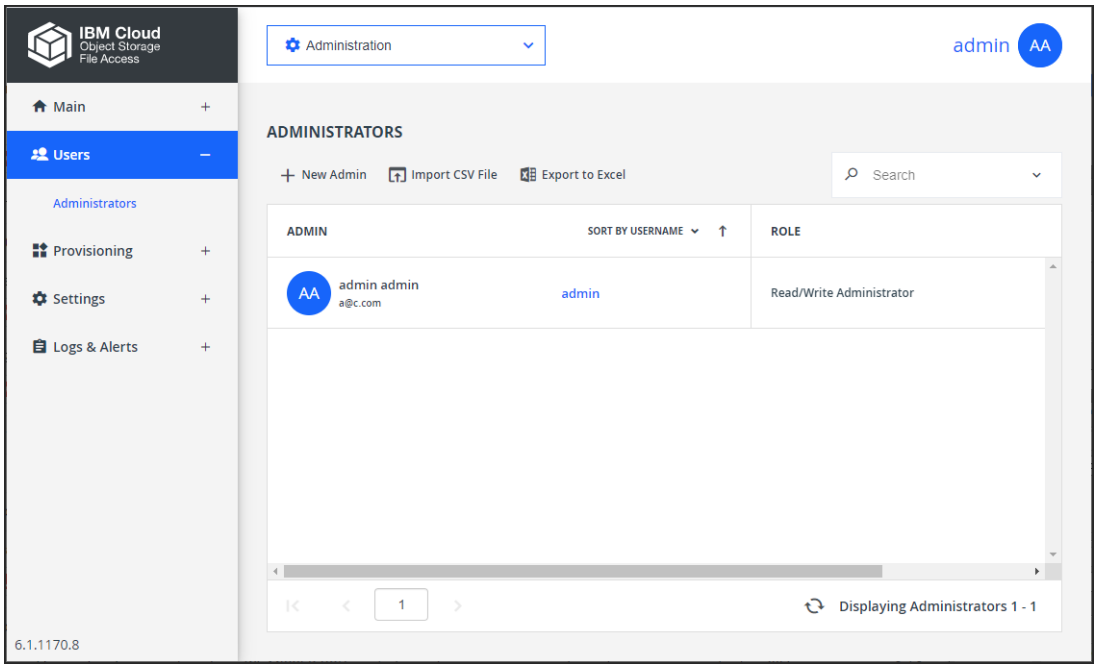
ADDING AND EDITING GLOBAL ADMINISTRATORS

You can create an administrator and then configure what events and alerts you want to receive to the administrator email.

Note: You can also import administrators from Active Directory. For details, see Using Directory Services To Import Users.

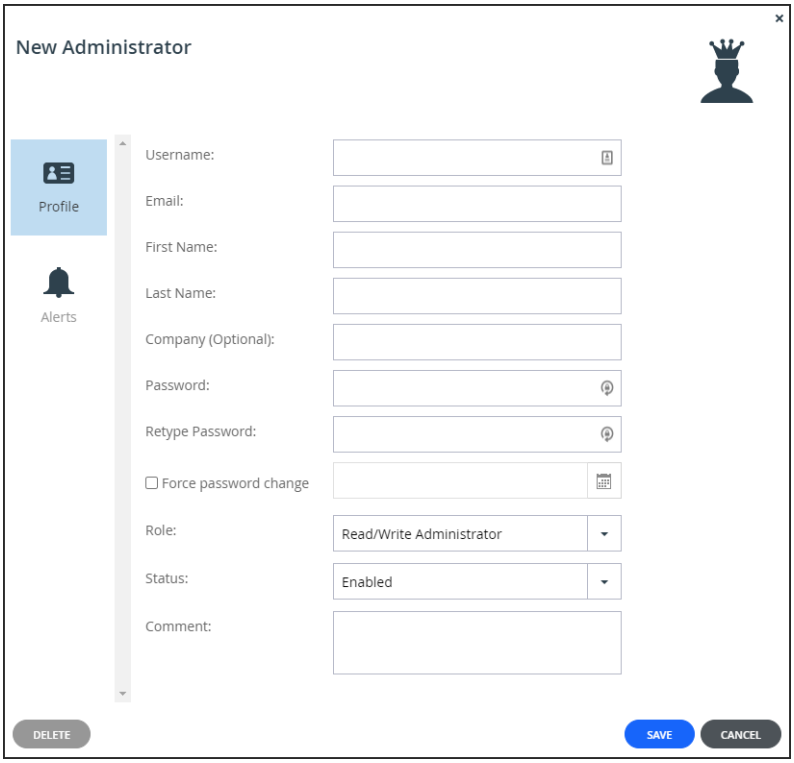
To add or edit a global administrator:

1 In the global administration view, select **Users > Administrators** in the navigation pane.
The **ADMINISTRATORS** page is displayed.



2 Either,

- Add an administrator, click **New Admin**.
The **New Administrator** window is displayed.



Or,

- Edit an existing administrator, click the administrator's name**.** The administrator window is displayed with the username of the administrator as the window title and account details: The creation date of the account and the last login.

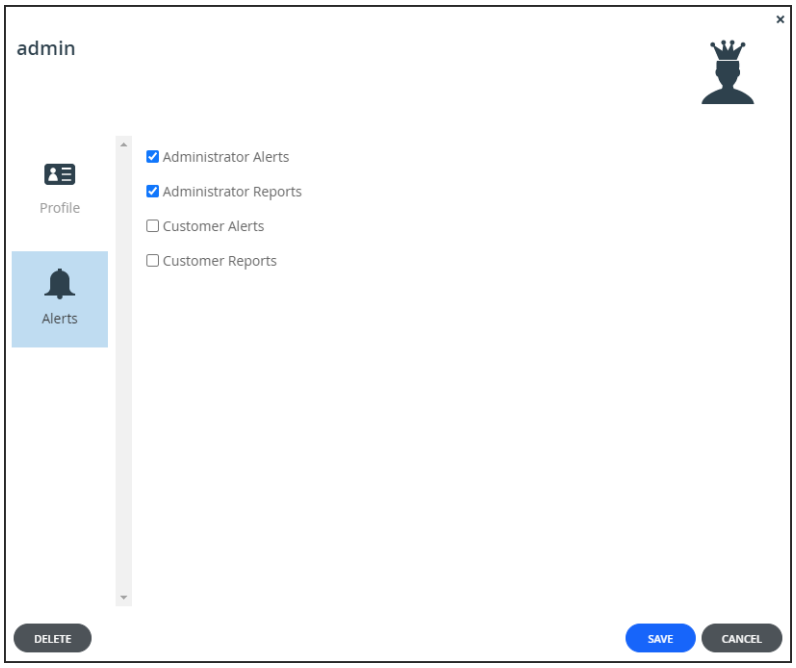
3 Enter the **Profile** details:
Username – A user name for the administrator.
Email – The administrator's email address.
First Name – The administrator's first name.
Last Name – The administrator's last name.
Company (Optional) – The name of the administrator's company.
Password – A password for the administrator. By default, the password must be at least 7 characters long. The minimum password length can be changed. See Administrators Password Policy.
Retype Password – Retype the password.
Force password change – To specify an expiration date for the administrator's password. When the password has expired, the administrator must specify a new password on the next login.
Role – Specify the administrator's role. IBM COS FA Portal includes built-in global administrator roles:

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.
Note: You can customize these roles, adding or removing permissions as described in Customizing Administrator Roles.

Status – The administrator status.
Enabled – The account is enabled, and the administrator can access the IBM COS FA Portal.
Disabled – The account is disabled, and the administrator cannot access the IBM COS FA Portal.

The default value for new administrators is *Enabled*.
Note: The currently logged in administrator cannot be disabled.
Comment – A description of the administrator.

4 Optionally, select the **Alerts** option.



5 Check the types of alerts to receive:
Administrator Alerts – Notifications about portal-level problems.
Administrator Reports – Notifications reporting portal-level activity.
Customer Alerts – Notifications about device-level problems.
Customer Reports – Notifications about customer activity.

6 Click **SAVE**.

DELETING GLOBAL ADMINISTRATORS

To delete a global administrator:

1 In the global administration view, select **Users > Administrators** in the navigation pane.
The **ADMINISTRATORS** page is displayed.

2 Either,

a Select the administrator to delete and click **Delete Administrator**.
A confirmation window is displayed.

b Click **DELETE ADMINISTRATOR** to confirm.

Or,

a Click any of the **ADMIN** values: First and last name, email address, or username.
The administrator window is displayed with the username of the administrator as the window title.

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

c Click **YES** to confirm.

The administrator is deleted.

EXPORTING GLOBAL ADMINISTRATORS TO AN EXCEL FILE

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

To export the list of administrators to an Excel file:

1. In the global administration view, select **Users > Administrators** in the navigation pane.
   The **ADMINISTRATORS** page is displayed.
2. Click **Export to Excel**.

The administrator list is downloaded to your computer.

IMPORTING GLOBAL ADMINISTRATORS FROM A FILE

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

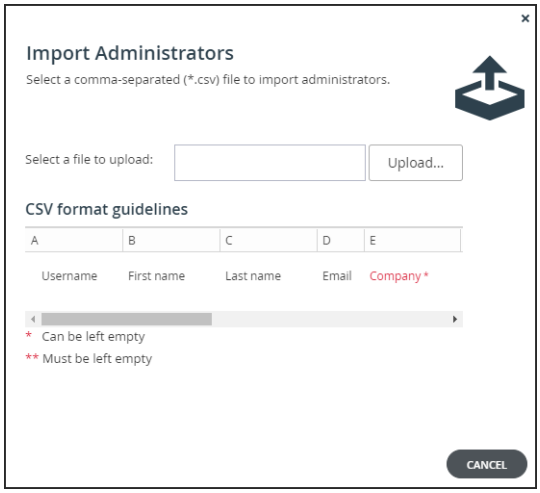
The *.csv file's columns must be in the following order:

1. Username
2. First name
3. Last name
4. Email address
5. Company (Optional)
6. Password
7. Role
8. – (this column must not contain a value)
9. – (this column must not contain a value)
10. – (this column must not contain a value)
11. Comment (Optional)
12. Status (Optional)

Optional fields can be left blank.

To import administrators from a *.csv file:

1. In the global administration view, select **Users > Administrators** in the navigation pane.
   The **ADMINISTRATORS** page is displayed.
2. Click **Import CSV File**.
   The **Import Administrators** window is displayed.



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

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

5 Click **FINISH**.

CUSTOMIZING ADMINISTRATOR ROLES

IBM COS FA Portal includes the following roles for global 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.

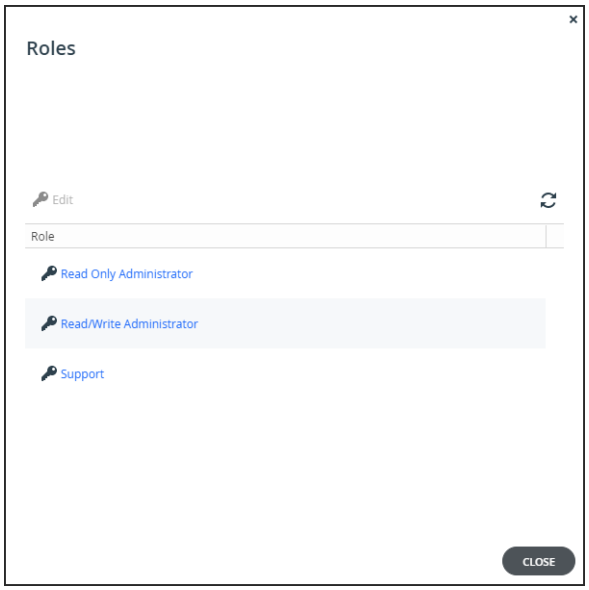
You can customize these roles, adding or removing permissions.

To customize an administrator role:

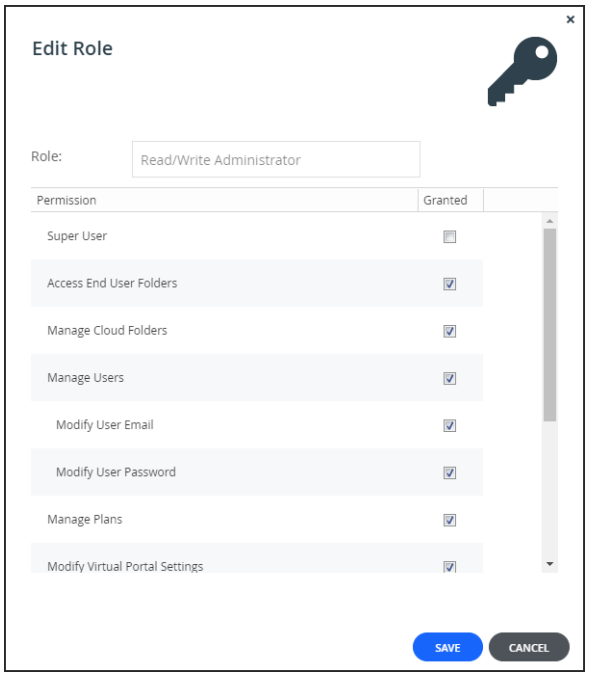
1 In the global administration view, select **Settings** in the navigation pane.
The **Control Panel** page is displayed.

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

The **Roles** window is displayed.



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



4 Check the permissions you want to include in the role, and uncheck those that you don't want to include.
Super User – Give all permissions to administrators.
Access End User Folders – Allow administrators to access and modify end user files and 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 remove, rename and change the owner of cloud folders.

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.

Manage Log Settings – Allow administrators to access the log settings.

5 Click **SAVE**.

Permissions Available to Roles

The different administrator roles have different permissions.

Permission	Read/Write Administrator	Read Only Administrator	Support
Super User	Yes	No	No
Access End User Folders	Yes	Yes	Yes (Default is No)
Manage Cloud 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)
Allow Single Sign On to Devices	Yes	Yes (Default is No)	Yes (Default is No)

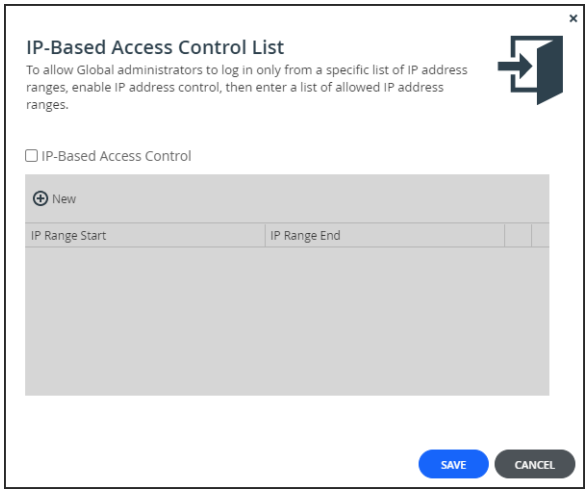
CONFIGURING AN IP-BASED ACCESS CONTROL LIST

You can configure an IP-based access control list, specifying the IP address ranges from which administrators can access the IBM COS FA Portal interface.

To configure an IP-based access control list:

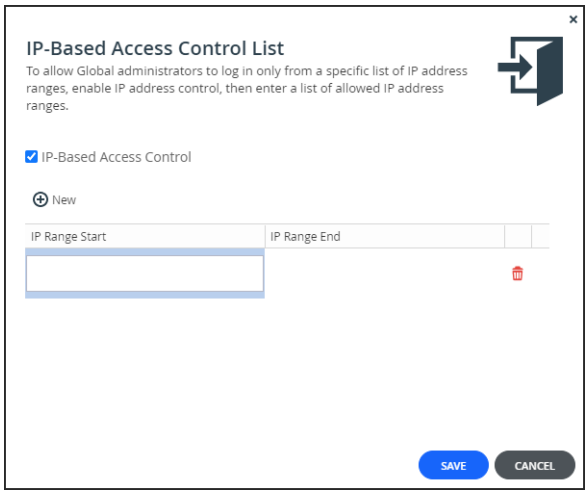
1 In the global administration view, select **Settings** in the navigation pane.
The **Control Panel** page is displayed.

2 Select **Global Administrators Access Control**, under **USERS** in the **Control Panel** page.
The **IP-Based Access Control List** window is displayed.



3 Check the **IP-Based Access Control** box.
The list box is enabled.

4 Click **New** to add an IP address range from which access to the IBM COS FA Portal interface is allowed.
A new row is added to the list box.



5 Click in the **IP Range Start** field, and enter the start IP address.

6 Click in the **IP Range End** field, and enter the end IP address.

Note: To remove an IP address range, in the IP address range's row, click . The IP address range is removed.

7 Click **SAVE**.

CHAPTER 4. MANAGING THE IBM COS FA PORTAL LICENSE

The IBM COS FA Portal license limits the number of IBM COS FA Gateway licenses and Cloud Drive licenses, that can be provisioned throughout the IBM COS FA Portal.

When a IBM COS FA Portal license is about to expire, notifications appear on the notifications page of IBM COS FA Portal's administration interface, and emails are sent to the IBM COS FA Portal administrators. If the IBM COS FA Portal license expires, the IBM COS FA Portal continues to function but adding new devices is disabled.

In this chapter

HOW THE IBM COS FA PORTAL LICENSE WORKS

The IBM COS FA Portal license specifies license quotas for each of the following:

- **IBM COS FA Portal License**
  The amount of storage allowed, in blocks of 50TB.
- **IBM COS FA Gateway Licenses**
  The number of IBM COS FA Gateway licenses that can be provisioned. An IBM COS FA Gateway license is consumed by an IBM COS FA Gateway connected to a IBM COS FA Portal user account.
- **IBM Cloud Drive Licenses**
  The number of Cloud Drive licenses that can be provisioned. Each IBM Cloud Drive license enables use of the Cloud Drive service for a single user account.

The license is subdivided when you allocate quotas to virtual IBM COS FA Portals, by assigning the virtual IBM COS FA Portals to global plans.

With each virtual IBM COS FA Portal, the IBM COS FA Portal license can be further subdivided.

TEAM IBM COS FA PORTALS LICENSES

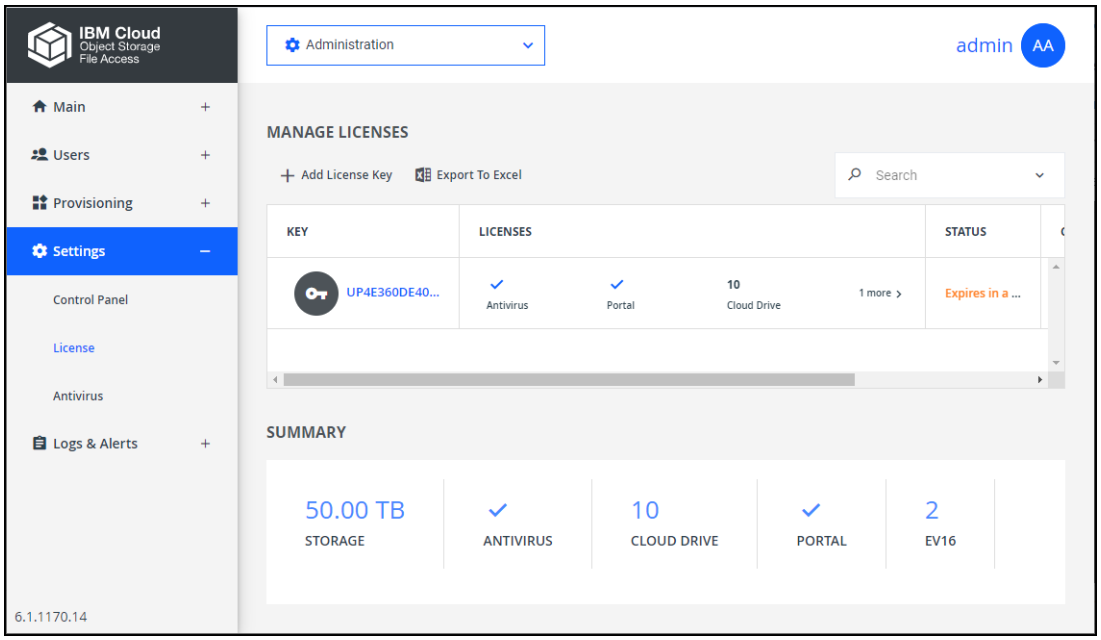
Any licenses provisioned to a specific team IBM COS FA Portal are immediately consumed from the IBM COS FA Portal license.

The number of licenses in use must be less than or equal to the number provisioned for the team IBM COS FA Portal. The number provisioned for the team IBM COS FA Portal is the limit for that IBM COS FA Portal.

VIEWING IBM COS FA PORTAL LICENSE INFORMATION

To view IBM COS FA Portal **license information:**

1 In the global administration view, select **Settings > License** in the navigation pane.
The **MANAGE LICENSES** page is displayed.



The following information is displayed for each license:

KEY– The license key.

LICENSES – The license details.

Antivirus – The license includes the antivirus service.

Cloud Drive – The number of cloud drive licenses included in the license key. Cloud drive licenses are per IBM COS FA Portal user.

Portal – The IBM COS FA Portal license is operational or not.

EV16 – The number of IBM COS FA Gateway licenses included in the license key. You can have as many IBM COS FA Gateways in the IBM COS FA Portal as you have licenses.

STATUS – The license key's status.

OK – The license is current.

Expired on *date* – The license expired on the specified date.

Expires in *X* **days** – The license will expire *X* days from now.

COMMENTS– Any comment about the license key.

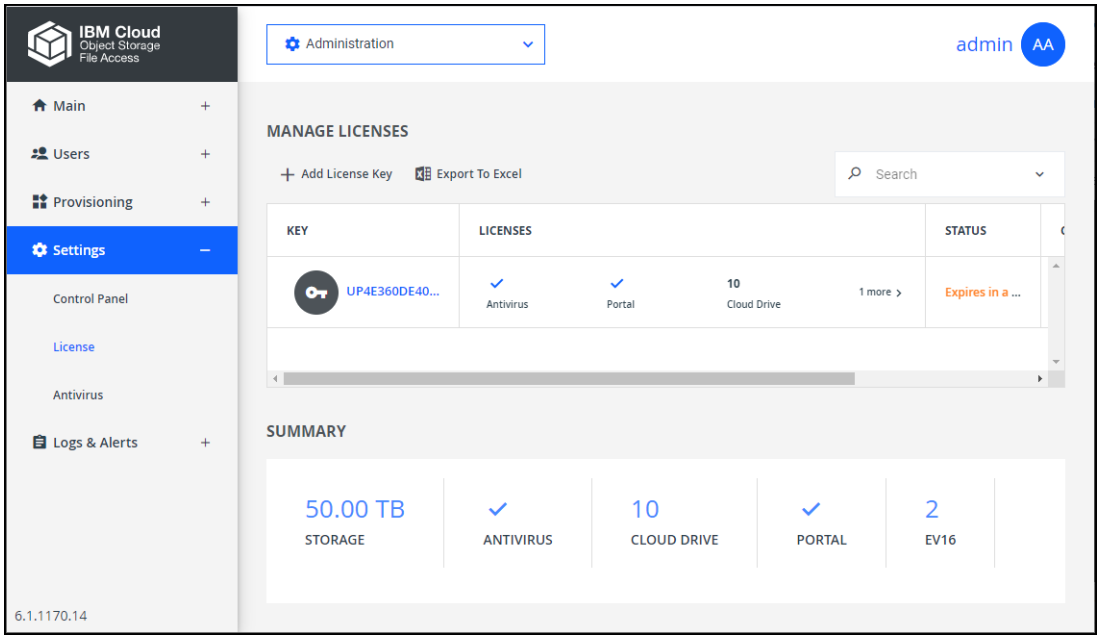
ADDING LICENSE KEYS

As a prerequisite, you must purchase a license key from IBM, specifying your IBM COS FA Portal's DNS suffix, and the number of required IBM COS FA Gateway licenses. You receive one or more license keys.

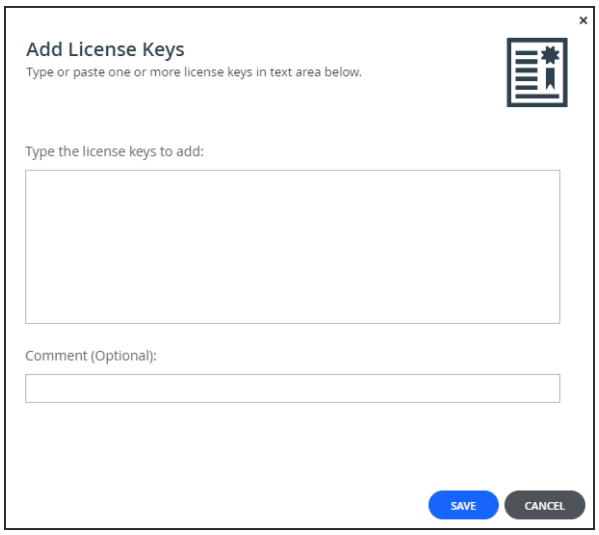
Note: You can view your IBM COS FA Portal's DNS suffix, in the global administration view's **Settings > Control Panel > Global Settings** page. This DNS suffix was set up when you installed the IBM COS FA Portal, as described in the installation guide for your environment.

To add a license key:

1 In the global administration view, select **Settings > License** in the navigation pane.
The **MANAGE LICENSES** page is displayed.



2 Click **Add license key**.
The **Add License Keys** window opens.



3 Copy the license key you received from IBM, and paste it into the text box.
To add more than one key, paste each key on a new line.
The system verifies and activates the license keys by contacting the IBM Activation service. As each license key is activated, it is associated with this installation of IBM COS FA Portal.

4 Optionally add a comment in the **Comment** field. The comment is displayed in the **MANAGE LICENSES** page.

Note: You can use this comment to document information such as the purchase order number associated with the license.

5 Click **SAVE**.

ADDING OR EDITING A COMMENT FOR A LICENSE

To add or edit a license comment:

1 In the global administration view, select **Settings > License** in the navigation pane.
The **MANAGE LICENSES** page is displayed.

2 Click the license key.
The **Edit License Comment** window is displayed.

3 Change the contents of the **Comment** t field.

4 Click **SAVE**.

REMOVING LICENSE KEYS

To remove a license key:

1 In the global administration view, select **Settings > License** in the navigation pane.
The **MANAGE LICENSES** page is displayed.

2 Select the license key and click **Delete License**.
A confirmation window is displayed.

3 Click **DELETE LICENSE**.
The license key is deleted.

EXPORTING LICENSE KEYS TO EXCEL

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

To export license keys:

1 In the global administration view, select **Settings > License** in the navigation pane.
The **MANAGE LICENSES** page is displayed.

2 Click **Export to Excel**.
The details of the license keys are exported to your computer.

CHAPTER 5. MANAGING CERTIFICATES

Certificates are used as part of the Transport Level Security (TLS) protocol. They enable using Web browsers, IBM COS FA Gateways to verify that the IBM COS FA Portal server with which they are communicating is authentic and not spoofed.

If the IBM COS FA Portal does not have a valid certificate installed, a warning is displayed to the end user when logging a device into the IBM COS FA Portal, offering the option to proceed anyway.

This warning dialog is presented every time a user connects a device to the IBM COS FA Portal, until a valid certificate is installed.

A valid SSL certificate must meet the following requirements:

- If multiple virtual IBM COS FA Portals are configured, then each virtual IBM COS FA Portal has its own DNS name. In this case, the SSL certificate should be a wildcard certificate, that is, the DNS name embedded in the certificate should start with "*". For example, if the IBM COS FA Portal's DNS suffix is *myportal.com*, and there are two virtual IBM COS FA Portals, *portal1.myportal.com* and *portal2.myportal.com*, you need a wildcard certificate for *.*myportal.com*.
- If you have only one IBM COS FA Portal, and do not intend to configure multiple virtual IBM COS FA Portals, then a regular SSL certificate is preferable and not a wildcard certificate. For example, if your IBM COS FA Portal's DNS name is *portal1.myportal.com*, then you need a certificate for *portal1.myportal.com*.
- It is possible to specify multiple alternative names, using the `subjectAltName` certificate extension.
- The certificate must in *.zip format and contain certificate files in *.pem format.

You can automatically generate a certificate request to send to any public SSL certificate authority, such as Godaddy, recommended by IBM, Verisign, or Thawte, as described in Generate a Certificate Signing Request. Once you have received a certificate from the certificate authority, you must the install it, as described in Install the Signed Certificate on IBM COS FA Portal.

Alternatively, you can export a certificate from another IBM COS FA Portal, described in Exporting the Installed SSL Certificate, and install it on this IBM COS FA Portal, described in Importing an SSL Certificate.

Note: When generating a certificate request and installing the received certificate, the private key is generated on the IBM COS FA Portal and never leaves it. In contrast, when exporting and importing certificates, the private key is exported and imported along with the certificate, and it is therefore important to keep the exported file confidential.

In this chapter

INSTALLING AN SSL CERTIFICATE

Perform the following steps to install a certificate on IBM COS FA Portal:

1 Note the IBM COS FA Portal's DNS Suffix.

2 Obtain an SSL Certificate.

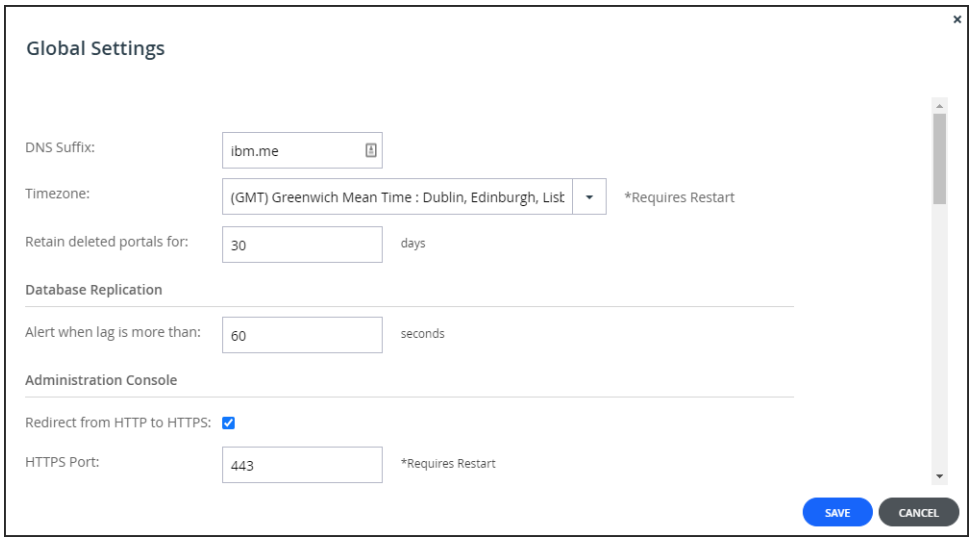
3 Generate a Certificate Signing Request.
4 Sign the Certificate Request.
5 Validate and Prepare Certificates for Upload.
6 Install the Signed Certificate on IBM COS FA Portal.

Note the IBM COS FA Portal's DNS Suffix

You need the IBM COS FA Portal's DNS suffix for use in later steps.

To view your IBM COS FA Portal's DNS suffix:

1 In the global administration view, select **Settings** in the navigation pane.
The **Control Panel** page is displayed.
2 Select **Global Settings**, under **SETTINGS** in the **Control Panel** page.
The **Global Settings** window is displayed.



3 Note the IBM COS FA Portal's DNS Suffix in the **DNS Suffix** field.

Obtain an SSL Certificate

It is necessary to obtain a valid certificate signed either by a well-known certificate authority, or by your own internal certificate authority.

Note: If you intend to generate a signed certificate using your own internal certificate authority, contact IBM Support beforehand.

The SSL certificate can be either of the following:

- **A wildcard certificate**
A wildcard SSL certificate secures your website URL and an unlimited number of its subdomains. For example, a single wildcard certificate for `*.ibm.com` can secure both `company01.ibm.com` and `company02.ibm.com`, which may be for virtual IBM COS FA Portals *company01* and *company02*.
A wildcard certificate is mandatory if you plan for your service to consist of more than one virtual IBM COS FA Portal.
- **A domain certificate**
A domain certificate secures a single domain or subdomain only. For example: `company01.ibm.com`.
This option is relevant if you are planning to provision a single virtual IBM COS FA Portal only.

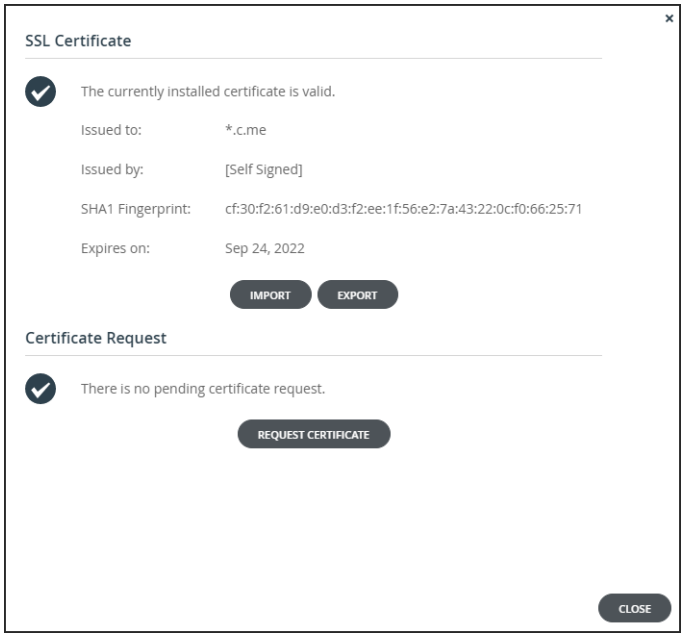
Note: To obtain a self-signed certificate for testing and evaluation purposes only, contact IBM Support and specify your IBM COS FA Portal's DNS suffix see Note the IBM COS FA Portal's DNS Suffix. IBM will generate a self-signed certificate for your DNS suffix and provide you with a ZIP file that you can upload to your IBM COS FA Portal environment.
IBM COS FA Portal also supports certificates with Subject Alternative Names: SAN certificates. This option enables you to secure multiple domain names with a single certificate.

Generate a Certificate Signing Request

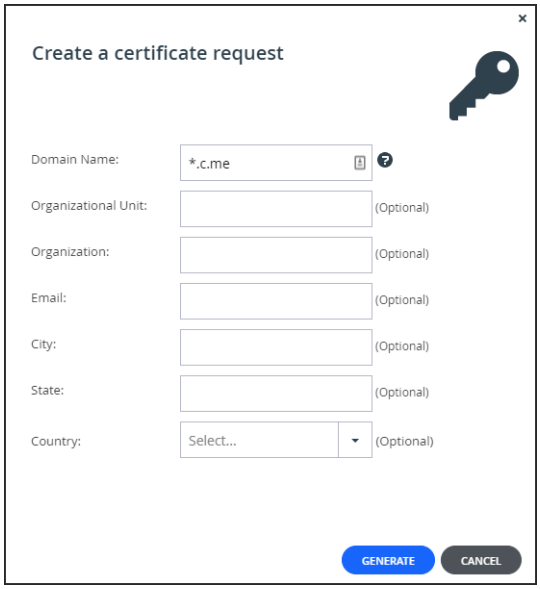
You need to generate a certificate signing request, CSR, for your domain.

To generate a certificate signing request for your domain:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.
2. Select **SSL Certificate** under **SETTINGS** in the **Control Panel** page.
   The **SSL Certificate** window is displayed.



3. Click **REQUEST CERTIFICATE**.
   The **Create a certificate request** window is displayed.



4 In the **Domain Name** field, enter the domain name for which you want to request a certificate.
The value entered must match the type of certificate you chose to use. For example, if you chose a wildcard certificate, the domain name might be `*.example.com`.
If you chose a domain certificate, the domain name might be `company01.example.com`, where `company01` is the name of your virtual IBM COS FA Portal.
If multiple virtual IBM COS FA Portals are configured, each virtual IBM COS FA Portal has its own DNS name. In this case, the SSL certificate should be a wildcard certificate with an asterisk before the DNS suffix, for example, `*.example.com`.
If you have only one IBM COS FA Portal, and do not intended to configure multiple virtual IBM COS FA Portals, then use a regular SSL certificate and not a wildcard certificate.
To request a certificate that specifies multiple alternative names, type the multiple names in this field, separated by semicolons. The certificate will include the `subjectAltName` certificate extension.

