Oracle® Revenue Management and Billing Cloud Service

Release 8.1.1

SFTP Authentication and Access Permissions Guide

Revision 2.1

F75584-01

November 2022

ORACLE

Oracle Revenue Management and Billing Cloud Service SFTP Authentication and Access Permissions Guide

F75584-01

Hazardous Applications Notice

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Third-Party Content, Products, and Services Disclaimer

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Preface

About This Document

This document will help you to understand how to generate the public and private keys for SFTP user authentication. It explains how to establish authentication with the SFTP hosts in the ORMB cloud service using the public and private keys.

It also explains how to access the SFTP server using WinSCP, how to create the directories and files on the SFTP server, and how to set the read, write, and execute permissions for a file or folder on the SFTP server. In addition, it explains how to upload the files and folders to the SFTP server and download the files and folders from the SFTP server.

Intended Audience

This document is intended for the following audience:

- End-Users
- System Administrators
- Consulting Team

Organization of the Document

The information in this document is organized into the following sections:

Section No.	Section Name	Description
Section 1	SFTP Authentication	Explains how to generate the SSH key pair (i.e., public and private keys) for each user who requires SFTP access.
Section 2	Accessing the SFTP Server	Explains how to access the SFTP server using WinSCP.
Section 3	Creating Directories on the SFTP Server	Explains how to create the directories or folders on the SFTP server.
Section 4	Setting the Recursive Permissions for a Directory	Explains how to set the recursive permission for a directory on the SFTP server.
Section 5	Setting the Permissions for a File	Explains how to set the permission for a file on the SFTP server.
Section 6	Transferring the Files using WinSCP	Explains how to upload and download the files from the SFTP server using WinSCP.

Conventions

The following conventions are used across the document:

Convention	Meaning
boldface	Boldface indicates graphical user interface elements associated with an action, or terms defined in the text.
italic	Italic indicates a document or book title.
monospace	Monospace indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or information that an end-user needs to enter in the application.

Acronyms

The following acronyms are used in this document:

Acronym	Meaning
ORMB	Oracle Revenue Management and Billing
SFTP	SSH File Transfer Protocol
SSH	Secure Socket Shell

Related Documents

You can refer to the following documents for more information:

Document Name	Description
Oracle Revenue Management and Billing Cloud Service Release 8.1.1 Release Notes	Lists the feature enhancements and client platforms and browsers that are supported in this release. It highlights different roles and responsibilities of Oracle and Customer in deploying, configuring, and maintaining the Oracle Revenue Management and Billing Cloud Service. It also highlights the known issues in this release.
Oracle Revenue Management and Billing Cloud Service Licensing Guide	Lists different features which are offered when you acquire a license for the following cloud services: • Oracle Financial Services Revenue Management and Billing • Oracle Insurance Revenue Management and Billing It also provides the licensing information of Oracle software and third-party JARs and components which are included in the above-mentioned cloud services.

Document Name	Description
Oracle Revenue Management and Billing Cloud Service Federated Identity Configuration Using IDCS	Provides an overview of federated SSO login. It explains how to configure federated SSO login with SAML for the ORMB Cloud Service.
Oracle Revenue Management and Billing Cloud Service REST Services Configuration Guide	Explains how to configure federated Web service login to access protected REST services on the ORMB Cloud environments.
Oracle Revenue Management and Billing Cloud Service End-User Onboarding Using IDCS	Explains how to setup the security administrator account for the ORMB Cloud Service. It also explains how to manage users and user groups for the ORMB Cloud Service. In addition, it explains how to import and export bulk users and user groups for the ORMB Cloud Service.
Oracle Revenue Management and Billing Cloud Service SaaS Reporting using OAS	Provides an overview of the ORMB SaaS reporting architecture. It also explains how to use Oracle Analytics Server for ORMB SaaS reporting.
Oracle Revenue Management and Billing Cloud Service Federated Identity Configuration Using IAM	Provides an overview of federated SSO login. It explains how to configure federated SSO login with SAML for the ORMB Cloud Service.
Oracle Revenue Management and Billing Cloud Service End-User Onboarding Using IAM	Explains how to setup the security administrator account for the ORMB Cloud Service. It explains how to manage users and groups for the ORMB Cloud Service. In addition, it explains how to import and export bulk users and groups for the ORMB Cloud Service and how to use SAML on the Cloud environment for single sign-on.

Change Log

Revision	Last Update	Updated Section	Comments
2.1	05-Jul-2023	Related Documents	Added Information

Contents

1. SFTP Authentication

The SSH File Transfer Protocol (SFTP) is a secure file transfer protocol. It runs over the SSH protocol. You use the SFTP user accounts to sign in to the SFTP server so that you can perform FTP operations related to the Oracle Revenue Management and Billing Cloud Service.

You can use SSH keys to establish an SFTP connection. SSH keys is a pair of public and private keys used to authenticate a client when it connects to an SFTP server. The user's private key is kept secret and stored locally on the user's computer while the user's public key is used for verification on the SFTP server where the user wants to connect. These public and private keys use asymmetric cryptography to establish the client's identity.

1.1 SFTP Authentication Process

The following figure illustrates how an SFTP connection is established using the public and private keys.

