

Configuring and using PuTTY/Pageant

PuTTY is a free and easy to use <u>ssh client</u> for **Windows**. You can use it to connect to your favorite remote Linux servers in text mode, and start remote graphical applications if you also have a running <u>X server</u>

Installation

Official web site: PuTTY Web site [https://www.chiark.greenend.org.uk/~sgtatham/putty/]

You can install the latest version of PuTTY directly from Microsoft Store [https://apps.microsoft.com/store/detail/XPFNZKSKLBP7RJ], or download the latest 64-bit msi installer [https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html]

Updating PuTTY

Download the latest version, or just type winget upgrade --id XPFNZKSKLBP7RJ in a Windows Terminal

Launching PuTTY/Pageant

You could directly launch PuTTY (Start \Rightarrow PuTTY), but it is actually **more efficient** to use Pageant for opening terminals, especially if you are often going to connect to the same server(s)

Starting Pageant: Start \Rightarrow PuTTY \Rightarrow Pageant

- Pageant is an ssh agent for Windows, but this page also explains how to use it for easily creating and using connection profiles (aka *Sessions*) to connect to remote Linux servers
 - Some applications (e.g. <u>WinSCP</u>) will automatically try to use Pageant as an *ssh-agent*, instead of asking you to type your <u>ssh passphrase</u>
- It will seem that nothing happens when you start Pageant, but you should get the Pageant icon at the bottom right of your screen.



If you right click on the Pageant icon, you can manage sessions with the New Session option, use Saved Sessions profiles and manage *ssh keys* (View Keys, Add Key).

You can also view/add ssh keys by double-clicking on the Pageant icon

other:putty_conf [PMIP3 wiki]

| New Session | | | | |
|----------------|---|-----|---|----|
| Saved Sessions | > | | | |
| View Keys | | | | |
| Add Key | | ß | - | 8 |
| Help | | | | ~ |
| About | | 2 | - | Ö, |
| Exit | | a., | | |
| | | - | | |

Configuring PuTTY

Launch the PuTTY Configuration manager: (Right click on) $Pageant \Rightarrow New Session$

| 🕵 PuTTY Configuration | | ? | \times |
|---|---|--|----------|
| Category: | | | |
| Session Logging Terminal Keyboard Bel Sel Sel | Basic options for your PuTTY se Specify the destination you want to conner Host Name (or IP address) Connection type: O Raw O Telnet O Riogin () SSP Load, save or delete a stored session Saved Sessions Default Settings Close window on esit: O Always O Never () Only on c | ession ect to Port 22 H O Se Loac Savy Delet dean exit | fial |
| About Help | Open | Cance | al |

• You can keep most PuTTY's default settings. This section will show you how to create your first *session profile*, with some **highly recommended options**.

If you want to add another session later, just Load an existing (and properly configured) session, Save it under a new name, change the session details, and then save the session again.

- When changing a setting, select a (sub-)**Category in the left part** of the PuTTY Configuration window, and change the displayed **settings in the right part** of the window.
- After changing the settings of an existing Session, do not forget to go back to the Session category (at the top left of the Putty Configuration window) and click Save!

Creating a new session

In the Session Category:

- Specify a **Host Name**: e.g. ssh1.lsce.ipsl.fr for the *LSCE access server* (also called *LSCE gateway*)
- Specify a matching session name in **Saved Sessions**: e.g. ssh1
- Click on **Save** to save the new session (that will only have default settings for now)

| 🕵 PuTTY Configuration | | ? | \times |
|--|--|--|----------|
| Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Colours Connection Data Proxy Telnet Rlogin SSH Serial | Basic options for your PuTTY set Specify the destination you want to conner Host Name (or IP address) ssh1.lsce.ipsl.fr Connection type: O Raw O Telnet O Rlogin O SSH Load, save or delete a stored session Saved Sessions ssh1 Default Settings Close window on exit: O Always O Never O Only on cl | ssion ct to Port 22 Concel Cancel Cancel | al |
| About Help | Open | Cancel | |

If you are in a hurry, you can connect to the Linux server specified in the Host Name field by clicking on Open

Changing some useful settings

- Load an existing session (e.g. the <u>ssh1</u> profile defined above), that will serve as a **template (with the recommended settings)** for the future sessions
- In the Window \Rightarrow Selection category:
 - Select **xterm** in the *Actions of mouse buttons* section.

