

Oracle Financial Services Revenue Management and Billing Cloud Service

sftp Authentication

ORACLE WHITE PAPER | JANUARY 2016



Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.



Table of Contents

Disclaimer	1
Introduction	1
Authentication Overview	1
Establishing Authentication	2
Generate Public/Private Key Pair	2
Step 1 – open puttygen.exe	2
Step 2: Generate keys.	4
Step 3: Save private key	4
Step 4: Save public key to text file	4
Submit public key to Oracle	6
Logging on with Key Based Authentication	6
Windows - WinSCP	6
References	7

.

Introduction

This document outlines how to establish authentication with the sftp hosts in the ORMB cloud service using keys.

Authentication Overview

Authentication is based on a public and private key being generated. The public key is placed on the server, while the private key remains in a secure location on the client computer. These public/private keys use asymmetric cryptography to establish the clients identity.



Summary of ssh key based authentication.

When using Key based Authentication the following occurs:

- » An initial connection is made by the client providing the username and request to authenticate using keys.
- » The sftp server (sshd) takes the public key for that user and constructs a message based on the public key. This message (or challenge) is returned to the sftp client.
- » The client locates the local private key and prompts for a passphrase to access to local key (when necessary).
- » The client then generates a response to the challenge message using the private key. This response is sent to the sever.
- » The server takes the message response and validates it using the public key and grants access.

Establishing Authentication

Generate Public/Private Key Pair

Use puttygen.exe to generate the public private key pair. From WinSCP there is a menu item to for PuttyGen under the Tools menu as shown here:

Standard WinSCP Login		X
New Site	Session File protocol: SFTP Host name:	Port number:
Import Sites	_ <u>U</u> ser name:	Password:
Import/Restore Configuration Export/Backup Configuration Clean Up	Save V	A <u>d</u> vanced ▼
Run Pageant	-	
Run PuTTYgen		
Check for Updates		
Preferences About		
Tools	Login 🗸	Close Help

Step 1 - open puttygen.exe

le Key Convers	ions Help		
Kev			
No key.			
-			
Actions			
Actions	And a law and		Connets
Actions Generate a public/p	rivate key pair		Generate
Actions Generate a public/p Load an existing priv	rivate key pair vate key file		Generate Load
Actions Generate a public/p Load an existing priv Save the generated	rivate key pair vate key file key	Save public key	Generate Load Save private key
Actions Generate a public/p Load an existing priv Save the generated Parameters	rivate key pair vate key file key	Save public key	Generate Load Save private key
Actions Generate a public/p Load an existing priv Save the generated Parameters Type of key to gene © SSH-1 (RSA)	rivate key pair vate key file key rate:	Save public key	Generate Load Save private key

Select options

- » Type of key generate : SSH-2 RSA
- » Number of bits in a generated key: 2048

File Key Conversions Help Key No key.	
Actions Generate a public/private key pair	Generate
Actions Generate a public/private key pair Load an existing private key file	Generate
Actions Generate a public/private key pair Load an existing private key file Save the generated key	Generate Load Save public key Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters	Generate Load Save public key Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters Type of key to generate: SSH-1 (RSA)	Generate Load Save public key Save private key

Step 2: Generate keys.

Click on the Generate button and move the mouse as directed until the keys are generated.

Assign a comment to the key so that it can be identified.

Step 3: Save private key

Once the keys are generated – save the private key to a secure location, assigning a pass phrase. While assigning a passphrase is not required it is strongly recommended. This passphrase will be required to subsequently access the private key.

Important: It is critically important that the private key file is secured and protected at all times.

Step 4: Save public key to text file

Using the button "Save public key" saves the key in the incorrect format, a better way is to copy the public key text and from the puttygen screen and paste it into a text file to save it.

