Setup client step-cli: Windows users

- Windows PowerShell
 - Configuration of the step client
 - Activation of the ssh-agent
 - Subsequent use
- Windows Subsystem Linux (WSL)
- Windows SSH/SFTP Clients

The SmallStep client installation on Windows can be done in different ways depending on the environment you want to use to work and activate connections to the machines:

- using package manager scoop on PowerShell
- using Windows Subsystem for Linux (WSL) with a Linux distribution installed from Microsoft Store

Windows PowerShell

Open the PowerShell, and the window as shown below appears



Then type the following commands in the PowerShell window:

Download and install scoop

iwr -useb get.scoop.sh | iex

• Test scoop:

scoop help

· Install git support for scoop

scoop install git

Install smallstep

scoop bucket add smallstep https://github.com/smallstep/scoop-bucket.git

scoop install smallstep/step

· Verify smallstep

step

Configuration of the step client

Initialize the client with the command:

step ca bootstrap --ca-url=https://sshproxy.hpc.cineca.it --fingerprint 2ae1543202304d3f434bdc1a2c92eff2cd2b02110206ef06317e70c1c1735ecd

If everything is fine the following messagg will compare on the shell:

The authority configuration has been saved in C:\Users\e.rossi\.step\config\defaults.json. PS C:\Users\e.rossi> Get-Service --Name ssh-agent

Activation of the ssh-agent

On the system windows 10/11 the ssh-agent is active by default. You can verify it with the command:

Get-Service -Name ssh-agent

and the output on the PowerShell will be:



If the service is not in "running status" it can be activated with:

Start-Service -Name ssh-agent

If is still not working , it is necessary to open the PowerShell as admin:

Tutti App Documenti Impostaz	zioni Altro	• • • • • • • • • • • • • • • • • • •	
Corrispondenza migliore			
Windows PowerShell		\geq	
Арр		Windows PowerShell	
PowerPoint	>	Арр	
Windows PowerShell ISE	>	🕜 Apri	
> Windows PowerShell (x86)	>	Esegui come amministratore	
Windows PowerShell ISE (x86)	>	 Esegui ISE come amministratore Windows PowerShell ISE 	
Documenti - Questo PC (11+)			~
Cartelle (1+)			
Impostazioni (7+)			

and execute the following commands:

\$ Set-Service -Name ssh-agent -StartupType Auto \$ Start-Service ssh-agent

Subsequent use

Run the following command to get the timed certificate:

step ssh login <your-email> --provisioner cineca-hpc

Enter your HPC credentials in the web interface window/tab that opened.

To view the issued certificate and its validity status:

step ssh list

PS C:\Users\e.rossi> step ssh list 256 SHA256:mE3gEbhzw0nphgE41dVFE9ciVcRyMy1MT2tiMEsg/O0 e.rossi@cineca.it (ECDSA-CERT) 256 SHA256:8NJAkMmK3Xb3hxnnVDg37DGXxmnrL35ImFfiZYVrw3c e.rossi@cineca.it (ECDSA-CERT) PS C:\Users\e.rossi>

step ssh list --raw <user_email> | step ssh inspect

PS	C:\Users\e.rossi> step ssh listraw e.rossi@cineca.it step ssh inspect
-:	
	Type: ecdsa-sha2-nistp256-cert-v01@openssh.com user certificate
	Public key: ECDSA-CERT SHA256:KeybJDjkgmHtXhFXdSFNGrKh+R3EHAfG10YRZo59Yu4
1	Signing CA: ECDSA SHA256:e0ZF6AnnUzi0g7Db9nOaXxkEjRq9D6Ka4tV04XqiIgM
	Key ID: "e.rossi@cineca.it"
1	Serial: 2582704634100630444
1	Valid: from 2022-04-04T17:42:36 to 2022-04-05T01:43:36
	Principals:
	erossi00
	Critical Options: (none)
5	Extensions:
	permit-X11-forwarding
1	permit-agent-forwarding
1	permit-port-forwarding
	permit-pty
	permit-user-rc
PS	C:\Users\e.rossi>

Now you can login to the cluster.