This will allow you to use the mouse buttons in the PuTTY terminal the same way you would use them in an standard Linux *xterm* terminal:

- Select and Copy text (at the same time) with the left button
- Paste text with the middle button

| Image: Putty Configuration ? × Category: Options controlling copy and paste Image: Logging Options controlling copy and paste Image: Terminal Keyboard Image: Bell Control use of mouse Image: Features Options controlling copy and paste Image: Window Appearance Image: Behaviour Translation Image: Selection Options copy/paste actions to clipboards Image: Connection Data Image: Proxy Telnet Image: Rogin System clipboard Image: StH Serial | | | | | |
|---|--|--|--|------------|--|
| Category: | | | | | |
| Seission Logging Ferminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial | Options cor Control use of mouse Action of mouse buttor Windows (Middle e Compromise (Middle attem (Right extend Shift overrides apple Default selection mode Normal | ntrolling copy and past ns: xtends, Right brings u e extends, Right paste ls, Middle pastes) ication's use of mouse e (Alt+drag does the of C Rectangular | e p menu) s) ther onej r block |): | |
| | Assign copy/paste act Auto-copy selected Mouse paste action: {Ctrl,Shift} + Ins: Ctrl + Shift + {C,V}: Control pasting of text f | I text to system clipboard System clipboard System clipboard No action from clipboard to termi acters in pasted text | nal | > > | |
| About Help | | Open | Cance | ; | |

- In the Window \Rightarrow Appearance category:
 - You can choose a font more readable than the default one!
 We recommend the Cascadia Code font that comes with the Windows Terminal application (which means that you first have to install Windows Terminal first, but you will probably need it anyway)
 IF Windows Terminal is not installed yet, you can select the modern Consolas
 [https://en.wikipedia.org/wiki/Consolas] font in the list of available fonts
 - Use the Change... button in the Font settings section, and select Cascadia Code and Regular (you can also experiment with styles different from Regular, and different font sizes), or Consolas and Regular or Bold



| Police | × |
|---|--|
| Police: Cascadia Code @NSimSun @SimSun-ExtB Cascadia Code | Style de police :Taille :Regular10Italic11SemiBold14 |
| Cascadia Mono Consolas Courier v | SemiBold Itali Bold Bold Italic v |
| | Script : Occidental |
| Autres polices | OK Annuler |

- In the Connection \Rightarrow Data category:
 - Specify your login name (on the LSCE servers) in **Auto-login username**. This way you won't have to type it when you connect to the Linux server!

| Putty Configuration ? X Category: • Session • Logging • Teminal • Keyboard • Bel • Features • Window • Appearance • Behaviour • Translation • Selection • Colours • Connection • Data • Proxy • SSH • Serial • Teminat • Riogin • SUPDUP Image: Data to send to the server Login details Auto-login usemame your_login When usemame is not specified: • Prompt • Use system usemame (ypeter) Terminal details Terminal speeds 38400,38400 Environment variables Variable Add Value Remove [| | |
|--|---|--|
| Category: | | |
| Session Logging Logging Keyboard Bell Features Window Appearance Behaviour Translation | Data to send Login details Auto-login usemame When usemame is not spec Prompt O Use system Terminal details Terminal type string Terminal speeds | to the server your_login ified: m usemame (jypeter) xterm-256color 38400 38400 |
| Selection Colours Connection Data Proxy SSH Serial Telnet Rlogin SUPDUP | Environment variables Variable Value | Add |
| About Help | | Open Cancel |

- You should also specify xterm-256color instead of the default xterm terminal type in the Terminal-type string field. This will allow you to display nicer colors in the terminals (for the applications that use fancy colors)
 - You can later open a terminal and type msgcat --color=test, and check if you get something like

other:putty_conf [PMIP3 wiki]



• In the Connection \Rightarrow SSH \Rightarrow Kex category:

• Unselect Attempt GSSAPI key exchange!

