CUSTOMER

Sharing Private Keys

Typographic Conventions

Type Style	Description
Example	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Textual cross-references to other documents.
Example	Emphasized words or expressions.
`EXAMPLE`	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE`	Keys on the keyboard, for example, `F2` or `ENTER`.

Document History

Version	Date	Change
1.0	< 2015-09-01>	Created Sharing Private Keys

Contents

1 Document Purpose

There is a requirement to add the customer-specific security artifacts (for instance XML signature, key pair) into the key store of the customer tenant. Since customers do not have authorization to update this by themselves, they have to raise a request to SAP cloud support to trigger these steps.

This document outlines the steps to the customer has to perform to share this private key file to the SAP cloud support.

2 Important Notes

The SFTP account created for sharing your security artifacts will be active only for 5 working days.

The password corresponding to security artifacts should never be shared in the SFTP account or in the ticket. It should always be shared via mail / preferably encrypted e-mail.

Once the security artifacts password E-Mail is sent to sap_hci_saas_administrator@sap.com mailbox, you will have to send back the ticket to SAP cloud support for further processing.

3 Steps to Upload Security Artifacts to SAP SFTP Server and Send Its Password

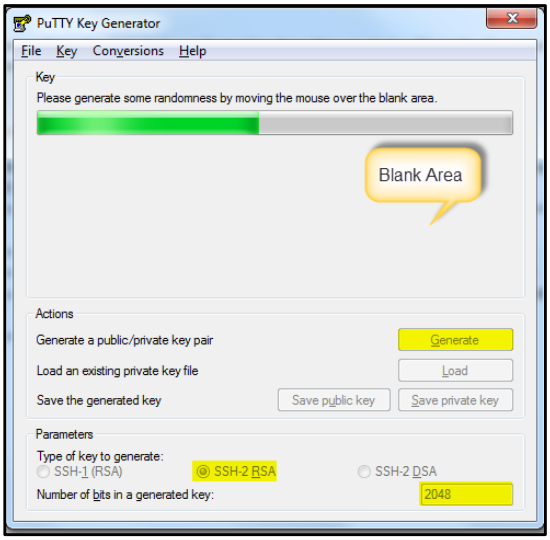
- Create SSH Keypair (private & public) to connect to SAP SFTP server
- Share the Public SSH Key to SAP
- Logon to the SAP SFTP Server using SSH private key
- Upload the security artifacts to SAP SFTP Server
- Send password of the security artifacts via Encrypted/Unencrypted email to SAP

3.1 Create SSH Keypair (private & public) to connect to SAP SFTP server

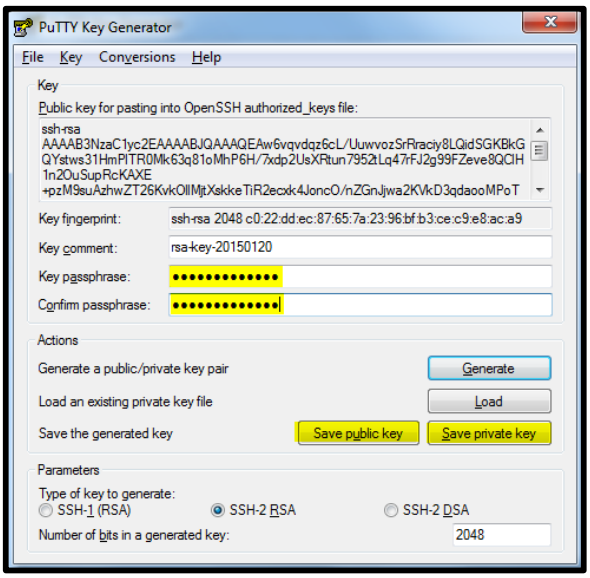
1. Open the PuttyGen tool.
2. Select '*Type of key to generate*' value as '*SSH-2 RSA*'.
3. Enter '*Number of bits in a generated key*:' value as **2048**.

