Oracle® Cloud
Using File Server in Oracle Integration 3

F45542-17
June 2025

ORACLE®

Contents

Preface

1   Get Started with File Server

2   Administer File Server

3   Troubleshoot File Server

Preface

Using File Server in Oracle Integration 3 describes how to configure and manage the File Server in Oracle Integration.

Topics:

- Audience
- Documentation Accessibility
- Diversity and Inclusion
- Related Resources
- Conventions

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 `https://www.oracle.com/corporate/accessibility/`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `https://support.oracle.com/portal/` or visit `Oracle Accessibility Learning and Support` 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 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

Get Started with File Server

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

Topics:

- About File Server
- Three Reasons to Use File Server
- File Server FAQ
- Supported SFTP Clients
- File Server Use Cases

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.

Prerequisite: Enable File Server

An administrator must enable File Server before your organization can start using it. An administrator enables File Server for a given Oracle Integration instance by working in the Oracle Cloud Infrastructure. See Enable File Server.

How to Connect to File Server from an Integration

When designing an integration that connects to File Server, you have the following options:

- Connect to File Server using the File server action.

  The File server action offers improved performance and easier setup, compared to the FTP Adapter.

- Connect to File Server using the FTP Adapter.

  The FTP Adapter offers some capabilities that aren't available with the File server action. For details, see Interact with Files in File Server in *Using Integrations in Oracle Integration 3*.
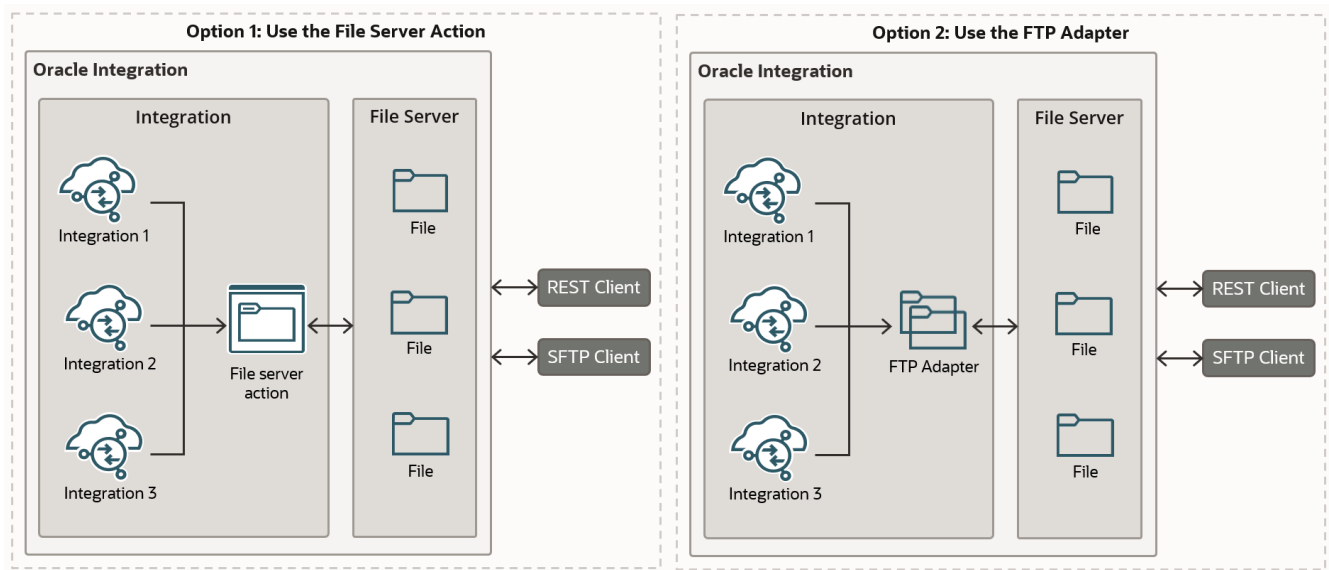
How to Connect to File Server Outside an Integration

You can reach File Server, even when you're not working in Oracle Integration. Use any standalone SFTP client that is supported. See Supported SFTP Clients.

File Server Roles

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

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 or File server action 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.
• ServiceMonitor • ServiceDeployer • ServiceInvoker • ServiceViewer	These roles do not have any privileges in File Server.

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.

Availability and Limits FAQs

Is File Server Available to Me?

File Server is available for new and existing Oracle Integration 3 instances in all regions.

File Server is available with the Standard, Enterprise, and Healthcare Editions of Oracle Integration.

Additionally, File Server is available in both Oracle Integration and Oracle Integration for SaaS.

Is File Server Enabled by Default?

No, but your organization enable it at any time.

If you're an administrator, when you click **Settings** in the navigation pane, the **File Server** menu option is visible. If your organization hasn't enabled File Server yet and you click the menu option, you see directions for enabling it in the Oracle Cloud Infrastructure Console. See Enable File Server.

How Is File Server Metered?

There is no extra cost associated with File Server.

When using the FTP Adapter or File server action to write files in File Server, the standard pricing 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 3*.

How Much Storage Is Allowed, and What Is the Size Limit for Files?

Each File Server service instance provides 500GB of storage. If you reach this limit, any calls to write files to File Server fail.

When accessing File Server from an integration in Oracle Integration, you can use the use the FTP Adapter or the File server action. For both options, the file limit is 1 GB.

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.

How Many Concurrent Connections Can I Have?

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:** 30 simultaneous connections from an SFTP client, and 20 connections from the Integration FTP Adapter (1 for each FTP connection)

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.

Can Multiple Clients Use the Same Connection?

Allowing multiple clients to use the same connection isn't recommended due to performance issues.

File Server allows multiple clients to share a connection. However, connection sharing can result in severe performance issues.

Security and Access FAQs

Can I Create an Allowlist for File Server?

Yes. You must create an allowlist (formerly a whitelist) that identifies the entities that are explicitly allowed access to File Server. Only users from the entities that you specify can connect to File Server. Tenant administrators are responsible for creating the allowlist.

How to manage the allowlist: If you're responsible for managing the allowlist for HTTP connections, you already know how to manage the allowlist for File Server. Follow the same steps to manage both lists. For instructions, see Configure an Allowlist for Your Instance in *Provisioning and Administering Oracle Integration 3*.

How Are Files Protected?

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

What Encryption Options Are Available When Reading and Writing Files?

You have the following options for accessing files from File Server:

- File server action

  Encryption and decryption are currently not supported for the File server action. However, you can use the File server action with the stage file action to achieve these goals. See Interact with Files in File Server in *Using Integrations in Oracle Integration 3*.

- FTP Adapter

  Leverage the encryption and 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.

  – 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 3*.

What File Signing and Verification Options Are Available?

You can perform signing using the private key to allow the receiver to verify that the file contents were not altered during transit. You can also perform signature verification using the public key on the incoming file to verify that the contents were not altered during transit.

You have the following options:

- File server action

  File signing and verification are currently not supported for the File server action. However, you can use the File server action with the stage file action to achieve these goals. See Interact with Files in File Server in *Using Integrations in Oracle Integration 3*.

- FTP Adapter

  Leverage the file signing and verification features supported by the FTP Adapter. Learn more about the FTP Adapter encryption in FTP Adapter Encryption Decryption in *Using the FTP Adapter with Oracle Integration 3*.

How Do I Access File Server Administration?

To access File Server administration in Oracle Integration, you must be an Oracle Integration administrator assigned the ServiceAdministrator role. In the navigation pane, click **Settings**, then **File Server**.

Can Administrators See the Files 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.

Where Are Users and Groups Stored, and How Are They Managed?

Users and groups are stored in Oracle Cloud Infrastructure Identity and Access Management (IAM). After an administrator configures the users and groups, a File Server administrator can configure their access to File Server.

What Roles Do Administrators Need?

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

Where Do I View Audit and Log Information?

Audit and log information is available for several types of interactions:

- **Actions that a person completes in the user interface**

  All actions that you perform in the File Server user interface, such as disabling a user or creating a folder, are logged in the Design Time Audit. See Check the Audit History for an Integration or Other Component in *Using Integrations in Oracle Integration 3*.

- **Actions that an integration performs**

  For all File Server interactions done through an integration, view log information under Integrations observability options.

- **Actions performed from an SFTP client**

  View the logs in the SFTP client.

