Australian Government | acma

Australian Communications and Media Authority

communicating | facilitating | regulating

DO NOT CALL REGISTER

AUTOMATED WASHING SERVICE FACT SHEET

This fact sheet provides instructions on how Access-seekers can connect to Do Not Call Register's SFTP server and utilise the Automated Washing Service. **Please note that no support will be provided on third-party tools/utilities.**

Prerequisites

Access-seekers can authenticate using Username and Password combination or Username and SSH key combination.

Please refer to the document titled " Do Not Call Register - SSH Key Authentication" for instructions on how to generate SSH keys. The saved Public Key needs to be provided to the Do Not Call Register to be associated with the Access-seeker account before successful connection can be made.

Connecting to the SFTP Server

Connecting from a Linux machine

1. Connect to the sFTP Server:

   Hostname: sftp.donotcall.gov.au

   Username: <your current username>

   Password: <your password> (only if you are not using SSH Keys)

   Example:

```
salmat@ubuntu:~$ sftp 00000@sftp.donotcall.gov.au
The authenticity of host 'sftp.donotcall.gov.au (180.92.221.211)' can't be established.
RSA key fingerprint is 2d:02:bd:50:0e:c5:c3:33:5e:fe:bb:40:ec:74:f0:71.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'sftp.donotcall.gov.au,180.92.221.211' (RSA) to the list of known hosts.
```

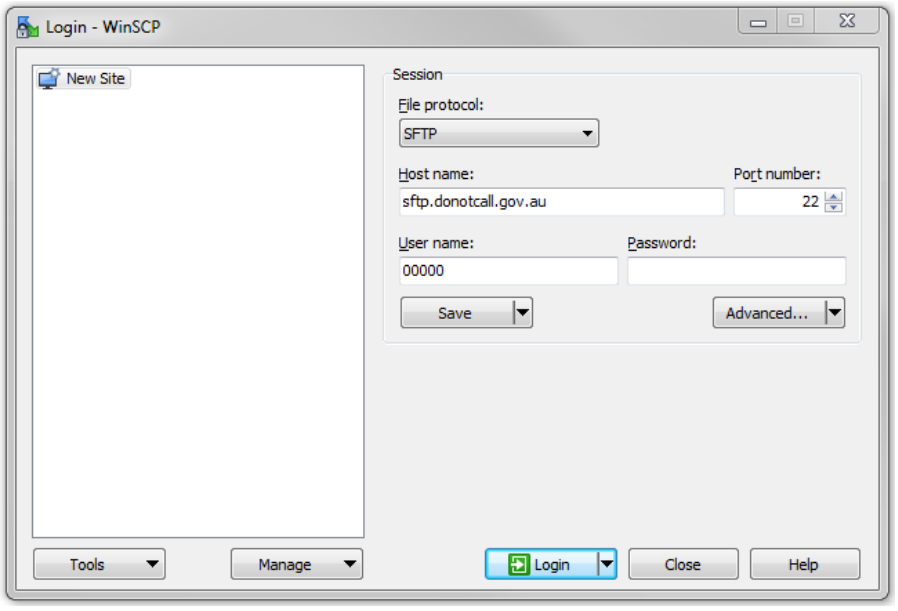
```
00000@sftp.donotcall.gov.au's password:
  Connected to sftp.donotcall.gov.au.
  sftp> dir
  archive   download  upload
  sftp>
```