5 Optionally, specify the following:
Organizational Unit – The name of your organizational unit.
Organization – The name of your organization.
Email – Your email address.
City – Your city.
State – Your state.
Country – Your country.

6 Click **GENERATE**.
A keypair is generated and stored on the IBM COS FA Portal.
The **Download a certificate request** window is displayed.

7 Click **DOWNLOAD**.
The certificate request file `certificate.req` is downloaded to your computer.
The **Certificate Request** area of the **SSL Certificate** window indicates that the certificate request is pending.

Warning: **When you generate a CSR, a `private.key` file is registered in the IBM COS FA Portal. If you now generate a *new* CSR, it will override the existing `private.key` file, and signing the *old* CSR will result in an error message indicating that the CSR does not match the `private.key` file. Therefore, do not generate a new CSR before installing the signed certificate.**

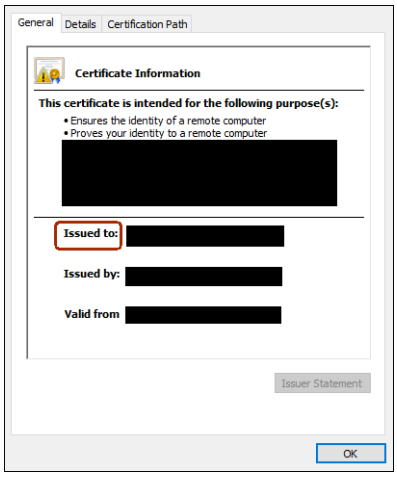
Sign the Certificate Request

To sign the certificate request:

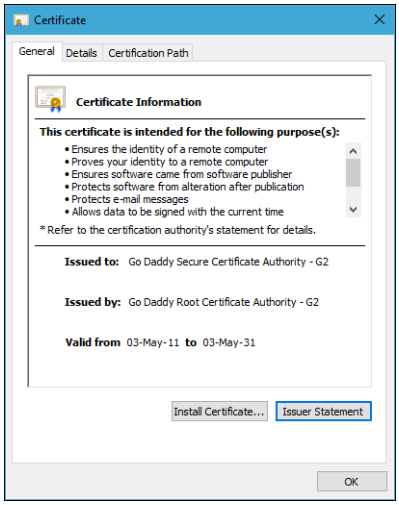
1 Send the certificate.req file you generated to your certificate authority for signing.
If the request is successful, the certificate authority will send back an identity certificate that is digitally signed with the certificate authority's private key.

Note: The certificate authority must return a **base-64** encoded identity certificate.

2 Open the identity certificate and verify that the **Issued to** field includes the DNS you provided upon creating the certificate request.



3 Build a certification chain from your identity certificate to your trusted root certificate.
You need to obtain all of the intermediate certificates, as well as your root certificate authority's self-signed certificate.
If you are using a well-known certificate authority, the intermediate certificates and the root certificate authority's self-signed certificate can be downloaded from your certificate authority website. If you are using your own internal certificate authority, contact the necessary entity to provide you with the required intermediate and self-signed certificate.
In the above example, the certificate was issued by **Go Daddy Secure Certification Authority** to ***.ibm.me**. To build the certification chain, obtain a certificate issued to **Go Daddy Secure Certification Authority**.



To continue the certification chain, you must obtain a certificate issued to the same authority that

the previous certificate was issued by. You continue the chain until the certification chain is complete, with the last certificate, which is a self-signed certificate, issued to and by the same entity.

Validate and Prepare Certificates for Upload

To validate and prepare certificates for upload:

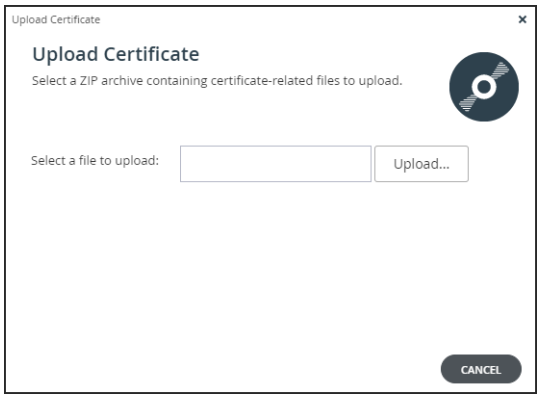
1. Verify that none of the certificates in the certificate chain are corrupted or using invalid encoding. To do so, open each certificate in a program such as Notepad or Word, and verify that it contains the following:
   `-----BEGIN CERTIFICATE-----`
   `...certificate_content...`
   `-----END CERTIFICATE-----`
2. Change the identity certificate issued to `*.ibm.me` to `certificate.crt`.
3. Change the file extension of the other certificates in the certificate chain to `crt`.
   For example, `certificate-name.crt`.
4. Archive all of the certificates, the identity certificate, the intermediary certificates, and the root self-signed certificate, in a ZIP file called `certificate.zip`.

Install the Signed Certificate on IBM COS FA Portal

Once you have obtained an SSL certificate you must install it on IBM COS FA Portal. The certificate must match the pending certificate request and keypair.

To install an SSL certificate:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.
2. Select **SSL Certificate** under **SETTINGS** in the **Control Panel** page.
   The **SSL Certificate** window is displayed.
   The **Certificate Request** area of the **SSL Certificate** window **i**ndicates that the certificate request is pending.
3. Click **INSTALL SIGNED CERTIFICATE** in the **Certificate Request** area of the **SSL Certificate** window.
   The **Upload Certificate** window is displayed.



4. Click **Upload** and browse to the `certificate.zip` file you created. All the certificates in the certificate chain must be in the ZIP file in X.509 format, and each file must have a *.crt* extension. The certificate is installed on IBM COS FA Portal.
5. Click **Open** and then **FINISH**.
6. Restart all the IBM COS FA Portal servers via the **Main > Servers** page. See Restarting and Shutting Down a Server. You can start the servers in any order.

7 Open the IBM COS FA Portal.
If the certificate update was successful, there won't be any security exceptions.

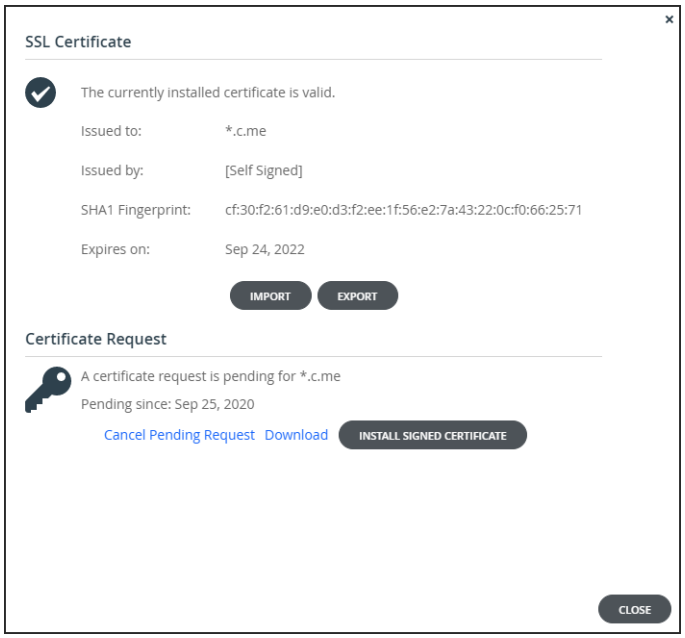
CANCELING A PENDING CERTIFICATE REQUEST

In order to make changes to the current certificate request, you must cancel it and then generate a new request as described in Generate a Certificate Signing Request.

To cancel a pending certificate request:

1 In the global administration view, select **Settings** in the navigation pane.
The **Control Panel** page is displayed.

2 Select **SSL Certificate** under **SETTINGS** in the **Control Panel** page.
The **SSL Certificate** window is displayed.



3 Click **Cancel Pending Request**.
A confirmation window is displayed.

4 Click **YES**.
The pending certificate request is canceled.

EXPORTING THE INSTALLED SSL CERTIFICATE

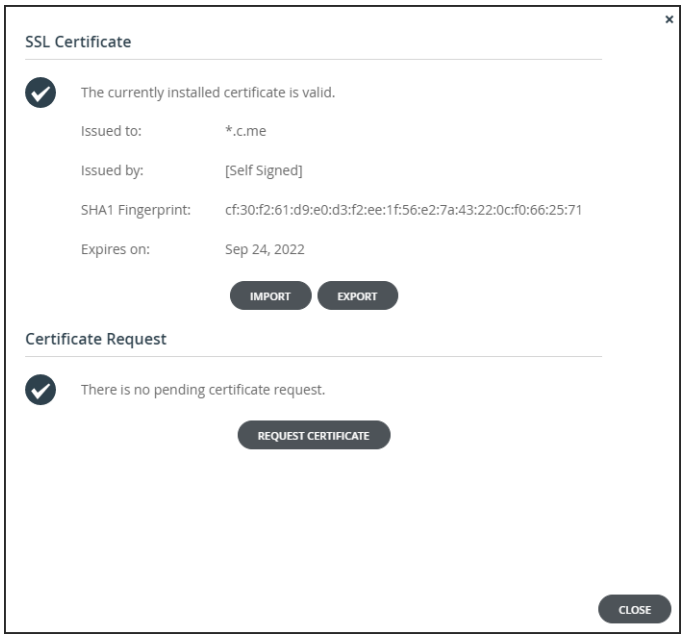
You can export the installed SSL certificate chain together with the corresponding private key.

To export the installed SSL certificate:

1 In the global administration view, select **Settings** in the navigation pane.
The **Control Panel** page is displayed.

2 Select **SSL Certificate** under **SETTINGS** in the **Control Panel** page.

The **SSL Certificate** window is displayed.



3 Click **EXPORT**.
A ZIP file, including the certificate and private key, is downloaded to your computer.

Warning: **This file is security sensitive, and sending it over an insecure link may enable the server to be compromised.**

IMPORTING AN SSL CERTIFICATE

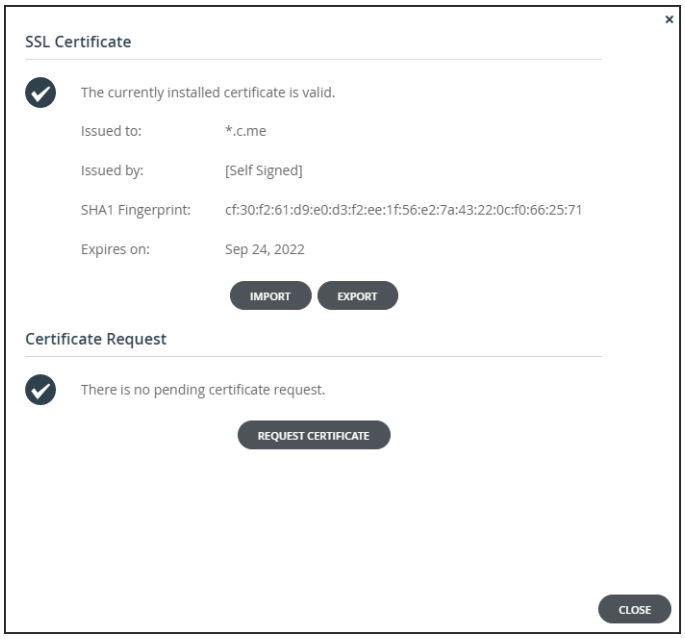
You can import an SSL certificate from another IBM COS FA Portal, including the private key.

To import an SSL certificate:

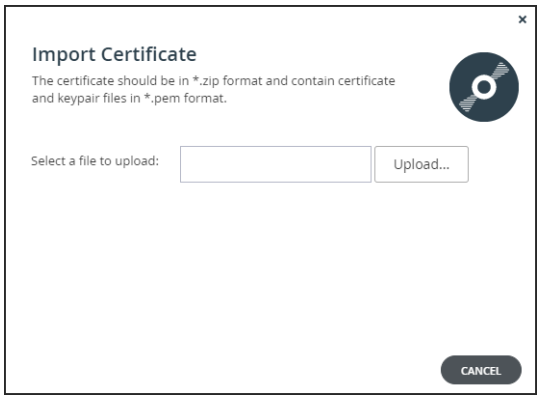
1 In the global administration view, select **Settings** in the navigation pane.
The Control Panel page is displayed.

2 Select **SSL Certificate** under **SETTINGS** in the **Control Panel** page.

The **SSL Certificate** window is displayed.



3 Click **IMPORT**.
The **Import Certificate** window is displayed.



4 Click **Upload** and browse to the ZIP file containing the certificate components.
5 Click **Open** and then **FINISH**.

CHAPTER 6. MANAGING STORAGE NODES

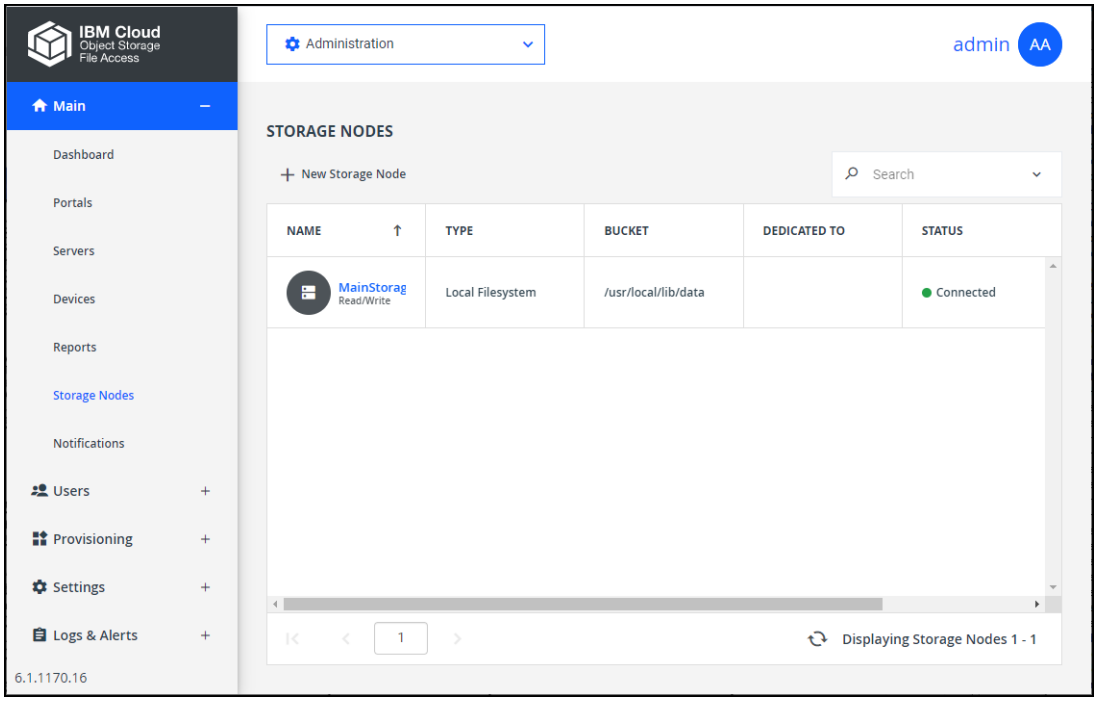
IBM COS FA Portal can write your data to IBM COS storage nodes. The Storage Nodes page in the Global Administration view enables you to easily add new storage nodes, dedicate storage nodes to virtual IBM COS FA Portals, stop and start writing to different storage nodes, and migrate data seamlessly from a storage node to other storage nodes.

In this chapter

VIEWING STORAGE NODES

To view all storage nodes in the system:

- In the global administration view, select **Main > Storage Nodes** in the navigation pane. The **STORAGE NODES** page is displayed.



The following information is displayed for each storage node:

NAME – The storage node's name.

Status (under the name) – Whether the storage node is read/write enabled or read and delete only.

TYPE – The storage node's type.

BUCKET – The name of the storage node's bucket.

DEDICATED TO – The name of a single virtual IBM COS FA Portal to which the storage node is

dedicated, if applicable.

STATUS – The storage node's current status. This can be either of the following:

- Connected
- Not Connected

The IBM COS FA Portal does not attempt to store new blocks in storage nodes that are not connected.

STORAGE USAGE – The amount of storage available, followed by the amount of used storage. This field is only relevant for the **Local Filesystem** storage node, which is the default storage node when setting up the IBM COS FA Portal.

Note: You cannot use **Local Filesystem** storage node for storage that exceeds 20TB.

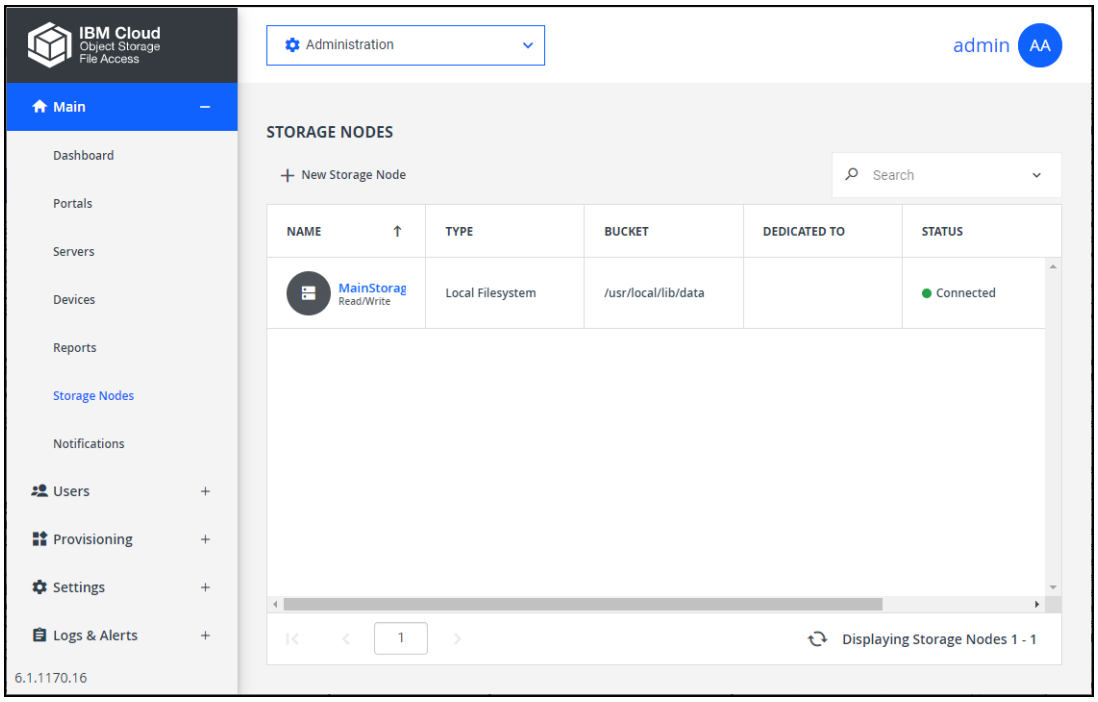
To view details of a specific node:

- Click the node name on the **STORAGE NODES** page.
  The storage node window is displayed with the storage node name as the window title.

ADDING AND EDITING STORAGE NODES

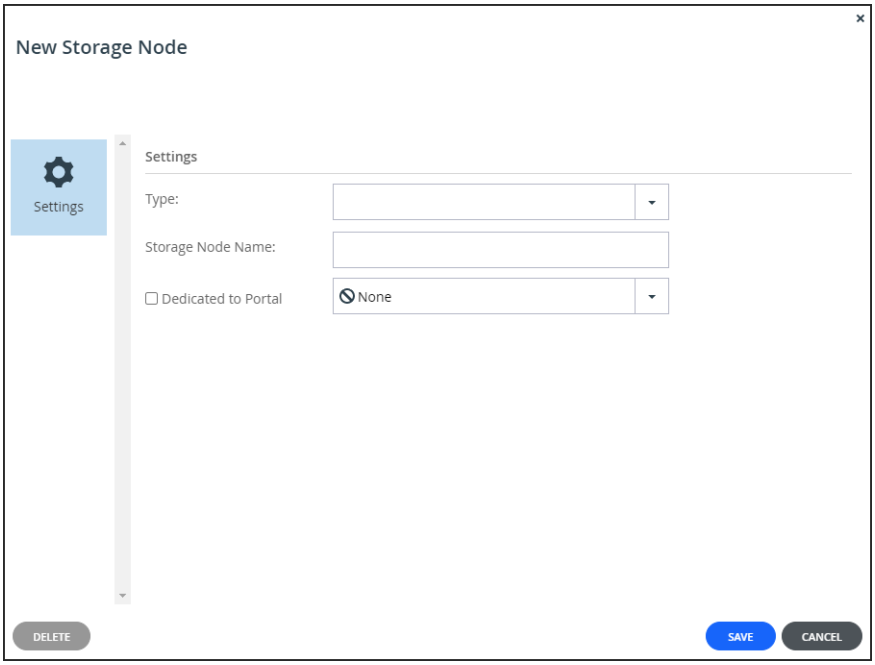
To add or edit a storage node:

1 In the global administration view, select **Main > Storage Nodes** in the navigation pane.
The **STORAGE NODES** page is displayed.



2 Either,

- Add a storage node, click **New Storage Node**.
  The **New Storage Node** window is displayed.

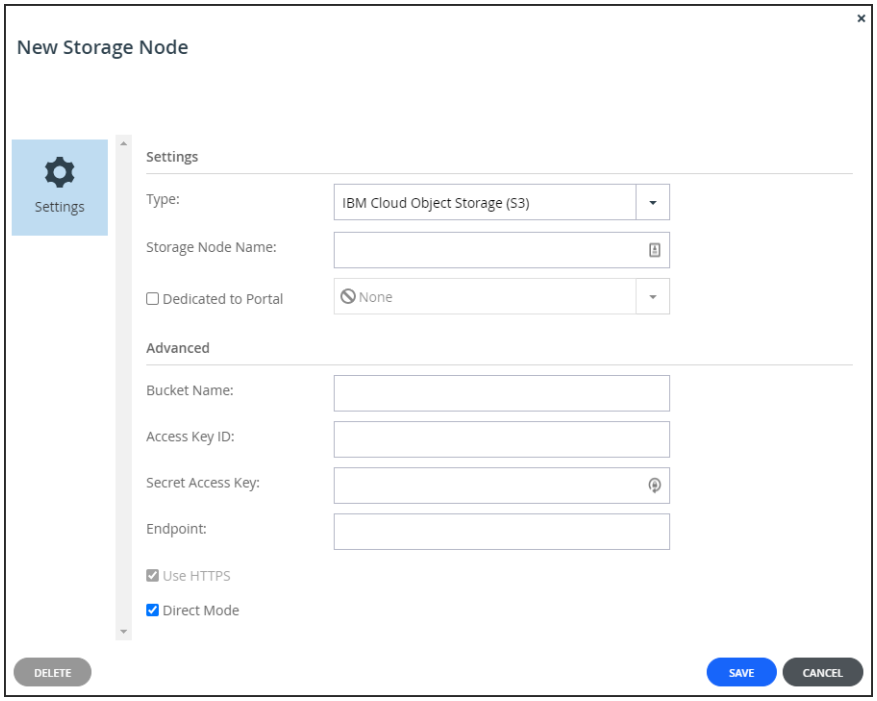


Or,

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

3 Enter the generic details for the storage node. These details are the same for every type of storage node.
Type – The type of storage node you are adding. When you select the type, more fields are displayed so that you can add the specific details for the type, as described in step 4.
Storage Node Name – A unique name to identify the storage node.
Dedicated to Portal – Dedicate the storage node to one virtual IBM COS FA Portal selected from the drop-down list.

4 Complete the additional fields that are displayed when you choose **IBM Cloud Object Storage (S3)**.

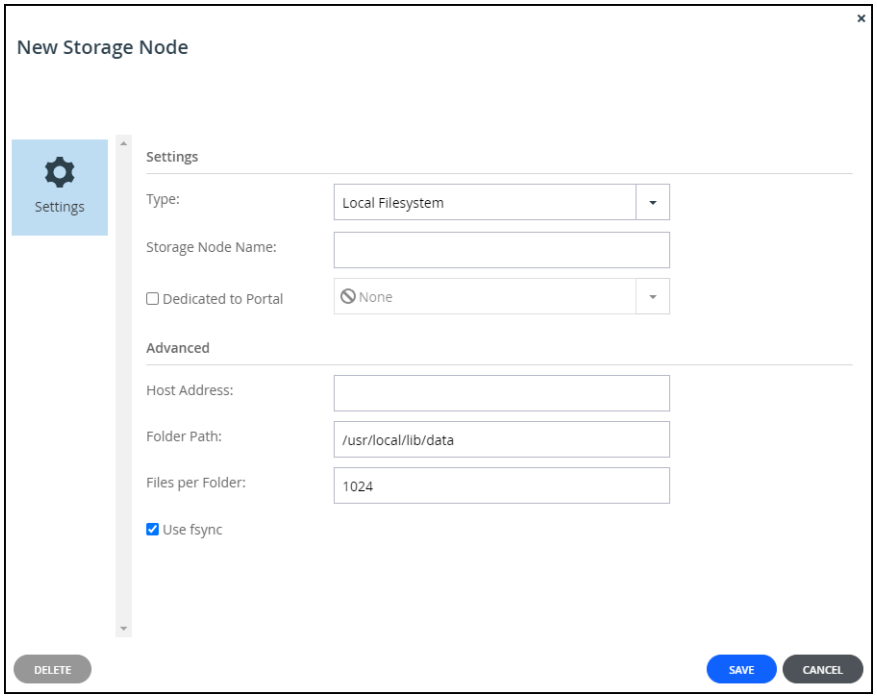


Bucket Name – The unique name of the IBM Cloud Object Storage bucket that you want to add as a storage node.
Access Key ID – The IBM Cloud Object Storage access key ID.
Secret Access Key – The IBM Cloud Object Storage secret access key.
Endpoint – The endpoint name of the IBM Cloud Object Storage service.
Use HTTPS – Use HTTPS to connect with the storage node.
Direct Mode – Data is uploaded directly to the storage node and not via the IBM COS FA Portal. IBM recommends keeping the default 4MB fixed block size. For details, see Default Settings for New Folder Groups.

Note: Both **Direct Mode** and **Use HTTPS** options are checked and cannot be unchecked.

5 Complete the additional fields that are displayed when you choose **Local Filesystem**.
The **Local Filesystem** storage node is the default storage node after installing IBM COS FA Portal.

Note: You cannot use **Local Filesystem** storage node for storage that exceeds 20TB.
When using a **Local Filesystem** storage node, data blocks are stored in a specific folder in the primary IBM COS FA Portal server's local file system.



Host Address – The host address of the primary server.
Folder Path – The path in where files should be stored in the local file system.
Files per Folder – The maximum number of files to store in a folder. The default value is 1024.
Use fsync – Blocks of data should be flushed to disk immediately. Using fsync prevents data loss in the event of a power failure.

6 Click **SAVE**.

ENABLING AND DISABLING WRITES TO A NODE

When you create a storage node, the node is by default in read/write mode.

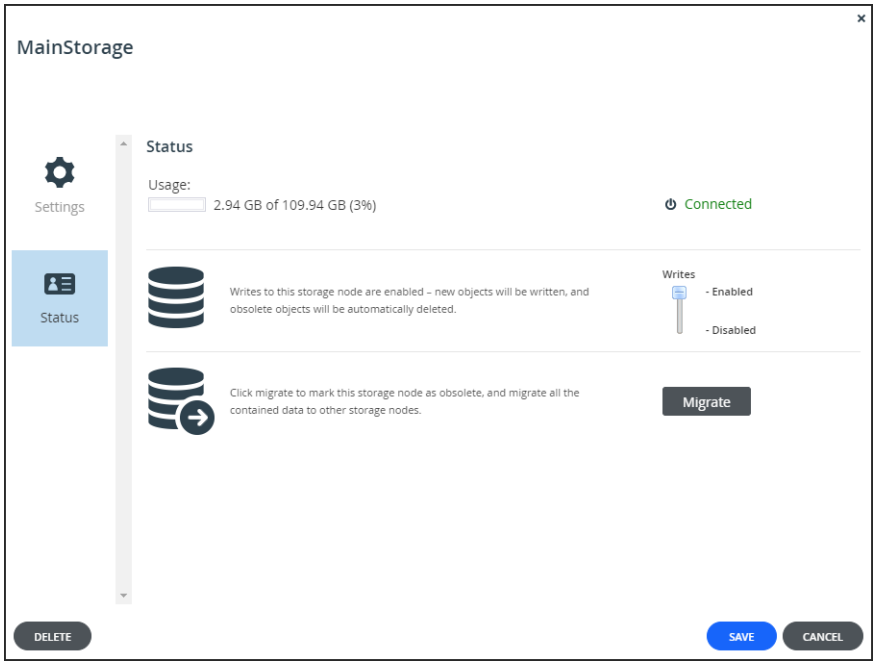
You can enable or disable writes to a storage node whenever needed, such as when you are about to replace a storage node and you want to stop new data blocks from being written to the node. While writes are disabled on a node, any new data blocks to be written are directed to other storage nodes that are write-enabled. Also, the node goes into read-delete mode, in which IBM COS FA Portal deletes any blocks on the node deemed to be no longer in use.

To enable or disable writes to a storage node:

1 In the global administration view, select **Main > Storage Nodes** in the navigation pane.
The **STORAGE NODES** page is displayed.

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

3 Select the **Status** option.



4 Slide the **Writes** bar to **Enabled** or **Disabled**.

MIGRATING STORAGE NODES

IBM COS FA Portal is a storage-agnostic platform that supports a variety of block and object storage vendors. By abstracting the backend storage using a software-defined storage architecture. IBM COS FA Portal can migrate data between storage nodes, including between on-premises and cloud storage block/object storage nodes. This helps you to manage and implement infrastructure changes, hardware retirement policies, and business objectives. The migration does not require down time, as it is performed in the background while the service remains fully operational. Users can continue to access data during the data migration process.

Migrating to Multiple Storage Nodes

If more than one storage node is connected to the IBM COS FA Portal, data is migrated to all the storage nodes connected at the time the migration is performed that are not defined as dedicated storage nodes and are write-enabled. For details about defining a storage node as write enabled, the default, see Enabling and Disabling Writes to a Node.

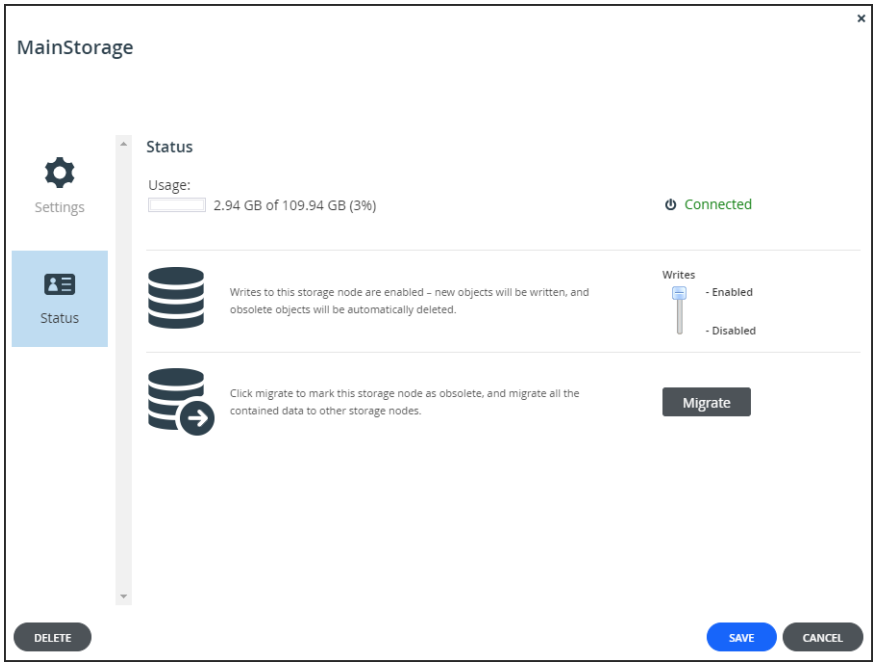
Migrating from a Dedicated Storage Node

If the source storage node is dedicated to a single virtual IBM COS FA Portal, its data is migrated **only** to other storage nodes that are dedicated to the same IBM COS FA Portal. If more than one dedicated storage node is connected to the IBM COS FA Portal, data is migrated to all the dedicated storage nodes connected at the time the migration is performed that are write-enabled. For details about defining a dedicated storage node, see Adding and Editing Storage Nodes.

The Migration Procedure

To migrate a storage node:

1. In the global administration view, select **Main > Storage Nodes** in the navigation pane.
   The **STORAGE NODES** page is displayed.
2. Click the storage node's name.
   The storage node window is displayed with the storage node name as the window title.
3. Select the **Status** option.



4. Click **Migrate**.
   A message is displayed, recommending contacting IBM support before starting the migration as the storage migration is an irreversible process.
5. If you have already contacted IBM Support and understand the implications of the migration, click **CONTINUE**, otherwise, click **CANCEL**.

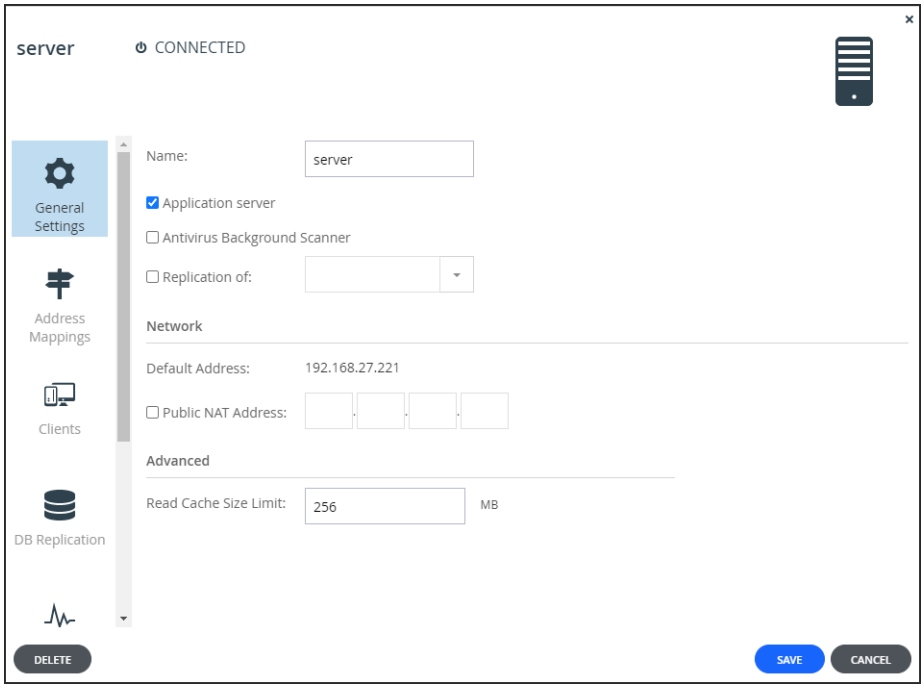
All of the data on the storage node is transferred to the other available write-enabled nodes.

Monitoring the Migration

The migration process can be monitored in the **Activity** tab of the server manager. To open the server manager, click the server's name in the **Main > Servers** page. Select the **Activity** tab.

To monitor a migration operation:

1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed.
2. Click the server hosting the storage node being migrated.
   The server window is displayed with the server name as the window title.



3 Click the **Activity** option and scroll down to the graphs displaying the migration operation:
- The amount of storage migration traffic, in KB/second.
  You can use this information together with the total storage that needs to be migrated, which is displayed in the storage node status option, to calculate approximately how long the migration will take to complete.
- The number of blocks migrated, in blocks/second.

DELETING A STORAGE NODE

To delete a storage node:

1 In the global administration view, select **Main > Storage Nodes** in the navigation pane.
The **STORAGE NODES** page is displayed.

2 Either,

a Select the storage node to delete and click **Delete**.
A confirmation window is displayed.

b Click **DELETE STORAGE** to confirm.