Other File Server interactions aren't logged.

What Types of Authentication Are Supported?

File Server supports:

- Password
- Open SSH Key based
- Both

How Do Integrations and People Connect to File Server?

Integrations connect to File Server using either of the following options:

- File server action

  See Interact with Files in File Server in *Using Integrations in Oracle Integration 3*.

- FTP Adapter

  See Create an Integration to Import and Process Bulk Files.

People connect to File Server in different ways, depending upon their roles:

- Administrators can use the interface in Oracle Cloud Infrastructure Console or the File Server REST APIs.

- Anyone who wants to transfer files manually can use a supported SFTP client or an SFTP command line interface.

  See Supported SFTP Clients.

Which SFTP Clients Are Supported?

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

ee Supported SFTP Clients.

Can I Connect to File Server Using the File Adapter?

No. To connect to File Server, use the File server action or the FTP Adapter.

If I Use File Server, Can I Enable Multi-Factor Authentication (MFA) in Oracle Cloud Infrastructure Identity and Access Management (IAM)?

No. MFA is not supported for File Server.

Can Users Access File Server Using Their SSO (Single Sign-on) Access?

SSO is not currently supported. SFTP users must use their Oracle Cloud Infrastructure Identity and Access Management (IAM) credentials to access File Server.

Can I Change the Default Public IP Address and Port Number?

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

Usage FAQs

How Do I Clean Up Files?

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 (In the navigation pane, click **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.

Which Activities in File Server Raise System Events?

Several activities in File Server raise system events. You can design an event integration that subscribes to a system event, and then the integration then runs whenever the activity occurs in File Server.

For example, subscribe to the **File created** system event to run an integration when a file is added to File Server.

The following activities in File Server raise a system event.

System event name	Activity that raises the event
File created	Creating a file
	Note: A system event currently isn't raised when you create a file using the File server action. All other methods of creating a file do raise an event.
File deleted	Deleting a file
	Note: A system event currently isn't raised when you delete a file using the File server action. All other methods of deleting a file do raise an event.
File downloaded	Downloading a file
	Note: A system event currently isn't raised when you download a file using the File server action. All other methods of downloading a file do raise an event.
Folder created	Creating a folder
Folder deleted	Deleting a folder

For a sample use case, see Subscribe to a File Server System Event.

Options for Connecting to File Server

How to Connect to File Server from an Integration

You have several options for connecting to File Server from within an integration.

- Use the File server action in an integration

  See Interact with Files in File Server in *Using Integrations in Oracle Integration 3*.

- Use a connection to the FTP Adapter in an integration

An administrator can 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 3*.

Supported SFTP Clients

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

- FileZilla
- CyberDuck
- WinSCP
- SFTP commands that are run natively in shell script for *nix/Linux

Supported Encryption Algorithms

Oracle provides the list of encryption algorithms that File Server supports.

To find the list of supported encryption algorithms:

- In the navigation pane, click **Settings**, then **File Server**, then **Settings**.

  Look in the Security section.

Determine Whether an SFTP Client is Compatible with the Encryption Algorithms

Check the documentation for your SFTP client to determine whether the SFTP client is compatible with the encryption algorithms.

File Server Use Cases

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

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.

Use Case	Description
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.

Write Files from an SFTP Client to File Server

This use case 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. In the navigation pane, click **Settings**, then **File Server**, then **Users**.

2. Configure an end user for File Server access.

   a. Search for and find a user.
   Only users who have been configured Oracle Cloud Infrastructure Identity and Access Management (IAM) appear in the list.

   b. Hover over the user, and click **Configure** ✎ .

   c. In the Property panel, enable the user for access, upload a public key for authentication, and configure a default home folder.

   d. After you finish making changes, click **Save**.

3. Set folder permissions for the user's default home folder.

   a. Hover over the user, and click **Open Details** ⌄

   b. Next to Home Folder Permissions, click **Go to Home Folder Permissions** ⚲ .

   c. On the Permissions page, grant all permissions to the user.

   d. Click **Save**.

   e. Click **Go Back** ‹ to return to the Users page.

4. Provide connectivity information to the end user.
   The end user needs to enter this information into their SFTP client so they can connect to File Server.

   a. In the navigation pane, click **Settings**.

   b. In the General section, copy the IP address and port number, and share this information with the user.

ORACLE

End user steps:

1. Connect to File Server from an SFTP client.

   a. Launch the SFTP client.

   b. Connect to File Server using the IP address and port number shared by the admininstrator, and your Oracle Integration username and password.

2. View your home folder, which the administrator configured, and upload files to it.

Read Files from a Standalone SFTP Server and Write Them to File Server

This use case 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. In the navigation pane, click **Settings**, then **File Server**, then **Folders**.

2. Find a folder and configure its permissions.

   a. Hover over the folder, and click **Permissions** .

   b. 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.

   - In the navigation pane, click **Design**, then **Connections**.

2. Create a source connection based on the FTP Adapter that points to a standalone SFTP server.

3. Complete one of the following tasks:

   - Add a File server action to the integration.

   - 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 Observability area, monitor the integration's run.
   For example, view its run details and its activity stream.

Subscribe to a File Server System Event

This use case involves the **File created** system event. An integration subscribes to the event and runs when a file is uploaded to a specific folder. Next, the integration reads the file and moves it to a different folder.

This use case focuses on the integration developer's work at a high level. It assumes that an administrator has already configured File Server for the Oracle Integration service instance.

To understand the activities that raise system events, see Available System Events in *Using Integrations in Oracle Integration 3*.

Step	More information
Create an event integration that subscribes to a File Server system event	Subscribe to Events in an Integration in *Using Integrations in Oracle Integration 3*.
Filter the events so that the integration subscribes to events for a specific file name	Define Custom Header Filters to Trigger Integrations in *Using Integrations in Oracle Integration 3*.
Move the file to a different folder: Add a File server action to the integration, and select the Move File operation for the action	Interact with Files in File Server in *Using Integrations in Oracle Integration 3*.
For the Map action that comes before the File server action, identify the name of the file that is uploaded, as well as the path to the folder that the file is uploaded to	About the Expression Builder in *Using the Oracle Mapper with Oracle Integration 3*.

File Server Patterns for Allowlisting

By default, File Server provides a high level of security by authenticating all access using either user logins or a public key. You can supplement this security by configuring an allowlist for File Server.

When you use the File Server allowlist, the following patterns are available for access requests that go to File Server.

Pattern	Description
1. Requests from outside Oracle Cloud	This pattern is the only option for access requests that originate outside Oracle Cloud.
2. Oracle Cloud requests through the Service Gateway	By default, access requests that originate within the Oracle Cloud go through the Service Gateway. Your organization must add the CIDR block for the Service Gateway to the File Server allowlist.
3. Oracle Cloud requests through a NAT Gateway	If your organization doesn't want to add the CIDR block for the Service Gateway to the File Server allowlist, you can bring your own load balancer, create a NAT gateway, and add the NAT gateway's IP address to the allowlist instead.

> **✎ Note:**
>
> The File Server allowlist is separate from the Oracle Integration allowlist. See Create an Allowlist for Public IP Addresses.

Pattern 1. Requests from Outside Oracle Cloud

All File Server access requests that come from outside Oracle Cloud must be from IP addresses that are identified on the File Server allowlist.

To configure this pattern, update the self-service File Server allowlist so that it contains the IP address of all clients that much access File Server. See Create an Allowlist for Public IP Addresses.

Pattern 2. Oracle Cloud Requests Through the Service Gateway

By default, all File Server access requests that come from Oracle Cloud are routed through the service gateway. Therefore, the File Server allowlist must grant access to the service gateway's CIDR block.

To configure this pattern, update the self-service File Server allowlist so that it contains the CIDR block for the service gateway: **240.0.0.0/4**. See Create an Allowlist for Public IP Addresses.

Pattern 3. Oracle Cloud Requests Through a NAT Gateway

Some organizations don't want to add the CIDR block for the service gateway to the File Server allowlist. In such cases, you can bring your own load balancer and route access requests for File Server through a NAT gateway.

