Oracle® Cloud

Using File Server in Oracle Integration Generation 2

F25320-21
August 2023

Oracle Cloud Using File Server in Oracle Integration Generation 2,

F25320-21

Primary Author: Oracle Corporation

Contents

Preface

Using File Server in Oracle Integration Generation 2 describes how to configure and manage the File Server in Oracle Integration.

Topics:

Audience

This document is intended for users who are responsible for managing settings, users, and folders for the SFTP-compliant file server.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Resources

For more information, see these Oracle resources:

- Oracle Integration documentation in the Oracle Cloud Library on the Oracle Help Center.

Conventions

The following text conventions are used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

File Server Overview

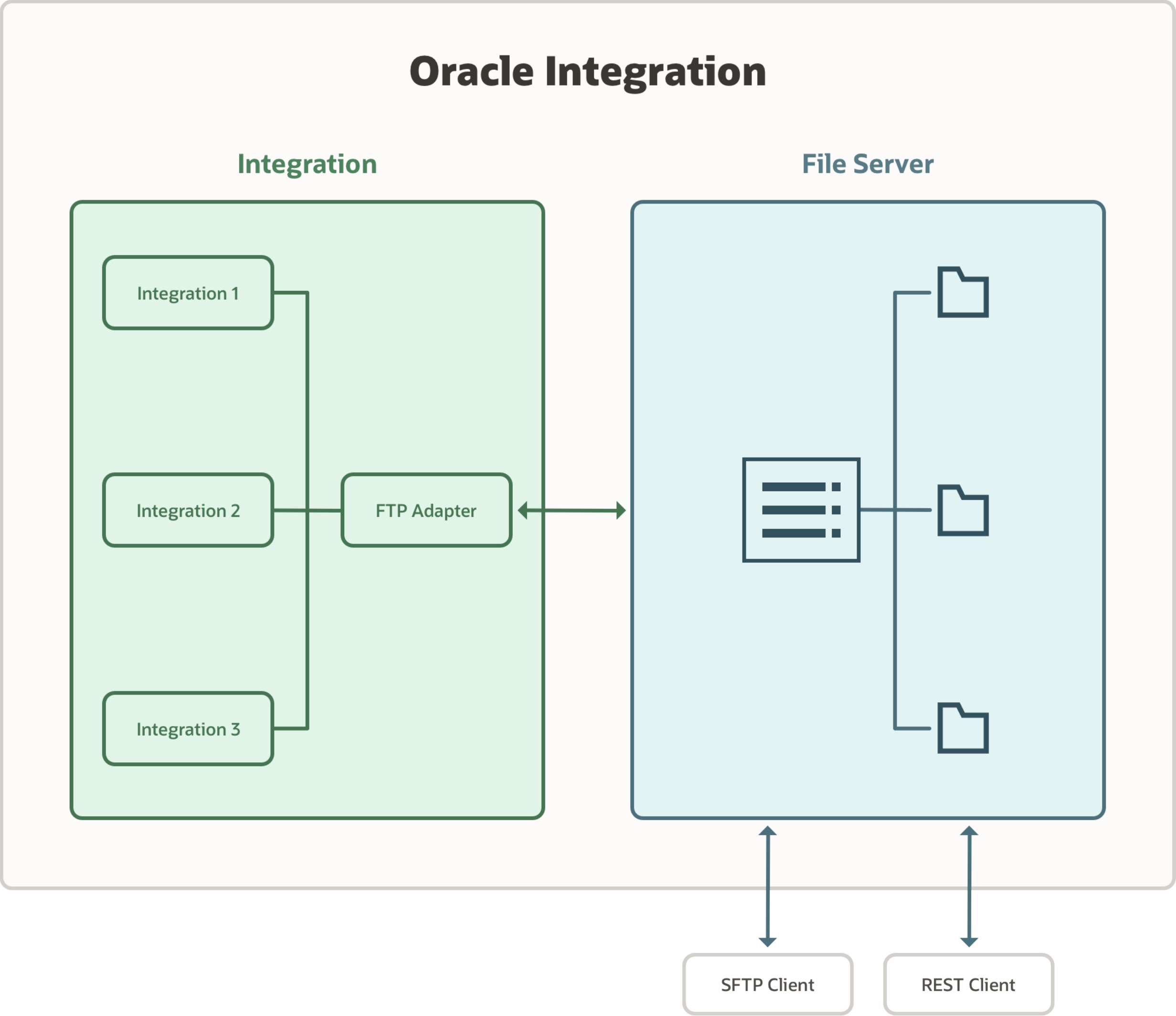
File Server provides an SFTP-compliant repository for storing and retrieving files.

Topics:

About File Server

File Server provides an embedded SFTP server within Oracle Integration, enabling organizations to focus on building integrations without needing to host and maintain a separate SFTP server.

> **Note:**
>
> Before use, File Server must be enabled for the Oracle Integration instance. Enabling File Server is a one time action completed in Oracle Cloud Infrastructure by an administrator with manage access to the instance. See Enable File Server in *Using File Server in Oracle Integration Generation 2*.



File Server Roles

Permissions in File Server are defined by a subset of Oracle Integration roles.

> **Note:**
>
> The following roles do not have any privileges in File Server:
>
> - ServiceMonitor
> - ServiceDeployer
> - ServiceEndUser
> - ServiceInvoker
> - ServiceViewer

The following table lists predefined roles available in Oracle Integration, and the File Server tasks that users with those roles can perform.

Oracle Integration Roles	Personas and Permissions in File Server
ServiceAdministrator	Users with this role can manage server settings and configure users, groups, and folders, including permissions. To administer File Server as described in this guide, you must be assigned the ServiceAdministrator role in Oracle Integration.
ServiceDeveloper	Users with this role can use File Server along with the FTP adapter in Integrations to read and write files.
ServiceUser	Users with this role can access File Server using an SFTP client. These users must be configured and enabled as users in File Server. Their access is controlled by their assigned folders and folder permissions.

File Server REST APIs

APIs are provided for File Server administration, as described in REST API for File Server in Oracle Integration.

Three Reasons to Use File Server

File Server is an SFTP server that is bundled with Oracle Integration. With File Server, you get 500 GB of storage for free, allowing you to store, share, and receive files, including files for SaaS integrations and third-party transfers.

Keep reading to learn more about how File Server can help your organization.

1. Eliminate the cost and operational expenses associated with hosting and maintaining an SFTP server

Managing a do-it-yourself file-based storage system is complex and daunting. From setting up hardware to maintaining the server, implementing a homegrown solution costs both time and money. With File Server, you get free file storage. Moreover, Oracle manages the operational tasks for you, so you can focus on solving more pressing business problems.

2. Create file-based integrations easily

If your organization needs an integration solution that supports file-based integrations, File Server is for you. And because File Server is embedded in Oracle Integration, you can start building file-based integrations quickly.

3. Manage permissions in one place, using in an intuitive interface

Configuring and managing multiple users, groups, and folders in an SFTP environment can be challenging, but this work is simplified with File Server. File Server has a powerful administrative console that contains the core set of features that you expect from an SFTP server, all in an intuitive user interface that streamlines your workflows.

Want to learn more? Get answers to the most commonly asked questions in the File Server FAQ.

Ready to start using File Server? A tenant administrator can enable it in just a few minutes from the Oracle Cloud Infrastructure Console. For step-by-step instructions, see Enable File Server.

File Server FAQ

Find answers to common questions about File Server and its capabilities in Oracle Integration Generation 2.

1: How can I find out if File Server is available to me?

File Server is available for new and existing Oracle Integration Generation 2 instances in all regions.

2: Is File Server enabled by default in Oracle Integration Generation 2?

No, organizations can choose to enable it. The **File Server** link always appears to administrators in the Settings menu. If File Server isn't yet enabled, selecting the link directs to instructions for enabling it in the Oracle Cloud Infrastructure Console. See Enable File Server.

3: How do I access File Server administration in Oracle Integration?