Windows Subsystem Linux (WSL)

It is necessary to open a shell and install step following exactly the installation instructions for the linux environment.

Please note that WSL doesn't support separate tabs, and if you open a new window, this by default doesn't see the step certificate already issued from the previous tab. To avoid creating a new timed certificate for each session, we suggest to implement in your .bashrc an automatic verification of the created certificate based on the variables initialized by the "eval \$(ssh-agent)" command, that can be redirected in an appropriate text file. For example:

```
if [ -f ~/.bash_agent ]; then
        . ~/.bash_agent
fi
steptest=$(step ssh list --raw '<user-email>'| step ssh inspect | grep "Valid")
if [ -z "$steptest" ]
then
        eval $(ssh-agent)
        echo "export SSH_AUTH_SOCK=$SSH_AUTH_SOCK" > ~/.bash_agent
        echo "export SSH_AGENT_PID=$SSH_AGENT_PID" >> ~/.bash_agent
        step ssh login '<user-email>' --provisioner cineca-hpc
fi
```

Windows SSH/SFTP Clients

There are many SSH or SFTP Clients available for Windows, that are of common usage but are not automatically configured for working with the new 2FA system. It is although possible to login with them by exploiting the OpenSSH agent forwarding that can be set by taking advantage of another tool installable on Powershell, that is WinSSH-Pageant.

The procedure is as follows:

- Follow the setup of the Two-factor authentication for Powershell as documented in our Userguide, up to and including paragraph "Activation of the sshagent";

- Download WinSSH-Pageant by executing the following command in Powershell:

winget install winssh-pageant

- You should find a new executable in this path:

C:\Users\\$Env:UserName\AppData\Local\Programs\WinSSH-Pageant\winssh-pageant.exe

the only difference is in \$Env:UserName, that is specific to your workstation.

In principle this command has to be launched with its full path, but you may want to setup an easier way to access it. The most simple way would be to cre ate an alias:

New-Alias winssh-pageant C:\Users\\$Env:UserName\AppData\Local\Programs\WinSSH-Pageant\winssh-pageant.exe

Keep in mind though that Powershell keeps an alias alive only until the shell is closed. An easy permanent solution would be to **copy the program** winsshpageant.exe to another folder, for example C:\Users\\$Env:UserName\scoop\shims that has been already included permanently in the PATH variable by the previous installation of step and is therefore recognized by Powershell without the need of expliciting the full path.

- From Powershell, launch the WinSSH-pageant with this command:

winssh-pageant --sshpipe

(assuming that you have estabilished a shortcut, otherwise use the full path as mentioned previously)

It is possible to check if the previous command worked and a WinSSH-pageant process is active, with the command:

Get-Process | Select-String pageant

The expected output is as in this screenshot:



Now, everytime you need to create a new certificate you can use the typical step command from Powershell:

step ssh login <your-email> --provisioner cineca-hpc

And at this point you can connect with a SSH/SFTP client opening a session with a specific configuration, that usually can be saved for subsequent uses.

The method has been tested with the following clients:

Putty:

In the login window, check the category "Connection --> SSH --> Auth" and be sure that the boxes "Attempt authentication using Pageant" and "Allow agent forwarding" are ticked.



WinSCP:

In the login window, from the Advanced settings go to "SSH--> Authentication" and tick the boxes "Attempt authentication using Pageant" and "Allow agent forwarding". Be sure that the file protocol is set to "SCP".