Then, instead of adding the CIDR block for the service gateway to the File Server allowlist, you add the IP address for the NAT gateway. The File Server allowlist verifies that the request is from the NAT gateway's IP address.
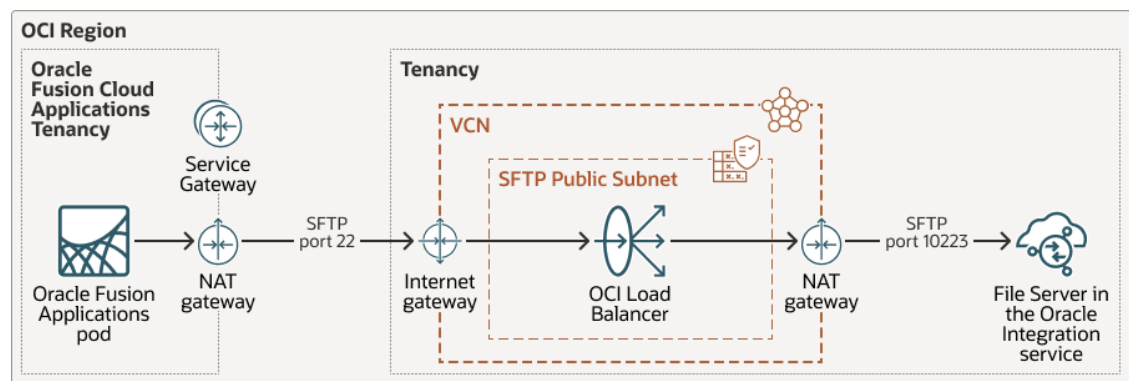
> **Note:**
>
> - The diagram shows traffic originating from an Oracle Fusion Cloud Applications tenancy, but traffic could also originate from another source. For example, a private subnet.
> - The File Server allowlist includes the IP address for the NAT gateway on the VCN.

How Requests Are Routed

Requests go through a load balancer and NAT gateway and then on to File Server.

1. The access request goes through a NAT gateway from the client, which could be a Oracle Fusion Cloud Applications tenancy or a private subnet.

   This diagram shows the NAT gateway routing the request through SFTP port 22 to an internet gateway, but you can use an alternate port.

2. The internet gateway routes the access request to a load balancer that you set up in your virtual cloud network (VCN). The load balancer contains an SFTP TCP listener.

3. The load balancer sends the request through a NAT gateway on the VCN.

4. The NAT gateway routes the request through SFTP port 10223 to the allowlist for File Server.

5. If the allowlist includes the IP address for the NAT gateway that is on the VCN, the allowlist grants access.

Configure This Pattern

To route requests through a NAT gateway, complete the following tasks.

Task	More information
1. Configure a VCN	If your organization doesn't have a virtual cloud network (VCN), configure one. See Creating a VCN in Oracle Cloud Infrastructure Documentation.
2. Configure a NAT gateway	If the VCN doesn't already have a NAT gateway, configure one. See Configure NAT gateway for private compute instances.
3. Configure a subnet	Create a public subnet in the VCN. See Creating a Subnet in Oracle Cloud Infrastructure Documentation.
4. Configure the route rules for the VCN	Configure rules that perform the following tasks: 1. For traffic that is going to File Server, route the traffic through the NAT gateway by specifying the IP address for File Server. Find the IP address for File Server on the Settings page in File Server. See Configure File Server Settings in *Using File Server in Oracle Integration 3*. 2. Route traffic that comes from the client through an internet gateway. See VCN Route Tables in Oracle Cloud Infrastructure Documentation.

Task	More information
5. Set up a load balancer	Create a load balancer, and perform the following configuration steps:

<table>
<tr><td></td><td>1. Within the load balancer, create an SFTP TCP listener that listens for the port of your choice, such as port 22.

See Creating a Load Balancer Listener in the Oracle Cloud Infrastructure Documentation.</td></tr>
<tr><td></td><td>2. Add the IP address and port number for File Server to the load balancer.

Find the IP address for File Server on the Settings page in File Server. See Configure File Server Settings in <i>Using File Server in Oracle Integration 3</i>.</td></tr>
</table>

Task	More information
6. Create a security list for the subnet	For the public subnet, add an **ingress** rule that allows inbound traffic from the client through the port of your choice, such as port 22.
7. Update your allowlist	Update the allowlist for File Server by adding the IP address for the NAT gateway on the VCN. See Create an Allowlist for Public IP Addresses.

Tutorial: Read Files and Write the Files to File Server

Learn how to use the File server action to read one or more files that are on an FTP server and then write the files to File Server in Oracle Integration.

Audience

This tutorial is most helpful if your organization already uses File Server or is considering using it. That's because the tutorial requires you to enable and set up File Server.

This tutorial is also helpful if you want hands-on practice using the File server action. If you just want step-by-step instructions for using the File server action, see Interact with Files in File Server in *Using Integrations in Oracle Integration 3*.

In This Tutorial

- Prerequisites
- Step 1. Create a schedule integration and define its trigger
- Step 2. Connect to an FTP server and list the files in a directory
- Step 3. Pass the folder from the integration's schedule to its invoke action
- Step 4. Loop through the files and process them one at a time
- Step 5. Write the file to File Server
- Step 6. Understand what you've done
- Learn More

Prerequisites

- Set up an invoke FTP connection to your FTP server, and name it `Supplier_FTP`.
- Enable File Server and complete all of the setup steps.

  See Administer File Server in *Using File Server in Oracle Integration 3*.
- Place a file on your organization's FTP server so that you can move the file to File Server. Note the file name and its directory.

Step 1. Create a schedule integration and define its trigger

Start by creating a schedule integration. You pass in two parameters for the integration's trigger.

1. In the navigation pane, click **Design**, then **Integrations**.

2. Select **Create**.

3. Select **Schedule**, and fill in the following field.

Field	Value to use
Name	`Poll_For_New_Files`

4. Select **Create**.

   The integration canvas appears, and a menu of options appears.

5. Select anywhere on the canvas to close the menu.

6. On the canvas, point to the **Schedule** action, select **...**, and select **Edit**.
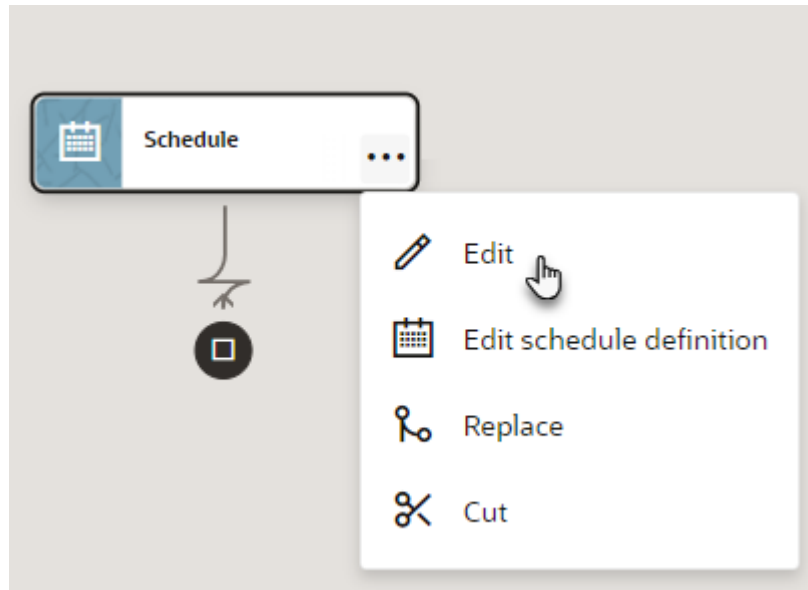
7. Define the parameters for the integration's trigger:

   These parameters let you pass in the file pattern and path of the file you're picking up from your FTP server.

   a. Select **+**, and fill in the following fields.

Field	Value to use
Parameter name	`file_pattern`
Default value	`"*.csv"`

   b. Select **+**, and fill in the following fields.

Field	Value to use
Parameter name	`directory`
Default value	`"/"`

   c. Select **Save**.

You've created a schedule integration that passes in two parameters.

Step 2. Connect to an FTP server and list the files in a directory

Now that you've created an integration, it's time to add an action to it. The invoke action calls your FTP server and lists all the files in a specific directory. You passed the directory into the integration's schedule when you defined its trigger.