Access File Server administration through the **Settings** menu from the Oracle Integration home page. You must be an Oracle Integration administrator assigned the ServiceAdministrator role.

4: How do I connect to File Server?

Your role determines how you connect to File Server.

- If you're an administrator, both of the following options let you to perform the same tasks:
  - Use the interface in Oracle Cloud Infrastructure Console.
  - Use the File Server REST APIs.
- If you're responsible for transferring files, here are your options:
  - Use an SFTP client of your choice.
  - Use an SFTP command line interface.
- If you need to transfer files as part of an integration–for example, if an event should trigger a file transfer, or if a file transfer should run on a schedule–use the FTP Adapter to connect to File Server. See Create an Integration to Import and Process Bulk Files.

5: Where are File Server users and groups stored and how are they managed?

Users and groups are stored in Oracle Identity Cloud Service (IDCS). Once configured in IDCS, File Server administrators can enable and configure them for File Server access.

6: What types of authentication are supported by File Server?

File Server supports:

- Password
- Open SSH Key based
- Both

7: Can I find log information for File Server?

File Server-only log information isn't provided.

- For all File Server interactions done through an integration, view log information under Integrations monitoring options.
- When accessing File Server from an SFTP client, you can view the logs in the client.

8: How many concurrent connections can I have to File Server?

You can have a maximum of 50 connections per service instance.

When you use the FTP Adapter to connect to File Server, you don't need to worry about connections remaining live throughout the instance flow. That's because connections are closed in the FTP Adapter immediately after the interaction completes, regardless of whether the interaction was done using parallel processing or sequential processing. However, keep in mind that if an integration has a for-loop with parallel processing, and the for-loop contains a trigger or invoke action in which the FTP Adapter connects to File Server, every iteration of the for-loop is counted as an individual connection while the connection is open.

- **Example 1:** 50 simultaneous connections from an SFTP client
- **Example 2:**
  - 20 simultaneous connections from an SFTP client
  - 10 connections from the Integration FTP Adapter (1 for each FTP connection)
  - 20 connections from REST APIs

9: How are files in File Server protected?

We apply fine-grained user access to control access to files in File Server. Files are encrypted on the disk.

10: What is the total amount of storage allowed?

Each File Server service instance provides 500GB of storage.

11: What is the size limit on files uploaded or downloaded?

When accessing File Server from an integration in Oracle Integration, you must use the FTP Adapter. The file limit is 1GB.

When you upload and download files using an SFTP client, files can be of any size, as long as they do not exceed your allocated storage limits.

12: What encryption options are available when reading files from and writing files to File Server?

When accessing files from File Server, you can leverage the encryption/decryption features supported by the FTP Adapter. The FTP Adapter supports Pretty Good Privacy (PGP) encryption, which:

- Enables you to encrypt a file that is being uploaded to remote FTP/SFTP servers using Pretty Good Privacy (PGP) cryptography.
- Enables you to decrypt a file that is being read or downloaded from a remote FTP/SFTP server using Pretty Good Privacy (PGP) cryptography.

Learn more about the FTP Adapter encryption in FTP Adapter Encryption Decryption in *Using the FTP Adapter with Oracle Integration Generation 2*.

13: Is File Server available in the Standard Edition of Oracle Integration?

Yes, File Server is available on both Standard and Enterprise Editions.

14: Is File Server administrator access granted based on one of the predefined roles in Oracle Integration?

Yes, Oracle Integration users must be assigned the ServiceAdministrator role to grant access to File Server.

15: Can the file adapter be used with File Server in Oracle Integration?

No, the FTP Adapter must be used to access File Server.

16: Is File Server available in Oracle Integration for SaaS?

Yes, File Server is available in both Oracle Integration and Oracle Integration for SaaS, Generation 2.

17: Does File Server support IP allowlisting?

Certain public IP addresses can be allowlisted (where identified entities are explicitly allowed access; formerly called whitelisting). See Create an Allowlist for Public IP Addresses.

18: Can the default public IP address and port number of File Server be changed?

No, the default public IP address and port number of File Server, which are displayed in the Settings page, cannot be changed.

19: How is File Server metered?

There is no extra cost associated with File Server. When using the FTP adapter to write files in File Server in Oracle Integration, the standard pricing applicable to the FTP adapter applies. Any file read or write over 50KB is considered a message. For example, 110KB is considered 3 messages (50KB each).

For information on File Server usage, see Monitoring Billable Messages in *Provisioning and Administering Oracle Integration Generation 2*.

20: Can administrators see files listed in File Server folders?

Yes, when you open a folder on the Files page, a list of its files and folders is displayed. You can sort and filter the list.

21: Can users access File Server using their SSO (Single Sign-on) access?

SSO is not currently supported. SFTP users must use their IDCS credentials to access File Server.

22: How do I know if my SFTP client can be used with File Server?

The File Server capabilities are compatible with commonly used SFTP clients. See Supported SFTP Clients.

23: How do I clean up files in File Server?

Need to remove or organize the files in File Server? You have a couple options.

The simpler option is to use any standalone (UI-based or command line) SFTP client. Use the connection settings on the Settings page (from the side pane of the Home page, choose **Settings**, then **File Server**, then **Settings**). To delete files at regular intervals, work in the command line and write a script that invokes SFTP commands to delete folders. When using a UI-based SFTP client, use the options made available by that specific client to delete folders and files.

Alternatively, you can:

- Use the File Server REST API to clean up folders and files.
  You can't use the REST API to delete a single file.
- Create an integration that obtains the list of files on the server and then deletes them. Schedule the integration, if needed.

24: If I use File Server, can I enable Multi-Factor Authentication (MFA) in Oracle Identity Cloud Service ?

No. MFA is not supported for File Server.

25: Can I update the same file using multiple integrations?

Yes, but you might experience issues under some circumstances.

For example, if one or more integrations attempt to update the same file by appending data to it, and the updates occur in parallel, leading to changing the file simultaneously, all data is sometimes removed from the file. The empty file can then cause one or more integrations to fail because the integrations expect the file to contain data.

Supported SFTP Clients

The File Server capabilities are compatible with several commonly used SFTP clients.

File Server is compatible with the following SFTP clients:

- FileZilla
- CyberDuck
- WinSCP version 5.x and earlier
- SFTP commands that are run natively in shell script for *nix/Linux

Oracle also provides the list of encryption algorithms that File Server supports. You can check the documentation for your SFTP client to determine whether the SFTP client is compatible with the encryption algorithms.

To find the list of supported encryption algorithms, from the navigation pane of the Oracle Integration home page, choose **Settings**, then **File Server**, then **Settings**, and look in the Security section.

File Server Use Cases

File Server users use SFTP to work with files stored on File Server based on their folder access and permissions.

Typically, administrators configure the Oracle Integration FTP Adapter to use File Server to manage and retrieve files for use in Oracle Integration. See FTP Adapter Capabilities in *Using the FTP Adapter with Oracle Integration Generation 2*.

Common Use Cases

File Server can be used in a variety of scenarios. Here are some common use cases.

Use Case	Description
Communication with trading partners	Communication with trading partners such as customers and suppliers. In these cases, File Server enables trading partners to send information such as purchase orders, invoices, and shipping information using SFTP.
Integration with SaaS applications	SaaS (or on-premises) applications often export bulk data to files on an SFTP server such as File Server. For example, Oracle E-Business Suite generates a zip file with external transactions, which need to be bulk uploaded to ERP. Oracle Integration can pick up the files, process them, and send them to a target system.
SFTP server lift-and-shift	If your organization is running an on-premise SFTP server with Oracle Integration using the FTP Adapter, you may want to move this SFTP server to the cloud. Move the SFTP files into the Oracle Integration File Server, and redirect the FTP Adapter.

Scenario 1: Write files from an SFTP client to File Server

This scenario configures an individual user access to use an SFTP client to write files to File Server.

This simple end-to-end scenario involves two personas:

- an Oracle Integration administrator who configures a user’s folder and its permissions in File Server
- an end user who uses an SFTP client to connect to File Server and upload files to his or her configured folder.