If you forget to do this, connecting to a server will seem to take forever (if it works at all)...



- In the Connection \Rightarrow SSH \Rightarrow Auth category:
 - Select Allow agent forwarding. This is the same as using ssh with the -A option



- In the Connection \Rightarrow SSH \Rightarrow X11 category:
 - Select **Enable X11 forwarding**. This is the same as <u>using ssh with the -X option</u> Note: remember that you will also need an <u>X server running</u> in order to display graphics!

| 🕵 PuTTY Configuratio | n | ? | × |
|----------------------|---|---------------|---------|
| Category: | | | |
| | ♦ Options controlling SSH X11 for ■ X11 forwarding ■ Enable X11 forwarding X display location ■ Remote X11 authentication protocol ● MIT-Magic-Cookie-1 ○ XDM-Au X authority file for local display | uthorization- | .1 e |
| About H | Help Open | Canc | el |

• When you have finished updating the settings, do not forget to go back to Category ⇒ Session and Save the session!

| 🕵 PuTTY Configuratio | on | | ? × |
|---|------|---|----------|
| Category: | | | |
| <mark>⊫-</mark> Session | ^ | Basic options for your PuTTY set | ssion |
| | | Specify the destination you want to connect | ct to |
| | | Host Name (or IP address) | Port |
| Reyboard | | ssh1.lsce.ipsl.fr | 22 |
| Features | | Connection type: | |
| Window | | ◯ Raw Ö Telnet ◯ Rlogin ◉ SSH | ○ Serial |
| | | Load, save or delete a stored session Saved Sessions ssh1 | |
| Colours | | Default Settings | Load |
| Data | | 3311 | Save |
| - Telnet | | | Delete |
| | | | |
| ···· Kex ···· Host keys ···· Cipher | • | Close window on exit: Always Never Only on cl | ean exit |
| < > | | | |
| About H | Help | Open | Cancel |

• Click on Open to connect to the specified host with the updated settings, and check that things are working properly The first time you connect to a server, you will get a PuTTY Security Alert window, where you have to click on Accept to tell PuTTY that you trust the connection to this new server

| PuTTY S | ecurity Alert | \times |
|---------|--|----------|
| ? | The host key is not cached for this server: ssh1.lsce.ipsl.fr (port 22) You have no guarantee that the server is the computer you think it is. The server's ssh-ed25519 key fingerprint is: ssh-ed25519 255 SHA256:7piG/wA9i+workxgcuRdg3nLev0OuRgDnGRldzQe9UY | |
| | If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting. | |
| | If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once". | |
| | If you do not trust this host, press "Cancel" to abandon the connection. | |
| Hel | p More info Accept Connect Once Cancel | |

Adding more connection profiles

Start Pageant, and then the *PuTTY Configuration manager*: (Right click on) Pageant \Rightarrow New Session

New profile for a direct connection to a remote server

- Select an existing (and correctly configured) session (e.g. the ssh1 profile defined above) and click on Load
- Update the values of the **Host Name** and **Saved Session** (the name of the new profile you want) text fields, and settings
 - Example: connecting to **LSCE from INSIDE LSCE** (inside ⇔ computer connected to the wired network):
 - Host Name \Rightarrow obelix

- Saved Session \Rightarrow obelix (direct connection)
- Example: connecting to spirit [https://documentations.ipsl.fr/spirit/spirit_clusters/head_nodes.html]:
 - Host Name \Rightarrow spirit1.ipsl.fr
 - **WARNING!** You can only connect to spirit using a pair of *ssh keys*. Be sure to read the <u>Using ssh</u> keys with PuTTY/Pageant section below
 - You can also use spirit2, spiritx1 or spiritx2 depending on which IPSL server you want to access [https://documentations.ipsl.fr/spirit/spirit_clusters/head_nodes.html]
 - Saved Session $\Rightarrow \texttt{spirit1}$
 - do not forget to **specify your IPSL login** in: Connection ⇒ Data ⇒ Auto-login username
- Go back to Category \Rightarrow Session and Save the session

