Oracle[®] Revenue Management and Billing Cloud Service

Release 8.1 Patch Set

SFTP Authentication and Access Permissions Guide

Revision 2.0

F74327-01 November 2022



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

F74327-01

Copyright Notice

Copyright © 2014, 2022 Oracle and/or its affiliates. All rights reserved.

Trademark Notice

Oracle, Java, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

License Restrictions Warranty/Consequential Damages Disclaimer

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or de-compilation of this software, unless required by law for interoperability, is prohibited.

Warranty Disclaimer

The information contained herein is subject to change without notice and is not warranted to be errorfree. If you find any errors, please report them to us in writing.

Restricted Rights Notice

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, documentation, and/or technical data delivered to U.S. Government end users are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, documentation, and/or technical data shall be subject to license terms and restrictions as mentioned in Oracle License Agreement, and to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). No other rights are granted to the U.S. Government.

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.

Acronyms

The following acronyms are used in this document:

Acronym	Meaning
ORMB	Oracle Revenue Management and Billing

Acronym	Meaning
SFTP	SSH File Transfer Protocol
SSH	Secure Socket Shell

Contents

1.	SFTP	Authentication	. 1
	1.1	SFTP Authentication Process	. 1
	1.2	Generating SSH Key Pair using PuTTY Key Generator	. 2
	1.3	Submitting the Public Key to Oracle AMS Team	. 5
2.	Acce	ssing the SFTP Server	. 6
3.	Crea	ting Directories on the SFTP Server	10
4.	Setti	ng the Recursive Permissions for a Directory	11
5.	Setti	ng the Permissions for a File	13
6.	Tran	sferring the Files using WinSCP	14

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.

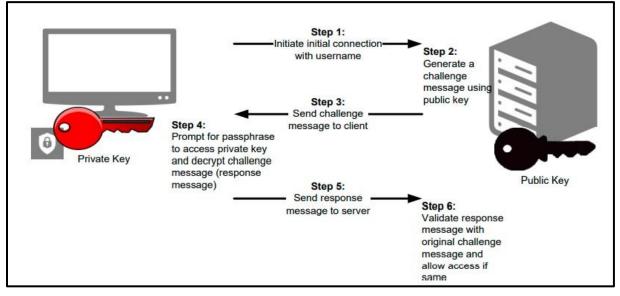


Figure 1: SFTP Authentication Process

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.

New Site		Session		
		File protocol:		
		SFTP 🗸		
		Host name:	P	ort number:
				22 🛓
Import Sites		User name: Pa	assword:	
Import/Restore Configuration				
Export/Backup Configuration Clean Up	0	Save 🗸	Ac	lvanced 🖛
Run Pageant				
Run PuTTYgen				
Check for Updates				
Preferences				
About				
Tools	e 🔻	E Login	Close	Help

Figure 2: WinSCP Login Window

🚰 PuTTY Key Generator		? ×
<u>F</u> ile <u>K</u> ey Con <u>v</u> ersions <u>H</u> elp		
Кеу		
No key.		
Actions		
Generate a public/private key pair		<u>G</u> enerate
Load an existing private key file		Load
Save the generated key	Save p <u>u</u> blic key	<u>S</u> ave private key
Parameters		
Type of key to generate: ● RSA ● DSA	EdD <u>S</u> A) SSH- <u>1</u> (RSA)
Number of <u>b</u> its in a generated key:		2048

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

Figure 3: PuTTY Key Generator Window

 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.

📽 PuTTY Key Generator	? ×				
<u>File K</u> ey Con <u>v</u> ersions <u>H</u> elp					
Key <u>Public key for pasting into OpenSSH authorized keys file:</u>					
sh-rsa AAAAB3NzaC1yc2EAAAADAQABAA +Z0IVLFESnD4ZbAhRVk+9bTjpld0RezVw7sWRa+X0EghrV3J5Flg8G55IREMimlhDCwVlrb2mJJt +B4mNhcdB6A7C3ZEuXcWyw5Bib/GZdKsIEIZiBIHHac4K3b0u23Ce ⁺⁺⁺⁺ ORgq/KDWTkJsFcw95p8bWhqkU hk3hpzS9§ '08YfAw0JK9TcM7b86/ssM9rzP34MuPUQpcezBLJSAnRibpxX1M3zc7oPfFvMcZJNNS0+Ntn					
Key fingerprint: ssh-rsa .					
Key <u>c</u> omment: rsa-key-					
Key passphrase:					
Confirm					
Actions					
Generate a public/private key pair	<u>G</u> enerate				
Load an existing private key file	Load				
Save the generated key Save public key	<u>S</u> ave private key				
Parameters					
Type of key to generate: • <u>R</u> SA • <u>D</u> SA • <u>E</u> CDSA • EdD <u>S</u> A • EdD <u>S</u> A • EdDSA • EdD	○ SSH- <u>1</u> (RSA)				
Number of <u>b</u> its in a generated key:	2048				

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 protected at all times.