Oracle Integration administrator steps:

1. Navigate to File Server.
   a. Sign in to Oracle Integration as an administrator.
   b. From the navigation pane of the Oracle Integration home page, choose **Settings**, then **File Server**.
2. Search and find an end user, and configure the user for File Server access.
   a. Choose **Users** from File Server's options.
   b. Search and find a user from those configured for Oracle Identity Cloud Service.
   c. Click **Edit Configuration** for the user.
   d. Enable the user for access, configure a default home folder, and upload a public key for authentication.
3. Set folder permissions for the user's default home folder.

   a. Click ⌄ to view the user's details.
   b. Click **Home Folder Permissions** and grant all permissions.
4. Provide connectivity information to the end user, which is needed in the SFTP client to connect to File Server.
   a. Choose **Settings** in the navigation pane.
   b. View the File Server's IP and Port, and provide by email to the user.

End user steps:

1. Connect to the Oracle Integration File Server from an SFTP client.

   Launch the SFTP client and connect using the connectivity information (IP address and port number) shared by the admininstrator, and your Oracle Integration username and password.
2. View your home folder (configured by the administrator) and upload files to it.

Scenario 2: Configure an integration to read files from a standalone SFTP server and write them to File Server

This scenario uses an integration based on a scheduled file transfer that reads files uploaded to a standalone SFTP server and write them to File Server.

This end-to-end scenario involves these personas:

- an Oracle Integration administrator who configures a user’s folder and its permissions in File Server.
- an Oracle Integration developer who first creates connections for source (standalone SFTP server) and target (File Server) endpoints, and then creates an integration that reads files from the standalone SFTP server and writes them to File Server.

Oracle Integration administrator steps:

1. Navigate to File Server.
   a. Sign in to Oracle Integration as an administrator.
   b. From the navigation pane of the Oracle Integration home page, choose **Settings**, then **File Server**.
2. Find a folder and configure its permissions.
   a. Choose **Folders** from the File Server navigation pane.
   b. Navigate to a folder.
   c. Hover over the folder and click its **Permissions** icon.
3. Set folder permissions.
   - Grant all permissions on the user’s home folder permissions, and save.

Oracle Integration developer steps:

1. In Oracle Integration, navigate to integrations and connections.
   - Sign in to Oracle Integration as a developer.

- Navigate to **Integrations**, then **Connections**.

2. Create a source connection based on the FTP adapter that points to a standalone SFTP server.
3. Create a target connection based on the FTP adapter that points to File Server.
4. Create an integration based on the scheduled file transfer pattern that reads files from the standalone SFTP server and writes them to File Server.
5. Run the integration to move the files from source to target. (Run as an ad hoc request to test it.)
6. In the Integrations Monitoring area, monitor the integration’s run.

   For example, view its run details and its activity stream.

2 Administer File Server

Oracle Integration administrators use the File Server options to configure settings, users, groups, and folder permissions.

To administer File Server, you must be an Oracle Integration administrator assigned the ServiceAdministrator role. See Assigning Service Roles for Oracle Integration in *Provisioning and Administering Oracle Integration Generation 2*.

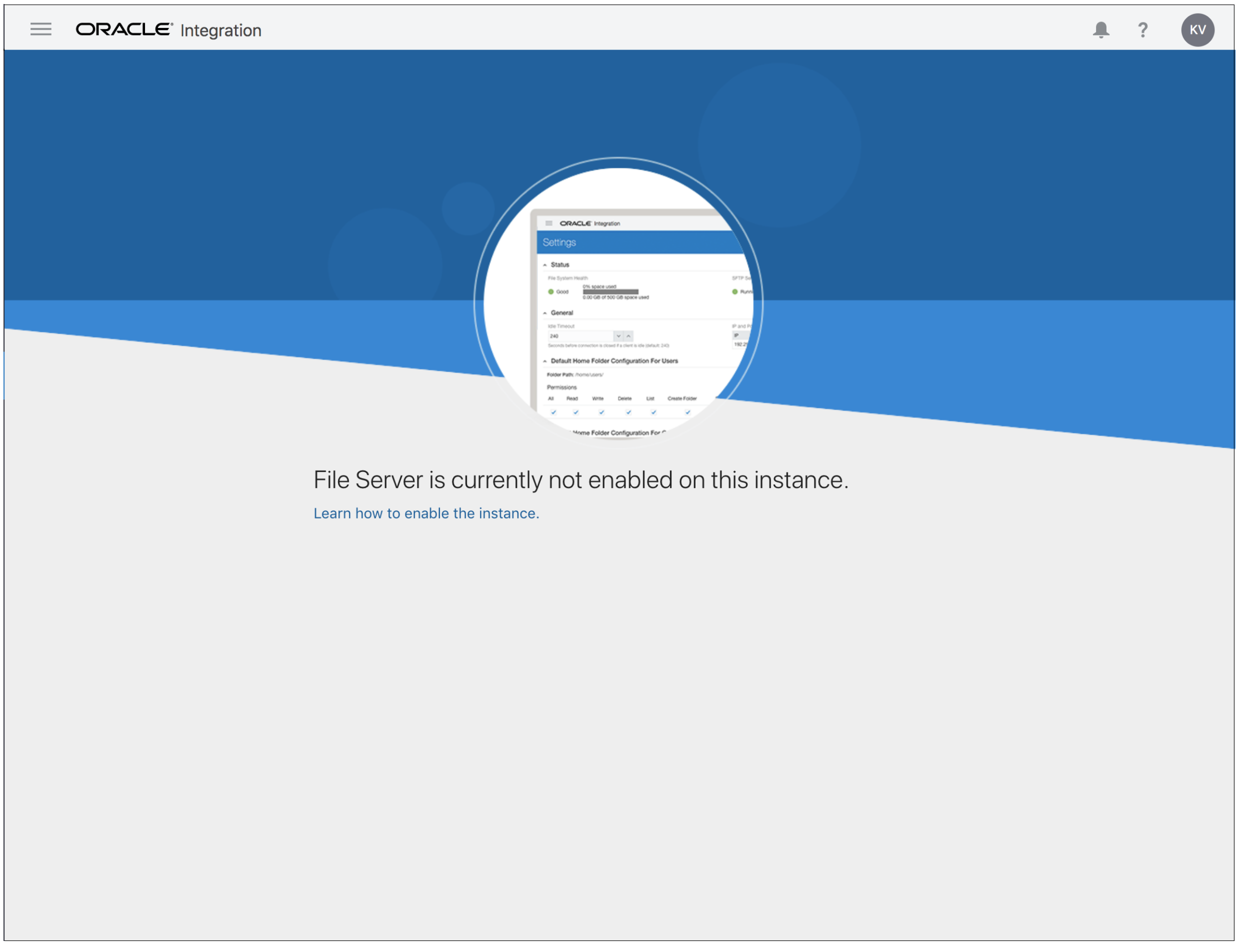
Topics:

- Enable File Server
- Configure File Server Settings
- Configure Groups
- Configure Users
- Configure Folders and View List of Files
- Create an Allowlist for Public IP Addresses

Enable File Server

To begin using File Server in Oracle Integration, it must first be enabled for the Oracle Integration instance in the Oracle Cloud Infrastructure Console. Enabling File Server is a one time action.

If you select File Server from the navigation pane and it's not yet enabled for Oracle Integration, the following message appears:



File Server is currently not enabled on this instance.

Learn how to enable the instance.