1. Point to the line that comes out of the **Schedule** box until a **+** appears, and select the **+**.
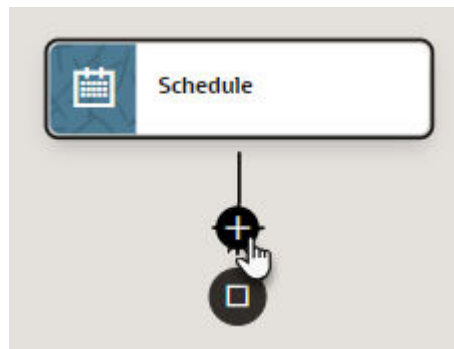
2. In the search field, type **Supplier**, and select the **Supplier_FTP** connection that you created as a prerequisite task.

   An Invoke action appears on the canvas, and the Configure Basic Info panel appears.

3. Fill in the following fields.

Field	Value to use
What do you want to call the endpoint?	`listFiles`
B2B Trading Partner Mode	Do not select this checkbox.

4. Select **Continue**.

5. From the **Select operation** drop-down list, select **List Files**.

6. Fill in the following fields.

Field	Value to use
Input directory	`/` This value is a placeholder. Later on, you'll map the scheduled parameter to it.
File name pattern	`*.csv`
Max files	Leave the default value.
Minimum age	Leave the default value.
List File Recursively	Deselect this option.

Field	Value to use
Ignore File Permissions	Leave this option deselected.

7. Select **Continue**.

8. Review the settings, and select **Finish**.

You finished creating the call to your remote FTP server. The call lists the files in a specific directory.

A Map action appears on the canvas before the Invoke action.

> **Tip:**
>
> To view the actions horizontally on the sanvas, select **Horizontal** ▪▪ on the toolbar.

Step 3. Pass the folder from the integration's schedule to its invoke action

You've defined the invoke action, and now it's time to dynamically pass the directory into it using the Map action.

1. On the canvas, point to the **Map** action, select **...**, and select **Edit**.

   The mapper appears.

2. In the Sources list on the left, observe the two parameters that you configured: **directory** and **file_pattern**.

3. In the Target list on the right, expand **List Request**, then expand **FTP List Header**.

4. In the Sources list, select **directory**, and drag it to the **Directory** entry in the Target list.

5. In the Sources list, select **file_pattern**, and drag it to the **File Name Pattern** entry in the Target list.
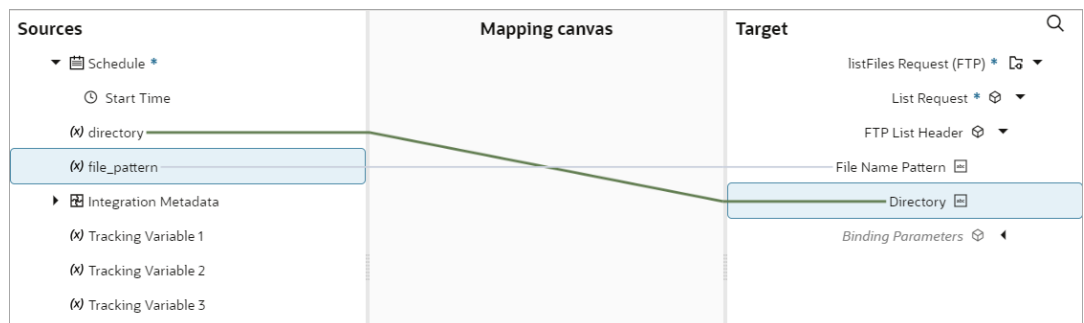
6. Select **Validate**, and then select **<** to return to the canvas.

7. Save your changes.

Now you are passing the directory into the invoke action dynamically using the trigger of the integration.

Step 4. Loop through the files and process them one at a time

The integration must loop through all the files that the invoke action returns. The integration processes the files one at a time using a for each action.

1. Add the for each action to the integration:

   a. Point to the arrow that comes out of the **Invoke** box, and select **+**.

   b. In the pop-up, select the **Actions** tab.

   c. Scroll to and select **For each**.

      A For each action appears on the canvas, and the Configure for each panel appears.

   d. In the panel, select **Edit** ✏️ , and fill in the following field.

Field	Value to use
Name	ForEachFileFound

   e. Select ✔️ .

   f. In the Input sources panel, expand **$listFiles**, then **ListFileResponse**, then **ListResponse**, then **FileList**, and then **File**.

      File lists the properties of each file.

   g. Drag the **File** entry to the **Repeating** element field.

      File is the element that the for each loop repeats on.

   h. In **Current element name**, enter `currentFileDetails`.

      This is the name that the integration uses to refer to the File element in the loop.

   i. Select anywhere in the canvas to close the panel.

2. Specify how the for each loop processes each file.

   The first action downloads a file.

   a. On the canvas, in the box for the For each action, select **+**.

   b. In the search field, type **Supplier**, and select the **Supplier_FTP** connection that you created as a prerequisite task.

      This connection allows you to make a connection to your FTP server.

   c. Fill in the following fields.

Field	Value to use
What do you want to call the endpoint?	downloadFile
B2B Trading Partner Mode	Leave this option deselected.

   d. Select **Continue**.

   e. Fill in the following fields.

Field	Value to use
Select operation	Select **Download File**.
Select a Transfer Mode	Leave **Binary** selected.
Input directory	Leave this field blank for now. Later on, you'll dynamically populate this field using the mapper.
File name	Leave this field blank for now. Later on, you'll dynamically populate this field using the mapper.
Download directory	`/stage/files` This is the location in Oracle Integration where you'll temporarily store the downloaded file.
Checkboxes on the page	Leave all the checkboxes deselected.

    f.   Select **Continue**.

    g.   Review the settings, and select **Finish**.

You return to the canvas. The Invoke action that you configured appears within the For each action, and a Map action appears before it. The invoke action downloads a file and stores it in a temporary location.

3. Pass the relevant data to the Invoke action.

This action ensures that within the loop, for each file that the integration finds, the integration downloads the file to the local staging area.

    a.   Within the For each action, point to the **Map** action, select **...**, and select **Edit**.

        The mapper opens.

    b.   In the Sources list on the left, expand **CurrentFileDetails**, then expand **File**.

        The containers hold information about the current file that has been returned from when you collected a list of files in a directory.

    c.   In the Target list on the right, expand **Download Request**.

        This container holds information about the action you defined for downloading the file.

    d.   In the Sources list, select **Directory**, and drag it to the **Directory** entry in the Target list.

    e.   In the Sources list, select **Filename**, and drag it to the **Filename** entry in the Target list.
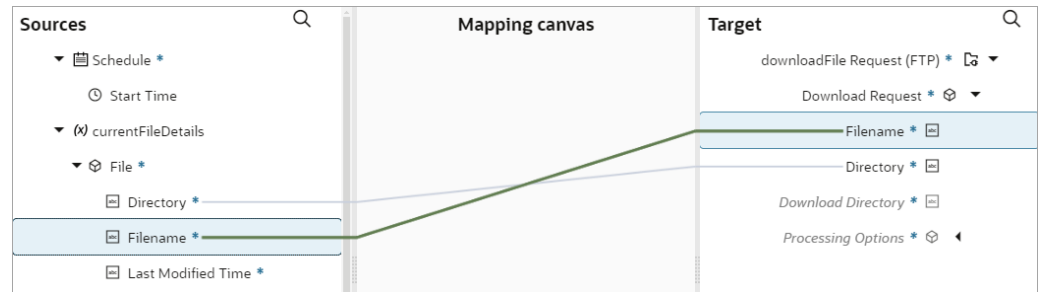
f. Select **Validate**, and then select **<** to return to the canvas.

g. Save your changes.

Step 5. Write the file to File Server

The for each loop processes the files one at a time. After processing a file, the integration writes the file to File Server.

1. In the vertical toolbar to the right of the canvas, select , and find the **File server** entry.

2. Drag the **File server** entry to the **+** that appears on the **Invoke** action that is within the **For each** action.

   This panel offers an alternate way to add actions to an integration.

A File server action appears in the For each action, and the **Configure FS Native Action** panel appears.

3. Fill in the following fields.

Field	Value to use
What do you want to call your endpoint?	`writeFileToFileServer`
Select resource	Select **File**.
Select operation	Select **Write File**.
Specify an Output Directory	`/inbound/supplier/invoices` This is the directory that you want to write the file to in File Server.

Field	Value to use
File Name	`file.txt` Later on, you'll overwrite this value in the mapper. You'll use the file name that you got when you listed the file names.

4. Select **Continue**.

5. Review the settings, and select **Finish**.

   You return to the canvas. The File server action that you configured appears within the For each action, and a Map action appears before it. The File server action writes a file to File Server.
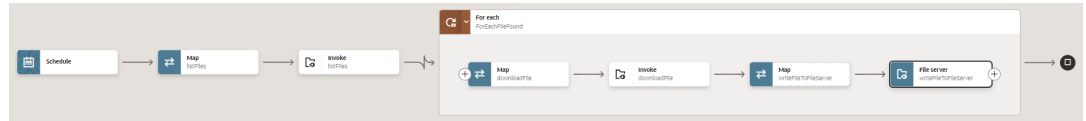
   Now you need to pass in the name of the file to be written, as well as the file itself, to the File server action.

6. Pass the relevant data to the File server action.

   a. Point to the **Map** action that is before the **File server** action, select **...**, and select **Edit**.

      The mapper opens.

   b. In the Source list on the left, expand **downloadFile Response (FTP)**, then **Download File to ICS Response**, then **Download Response**, then **ICS Files**, then **ICS File**.

      The elements are the output of the operation to download the file from the FTP server.

   c. In the Target list on the right, expand **File Definitions Write Request**.

      Its child elements are the properties that the file operation accepts.

   d. In the Sources list, select **File Reference**, and drag it to the **File Reference** entry in the Target list.

      You are passing the contents of the file that you downloaded to the staging area to the File server action in the integration.

   e. In the Sources list, below **File Reference**, expand **Properties**.

   f. In the Sources list, select **Filename**, and drag it to the **Output File Name** entry in the Target list.

      You are passing the name of the file to the File server action.
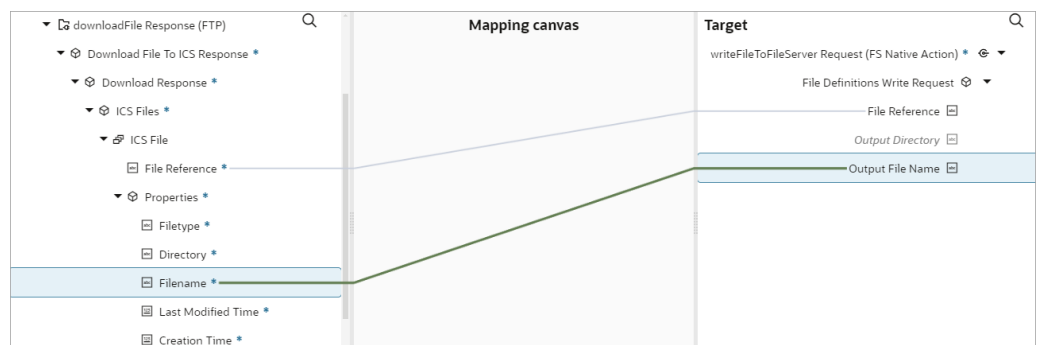
g. Select **Validate**, then select **<** to return to the canvas.

The integration retrieves a list of files from an FTP server and writes the files to File Server in Oracle Integration using the File server action.

Step 6. Understand what you've done

Let's review a few key actions in the integration so that you understand the integration that you just designed.

Action	Goal
Schedule action	You created a schedule integration, which runs on demand or by the clock.
Invoke action	The integration's first action is to make a call to your FTP server to list the files in a directory. You specify the directory using the Map action that is before the Invoke action.
For each action	The integration loops through the files that are in the list of files that you just got. For each file in the list, the integration performs several actions. • **Invoke action:** The integration downloads the file. • **File server action:** The integration writes the file to File Server.

Learn More

To review all of your options for the File server action, including encrypting and decrypting files, see Interact with Files in File Server in *Using Integrations in Oracle Integration 3*.

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 3*.

Topics:

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

Enable File Server

An administrator must enable File Server before an organization can start using it with their Oracle Integration instance. Enabling File Server is a one-time action in the Oracle Cloud Infrastructure Console.

If your organization hasn't enabled File Server yet, and you select File Server from the navigation pane, the following message appears:
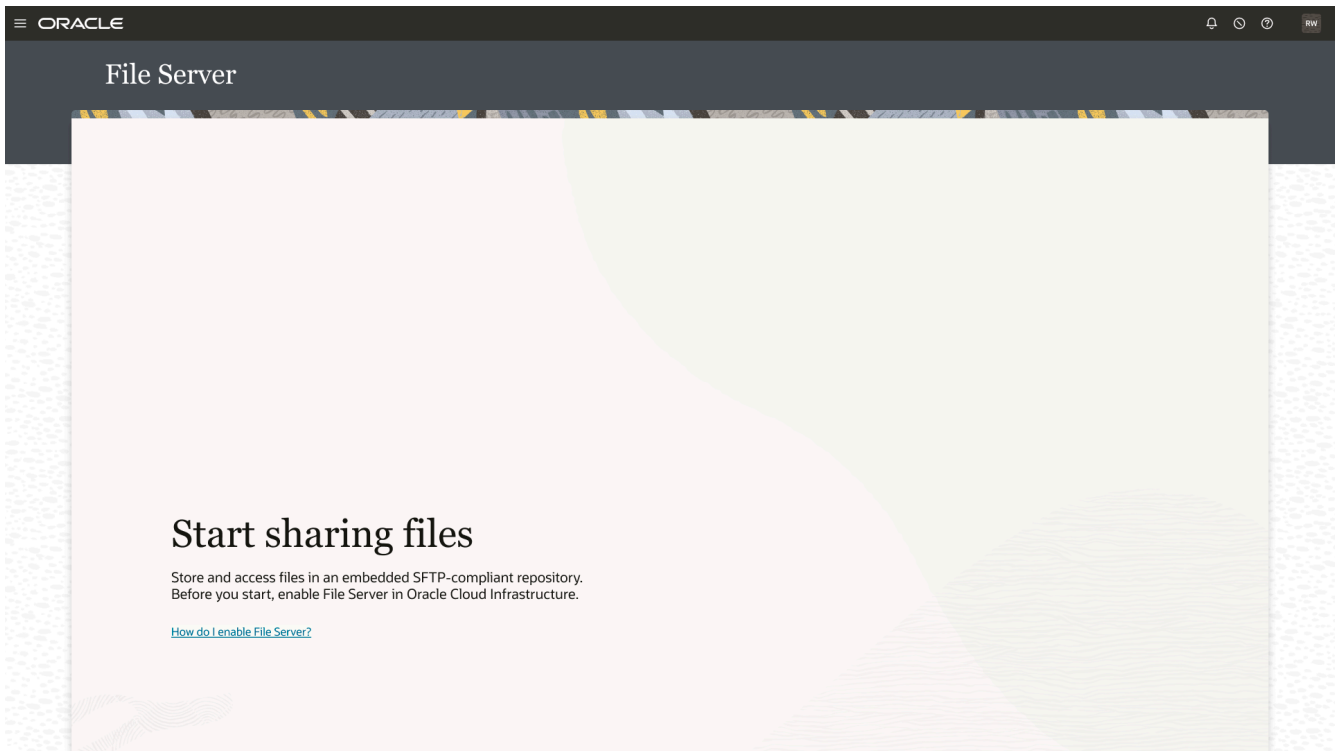
> **✎ Note:**
>
> To enable File Server for an Oracle Integration instance, you must have Oracle Cloud Infrastructure manage access to the instance. See Creating an OCI Policy to Manage Instances in *Provisioning and Administering Oracle Integration 3*.

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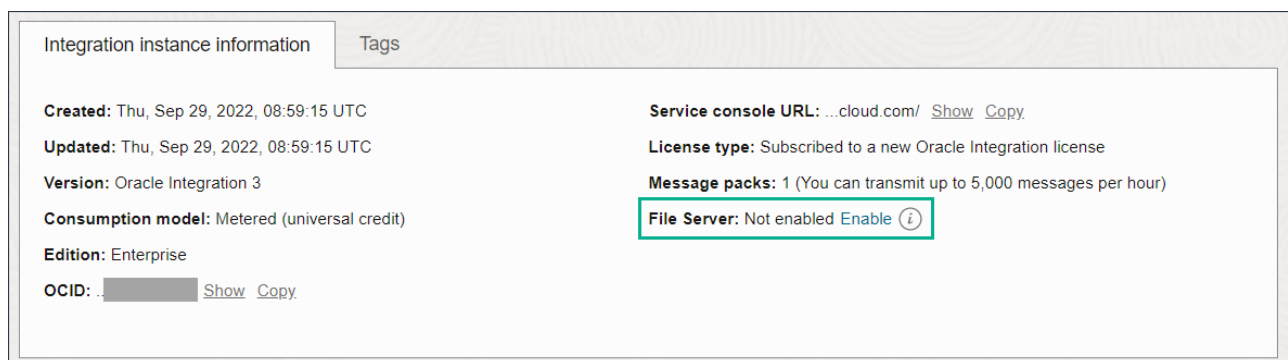
3. When prompted to confirm enabling File Server, click **Enable**. The OIC icon turns orange and its status changes to Updating. Enablement can take several minutes.

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. In the navigation pane, click **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. In the navigation pane, click **Settings**, then **File Server**, then **Settings**.

   The Settings page is displayed.

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

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**, specify a timeout and note the hostname, IP, and port settings.

Field	Descripton
Idle Timeout	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).
Host, IP and Port Information	Review the values for File Server's IP address, port number, and hostname. Oracle assigns these read-only values during provisioning. **When you need these values** You need these values to connect to File Server using the following methods: • Connect by configuring an SFTP client • Connect by configuring a connection that is based on the Oracle Integration FTP Adapter. **Options for specifying these values** When configuring these methods, you can provide either of the following values: • Use the provided port and hostname. • Use the provided port and IP address. > ⚠️ **Caution:** > > If your organization has configured a disaster recovery solution, **you must use the provided port and hostname**, rather than the IP address and hostname. If you use the IP address, the failover for File Server occurs. However, none of your connections to File Server work after the failover.

4. Under **Default Home Folder Configuration for Users**, 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.

Field	Description
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 Folder:** Allow subfolders to be created. • **Rename Folder:** Allow subfolders to be renamed. • **Delete Folder:** 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 (located below the **Save** button) when configuring subfolder permissions from the Permissions page.

5. Under **Default Home Folder Configuration for Groups**, 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]`.
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. • **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 Folder:** Allow subfolders to be created. • **Rename Folder:** Allow subfolders to be renamed. • **Delete Folder:** 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 (located below the **Save** button) when configuring subfolder permissions from the Permissions page.

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

Some fields include multiple values. To remove a value, click its **x**. If you remove a value, File Server doesn't support the value until you add it back. To add a value back, click within a field and select from the list that appears.

> **Note:**
>
> The SFTP 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 cannot connect to File Server.

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 3*. > **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.
Signature Algorithms	**RSA algorithms** • `rsa-sha2-256` • `rsa-sha2-512` • `ssh-rsa` **EdDSA algorithm** • `ssh-ed25519` **ECDSA algorithms** • `ecdsa-sha2-nistp256` • `ecdsa-sha2-nistp384` • `ecdsa-sha2-nistp521` > **WARNING:** > If you connect to File Server and then change your algorithms, you must update the `known_hosts` file. If you don't, your connection to File Server closes and a warning appears. See Update the List of Supported Algorithms. See IETF RFC 4253 - SSH Transport Layer Protocol for detailed descriptions.
Key Exchange Algorithms	File Server supports the following options: • diffie-hellman-group-exchange-sha256 • diffie-hellman-group14-sha1 See IETF RFC 4253 - SSH Transport Layer Protocol for detailed descriptions.

Chapter 2
Update the List of Supported Algorithms

Field	Description
Cipher Suites	File Server supports the following options: • aes128-ctr • aes192-ctr • aes256-ctr See IETF RFC 4253 - SSH Transport Layer Protocol for detailed descriptions.
Message Authentication Algorithms	File Server supports the following options: • hmac-sha2-256 • hmac-sha2-512 See IETF RFC 4253 - SSH Transport Layer Protocol for detailed descriptions.
Compression Methods	File Server supports the following options: • Zlib • zlib@openssh.com • No Compression See IETF RFC 4253 - SSH Transport Layer Protocol for detailed descriptions.

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.

Update the List of Supported Algorithms

After you enable a new algorithm to encrypt files in File Server, you must make some quick and easy updates to the `known_hosts` file. Otherwise, your connection to File Server closes and a warning appears.

Who needs to update the known_hosts file

The warning appears if any of the following statements are true:

• You've connected to File Server before and then enable an additional algorithm.

• You've never saved changes on the File Server Settings page before and File Server introduces an algorithm in a functional release.

The warning doesn't appear under any of the following circumstances:

• An integration uses the FTP adapter to connect to File Server.

• You enable an additional algorithm and have never connected to File Server before.

• You enable an additional algorithm but want to continue using your previously selected algorithm.

ORACLE

2-7

Warning text and why it occurs

If you remove the algorithm that you previously used, or if you pass an argument for using the new algorithm when connecting to File Server, the connection closes. Additionally, warning text that is similar to the following message appears in your SFTP client.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!    @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
<fingerprint>.
Please contact your system administrator.
Add correct host key in ~/.ssh/known_hosts to get rid of this message.
Offending RSA key in ~/.ssh/known_hosts:<line_no>
Host key for [<fileserver-ip>]:<fileserver-port> has changed and you have
requested strict checking.
Host key verification failed.
Connection closed.
Connection closed
```

The warning text appears because your `known_hosts` file recognizes only the algorithm you previously used to connect to File Server. When you try to connect using a new algorithm, or if the algorithm that you previously used is no longer enabled, File Server appropriately recognizes that the connection attempt could be an attack and prevents you from making the connection.

Why an update is needed

To connect File Server again and keep working, you must update your `known_hosts` file so that File Server knows that it's safe to transmit files using the new algorithm.

To update the list of supported algorithms and the known_hosts file:

1. In Oracle Integration, update the algorithms that you support.

   a. In the navigation pane, click **Settings**, then **File Server**, then **Settings**.

      The Settings page is displayed.

   b. Under **Security**, update algorithm settings as needed.

      For example, click within the **Signature Algorithms** field, and select one or more additional algorithms. To remove a value, click its **x**.

   c. Click **Save**.

2. Delete the key for the previously supported algorithm from the `known_hosts` file.

   For example, if you previously used the `ssh-rsa` algorithm, delete the entry for `ssh-rsa`, its port, and its signature.

3. Connect to File Server, and pass the new algorithm as an argument in your connection string.

   For example, use the following connection string if you're using the `ssh-ed25519` algorithm.

```
sftp -oHostKeyAlgorithms=ssh-ed25519 -oPort=fileserver-port user@fileserver-ip
```

4. When your SFTP client asks whether to update the `known_hosts` file, type **yes** and press **Enter**.

You can now continue using File Server as you did before.

Configure Users

On the Users page, you give people access to File Server, configure people's public keys, and specify details for their home folders.

Before configuring users, you should Configure File Server Settings.

1. In Oracle Cloud Infrastructure Identity and Access Management (IAM), create users whom you want to access File Server.

    See Managing Users in the Oracle Cloud Infrastructure Documentation.

   After adding users, you can give them access to File Server.

2. Find the user to configure.

    a. In the navigation pane, click **Settings**, then **File Server**, then **Users**.

        The Users page displays a list of user identities from IAM. The table shows whether each user is configured and enabled, as well as their home folder. When you hover over a row, icons appear for configuring users and viewing user details.

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

    c. If needed, click **Filter** ≂ to narrow the results list by users' configured and enabled status.
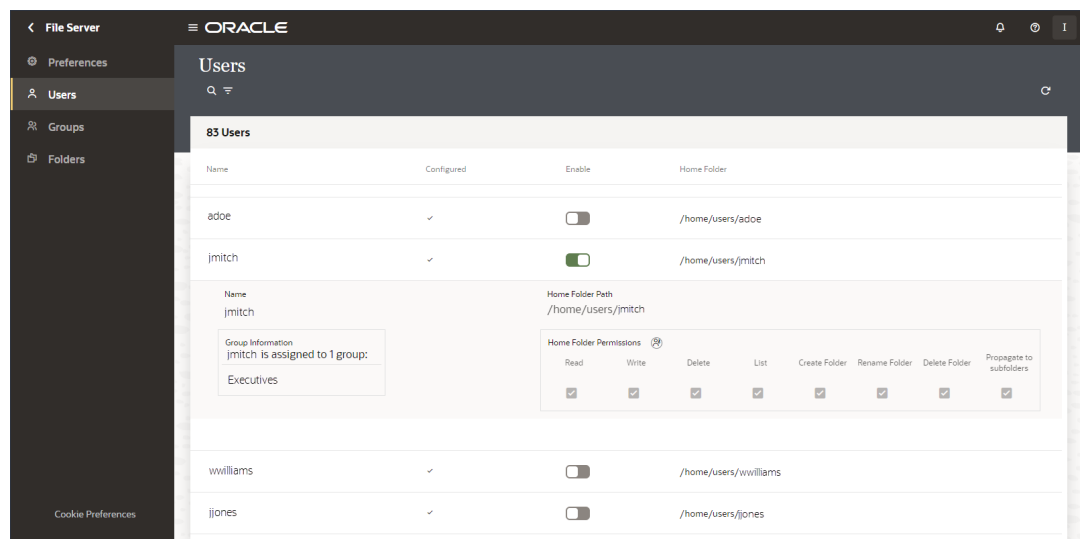
3. Configure a user's access to File Server.

    a. Hover over a user and click **Configure** ✏.

    b. Update the fields as necessary.

Field	Description
User's name	Enable or disable the user. Only enabled users can access File Server. You can configure a user and leave the user disabled until they need access to File Server. You can also temporarily disable the user's File Server access without removing their public key and permissions.
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 public key** ⬆, then **Choose File**, 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.
Home Folder	View the user's home folder path.

    c. Click **Save**.

4. View user details.

    a. Hover over a user and click **Open Details** ⌄.

      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.

    b. To view and change permissions of the user's home folder, next to Home Folder Permissions, click **Go to Home Folder 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 Cloud Infrastructure Identity and Access Management (IAM), create groups that you want to enable with SFTP access to File Server.

    See Managing Groups in the Oracle Cloud Infrastructure Documentation.

    After adding groups, you can give them access to File Server.

2. Find the group to configure.

   **a.** In the navigation pane, click **Settings**, then **File Server**, then **Groups**.

      The Groups page is displayed, showing group identities from IAM.

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 and viewing group details.

b. Click **Search** Q, enter a full or partial name to find, and press **Enter**.

c. If needed, click **Filter** to narrow the results list by groups' configured and enabled status.
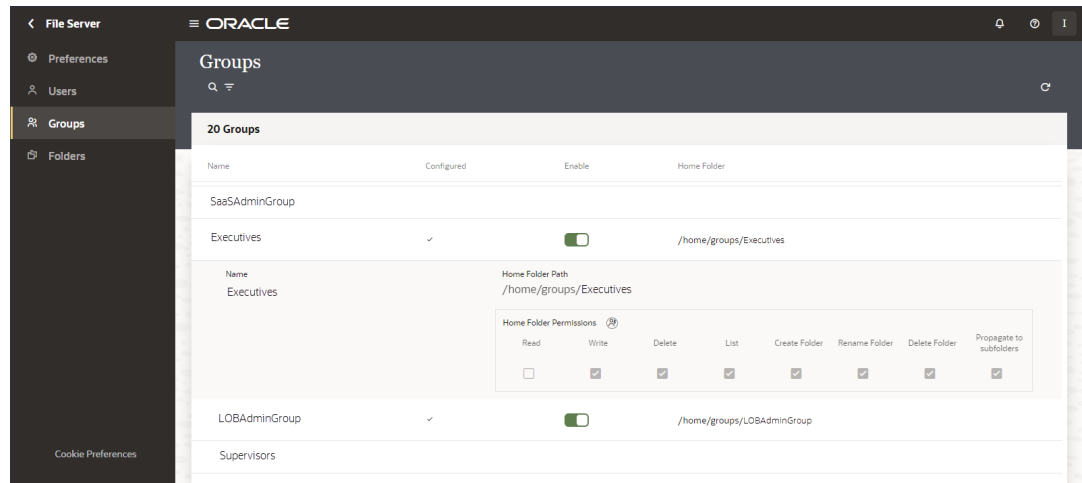

3. Configure a selected group for File Server access.

a. Hover over a row and click **Configure** .

The Property panel is displayed.

b. Update the fields as necessary.

Field	Description
Group name	Specify whether the selected group can currently access the SFTP server by enabling or disabling the group.
	For example, you can configure a group and leave the group disabled until the group needs access to File Server. You can also temporarily disable a group's access without removing its permissions.
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.
Home Folder	View the group's home folder path.

c. Click **Save**.

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 .

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

Configure Folders and View List of Files

Use the Folders 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.

After you configure folders, 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. In the navigation pane, click **Settings**, then **File Server**, then **Folders**.

   The Folders page is displayed, with the current folder's path shown. The selected folder appears above the table, and the subfolders appear in the table. Files are listed with name, last modified date, and size displayed.

2. Optional: Find a folder or file by sorting, searching, or filtering.

   - 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 the **X** on the search bar to return to the default display.

   - Click **Filter** ▼, choose whether to view folders or files, and click **Apply**. Click the **X** on the filter to return to the default display.

3. Optional: Create, rename, or delete folders as needed.

   - To add a folder in the currently selected path, click **Create**, enter a name, and click **Create**.

   - To rename a folder, hover over the folder and click **Actions** ⋯. Select **Rename**, enter a new name, and click **Rename**.

   - To delete a folder, hover over the folder and click **Delete** 🗑. Deleting a folder deletes its contents, too, including any subfolders and files.

   > **Tip:**
   >
   > To open a folder and view its list of folders and files, click the folder name.
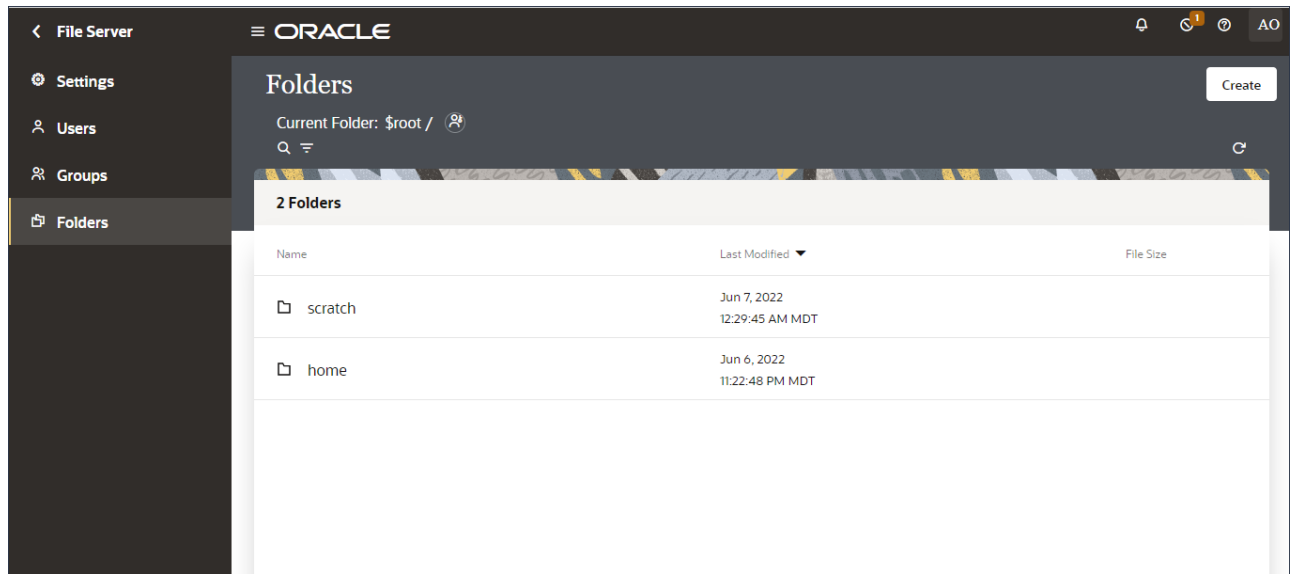
4. Set folder permissions.

   a. Hover over a folder and click **Permissions** .

      The Permissions page appears.

   b. Follow the steps in Set Folder Permissions.

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

6. Click **Save**.

After configuring folders, create an allowlist for File Server. See Create an Allowlist for Public IP Addresses.

Set Folder Permissions

On the Permissions page, choose the people who can read, write, delete, and perform other actions on a folder and its files.

1. In the navigation pane, click **Settings**, then **File Server**, then **Folders**.

2. Hover over a folder, and click **Permissions** .

   The Permissions page is displayed, showing a list of users or groups with permissions configured for the current folder. The icon next to each entry identifies whether it is a user or a group.

3. Change permissions as needed. For example:

   • To change permissions for the users and groups, select or deselect permission checkboxes.

   • To remove all permissions for a user or group, click **Delete Identity** .

4. To block permissions that are set to **Propagate to Subfolders** from applying to the folder, select **Do not inherit**.

   This setting prevents permissions from being propagated to this folder and its subfolders.

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

a. Click **Add Permissions**.

b. In the Select Users or Groups panel, click the **Users** or **Groups** tab, select one or more identities, and click **Add**. The new identities are added to the permissions list.

c. Click **Close**.

d. Select checkboxes to set specific permissions. Select a checkbox at the top of the table to assign a permission to all listed users and groups.
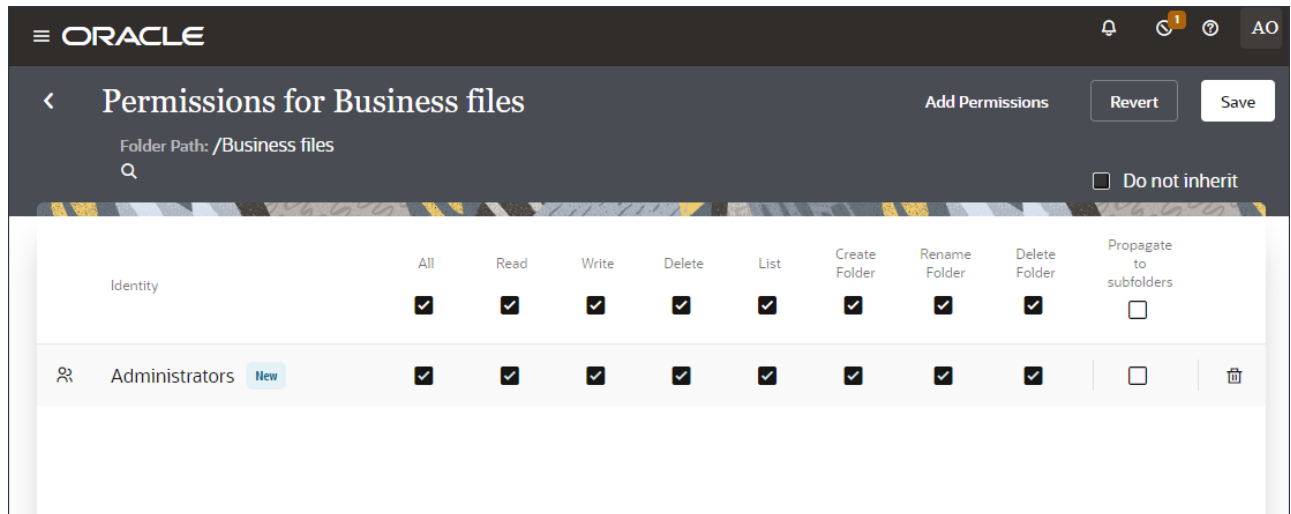
Field	Description
All	Assign all permissions to this user or group.
Read	Allow files to be downloaded.
Write	Allow files to be uploaded.
Delete	Allow files to be deleted.
List	Allow listing of the folder's contents.
Create Folder	Allow subfolders to be created.
Rename Folder	Allow renaming of subfolders.
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. If needed, revert changes made to folders since the last save by clicking **Revert**.

7. Click **Save**.

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

Options for Working Folders

The top-level directory for File Server is named `root`. The `root` folder contains the `home` folder.

• **The `root/home` folder is where File Server creates the default folders**

An administrator creates users and groups in Oracle Cloud Infrastructure Identity and Access Management (IAM). When you enable a user's or group's access to File Server, File Server creates a folder for them:

– Group folders are created in `root/home/groups/<group>`

– User folders are created in `root/home/users/<user>`

Be aware of the following rules for the `root/home` folder:

– You cannot delete the folders that File Server creates. However, you can delete the files and sub-folders within the folders that File Server creates.

– You cannot create folders in the following folders: `root/home`, `root/home/groups`, and `root/home/users`. However, you can create folders within each user's and group's folder.

– If an administrator deletes a group in IAM, 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.

• **The `root` folder is where you create your working folders**

  Create folders as needed within the `root` folder.

Create an Allowlist for Public IP Addresses

A tenant administrator must create an allowlist (formerly a whitelist) for File Server. Only users from the entities that you specify in the allowlist can connect to File Server. You create the allowlist in the Oracle Cloud Infrastructure Console, the same place where you enable File Server.

Prerequisites

Before creating an allowlist, you should create and manage folders and their permissions. See Configure Folders and View List of Files.

About the Allowlist

With the allowlist, you allow one or more of the following entities to access File Server:

• Single IP address, such as 10.10.10.10

• Classless Inter-Domain Routing (CIDR) block (that is, an IP address range), such as 10.0.0.0/24

You can create up to 15 rules for File Server, in addition to the 15 rules that you can create for HTTP connections. A rule can also apply to both File Server and HTTP.

Required Updates After Upgrading to Oracle Integration 3

If you had a File Server allowlist in Oracle Integration Generation 2 and upgraded to Oracle Integration 3, Oracle assigned you new IP and port values for the File Server SFTP server. The Oracle Integration Generation 2 IP and port values remain valid for SFTP runtime traffic for four months after the upgrade. Understand how the new IP and port values that Oracle assigns after the upgrade affect your File Server allowlist:

• For SFTP clients that were on your File Server allowlist in Oracle Integration Generation 2

These SFTP clients can continue accessing File Server using the Oracle Integration Generation 2 IP and port values. This access is granted for up to four months after the upgrade and persists even if you remove the SFTP clients from your self-service File Server allowlist.

You have the following action items:

– Within the four-month time window, you must update all integrations and SFTP clients so that they use the new IP and port values.

  While you don't have to update the values immediately after the upgrade, Oracle recommends completing this step then. Otherwise, you risk forgetting to update the values and then experiencing issues when Oracle retires the IP and port values.

– If you want to block the integrations and SFTP clients from accessing File Server, enter a service request (SR).

• For SFTP clients that weren't on your File Server allowlist in Oracle Integration Generation 2, such as new SFTP clients that you configure after upgrading

You have the following action items:

– Ensure that all integrations and SFTP clients use the Oracle Integration 3 IP and port values to access File Server.

– Add the SFTP clients to the File Server allowlist.

To Manage the Allowlist:

• Manage the allowlist in the Oracle Cloud Infrastructure Console.

See Configure an Allowlist for Your Instance in *Provisioning and Administering Oracle Integration 3*.

3
Troubleshoot File Server

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

An SFTP client cannot connect to File Server

Complete these troubleshooting steps.

1. **Access your personal Home folder using a supported SFTP client.**
   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. Work with an administrator to update your permissions.

2. **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.

3. **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.

4. **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.

5. **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. In the navigation pane, click **Settings**, then **File Server**, then **Settings**.
      The Settings page is displayed.

   b. Below the Security heading, review the options in the following fields:

      • Authentication Type

      • Signature Algorithms

      • 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.

6. **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.

File Server isn't 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.

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.

Folders for users and groups can't be deleted

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.

The connection closes and a warning appears when you connect to File Server after an algorithm update

If you enable additional algorithms but don't update your `known_hosts` file, and you attempt to connect to File Server, your connection closes. Additionally, warning text similar to the following message appears.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
<fingerprint>.
Please contact your system administrator.
Add correct host key in ~/.ssh/known_hosts to get rid of this message.
Offending RSA key in ~/.ssh/known_hosts:<line_no>
Host key for [<fileserver-ip>]:<fileserver-port> has changed and you have
requested strict checking.
Host key verification failed.
Connection closed.
Connection closed
```

See Update the List of Supported Algorithms.