Or,

a Click the storage node name.
The storage node window is displayed with the storage node name as the window title.

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

c Click **YES** to confirm.

The storage node is deleted.

CHAPTER 7. CONFIGURING GLOBAL SETTINGS

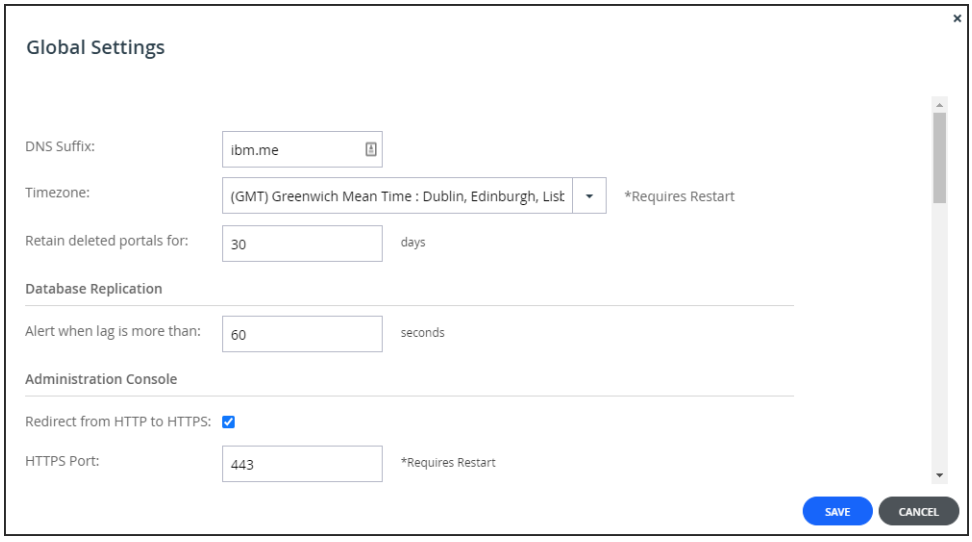
IBM COS FA Portal includes global settings that apply across all virtual IBM COS FA Portals:

- The DNS suffix that is appended to each virtual IBM COS FA Portal's name, in order to create the virtual IBM COS FA Portal's DNS name.
- The IBM COS FA Portal time zone.
- Password policy for IBM COS FA Portal administrators.

To configure global settings:

1 In the global administration view, select **Settings** in the navigation pane.

2 Select **Global Settings** under **SETTINGS** in the **Control Panel** page.
The **Global Settings** window is displayed.



3 Make changes as needed.
DNS Suffix – The global DNS suffix to use for all virtual IBM COS FA Portals. The DNS suffix was set when the IBM COS FA Portal was installed, as described in the installation guide for the environment.

Warning: **Changing the DNS suffix from the suffix specified when the IBM COS FA Portal was installed, requires IBM to issue a new license as well as possible changes to system settings, such as the hosts file.**

The DNS suffix is the suffix that is appended to each virtual IBM COS FA Portal's name, in order to create the virtual IBM COS FA Portal's DNS name. For example, if a virtual IBM COS FA Portal's name is *myportal*, and the DNS suffix is *example.com*, then the virtual IBM COS FA Portal's DNS name will be *myportal.example.com*. The DNS name is used to connect directly to a virtual IBM COS FA Portal.

Note: The name of each virtual IBM COS FA Portal is configurable in the **Main > Portals** page. Click the IBM COS FA Portal name to change the name.

Timezone – The IBM COS FA Portal's time zone.

Retain deleted portals for – The number of days to retain a deleted virtual IBM COS FA Portal. During this retention period, the administrator can undelete the IBM COS FA Portal, but after this period, the IBM COS FA Portal is permanently deleted along with the IBM COS FA Portal content. For details, see Deleting and Undeleting Virtual IBM COS FA Portals.

Database Replication

Alert when lag is more than – In the event that replication falls behind, IBM COS FA Portal administrators are notified via email after a lag time of specified number of seconds.

Administration Console

Redirect from HTTP to HTTPS – Enable automatic redirection from HTTP to HTTPS.
HTTPS Port – An HTTPS port number to change the administration IBM COS FA Portal HTTPS access port. The following HTTPS ports are allowed: 443, 1024 to 65535. Restart the IBM COS FA Portal for the new port to take effect. For more information, see Access URLs for Administrators.

EndUser Portal

Redirect from HTTP to HTTPS – Enable automatic redirection of the end user interface for team administrators from HTTP to HTTPS.

Web Session Control

Session Timeout – The amount of time the session remains open when there is no activity.

Administrators Password Policy

Minimum Password Length – The minimum number of characters that must be used in a IBM COS FA Portal administrator's account password.
Require password change on first login – Require administrators to change their password on their first login.
Require password change every – Require administrators to change their password after a certain number of months, then specify the desired number of months in the field provided. When the specified number of months has elapsed, the administrator's password will expire, and they will be required to configure a new password upon their next login.
Prevent reusing last... passwords – Prevent administrators 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 administrators 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 administrators from using their personal details in their password, including first name, last name, email, username, and company name. After checking this page, edit the content of the consent page.

Consent Page

Display consent page after login – After logging in to the IBM COS FA Portal the user is redirected to a consent page and only after the user accepts the terms in the consent page can the user access the IBM COS FA Portal.

4 Click **SAVE**.

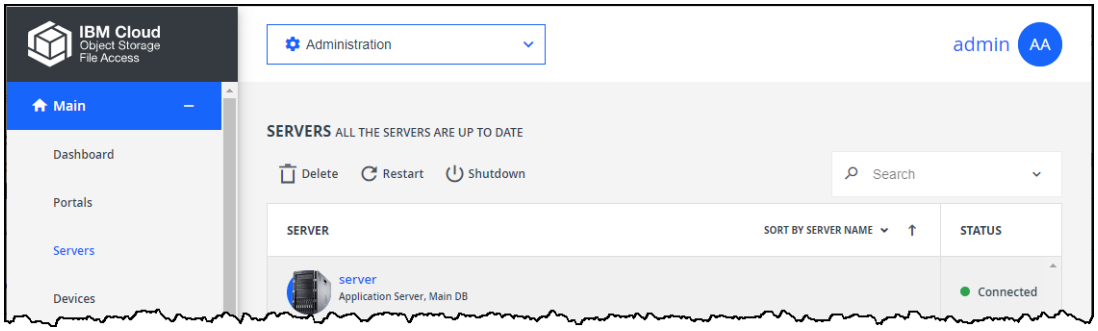
5 If you changed the **Timezone**, restart the IBM COS FA Portal servers in the following order:

a Main database server.

b Replication database server, if available.

c All application servers.

Select each server in turn and click **Restart** on the **Main > Servers** page.



The **Timezone** change is implemented after the restart.

CHAPTER 8. 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

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 Managing Subscription Plans and specifically in steps **6** and **7** of the procedure To add or edit a subscription plan:, in the S**napshot Retention Policy** window.

APPLYING A SNAPSHOT RETENTION POLICY

The snapshot retention policy defined in the subscription plan can be applied globally as the default plan to team portals.

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 9. MANAGING SUBSCRIPTION PLANS

You provision licenses to virtual IBM COS FA Portals, by assigning the virtual IBM COS FA Portals to global plans.

Global Plans

When a team IBM COS FA Portal is assigned to a global plan, IBM COS FA Portal automatically creates a default subscription plan containing the licenses specified in the global plan, and assigns all user accounts in the team IBM COS FA Portal to this plan. you can create alternate subscription plans and assign those to individual user accounts. Users in a team IBM COS FA Portal obtain services through their subscription plans for an open-ended period of time without payment.

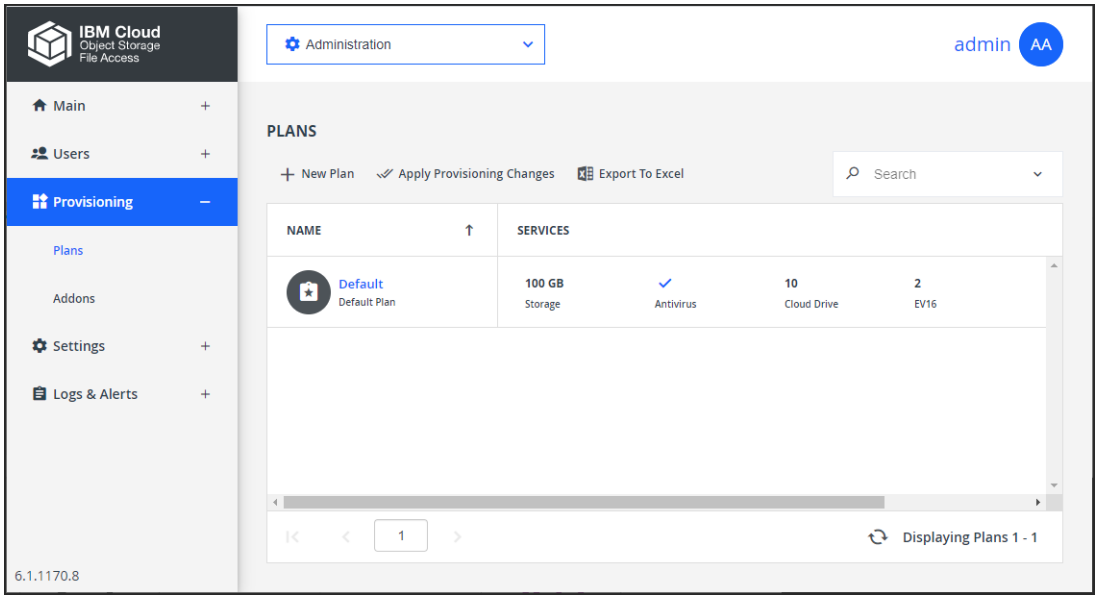
This chapter explains how to use subscription plans to provision services to users' devices and how to provision services to virtual IBM COS FA Portals via global plans.

In this chapter

VIEWING SUBSCRIPTION PLANS

To view all plans:

- In the global administration view, select **Provisioning > Plans** in the navigation pane.
  The **PLANS** page is displayed.



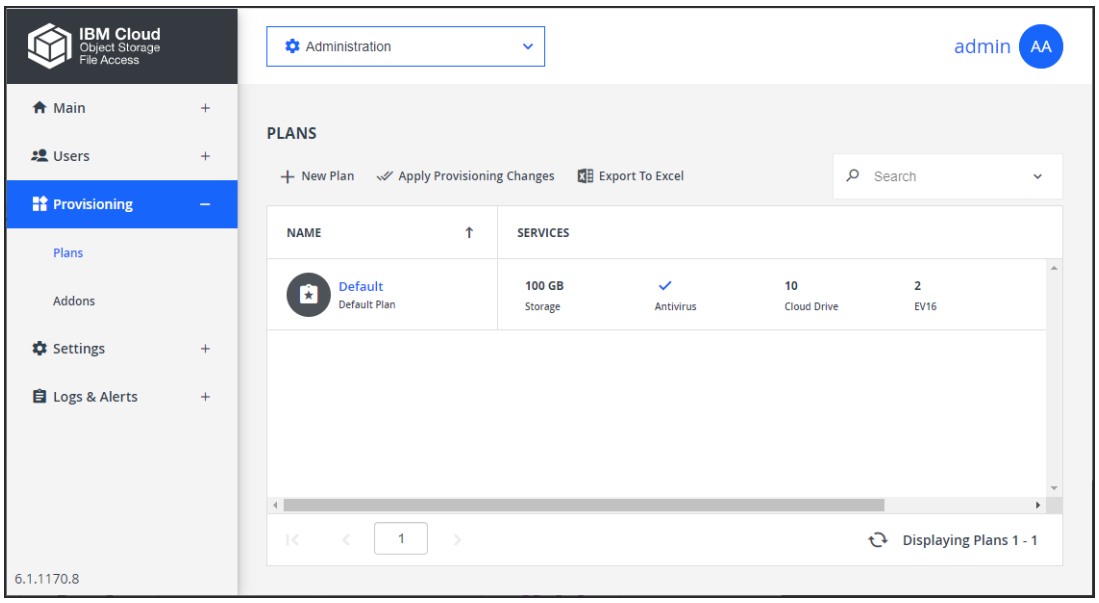
The page includes the following:
NAME – The subscription plan's name. `Default Plan` is displayed under the plan name for the default plan.

SERVICES – The services provisioned in the plan.
Storage – The amount of storage allocated for the plan.
Antivirus – The plan includes the antivirus service.
Cloud Drive – The number of administrators are included in the plan.
Portal – The IBM COS FA Portal license is operational or not.
EV16 – The number of IBM COS FA Gateway licenses included in the license key. You can have as many IBM COS FA Gateways in the IBM COS FA Portal as you have licenses.
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

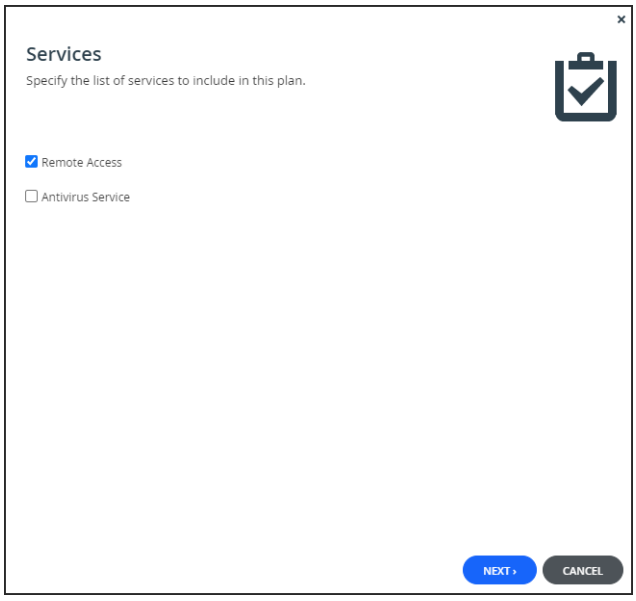
To add or edit a subscription plan:

1 In the global administration view, select **Provisioning > Plans** in the navigation pane.
The **PLANS** page is displayed.



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.

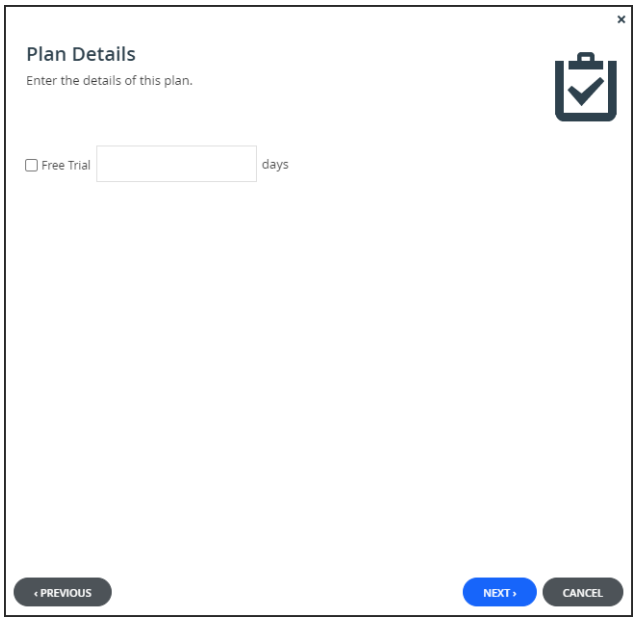


3 Choose which services to include in the plan:
Remote Access – Include remote access in the subscription plan. Remote access includes both access to the device's management interface via the IBM COS FA Portal and a dedicated URL, access to the user's files via the IBM COS FA Portal and a dedicated URL.

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

Antivirus Service – Include the Cloud Drive antivirus service in the plan. When antivirus is activated, files are scanned for malware automatically and transparently, before they are downloaded for the first time. The Cloud Drive antivirus service requires an additional license.

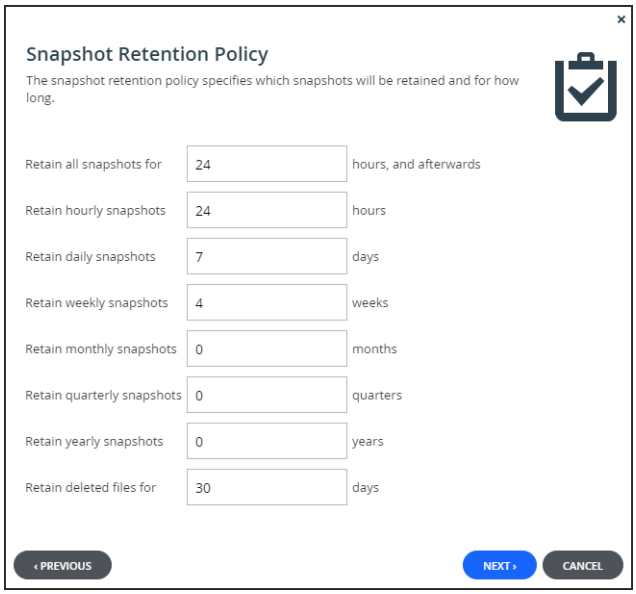
4 Click **NEXT**.
The **Plan Details** window is displayed.



5 Set the plan details.

Free Trial – Include a free trial period in the plan. Enter the number of days that subscribers can receive the plan for free.

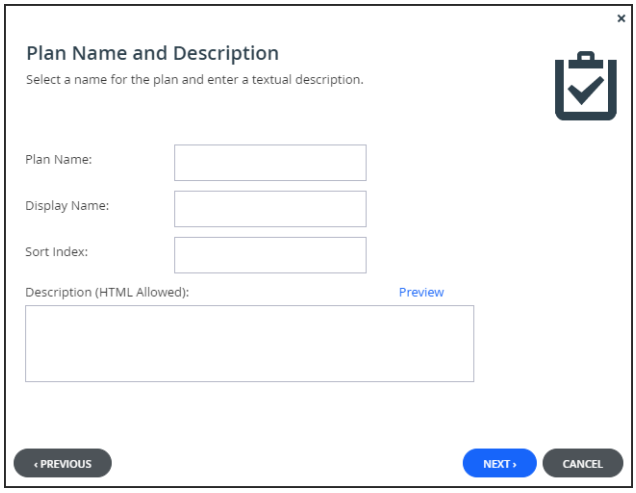
6 Click **NEXT**.
The **Snapshot Retention Policy** window is displayed.



7 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 value is 7 days.

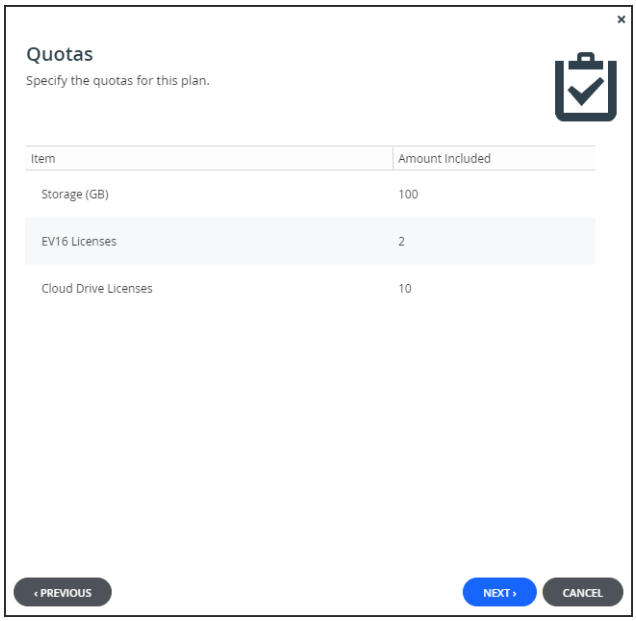
Note: For an additional explanation of each policy, see IBM COS FA Portal Snapshots.

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



9 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.

10 Click **NEXT**.
The **Quotas** window is displayed.



11 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.

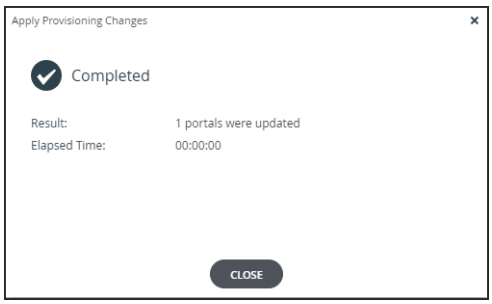
Note: The quotas must not exceed the number specified in the license. An error message is displayed when you attempt to assign a user to a plan with a quota that exceeds the number specified in the license.

12 Click **NEXT**.
The **Wizard Completed** screen is displayed.

13 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. After the changes have been applied click **CLOSE**.



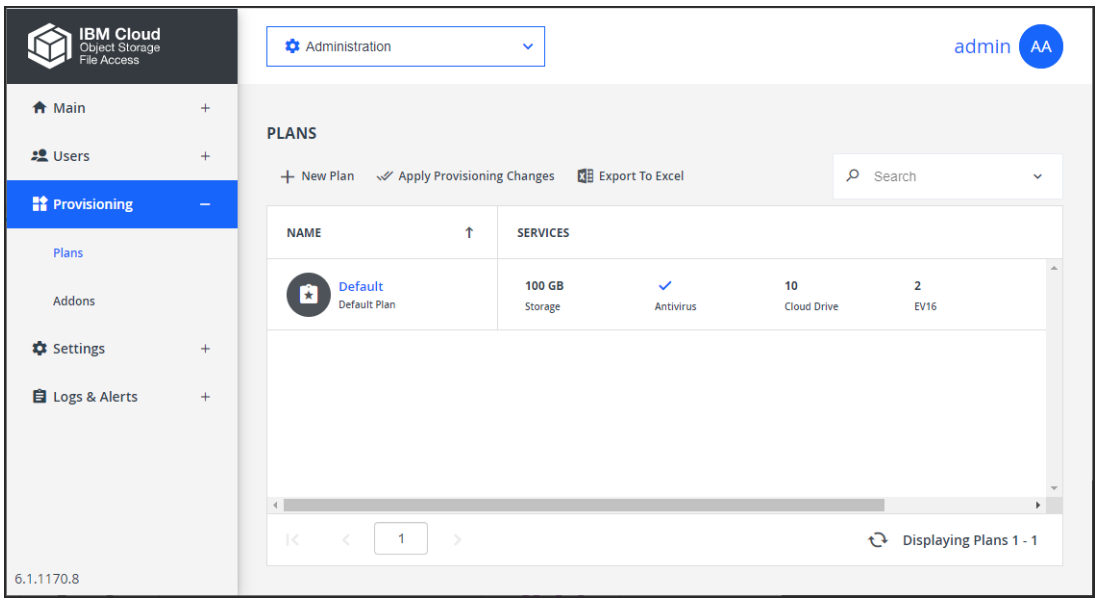
While the changes are being applied you can either stop the process, by clicking **STOP** or close the window while the process continues to run in the background by clicking **CONTINUE IN BACKGROUND**.

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 In the global administration view, 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 In the global administration view, 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.

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. In the global administration view, 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. In the global administration view, 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 10. MANAGING ADD-ONS

In a team portal, all users obtain additional services for a specified period of time, when the IBM COS FA Gateway is subscribed to a *global add-on*.

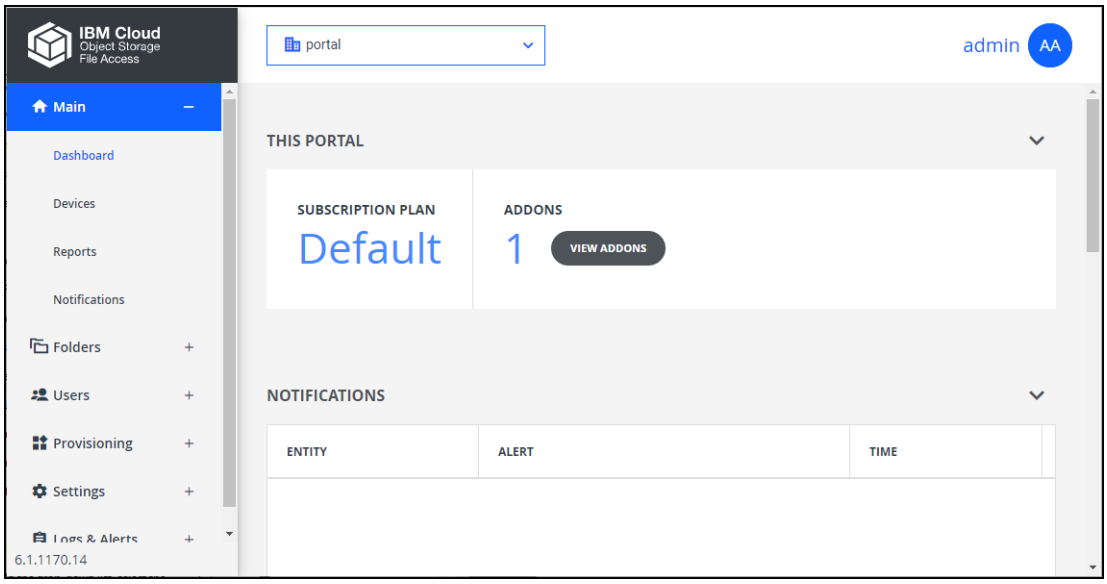
This chapter describes how to manage add-ons to provision services for a team portal.

The following tasks must be performed in the global administration view.

In this chapter

VIEWING ADD-ONS

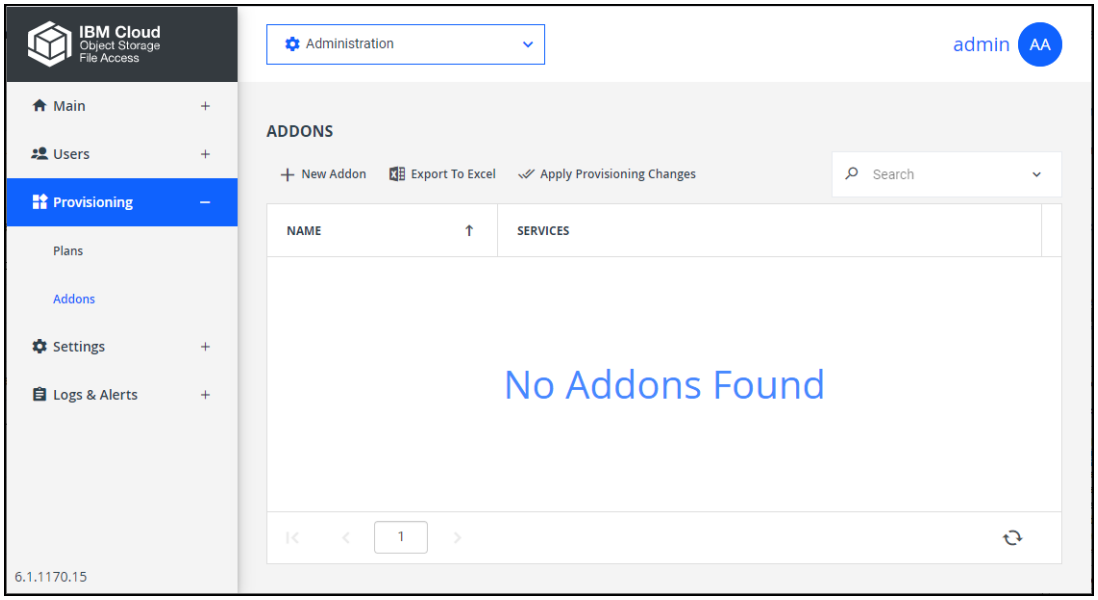
You can view the add-ons for a specific portal in the dashboard for that portal.



If add-ons are defined for the portal, as described in Assigning Add-ons to Virtual IBM COS FA Portals, click **VIEW ADDONS** to display details.

To view all add-ons:

- In the global administration view, select **Provisioning > Add-Ons** in the navigation pane. The **ADDONS** page is displayed.



The page includes the following:

NAME – The add-on name. The add-on display name, displayed in the End User Portal and notifications, is displayed under the name.

SERVICES – The services that the add-on applies to.

Storage – The amount of storage for the add-on.

Antivirus – The add-on includes the antivirus service.

Cloud Drive – The number of IBM Cloud Drive licenses included in the add-on.

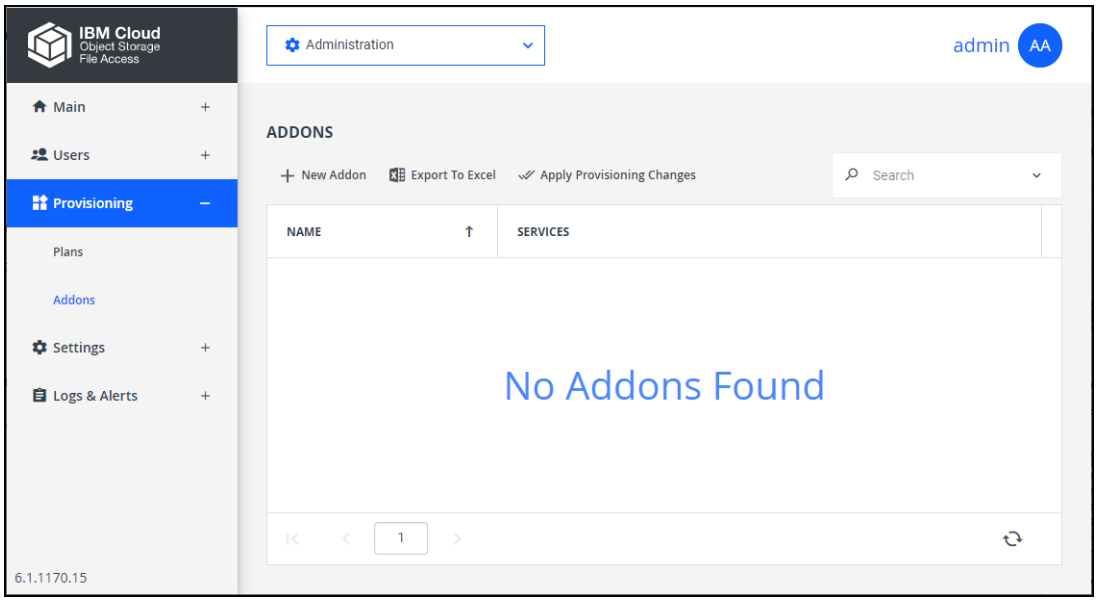
EV16 – The number of IBM COS FA Gateways included in the add-on.

EXPIRES – The number of days after adding this add-on, that the add-on will expire.

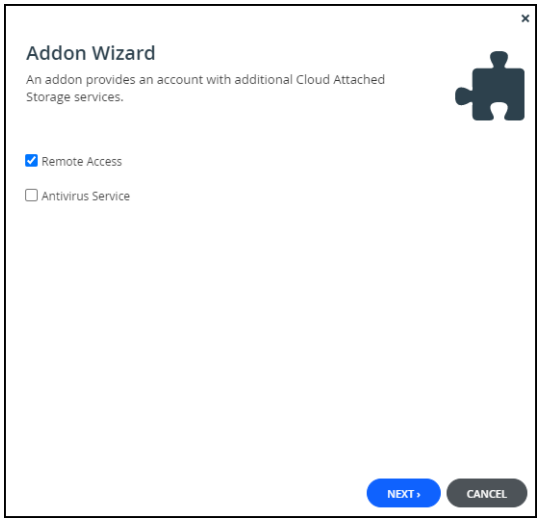
ADDING AND EDITING ADD-ONS

To add or edit an add-on:

1 In the global administration view, select **Provisioning > Add-Ons** in the navigation pane.
The **ADDONS** page is displayed.



2 To add a new add-on, click **New Addon**.
Or,
To edit an existing add-on, click the add-on name**.**
The **Add-on** wizard opens.



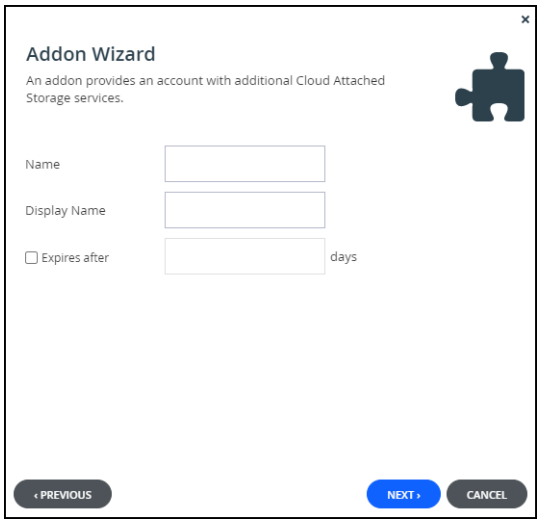
3 Choose which services to include in the add-on:
Remote Access – Include remote access in the subscription plan. Remote access includes both access to the device's management interface via the IBM Portal and a dedicated URL, access to the user's files via the IBM Portal and a dedicated URL.

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

Antivirus Service – Include the antivirus service in the plan. When antivirus is activated, files are

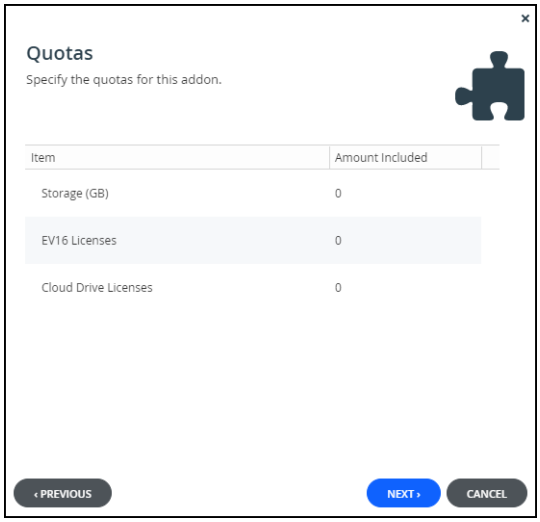
scanned for malware automatically and transparently, before they are downloaded for the first time. The Cloud Drive antivirus service requires an additional license. For details, see Antivirus File Scanning.

4 Click **NEXT**.



5 Set the add-on details.
Name – A name for the add-on. Only letters and numbers can be used for the name.
Display Name – The name to use when displaying this add-on in the end user portal and notifications.
Expires after – The number of days after adding this add-on, that the add-on will expire.

6 Click **NEXT**.
The **Quotas** window is displayed.

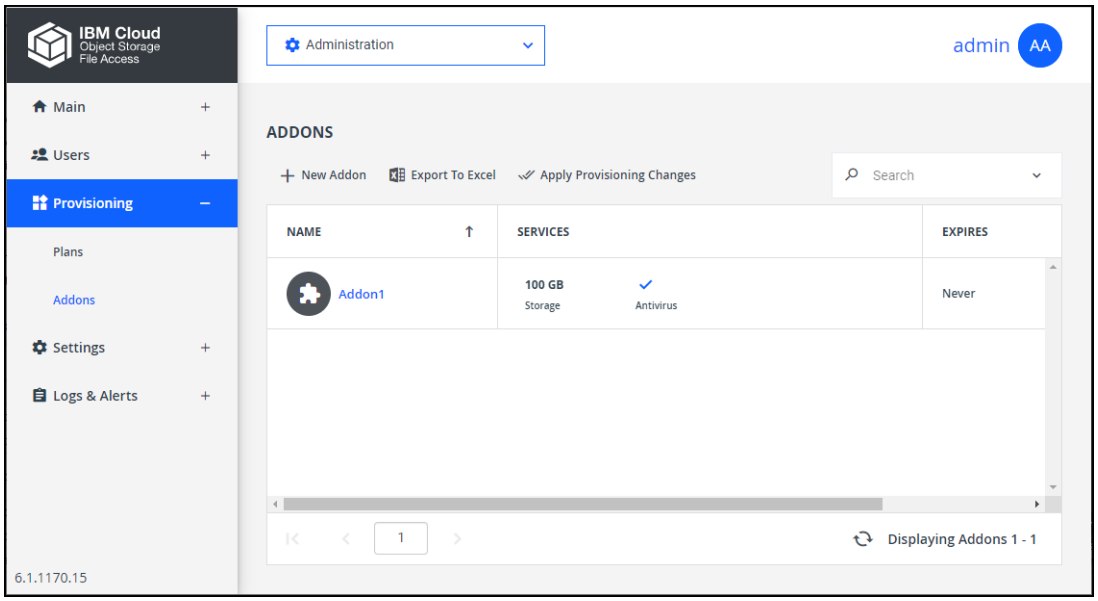


7 For each item, click in the quota field and enter the number to include in the plan.
For example, to include 100GB of storage space, click in the Storage (GB) item's quota field and enter 100.