Note:

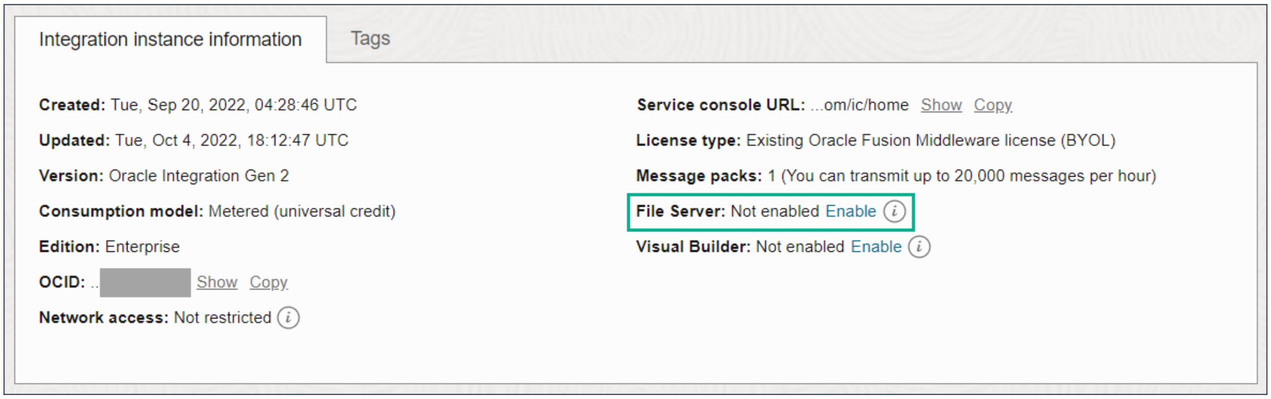
To enable File Server for an Oracle Integration instance, you must have Oracle Cloud Infrastructure manage access to the instance. See Creating an OCI Policy to Manage Instances in *Provisioning and Administering Oracle Integration Generation 2*.

To enable File Server:

1. Select your instance in the Oracle Cloud Infrastructure Console.

   The Integration Instance Details page is displayed.

2. Click the **Enable** link for File Server on the Integration Instance Information tab.



Created: Tue, Sep 20, 2022, 04:28:46 UTC

Updated: Tue, Oct 4, 2022, 18:12:47 UTC

Version: Oracle Integration Gen 2

Consumption model: Metered (universal credit)

Edition: Enterprise

OCID: ..[redacted] Show Copy

Network access: Not restricted ⓘ

Service console URL: ...om/ic/home Show Copy

License type: Existing Oracle Fusion Middleware license (BYOL)

Message packs: 1 (You can transmit up to 20,000 messages per hour)

File Server: Not enabled Enable ⓘ

Visual Builder: Not enabled Enable ⓘ

3. When prompted to confirm enabling File Server, click **Enable**. The OIC icon turns orange and its status changes to Updating. Enablement can take several minutes.

   Once complete, the OIC icon changes back to green with an Active status, and File Server shows as Enabled.

4. Configure File Server settings.

   a. Click **Service Console** from the buttons along the top of the Integration Instance Details page.

      Oracle Integration is displayed.

   b. From the left navigation pane, select **Settings**, then **File Server**, then **Settings**.

After enabling and configuring File Server, your next step is to configure settings so that you can monitor its health.

Configure File Server Settings

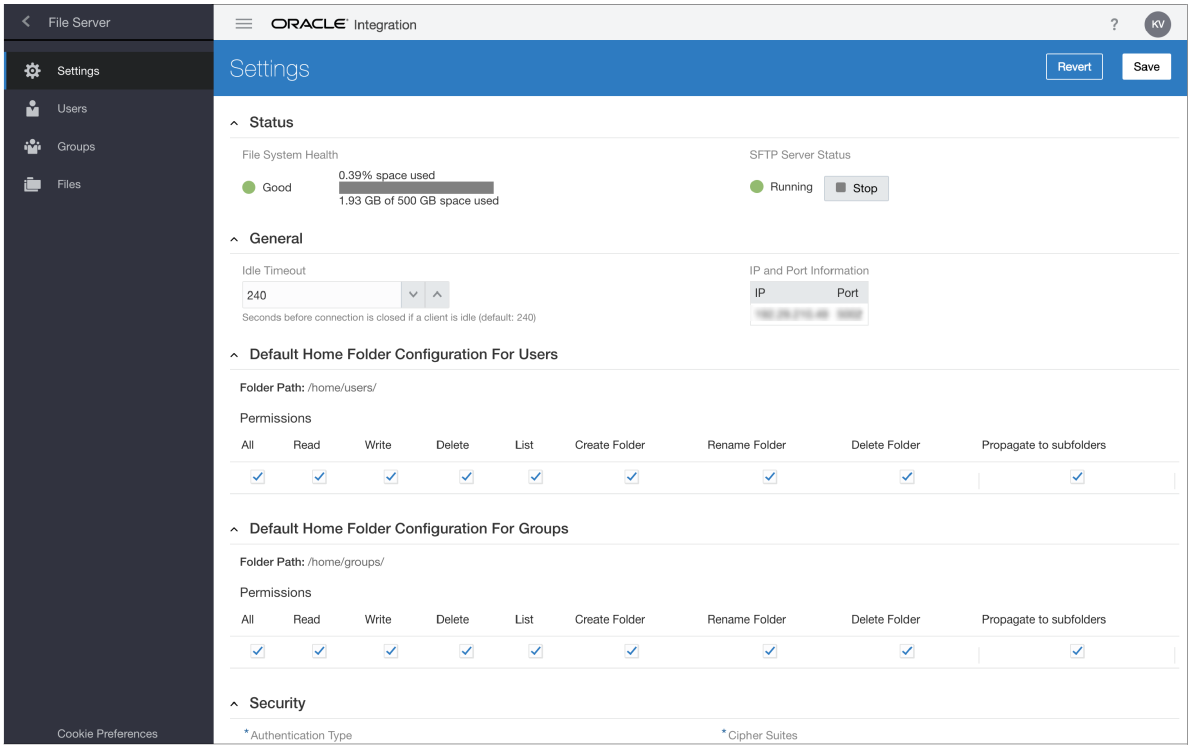
Use the Settings page to monitor the overall health of File Server and to change its main settings.

Before configuring settings, you must Enable File Server.

1. From the side pane of the Oracle Integration Home page, choose **Settings**, then **File Server**, then **Settings**.

   The Settings page is displayed.

2. Under **Status** settings, monitor the server's status, and stop or restart as needed.



Settings

Status

File System Health

● Good — 0.39% space used — 1.93 GB of 500 GB space used

SFTP Server Status

● Running — Stop

General

Idle Timeout

240

Seconds before connection is closed if a client is idle (default: 240)

IP and Port Information

IP	Port
[redacted]	[redacted]

Default Home Folder Configuration For Users

Folder Path: /home/users/

Permissions

All	Read	Write	Delete	List	Create Folder	Rename Folder	Delete Folder	Propagate to subfolders
☑	☑	☑	☑	☑	☑	☑	☑	☑

Default Home Folder Configuration For Groups

Folder Path: /home/groups/

Permissions

All	Read	Write	Delete	List	Create Folder	Rename Folder	Delete Folder	Propagate to subfolders
☑	☑	☑	☑	☑	☑	☑	☑	☑

Security

*Authentication Type

*Cipher Suites

Field	Description
File System Health	View the total space and percent in use. Each File Server service instance provides 500GB of storage. • If the available space falls below 10%, a warning is displayed. • If no space is available, a red indicator is displayed and uploading stops, although operations that do not use additional space still function.
SFTP Server Status	View the SFTP server's state: Running or Stopped. • Click **Stop** to stop the server at any time. File Server stops after all current file transfers are complete. • Once stopped, the button's name changes to **Start**. Click **Start** to restart the server.

3. Under **General** settings, specify a timeout and note the IP and Port settings.

Field	Descripton
Idle Timeout (sec)	Set the number of seconds that an SFTP client can be idle before being disconnected by File Server. The default timeout value is 240 seconds (4 minutes) and the maximum value is 300 seconds (5 minutes).
IP and Port Information	Note the read only, public IP and port values of the SFTP server for this Oracle Integration instance, which were assigned during provisioning. Use these values in configuring the Oracle Integration FTP adapter and SFTP clients.