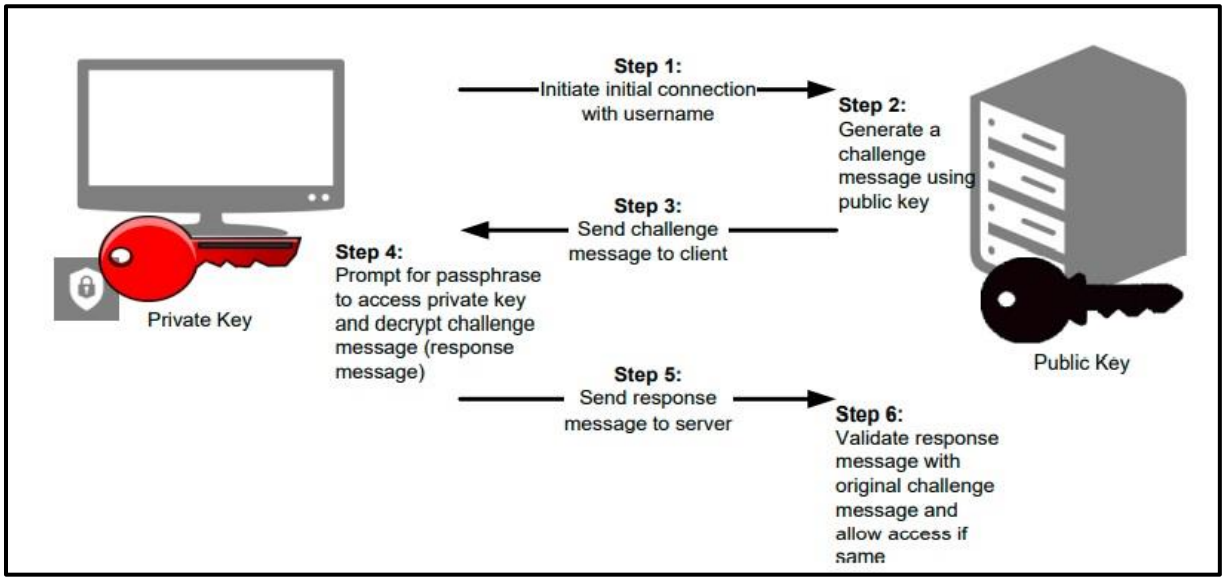

Figure 1: SFTP Authentication Process

The following steps are involved while establishing SFTP connection using the SSH key based authentication:

1. The SFTP client tries to connect to the SFTP server using the username and private key.
2. The SFTP server considers the public key of the respective user and constructs a challenge message based on the public key. This challenge message is then returned to the SFTP client.
3. The SFTP client locates the private key on the local machine and prompts for a passphrase to access the private key (when necessary).
4. The SFTP client then generates a response to the challenge message using the private key. This response is then sent to the SFTP server.
5. The SFTP server takes the message response and validates it using the public key and then grants the required access.

1.2 Generating SSH Key Pair using PuTTY Key Generator

To generate the SSH key pair (i.e., public and private keys) for a user who requires SFTP access:

1. Open the **WinSCP** application on your local machine. The **Login** window appears.
2. Click **Tools**. A menu appears.