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.

NinSCP					\times
Local Mark Files Commands Session	Options Remote Help				
🕀 🕃 🕼 Synchronize	🕸 🗐 Queue 🔹 Transfer Settings Default	• <i></i> •			
Vew Session	1				
👡 E: Data 🔹 📲 🕶 🛐 🔹 🛅	🐛 Login	- 🗆 X	Files 📴 🖛 🔹 🔹		
🗐 🕼 Upload 👻 📝 Edit 👻 💢 🔂 P	😭 New Site	Session	New - + - 🗸		
E:\	sftp.iad.icprod.oracleindustry.com	File protocol:			
Name Size		SFTP V	Rights	Owner	
app ELK mRemoteng NotePad++ oraclehomes Putty sqldeveloper WinSCP Xming	Tools Manage Show Login dialog on startup and when the last set	Host name: Port number: 22 🐨 User name: Password: Save V Advanced V Save October Help ssion is dosed			
0 B of 0 B in 0 of 9			8 8 8 8	Ξ	
0 B of 0 B in 0 of 9 Not connected.	3	3 hidden			

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</customername>	Used when you want to upload the files on the SFTP server.
<customername>_download</customername>	Used when you want to download the files from the SFTP server.

User Access Role	Description
<customername>_config</customername>	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.

Session <u>F</u> ile protocol:		
SFTP	\sim	
<u>H</u> ost name:		Po <u>r</u> t number:
ormb-sftp.	oracleindustry.com	22 🜩
User name:	Passw	ord:
download		
<u>S</u> ave		Advanced
	•	
E Log	gin ▼ (Close Help

Figure 6: New WinSCP Session Details

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

Advanced Site Settings		?	×
Environment Directories Recycle bin Encryption SFTP Shell Connection Proxy Tunnel SSH Key exchange Authentication Bugs Note	Bypass authentication entirely Authentication options Attempt authentication using Pageant Attempt authentication using Pageant Attempt authentication using Pageant Attempt keyboard-interactive' authentication Respond with a password to the first prompt Attempt TIS or CryptoCard authentication (SSH-1) Authentication parameters Allow agent forwarding Private key file: [C:\Users\	My_priva	
Color 🔻	OK Cancel	He	lp

Figure 7: Advanced Site Settings Window

 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.

🔁 Login		- 🗆 X
New Site	Session File protocol: SFTP Host name:	Port number:
	User name: Passwo	22
Tools Manage		lose Help
Show Login dialog on startup and when the		neip

Figure 8: Login Window

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

Warning	? ×
	Continue connecting to an unknown server and add its host key to a cache?
	The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is.
	The server's Ed25519 key details are:
	Algorithm: ssh-ed25519 255 SHA-256: dVjyo4LZhpDDCjeVv1+9U5+d+tqxKJfQHMnGqC7FPoU= MD5: f2:36:c3:59:b2:5c:90:8d:4d:ff:26:2f:c0:8a:93:b1
	If you trust this host, press Yes. To connect without adding host key to the cache, press No. To abandon the connection press Cancel.
	Copy key fingerprints to clipboard
	Yes Ves No Cancel Help

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:

Authentication Banner - 🔜_download@🚘 📩 ormb-s	\times
======================================	~
= This site is for the exclusive use of Oracle and =	
= its authorized customers and partners.	
= Use of this site by customers and partners is subject to the	
=	
= Terms of Use and Privacy Policy for this site, =	
as well as your contract with Oracle.	
= Use of this site by Oracle employees is subject to =	
= company policies, including the Code of Conduct.	
Unauthorized access or breach of these terms may result in	
termination of your authorization to use this site and/or	
=	
= civil and criminal penalties. = = Terms of Use =	\sim
= rema or oae =	
Never show this banner again Continue Help	

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.

📕 📩 _downl 👻 🚰 👻] - 🖬 🔽 🕯	🞧 쥗 🖻 Find Files			
📱 📄 Download 👻 📝 Edit 👻 💢 🖓 🕞 Properties 🚰 New 🕶 📳 🖃 🗹					
/==_download/					
Name	Size	Changed	Rights	Owner	
		27-07-2021 01:26:21	rwxr-sr-x	0	
📕 ap_upload		02-12-2021 12:57:32	rwxr-xr-x	117824	
📕 gl_upload		12-10-2021 17:53:23	rwxr-xr-x	117824	
processed_files_AP		02-12-2021 12:57:32	rwxr-xr-x	117824	
processed_files_GL		27-10-2021 13:27:21	rwxr-xr-x	117824	

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.

