

Secure Shell (SSH)

[Return to Glossary](#)

Secure Shell (SSH) is a cryptographic network [Protocol](#) for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH.

SSH provides a secure channel over an unsecured network by using a [Client-Server](#) architecture, connecting an SSH [Client](#) application with an SSH [Server](#). The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2. The standard TCP port for SSH is 22. SSH is generally used to access Unix-like operating systems, but it can also be used on Microsoft Windows. Windows 10 uses OpenSSH as its default SSH client and SSH server.

Despite popular misconception, SSH is not an implementation of Telnet it is a replacement with cryptography provided by the [Secure Sockets Layer \(SSL\)](#).

Source: [https://en.wikipedia.org/wiki/SSH_\(Secure_Shell\)](https://en.wikipedia.org/wiki/SSH_(Secure_Shell))

From:

<https://www.omgwiki.org/dido/> - **DIDO Wiki**

Permanent link:

https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:s:ssh&rev=1605472910

Last update: **2020/11/15 15:41**