New profile with a connection through a gateway

- Select an existing *gateway* session (e.g. ssh1) and click on Load.
 For connecting to LSCE from OUTSIDE LSCE, select the <u>ssh1 profile</u>
 If you are at LSCE, but use the *eduroam* or the *guest* WiFi network, you are considered as being *outside LSCE*!
- In the Connection ⇒ SSH category, specify the command used to connect to the target server from the *gateway*, in the **Remote command** field

e.g. for LSCE, use:

• ssh -X -A obelix (check the useful ssh options for more details on the options)

| 🕵 PuTTY Configuration | ? × | | | |
|--|--|--|--|--|
| PuTTY Configuration Category: Catego | ? × Options controlling SSH connections Data to send to the server Remote command: ssh -X -A obelix Protocol options Don't start a shell or command at all Enable compression SSH protocol version: | | | |
| Translation Selection Colours Onnection Data Proxy SSH Serial Telnet Rlogin SUPDUP | SSH protocol version: 2 1 (INSECURE) Sharing an SSH connection between PuTTY tools Share SSH connections if possible Permitted roles in a shared connection: ✓ Upstream (connecting to the real server) ✓ Downstream (connecting to the upstream PuTTY) | | | |
| About Help | Open Cancel | | | |

Go back to Category ⇒ Session, specify a new profile name in Saved Sessions (e.g. obelix via ssh1) and Save the session

| 🕵 PuTTY Configuration | | ? × |
|--|--|---|
| Putty Configuration Category: □ Session □ Logging □ Terminal □ Keyboard □ Bell □ Features □ Window □ Appearance □ Behaviour □ Translation □ Selection □ Colours □ Data □ Proxy □ Telnet □ Rlogin □ SSH | Basic options for your PuTTY set Specify the destination you want to connect Host Name (or IP address) ssh1.lsce.ipsl.fr Connection type: Raw O Telnet O Rlogin SSH Load, save or delete a stored session Saved Sessions obelix via ssh1 Default Settings obelix via ssh1 ssh1 | ? × ssion ct to Port 22 4 O Serial Load Save Delete |
| Serial | Close window on exit: Always Never Only on cl | ean exit |
| About Help | Open | Cancel |

Daily usage of PuTTY/Pageant

Note: PuTTY will ask your password each time you open a session, unless you have <u>ssh keys</u>, and you use Pageant to store your passphrase

Starting a session from Pageant

Once you have <u>started pageant</u>, and <u>configured sessions</u>, you can easily open terminals on the remote servers by right-clicking on the pageant icon, and selecting a **Saved Session**.



Starting a session from a desktop shortcut

It is possible to create a shortcut on the desktop to start a specific session [https://the.earth.li/~sgtatham/putty/0.77/htmldoc/AppendixA.html#QA.6.4]!

• Right-click on the desktop and select $New \Rightarrow Shortcut$

- Specify the location of putty.exe in the *path* field, and click Next:
 "C:\Program Files\PuTTY\putty.exe" (with the quotes!)
- Specify the name of the shortcut (as it will appear on the desktop), and save the shortcut e.g. obelix via ssh1
- Right-click on the shortcut and select **Properties**, then add the name of the desired profile to the content of the *Target* field
 - Warning:
 - you have to use an existing session name (as it appears in Pageant ⇒ Session ⇒ Saved Sessions)
 - you have to **use quotes correctly**, otherwise you will get an error message!
 - Examples:
 - "C:\Program Files\PuTTY\putty.exe" -load "obelix via ssh1"
 - "C:\Program Files\PuTTY\putty.exe" -load "obelix (direct)"
- Click **OK** to save the changes
- You can now connect to the remote server just by clicking on the desktop shortcut, instead of right-clicking on the Pageant icon!