Connecting from a Windows machine using WinSCP

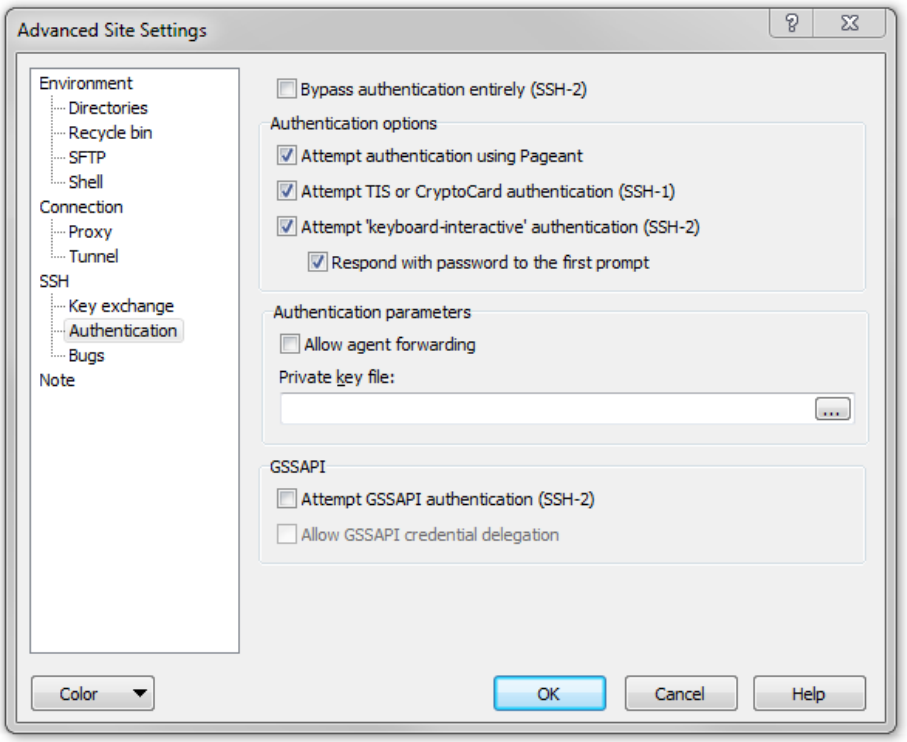
1. Open **WinSCP**. Key in **HOSTNAME** (sftp.donotcall.gov.au) and **USERNAME** (Telemarketer ID).

If you are **not using SSH Keys**, **type also** your **Password** and **click** on **Login** and **go to step 8**.

