SSH Academy

PuTTY - Secure Download

PuTTY is a popular SSH, Telnet, and SFTP client for Windows. It is typically used for remote access to server computers over a network using the SSH protocol. This is the download page.

For more information on PuTTY, see the **PuTTY page**. For information on SSH (Secure Shell), see **here**. For information on Telnet, see **here**. For information on SFTP secure file transfers, see **here**.

Contents

Download PuTTY installation package for Windows

Master download site

Simon Tatham publishes new PuTTY versions on his personal home page.

Installation and setup instructions

- Installation instructions for Windows
- Setting up public key authentication using PuTTYgen

Verifying release signatures

The releases are signed with GPG, using the PuTTY release key.

To verify the signatures, you need the gpg tool. On Debian-based Linux, it can be installed with `aptitude install gnupg`. On Red Hat 7, it can be installed with `yum install gnupg2`.

To import the signature key into GPG, use:

```
gpg --import putty-release-2015.asc
```

To check the signature of a file, use:

```
gpg --verify <signaturefile> <datafile>
```

For example:

```
gpg --verify putty-64bit-0.69-installer.msi.gpg putty-64bit-0.69-installer.msi
```

Package contents: putty.exe, puttygen.exe, psftp.exe, pscp.exe, pagent.exe

The installation package includes `putty.exe`, `puttygen.exe`, `psftp.exe`, `pscp.exe`, and `pagent.exe`.

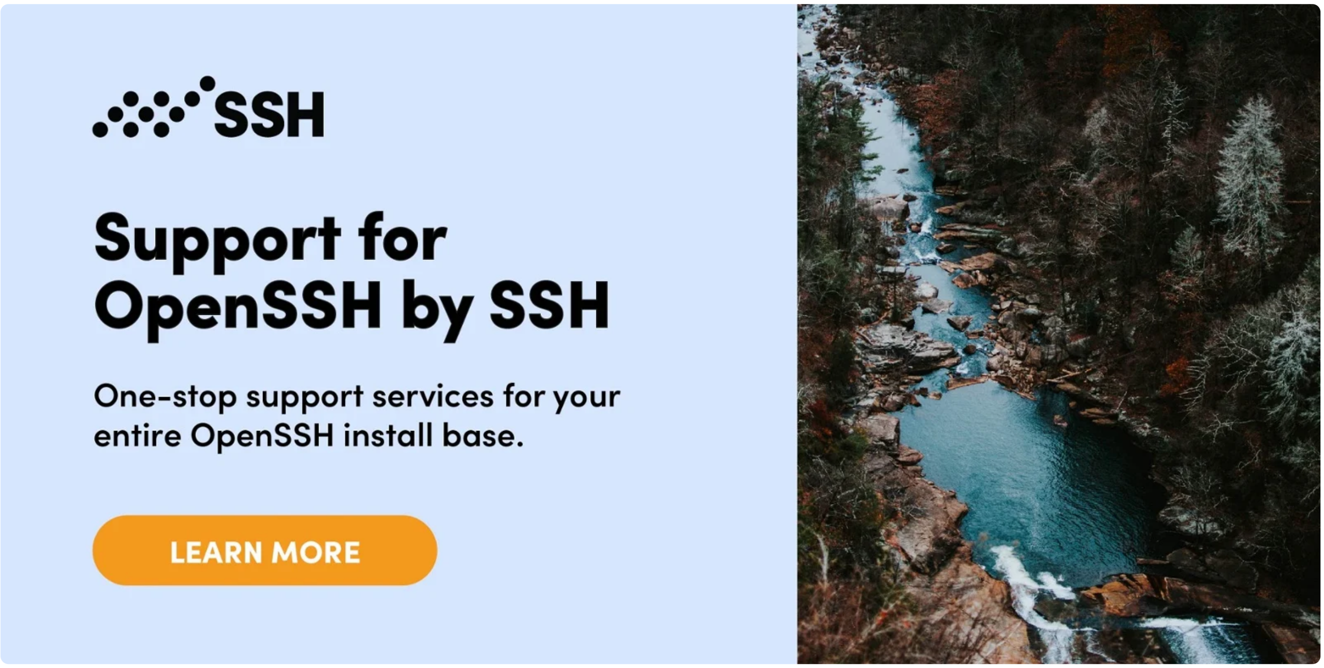
`putty.exe` is the main executable for the terminal client. It can also be used standalone, without the installation package, by simply copying the executable to a USB stick and running it on a new machine. This way, the user can carry the executable with them. However, this should not be assumed to provide great security - malware on the machine where it is used can still compromise the software (cf. CIA hacking tool bothanspy) and viruses may get installed on the USB stick whenever it is inserted in a new machine.