Using ssh keys with PuTTY/Pageant

In this section, we will use *key* files that have the same base name, and **different extensions**: e.g. id_ed25519, id_ed25519.pub and id_ed25519.ppk

You should **make sure that you can <u>see hidden folders</u>, and files' extensions** before you go further!

Read the Using ssh keys section if you don't already know what ssh keys are

Do not lose the (existing) ssh keys files you have, or the keys that you will create
It is recommended to keep a copy of these files on another computer!

- **Do not forget** the passphrase that will be used to unlock the private key
 - If you save the passphrase in a file, **do not** put this file in the same place as the ssh keys
 - Read Do not forget your passphrase! if you need some advice about passphrases
- The best thing to do is probably to **store the** *key* **files in the standard <u>ssh</u> <u>configuration directory</u> of each desktop/laptop/servers you use!**

Converting existing ssh keys with PuTTYgen

If you already have a private ssh key generated on another computer (e.g. an id_ed25519 text file), you just have to use PuTTYgen to **import the existing private key**, and then export it to a *converted* id_ed25519.ppk file that Pageant can use

- Move the id_ed25519 key file to the Windows ssh configuration directory
 - ⇒ C:\Users\your_windows_login\.ssh\id_ed25519
- Launch the PuTTY Key Generator: $\texttt{Start} \Rightarrow \texttt{PuTTY} \Rightarrow \texttt{PuTTYgen}$
- Open the Conversions \Rightarrow Import key menu

| PuTTY Ke | y General | tor | | | 7 | 3 |
|---|-------------------------|---|---------------------------|---------------------|------------------|---|
| le Key C | onversio | ns Help | | | | |
| Key Import key Public ke Export OpenSSH key set=e425 Export OpenSSH key (force new file format) Export ssh-com key Export ssh-com key | | at) (Scquq | Scquq/mtG2Evw(LNmY eddsa- | | | |
| Key fingerpri Key commer Key passphr | nt: [t: [ase: [| sah-ed.25519 255 : eddsa k.ey-202303 | 5HA256.PUq/3e06+Je 110 | in+u2HvBcl+urASINin | gloZDeKdgf2nSI | |
| Confirm peer | phrase: | ••••• | | | | |
| Actions Generate a p | ubic/pn | rate key pair | | | Generate | |
| Load an exis | ting prival | te key file | | | Load | |
| Save the ge | nerated k | ey | | Save public key | Save private key | |
| Parameters | | | | | | |
| Type of key ORSA | to general | ODSA | OECDSA | ● EdDSA | O SSH-1 (RSA) | |
| | | | | | | |

- Select the existing id_ed25519 private key file (or another valid private key) and type the passphrase to unlock and import it
- Click on the Save private key button, and create an id_ed25519.ppk file in the Windows ssh configuration directory
 - \Rightarrow C:\Users\your_windows_login\.ssh\id_ed25519.ppk

Creating ssh keys with PuTTYgen

If you don't already have an existing set of *recent-enough* ssh keys, follow the steps below to **create a set of private and public keys**.

Notes:

- by *recent-enough*, we mean ssh keys of type *rsa* and preferably *ed25519* (*dsa* is deprecated)
- extra technical details (that you can probably safely ignore) are available in the official <u>Using PuTTYgen</u>, the PuTTY key generator [https://the.earth.li/~sgtatham/putty/0.78/htmldoc/Chapter8.html#pubkey-puttygen] documentation

Steps:

- Launch the PuTTY Key Generator: Start \Rightarrow PuTTY \Rightarrow PuTTYgen
- Make sure that the selected *Type of key to generate* (at the bottom of the PuTTYgen window) is EdDSA (short for *Edwards-curve DSA*), with the default 255 bits.