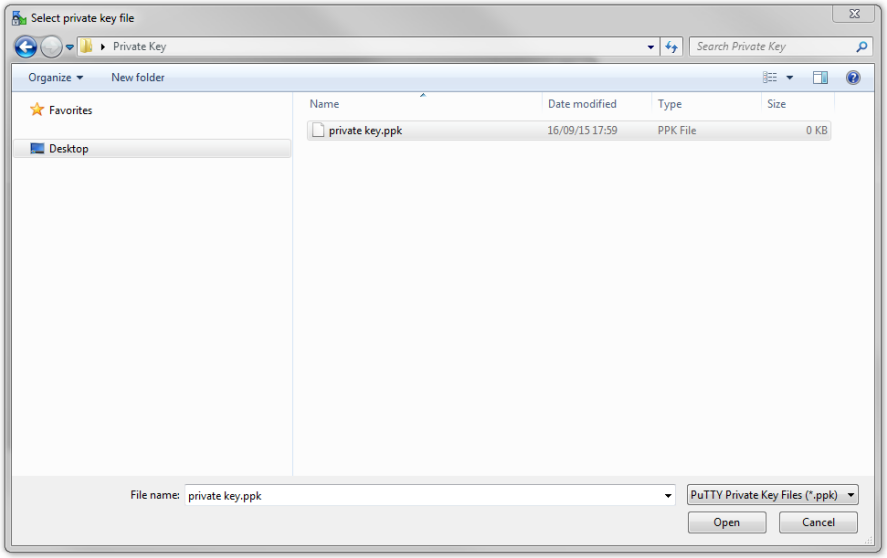
2. Click on the **Advanced** button



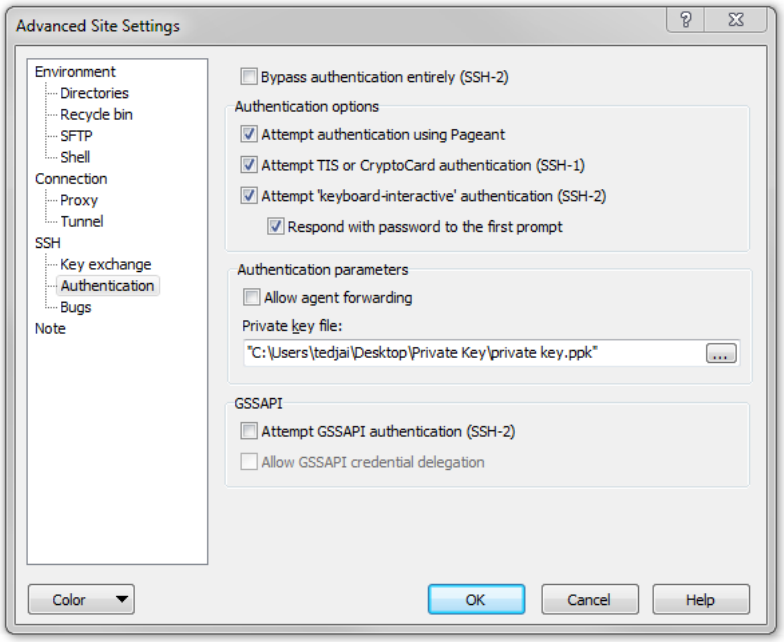
3. and select Authentication:



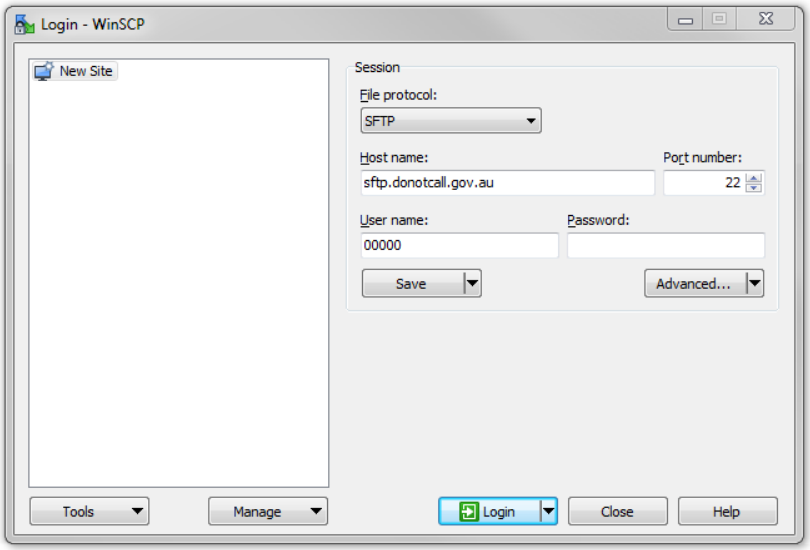
4. Click on the "…" button and select the PRIVATE KEY to use.



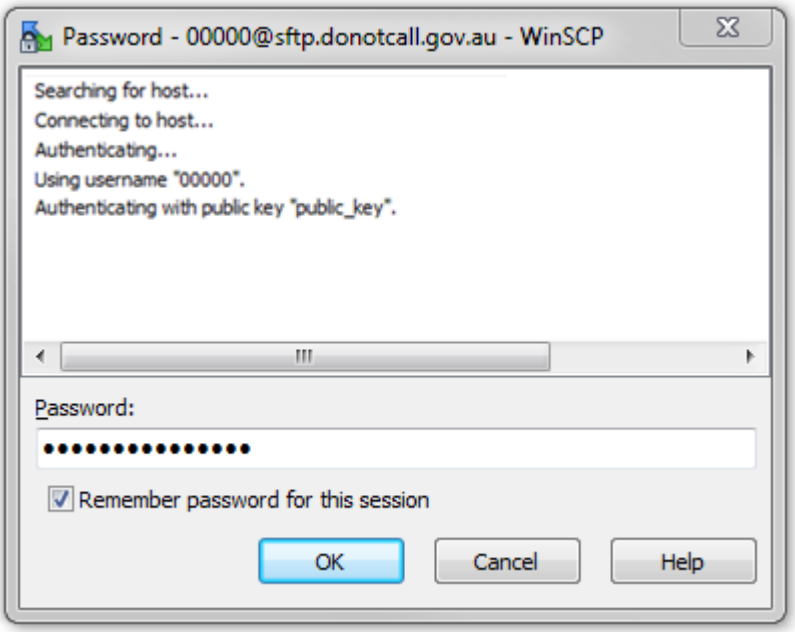
5. Once the private key file is selected, click the OK button.