`puttygen.exe` is can be used for generating SSH keys on Windows. See the separate puttygen page on how to create and set up SSH keys with it.

`psftp.exe` is an SFTP file transfer client. It only works on the command line, and does not support graphically dragging and dropping files between systems. See Tectia SSH if you'd like that functionality.

pscp.exe is a command line SCP client.

pagent.exe is an SSH agent for PuTTY. Keys are first created with puttygen.exe and can then be loaded into pagent for automating logins and for implementing single sign-on.


SSH
Support for OpenSSH by SSH
One-stop support services for your entire OpenSSH install base.
LEARN MORE

Alternatives

For other SSH clients and comparison, see the SSH clients page. Several more modern alternatives are available.

Server for Windows or other platforms

You don't need to worry about a server if you are going to connect to a school or work server. However, if you are planning to use PuTTY to log into your own systems, then you may need to install and enable a server.

Most Linux and Unix systems come with OpenSSH preinstalled. On some distributions, you may need to install the server. On Debian-derived systems, the following will install the server:

```
sudo aptitude install openssh-server
```

On Red Hat systems, the following will install the server:

```
sudo yum install openssh-server
```

Depending on the system, you may also need to start the server if you don't want to reboot. The following should work on most systems:

```
sudo service sshd restart
```

For Windows, the Tectia SSH is a popular choice and comes with commercial support services. It also runs on IBM z/OS mainframes. Unix/Linux are available with support for business-critical applications.

SSH key management needs attention

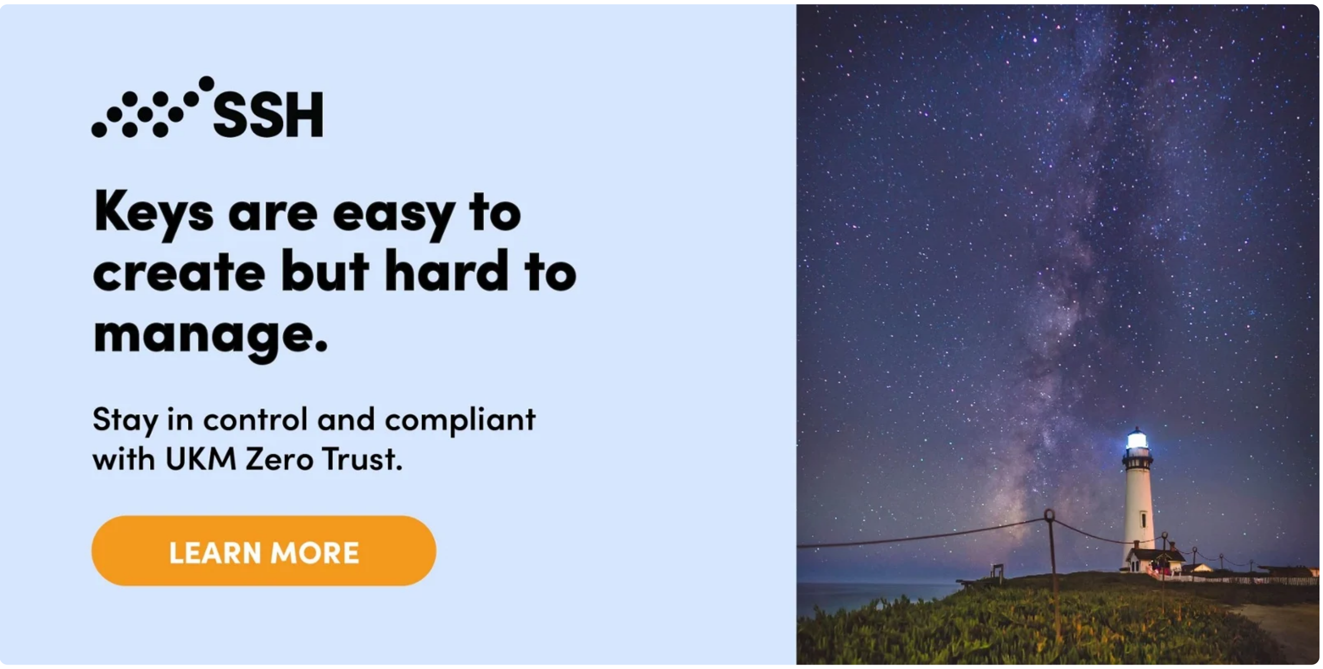
SSH is often used with public key authentication to implement automation and single sign-on.