 \times

22

Vew Site		Session								
📮 amarani0@logir	n.marconi.cineca.it	File protocol:								
		SCP								
		Host name:		Port number						
		login.marconi.cineca.it								
		User name:	Password:							
		amarani0								
				-						
		Edit		Advanced						
vanced Site Settings			? ×							
nvironment	Bypass authentication	n entirely								
Directories	Authentication ontions	,								
- Recycle bin	ridenencederon operono	Attempt authentication using Pageant								
SCP/Shell	Attempt authenticatio	n using Pageant								
SCP/Shell Connection	Attempt authenticatio	on using Pageant								
SCP/Shell Connection Proxy	Attempt authenticatio Attempt 'keyboard-in	on using Pageant teractive' authentication								
SCP/Shell Connection Proxy Tunnel SSH	 Attempt authentication Attempt 'keyboard-in Respond with a point 	on using Pageant teractive' authentication password to the first prompt								
SCP/Shell Connection - Proxy - Tunnel SH - Key exchange	Attempt authenticatio Attempt 'keyboard-in Respond with a p Authentication parameter	on using Pageant teractive' authentication password to the first prompt s								
SCP/Shell connection Proxy Tunnel SH Key exchange 	Attempt authenticatio Attempt 'keyboard-in Respond with a p Authentication parameter Authentication parameter Allow agent forward	on using Pageant teractive' authentication password to the first prompt s								
SCP/Shell connection - Proxy - Tunnel SH - Key exchange - Authentication - Bugs lote	Attempt authenticativ Attempt 'keyboard-in @ Respond with a p Authentication parameter Allow agent forward Private key file:	on using Pageant teractive' authentication password to the first prompt s ng								
SCP/Shell Connection Proxy Tunnel SCH Key exchange Authentication Bugs lote	Attempt authenticati Attempt 'keyboard-in Respond with a Authentication parameter Allow agent forwardi Private key file:	on using Pageant teractive' authentication aassword to the first prompt s								
SCP/Shell connection – Proxy – Tunnel SH – Key exchange – Authentication – Bugs tote	Attempt authenticati Attempt 'keyboard-in Respond with a Authentication parameter Allow agent forwardi Private key file:	on using Pageant teractive' authentication assaword to the first prompt s ng								
SCP/Shell connection – Proxy – Tunnel SH – Key exchange – Authentication – Bugs ote	Attempt authenticati Attempt 'keyboard-in Respond with a Authentication parameter Allow agent forwardi Private key file: Display Public	on using Pageant teractive' authentication password to the first prompt s ng : Key Tools								
- SCP/Shell Connection - Proxy - Tunnel SSH - Key exchange - Authentication - Bugs lote	Attempt authenticati Attempt 'keyboard-in Respond with a j Authentication parameter Allow agent forwardi Private key file: Display Public Certificate to use with th	on using Pageant teractive' authentication bassword to the first prompt s ng : Key Tools • te private key:								
- SCP/Shell Connection - Proxy - Tunnel SH - Key exchange - Authentication - Bugs lote	Attempt authenticati Attempt 'keyboard-in Respond with a Authentication parameter Allow agent forwardi Private key file: Display Public Certificate to use with th	on using Pageant teractive' authentication password to the first prompt s ng : Key Tools T ie private key:								
- SCP/Shell onnection - Proxy - Tunnel SH - Key exchange - Authentication - Bugs ote	Attempt authenticati Attempt 'keyboard-in Respond with a p Authentication parameter Allow agent forwardi Private key file: Display Public Certificate to use with th GSSAPI	on using Pageant teractive' authentication baseword to the first prompt s ng : Key Tools T ee private key:								
- SCP/Shell onnection - Proxy - Tunnel SH - Key exchange - Authentication - Bugs ote	Attempt authenticati Attempt 'keyboard-in Respond with a p Authentication parameter Allow agent forwardi Private key file: Display Public Certificate to use with th GSSAP1 Attempt GSSAP1 auth	on using Pageant teractive' authentication bassword to the first prompt s ng : Key Tools T								
- SCP/Shell connection - Proxy - Tunnel - SH - Key exchange - Authentication - Bugs ote	Attempt authenticati Attempt 'keyboard-in Respond with a p Authentication parameter Allow agent forwardi Private key file: Display Public Certificate to use with th GSSAPI Attempt GSSAPI auth Oligne GSSAPI auth	on using Pageant teractive' authentication password to the first prompt s ng : Key Tools • expression • entropy • • • • • • • • • • • • • • • • • • •								

Note: It is possible that if you try to edit an already saved site, the ssh-agent won't be recognized. If this is the case, we recommend to create a new site from scratch and configure it accordingly. The new site can then be saved and will keep working. Note: In certain cases, we noted that the procedure may not work at first try, and you will get an error at login even if everything is in order. In most cases,

a simple reboot of your workstation solves the problem and the issue will not occur again.