This will generate *ed25519* keys that are now recommended on the IPSL servers

| PuTTY Key Generator | | | | | > | | |
|---|--------------------|--------------------|-------------------------|------------------|---|--|--|
| le Key Conversio | ons Help | | | | | | |
| Key | | | | | | | |
| Public key for pasting | into OpenSSH aut | norized_keys file: | | | | | |
| ssh-ed25519 AAAAO key-20230310 | 3NzaC1IZDI1NTE | AAAAIAsiYyl/X4RkW | 173eoFqd53II/g6cquq/mtG | 2EvwjLNmY eddsa- | ^ | | |
| | | | | | ~ | | |
| Key fingerprint: ssh-ed25519 255 SHA256:PUqI3c06+Jdm+u2HvBcl+urA6IMrqdoZDeKdlgf2mSI | | | | | | | |
| Key comment: | eddsa-key-20230310 | | | | | | |
| Key passphrase: | | | | | | | |
| Confirm passphrase: | | | | | | | |
| Actions | | | | | | | |
| Generate a public/private key pair Generate | | | | | | | |
| Load an existing private key file Load | | | | | | | |
| Save the generated key | | | Save public key | Save private key | | | |
| Parameters | | | | | | | |
| Type of key to genera ORSA | o DSA | OECDSA | EdDSA | O SSH-1 (RSA) | | | |
| | | | | | | | |

- You could also use RSA and 4096 bits, but ed25519 keys are now recommended to access the <u>IPSL servers</u> [https://documentations.ipsl.fr/spirit/spirit_clusters/head_nodes.html]
- Click on the Generate button and move your mouse to generate some random information
- Type your Key passphrase and confirm it
 - Read Do not forget your passphrase! if you need some advice about passphrases
- Click on the Save private key button, and create the id_ed25519.ppk Pageant private key file
 - We recommend that you save this file in the the Windows <u>ssh configuration directory</u> ⇒ C:\Users\your_windows_login\.ssh\id_ed25519.ppk
 - Note: files with a .ppk extension can only be used by PuTTY/pageant. That's why you also need to *export* the private key, as shown below
- Important! Click Conversions⇒Export OpenSSH Key and create the id_ed25519 standard *private* key file (a text file with **no**.ppk extension)
 - \Rightarrow C:\Users\your_windows_login\.ssh\id_ed25519
 - You will not need this file when you use PuTTY, but you may need to use this private key in a standard text format later, on Linux computers/servers
- Open a text editor and create the id_ed25519.pub standard public key file
 - \Rightarrow C:\Users\your_windows_login\.ssh\id_ed25519.pub
 - Save the content of the Public key for pasting into OpenSSH authorized_keys file field in the id_ed25519.pub file

Something looking like

ssh-ed25519 AAAAC3NzaC1lZDI[... lots of characters ...]vwjLNmY eddsa-key-20230310

- This is the *public* key that you will need to <u>install</u> on all the remote Linux server that you want to connect to using the ssh agent, instead of typing your password
- WARNING! Do **not** use the Save public key button to create the public key file, because the resulting file will not be standard enough to be used directly on Linux computers

Using the private key in Pageant

We assume that the **private key file** is available locally in <some_disk_different_from_c>:\Users\<your_login>\ssh\

- Start Pageant and open the Pageant Key List window by:
 - Double-clicking (left mouse button) on Pageant
 - Or right-clicking on Pageant and choosing View keys
- Click on Add Key, navigate to the directory where you have stored the .ppk converted private key file (e.g. \Users\ <your_login>\ssh\), open it and type your passphrase. You can Close the Pageant Key List once the key appears there

| Pageant K | ey List | | 7 | × |
|----------------------------|---------|--|-------|---|
| ssh das | 1024 | SH4256.vC3Me8e9WFR881gWbZvFveYgYrtMg52Acu7c1Q4 imported openaethikey | , | |
| Fingerprint Add Help | Key | SHA256 V Add Key lenospted) Perencept | Renov | |

• If everything was done correctly, you should now be able to open the *Sessions* defined in Pageant, on remote servers where the **public key matching the private key** used in Pageant was installed correctly

[PMIP3 Wiki Home] - [Help!] - [Wiki syntax]

other/putty_conf.txt · Last modified: 2024/05/29 15:43 by jypeter