

SSH on dedicated server

SSH is installed on every server. It ensures secure connection to the server and gives you full control over your machine.

SSH applications

- for Windows

Putty (free):

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

SecureCRT (paid):

<http://www.vandyke.com/products/securecrt/>

- for Mac

http://directory.google.com/Top/Computers/Security/Products_and_Tools/Cryptography/SSH/Clients/Macintosh/?tc=1

– Terminal is available with Mac OS X and is automatically installed.

http://pro.wanadoo.fr/chombier/MacSSH/SSH_info.html

<http://sourceforge.net/projects/macssh/>

- for Linux

Openssh (free):<http://www.openssh.org>

First connection

To connect with the server via ssh you need to know:

- server's IP or its name
- server's root password

Example of connection with openssh :

```
$ ssh root@bmw
```

```
The authenticity of host 'bmw (213.186.32.1)' can't be established.
```

```
RSA key fingerprint is a9:bb:55:35:86:4d:ca:81:7f:9e:2b:2c:79:10:96:3c.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added 'bmw,213.186.32.1' (RSA) to the list of known hosts.
```

```
Password:
```

```
$
```

During the connection your ssh application receives RSA key fingerprint, which is the server key. It is verified during every connection. If the key changes, you'll be informed about it. It means that something has changed on your server, for example the server has been reinstalled, or ssh server has been reinstalled or you have connected to the wrong server.

During the first connection you should accept the key which will be registered in your ssh application.

Next step

You may consult the manual which describes operations in shell under bash: ShellBash

Update

If you update ssh on your server, don't forget to enable telnet. Telnet is unsecured version of ssh and it doesn't allow direct connection as root. However it is an option that allow your access to the server in case of unsuccessful ssh update. to check your version of ssh insert **ssh -V**.

```
# ssh -V
```

```
OpenSSH_3.7.1p2, SSH protocols 1.5/2.0, OpenSSL 0.9.6i engine Feb 19 2003
```

OpenSSH lower than 3.7.1p2 are vulnerable to hack attempts. We advise you to update your server. Here are some tips: ReleasePatch.

Attention: Starting from 3.7.1p2 you should use UsePAM yes w /etc/ssh/sshd_config

If with this option ssh doesn't restart, it means that you don't have 3.7.1p2 version (update was unsuccessful).

Errors

If you have ssh version higher than 3.7, you may have problems with connection to your server if you use older version of ssh program for Windows. To avoid this problem, install the latest version of your application. If you use Putty, the connection should be done through SSH2. If you use SecureCRT, you need to configure primary authentication in "password". This problem is not related to the server but concerns the ssh application.