4. Under **Users Default Configuration for Home Folder**, view the user home folder's base path and specify the folder's default permissions.

Field	Description
Folder Path	Displays the default home folder path for users. (Configure individual users on the Users page, as described in Configure Users.) You can't change the system's default home. - For users, the default home path is `home/users/`. If you leave a user configured to use the default home (choose **User Default** as **Home Folder Type** on the Users page), the full path to the user's home is `/home/users/[username]`. - If a user's home folder is set to **Group Inherited** on the Users page and the user is a member of a group, then the user will inherit the group's home folder.
Permissions	Set default permissions for the user home folder. (Configure permissions for specific folders on the Folders page, as described in Configure Folders and View List of Files.) If you don’t assign specific permissions, these settings are used. - **All:** Assign all permissions to the user home folder. - **Read:** Allow files to be downloaded. - **Write:** Allow files to be uploaded. - **Delete:** Allow files to be deleted. - **List:** Allow folder contents to be listed. - **Create Folders:** Allow subfolders to be created. - **Rename Folders:** Allow subfolders to be renamed. - **Delete Folders:** Allow subfolders to be deleted. - **Propagate to subfolders:** Apply the selected permissions to all subfolders. You can block this setting using the **Do not inherit** setting when configuring subfolder permissions from the Folders page.

5. Under **Groups Default Configuration for Home Folder**, view the home folder's base path and specify the folder's default permissions.

Field	Description
Folder Path	Displays the base path for group home folders. (Configure individual groups on the Users page, as described in Configure Users.) You can't change the system's default home. For groups, the default home path is `home/groups/`. If you leave a group configured to use the default home (choose **Group Default** as **Home Folder Type** on the Users page), the full path to the group's home is `/home/users/[groupname]`.

Field	Description
Permissions	Set default permissions for the group home folder. (Configure permissions for specific folders on the Folders page, as described in Configure Folders and View List of Files.) If you don’t assign specific permissions, these settings are used. • **Propagate to subfolders:** Apply the selected permissions to all subfolders. You can block this setting using the **Do not inherit** setting when configuring subfolder permissions from the Folders page. • **All:** Assign all permissions to the user or group home folder. • **Read:** Allow files to be downloaded. • **Write:** Allow files to be uploaded. • **Delete:** Allow files to be deleted. • **List:** Allow folder contents to be listed. • **Create Folders:** Allow subfolders to be created. • **Rename Folders:** Allow subfolders to be renamed. • **Delete Folders:** Allow subfolders to be deleted.

6. Under **Security**, select an authentication type and change security settings as needed.

Field	Description
Authentication Type	Specify whether authentication is by password, SSH key based, or either. To configure SSH key based authentication: a. Generate an SSH key pair. See Generate SSH Keys in PEM Format to Connect to a Public or On-Premises sFTP Server in *Using the FTP Adapter with Oracle Integration Generation 2*. **Note:** Key based authentication supports Open SSH format only. b. On the Users page in File Server, select the user and upload the OpenSSH format key. c. On the Users page, enable the user. d. Use the private key to connect via the sftp client.

Field	Description
Security Settings	Specify values from the standard SSH/SFTP settings listed below, which are made up of a list of allowed values. To remove a value, click its **x**. If you remove a value, File Server no longer supports the value (until you add it back). Add new values by clicking a field and selecting from the list that appears. • Signature Algorithms • Key Exchange Algorithms • Cipher Suites • Message Authentication Algorithms • Compression Methods See IETF RFC 4253 - SSH Transport Layer Protocol for detailed descriptions. **Note:** The FTP client that connects to File Server must support the same configuration that is defined in this section. For example, if your FTP client doesn't support one of the Key Exchange Algorithms that File Server supports, the FTP client won't be able to connect to File Server.

7. If needed, revert changes made to these server settings since their last save by clicking **Revert**.
8. Click **Save**.

After configuring settings, you must configure users, including uploading a public key and specifying folder types.

Configure Users

Use the Users page to enable File Server access for selected users, upload a public key for a user, and specify a user's folder type.

Before configuring users, you should Configure File Server Settings.

1. In Oracle Identity Cloud Service, create users whom you want to access File Server.

   You create and manage users in Oracle Identity Cloud Service. See Manage Oracle Identity Cloud Service Users in *Administering Oracle Identity Cloud Service*.

   Once added, you can enable their access to File Server.

2. In File Server, search for a user on the Users page.

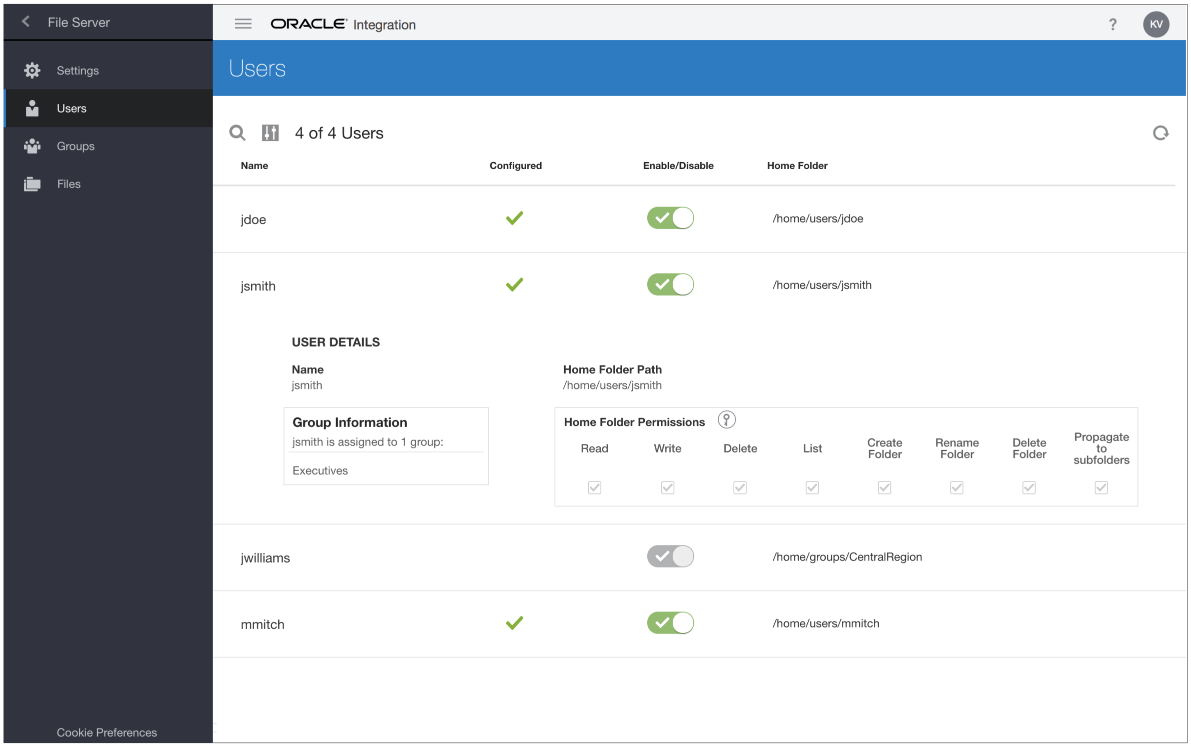
   a. From the side pane of the Oracle Integration Home page, choose **Settings**, then **File Server**, then **Users**.

      The Users page is displayed, with user identities from Oracle Identity Cloud Service shown.

      The table shows each user's status (configured or not configured), whether they are enabled or disabled, and their home folder. When you hover over a row, icons appear for adding/editing its configuration, deleting its configuration, or viewing user details.

   b. Click 🔍, enter a full or partial name to find, and press Enter.

c. If needed, click to narrow the results list by status (All, Configured, or Enabled/Disabled).