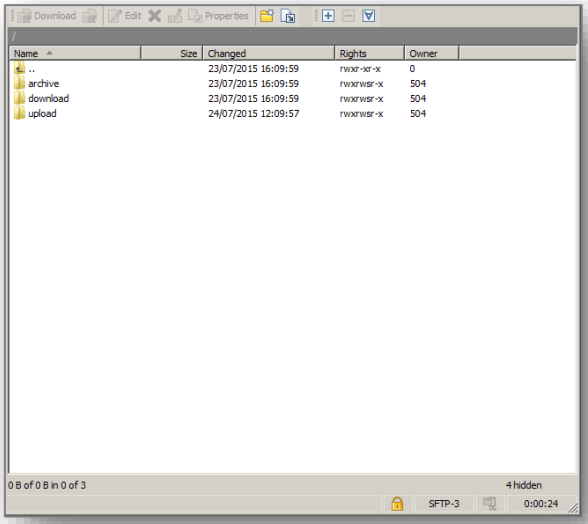
6. Click the Login button.



7. Enter the Password and click OK



8. The site structure will look as follows:

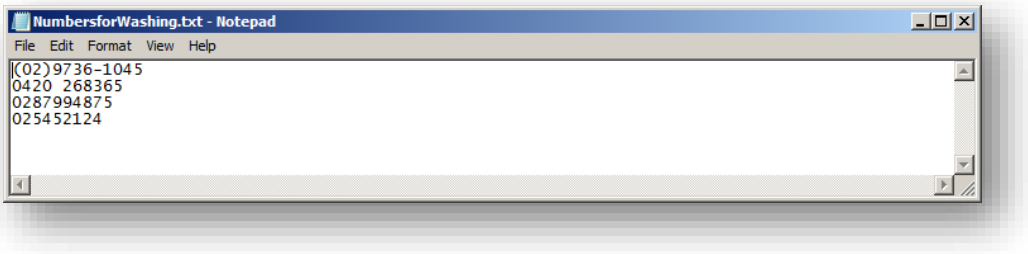


Upload and wash numbers

1. Upload the **Data file to be washed** to the **/public/upload** directory once logged in.
    - **File Name:** alphanumeric with no spaces
    - **Data File Extension:** .DAT, .TXT or .CSV
    - **Compressed file format**: .ZIP or .GZ
    - **Content**:
        - The .DAT file must be in a plain text CSV format
        - The .DAT file must contain only a single column of the numbers to be washed
        - Column headers can be included, but will be counted and rejected as not being a valid number
        - The number column must be no greater than 30 characters (including any leading or trailing spaces)
        - Each record (or row) must be on a separate line
        - Allowable characters for the number column are:
            - Numbers 0 through 9
            - Brackets "(" and ")"
            - Dashes or hyphens
            - Spaces
        - Numbers must be in ten digit format (once formatting characters have been removed), with the first character commencing with a 0 (zero)

If files are submitted in a compressed format, the resulting files will be returned in the same format.

Data File Example

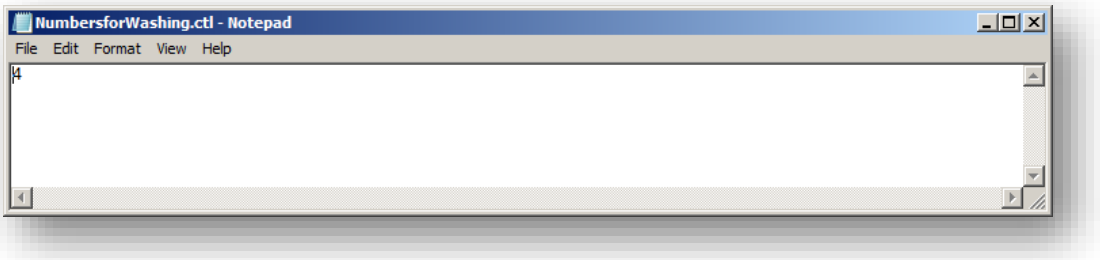


2. Once the data file is uploaded then upload the **Control of the Data file** to **upload** directory as well.
    - **File Name**: <same data file name>
    - **Control File Extension**: .CTL
    - **File Content:**
        - The .CTL file must be in a plain text format
        - The contents of the .CTL must consist of a single record, which equates to the number of records in the associated .DAT file

---

The .CTL file should not be compressed.