Note: The quotas must not exceed the number specified in the license.

8 Click **NEXT**.
The **Wizard Completed** screen is displayed.

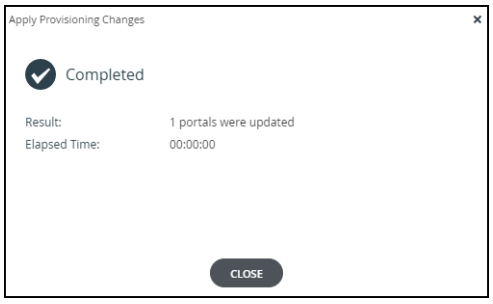
9 Click **FINISH**.
The **ADDONS** page is displayed with the add-on.



10 Assign the add-on to virtual portal, as described in Assigning Add-ons to Virtual IBM COS FA Portals.

If you edited an existing add-on, IBM 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. After the changes have been applied click **CLOSE**.



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**.

EXPORTING ADD-ON DETAILS TO EXCEL

You can export the list of add-ons and their details to a comma separated values (*.csv) Excel file.

To export the list of add-ons to an Excel file:

1 In the global administration view, select **Provisioning > Addons** in the navigation pane.
The **ADDONS** page is displayed.

2 Click **Export to Excel**.

The add-on list is downloaded to your computer. The list includes quotas and the number of days before the add-on expires.

DELETING AN ADD-ON

To delete an Add-on:

1. In the global administration view, select **Provisioning > Plans** in the navigation pane.
   The **ADDONS** page is displayed.
1. Select the add-on row.
2. Click **Delete Addon.**
   A confirmation window is displayed.
3. Click **DELETE** to confirm.

The add-on is deleted.

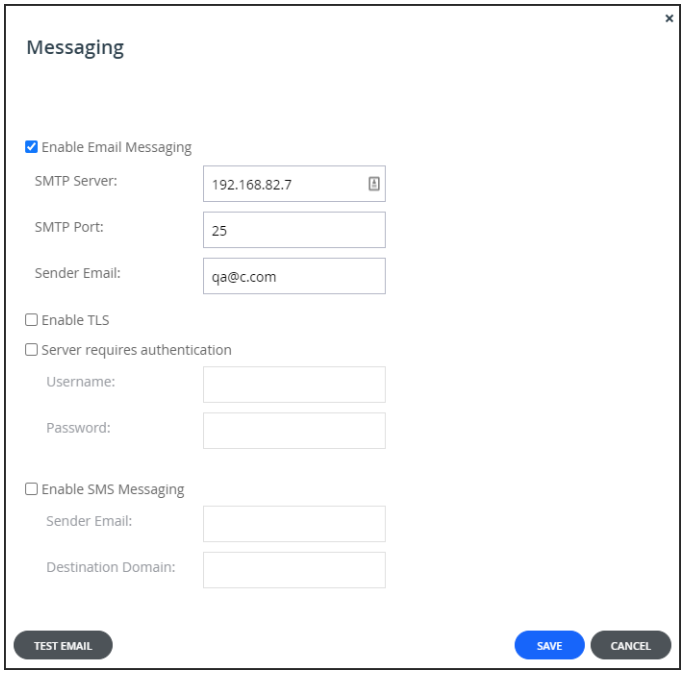
CHAPTER 11. CONFIGURING MESSAGE SETTINGS

You can configure global messaging settings that will be inherited by all servers. For information on overriding these settings on a per-server basis, see Editing Server Settings.

To configure messaging settings:

1 In the global administration view, select **Settings** in the navigation pane.

2 Select **Messaging Settings** under **NOTIFICATIONS AND LOGS** in the **Control Panel** page. The **Messaging** window is displayed.



3 Complete the fields.

Enable Email Messaging – Enable sending email messages from the IBM COS FA Portal to users. The **SMTP Server**, **SMTP Port**, and **Sender Email** fields are enabled.

SMTP Server – The outgoing mail server address for sending email messages from the IBM COS FA Portal to users.

SMTP Port – The port number for sending email messages from the IBM COS FA Portal to users.

Sender Email – The email address to use in the From field of notifications sent to global administrators by the global portal.

Enable TLS – Use Transport Layer Security (TLS) encryption for sending email messages from the IBM COS FA Portal to users.

Server requires authentication – The SMTP server requires authentication. The **Username** and **Password** fields are enabled.

Username – The user name that the IBM COS FA Portal uses when authenticating to the SMTP server.

Password – The password that the IBM COS FA Portal uses when authenticating to the SMTP server.

Enable SMS Messaging – Enable sending passcodes via text message to protect access to guest invitations. To effectively enable SMS messaging, you must register with an SMS gateway and then enter the sender email and destination domain in the fields below.

Sender Email – The sender email address registered with the SMS gateway.
Destination Domain – The DNS suffix of the sender email.

4 Click **SAVE**.

5 To validate SMTP mail server settings, click **Test Email** to send a test email. Verify that you receive the test mail at the email address defined in your administrator user account.

6 If you changed the SMTP settings, restart the portal servers in order for the changes to take effect.

CHAPTER 12. MANAGING VIRTUAL IBM COS FA PORTALS

The IBM COS FA Portal can be divided into tenants, known as *virtual portals*, each of which manages a subset of devices and IBM COS FA Portal user accounts: a **Team** IBM COS FA Portal. A team IBM COS FA Portal is designed for the needs of a company or team with multiple members. The users in the IBM COS FA Portal are the team members. Team IBM COS FA Portals are managed by *team administrators*, who are team members with the *Administrator* role.

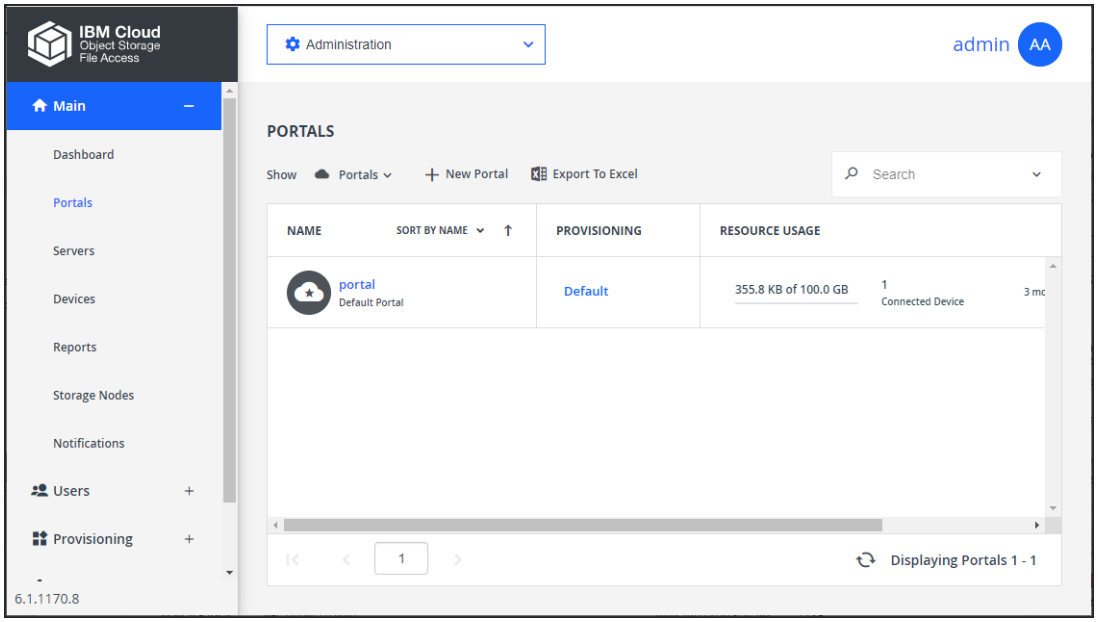
This chapter explains how to add, edit, and delete virtual IBM COS FA Portals, as well as log in to any virtual IBM COS FA Portal and manage its contents.

In this chapter

VIEWING VIRTUAL IBM COS FA PORTALS

To view all virtual IBM COS FA Portals

- In the global administration view, select **Main > Portals** in the navigation pane.
  The **PORTALS** page opens, displaying all the virtual IBM COS FA Portals.



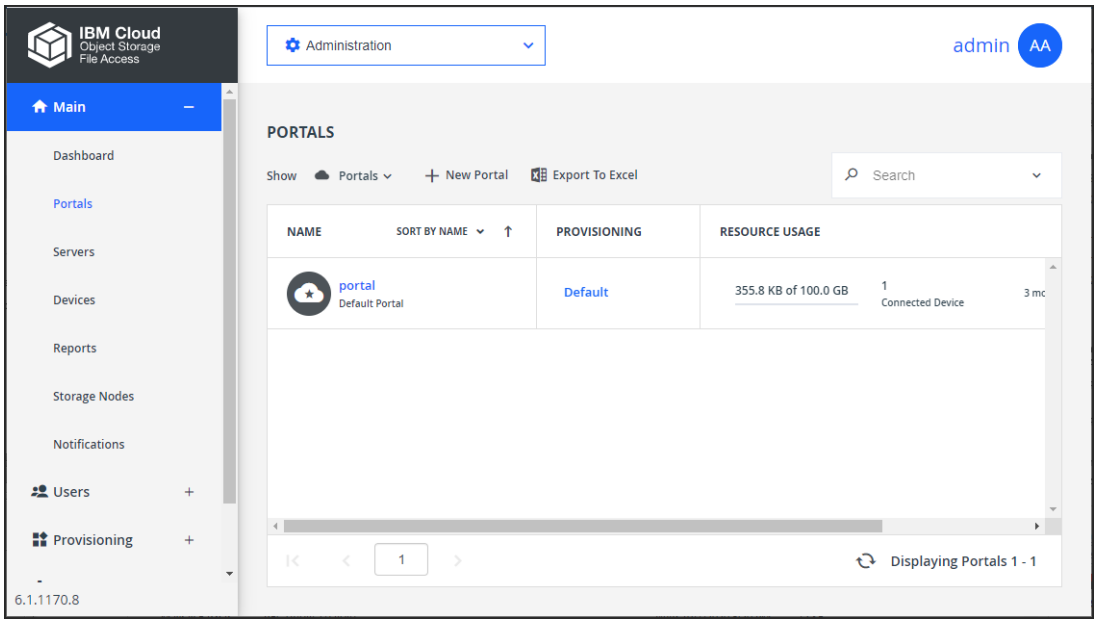
The page includes the following columns:

Field	Description
NAME	The virtual IBM COS FA Portal name. To edit the virtual IBM COS FA Portal, click the name. For further details, see Adding and Editing Virtual IBM COS FA Portals. If the IBM COS FA Portal is disabled, `Disabled` is displayed below the name.
PROVISIONING	The global plan to which this IBM COS FA Portal is assigned. To modify the plan, click the plan's name. For further details, see Adding and Editing Subscription Plans.
RESOURCE USAGE	The amount of storage in use by the virtual IBM COS FA Portal, out of the total provisioned amount. The number of IBM COS FA Gateway licenses and Cloud Drive licenses in use by the IBM COS FA Portal, out of the total provisioned number is displayed.
BILLING ID	The team IBM COS FA Portal owner's billing ID.

ADDING AND EDITING VIRTUAL IBM COS FA PORTALS

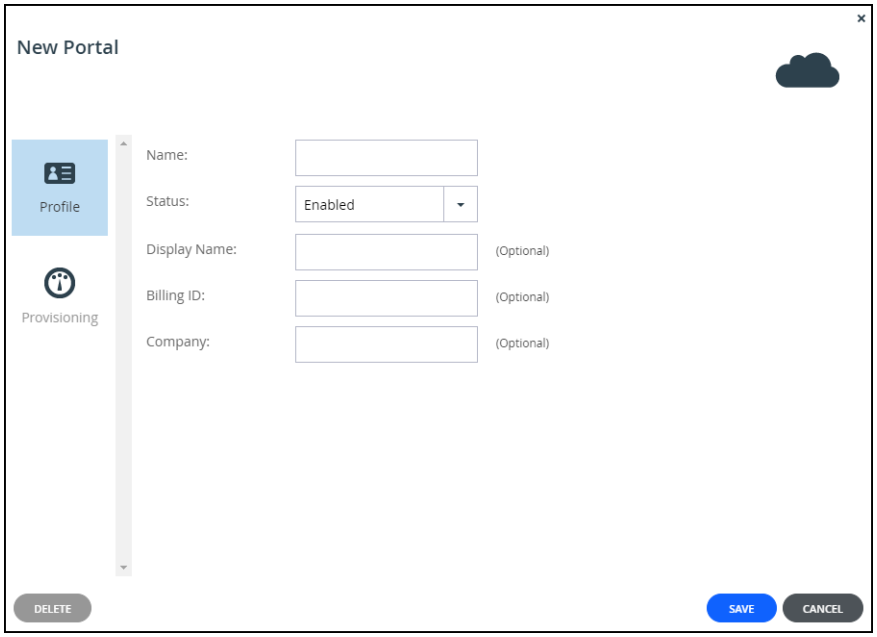
To add or edit a virtual IBM COS FA Portal:

1 In the global administration view, select **Main > Portals** in the navigation pane.
The **PORTALS** page opens, displaying all the virtual IBM COS FA Portals.



2 Either,

- Add a new virtual IBM COS FA Portal, click **New Portal**.
The **New Portal** window is displayed.



Or,

- Edit an existing IBM COS FA Portal, click the IBM COS FA Portal's name.
  The IBM COS FA Portal window is displayed with the IBM COS FA Portal name as the window title.

3 Complete the fields.
Name – Type a unique name for the virtual IBM COS FA Portal.
Status – The status: either **Enabled** or **Disabled**. If you set the status to disabled:
- Users cannot log in to the IBM COS FA Portal, and devices cannot connect.
- Reports and email notifications are not sent from the IBM COS FA Portal.
- User self-registration is disabled.

Global administrators can still connect to disabled IBM COS FA Portals via the *global administration view*.
Display Name – Optional. The name displayed.
Billing ID – Optional. The virtual IBM COS FA Portal owner's billing ID. This enables integration of the IBM COS FA Portal with an external billing system.
Company – Optional. The name of the company owning the IBM COS FA Portal.

4 Assign a plan, as described in Assigning Global Plans to Virtual IBM COS FA Portals.

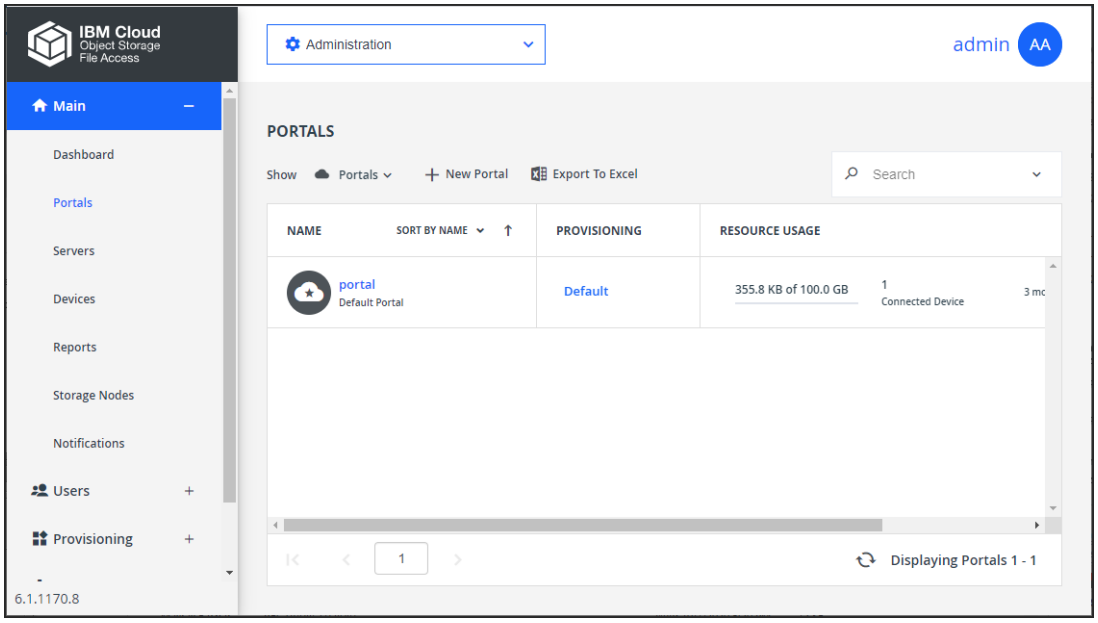
5 Click **SAVE**.

ASSIGNING GLOBAL PLANS TO VIRTUAL IBM COS FA PORTALS

A global plan can be added to a virtual IBM COS FA Portal for every user in the IBM COS FA Portal. Plans can be assigned to individual users in the virtual IBM COS FA Portal.

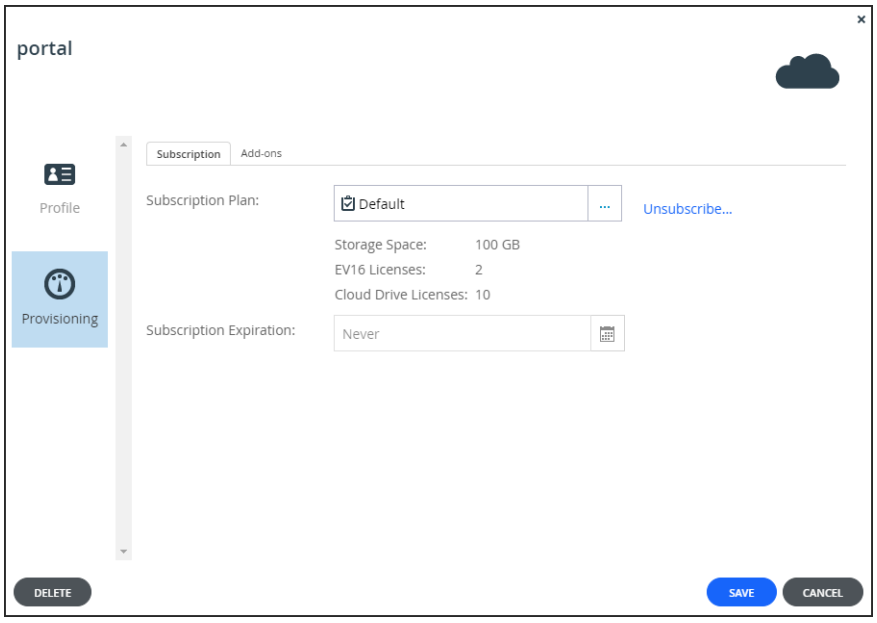
To assign a global plan to a virtual IBM COS FA Portal:

1 In the global administration view, select **Main > Portals** in the navigation pane.
The **PORTALS** page opens, displaying all the virtual IBM COS FA Portals.

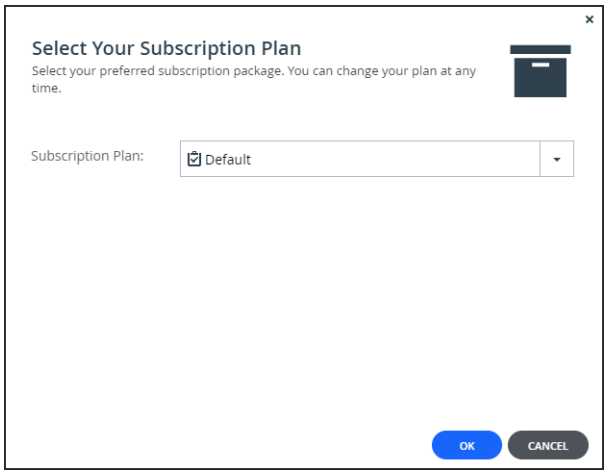


2 Click the IBM COS FA Portal name.

3 Click the **Provisioning** option.
The **Provisioning** window is displayed.



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



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

6 Click **OK**.

7 In the **Subscription Expiration** field, click  to specify the date on which the IBM COS FA Portal's subscription to the selected plan will expire. This field is only enabled for plans that are defined as time limited trial plans.

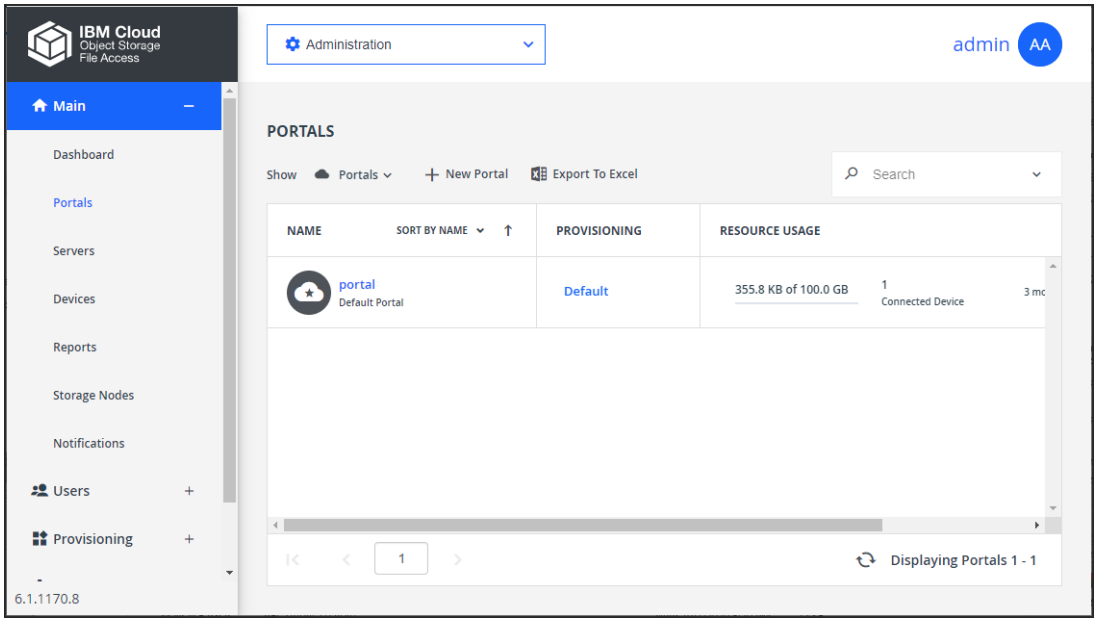
8 Click **SAVE**.
The virtual IBM COS FA Portal is assigned to the subscription plan.

ASSIGNING ADD-ONS TO VIRTUAL IBM COS FA PORTALS

An add-on can be added to a virtual IBM COS FA Portal as part of the provisioning for the IBM COS FA Portal and the add-on is valid for every user in the IBM COS FA Portal.

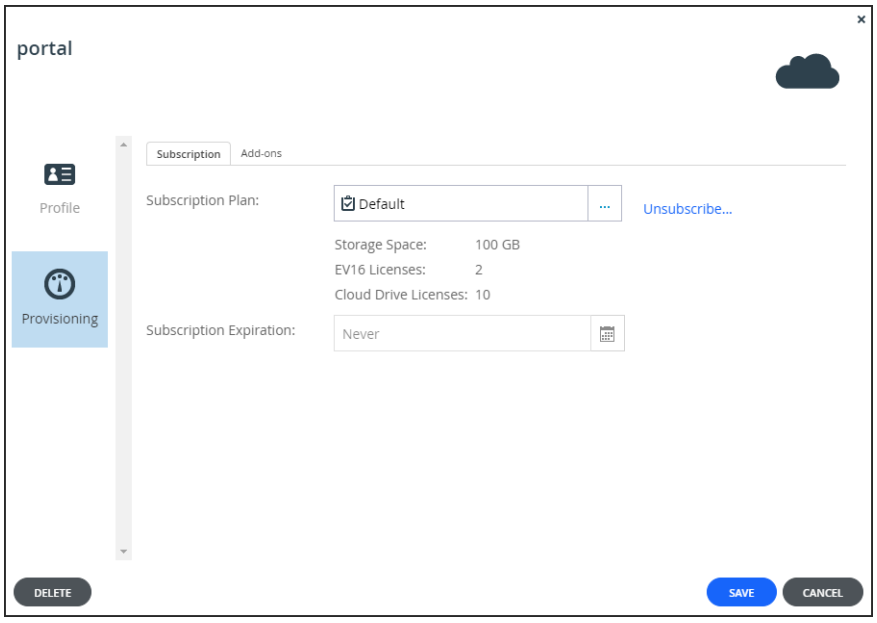
To assign global add-ons to a virtual IBM COS FA Portal:

1 In the global administration view, select **Main > Portals** in the navigation pane.
The **PORTALS** page opens, displaying all the virtual portals.

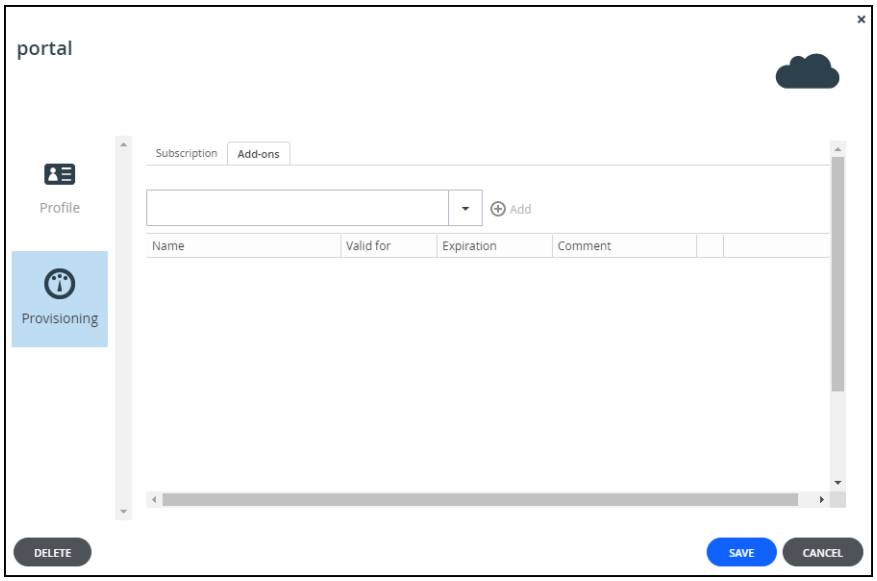


2 Click the portal name.

3 Click the **Provisioning** option.
The **Provisioning** window is displayed.



4 Select the **Add-ons** tab.



5 Add an add-on for the virtual IBM COS FA Portal:

a In the drop-down list, select the add-on.

b Click **Add**.
The add-on is displayed.

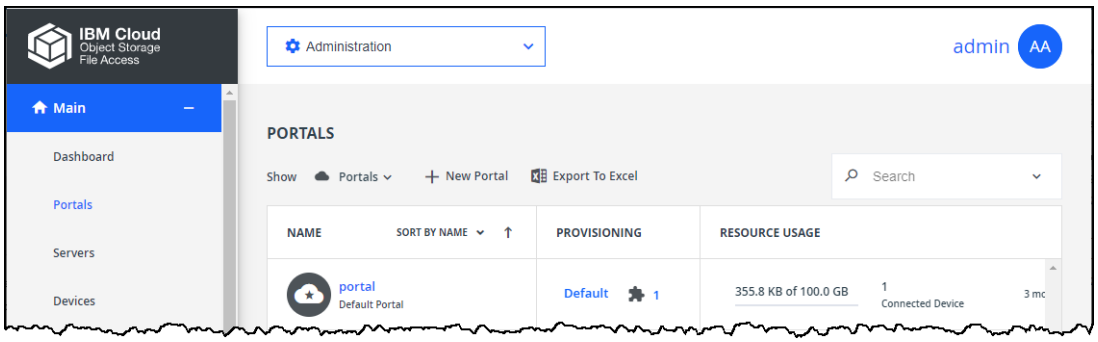
c To select a new date until when the add-on is valid, in the add-on row, click in the **Valid for** column and then either clear the value, type a new value or click to display a calendar to select a new date when the add-on subscription should end.
The **Expiration** column is updated accordingly.

d Optionally, enter a comment in the **Comment** column.

6 To remove an add-on from the virtual IBM COS FA Portal, in the add-on row in the list box, click .
The add-on is removed.

7 Click **SAVE**.

The add-on, identified by the icon, is assigned to the team IBM COS FA Portal.

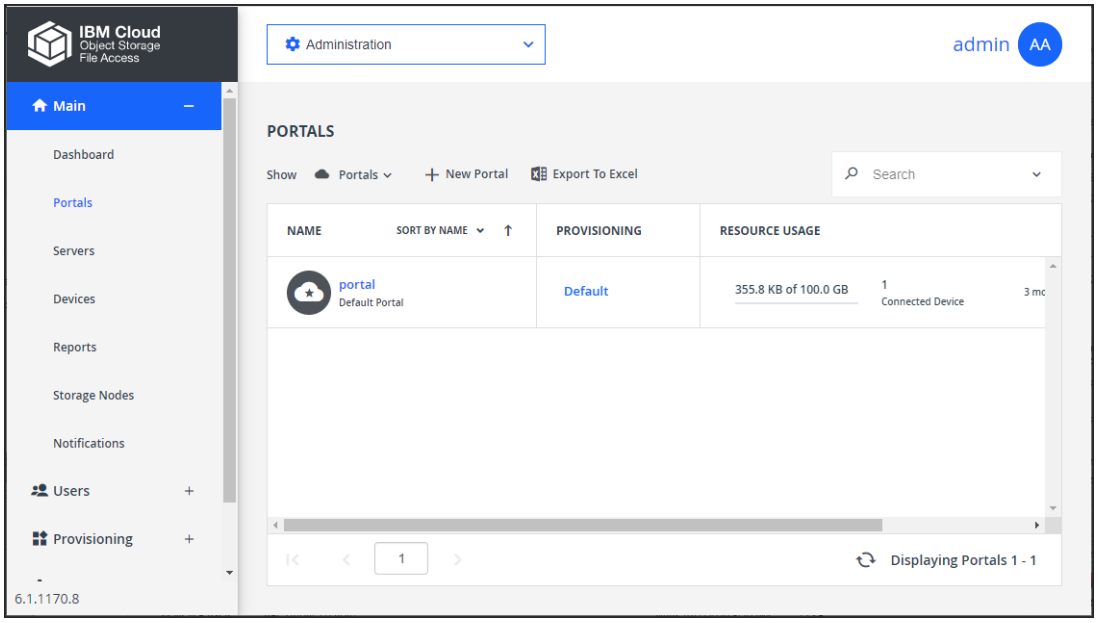


EXPORTING VIRTUAL IBM COS FA PORTALS TO EXCEL

You can export the list of virtual IBM COS FA Portals 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 In the global administration view, select **Main > Portals** in the navigation pane.
The **PORTALS** page opens, displaying all the virtual IBM COS FA Portals.



2 Click **Export to Excel**.
The list virtual IBM COS FA Portals with their details exported to your computer. The details include the provisioned plan for the IBM COS FA Portal, storage quotas and actual storage.

DELETING AND UNDELETING VIRTUAL IBM COS FA PORTALS

Warning: **When a virtual IBM COS FA Portal is deleted, all of its content is deleted as well.**

To delete a virtual IBM COS FA Portal:

1 In the global administration view, select **Main > Portals** in the navigation pane.
The **PORTALS** page opens, displaying all the virtual IBM COS FA Portals.

2 Select the row of the IBM COS FA Portal to delete and click **Delete Portal**.
A confirmation window is displayed.

3 Click **DELETE**.
The IBM COS FA Portal and all of its content is deleted.

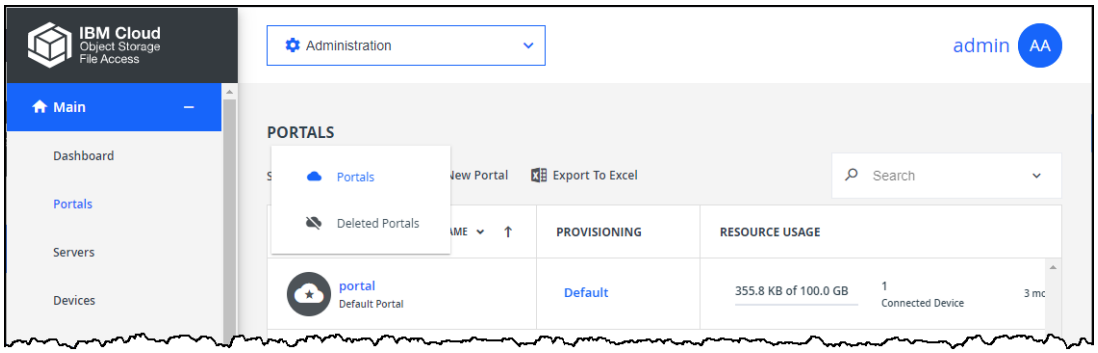
To restore a deleted IBM COS FA Portal:

Note: A deleted IBM COS FA Portal can be restored after it is deleted for the number of days specified in the **Retain deleted portals for** field in the global settings, where the retention period is defined. For details refer to the Configuring Global Settings.

1 In the global administration view, select **Main > Portals** in the navigation pane.
The **PORTALS** page opens, displaying all the virtual IBM COS FA Portals.

2 Change the view to display the deleted IBM COS FA Portals by clicking **Show Portals** and selecting

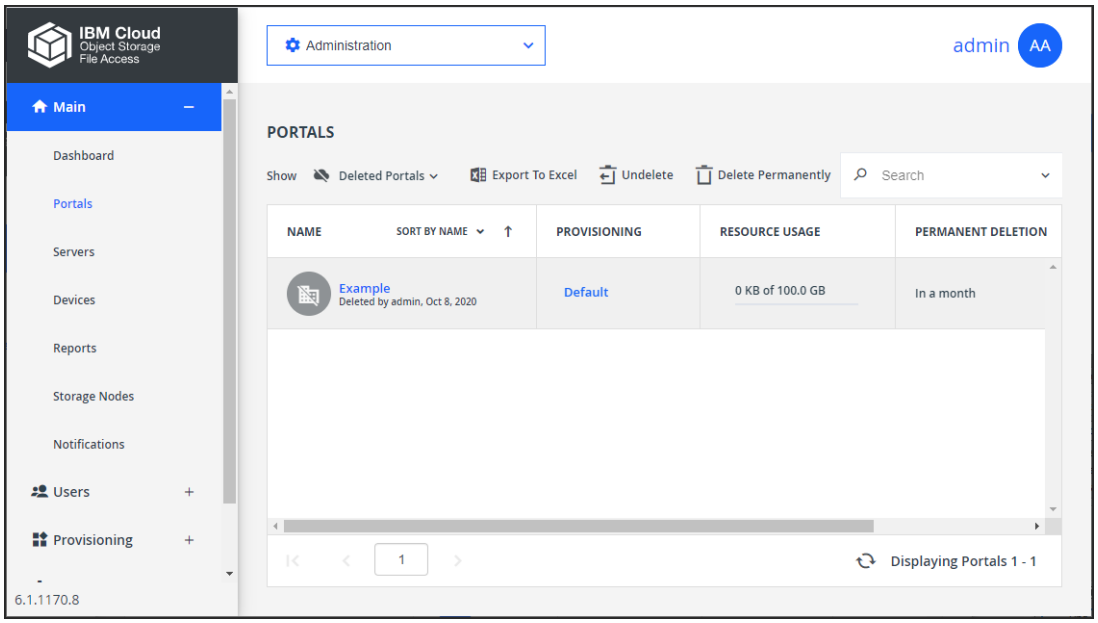
Deleted Portals.



The view changes to display deleted IBM COS FA Portals.

Note: Deleted IBM COS FA Portals in this list do not use any licenses or consume storage from storage quotas.