Users

4 of 4 Users

Name	Configured	Enable/Disable	Home Folder
jdoe	✓	✓	/home/users/jdoe
jsmith	✓	✓	/home/users/jsmith
jwilliams		✓	/home/groups/CentralRegion
mmitch	✓	✓	/home/users/mmitch

USER DETAILS

Name
jsmith

Home Folder Path
/home/users/jsmith

Group Information
jsmith is assigned to 1 group:
Executives

Home Folder Permissions

Read	Write	Delete	List	Create Folder	Rename Folder	Delete Folder	Propagate to subfolders
☑	☑	☑	☑	☑	☑	☑	☑

3. Configure a selected user for File Server access.

   Hover over a row and click **Configure** . A user side pane is displayed.

Field	Description
Authentication Public Key	If you chose key based authentication as the authentication type on the Settings page, configure the user's public ssh key. Use these key fields to upload, view, or delete the selected user's public key. • Click **Upload**, then **Browse**, and locate a public key file. The public key must be a valid OpenSSH format key. • If needed, delete a public key or upload a new one.
Home Folder Type	Specify how the home folder is defined for users. • **User Default**: Assigns the selected user a home folder in the default location shown on the Settings page. • **Group Inherited**: Skips assigning the selected user an individual home folder. Instead, the user inherits the home folder of any groups configured for SFTP access of which the user is a member. • **Custom**: Assigns the selected user the home folder you choose. Choose the user's home folder in the fields that display.

4. View user details.

   Hover over a user and click **Expand** .

You can see the groups the user is assigned to and the user's home folder path and permissions.

- If an unconfigured user is part of an active group, all properties from the groups are displayed in the list and the details section and status are grayed out.
- Click **Go to Home Folder Permissions** to view and change permissions of the user's home folder.

5. Enable or disable a user.

   Specify whether a selected user can currently access File Server. You can use this setting to configure a user but not enable their File Server access until needed, or temporarily disable their File Server access without removing their public key and permissions.

After configuring users, you must configure group access.

Configure Groups

Use the Groups page to enable SFTP access for selected groups, view home folder permissions, and specify the group's folder type.

Before configuring groups, you should configure users.

1. In Oracle Identity Cloud Service, create groups that you want to enable with SFTP access to File Server.

   You create and manage users and groups in Oracle Identity Cloud Service. See Manage Oracle Identity Cloud Service Groups in *Administering Oracle Identity Cloud Service*.

   Once added, you can enable their access to File Server.

2. In File Server, search for a group on the Groups page.

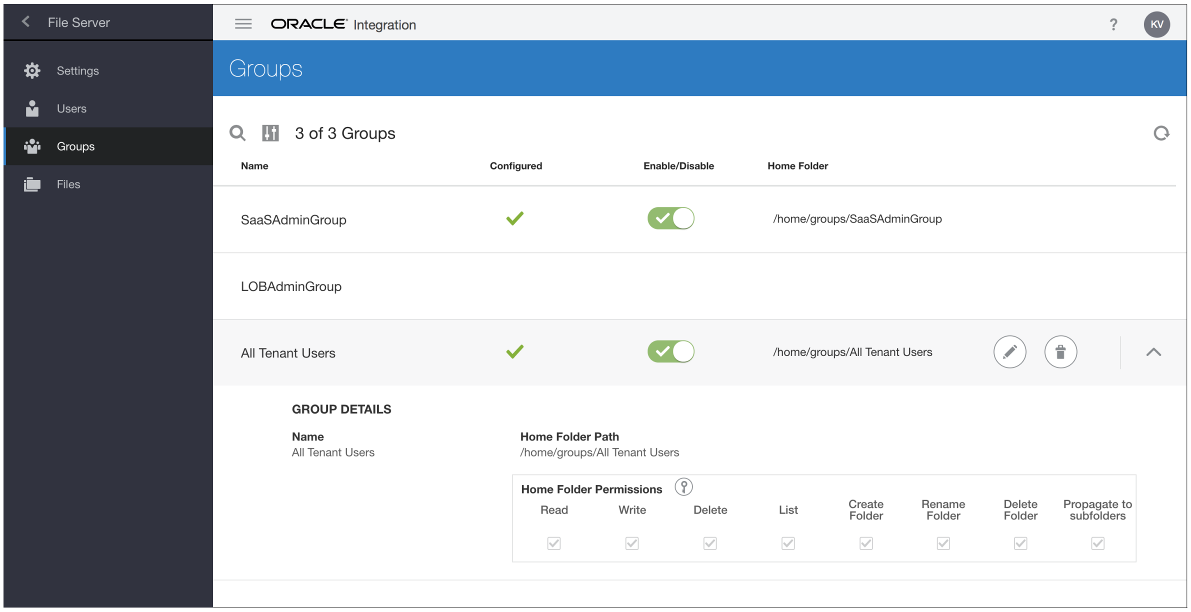
   a. From the side pane of the Oracle Integration Home page, choose **Settings**, then **File Server**, then **Groups**.

      The Groups page is displayed, with group identities from Oracle Identity Cloud Service shown.

      The table shows each group's status (configured or not configured), whether it is enabled or disabled, and its home folder. When you hover over a row, icons appear for editing its configuration, deleting its configuration, or viewing group details.

   b. Click 🔍, enter a full or partial name to find, and press Enter.

   c. If needed, click to narrow the results list by status (All or Configured).



Groups

3 of 3 Groups

Name	Configured	Enable/Disable	Home Folder
SaaSAdminGroup	✓	✓	/home/groups/SaaSAdminGroup
LOBAdminGroup			
All Tenant Users	✓	✓	/home/groups/All Tenant Users

GROUP DETAILS

Name
All Tenant Users

Home Folder Path
/home/groups/All Tenant Users

Home Folder Permissions

Read	Write	Delete	List	Create Folder	Rename Folder	Delete Folder	Propagate to subfolders
☑	☑	☑	☑	☑	☑	☑	☑

3. Configure a selected group for File Server access.

   - Hover over a row and click **Edit Configuration**. A group side pane is displayed.

Field	Description
Home Folder Type	Specify how the home folder is defined for groups. • **Group Default**: Assigns the selected group a home folder in the system default location shown on the Settings page. • **Custom**: Assigns the selected group the home folder you choose. Choose the group's home folder in the fields that display.

4. Hover over a group and click **Open Details** to expand group details.

   You can see the group's home folder path and permissions. To change permissions, click **Go to Home Folder Permissions**.

5. Enable or disable a group.

   Specify whether the selected group can currently access the SFTP server. You can use this setting to configure a group without enabling its File Server access until needed, or temporarily disable its File Server access without removing its permissions.

After configuring groups, you must create and manage folders and their permissions.

Configure Folders and View List of Files

Use the Files page to create and manage folders and set their permissions. A user’s permissions are a combination of individual assigned permissions and those of any groups the user is a member of.

Before you configure folders, you should configure group access.

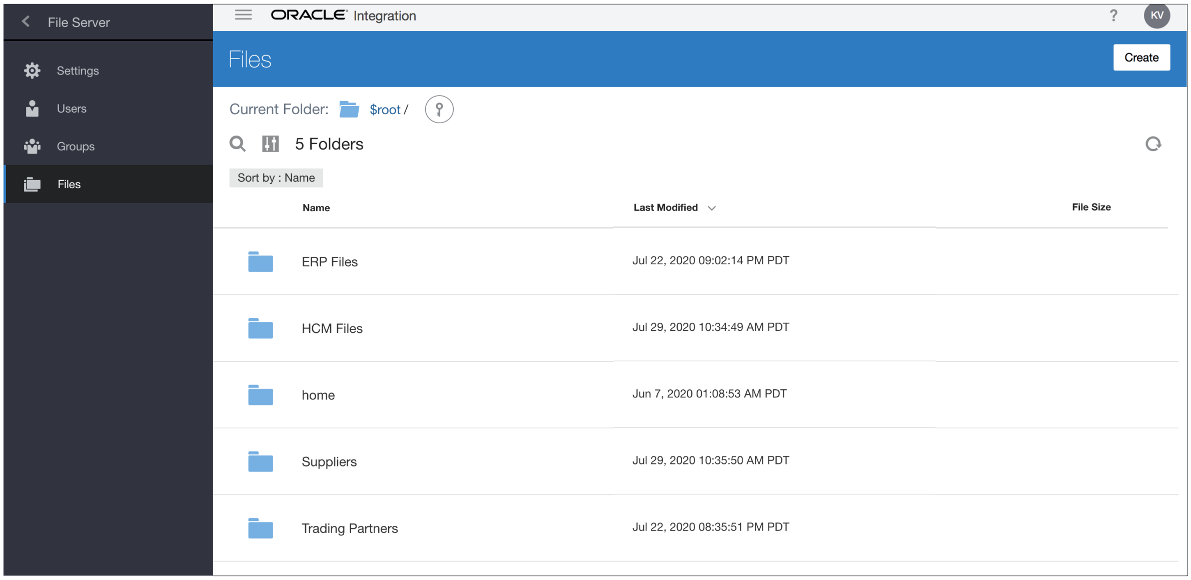
Once folders are configured, users with the appropriate permissions can add files to folders using an external SFTP client. Administrators can view these files in selected folders in File Server.