> **Note**
>
> You can see the steps to download and install PuttyGen in Appendix.

4. Once the values are maintained, select *Generate*.
5. Move the mouse pointer over the 'blank area' to generate the key pair.



6. Once the key is generated, enter the passphrase and select *Save private key* to save the SSH-2 private key in .ppk format. Also, save the public key by selecting *Save public key* in `.txt` format.
7. Make sure that the private key and its password, which are generated above, are kept safe as they are required to connect & access the SFTP account.



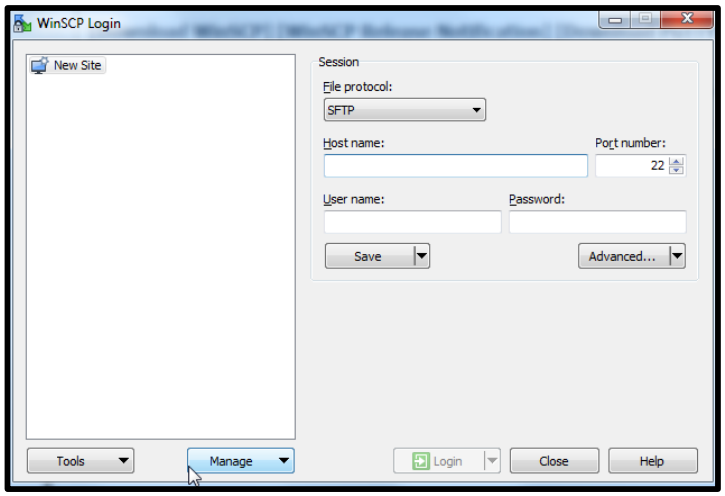
3.2 Share the Public SSH Key Pair with SAP

Attach the SSH-2 public key generated (refer to step 6 of section 3.1) in the request created to SAP cloud support.

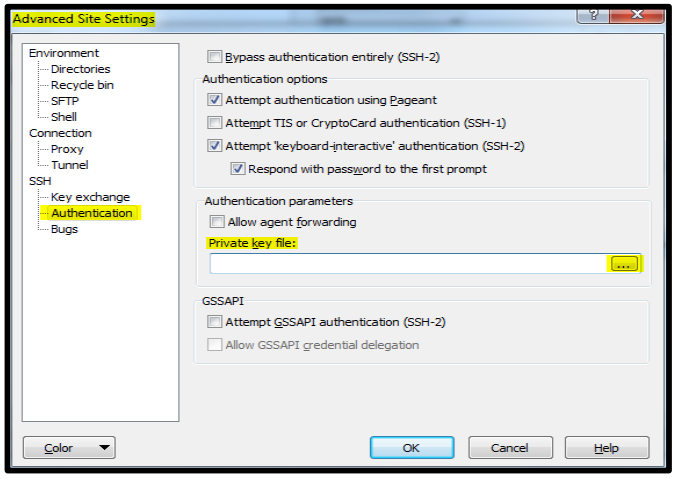
3.3 Logon to the SAP SFTP Server using Private SSH Key Pair

1. Open the WinSCP application from where it is installed.

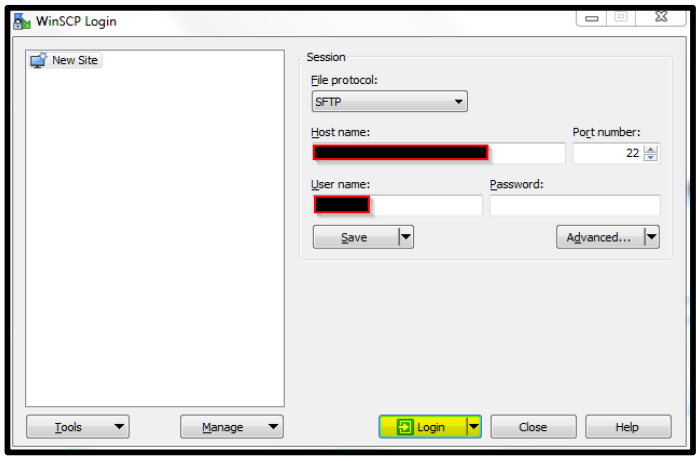
> **Note**
>
> You can find the WinSCP installation procedure in Appendix.