Specifically copy text from the top of the puttygen screen:

😴 PuTTY Key Generator	? 💌						
File Key Conversions Help							
Key							
Public key for pasting into OpenSSH authorized_keys file:							
1Ro46iZexes/1WeePer/98Z/Uwsjv1I	IZ172§dmJdXWH84uUAgLv5m7l496vSdgrYXPQ						
Yx9bxqeUdNz0M1A4/x9iuAZba41G4E zBCWt17.55(5555); 2mpUsWEEQ.	DaOFT2LYymEJy1+zetP9Blz3czA3VS9kPPXra94						
Key fingemeint	Undo						
Rey Ingerphini. sshi'sa zu	Cut						
Key comment:	Сору						
Key passphrase:	Paste						
Confirm passphrase:	Delete						
Actions							
Concerto o public (oriusto key pois	Select All						
Generate a public/private key pair	Right to left Reading order						
Load an existing private key file	Show Unicode control characters						
Save the generated key	Insert Unicode control character						
Parameters							
Type of key to generate: SSH-1 (RSA)							
Number of bits in a generated key:	2048						

And paste it in a text file.

ĺ	 Uı	ntitled	- Notepa	d						_	_	
	File	Edit	Format	View	Help							
	ssh-	•rsa	AAAAB3	NzaC1	yc2eaaaab	JQAAAQEA2ł	<bxdw1< th=""><th>Ронтh0h9q</th><th>Rx1H97</th><th>′FjuP6∟si5 </th><th>bhtRbv1Ro4</th><th>6izcxım2w</th></bxdw1<>	Ронтh0h9q	Rx1H97	′FjuP6∟si5	bhtRbv1Ro4	6izcxım2w

Save this text file containing the public key.

Tip: You may save the file with any extension, but ".pub" is a useful convention to indicate that this is a public key.

Once finished you should have two files, a file containing the private key and a file containing the public key.

The private key remains in your possession, and the public key is sent to Oracle so that it can use it for authentication of the sftp service.

Submit public key to Oracle

Raise a service request with Oracle Global Support and attach the public key file **only**. Identify both the user and environment you would like to use this public key to establish an authenticated session. The user should already have been created by Oracle and a temporary password provided. This key pair will replace the password authentication.

Oracle will take the public key and associate it with the relevant user on the relevant environment, updating the service request when done.

Logging on with Key Based Authentication

Windows - WinSCP

There are multiple sftp clients available and you will need to consult the documentation of the sftp client you are using to understand the syntax of how to refer to the private key when connecting.

As an example – using WinSCP, create a new site – entering the hostname and port. Then under Advanced>Authentication set path and filename of the private key as shown in screen shot.

	MinSCP Login		
Advanced Site Settings	Bypass authentication entirely (SSH-2) Authentication options Attempt authentication using Pageant Attempt TIS or CryptoCard authentication (SSH-1) Attempt TIS or CryptoCard authentication (SSH-2) Respond with password to the first prompt Authentication parameters Allow agent forwarding Private key file: The first first (test_private_key.ppk SSAPI Attempt GSSAPI authentication (SSH-2) Allow GSSAPI credential delegation OK Cancel Help	Session Elle protocol: SFTP Host name: I too to be operating to one the pacement User name: Dasword: Save Cancel	Port number: 22 🛋

Finally enter the User name – which is the same username you requested the public key to be associated with when sending the public key to Oracle, and leave the password blank.

Click Save, then Login and an authenticated session should be established.

If you put a pass phrase on your local private key, you will be prompted to enter that so that WinSCP can open the private key file.

References

https://docs.oracle.com/cloud/latest/dbcs_dbaas/CSDBI/GUID-4285B8CF-A228-4B89-9552-FE6446B5A673.htm#CSDBI3349



CONNECT WITH US

B blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

f

Oracle Corporation, World Headquarters 500 Oracle Parkway Redwood Shores, CA 94065, USA Worldwide Inquiries Phone: +1.650.506.7000 Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle 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. 0116

sftp Autentication Overview January 2016 Author: FSGBU