📕 📩 downl 🝷 🚰 👻 🕎	🔹 🔽 🏠 🎜 🚺 Find Files 🗧 🖛 🕶 🗸
📄 Download 🝷 📝 Edit	🗡 📝 🕞 Properties 🎬 New 🕶 🖃 🗹
/download/	File Shift+F4
Name	Siz Directory F7 Rights Owner Link Alt+F6 rwxr-sr-x 0
ap_upload gl_upload processed_files_AP	02-12-2 Create directory (F7) 824 12-10-2 Create new remote directory 824 02-12-2 Create new remote directory 824
processed_files_GL	27-10-2021 13:27:21 rwxr-xr-x 117824

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:

🔩 vbe_download - SFTP_	download@fsgbu	industry.com - WinSCP					×
🕀 🎇 🔯 Synchronize 🗾 🗊	: Session Options Remote Help P 💽 🍥 🎒 Queue 🔹 Transfer Settin sqbu : -ormb-sftp.oracleindustry.com ×		• 💋 •				
Desktop 🔹 🚰 🗸 🍸] • ■ 🔁 😭 🌮 🔚 🖛 • → •			 Image: Second sec			
Name	Size Type Changed Parent directory 07-06-2022 Create folder New folder name: Test_sftp_files Attributes ØS est permissions Owner R Group R W X	×	Name a_upload gl_upload processed_files_AP processed_files_GL	Size Changed 27-07-2021 01:26:21 02-12-2021 12:57:32 12-10-2021 17:53:23 02-12-2021 12:57:32 27-10-2021 13:27:21	Rights NVXT-ST-X NVXT-XT-X NVXT-XT-X NVXT-XT-X NVXT-XT-X	Owner 0 117824 117824 117824	
0 B of 0 B in 0 of 1			0 B of 0 B in 0 of 4	ß	SFTP-3	0:02	:03

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:

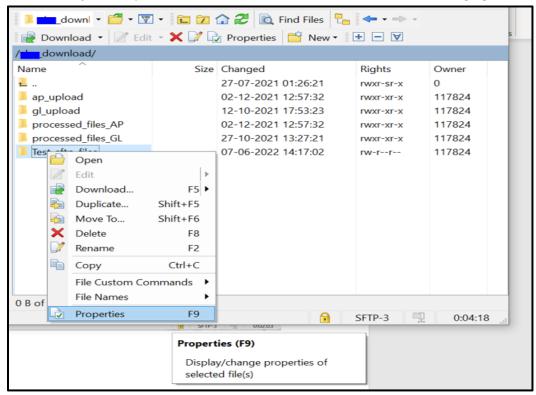


Figure 14: Directory Properties

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.

Test_sftp_files P	roperties	? ×			
Common Chec	ksum				
	Test_sftp_files				
Location:	/download				
Size:	Unknown	Calculate			
Group:	20003 [20003] ~]			
Owner:	117824 [117824] ~]			
Permissions:	Owner \bigtriangledown R \checkmark W \checkmark XGroup \bigtriangledown R \bigcirc W \checkmark XOthers \bigtriangledown R \bigcirc W \checkmark X	Set UID Set GID Sticky bit			
	Octal: 0755				
	Add X to directories				
Set group, owner and permissions recursively					
	OK Cancel	Help			

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.

Transaction1.txt	Properties	?	\times
Common Chee	cksum		
	Transaction1.txt		
Location:	/		
Size:	23 B		
Group: Owner: Permissions:	20003 [20003] ✓ 117824 [117824] ✓ Owner ✓ R ✓ W ✓ X Group ✓ R ✓ W ✓ X	Set UID	_
	Others R W X Octal: 0644	Sticky bit	t
	OK Cancel	Hel	р

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).

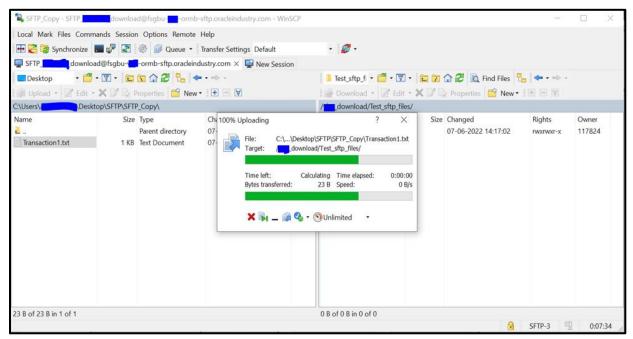


Figure 17: Uploading Files to SFTP Server

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).