2. Fill in the *Host name* and *User name* values shared by SAP cloud support.
3. Choose *Advanced*.
4. In the *Advanced Site Settings* window, select the *Authentication* option.
5. On the right side pane, select Private Key file option to select the .ppk file which was generated (refer to step 6 of section 3.1).



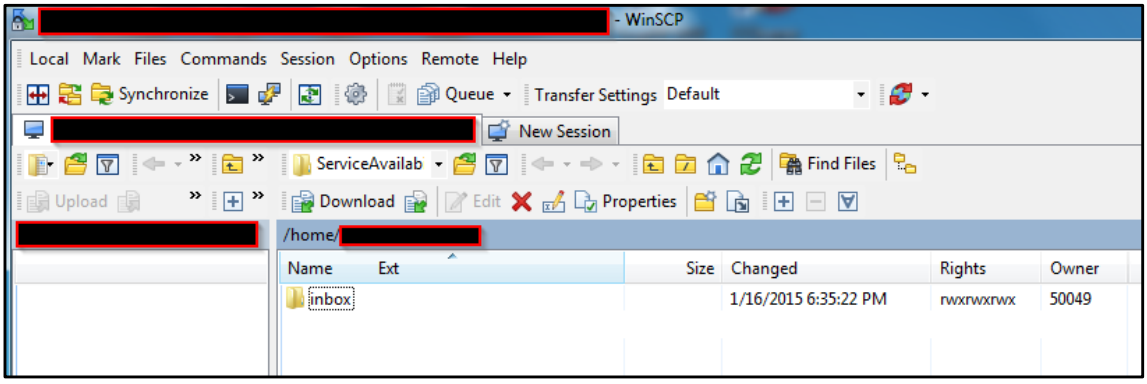
6. Once the private key file (.ppk) is selected, select *OK* to save the settings maintained.
7. Choose *Login* to initiate connection to the SFTP account.



8. The tool prompts for the password to continue, where the SSH2 private key file password need to be entered (refer to step 6 of section 3.1). Then continue to login to the SFTP account.

3.4 Upload the security artifacts to SAP SFTP Server

Once the login is successful, the interface looks as shown below. Open the 'inbox' folder from the tool and place the security artifacts into that. Also, ensure that the complete file is transferred.



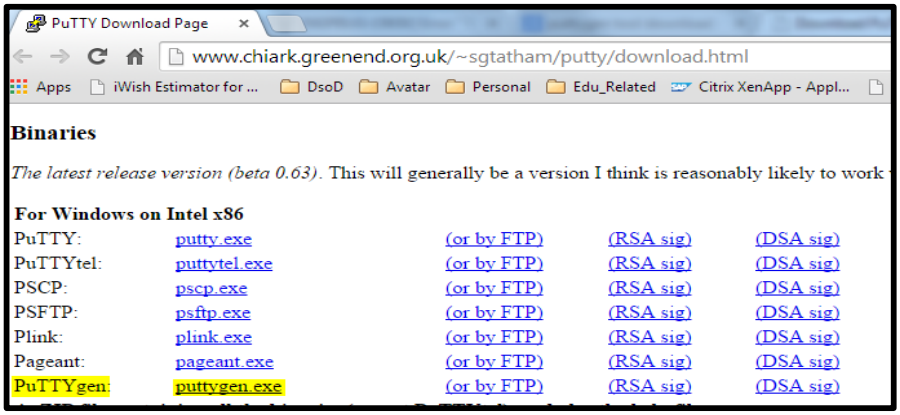
3.5 Send password of the security artifacts via Encrypted/Unencrypted email to SAP

The password of the security artifacts should be sent via email to sap_hci_saas_administrator@sap.com. If possible, the mail is to be encrypted using PGP.