Filezilla:

In your site configuration, be sure that the Protocol is set to "SFTP - SSH File Transfer Protocol" and the Logon type is set to "Normal".

Site Manager								×				
Select entry:					General Advanced Transfer Settings Charset							
My Sites				Protocol:	SFTP - SSH File Transfer Protocol			~				
± nonoice				Host:	login.marconi.cineca.it		Port	:				
				Logon Type:	Normal			~				
				User:	amarani0							
				Password:								
				Background	color: None ~							
				Comments:								
	New site	New folder										
	New Bookmark	Rename										
	Delete	Duplicate						Ŧ				
							0.11					

MobaXTerm:

In the upper menu bar with the general options, make sure that in "Settings" "Configuration" "SSH" the box "Use external Pageant" is ticked (it should be by default).

General	🚺 Terminal	X X11	SSH	👤 Display	🔑 Toolbar	ጳ Misc			
SSH-brow	ser settings								
🛃 Enab	le graphical SSI	H-browser	🔽 Αι	utomatically swi	tch to SSH-bro	wser tab afte	er login		
🗌 Rem	ote-monitoring (experimental)	🗌 Pr	reserve files dat	tes during SSH	-browser tra	nsfers		
- SSH settin	gs witt login: <con< td=""><td>a ao Mindou</td><td></td><td></td><td>SSH ongi</td><td></td><td></td><td></td><td></td></con<>	a ao Mindou			SSH ongi				
			s login>			Hewe			
SSH	keepalive	Display SS	Hbanner	Valida	te host identity	at first conne	ection		
🛃 GSS	API Kerberos	Domain:		GSSA	API library: <na< td=""><td>ative Window</td><td>'s> ~</td><td></td><td></td></na<>	ative Window	's> ~		
								-	۵Ť
SSH agen	s								•
Use	internal SSH ag	ent "MobAgen	t"	🔍 Show key	s currently load	led in MobAg	ent		
Load fo	lowing keys at I	lobAgent star	up						
							+		
🔽 Use	external Pagear	t 🗌) Prompt I	before serving l	keys				

After that, opening a simple ssh session should do.

sion set	tings													
SSH	Telnet	<mark>⊮</mark> Rsh	Xdmcp	I RDP	VNC	🌏 FTP	8 SFTP	∛ Serial	Q File	Shell	(Browser	💕 Mosh	ঞ্জ Aws S3	III WSL
🖪 Bas	sic SSH se	ttings												
Rem	note host *	login.g10	0.cineca.it	t		🔽 Specif	y usernai	me amar	ani0		~ 2		Port 22	\$
	🔽 X11	-Forward	ling	C 🖸	ompressi	on R	emote ei	nvironment	Interac	ctive shell	~			
	Execut	e comma	and:	0	ompressi	on n			wit offer a		ondo		_	_
	SSH-b	prowser ty	ype: SFT	P protoco	I			Follow S	SSH path	(experim	ental)		\$	
	Use	private k	ey					🙎 E:	xpert SSI	H settings				
			Execute	macro at	session :	start: <nc< td=""><td>ne></td><td></td><td>~</td><td></td><td></td><td></td><td></td><td></td></nc<>	ne>		~					

Other SSH/SFTP clients don't seem to be working with this method and are currently not supported by CINECA (for example BitviseSSH), or haven't been tested yet. We will keep updating the Userguide when other clients will be proven compatible.