- **Screenshots**
- **Translations**
- **Support**
- **Forum**
- **Tracker**
- **History**

Contents » Getting Started » **Protocols** »

Understanding SSH

SSH is a cryptographically protected remote login protocol that replaces insecure telnet and rlogin protocols. It provides strong protection against password sniffing and third party session monitoring, better protecting your authentication credentials and privacy. In addition, SSH offers additional authentication methods that are considered more secure than passwords, such as **public key authentication** and extensive protection against spoofing.

The SSH employs a public key cryptography that uses **two keys pairs, for host and user**.

Authentication in SSH

SSH servers offer the client a selection of authentication methods. The server advertises what it supports, and the client attempts to authenticate over each method that it can support. Generally, the client will choose methods that are the least intrusive to the user, if they are available. In most cases, the client provides the option to choose which methods can be used. In WinSCP, you can configure this on ***SSH > Authentication page*** of Advanced Site Settings dialog.

The actual order of authentication methods is as follows: **GSSAPI** (SSH-2 only), **public key** (using **Pageant**), public key (using **configured file**), keyboard-interactive (SSH-2 only), TIS or Cryptocard (SSH-1 only), password.

Verifying the Host Key

To prevent **man-in-the-middle attacks [https://en.wikipedia.org/wiki/Man-in-the-middle_attack]**, each SSH server has a unique identifying code, called a host key. These keys prevent a server from forging another server's key. If you connect to a server for the first time or if the server presets a different key then previously, WinSCP will prompt you to **verify the key**.

Encryption in SSH

SSH clients and servers can use a number of encryption methods. Most widely used encryption methods in SSH-2 are AES and Blowfish. By default, AES is used if supported by the server. While AES is considered to be highly secure, AES encryption requires substantial processor overhead. Blowfish is also considered secure, but with less computational overhead, it's also theoretically easier to perform a brute-force attack. Depending on your security and performance requirements, you may wish to configure WinSCP to prefer the Blowfish algorithm. 3DES and DES are used with SSH-1 servers. DES is widely regarded as insecure, as the resources to perform an exhaustive brute-force attack have been well within the realm of commercial feasibility for some time.

SSH Protocols

Two major versions of the SSH protocol exist, SSH-2 and SSH-1. Most SSH servers nowadays allow modern and secure SSH-2 only.

WinSCP's default setting is to use SSH-2. If you need to use deprecated and insecure SSH-1 at all, you can configure this in **SSH preferences**.

Compression

SSH supports data stream compression between the client and the server. On slow links, this may increase throughput, while in faster connections the added CPU overhead may actually result in slower transfers, particularly depending on the data type you're transferring. Large text files may still benefit significantly, while binaries may transfer more slowly. You may want to experiment to find what works best in your situation. Compression may also improve security slightly, in part by rendering known cyphertext attacks more difficult and by providing less data for cryptanalysis.

ssh.txt · Last modified: 2017-01-07 by martin