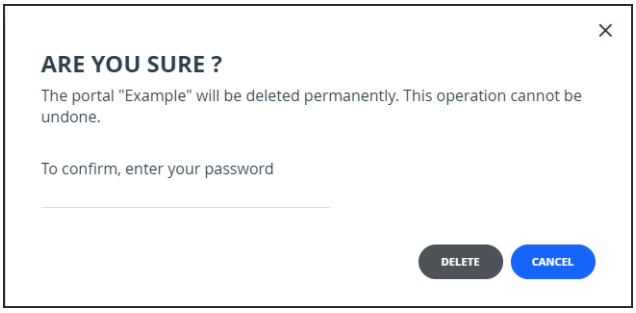
3 Select the row of the IBM COS FA Portal to recover and click **Undelete**.



The IBM COS FA Portal and IBM COS FA Portal content is restored.

Note: You can export the list of deleted IBM COS FA Portals with information such as the storage used by the IBM COS FA Portal, when it was deleted and licenses for the IBM COS FA Portal, by clicking **Export to Excel**.

You can click **Delete Permanently** to immediately delete the IBM COS FA Portal and all the content. In this case, you are prompted to confirm that you want to permanently delete the IBM COS FA Portal by entering you administrator password.



Note: The audit log includes an entry for a IBM COS FA Portal that is deleted, undeleted or permanently deleted.

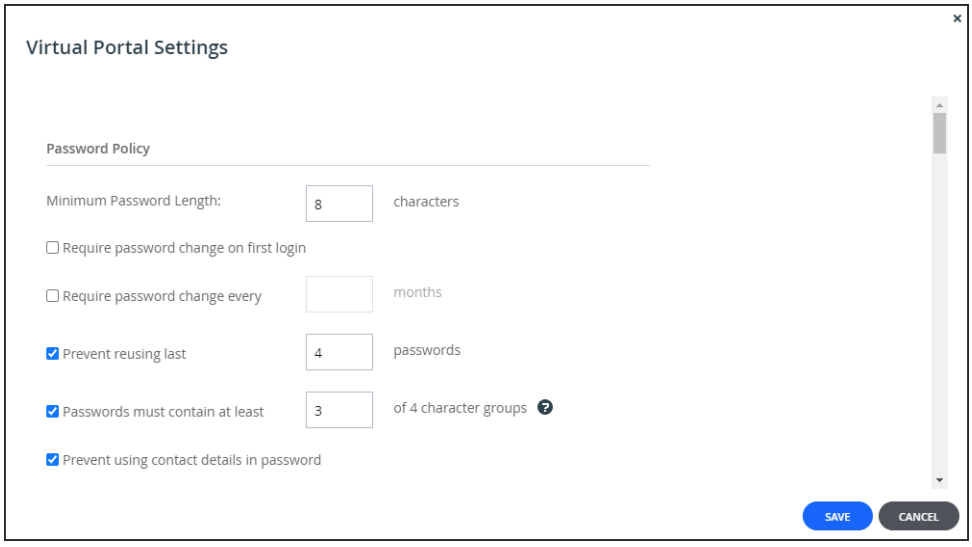
CHAPTER 13. CONFIGURING VIRTUAL PORTAL SETTINGS

Virtual portal settings are default settings that apply to all virtual portals. Global settings can be overridden for each virtual portal from that virtual portal's administration interface.

In this chapter

To set virtual 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.



3. Change settings as required, as described below.
4. Click **SAVE**.

PASSWORD POLICY

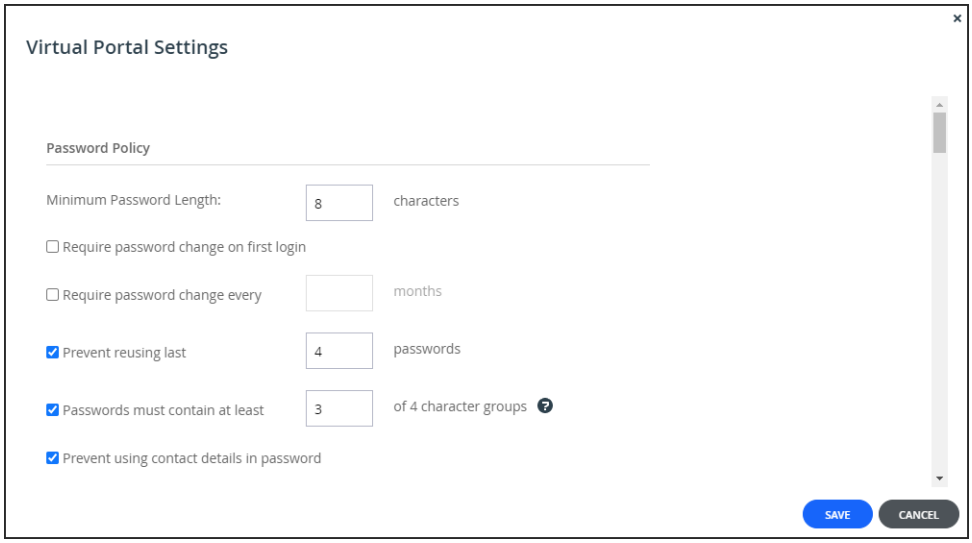
IBM COS FA Portal features a password strength policy to comply with security standards. You can:

- 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.



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

Support Email – The email address to which support requests are sent.
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 portal.

GENERAL SETTINGS

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

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.mIBM 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.

DEFAULT SETTINGS FOR NEW USER

Interface Language – The default language for new team administrators.

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

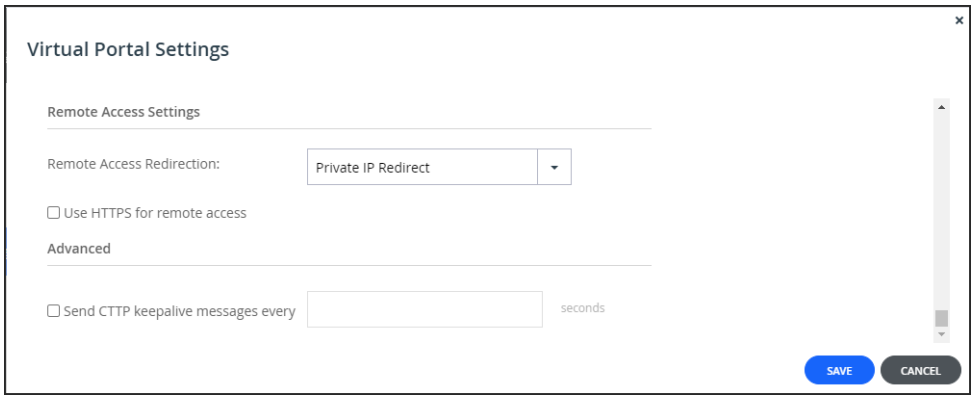
User – Create a single folder group for each user account, containing all of the user account's cloud folders. Deduplication is performed for the user account's folder group.
Portal – Create a single folder group for each virtual IBM COS FA Portal, containing all of the cloud folders in the team IBM 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

Cloud Drive Logging Level – 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



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 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

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 14. MANAGING DEVICES

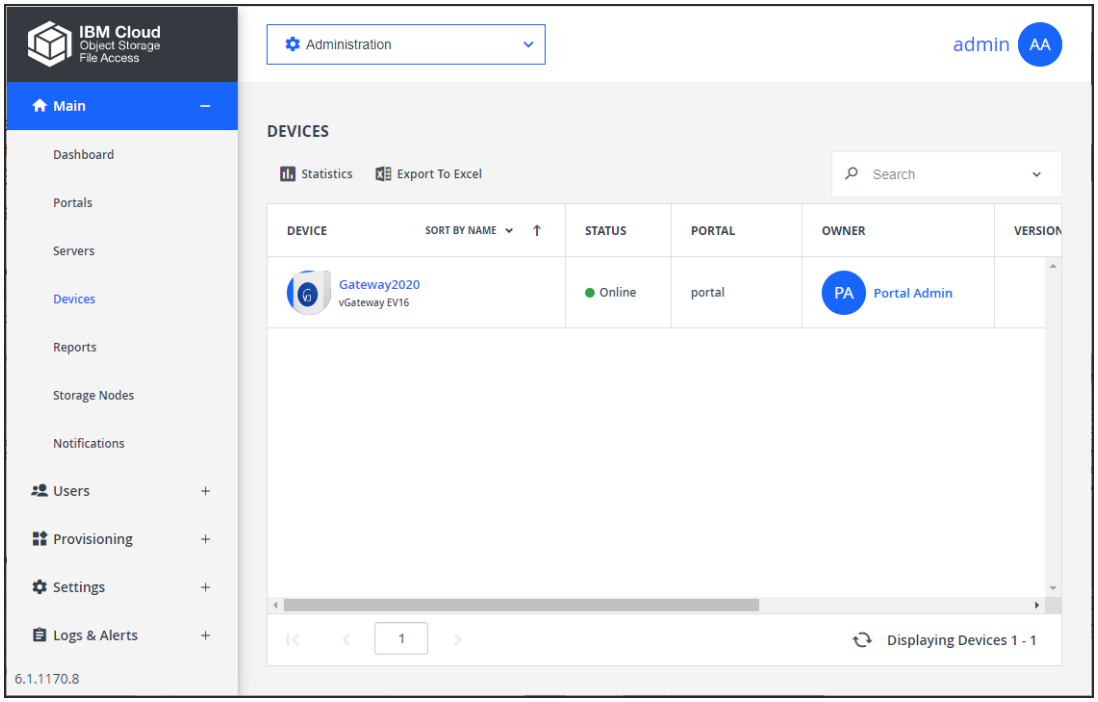
A *device* refers to an IBM COS FA Gateway connected to the IBM COS FA Portal. Devices are automatically added to the IBM COS FA Portal, when their owners connect the device to the IBM COS FA Portal.

In this chapter

VIEWING ALL DEVICES

To view all devices connected to all virtual portals:

- In the global administration view, select **Main > Devices** in the navigation pane.
  The **DEVICES** page opens, displaying all the devices connected to the portals.



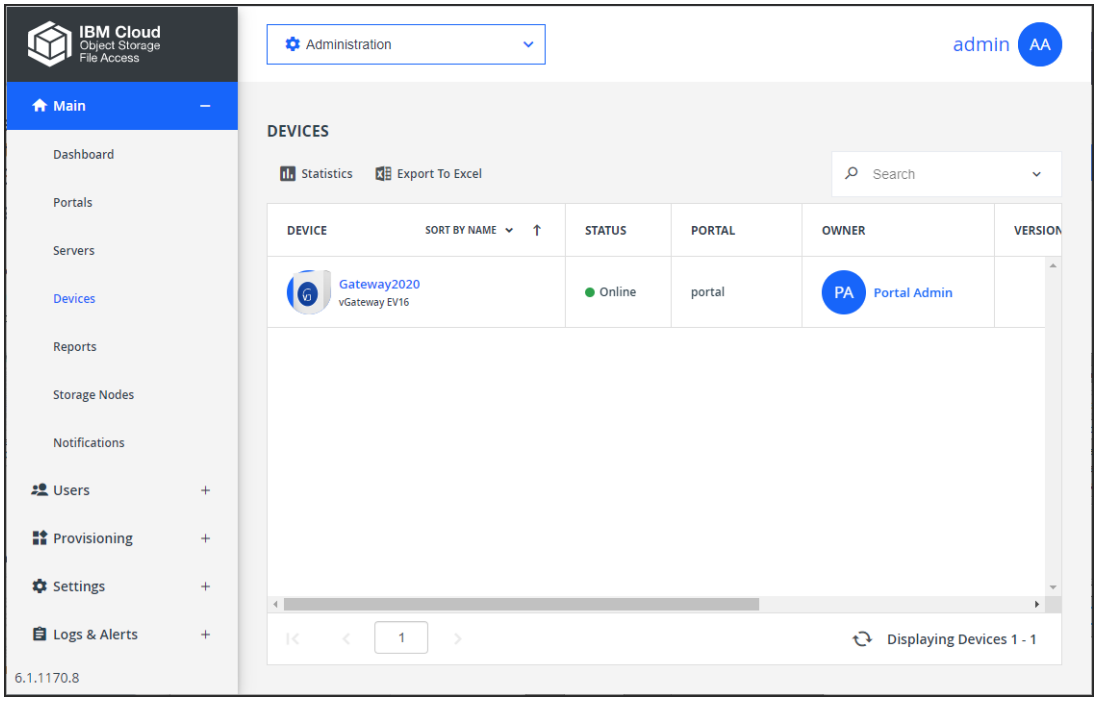
The page includes the following columns:

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**.
PORTAL	The virtual portal in which the device is defined.
OWNER	The user account name of the device's owner. To edit the user account, click the user account name. You are prompted to confirm that you the display will change to the portal with this user.
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:

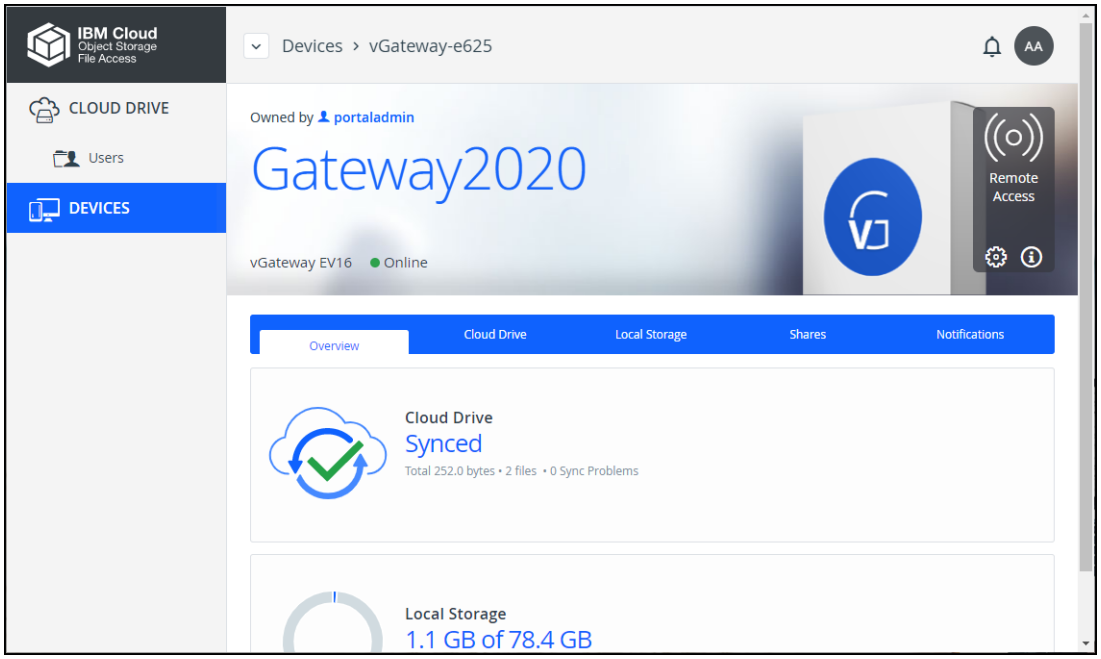
1 In the global administration view, select **Main > Devices** in the navigation pane.
The **DEVICES** page opens, displaying all the devices connected to the portals.



2 Click the device name.

3 A warning is displayed that you will be redirected to the portal the selected device belongs to.

4 Click **CONFIRM**.
The device details are displayed in a new browser window. The details are different whether the device is online or not.



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.

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

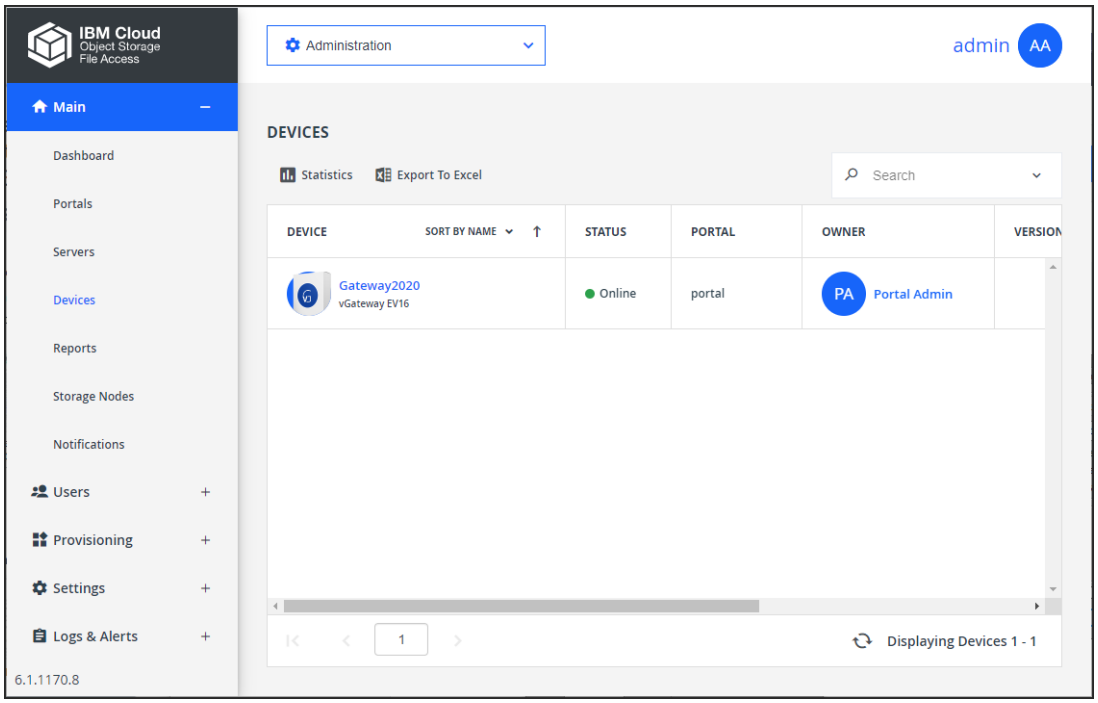
You can manage the following details for a device:

- 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 portal.

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

To manage individual device details:

1 In the global administration view, select **Main > Devices** in the navigation pane.
The **DEVICES** page opens, displaying all the devices connected to the portals.

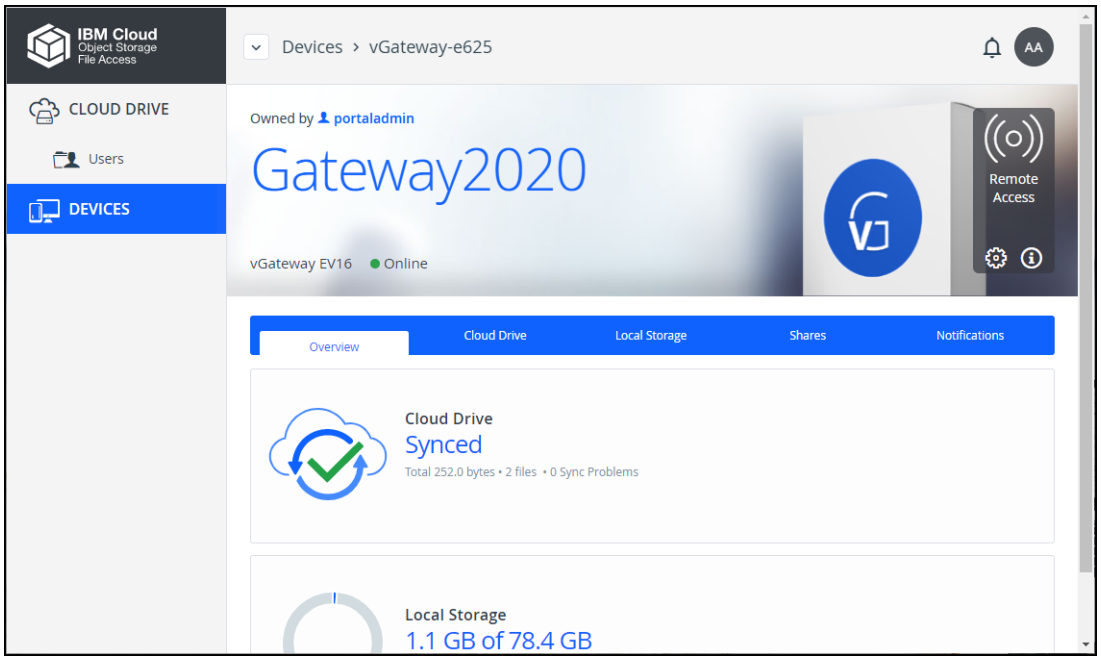


2 Click the device name.

3 A warning is displayed that you will be redirected to the portal the selected device belongs to.

4 Click **CONFIRM**.

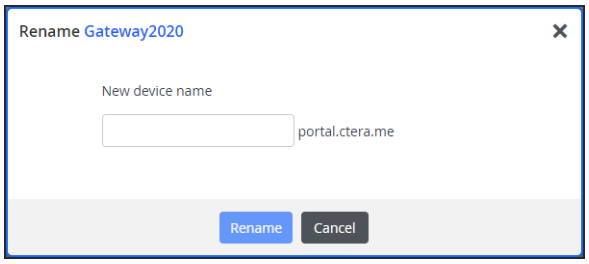
The device details are displayed in a new browser window.



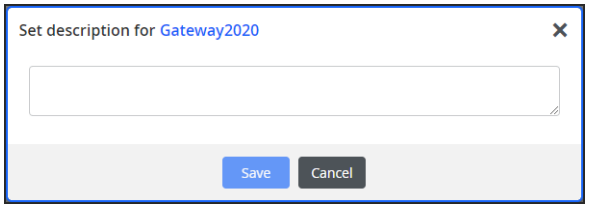
5 Click the  icon and select the option required for the device.

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.

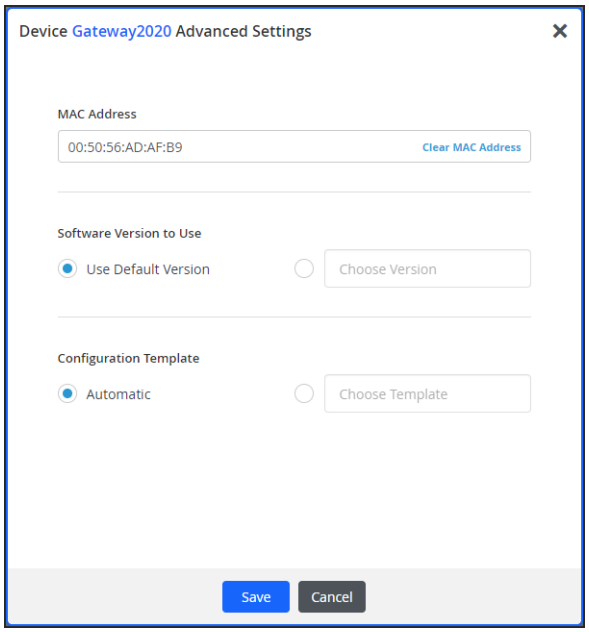
When **Rename Device** is selected, the **Rename** window is displayed.



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.



Enter any information you want to describe the device and click **Save**.
When **Advanced Settings** is selected, the **Device Advanced Settings** window is displayed.



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

To delete a device, see Deleting Devices.

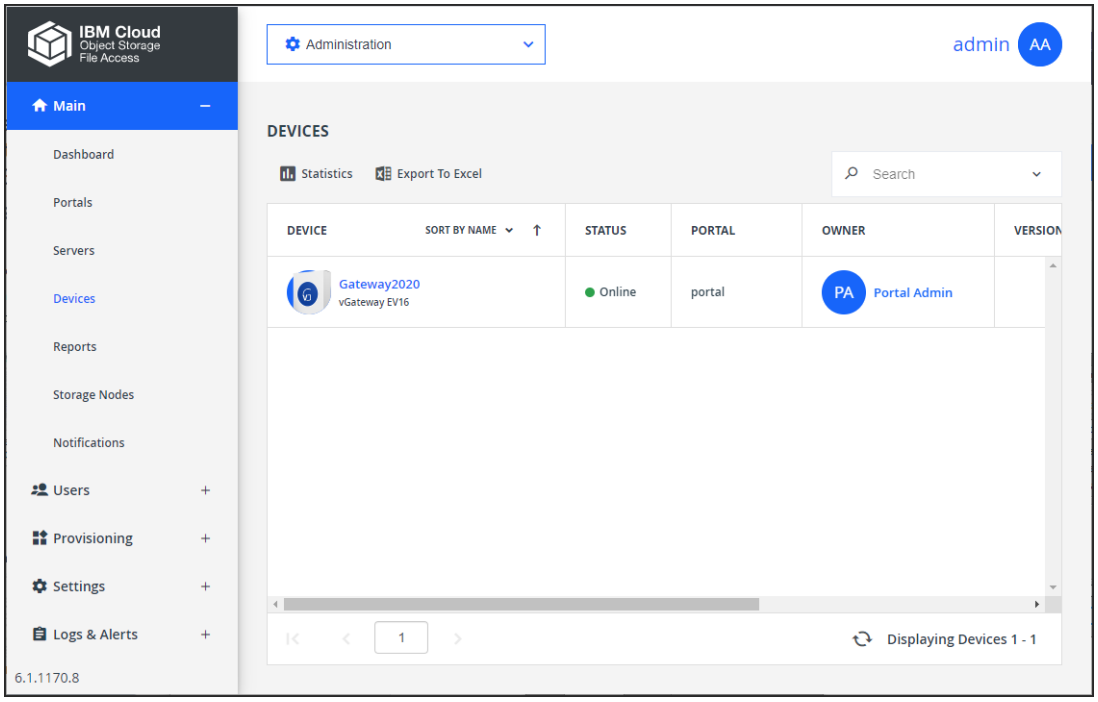
SYNCING CONTENT TO THE IBM COS FA PORTAL

When a IBM COS FA Gateway is connected to the IBM COS FA Portal, files are synced between the IBM COS FA Gateway and the IBM COS FA Portal. You sync content with the 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 portal.

To sync content from the IBM COS FA Portal:

1 In the global administration view, select **Main > Devices** in the navigation pane.
The **DEVICES** page opens, displaying all the devices connected to the portals.

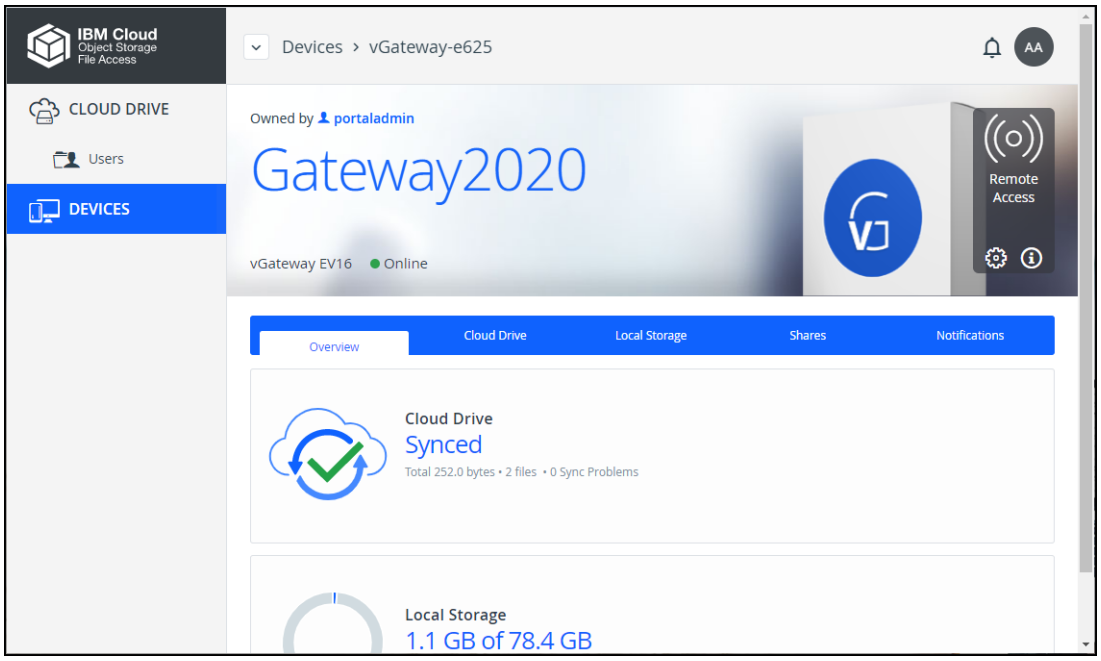


2 Click the device name.

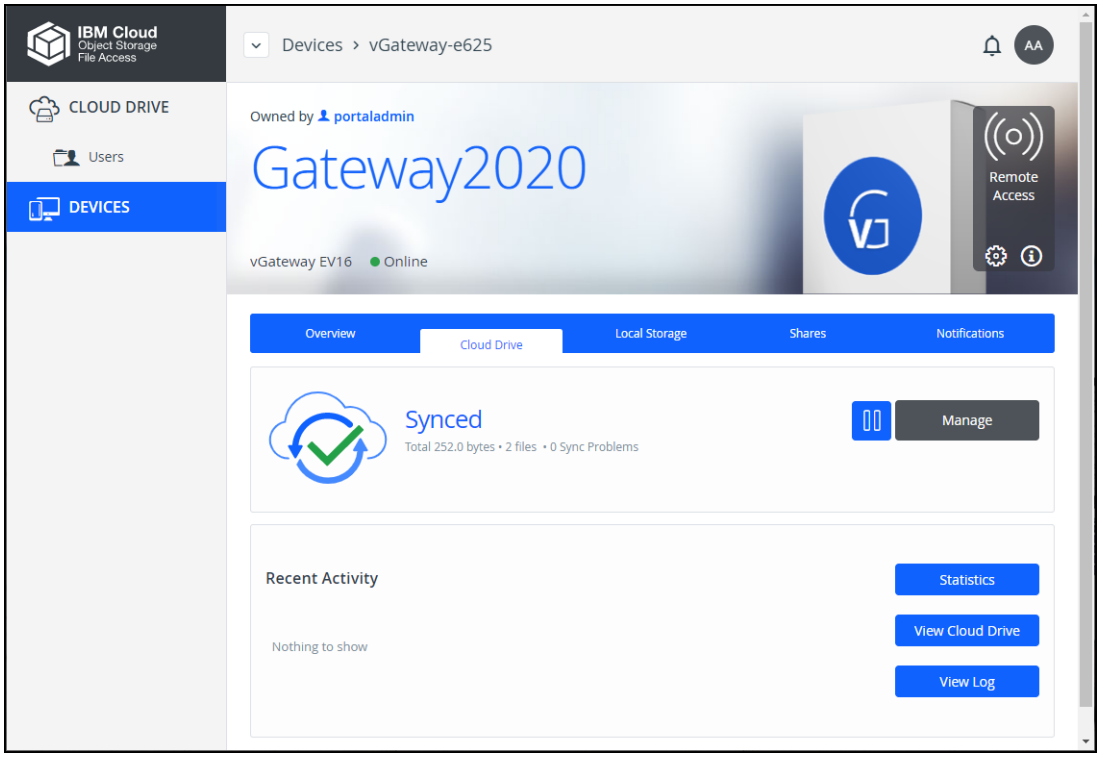
3 A warning is displayed that you will be redirected to the portal the selected device belongs to.

4 Click **CONFIRM**.

The device details are displayed in a new browser window.



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



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

To resume a sync that is suspended running, click  .

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

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.

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 In the global administration view, select **Main > Devices** in the navigation pane.
The **DEVICES** page opens, displaying all the devices connected to the portals.

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 THE 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 in the drop-down after clicking the  icon to view information about the device.

For details about activating this feature, contact IBM.

DELETING DEVICES

To delete a device:

1 In the global administration view, select **Main > Devices** in the navigation pane.
The **DEVICES** page opens, displaying all the devices connected to the portals.

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 15. IBM COS FA PORTAL NOTIFICATIONS

As an administrator, you can receive and view notifications about all portals 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 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.

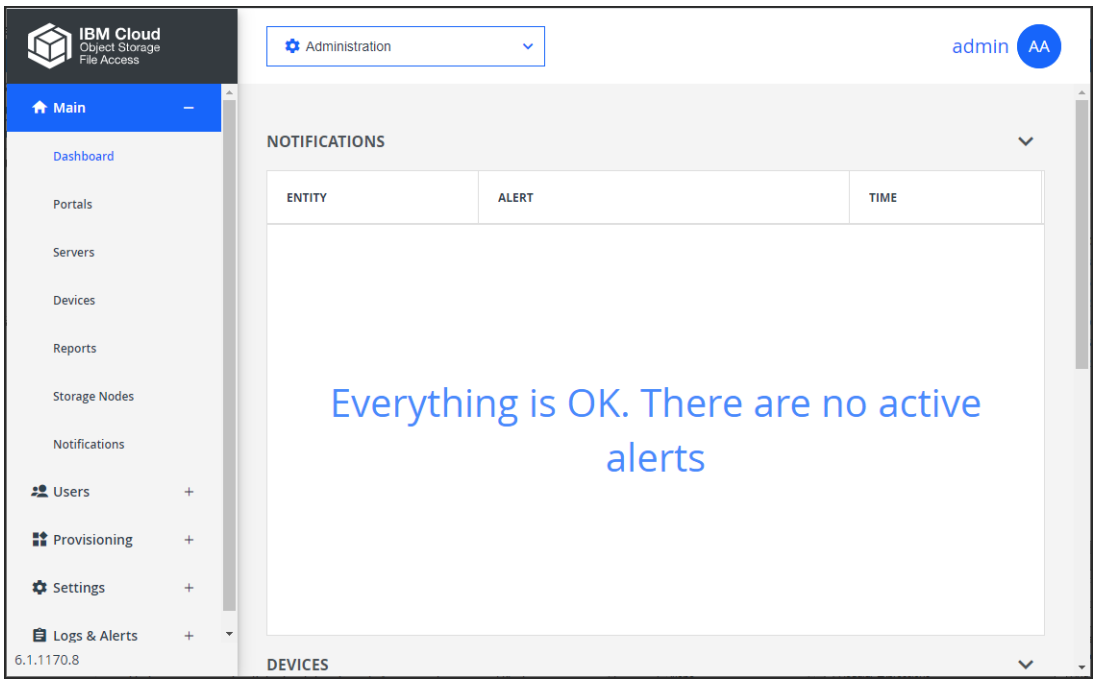
In this chapter

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.

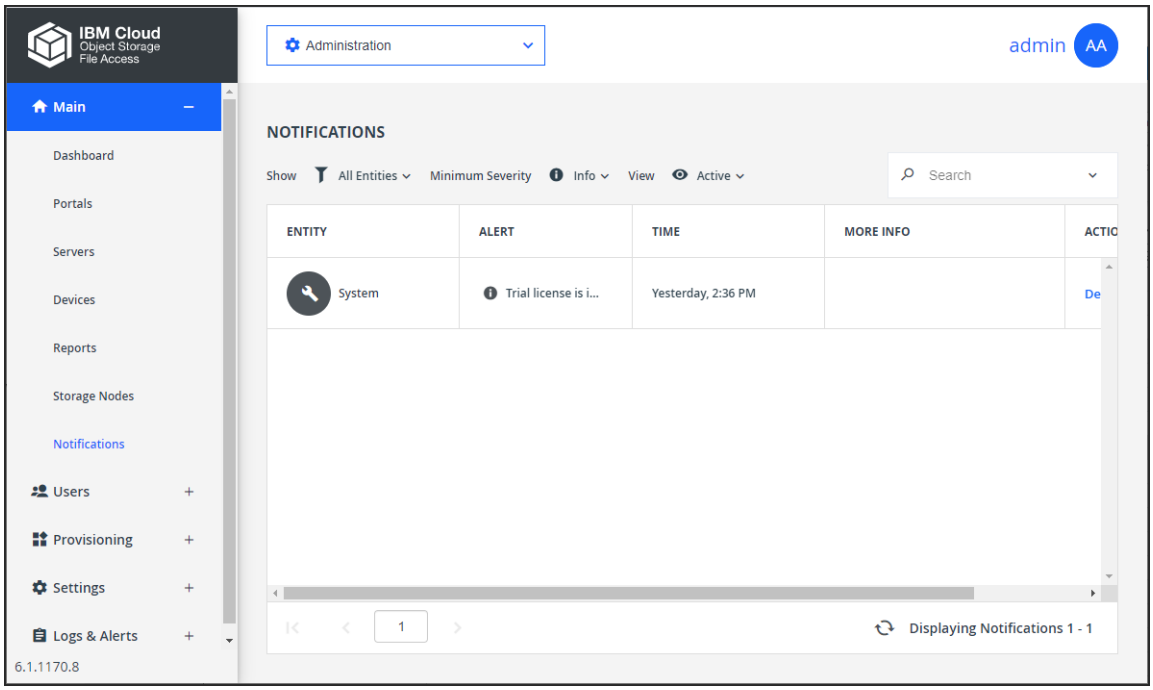


If there are notifications you can go directly to the NOTIFICATIONS page by clicking **SHOW IN NOTIFICATION MANAGER** which is displayed at the bottom of the NOTIFICATIONS panel.

