ssh

Secure Shell is a protocol used to securely log onto remote systems.
It can be used for logging or executing commands on a remote server.

- Connect to a remote server:

`ssh {{username}}@{{remote_host}}`

- Connect to a remote server with a specific identity (private key):

`ssh -i {{path/to/key_file}} {{username}}@{{remote_host}}`

- Connect to a remote server using a specific port:

`ssh {{username}}@{{remote_host}} -p {{2222}}`

- Run a command on a remote server:

`ssh {{remote_host}} {{command -with -flags}}`

- SSH tunneling: Dynamic port forwarding (SOCKS proxy on localhost:9999):

`ssh -D {{9999}} -C {{username}}@{{remote_host}}`

- SSH tunneling: Forward a specific port (localhost:9999 to slashdot.org:80):

`ssh -L {{9999}}:slashdot.org:80 {{username}}@{{remote_host}}`

- Enable the option to forward the authentication information to the remote machine (see `man ssh_config` for available options):

`ssh -o "ForwardAgent=yes" {{username}}@{{remote_host}}`