4 Appendix

4.1 PuttyGen Installation Procedure

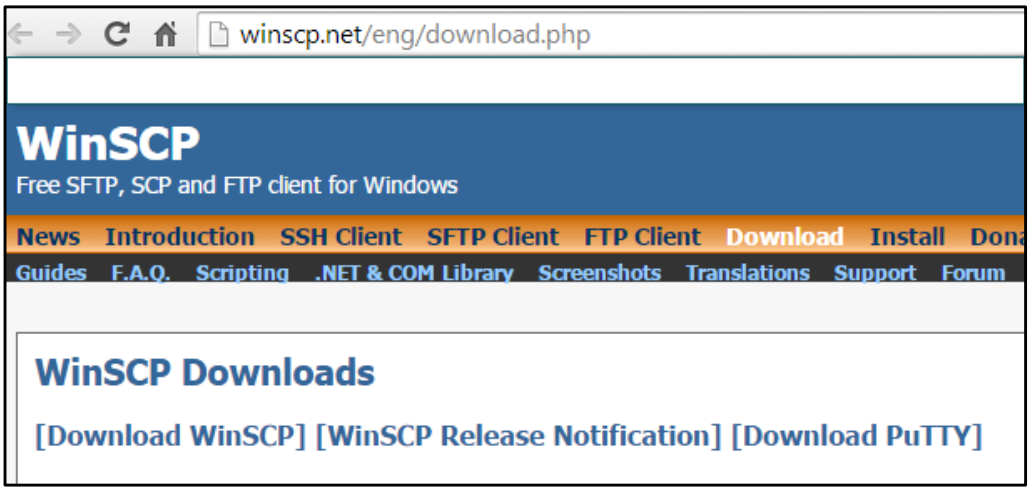
1. You can download the installation file from this URL.
   http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

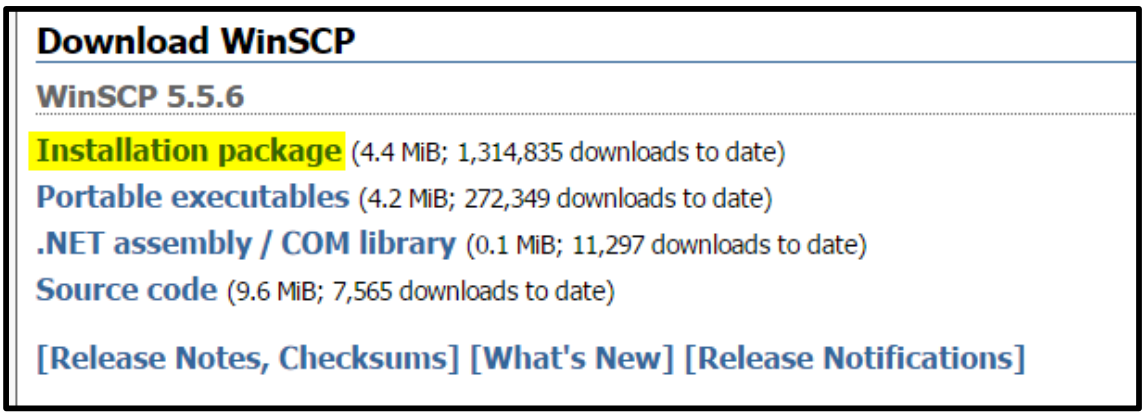


2. Once the 'puttygen.exe' file is downloaded, open the file to access the tool. No further installation need to done.

4.2 WinSCP Installation Procedure

You can download the installation file from http://winscp.net/eng/download.php





Once the installation packages are downloaded, open the exe file and proceed with normal setup procedure. This tool should be installed locally in the system from where the SFTP user account needs to be accessed.

www.sap.com/contactsap

Material Number: