

## Access to the unit via CLI



Successfully pass the free certification exam at IW Academy and become an Infinet Certified Engineer.

[To the certification exam](#)

Remote device control by the command line is available using Telnet and SSH protocols.

In order to connect to the unit use 10.10.10.1 IP-address that is configured for the Ethernet interface of the device by default.

If all above are completed correctly, you will see the **WanFlex OS** prompt.

### telnet

Sets up a connection with a remote host specified by the IP address in the terminal emulation mode. The "*telnet*" command uses transparent symbols stream without any intermediate interpretation; therefore, the terminal type is defined by the terminal from which the command has been executed. To interrupt the terminal emulation session, press "Ctrl/D".

#### Syntax:

```
telnet address [port] [-S source]
```

Parameter	Description
<i>port</i>	Telnet port.
<i>-S source</i>	Device's IP address.


### SSH protocol

SSH (Secure Shell) protocol allows secure remote management of network devices. Its functionality is similar to Telnet protocol but, as opposed to Telnet, SSH encodes all protocol messages/datagrams including transmitted passwords. SSH Server (SSH daemon) configuration is performed using "*sshd*" command. By default, the SSH Server is disabled.

#### Syntax:

```
sshd -help, -h
sshd -port=PORT
sshd -window=SIZE
sshd -keepalive=TIME
sshd -banner=on | off
sshd -log-level={emerg|alert|crit|error|warning|notice|info|debug|LEVEL} [notice]
sshd -algo-list
sshd -kex-algos[=ALGO-LIST]
sshd -hostkey-algos[=ALGO-LIST]
sshd -cipher-algos[=ALGO-LIST]
sshd -hash-algos[=ALGO-LIST]
sshd -comp-algos[=ALGO-LIST]
sshd -auth-methods[=AUTH-METHODS-LIST]
sshd start
sshd stop
sshd newkeys
sshd pub[key] {sh[ow] | cl[ear] | de[lete] N}
sshd pub[key] {in[stall] | im[port] [LOGIN[:PASSWORD]@]HOST/FILE} [COMMENT]
```

Parameter	Description
<i>-help, -h</i>	Displays the command syntax.

<b>-port=PORT</b>	SSH Server TCP port number, which is used to receive connections SSH, by default is 22.
<b>-window=SIZE</b>	Allows changing SSH Server internal receiving window size in bytes. SSH Server window size defines maximum allowed bandwidth for "SSH Client - SSH Server" data channel. By default, SSH Server window size is 24576 bytes.
<b>-keepalive=TIME</b>	Sets session activity check duration period in seconds. By default server doesn't make activity check ("0" value).
<b>-banner=on   off</b>	Shows/hide IW WANFlex SSH information banner after login.
<b>-log-level={emerg alert crit error warning notice info debug LEVEL}[notice]</b>	<p>Allows choosing logging levels of the SSH Server service information that will be written into the system log, to manage system log please use "sys log" command.</p> <p>Different levels of logging can be chosen by "emerg", "alert", "error", "warning", "notice", "info", "debug" parameters or specified by the number of the needed level (from 0 to 7) using numeric "LEVEL" parameter. By default, "info" (6th level) is chosen.</p>
<b>-algo-list</b>	Shows a list of all available SSH algorithms for key exchange ( <i>kex</i> ), authentication ( <i>host key</i> ), data encoding (cipher), data verification ( <i>hash</i> ) and data compression ( <i>compress</i> ).
<b>-kex-algos[=ALGO-LIST]</b>	Choosing kex algorithms from the list of algorithms (ALGO-LIST), to be used in SSH key exchange process.
<b>-hostkey-algos[=ALGO-LIST]</b>	Choosing host key algorithms from the list of algorithms (ALGO-LIST), to be used in SSH Server-Client authentication process.
<b>-cipher-algos[=ALGO-LIST]</b>	Choosing cipher algorithms from the list of algorithms (ALGO-LIST), to be used in SSH data encoding.
<b>-hash-algos[=ALGO-LIST]</b>	Choosing hash algorithms from the list of algorithms (ALGO-LIST), to be used in SSH data verification.
<b>-comp-algos[=ALGO-LIST]</b>	Choosing compression algorithms from the list of algorithms (ALGO-LIST), to be used in SSH data compression.
<b>-auth-methods[=AUTH-METHODS-LIST]</b>	<p>Choosing an available authentication method from the (AUTH-METHODS-LIST) list.</p> <p>An "all" value enables all authentication methods (set by default).</p>
<b>start</b>	Starts SSH Server.
<b>stop</b>	Stops SSH Server.
<b>newkeys</b>	<p>Host Keys re-generation.</p> <div>  <b>NOTE</b>            When first-time started SSH Server generates DSS and RSA Host Keys to be used for public key based SSH Server authentication.         </div>
<b>pub[key] {show   clear   delete N}</b>	<ul style="list-style-type: none"> <li>"show" – shows SSH Client's public keys that are registered in the SSH Server list.</li> <li>"clear" – deletes all the SSH Client's public keys from the SSH Server.</li> <li>"delete" – deletes a certain SSH Client's public key from the SSH Server list. Parameter "N" – is an index of the key in the list.</li> </ul>
<b>pub[key] {install   import} [LOGIN[:PASSWORD]@]HOST /FILE [COMMENT]</b>	<p>Allows enabling public key based authentication of SSH Clients. In the Public key authentication mode SSH Server authorize SSH Client bypassing password login procedure. This mode is enabled automatically once a public key of the SSH Client is cached in SSH Server's registry:</p> <ul style="list-style-type: none"> <li>"install" – sets the SSH client public key in the SSH server registry.</li> <li>"import" – imports an SSH client's public key into the SSH server registry from a remote FTP server:             <ul style="list-style-type: none"> <li>"HOST" – remote FTP server IP address.</li> <li>"FILE" – file containing SSH Client's RSA/DSS public key in OpenSSH or SSH2 format. If login and password are set on the remote FTP server they should be specified as "LOGIN" and "PASSWORD" parameters.</li> <li>"COMMENT" – allows adding a comment to the public key entry in the SSH Server list of clients public keys. By default, a comment with clients IP address or FTP IP address from where the key was obtained is added.</li> </ul> </li> </ul>



### NOTE

By default SSH Server applies only password authentication. However, this may not be enough to provide the necessary security level. InfiNet Wireless devices have several built-in SSH authentication methods, which are managed by "*sshd pubkey*" and "*sshd -auth-methods*" command. At the same time, an SSH Server will keep the connected SSH client public key.

## Command Line

For device's management and configuration a Unix-like command line language is used. Every command starts having the power right after "**Enter**" key is pressed. However, each command lifetime duration is limited within one configuration session. In order to save a current configuration "*config save*" command is used.

Several commands can be grouped in one line using ";" character. If a wrong-syntax line is met in the group, the rest of the string is checked anyway and the wrong command is ignored. Command name can be shortened unless the ambiguity occurs.

If your terminal supports VT100 or ANSI standard you can move around the list of recently executed commands using cursor keys. Numbered list of these commands can be reviewed by "*!h*" command. Any command from this list can be available using "*!<NUMBER>*" command. "**TAB**" key performs substring search of recently executed commands.

"**Ctrl/R**" combination refreshes the command string if its content was disturbed by system messages.

The command executed with no arguments prints a short hint about its keys, parameters and syntax.

Context help can be obtained by printing "?" in any position of the line.