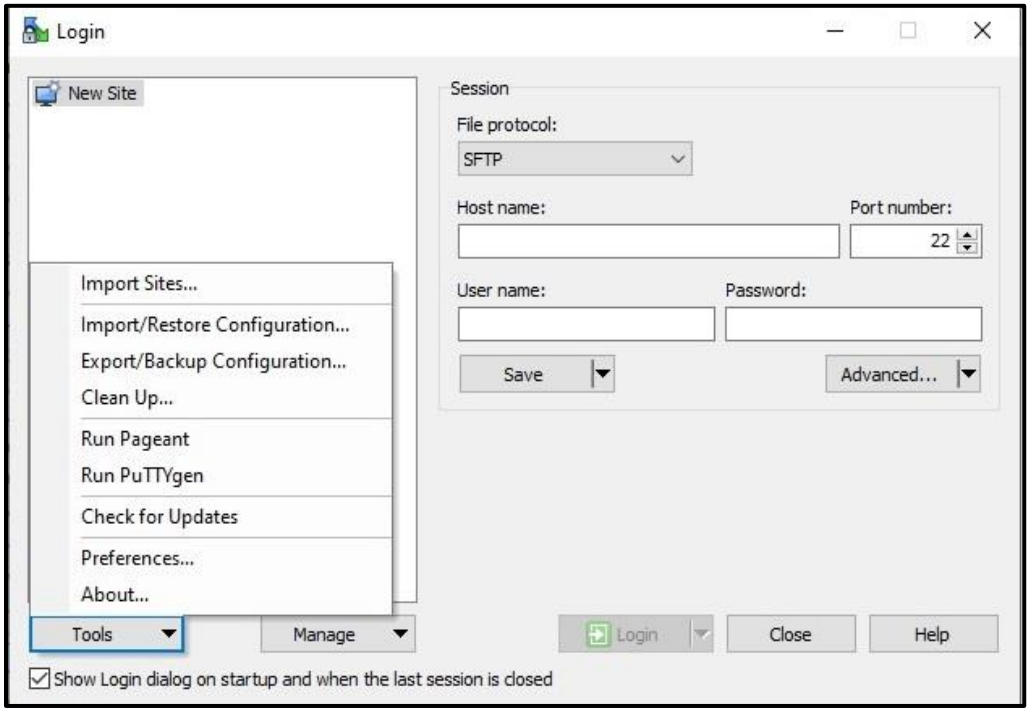

Figure 2: WinSCP Login Window

3. Click the **Run PuTTYgen** option from the menu. The **PuTTY Key Generator** window appears.

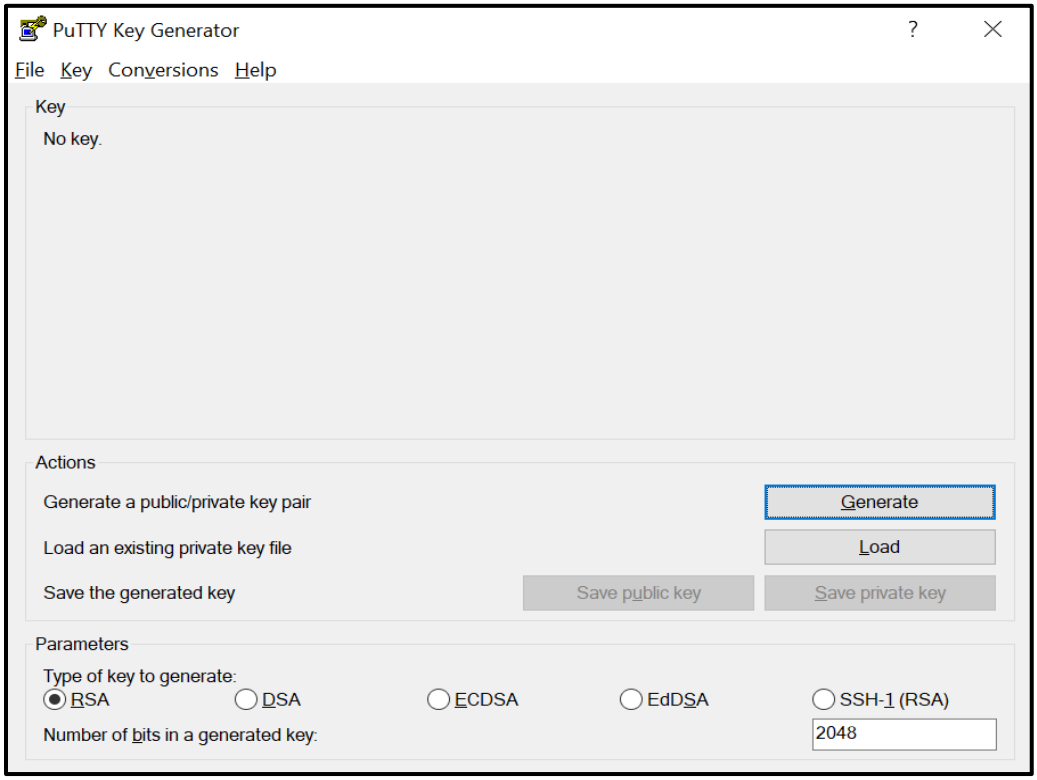

Figure 3: PuTTY Key Generator Window

4. Click **Generate**. The generated public and private keys appear in the **Key** section of the **PuTTY Key Generator** window. Note that you need to keep moving the mouse over the blank area in the **Key** section until the keys are generated.

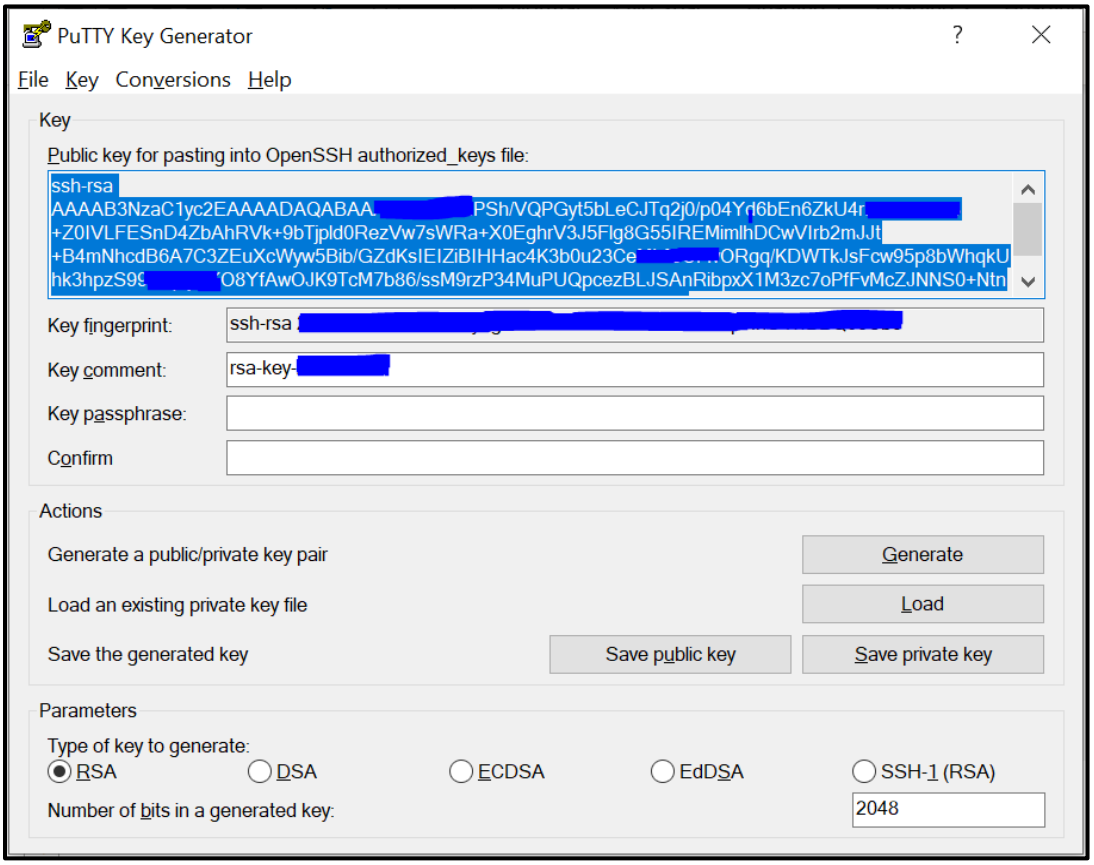

Figure 4: Public and Private Keys

5. Enter the phrase that functions like a password when there are two or more users with the same username in the **Key passphrase** field. If there are two or more users with the same username, the passphrase is required to subsequently access the private key.
6. Copy the public key from the **Key** section and then paste it in a text file.
7. Save the text file.

Note: You must share the public key with the **Oracle AMS** team for authenticating user on the SFTP server.

8. Click **Save private key** to save the private key on your local machine in a text file. By default, the file is named as `My_Private_key.ppk`.

Note: The private key is used to login to the SFTP server. It is critically important that the private key file is secured and always protected.

1.3 Submitting the Public Key to Oracle AMS Team

Raise a service request with Oracle Global Support and attach the public key file in the service request. Indicate the user and environment for which you want to use this public key to establish an authenticated session. Before creating the service request, ensure that the user is already created by Oracle AMS team with a temporary password. The SSH key pair will replace the temporary password.