Public key authentication uses a new kind of access credential, the SSH key, for authentication. It is much more secure than traditional password authentication, especially compared to hard-coded passwords in scripts, but the keys need proper management.

Most organizations with more than a hundred servers have large numbers of SSH keys. Usually, these keys have not been properly managed and audited. An SSH risk assessment is recommended. Organizations should consider deploying key management software to establish proper provisioning, termination, and monitoring for key-based access.

Risks of unmanaged SSH keys include uncontrolled attack spread across the server infrstructure, including to disaster recovery data centers and backup systems.

Organizations should also be aware of security risks related to SSH port forwarding. It is a technology that has many good uses, but it can also enable unfettered access across firewalls. Employees and attackers can leave tunnels back into the internal network from the public Internet. This particularly affects organizations using cloud computing services.



Using telnet is not recommended

In addition to SSH, the PuTTY can be used as a **telnet** client. Telnet is insecure. Its use is not recommended.

The main problem with `telnet` is that it transmits all passwords and any transmitted data in the clear. Anyone with access to any computer on the same network can steal user names and passwords that are transmitted. Such **password sniffing** attacks were very common on the Internet already in the 1990s.

`Telnet` sessions can also be **hijacked** in the network. Attackers can inject their own commands into `telnet` sessions. Protection from such attacks was the main reason why **Tatu Ylonen** developed SSH as a replacement for `telnet` in the first place. Use of `telnet` has not been recommended for 20 years.

SFTP file transfer support

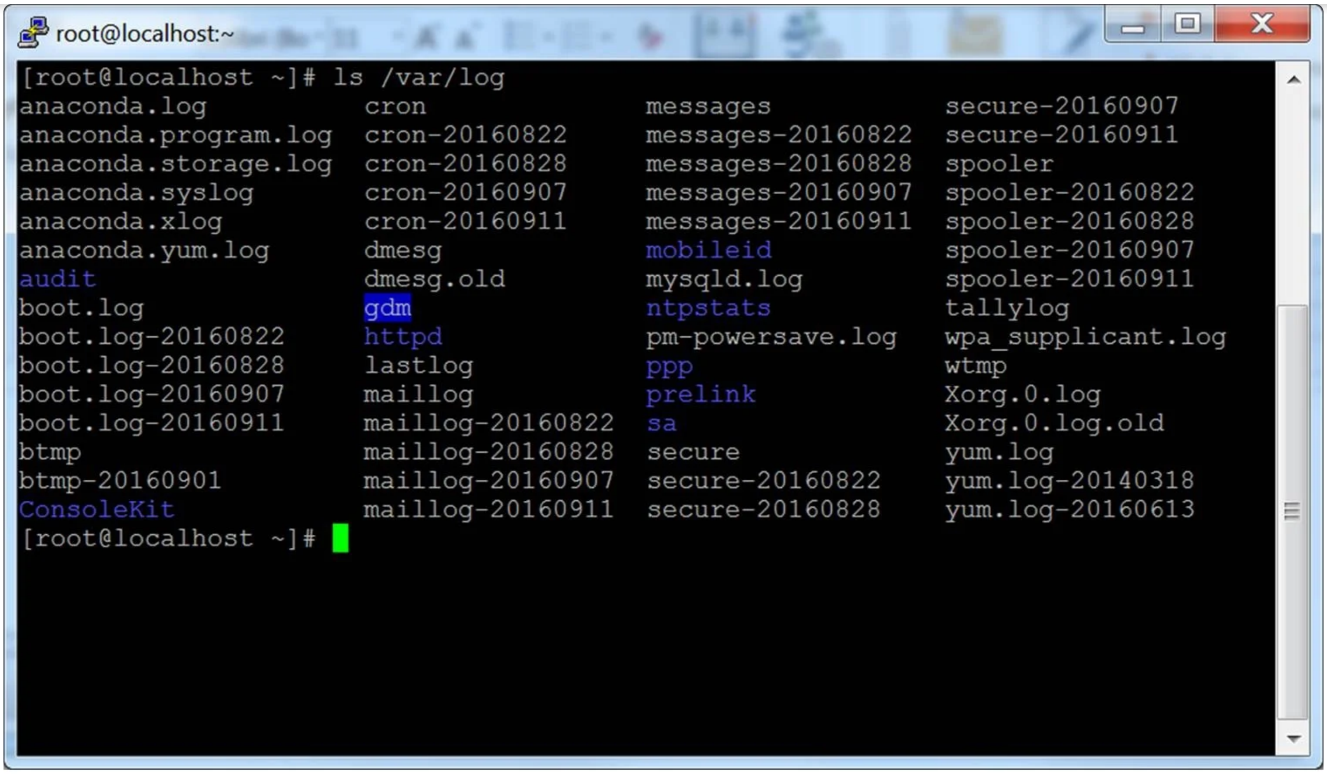
File transfer support is implemented as a separate program, `PSFTP.` It is available only as a command-line tool. There is no graphical user interface for file transfers.

