What is SSH (Secure Shell)? | SSH Academy

By Admin

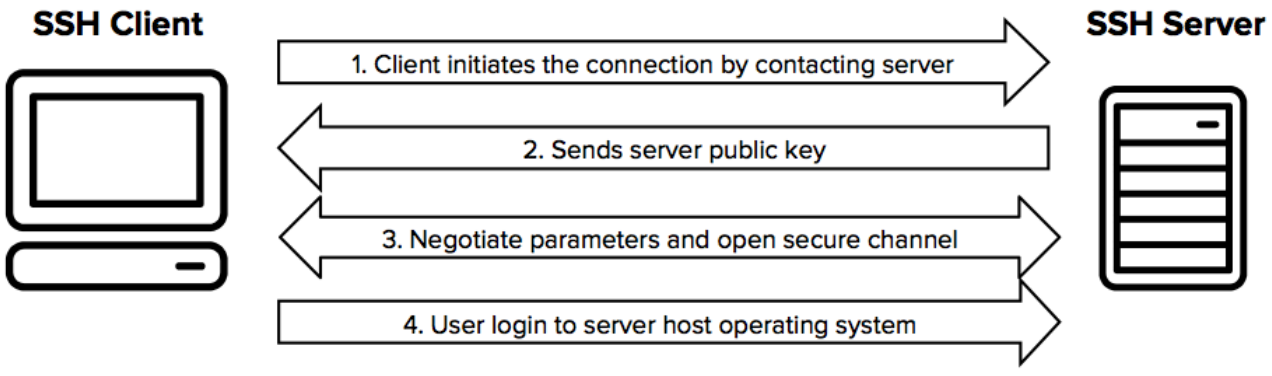
Published: 2019-08-27 · Archived: 2026-04-05 17:52:18 UTC

This is the start page for the SSH (Secure Shell) protocol, software, and related information. SSH is a software package that enables secure system administration and file transfers over insecure networks. It is used in nearly every data center and in every large enterprise.

This page was created by the inventor of SSH, Tatu Ylonen (twitter: @tjssh). He wrote ssh-1.x and ssh-2.x, and still works on related topics. The open source OpenSSH implementation is based on his free version.

The SSH protocol

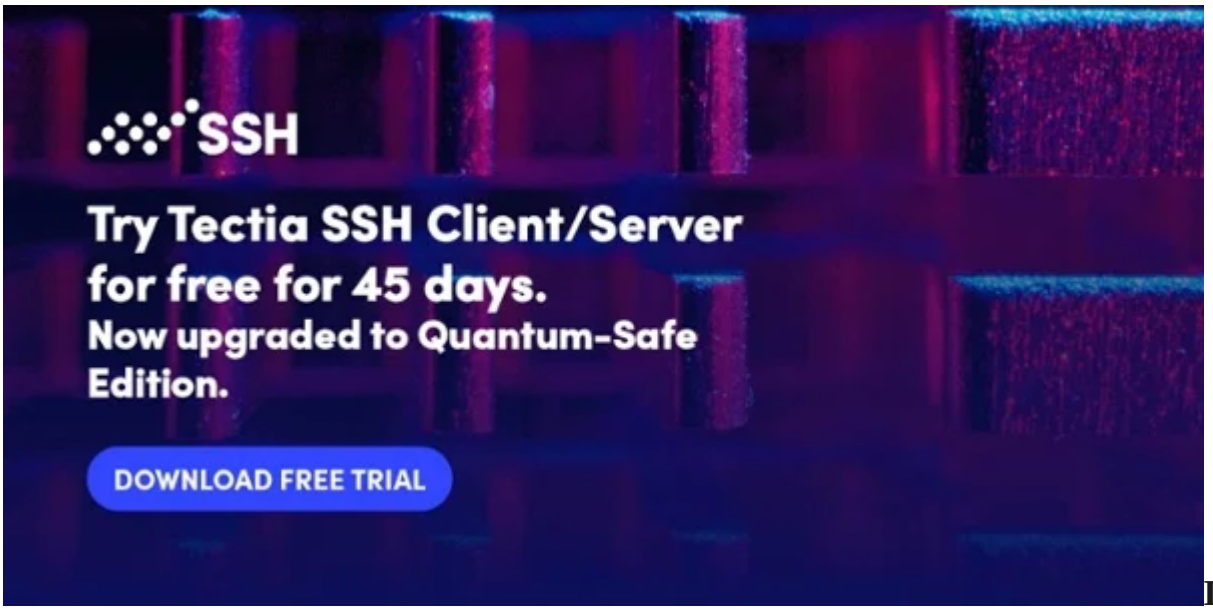
The SSH protocol uses encryption to secure the connection between a client and a server. All user authentication, commands, output, and file transfers are encrypted to protect against attacks in the network. For details of how the SSH protocol works, see the protocol page. To understand the SSH File Transfer Protocol, see the SFTP page.



Download client software

Here you can find links to download various free SSH implementations. We offer various free SSH implementations for download, and provide links to commercial implementations.

- Download PuTTY
- Download SSH clients



List of SSH implementations

We list various SSH implementations here. Feel free to submit additional implementations for this page. For many implementations we offer a review, installation instructions, guidance, and/or how-tos on this site.

- Tectia SSH client & server for Windows, Unix, Linux - with 24x7 support
- Tectia SSH for IBM z/OS client & server for IBM z/OS mainframes - with 24x7 support
- PuTTY client for Windows and Linux
- WinSCP client for Windows
- CyberDuck client for Mac
- OpenSSH server for Unix, Linux
- Overview of client alternatives
- Overview of server alternatives
- Windows SSH alternatives
- PrivX™ Privileged Access Management for multi-cloud

Running & configuring SSH

This section contains links topics around using, configuring, and administering SSH.

- Command line options
- Tectia SSH manuals
- sshd - The SSH server on Unix/Linux
- sshd_config - Server configuration file on Unix/Linux
- ssh_config - Client configuration file on Unix/Linux
- SSH port, and how it got that number

Security of SSH and attacks against it

The SSH protocol is believed to be secure against cryptographic attacks on the network, provided keys and credentials are properly managed. However, we do not recommend using `diffie-hellman-group1-sha1` key exchange. It uses a 768 bit Diffie-Hellman group, which may be breakable by governments today. Larger groups are probably ok. Recent OpenSSH versions have disabled this group by default. See sshd_config for configuring what key exchanges to use.

- Analysis of BothanSpy and Gyrfalcon - the presumed CIA hacking tools
- Man-in-the-middle attacks against SSH
- Imperfect forward secrecy - How Diffie-Hellman fails in practice

Automate with SSH keys, but manage them

SSH keys can be used to automate access to servers. They are commonly used in scripts, backup systems, configuration management tools, and by developers and sysadmins. They also provide single sign-on, allowing the

user to move between his/her accounts without having to type a password every time. This works even across organizational boundaries, and is highly convenient.

However, unmanaged SSH keys can become a major risk in larger organizations.

- What is an SSH key
- What SSH life cycle management means
- Universal SSH Key Manager
- ssh-keygen - Create keys
- ssh-copy-id - Provision access on servers
- authorized_keys - Authorized keys file format

The PrivX On-Demand Access Manager can be used as an alternative for SSH keys, eliminating the need for permanent keys and passwords on servers entirely.

History of the SSH protocol

The Secure Shell protocol was originally developed by Tatu Ylonen in 1995 in response to a hacking incident in the Finnish university network. A password sniffer had been installed on a server connected directly to the backbone, and when it was discovered, it had thousands of usernames and passwords in its database, including several from Ylonen's company.

That incident triggered Ylonen to study cryptography and develop a solution he could use himself for remote login over the Internet safely. His friends proposed additional features, and three months later, in July 1995, Ylonen published the first version as open source. It became OpenSSH. Later he took the protocol for standardization at the IETF and designed the SSH File Transfer Protocol (SFTP). He founded SSH Communications Security Corp in December 1995 to provide commercial support for the protocol.

Ylonen still works on topics related to Secure Shell, particularly around key management, as well as broader cybersecurity topics.

Today, the protocol is used for managing more than half of world's web servers and practically every Unix or Linux computer, on-premise and in the cloud. Information security specialists and system administrators use it to configure, manage, maintain, and operate most firewalls, routers, switches, and servers in the millions of mission-critical networks and environments of our digital world. It is also embedded inside many file transfer and systems management solutions.

The new protocol replaced several legacy tools and protocols, including telnet, ftp, FTP/S, rlogin, rsh, and rcp.
