

WinSCP Settings

Most of the WinSCP parameters that I use are the default settings. A few settings that need to be Modified are found on the opening page: SFTP, Host name of EC2 unit, and Port 22. The user name must be ec2-user. Under “Advanced Settings” authentication, a private key file that you created on AWS when launching your server must also be typed in.

Setting that work for me are shown stepwise in the following screenshots.

Dan Sweeney

Login

- New Site
- Similar_Partition_Screening
- SuspectScreening_SPS_with_m5zn_Virginia
- SuspectScreening_SPS_with_T2micro
- SuspectScreening_SPS_with_T2micro_Orego

Session

File protocol:

SFTP

Host name:

ec2-52-54-57-29.compute-1.amazonaws.com

Port number:

22

User name:

ec2-user

Password:

Save

Cancel

Advanced...

Tools

Manage

Login

Close

Help

Show Login dialog on startup and when the last session is closed

Advanced Site Settings



Environment

- Directories
- Recycle bin
- Encryption
- SFTP
- Shell

Connection

- Proxy
- Tunnel

SSH

- Key exchange
- Authentication
- Bugs

Note

Server environment

End-of-line characters (if not indicated by server):

LF

UTF-8 encoding for filenames:

Auto

Time zone offset: 0 hours 0 minutes

Detect automatically

Trim VMS version numbers

Daylight saving time

Adjust remote timestamp to local conventions

Adjust remote timestamp with DST

Preserve remote timestamp

PuTTY

PuTTY terminal settings:

Edit in PuTTY...

Color

OK

Cancel

Help

Advanced Site Settings



- Environment
 - Directories**
 - Recycle bin
 - Encryption
 - SFTP
 - Shell
- Connection
 - Proxy
 - Tunnel
- SSH
 - Key exchange
 - Authentication
 - Bugs
- Note

Directories

Synchronize browsing

Remember last used directory

Remote directory:

Local directory:
 ...

Local directory is not used with Explorer interface.

Directory reading options

Cache visited remote directories

Cache directory changes Permanent cache

Resolve symbolic links

Follow symbolic links to directories

Color ▼

OK

Cancel

Help

Advanced Site Settings



- Environment
 - Directories
 - Recycle bin
 - Encryption
 - SFTP
 - Shell
- Connection
 - Proxy
 - Tunnel
- SSH
 - Key exchange
 - Authentication
 - Bugs
- Note

Recycle bin

Preserve deleted remote files to recycle bin

Preserve overwritten remote files to recycle bin (SFTP only)

Remote recycle bin:

Color ▼

OK

Cancel

Help

Advanced Site Settings



- Environment
 - Directories
 - Recycle bin
 - Encryption
 - SFTP
 - Shell
- Connection
 - Proxy
 - Tunnel
- SSH
 - Key exchange
 - Authentication
 - Bugs
- Note

Encrypt files

Encryption options

Encryption key:

Show key

Generate Key

Color ▼

OK

Cancel

Help

Advanced Site Settings



- Environment
 - Directories
 - Recycle bin
 - Encryption
 - SFTP
 - Shell
- Connection
 - Proxy
 - Tunnel
- SSH
 - Key exchange
 - Authentication
 - Bugs
- Note

Protocol options

SFTP server:

Preferred SFTP protocol version:

Canonicalize paths on the server

Allow SCP fallback

Detection of known bugs in SFTP servers

Reverses order of link command arguments:

Misinterprets file timestamps prior to 1970:

Color ▼

OK

Cancel

Help

Advanced Site Settings



Environment

- Directories
- Recycle bin
- Encryption
- SFTP
- Shell

Connection

- Proxy
- Tunnel

SSH

- Key exchange
- Authentication
- Bugs

Note

Shell

Shell:

Return code variable:

Color ▼

OK

Cancel

Help

Advanced Site Settings



- Environment
 - Directories
 - Recycle bin
 - Encryption
 - SFTP
 - Shell
- Connection**
 - Proxy
 - Tunnel
- SSH
 - Key exchange
 - Authentication
 - Bugs
- Note

Connection

- Passive mode
- Optimize connection buffer size

Timeouts

Server response timeout: seconds

Keepalives

- Off
- Sending of null SSH packets
- Executing dummy protocol commands

Seconds between keepalives:

Internet protocol version

- Auto
- IPv4
- IPv6

Color ▼

OK

Cancel

Help

Advanced Site Settings



- Environment
 - Directories
 - Recycle bin
 - Encryption
 - SFTP
 - Shell
- Connection
 - Proxy**
 - Tunnel
- SSH
 - Key exchange
 - Authentication
 - Bugs
- Note

Proxy

Proxy type: None

Proxy host name: Port number:

User name: Password:

Proxy settings

Telnet command:

patterns

Consider proxying local host connections

Do DNS name lookup at proxy end: Auto

Advanced Site Settings



- Environment
 - Directories
 - Recycle bin
 - Encryption
 - SFTP
 - Shell
- Connection
 - Proxy
 - Tunnel
- SSH
 - Key exchange
 - Authentication
 - Bugs
- Note

Connect through SSH tunnel

Host to setup tunnel on

Host name: Port number:

User name: Password:

Tunnel options

Local tunnel port:

Tunnel authentication parameters

Private key file:

Color ▼

OK

Cancel

Help

Advanced Site Settings



Environment

- ... Directories
- ... Recycle bin
- ... Encryption
- ... SFTP
- ... Shell

Connection

- ... Proxy
- ... Tunnel

SSH

- ... Key exchange
- ... Authentication
- ... Bugs

Note

Color ▼

Protocol options

Enable compression

Encryption options

Encryption cipher selection policy:

AES
ChaCha20
Blowfish
3DES
-- warn below here --
Arcfour
DES

Up

Down

Enable legacy use of single-DES

OK

Cancel

Help

Environment

- Directories
- Recycle bin
- Encryption
- SFTP
- Shell

Connection

- Proxy
- Tunnel

SSH

- Key exchange
- Authentication
- Bugs

Note

Color



Key exchange algorithm options

Algorithm selection policy:

```
ECDH key exchange
Diffie-Hellman group exchange
Diffie-Hellman group 14
RSA-based key exchange
-- warn below here --
Diffie-Hellman group 1
```

Up

Down

 Attempt GSSAPI key exchange

Options controlling key re-exchange

Max minutes before rekey (0 for no limit):

60

Max data before rekey (0 for no limit):

1G

OK

Cancel

Help

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 'keyboard-interactive' authentication
- Respond with a password to the first prompt

Authentication parameters

Allow agent forwarding

Private key file:

~:\Amazon_Info\SPS_video.ppk

Display Public Key

Tools

GSSAPI

- Attempt GSSAPI authentication
- Allow GSSAPI credential delegation

Color

OK

Cancel

Help

Advanced Site Settings



- Environment
 - Directories
 - Recycle bin
 - Encryption
 - SFTP
 - Shell
- Connection
 - Proxy
 - Tunnel
- SSH
 - Key exchange
 - Authentication
 - Bugs
- Note

Detection of known bugs in SSH servers

Chokes on SSH ignore messages:	Auto
Chokes on WinSCP's SSH 'winadj' requests	Auto
Miscalculates SSH HMAC keys:	Auto
Miscalculates SSH encryption keys:	Auto
Requires padding on SSH RSA signatures:	Auto
Misuses the session ID in SSH PK auth:	Auto
Handles SSH key re-exchange badly:	Auto
Ignores SSH maximum packet size:	Auto

Color ▼

OK

Cancel

Help