SCP file transfers are supported via the PSCP program. This is also command-line only.

Modern implementations, such as **Tectia SSH**, have integrated file transfers in the terminal client.

Screenshots

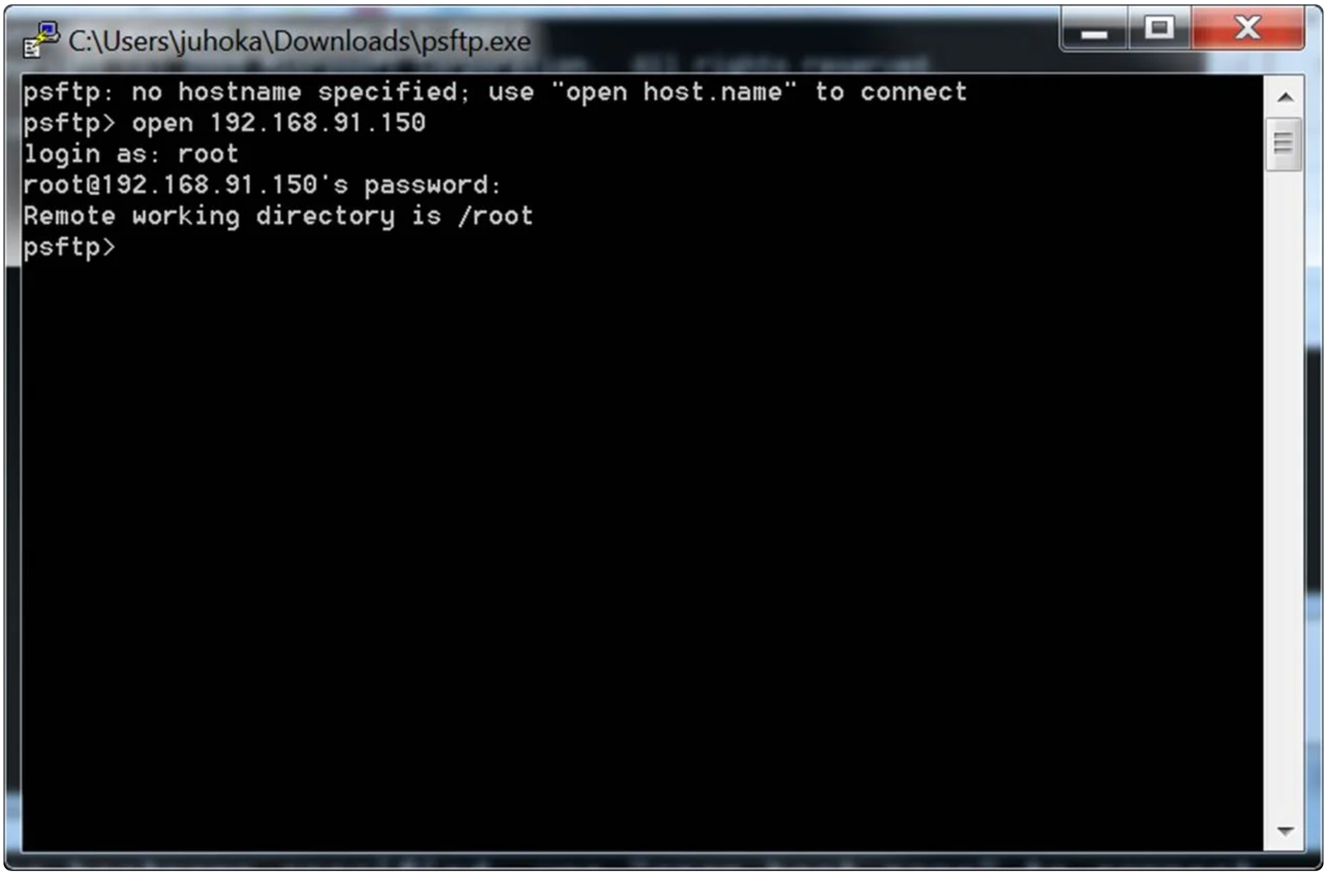
PuTTY terminal window



root@localhost:~

```
[root@localhost ~]# ls /var/log
anaconda.log           cron             messages          secure-20160907
anaconda.program.log   cron-20160822    messages-20160822 secure-20160911
anaconda.storage.log   cron-20160828    messages-20160828 spooler
anaconda.syslog        cron-20160907    messages-20160907 spooler-20160822
anaconda.xlog          cron-20160911    messages-20160911 spooler-20160828
anaconda.yum.log       dmesg            mobileid          spooler-20160907
audit                  dmesg.old        mysqld.log        spooler-20160911
boot.log               gdm              ntpstats          tallylog
boot.log-20160822      httpd            pm-powersave.log  wpa_supplicant.log
boot.log-20160828      lastlog          ppp               wtmp
boot.log-20160907      maillog          prelink           Xorg.0.log
boot.log-20160911      maillog-20160822 sa                Xorg.0.log.old
btmp                   maillog-20160828 secure            yum.log
btmp-20160901          maillog-20160907 secure-20160822   yum.log-20140318