Oracle will take the public key and associate it with the relevant user on the relevant environment, and then update the service request accordingly.

2. Accessing the SFTP Server

To access the SFTP server using WinSCP:

1. Open the **WinSCP** application on your local machine. The **Login** window appears.

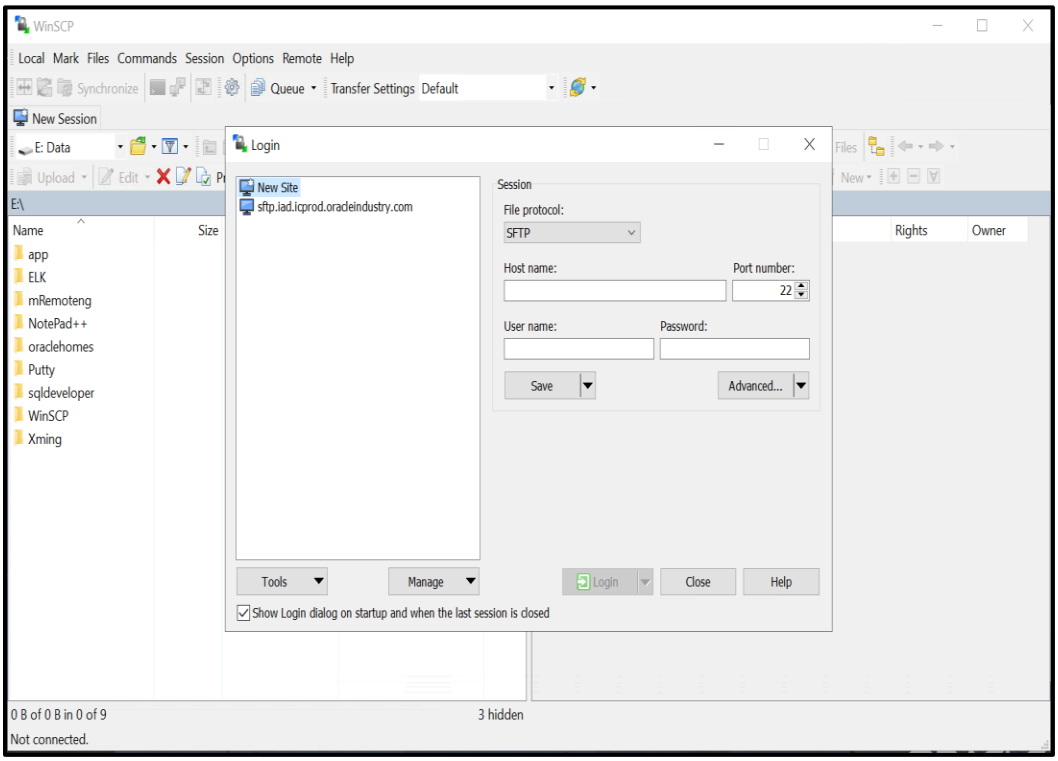

Figure 5: Login Window

2. To create a new **WinSCP** session, click the **New Site** option in the left pane of the **Login** window.
3. Enter the following details in the right pane of the **Login** window:
   - **File protocol** – Used to indicate that you want to use the SFTP protocol to connect to the SFTP server.
   - **Host name** – Used to specify the IP address of the SFTP server to which you want to connect. This SFTP endpoint URL is shared by the Oracle AMS team.
   - **Port number** – Used to specify the port number of the SFTP server to which you want to connect.
   - **User Name** – Used to specify the username using which you want to connect to the SFTP server. The specified user should have any of the following user access roles which are created by the Oracle AMS team:

User Access Role	Description
`<CustomerName>_upload`	Used when you want to upload the files on the SFTP server.
`<CustomerName>_download`	Used when you want to download the files from the SFTP server.

User Access Role	Description
<CustomerName>_config	Used when you want to place the configuration files on the SFTP server.

- **Password** – Note that you must leave this field blank as the user authentication is done using the user's private key.