Control File Example



Errors

Should any errors occur an error file will be generated and placed in the ***/root/public/download*** directory.

Error File

Error File Name: *[transaction_number]_[yyyymmdd][hhmmss]_orig_[uploaded_filename]*

Error File Extension: .ERR

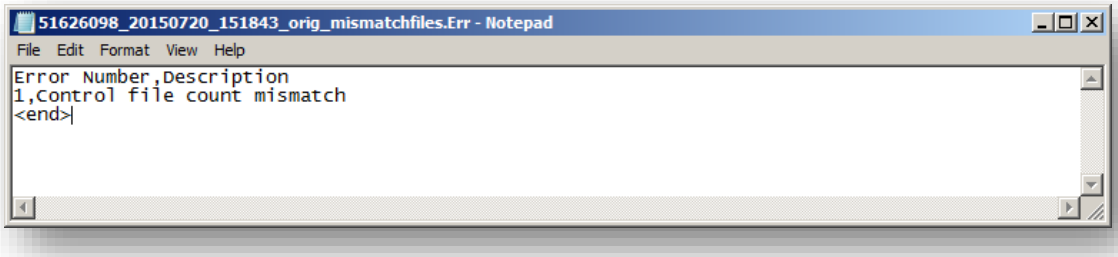
Error File Content: This file will be in plain text CSV format containing two columns: Error Number and Error Description separated by comma.

Error Codes:

Error Code	Description
0001	Control file count mismatch
0002	Unable to read/open control file
0003	Missing DAT file for CTL file
0004	Unable to read DAT file
0005	No subscription level selected
0006	TAP subscription expired
0007	TAP account suspended
9999	Other error

Both the original **Data file and the Control file** will be copied to the root/public/**archive** directory.

Error File Example:



Other Information

Connectivity

Access-seekers should ensure they are able to reach the Do Not Call Register's SFTP servers at the following IP addresses on port 22:

- 180.92.221.211 (Production)

  -AND-

- 203.47.114.61 (DR)

SFTP directory structure

Upload location: **/public/upload**
This is where Access-seekers need to place the files containing numbers to be washed.

Download location: **/public/download**
This is where wash results will be available for download by Access-seekers.

Archive location: **/public/archive**
This is where archived wash results are stored.

Security

Supported ciphers

For security reasons the SFTP server will only support modern cipher algorithms. Access Seekers using custom code to connect to and interact with the SFTP server should confirm that any SFTP libraries are compatible with supported ciphers.

The server supports the following options for **kex_algorithms**:

- diffie-hellman-group-exchange-sha1
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group1-sha1
- diffie-hellman-group14-sha1

The server supports the following options for **server_host_key_algorithms**:

- ssh-dss
- ssh-rsa

The server supports the following options for **encryption_algorithms_client_to_server**:

- aes128-ctr aes192-ctr aes256-ctr arcfour128 arcfour256

The server supports the following options for **encryption_algorithms_server_to_client**:

- aes128-ctr
- aes192-ctr
- aes256-ctr
- arcfour128
- arcfour256

The server supports the following options for **mac_algorithms_client_to_server**:

- hmac-ripemd160
- hmac-sha1
- hmac-sha2-256

- hmac-sha2-512
- umac-64@openssh.com

The server supports the following options for **mac_algorithms_server_to_client**:

- hmac-ripemd160
- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512
- umac-64@openssh.com

The server supports the following options for **compression_algorithms_client_to_server**:

- none
- zlib@openssh.com

The server supports the following options for **compression_algorithms_server_to_client**:

- none
- zlib@openssh.com