ConsoleKit             maillog-20160911 secure-20160828   yum.log-20160613
[root@localhost ~]#
```

PSFTP command line Use



C:\Users\juhoka\Downloads\psftp.exe

```
psftp: no hostname specified; use "open host.name" to connect
psftp> open 192.168.91.150
login as: root
root@192.168.91.150's password:
Remote working directory is /root
psftp>
```

We at SSH secure communications between systems, automated applications, and people. We strive to build future-proof and safe communications for businesses and organizations to grow safely in the digital world.

Solutions

Zero Trust Suite

Zero Trust Suite & Entra ID Integration

Quantum-Safe Cryptography (QSC)

Secure Collaboration 2024

Security Risk Mitigation

OT security

MSP Security

Just-in-Time Access

Secure vendor access

Hybrid cloud security

Credentials & Secrets Management

IT Audits & Compliance

Products

PrivX™ Hybrid PAM

UKM Zero Trust™

Tectia SSH Client/Server™

Tectia™ z/OS

SSH Secure Collaboration 2024

Secure Mail 2024

Secure Sign

NQX™ Quantum-Safe

Services

SSH Risk Assessment™

Professional Services

Support

Resources

Careers

References

Downloads

Manuals

Events & Webinars

Blog

Company

About us

Contact

Investors

Partners

Press

Stay on top of the latest in cybersecurity

Be the first to know about SSH's new solutions, product updates, new features, and other SSH news!