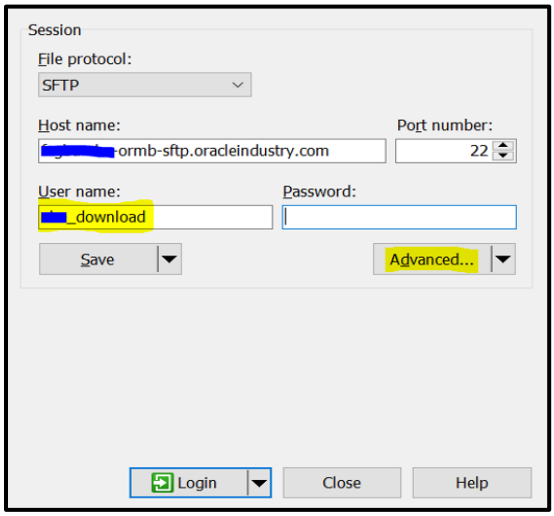

Figure 6: New WinSCP Session Details

4. Click **Advanced**. The **Advanced Site Settings** window appears.

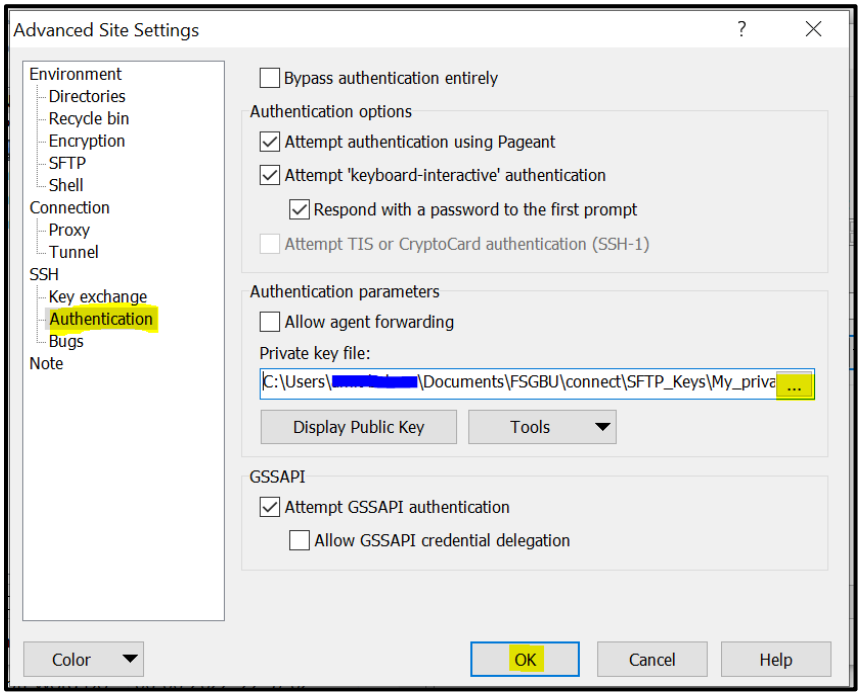

Figure 7: Advanced Site Settings Window

5. In the left pane of the **Advanced Site Settings** window, click the **Authentication** option from the **SSH** node. The authentication related settings appear in the right pane of the **Advanced Site Settings** window.

6. Ensure that the following options are selected in the **Authentication options** section:
   - Attempt authentication using Pageant
   - Attempt 'keyboard-interactive' authentication
   - Respond with a password to the first prompt
7. Do the following in the **Authentication parameters** section:
   a. Click the **Browse** button corresponding to the **Private key file** field.
   b. Browse to the location where you have placed the text file containing the private key.
   c. Select the **My_Private_key.ppk** file and then click **Open**. The private key file name appears (along with the absolute path) in the **Private key file** field.
8. Ensure that the **Attempt GSSAPI authentication** option is selected in the **GSSAPI** section.
9. Click **OK**. The **Login** window appears.

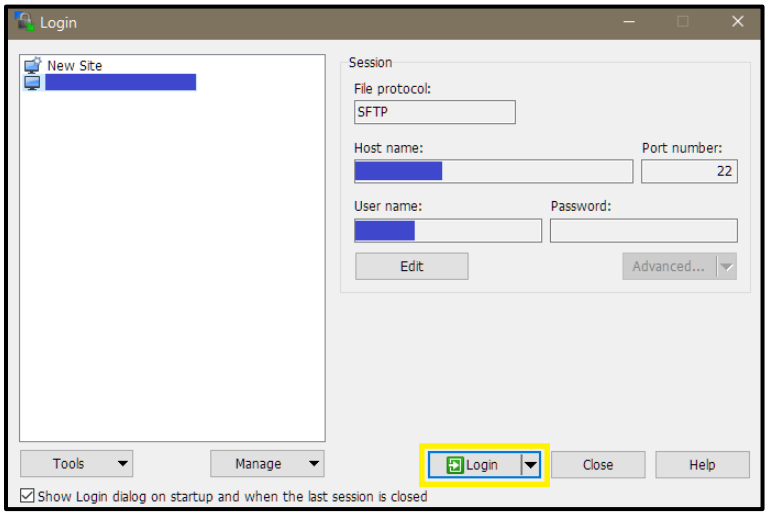

Figure 8: Login Window

10. Click **Login**. A warning message appears while establishing connection to the SFTP server, as shown in the following figure:

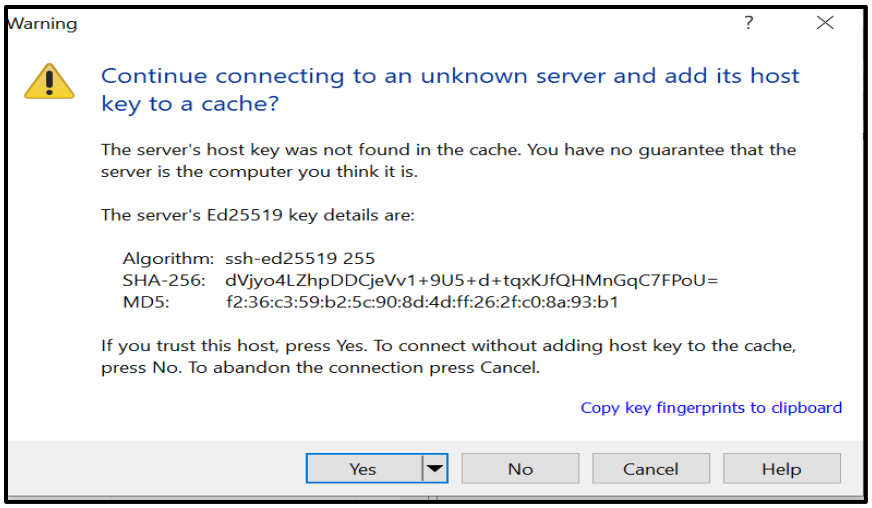

Figure 9: Warning Message

11. Click **Yes** to proceed with the user authentication process. The **Authentication Banner** window appears, as shown in the following figure:

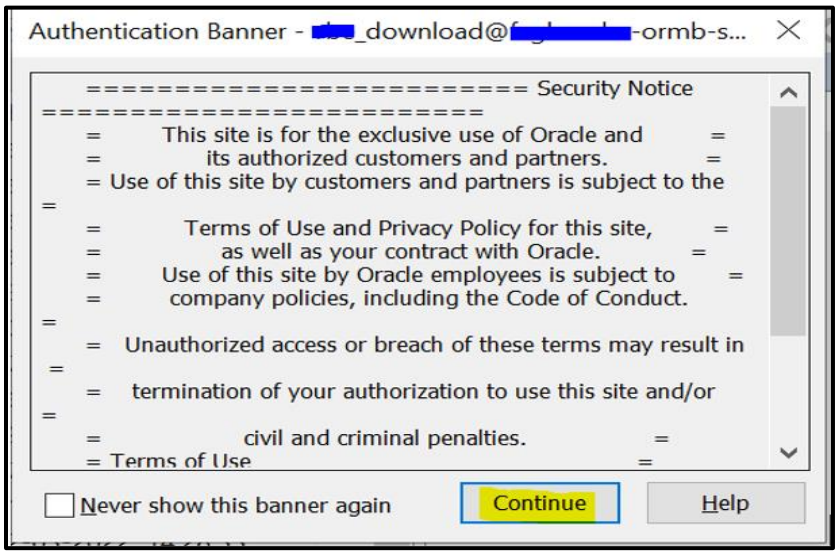

Figure 10: Authentication Banner Window

12. Click **Continue**. On successful user authentication, the SFTP endpoint redirects the authenticated user to the respective directory depending on the user's access role. In this example, the SFTP endpoint redirects the authenticated user to the download directory.

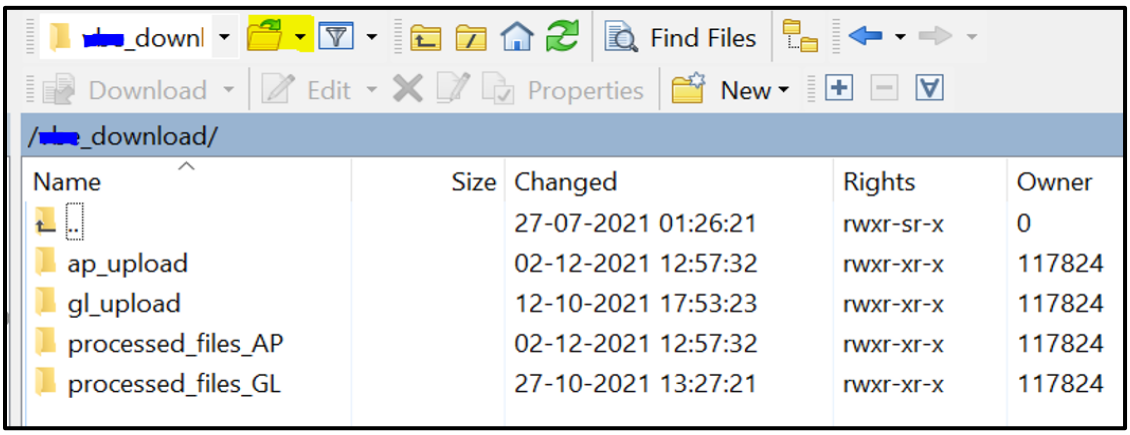

Figure 11: Download Directory

3. Creating Directories on the SFTP Server

To create a directory on the SFTP server:

1. Click the **New** menu in the **Files** toolbar. A menu appears.

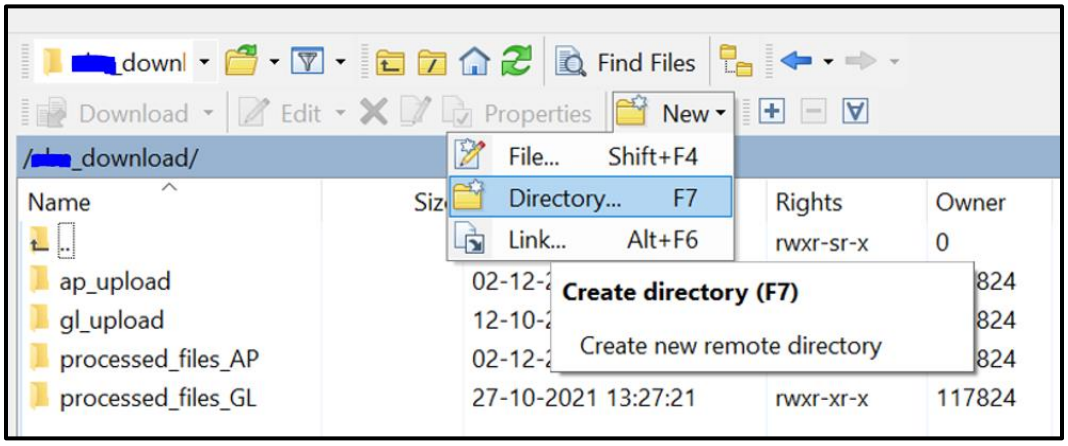

Figure 12: New Menu List

2. Click the **Directory** option from the menu list. The **Create folder** window appears.
3. Enter the folder name in the respective field.
4. Select the **Set permissions** option.
5. Provide the necessary permissions to the folder, as shown in the following figure:

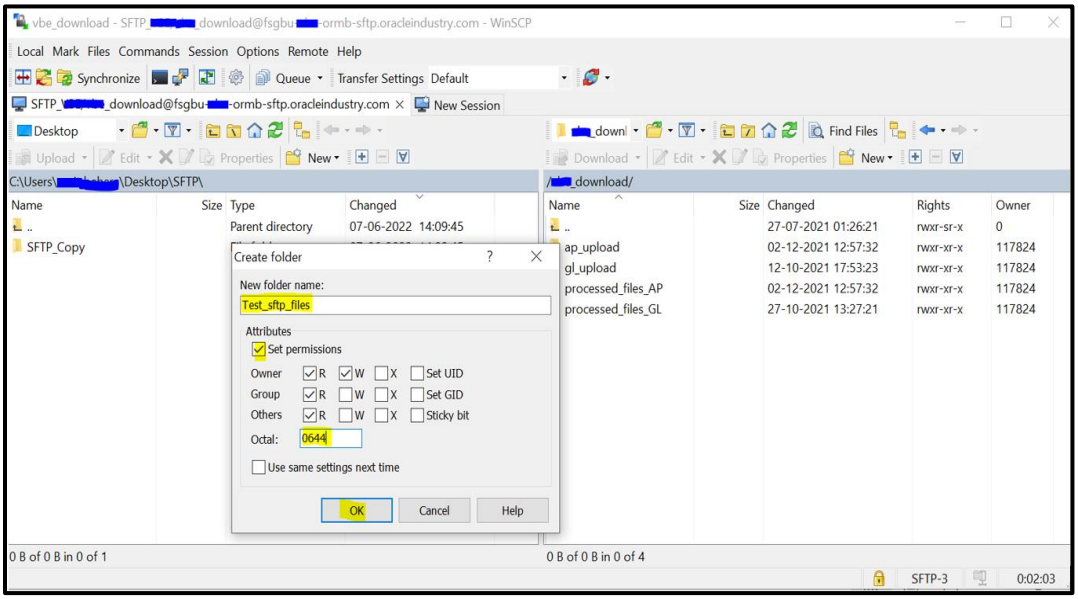

Figure 13: Setting Directory Permissions

6. Click **OK**. The folder is created with the specified permissions.

4. Setting the Recursive Permissions for a Directory

A directory or a folder is defined with a recursive permission when all the files within the folder possess the same set of permissions. By setting recursive permissions, you no longer need to modify the permissions of each file within the folder.

To set the recursive permissions for a directory:

1. Right-click the folder for which you want to set the recursive permissions. A shortcut menu appears.
2. Click the **Properties** option from the shortcut menu, as shown in the following figure:

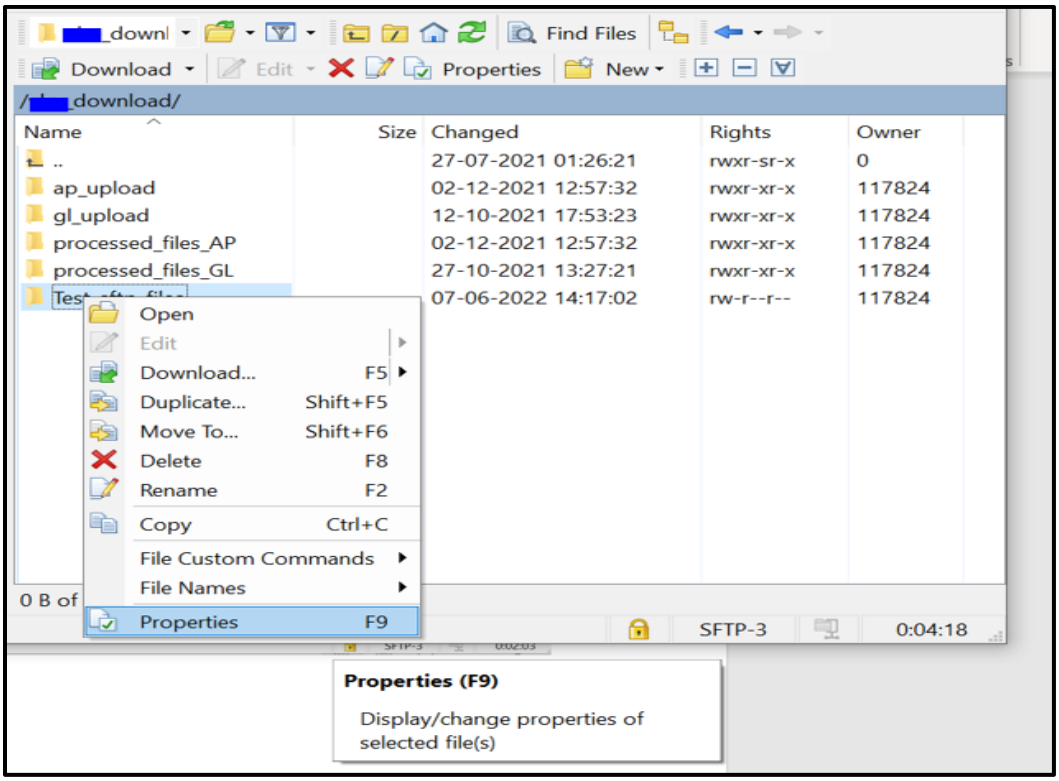

Figure 14: Directory Properties

The **<Directory> Properties** window appears.

3. Do either of the following:
   - Set the required read, write, and execute permissions for the **Owner**, **Group**, and **Others**.
   - Enter `0755` in the **Octal** field. It means that the owner has the read, write, and execute permissions, whereas the group and others have the read and execute permissions.

4. Select the **Set group, owner, and permissions recursively** option to change the permissions of all files and folders within the directory at once.

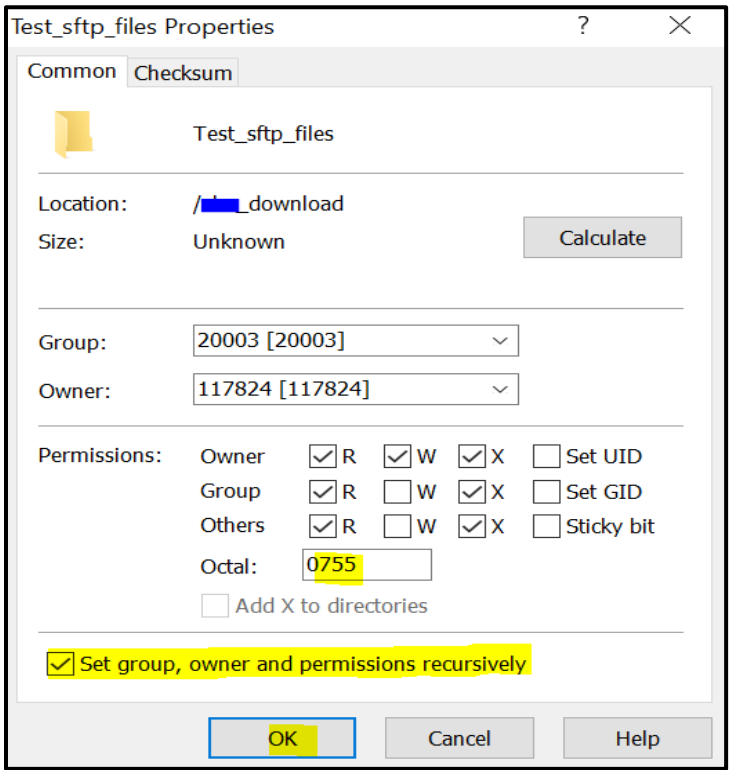

Figure 15: Setting Recursive File Permissions

5. Click **OK**.

5. Setting the Permissions for a File

To set the permissions for a file:

1. Right-click on the file for which you want to set the permissions. A shortcut menu appears.
2. Click the **Properties** option from the shortcut menu. The **<Filename.xxx> Properties** window appears.

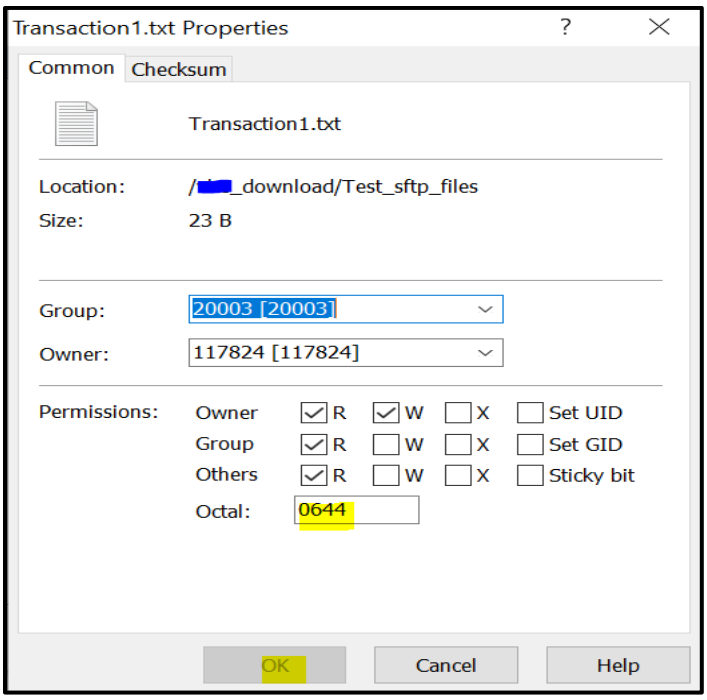

Figure 16: Setting File Permissions

3. Do either of the following:
   - Set the required read and write permissions for the **Owner**, **Group**, and **Others**.
   - Enter `0644` in the **Octal** field. It means that the owner has the read and write permissions, whereas the group and others have the read permission.
4. Click **OK**.

6. Transferring the Files using WinSCP

WinSCP allows you to upload a file or folder from the local machine to the SFTP server and download a file or folder from the SFTP server to the local machine using the drag and drop feature.

To upload a file from the local machine to the SFTP server:

1. Select the file or folder that you want to transfer to the SFTP server from the local machine.
2. Drag and drop the selected file or folder from the left pane (i.e., local machine directory) to the right pane (i.e. SFTP server directory).

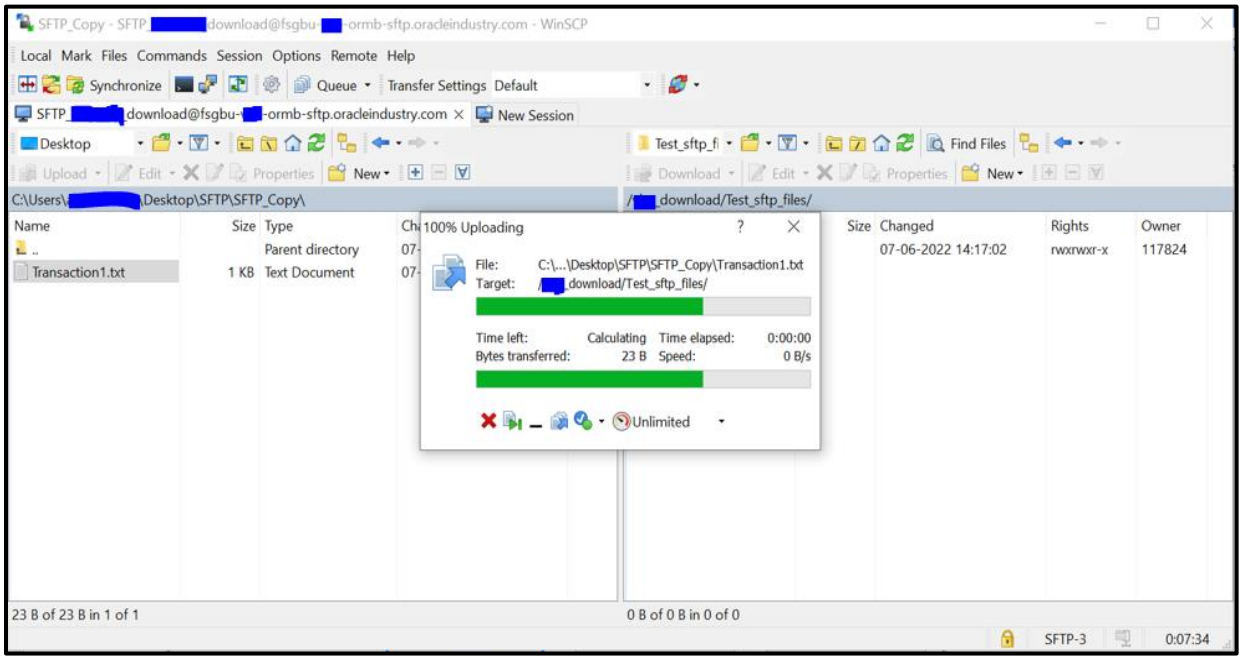

Figure 17: Uploading Files to SFTP Server

Similarly, to download a file from the SFTP server to the local machine:

1. Select the file or folder that you want to transfer to the local machine from the SFTP server.
2. Drag and drop the selected file or folder from the right pane (i.e., SFTP server directory) to the left pane (i.e., local machine directory).