Viewing Notifications in the Notification Page

To view notifications via the notification page:

1 In the global administration view, select **Main > Notifications** in the navigation pane.
The **NOTIFICATIONS** page is displayed.



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 system, storage nodes, and portals.
System – Notifications from the system.
Storage Node – Notifications from the storage nodes.
Portal – Notifications from the portal.
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.

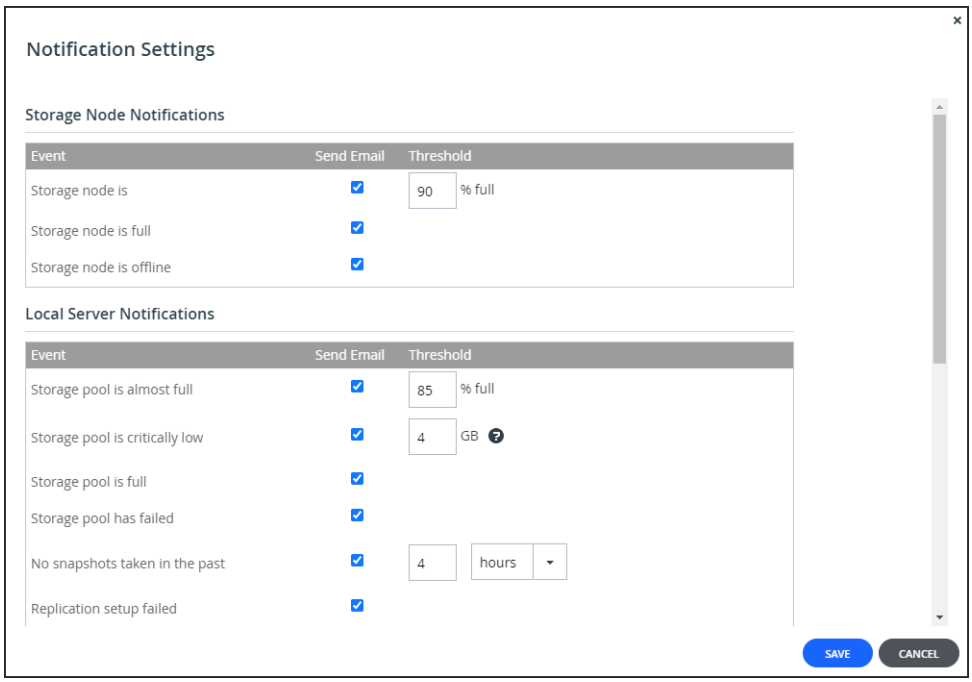
4 You can unhide an notification that you marked as hidden by filtering the display to show hidden notifications and then clicking the **Unhide** link in the **ACTIONS** column for a hidden alert or selecting the notification row and clicking **Unhide**.

CONFIGURING NOTIFICATION SETTINGS

To configure notifications for which emails are sent:

1 In the global administration view, select **Settings** in the navigation pane.

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



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

- Storage node notifications:
  - The storage node is a specified percentage full.
  - The storage node is 100% full.
  - The storage node is offline.
- Local server notifications:
  - The storage pool is a specified percentage full.
  - The storage pool is almost full, under a specified number of gigabytes.
  - The storage pool is full.
  - The storage pool has failed.
  - Snapshots of the storage pool have not been taken for a specified number of hours or days.
  - The storage pool replication failed.
- System notifications:
  - The portal certificate has a specified number of days remaining before it expires.
  - The server is offline.
- Portal notifications:
  - The portal trial is about to expire.
  - The number of devices used exceeds the quota.
  - The amount of storage used exceeds the quota.
  - The amount of storage used is over a specified percentage of the quota.
  - An addon is about to expire.

- An addon has expired.

4 Click **SAVE**.

CHAPTER 16. ANTIVIRUS FILE SCANNING

Antivirus software is used to prevent malware from infecting files in the organization. IBM COS FA Portal integrates with antivirus vendors through the ICAP protocol to ensure data protection.

To implement antivirus scanning of portal files, you require an antivirus license from IBM. Using portal subscription plans, you can activate or deactivate the antivirus feature for specific virtual portals.

When antivirus is activated, files are scanned for malware automatically and transparently, before they are downloaded from the 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 portal administrators can view files that are quarantined by the antivirus servers, the Cloud Drive location and the user who downloaded the files.

In this chapter

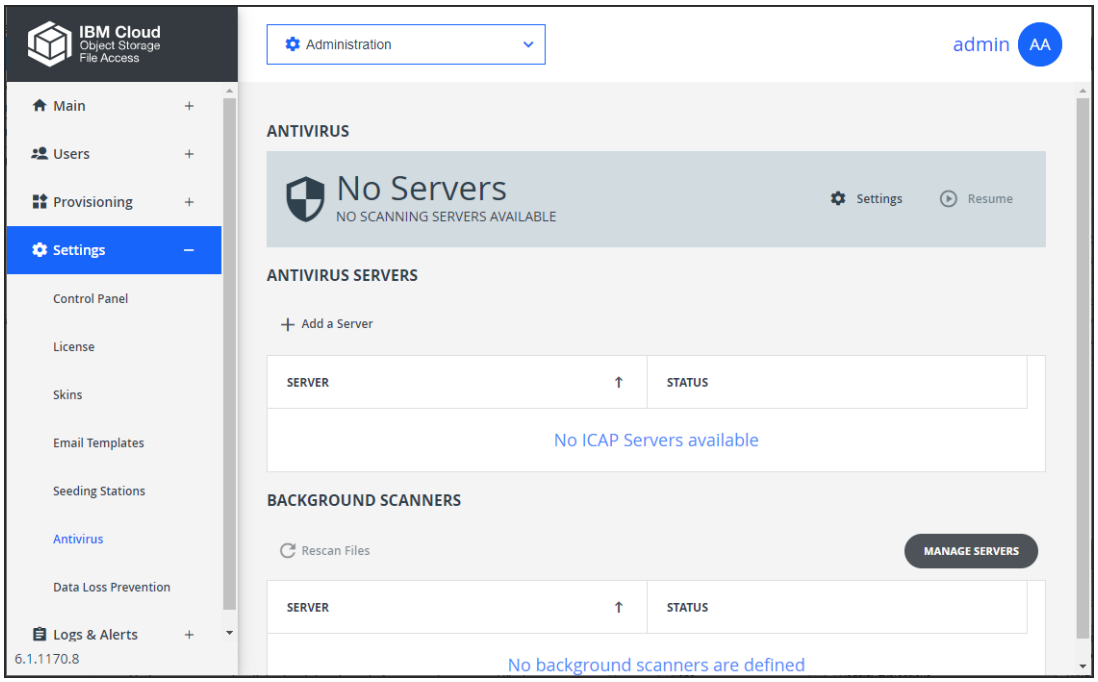
SETTING UP ANTIVIRUS FILE SCANNING

After adding the antivirus license, you add a antivirus server to the portal and then include antivirus scanning in a plan at the global level. Any portal assigned to this plan includes antivirus scanning.

Note: For details about adding a license, refer to Adding License Keys.

To add or edit an antivirus server:

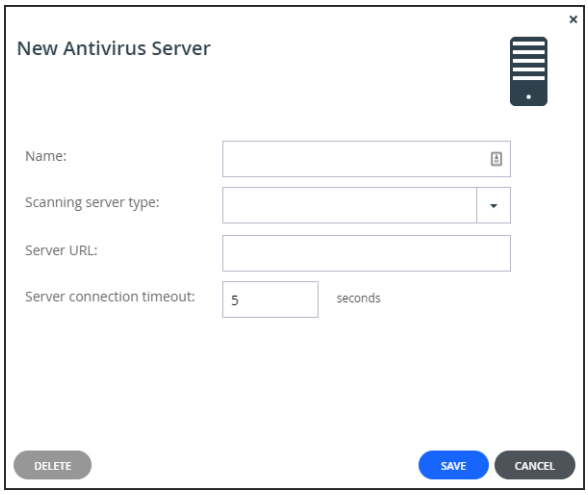
1 In the global administration view, select **Settings > Antivirus** in the navigation pane. The **ANTIVIRUS** page is displayed.



The **Antivirus Status** bar at the top of the page shows the current status:
Active – Antivirus is running on at least one server.
Disabled – Antivirus has been suspended.
Failed – There are no ICAP servers defined.

2 To add a new server, click **Add a Server**.

The **New Antivirus Server** window is displayed.



Or,
To edit an existing antivirus server, click the server's name.
The antivirus server window is displayed with the server as the window title.

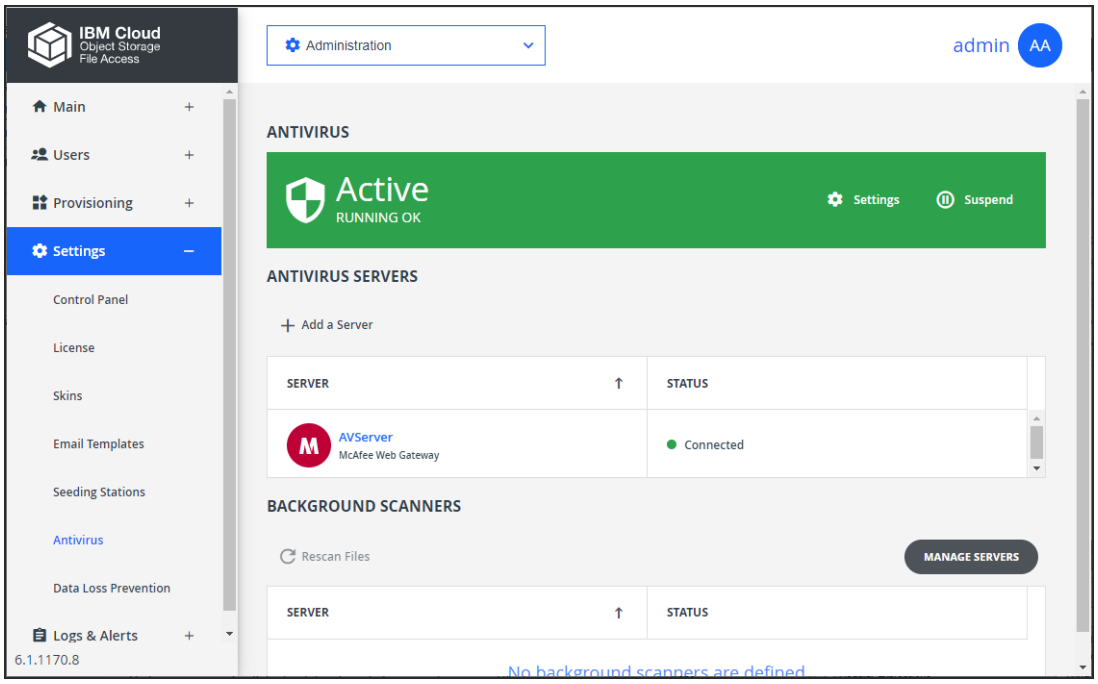
3 Specify the details:
Name – A name for the server.
Scanning server type – Select a supported antivirus:

- McAfee Web Gateway
- Symantec Protection Engine
- ESET Gateway Security
- Sophos AV
- McAfee VirusScan Enterprise for Storage
- Trend Micro InterScan

Server URL – The URL of the server, including the ICAP port and the name of the service. The default ICAP port is 1344. The antivirus service name is configurable in the antivirus server software. Assuming the default ICAP port and default antivirus service name:
For all the scanning server types except for ESET, the URL is `http://IP:1344/avscan`
For ESET the URL is `http://IP:1344/av_scan`
Server connection timeout – The server's connection timeout, in seconds.

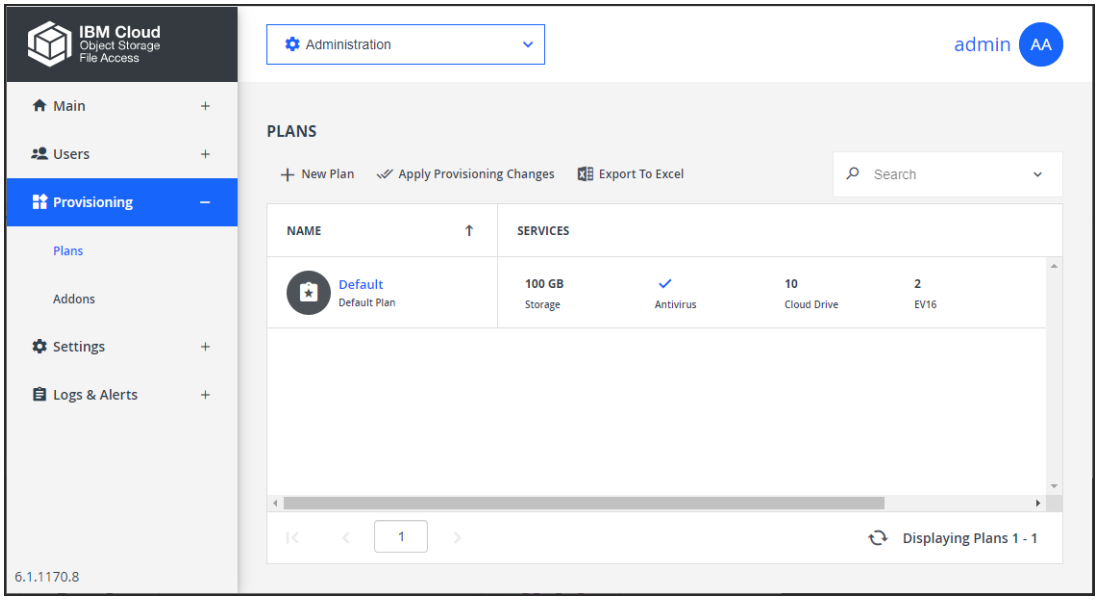
4 Click **SAVE**.

The **ANTIVIRUS** page is displayed.



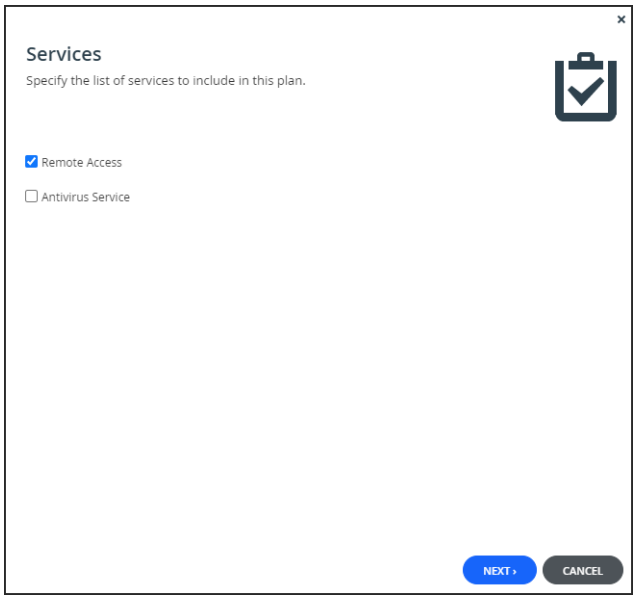
To set up antivirus scanning in a plan:

1 In the global administration view, select **Provisioning > Plans** in the navigation pane. The **PLANS** page is displayed.



2 Click the plan to configure antivirus scanning.

The plan wizard opens, displaying the **Services** window.



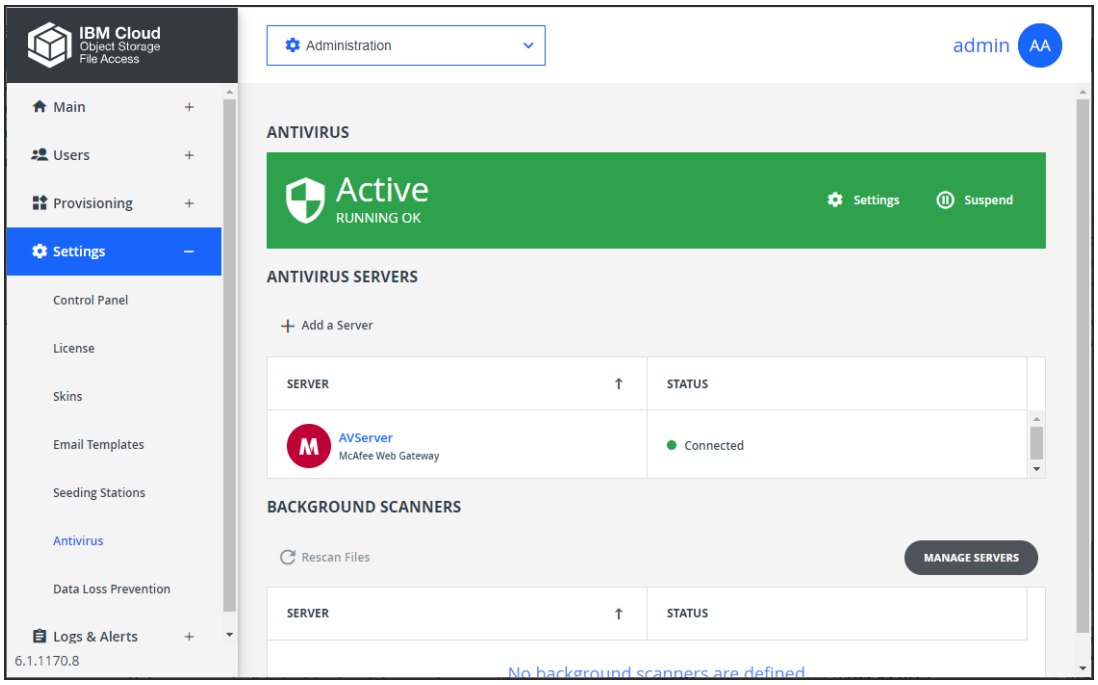
3 Check **Antivirus Service** to activate the antivirus feature and continue with the wizard to completion.
When antivirus is activated, files are scanned for malware automatically and transparently, before they are downloaded for the first time.

MANAGING ANTIVIRUS SERVERS

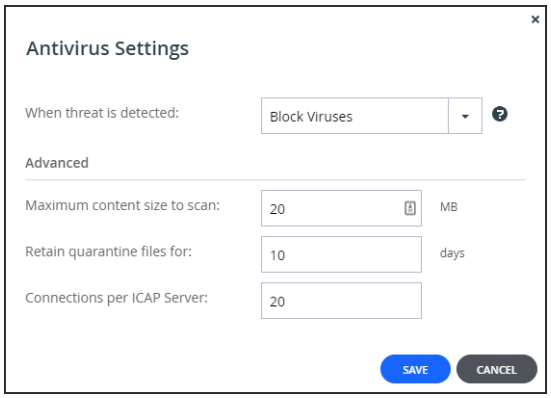
You can specify how infected files are handled and suspend antivirus scanning.

To configure how infected files are handled:

1 In the global administration view, select **Settings > Antivirus** in the navigation pane.
The **ANTIVIRUS** page is displayed.



2 Click **Settings** to configure antivirus scanning.
The **Antivirus Settings** window is displayed.



When a threat is detected – Specify how to handle infected files:

Log Only – An email is sent to the portal listing the file that might be infected and the file is copied to quarantine. It is still possible to download the infected file.

Block Viruses – The infected file is not downloaded and it is quarantined.

Note: Backed up files are not scanned for viruses during a restore.

Maximum content size to scan – The maximum size of a file to be scanned.

Retain quarantine files for – The number of days that files are kept in quarantine before being removed.

Connections per ICAP Server– The number of connections available for use by the portal for the ICAP server.

To suspend or resume antivirus scanning for all servers:

1. In the global administration view, select **Settings > Antivirus** in the navigation pane.
   The **ANTIVIRUS** page is displayed.
2. In the status bar, click **Suspend** to suspend antivirus scanning or **Resume** to resume antivirus scanning for all servers.

To suspend or resume antivirus scanning for a specific server:

1. In the global administration view, select **Settings > Antivirus** in the navigation pane.
   The **ANTIVIRUS** page is displayed.
2. Select the server row in the list of ANTIVIRUS SERVERS.
3. Click **Suspend** to suspend antivirus scanning or **Resume** to resume antivirus scanning for the server.
   The status for resumed servers is `Connected` and for suspended servers `Disabled`.

DELETING AN ANTIVIRUS SERVER

To delete an antivirus server:

1. In the global administration view, select **Settings > Antivirus** in the navigation pane.
   The **ANTIVIRUS** page is displayed.
2. Either,
   a. Select the antivirus server to delete and click **Delete**.
      A confirmation window is displayed.
   b. Click **DELETE SERVER** to confirm.

   Or,
   a. Click the antivirus server's name in the list of ICAP SERVERS.
      The antivirus server window is displayed with the server as the window title.
   b. Click **DELETE**.
      A confirmation window is displayed.
   c. Click **YES** to confirm.

VIRUS PROTECTION

When antivirus scanning is implemented, files are scanned for malware automatically and transparently, before they are downloaded from the 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.

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. In the virtual portal administration view, select **Settings > Antivirus** in the navigation pane.
   The **ANTIVIRUS** page is displayed.
   If no quarantined files were scanned, the quarantine block is displayed as follows:
   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 cloud folders. The number of infected files displayed is for all the folders. In the **Files** view the list of infected files displayed is only from cloud folders. However, 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.

BACKGROUND SCANNING AND RESCANNING FILES

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.

The background scan runs constantly, scanning new files. If there are no new files to scan the scan stops for 30 seconds before checking again for new files to scan.

If you need to run a scan on all the portal files, for example, when the antivirus software signatures database is updated with new viruses, you can initiate the scan. This scan checks all the files, both new files and files that were previously scanned.

It is recommended to manually rescan all the files after unquarantining files.

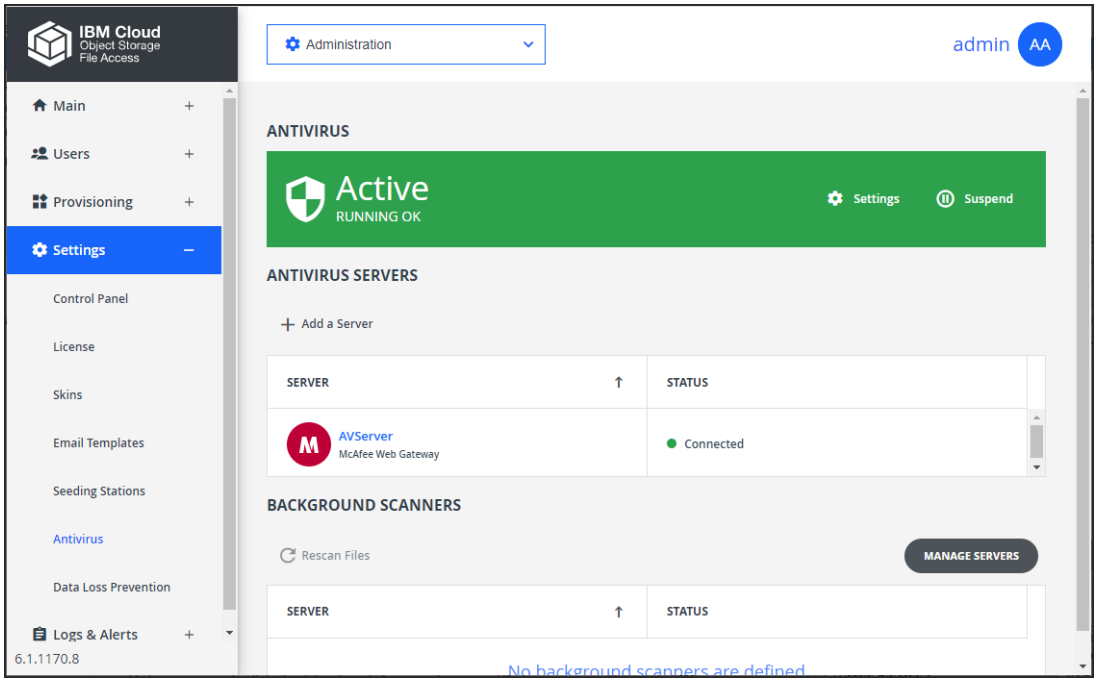
Note: The scan can take a long time, depending on the amount of data in your portal.

The following conditions apply to rescanning files:

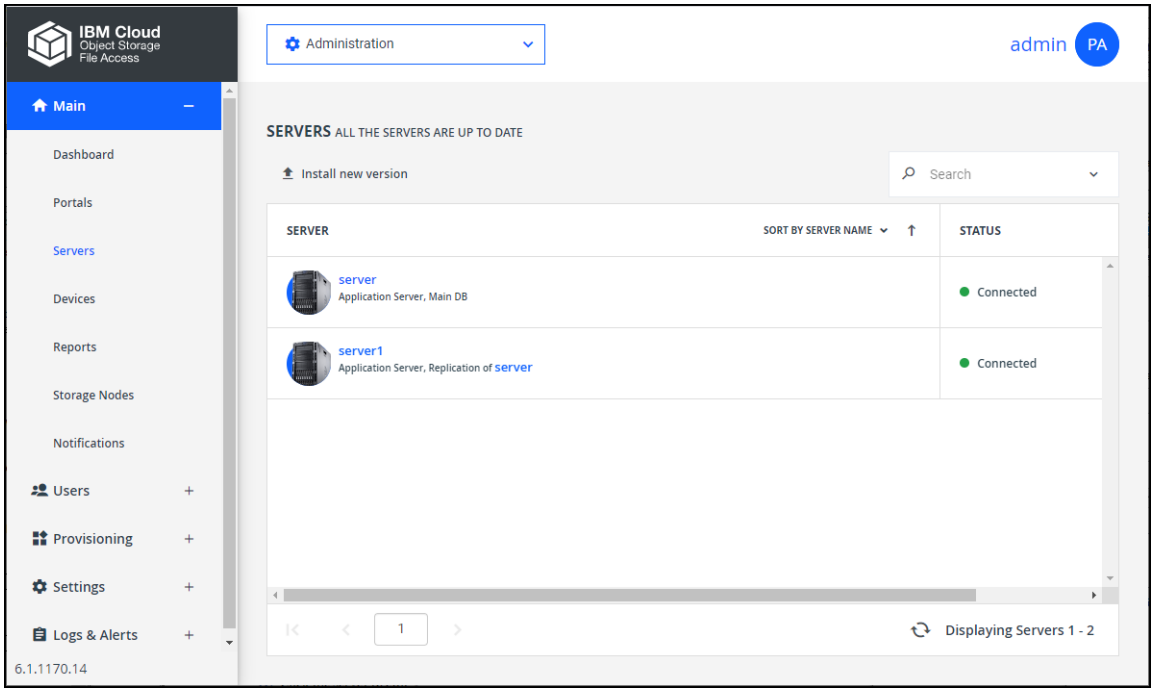
- If a background scan has a file to scan when a rescan is initiated, the background scan completes before the rescan proceeds and files scanned during the background scan are not rescanned.
- Renaming a folder is treated as if the folder and the files in the folder are new. During a background scan the files in the folder are scanned first.

To activate background scanning:

1 In the global administration view, select **Settings > Antivirus** in the navigation pane.
The **ANTIVIRUS** page is displayed.



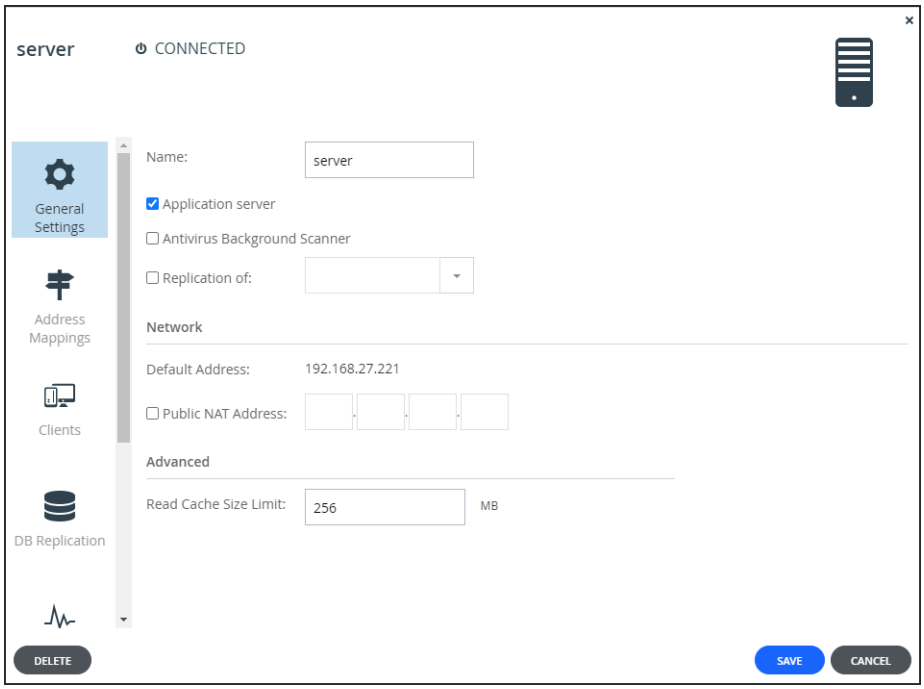
2 Click the **MANAGE SERVERS**.
The **SERVERS** page is displayed.



Note: You can access this page directly by selecting **Main > Servers** in the navigation pane.

3 Click the server to scan in background.

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



4 Check **Antivirus Background Scanner**.

To rescan files:

1 In the global administration view, select **Settings > Antivirus** in the navigation pane.
The **ANTIVIRUS** page is displayed.

2 Click **Rescan Files**.
A confirmation windows is displayed.

3 Click **RESCAN NOW**.

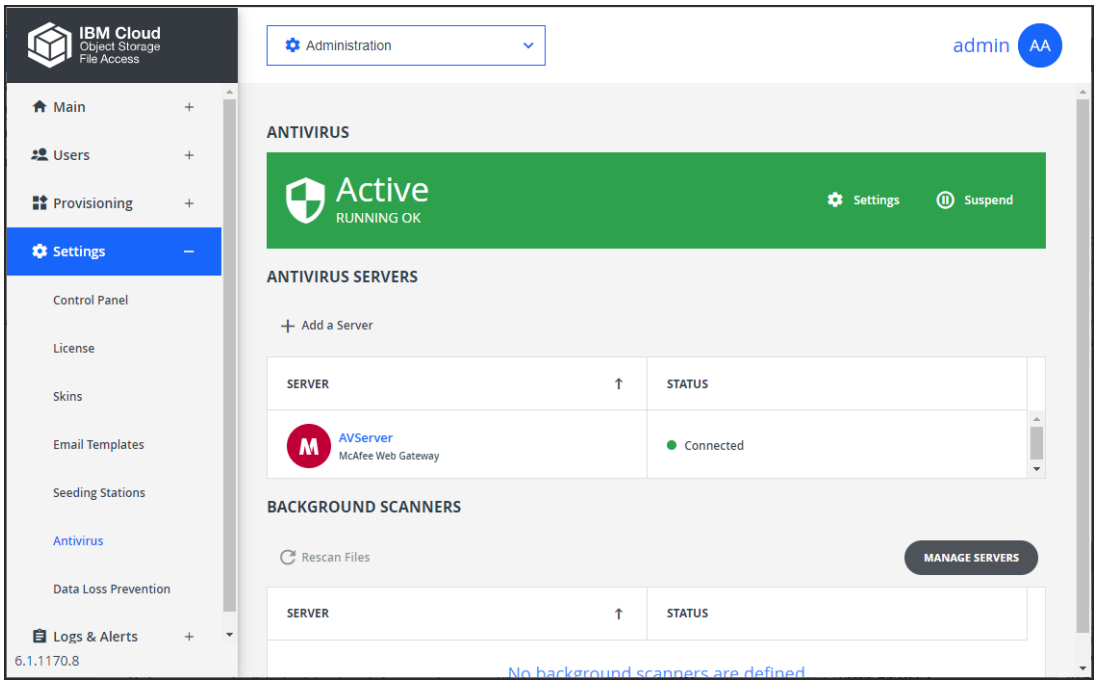
Files on the server are scanned for viruses.

MONITORING ANTIVIRUS SCANNING

You can monitor the antivirus scanning activity as well as the antivirus tasks.

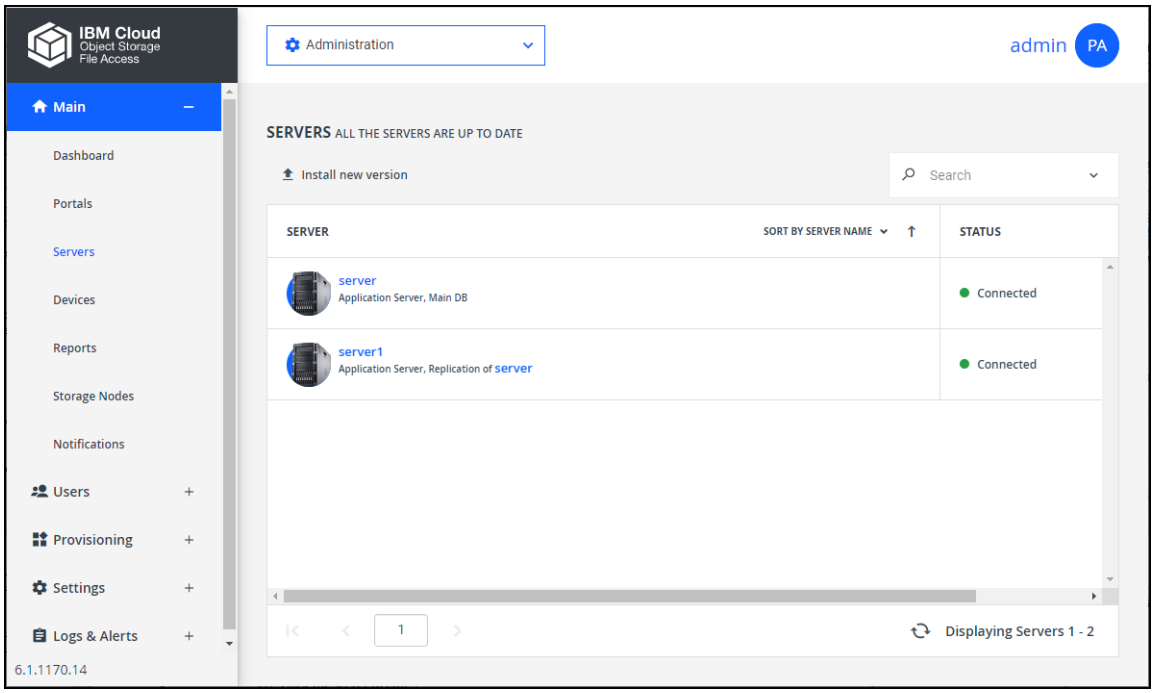
To monitor antivirus scanning:

1 In the global administration view, select **Settings > Antivirus** in the navigation pane. The **ANTIVIRUS** page is displayed.



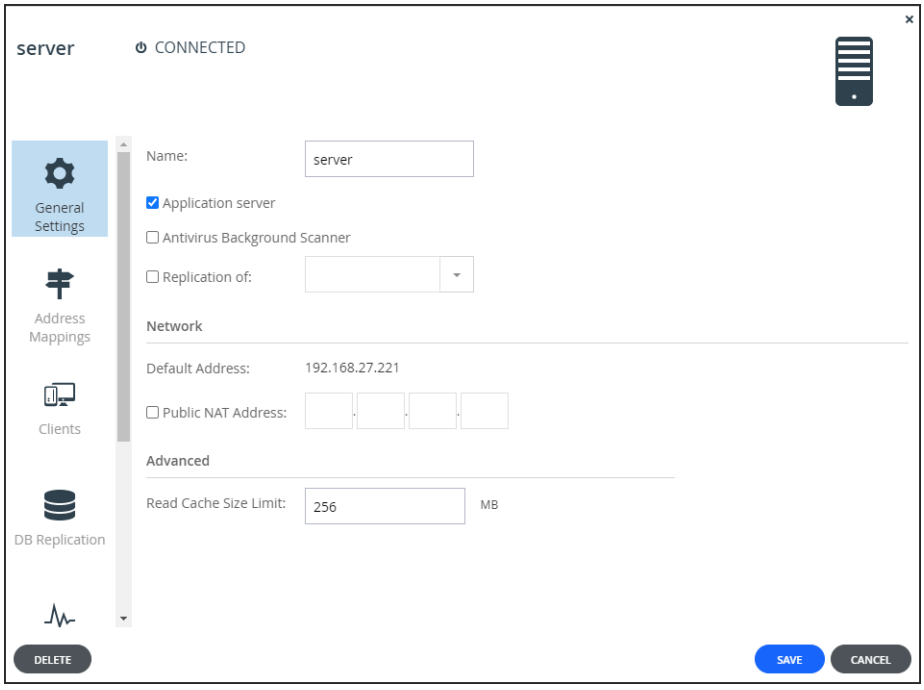
2 Click the **MANAGE SERVERS**.

The **SERVERS** page is displayed.



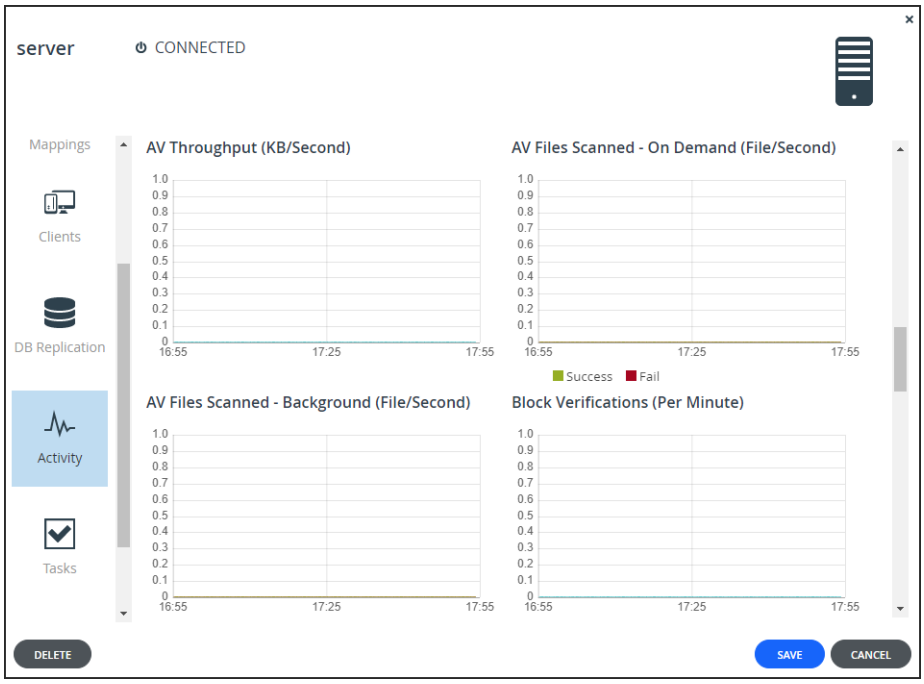
Note: You can access this page directly by selecting **Main > Servers** in the navigation pane.

3 Click the server to monitor.
The server window is displayed with the server name as the window title.



4 In the navigation pane, scroll to **Activity**.

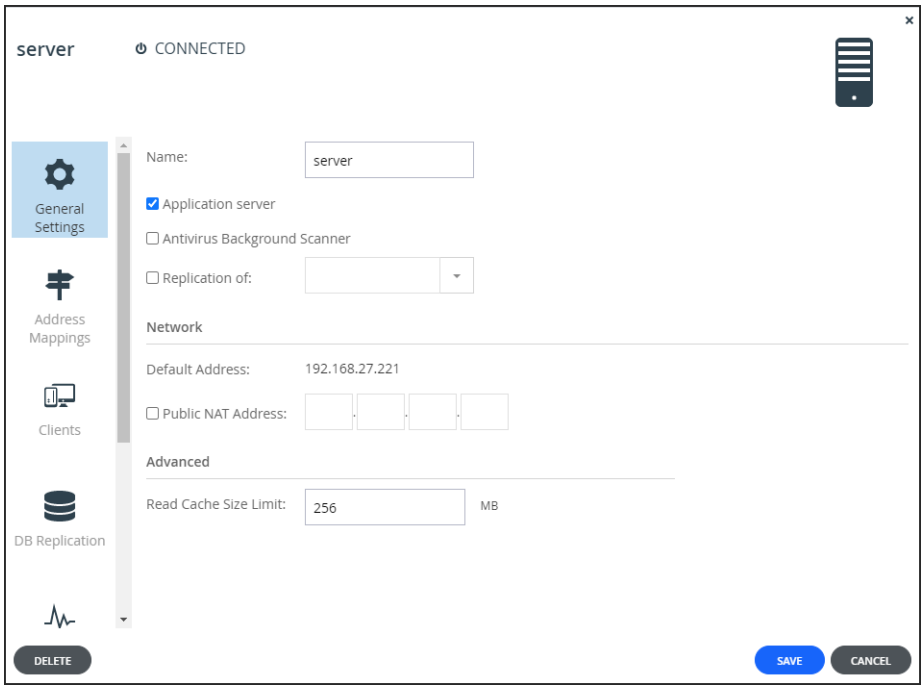
The activity graphs are displayed. Scroll to the antivirus graphs to monitor antivirus activity.



To monitor antivirus tasks:

1. In the administration view, select **Settings > Antivirus** in the navigation pane.
   The **ANTIVIRUS** page is displayed.
2. Click the **MANAGE SERVERS**.
   The **SERVERS** page is displayed.
   Note: You can access this page directly by selecting **Main > Servers** in the navigation pane.
3. Click the server to monitor.

The **server** window is displayed with the server name as the window title.



4 In the navigation pane, scroll to **Tasks**.
The tasks are displayed in the following tabs:

- Running Tasks
- Recently Completed
- Scheduled Tasks

CHAPTER 17. MANAGING LOGS

The portal **Log Viewer** includes the following logs:

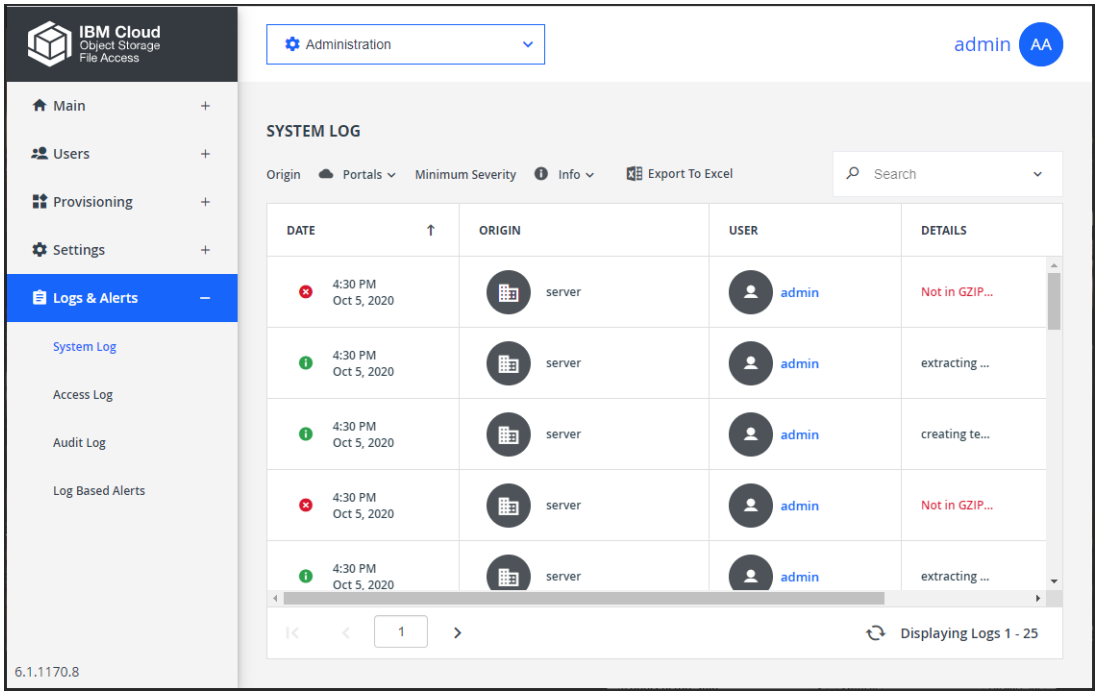
Log	Content
System	Events that do not belong in other log categories.
Access	User access to the IBM COS FA Portal events.
Audit	Changes to the IBM COS FA Portal configuration.

In this chapter

VIEWING SYSTEM LOGS

To view system logs:

- In the global administration view, select **Logs & Alerts > System Log** in the navigation pane. The **SYSTEM LOG** page opens, displaying the system logs connected to the portals.



The information in the System Log can be filtered by:

- The log origin: portal, device or both portal and device.
- The minimum severity: Debug, Info, Warning, Error.

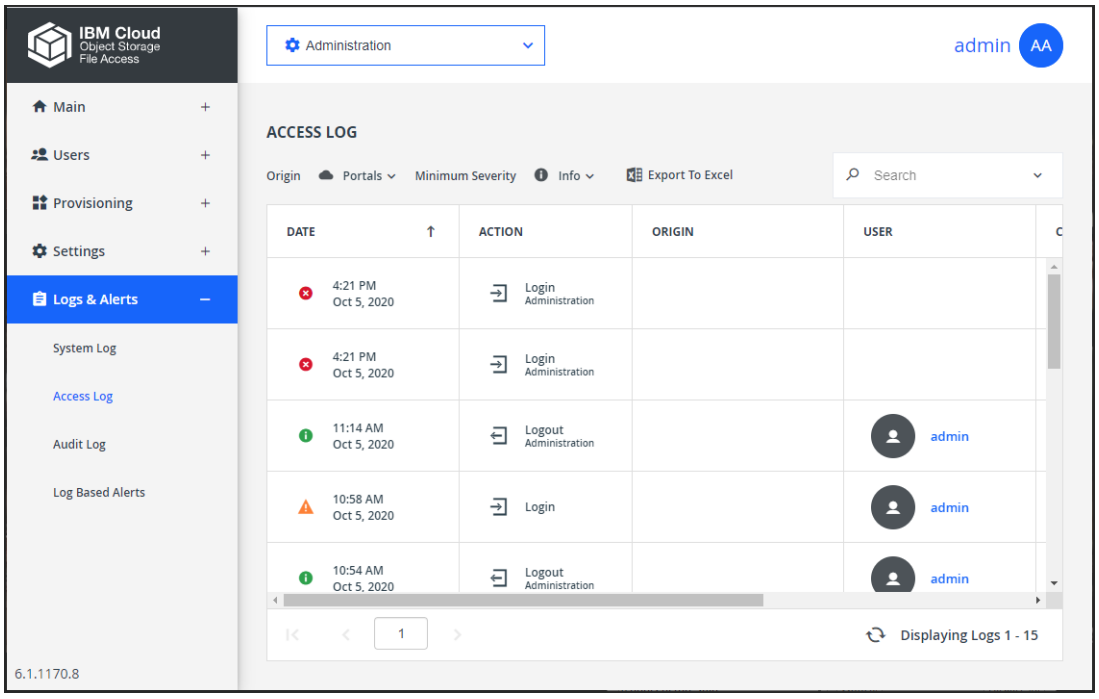
The page includes the following columns:

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 ACCESS LOGS

To view access logs:

- In the global administration view, select **Logs & Alerts > Access Log** in the navigation pane. The **ACCESS LOG** page opens, displaying the access to the portals.



The page includes the following columns:

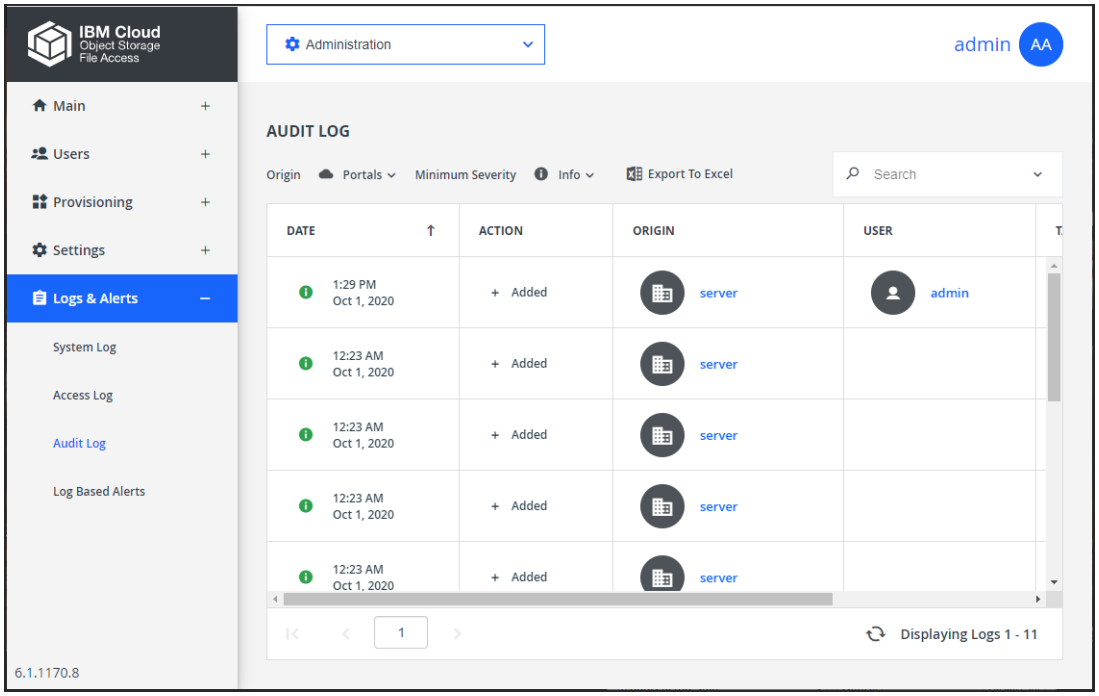
Field	Display
DATE	The date and time at which the event occurred. To the left of the date an icon identifies the event severity: – Info – Warning – Error – Debug
ACTION	The action performed.
ORIGIN	The entity that sent the log entry. To view details about the entity, click the entity name.
USER	The user 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. For example, the user logged out and a file was shared for collaboration.

VIEWING AUDIT LOGS

To view audit logs

- In the global administration view, select **Logs & Alerts > Audit Log** in the navigation pane. The **AUDIT LOG** page opens, displaying the audits to the portals.



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: Added, Modified or Deleted.
ORIGIN	The entity that sent the log entry. To view details about the entity, click the entity name.

Field	Display
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 portals to Excel:

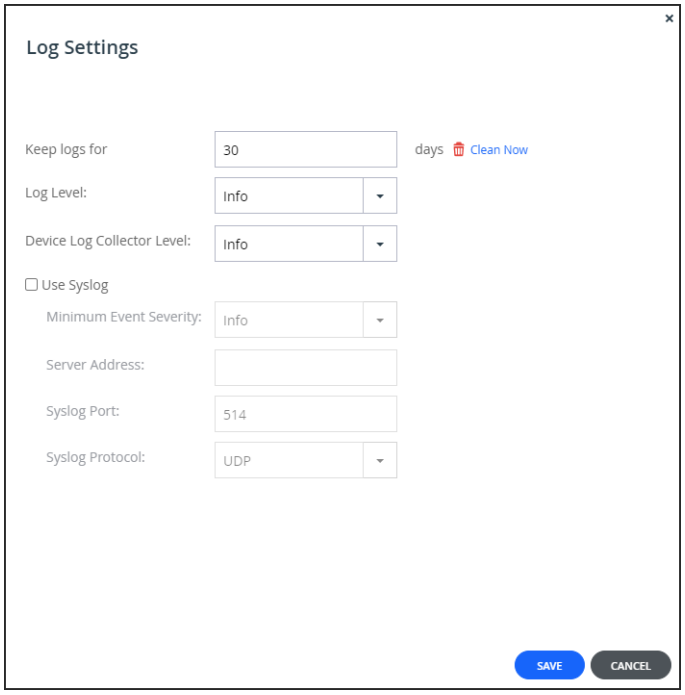
1. In the global administration view, select the log to export under **Logs & Alerts** in the navigation pane.
   The log page is displayed.
2. Click **Export to Excel**.
   The logs in the current log category are exported to your computer.

MANAGING LOG SETTINGS

You can configure IBM COS FA Portal log settings.

To configure log settings:

1. In the global administration view, select **Settings** in the navigation pane.
2. Select **Logs**, under **NOTIFICATIONS AND LOGS** in the **Control Panel** content page.
   The **Log Settings** window is displayed.



3 Complete the fields.
Keep logs for – The number of days that the IBM COS FA Portal should store logs. The default value is 30 days.
Log Level – The minimum log level to display in the IBM COS FA Portal. For example, if you select `Critical`, then only *Emergency*, *Alert*, and *Critical* logs entries are displayed in the IBM COS FA Portal log pages. The default value is `Info`.
Device Log Collector Level – The minimum log level to collect from each device. For example, if you select `Critical`, then only *Emergency*, *Alert*, and *Critical* log events are collected from devices. The default value is `Info`.

4 Check **Use Syslog** if you want to configure the IBM COS FA Portal to send logs to a Syslog server located on your network or in the cloud.

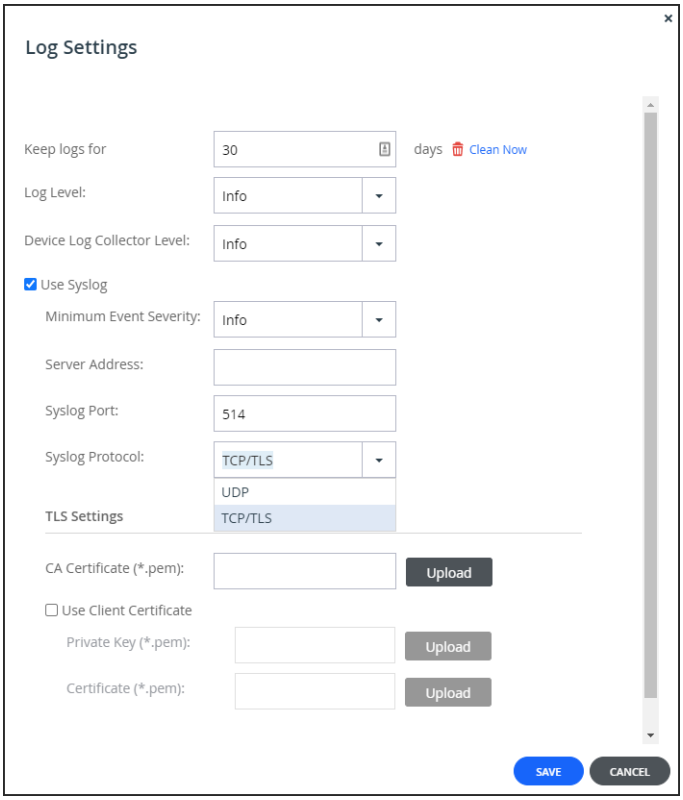
Note: You can obtain free Syslog servers online, such as Kiwi Syslog Daemon (http://www.kiwisyslog.com/).

Minimum Event Severity – The minimum log level to send to the Syslog server. For example, if you select `Critical`, then only *Emergency*, *Alert*, and *Critical* log events are sent to the Syslog server. The default value is `Info`.
Server Address – The Syslog server IP address.
Syslog Port – The Syslog server's port number. The default value is 514.
Syslog Protocol – The protocol to use to send logs. The default is **UDP**.

Note: To send logs securely over TLS the portal image must be 6.1.1059 or higher.

To send logs securely using TLS:

a Change the **Syslog Protocol** to **TCP/TLS**.



b Click **Upload** for **CA Certificate (*.pem)** and browse to your valid CA certificate, select it and click **Open**. The certificate must be in PEM format. If the certificate is valid, **CA Certificate (*.pem)** displays the certificate distinguished name.

c Optionally, check **Use Client Certificate** if you want authentication on both the client and server sides. If client side authentication is enabled:

i Click Upload for **Private Key (*.pem)**, browse to your private key, select it and click **Open**. The private key must be in PEM format.

ii Click **Upload** for **Certificate (*.pem)** and browse to your valid certificate, select it and click **Open**. The certificate must be in PEM format.

If the private key is valid, `Valid` is displayed for **Private Key (*.pem)**. If the certificate is valid, **Certificate (*.pem)** displays the certificate distinguished name.

5 Click **SAVE**.

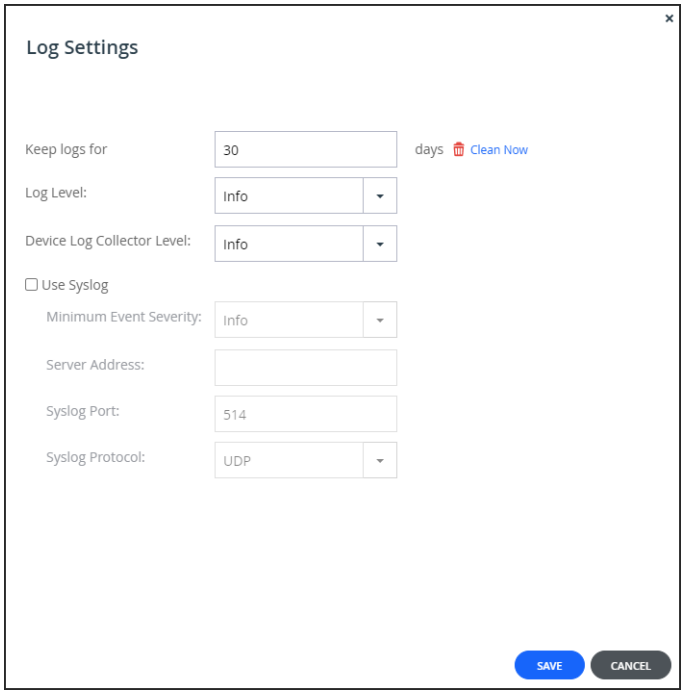
Clearing Logs

You can clear the logs of all virtual portals.

To clear all logs:

1 In the global administration view, select **Settings** in the navigation pane.

2 Select **Logs**, under **NOTIFICATIONS AND LOGS** in the **Control Panel** content page. The **Log Settings** window is displayed.



3 Click **Clean Now**.

Logs are cleared in all virtual portals.

MANAGING ALERTS BASED ON LOG EVENTS

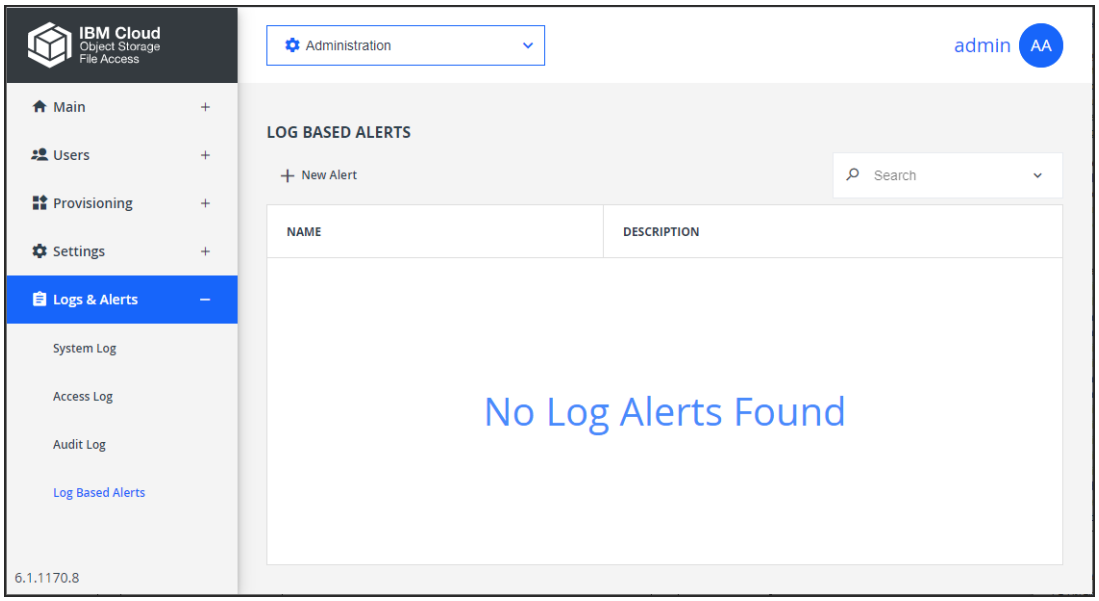
You can configure the IBM COS FA Portal to automatically send email alerts to end users and administrators upon certain IBM COS FA Portal log messages.

In this section

Viewing Log Based Alerts

To view all log based alerts:

- In the global administration view, 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:

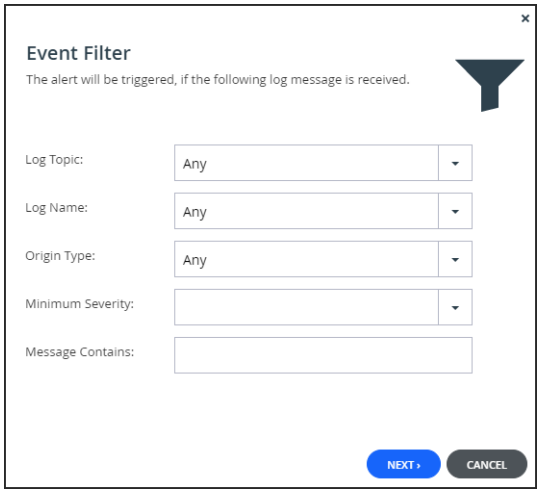
Field	Display
Name	The alert's name. To edit the alert, click the alert's name.
Description	A description of the alert.

Adding and Editing Alerts

To add or edit an alert:

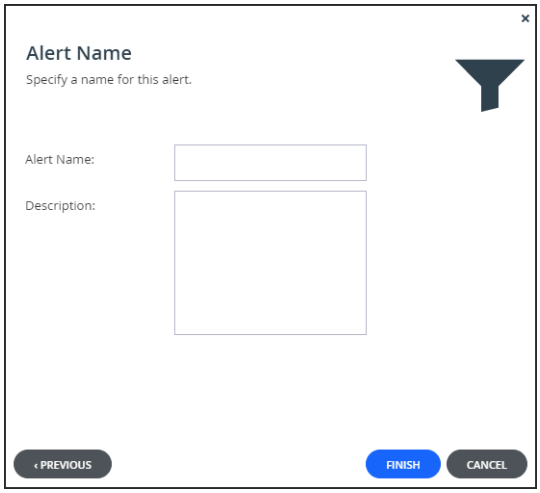
1. In the global administration view, select **Logs & Alerts > Log Based Alerts** in the navigation pane. The **LOG BASED ALERTS** page opens, displaying all the log based alerts.
2. To add a new alert-on, click **New Alert**.
   Or,
   To edit an existing alert, click the alert's name.

The **Event Filter** window is displayed.



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.



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. In the global administration view, select **Logs & Alerts > Log Based Alerts** in the navigation pane. The **LOG BASED ALERTS** page opens, displaying all the Log Based Alerts.
2. Select the alert's 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

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 • NFS • Rsync • iSCSI • CTTP • webdav • WebBrowser
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)

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)
SyncLinuxMaxUserWatches Exceeded	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)
TooMuchDataAsAvaliableOf fline	Too much data was marked as available offline. Please increase the cache size in settings	details (String)
TooMuchDataInNonEvictabl eFolders	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)
CatalogDatabaseIsNotRespondi ng	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)
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)
NfsBadPath	Received NFS request for an invalid path	request (String) host (String) path (String)

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

Class	Message	Additional Attributes
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)
UserLoggedIn	User logged in	Optional: protocol (SessionSource) Optional: clientAddr (String)

Class	Message	Additional Attributes
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)
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)

Class	Message	Additional Attributes
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)
Info	Info	details (String)
InfoLog	Informational Message	details (String)

Class	Message	Additional Attributes
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)

Class	Message	Additional Attributes
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 18. MANAGING REPORTS

The IBM COS FA Portal provides the global administration reports about the virtual portals and storage nodes.

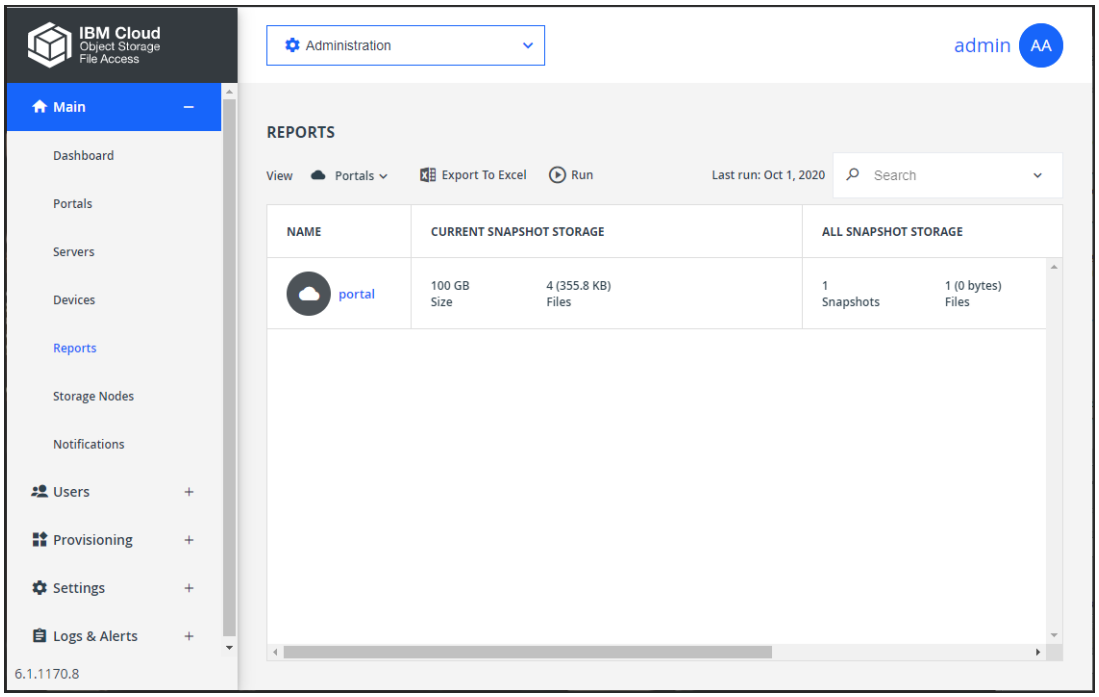
In this chapter

VIEWING THE PORTALS REPORT

Global administrators can view information about all virtual portals.

To view the Portals Report:

- In the global administration view, select **Main > Reports** in the navigation pane.
  The **REPORTS** page opens, displaying all the virtual portals.



Note: If the Portal report is not displayed, select **Portals** from the **View** drop-down list.

The following information is displayed.

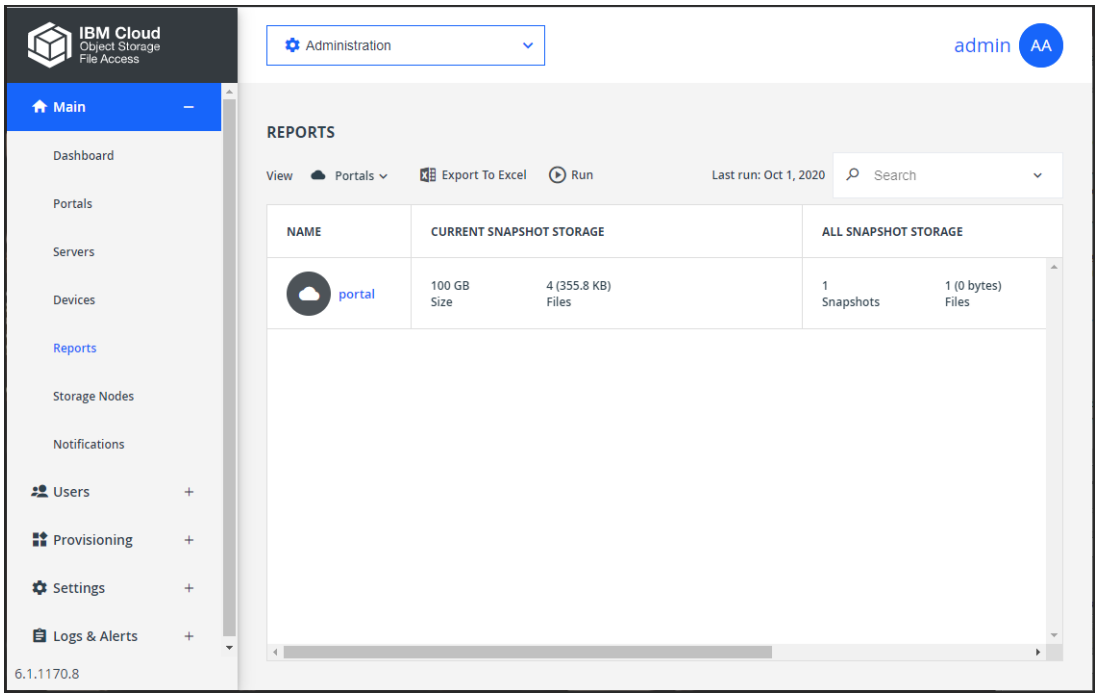
Field	Display
NAME	The virtual portal's name. To view details about the portal and the subscription plan and add-ons defined for the portal, click the portal name.
CURRENT SNAPSHOT STORAGE	Details about the latest snapshot: • The storage quota allocated to this virtual portal. If the quota is unlimited, this value is empty.This field displays the sum of all storage quotas currently being used by users in the portal. • The amount of storage space used in this virtual portal. • 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 portal. • The number of files currently being uploaded.

VIEWING THE STORAGE REPORT

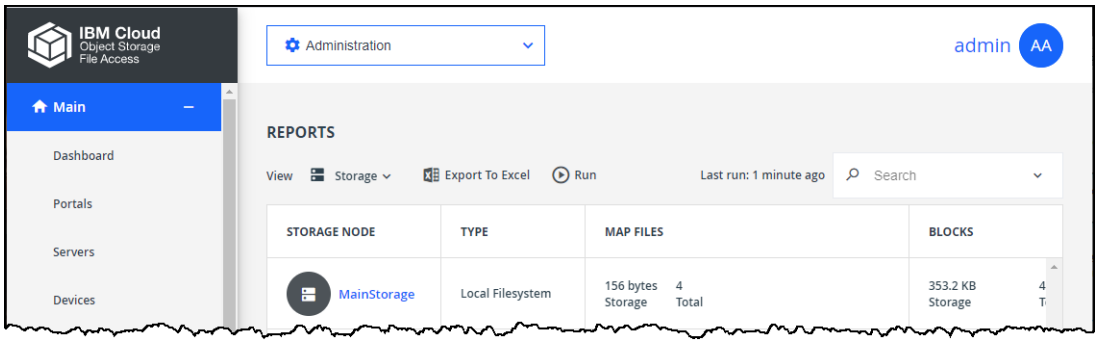
Global administrators can view information about the IBM COS FA Portal storage nodes.

To view the Storage Report:

1 In the global administration view, select **Main > Reports** in the navigation pane.
The **REPORTS** page opens, displaying all the virtual portals.



2 Select **Storage** 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
STORAGE NODE	The name of the storage node. To view details about the storage node and its status, click the storage node name.
TYPE	The storage node's type.
MAP FILES	Details about the storage node: • The amount of space consumed by the mapfiles for this storage node. • The total number of mapfiles in this storage node. • The number of mapfiles currently being uploaded to the storage node. • The number of missing mapfiles in this storage node.
BLOCKS	Details about the storage node: • The amount of space consumed by the blocks for this storage node. • The total number of blocks in this storage node. • The number of blocks currently being uploaded to the storage node. • The number of missing blocks in this storage node.

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. In the global administration view, select **Main > Reports** in the navigation pane.
   The **REPORTS** page is displayed.
2. Select the report to generate, **Portal** or **Storage**, from the **View** drop-down list.
3. Click **Run**.

The report is generated.

EXPORTING REPORTS TO EXCEL

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

To export a report to Microsoft Excel:

1. In the global administration view, select **Main > Reports** in the navigation pane.
   The **REPORTS** page is displayed.
2. Select the report to export, **Portal** or **Storage**, from the **View** drop-down list.
3. Click **Export to Excel**.

The report is exported to your computer.

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

Column	Description
Name	The virtual portal's name.
Quota	The storage quota allocated to this virtual portal in bytes.
Allocated	The amount of storage space used in this virtual portal in bytes.
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.
In Upload	The number of files currently being uploaded.
In Trashcan	The number of deleted files in the trashcan in the virtual portal.
Deleted on	The date the files were deleted.
Deleted by	The user who deleted the files.

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

Column	Description
Name	The name of the storage node.
Type	The storage node's type.
Mapfile Overhead	The amount of space consumed by the mapfiles for this storage node.
Total Mapfiles	The total number of mapfiles in this storage node.
In Upload Mapfiles	The number of mapfiles currently being uploaded to the storage node.
Missing Mapfiles	The number of missing mapfiles in this storage node.
Blocks Storage Space	The amount of space consumed by the blocks for this storage node in bytes.
Uploaded Blocks	The total number of blocks in this storage node.
In Upload Blocks	The number of blocks currently being uploaded to the storage node.
Missing Blocks	The number of missing blocks in this storage node.
Read Only	Whether the storage node is read only or not.

CHAPTER 19. MANAGING SERVERS

As a global administrator, you can manage the servers on which IBM COS FA Portal is installed.

IBM COS FA Portal servers are Tomcat servers (Apace Tomcat) running on CentOS Linux machines. The database used by the IBM COS FA Portal is a PostgreSQL database.

You can use third-party tools to monitor the tomcat servers and portal database. Use these tools to monitor the server. For example, Nagios, www.nagios.com, provides complete monitoring of CentOS Linux operating systems, including operating system metrics, service state, process state, and file system usage. To monitor the database you can use a tool such as Open PostgreSQL Monitoring (OPM).

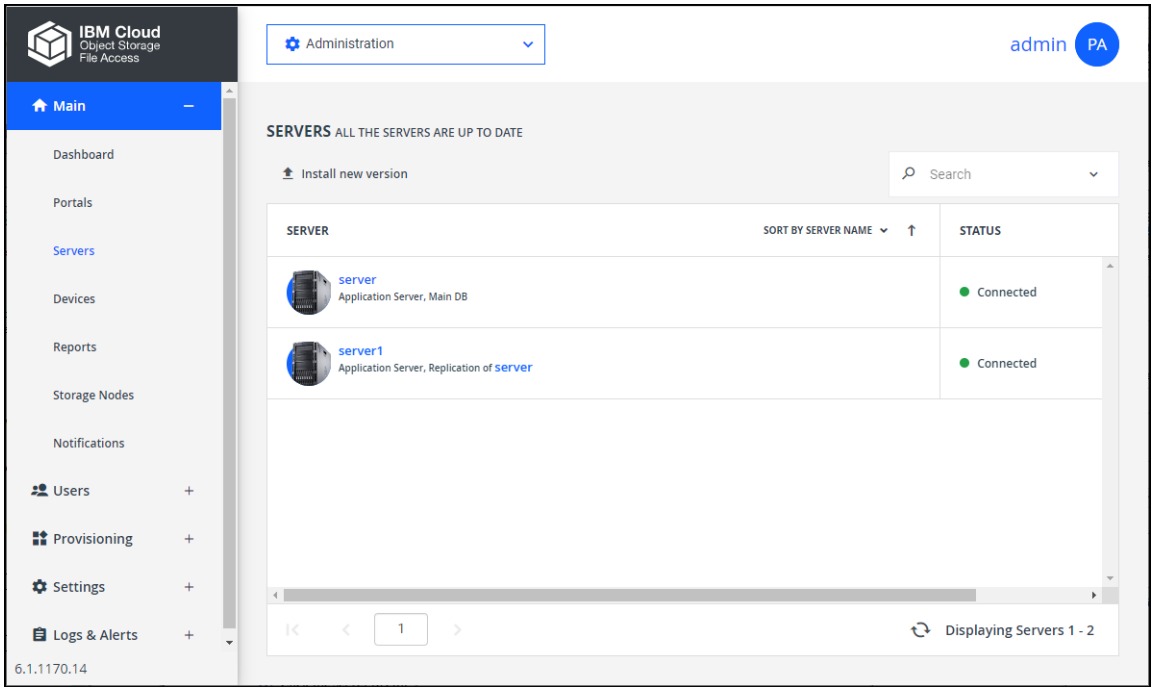
In this chapter

Note: For details about adding servers, refer to the installation documentation for your environment.

VIEWING SERVERS

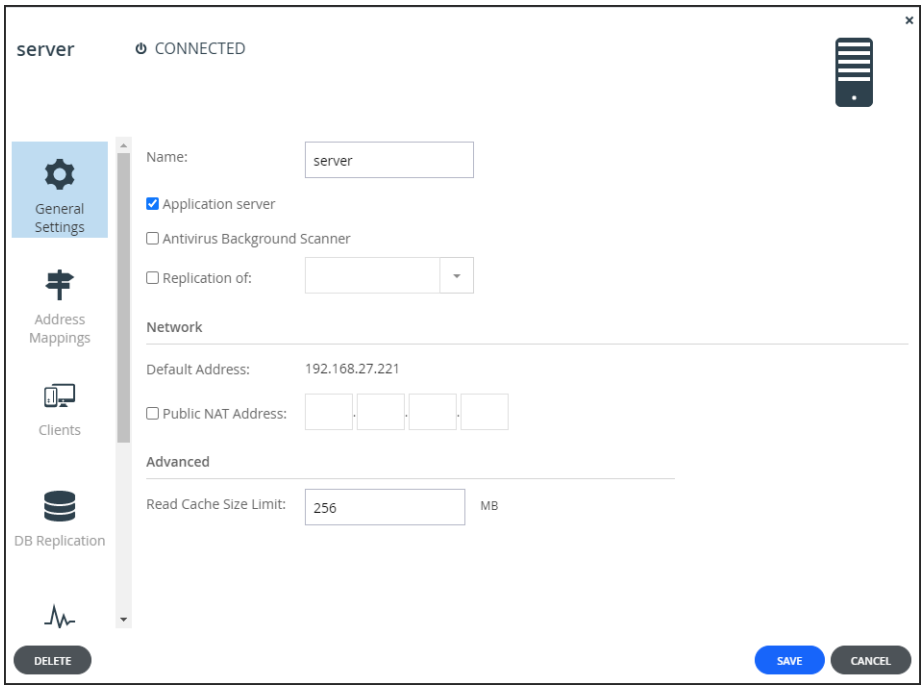
To view the IBM COS FA Portal servers:

1 In the global administration view, select **Main > Servers** in the navigation pane.
The **SERVERS** page is displayed, listing all the servers for the IBM COS FA Portal.



2 To view server settings, click the server name.

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



For details refer to Editing Server Settings.

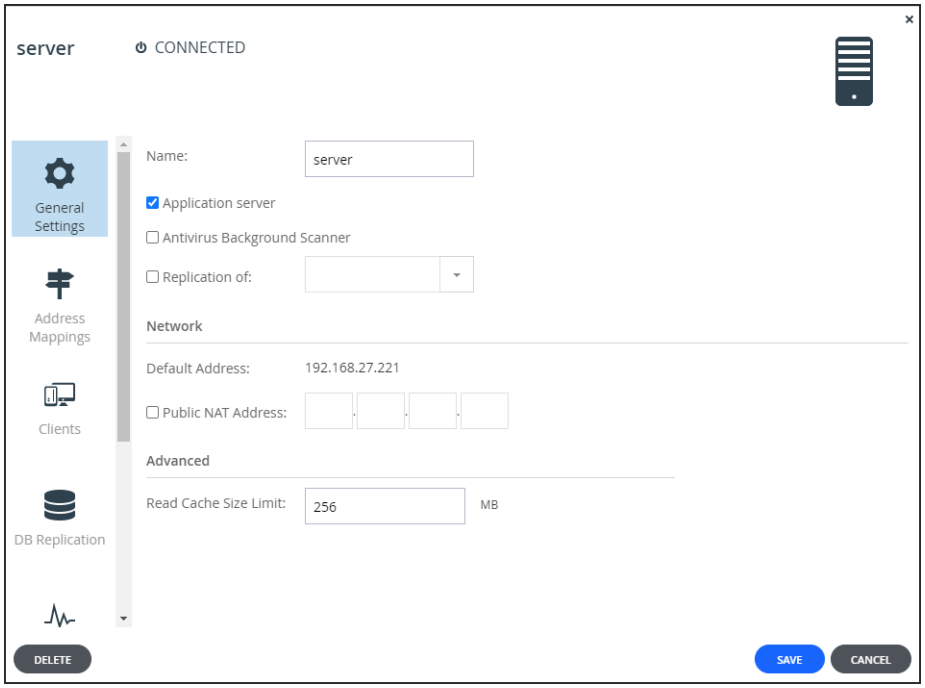
EDITING SERVER SETTINGS

To edit server settings:

1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed, listing all the servers for the IBM COS FA Portal.
2. Click the server to edit.
   The server window is displayed with the server name as the window title.
3. Edit and monitor the following settings:
   - General Settings
   - Address Mappings
   - Clients
   - DB Replication
   - Activity
   - Tasks
   - Status
4. Click **SAVE**.

General Settings

You can edit server settings, including configuring a server as an application server, setting the public IP address of the server, and the IP address to which each virtual portal's DNS should resolve. This allows you to restrict specific portals to be accessible only from a specific network interface.

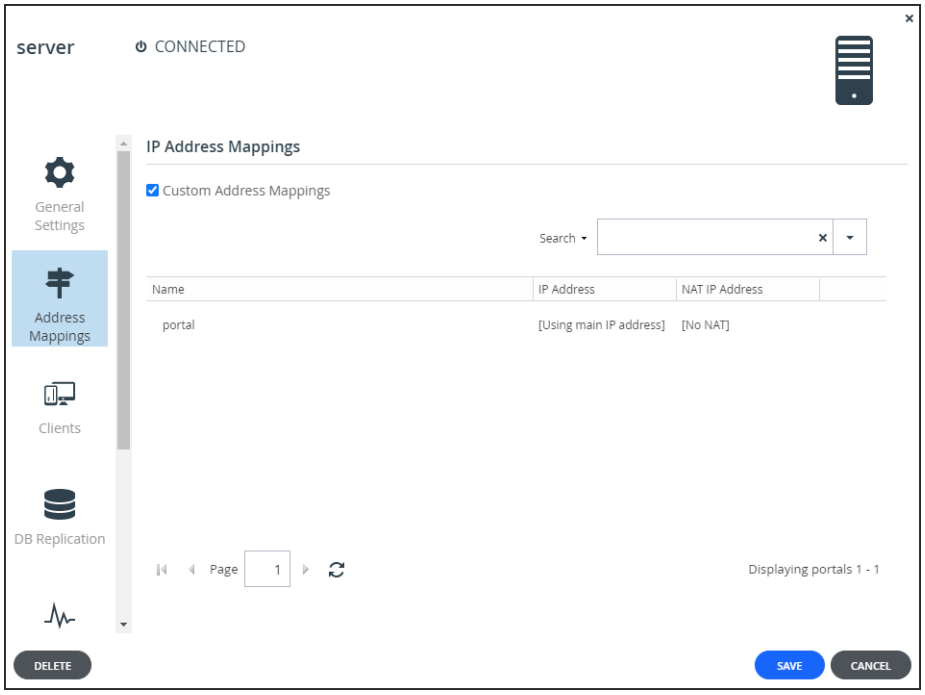


- In the **General Settings** option, you can edit the following settings:
  Name – The unique name of the server.
  Application server – The server is an application server. An application server accepts CTTP connections from IBM COS FA Gateways and HTTPS connections from end users. If unchecked, this server does not allow any client logins. IBM recommends designating at least two servers to act as application servers, for high availability.
  Antivirus Background Scanner – An antivirus background scan runs on this server.
  Replication of – The server is a replication server of the specified server. Replication is configured when the server is installed.
  Default Address – The default IP address of the server.
  Public NAT Address – The default IP address has a public Network Address Translation (NAT). Specify the public IP address. This controls the default IP address of this server that is exposed using DNS.
  Read Cache Size Limit – The maximum amount of server RAM to allocate to the read cache that is used to accelerate reads from the storage nodes.

5 Click **SAVE**.

Address Mappings

By default, IBM COS FA Portal listens to virtual portals on the default address. You can optionally bind specific virtual portals to other interfaces (specified by IP address) of the server, which will cause this IP address to be published by the DNS server, and will prevent access to the specified portal via other IP addresses of the server.

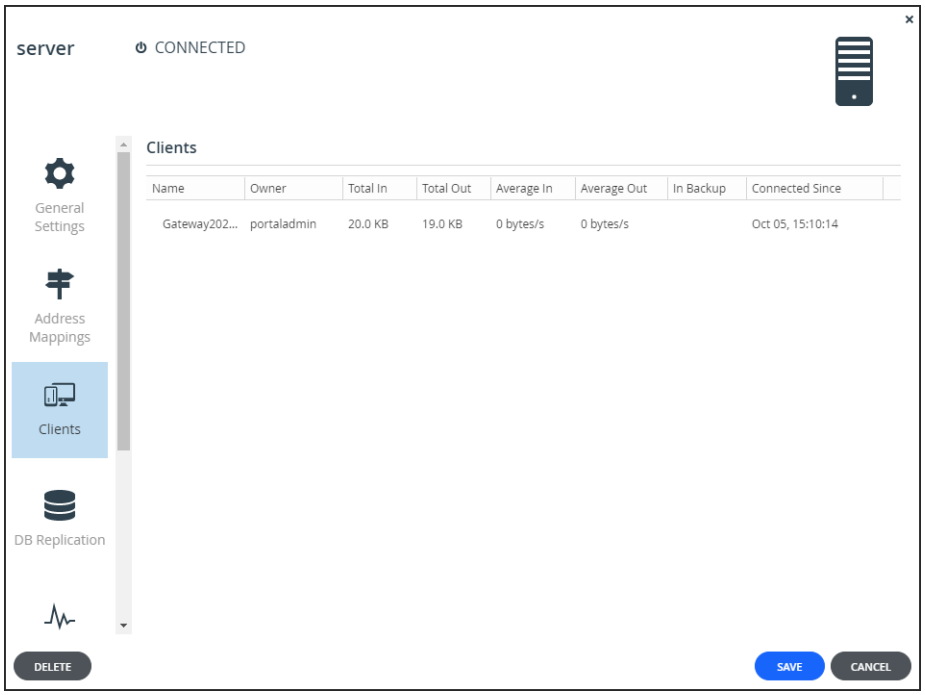


To set custom address mappings:

- In the **Address Mappings** option, you can edit the following settings:
  Custom Address Mappings – Check to enable the content for editing.
  Name – The name of a virtual portal.
  IP Address – The IP address for the virtual portal bound to an IP address of the server. If the virtual portal uses the default IP address, `Using main IP address` is displayed. You can change this to an IP address of the local interface to accept connections for clients.
  NAT IP Address – If NAT is used, and the public IP address of the interface differs from the private IP address, specify the IP address to which the original IP address should be translated. This public address will be published by the IBM COS FA Portal DNS server. To bind this virtual portal to the default IP address, do not enter a value in this field. To specify that the public IP address is equal to the private IP address, do not enter a value in this field.

Clients

You can view information about a server's currently connected devices.



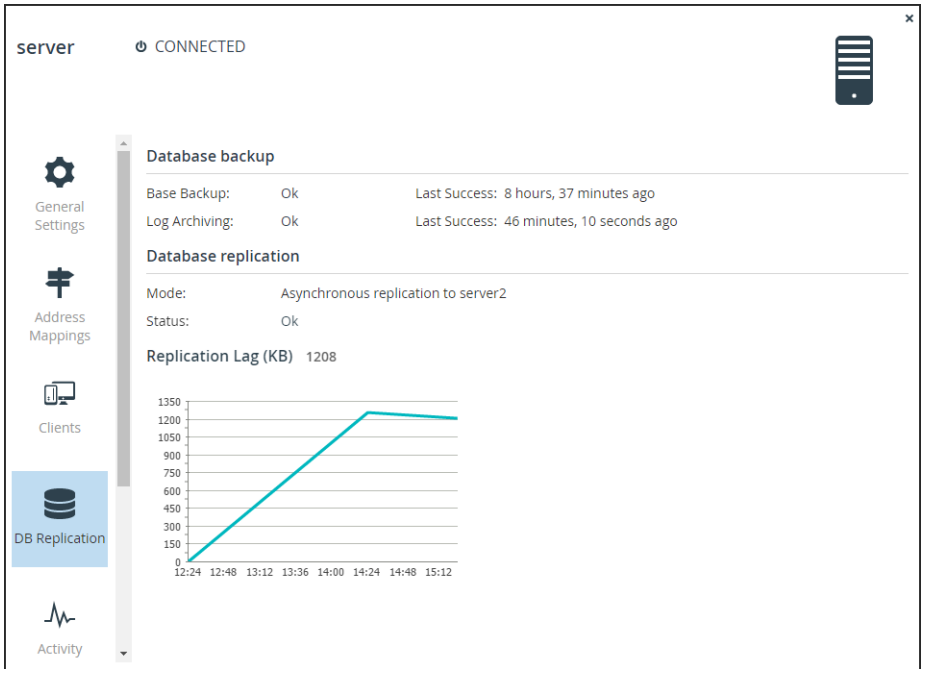
To view a server's currently connected devices:

- In the **Clients** option, you can view the following settings:
  Name – The name of the client device.
  Owner – The name of the client device's owner.
  Total In – The total CTTP traffic sent from the client device to the virtual portal.
  Total Out – The total CTTP traffic sent from the virtual portal to the client device.
  Average In – The average speed, throughput, of traffic sent from the client device to the virtual portal in bytes/second.
  Average Out – The average speed, throughput, of traffic sent from the virtual portal to the client device in bytes/second.
  Connected Since – The date and time when the connection started.

DB Replication

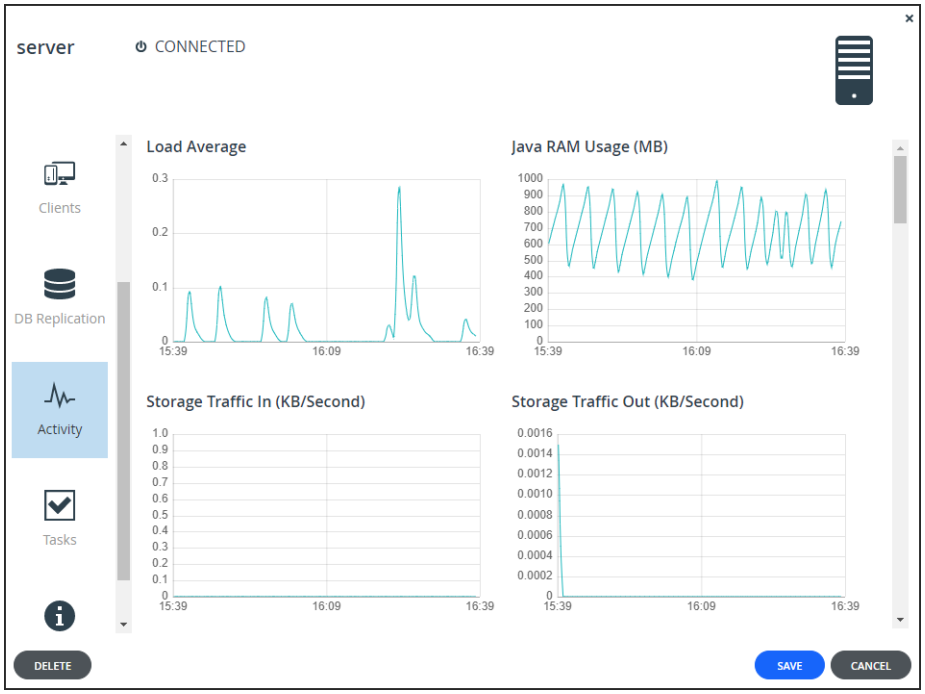
You can monitor the performance of the replication server by selecting the **DB Replication** tab in the server manager.

The portal reports the status of its scheduled base backups and transaction log archiving process, as well as additional metrics to help detect when database replication falls behind due to lags in the process. In the event that replication falls behind, portal administrators are notified via email. The relevant email templates are *Replication setup failed* and *Replication has errors*.



Activity

You can view charts displaying a server's activity data.



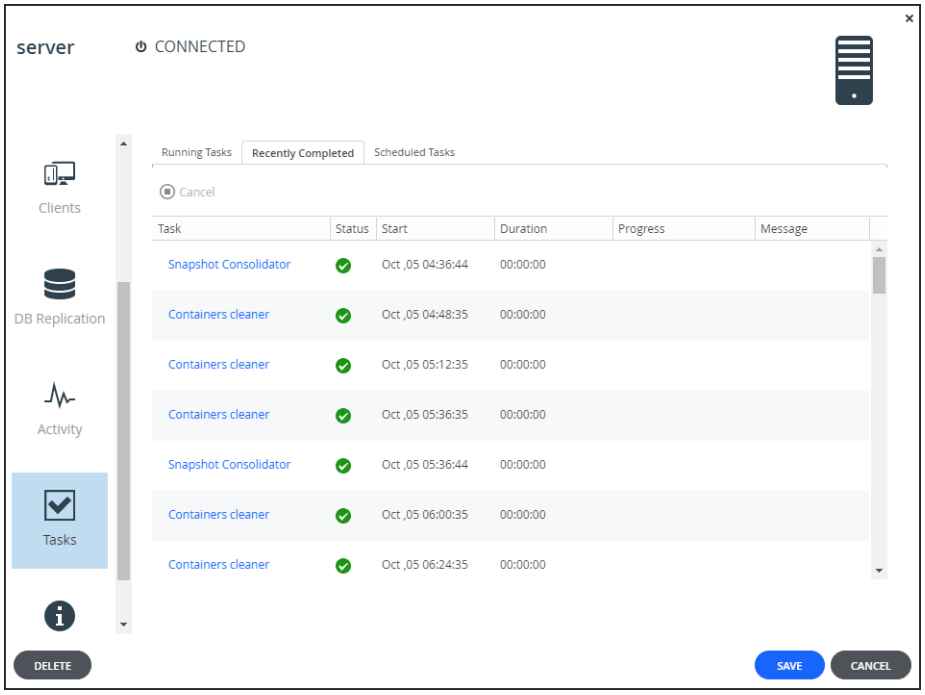
To view server activity:

- In the **Activity** option, you can view the following:
  Load Average – The server's average load over time. A server's *load* is the number of currently running processes that are using, or waiting to use, the CPU.

Java RAM Usage (MB) – The server's Java RAM usage in MB over time.
Storage Traffic In (KB/Second) – The incoming storage traffic in KB/second over time.
Storage Traffic Out (KB/Second) – The outgoing storage traffic in KB/second over time.
Storage Operation In (IO/Second) – The number of read operations performed by the IBM COS FA Portal on cloud storage nodes.
Storage Operation Out (IO/Second) – The number of store operations performed by the IBM COS FA Portal on cloud storage nodes.
CTTP Traffic In (KB/Second) – The incoming CTTP traffic in KB/second over time.
CTTP Traffic Out (KB/Second) – The outgoing CTTP traffic in KB/second over time.
Blocks Cleaned (Blocks/Second) – The number of blocks cleaned per second, as part of system maintenance.
Blocks Reclaimed (Blocks/Second) – The number of blocks deleted per second, as part of system maintenance.
AV Throughput (KB/Second) – The amount of throughput by Cloud Drive antivirus, in KB/second.
AV Files Scanned - On Demand (File/Second) – The number of files scanned by Cloud Drive antivirus.
AV Files Scanned - Background (File/Second) – The number of files scanned by the background scan.
Block Verifications (Per Minute) – The number of block verifications per minute. Block verifications are executed when the portal is executing a consistency check as part of system maintenance.
Commit Threads – The number of threads running and waiting.
Storage Migration Traffic (KB/Second) – The amount of storage node migration traffic, in Kb/second.
Blocks Migrated (Blocks/Second) – The number of blocks migrated in storage node migration, in Kb/second.
Mapfile Blocks Cleaned (Blocks/Second) – The number of mapfile blocks cleaned per second, as part of system maintenance.
Outbound Database Connections – The number of outbound database connections over time.
Inbound Database Connections – The number of inbound database connections over time.
Database Transactions (Per Minute) – Database transactions per minute.
Logged In Users – The number of IBM COS FA Portal administrators logged in over time.
Connected Devices – The number of connected client devices over time.

Tasks

You can view the server's currently running, completed, and scheduled tasks. These tasks run in background.



To view a server's tasks:

- In the **Tasks** option, view the following:
  Running Tasks tab **–** The currently running tasks.
  Recently Completed tab **–** The completed tasks.
  Scheduled Tasks tab **–** The scheduled tasks that have not started. The following information is displayed for scheduled tasks:
    Task – The type of task, described in the below table.
    Start – The date and time at which the task is scheduled to start.

Task	Description	Server	Default Frequency
Administrator report generator	Generates administrator reports.	Application	Daily
Agent licensing refresh	Refreshes agent licensing.	Application	Ongoing
Alert sender	Generate and send emails, such as log alerts.	Application	Every 60 seconds.
Antivirus background scanning - server			
Antivirus re-scanning server			
Apply Templates	Downloads templates to the connected devices.	Application	Every 600 seconds.

Task	Description	Server	Default Frequency
Attachments Cleaner	Deletes expired folders of email attachments.	Application	Daily
Certificate and licenses update			
Containers cleaner			
Disconnect devices of disabled accounts	Disconnects devices of disabled users.	Application	Daily
Expired invitations cleaner			
Frequent Contacts Cleaner	Cleans recently used contacts.	Application	Daily
FSCK	Runs file system check on the blocks in the system.	Main DB	On demand
Generate user notifications			
Inactive account cleaner	Does the following: • Deletes old *changing mail* pending requests from the database. • Deletes *recover password* pending requests from the database. • Deletes old inactive users and devices from the database. • Deletes old *invite to register* pending requests from the database. • Deletes old transient devices. • Permanently deletes already deleted devices.	Application	Daily
Logs Cleaner	Deletes old logs.	Application	Daily
Match auto-assignment rule	Matches templates for devices.	Application	Daily
Notification suppress cleaner	Re-enables sending emails for notifications that were already sent.	Application	Daily
Orphan Scanner	Find blocks that exist in the portal but not in the storage node.	Main DB	On demand
Portal Notifications Background Mail Sender	Enters new notifications to a queue.	Application	Every hour.

Task	Description	Server	Default Frequency
Report generator	Generates users reports.	Application	Once a day and on demand. Sends the report only when needed. For each end-user once a month.
Shared as team sync Synchronizer	Fixes domains of shared resources when a sharding problem occurs writing to a database.	Main DB	Daily
Snapshot cleaner	Deletes old temporary snapshots.	Main DB	Every 30 minutes.
Snapshot closer	Closes uncompleted snapshots and inactive snapshots open more than 2 days.	Main DB	Every 300 seconds.
Snapshot consolidator	consolidate snapshots to reduce the saved snapshots.	Main DB	Every hour.
Start Replication			
Storage Node cleaner	Cleans deleted blocks from storage nodes.	Main DB	Every 60 seconds.
Storage Usage Calculator	Recalculates storage usage for each user and portal.	Application	Daily
Storage Usage Cleaner	Deletes records from the storage usage table for old users and portals (not the actual data).	Application	Daily
Unused block cleaner	Deletes unused blocks.	Main DB	Every 60 seconds.
Update accounts	Updates users and groups from active directory, including deleting and adding users. Updates also user plans if needed.	Application	Daily

Status – The task's status:

 – Completed successfully.

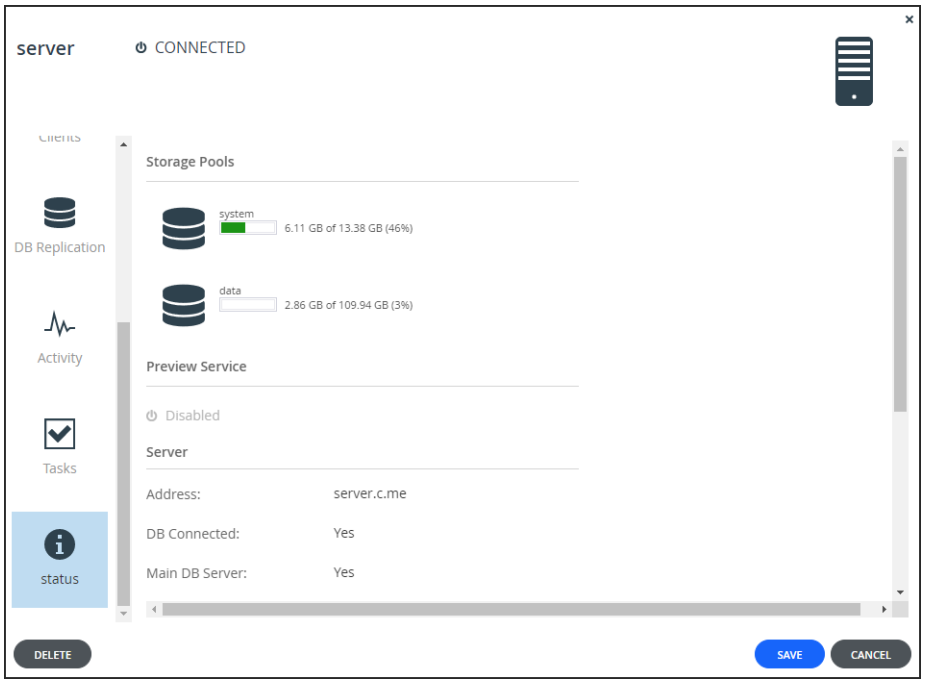
 – In progress.

 – Failed.

Start – The date and time at which the task started.
Duration – The amount of time the task took, or has taken so far.
Progress – The task's progress.
Message – Additional information about the task.

Status

You can view the current status of servers.



To view server statuses:

- In the **Status** option, you can view the following:
  Load Average – The server's average load over time. A server's *load* is the number of currently running processes that are using, or waiting to use, the CPU.
  The following information is available.
  Storage Pools – The status and amount of free storage on each server storage pool.
  Server – Details about the server:
  Address – The server's domain name.
  DB Connected – Whether the DB is connected to the IBM COS FA Portal application.
  Main DB Server – Whether the server is the main DB server.
  Operating System – The server's operating system.
  RAM – The server's RAM and the amount of free RAM.
  Number of CPUs – The number of CPUs.
  Portal Version – The IBM COS FA Portal version.
  Platform – The platform on which the IBM COS FA Portal is installed.
  Image Version – The version number of the server image.
  Uptime – The time that the server has been up.
  Tomcat Uptime – The time that the Tomcat application server has been up.

RESTARTING AND SHUTTING DOWN A SERVER

IBM COS FA Portal servers can be restarted and shut down from the global administration view.

To restart a server:

1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed.
2. Select the server to restart and click **Restart**.
   A confirmation window is displayed.
3. Click **RESTART** to confirm.

The server is restarted.

To shut down a server:

1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed.
2. Select the server to restart and click **Shutdown**.
   A confirmation window is displayed.
3. Click **SHUTDOWN** to confirm.

The server is shut down.

DELETING A SERVER

IBM COS FA Portal servers can be deleted from the global administration view.

To delete a server:

1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed.
2. Either,
   a. Select the server to delete and click **Delete**.
      A confirmation window is displayed.
   b. Click **DELETE** to confirm.

   Or,
   a. Click the server name.
      The server window is displayed with the server name as the window title.
   b. Click **DELETE**.
      A confirmation window is displayed.
   c. Click **YES** to confirm.

The server is deleted.

INSTALLING A NEW VERSION

A new version of a IBM COS FA Portal server can be installed from the global administration view.

You should only install new software with the help of IBM Support.

CHAPTER 20. MANAGING FIRMWARE IMAGES

Each IBM COS FA Gateway in the IBM COS FA Portal system is installed with an image that suits the device platform.

This chapter explains how to manage firmware images.

In this chapter

VIEWING FIRMWARE IMAGES

To view all firmware images in the system:

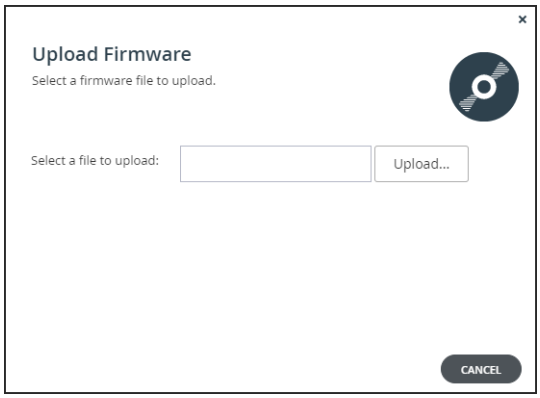
1. In the global administration view, select **Settings** in the navigation pane.
2. Select **Firmware Repository**, under **SETTINGS** in the **Control Panel** page.
   The **Firmware Repository** window is displayed. The window shows the firmware available in the portal firmware repository.

   The current firmware in the repository is marked with  .

UPLOADING FIRMWARE IMAGES

To upload a firmware image:

1. In the global administration view, select **Settings** in the navigation pane.
2. Select **Firmware Repository**, under **SETTINGS** in the **Control Panel** page.
   The **Firmware Repository** window is displayed.
3. Click **Upload**.
   The **Upload Firmware Wizard** opens displaying the **Upload Firmware** dialog box.



4. Click **Upload** and browse to the *.tgz file to upload.
5. Click **Open**.

The firmware image is uploaded to the relevant device platform category and a completed window is displayed.

6 Click **FINISH**.

MARKING A FIRMWARE IMAGE AS THE CURRENT FIRMWARE IMAGE

When you mark a firmware image as the current firmware image, all devices of the relevant device platform that are 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 global administration view, select **Settings** in the navigation pane.
2 Select **Firmware Repository**, under **SETTINGS** in the **Control Panel** page.
The **Firmware Repository** window is displayed. The firmware available in the portal firmware repository is displayed.
3 Select the firmware to make current.
4 Click **Mark as Current**.

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

To mark a firmware image as not current:

1 In the global administration view, select **Settings** in the navigation pane.
2 Select **Firmware Repository**, under **SETTINGS** in the **Control Panel** page.
The **Firmware Repository** window is displayed. The firmware available in the portal firmware repository is displayed.
3 Select the desired firmware image's row.
4 Click **Remove Current**.

VIEWING DEVICES THAT USE A SPECIFIC FIRMWARE IMAGE

You can view all devices that are configured to use a specific firmware.

To view devices with a specific firmware configured:

1 In the global administration view, select **Settings** in the navigation pane.
2 Select **Firmware Repository**, under **SETTINGS** in the **Control Panel** page.
The **Firmware Repository** window is displayed. The firmware available in the portal firmware repository is displayed.
3 Click the firmware image you want to search for.
4 Click **Show devices**.

The **Main > Devices** page opens, displaying the devices that are configured to use the specified firmware.

Note: You can achieve the same results by searching for the firmware in the **Main > Device** page.

DELETING FIRMWARE IMAGES

To delete a firmware image:

1 In the global administration view, select **Settings** in the navigation pane.
2 Select **Firmware Repository**, under **SETTINGS** in the **Control Panel** page.

The **Firmware Repository** window is displayed. The firmware available in the portal firmware repository is displayed.

3 Select the firmware image to remove from the repository.

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

5 Click **YES**.

The firmware image is deleted.