1. From the side pane of the Oracle Integration Home page, choose **Settings**, then **File Server**, then **Files**.

   The Files page is displayed, with the current folder's path shown. The top folder in the table, [Current Folder], represents the selected folder, and its subfolders are listed below. Navigate to a desired folder by clicking a folder name. Each folder has a context menu on the right side to access specific functionality.

2. If needed, find a folder using the search or filter functions.
   - Sort folder contents by clicking a column heading. Folders are listed above files. By default, folders are sorted by last modified date, starting with most recent.
   - Click **Search**, enter one or more characters in the folder's name, and press Enter. Click x to return to the default display.
   - Click **Filter**, sort by name or last modified date, and click **Apply**. Select **Clear Filters** to return to the default display.

3. Create, rename, or delete folders as needed.
   - Add a folder in the currently selected path by clicking **Create**, entering a name, and clicking **Create**.
   - Rename a folder by clicking the folder's **Actions** menu and choosing **Rename**, then entering a new name.
   - Delete a folder by clicking the folder's **Delete** icon. Deleting a folder deletes all contents, and any subfolders and files contained within it.



Current Folder: $root /

5 Folders

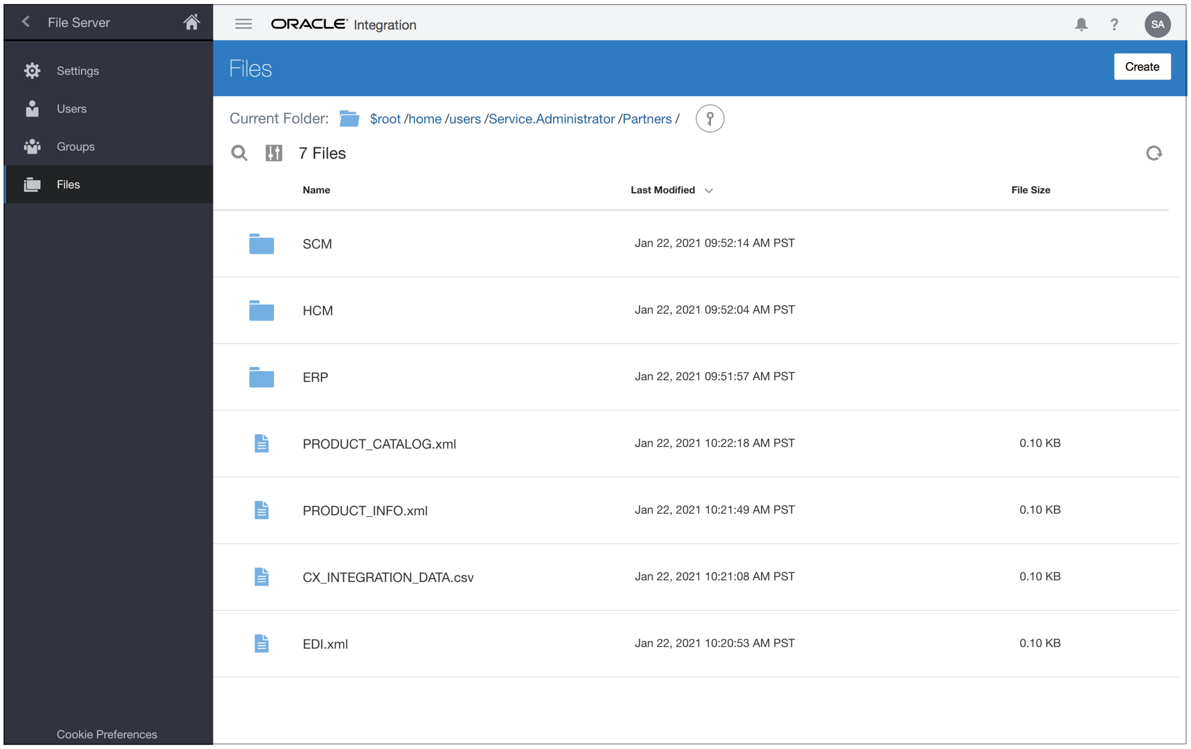
Sort by : Name

Name	Last Modified	File Size
ERP Files	Jul 22, 2020 09:02:14 PM PDT	
HCM Files	Jul 29, 2020 10:34:49 AM PDT	
home	Jun 7, 2020 01:08:53 AM PDT	
Suppliers	Jul 29, 2020 10:35:50 AM PDT	
Trading Partners	Jul 22, 2020 08:35:51 PM PDT	

4. Optionally, open a folder and view its list of folders and files.

   Files are listed with name, last modified date, and size displayed.

   - Sort the list of files by name, last modified date, or file size by clicking a column heading.
   - Search for a file by entering its full or partial name.
   - Filter the list to display folders or files only.



Current Folder: $root /home /users /Service.Administrator /Partners /

7 Files

Name	Last Modified	File Size
SCM	Jan 22, 2021 09:52:14 AM PST	
HCM	Jan 22, 2021 09:52:04 AM PST	
ERP	Jan 22, 2021 09:51:57 AM PST	
PRODUCT_CATALOG.xml	Jan 22, 2021 10:22:18 AM PST	0.10 KB
PRODUCT_INFO.xml	Jan 22, 2021 10:21:49 AM PST	0.10 KB
CX_INTEGRATION_DATA.csv	Jan 22, 2021 10:21:08 AM PST	0.10 KB
EDI.xml	Jan 22, 2021 10:20:53 AM PST	0.10 KB

5. Set folder permissions. Hover over a row and click **Permissions** . The Permissions screen appears.

   See Set Folder Permissions.

6. If needed, revert changes made to the folder's permissions since the last save by clicking **Revert**.

7. Click **Save**.

Set Folder Permissions

Use the Permissions page to set a selected folder's permissions.

1. From the side pane of the Oracle Integration Home page, choose **Settings**, then **File Server**, then **Folders**.

2. Click a folder's **Permissions** icon. The Folders Permissions page is displayed, showing a list of users or groups with permissions configured for the current folder. The left-most icon identifies a user versus a group.

3. Change permissions as needed. Select or deselect permission checkboxes to change permissions to the selected folder for the users and groups. Click **Delete** to remove a selected permission.

4. Optionally select **Do not inherit**.

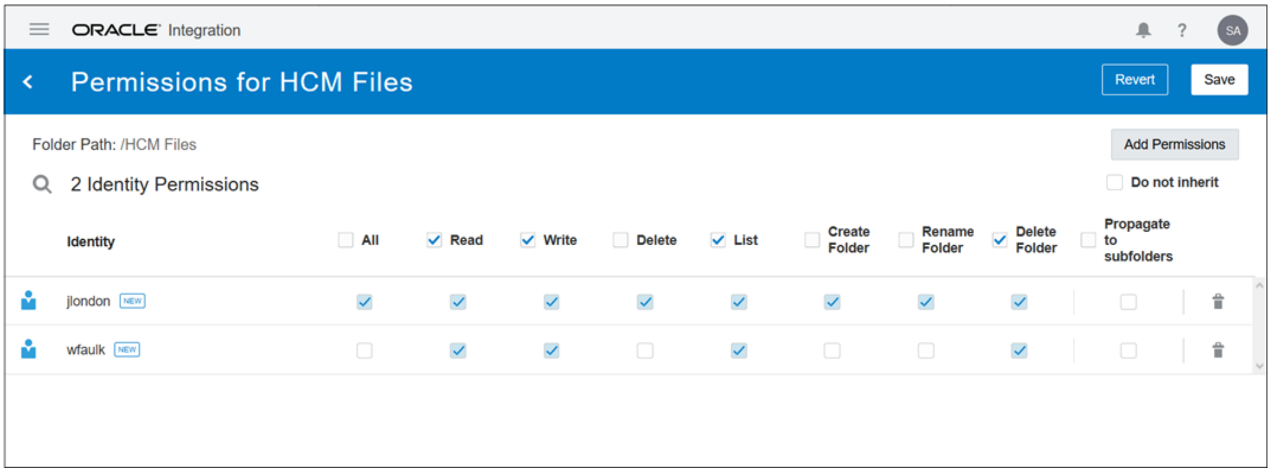
   This setting blocks any permissions set to **Propagate to Subfolders** from applying to the selected folder. This setting allows permissions to be propagated to all subfolders except those marked **Do Not Inherit**.

5. Grant additional users or groups permissions to the folder, as needed.

   a. Click **Add Permissions**.

   b. From the side pane that is displayed, click the **Users** or **Groups** tab, select one or more identities, and click **Add**. The new identities are added to the permissions list.

   c. Select checkboxes to set specific permissions. Select a top checkbox to assign a permission to all listed users and groups.



Permissions for HCM Files

Folder Path: /HCM Files

2 Identity Permissions

☐ Do not inherit

Identity	☐ All	☑ Read	☑ Write	☐ Delete	☑ List	☐ Create Folder	☐ Rename Folder	☑ Delete Folder	☐ Propagate to subfolders	
jlondon NEW	☑	☑	☑	☑	☑	☑	☑	☑	☐	🗑
wfaulk NEW	☐	☑	☑	☐	☑	☐	☐	☑	☐	🗑

Field	Description
Propagate to subfolders	Apply the selected permissions to all subfolders within the folder (and all child subfolders within and so on) unless you block this setting for a selected subfolder using the **Do Not Inherit** setting.
All	Assign all permissions to this user or group.
Read	Allow files to be downloaded.
Write	Allow files to be uploaded.
Delete	Allow files to be deleted.
List	Allow listing of the folder's contents.
Create Folder	Allow subfolders to be created.
Rename Folder	Allow renaming of subfolders.
Delete Folder	Allow deletion of subfolders.
Propagate to subfolders	Apply the selected permissions to all subfolders within the folder (and all child subfolders within and so on) unless you block this setting for a selected subfolder using the **Do Not Inherit** setting.

6. Click < to return to the Folders page.
7. If needed, revert changes made to folders since the last save by clicking **Revert**.
8. Click **Save**.

After setting folder permissions, you must create an allowlist so you can control access to File Server.

Default Folders for Users and Groups

In the File Server folder directory, the `root/home` folder contains default folders for groups and users that an administrator creates in Oracle Identity Cloud Service console and that you enable for File Server. You can delete the files and sub-folders within the folders but not the folders themselves.

The folders are in the following locations:

- When you enable a group's access to File Server, a folder for the group is created in `/home/groups/<group>`
- When you enable a user's access to File Server, a folder for the user is created in `/home/users/<user>`

If an administrator deletes a group in Oracle Identity Cloud Service console, the group no longer appears on the Groups page for File Server. Similarly, deleted users no longer appear on the Users page. However, the folder for the group or user remains in File Server to preserve access for people or groups who rely on the files in the folder.

Create an Allowlist for Public IP Addresses

As an administrator, you can request certain public IP addresses to be allowlisted for File Server.

To allowlist (formerly whitelist) one or more IP addresses, file a service request with Oracle Support.

You'll need to specify the CIDR (IP address range) to be allowlisted. For example:

- Single ip: 10.10.10.10
- CIDR block 10.0.0.0/24

3

Troubleshoot File Server

Having trouble with File Server? Keep reading to learn how to troubleshoot common issues.

My SFTP Client Cannot Connect to File Server

In general, when your SFTP client can't connect to File Server, you should try using a supported SFTP client to access your personal Home folder, which you always have access to. If you can establish a connection using a supported SFTP client, then your SFTP client might not be compatible with File Server. If you can connect to your Home folder, then you might need additional permissions to other folders.

Here are more detailed troubleshooting steps:

1. **Make sure the person completing the operation has access to File Server.**
   The person who is running the integration must have access to File Server. Only an administrator can enable the user and confirm that they've been enabled. See Configure Users.
2. **Make sure the person completing the operation has folder access.**
   The person who is running the integration must have permissions to access the folders that they obtain files from and copy files to. Only an administrator can grant access to folders. See Configure Folders and View List of Files.

   If an administrator isn't available to help right away, you can try accessing your personal Home folder using your SFTP client. As long as you're an enabled user, you always have access to your Home folder. If you can access your Home folder successfully, your permissions might be preventing you from accessing the other folders.
3. **Check whether you've exceeded the maximum number of concurrent connections.**
   The File Server FAQ contains details about the maximum concurrent connections. If you've already used your maximum number of concurrent connections, any additional connection attempts fail.
4. **Check whether your SFTP client is compatible with File Server.**
   Your SFTP client must support the security configuration that File Server uses, including algorithms, cipher suites, and compression methods.

   To check the security configuration for File Server and your SFTP client:

   a. From the side pane of the Oracle Integration Home page, choose **Settings**, then **File Server**, then **Settings**.
      The Settings page is displayed.
   b. Below the Security heading, review the options in the following fields:
      - Key Exchange Algorithms
      - Cipher Suites
      - Message Authentication Algorithms
      - Compression Methods

> **Note:**
>
> File Server provides multiple options for each field, but an administrator can remove one or more supported items. To see additional options, click within a field. If additional options are available, they appear in a drop-down list. Keep in mind that if you remove an option from a field, File Server no longer supports the option (until you add it back).

c. Check the documentation for your SFTP client, and determine whether the SFTP client supports the same configuration that is defined in the Security section. Your SFTP client must support one item from each of the following fields:

   - Key Exchange Algorithms
   - Cipher Suites
   - Message Authentication Algorithms
   - Compression Methods
     If the configurations don't match, the SFTP client is not compatible with File Server. You must use a supported SFTP client instead.

5. **Determine whether a network connectivity issue prevented the access.**
   For example:

   - Does the SFTP client have access to the internet?
   - Does the SFTP client have access to File Server?
     The SFTP client can connect to File Server only if the client is on the allowlist for File Server. See Create an Allowlist for Public IP Addresses.
   - Did your proxy server experience intermittent connection issues or cut the connection?
     For instance, your network might have a rule that doesn't allow a connection to be open more than 20 seconds. If you tried to download a large file, the connection might have closed before the download completed. Check with a network administrator to determine whether network rules might have interfered with the connection.

I Don't See File Server in the Menu

File Server might not be enabled for your organization. Only an administrator can enable File Server, and administrators enable File Server in the Oracle Cloud Infrastructure Console. See Enable File Server.

My Files Won't Upload

The file names might contain characters that aren't allowed. File names must not include the following characters:

- #
- ?
- ..

If any file names contain the characters, rename the files, and try uploading again.

I Can't Delete Folders for Users and Groups

When you enable group or user access to File Server, a folder is created for the group or user in the File Server directory. For example:

- `/home/users/<user>`
- `/home/groups/<group>`

You can delete the files and sub-folders within the folders but not the folders themselves.