

Package SSHD - Secure Shell Daemon

Version 3.10.5

Frank Meyer
email: frank@fli4l.de

The fli4l-Team
email: team@fli4l.de

February 16, 2016

Contents

1	Documentation Of Package SSHD	3
1.1	SSHD - Secure Shell, Secure Copy	3
1.1.1	Installation Of The Secure-Shell-Daemon	3
1.1.2	Installation Of Dbclient	7
1.1.3	Installation Of A Plink Client	7
1.1.4	Installation Of A Sftp Server	7
1.1.5	Literature	7
	List of Figures	8
	List of Tables	9
	Index	10

1 Documentation Of Package SSHD

1.1 SSHD - Secure Shell, Secure Copy

A secure shell enables you to open an encrypted connection with the fli4l router. By using secure copy files can be transmitted encrypted to the fli4l router. If in addition [Public Key Login](#) (Page 5) is used commands and file transfers can be executed driven by scripts from “outside”. As of version 2.1.7 only a SSH2 server is existing.

1.1.1 Installation Of The Secure-Shell-Daemon

OPT_SSHD Default setting: `OPT_SSHD='no'`

If the router should be accessible via ssh set `OPT_SSHD` to `'yes'`. This will install the ssh server Dropbear on the fli4l router. It will also enable copying of files to the router.

SSHD_ALLOWPASSWORDLOGIN Default setting: `SSHD_ALLOWPASSWORDLOGIN='yes'`

If `SSHD_ALLOWPASSWORDLOGIN` is set to `'no'` fli4l won't allow ssh login via password anymore. Login can only be done via private/public key. This assumes that a [public key](#) (Page 5) is present on the router.

SSHD_CREATEHOSTKEYS Default setting: `SSHD_CREATEHOSTKEYS='no'`

A ssh server needs a so-called host key that is unique to identify itself to a ssh client. The package SSHD provides a host key to allow a first login to the router but this key should be replaced with a self-generated one only known to you as fast as possible. Generating your own host key is the only way to be prepared against so called man-in-the-middle attacks and thus is very important. SSH will notice if someone pretends to be your fli4l router because his host key will differ and will warn you about the host key changing.

Generating your own host key will be done automatically if `SSHD_CREATEHOSTKEYS` is set to `'yes'`. This is a challenging task and can prolong boot time for several minutes. If the fli4l router starts with `SSHD_CREATEHOSTKEYS` activated one (or more) host key(s) will be created in the directory `/tmp/ssh`. Keyfiles found there have to be copied over to your fli4l build directory under `etc/ssh` (on the PC where fli4l's boot medium is created). In my case a directory listing of `config.babel` looks like this:

Please note that under the directory `config.babel` a subdirectory `etc` exists with another subdirectory `ssh`. Generated host keys have to be placed there. As of fli4l version 2.1.5 files in your `config` directory will be preferred over the ones from the `opt` directory. With the next update of your fli4l boot medium the files from `config/etc/ssh` will be integrated and not those in `opt/etc/ssh`. In this way every fli4l router you configure can have its own unique host key. When creating the fli4l files there will appear a message „appending config specific files to opt.img ...“ towards the end. All files coming from the `config` directory instead of `opt` will be listed there.



Figure 1.1: Directory structure of fli4l

```
#
# appending config specific files to opt.img ...
#
etc/ssh/dropbear_dss_host_key
etc/ssh/dropbear_rsa_host_key
```

If you created a new host key set `SSHD_CREATEHOSTKEYS` back to 'no' to avoid creating another host key on every reboot.

If you log in to your fli4l router after updating the host key a warning message (depending on the ssh client you use) will appear to inform you about the changed host key. In this case this is normal because you just changed your host key. Follow the routine necessary for your ssh client to accept the changed host key permanently. If some time in the future you see this warning again you will have to check why it appears. Don't just accept a changed host key blindly!

```

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!    @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
ca:a4:ab:e7:af:d8:68:05:d3:1f:e6:15:08:d6:ed:36.
Please contact your system administrator.
Add correct host key in /home/babel/.ssh/known_hosts to get rid of this message.
Offending key in /home/babel/.ssh/known_hosts:7
Password authentication is disabled to avoid man-in-the-middle attacks.
```

SSHD_PORT Default setting: `SSHD_PORT='22'`

By `SSHD_PORT` a non-standard port can be defined the ssh server should listen to.

If ssh login from outside should be allowed `INPUT_ACCEPT_PORT_x` (Page ??) has to be adapted to reflect the change.

The commands accessing fli4l from an Unix-/Linux client over protocol SSH are:

- ssh - Secure Shell
- scp - Secure Copy

Corresponding programs are available for Windows as well, see:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>
<http://winscp.net/eng/docs/lang:en>
<http://www.tectia.com/de/de.iw3>

SSHD_PUBLIC_KEY_N Default setting: `SSHD_PUBLIC_KEY_N='0'`

`SSHD_PUBLIC_KEY_N` holds the number of public keys to be copied to the fli4l router.

SSH allows authentication based on asymmetric encryption. Authentication is done via username and public/private key instead of username and password. This way entering a

password can be omitted. Generate your key pair by the help of ssh-keygen (or puttygen if putty under Windows is used as the ssh client). When generating keys you can optionally specify a passphrase (a password for using the key) to increase security even more. If using a passphrase you may consider working with an ssh agent (ssh-agent or pageant).

Important: *The private part of the keypair has to be guarded as careful as a password because it has the same function. The private part of your keypair is only known to your ssh client. The public part of the key will be needed on the fli4l router and is provided to it by SSHD_PUBLIC_KEY_x or SSHD_PUBLIC_KEYFILE_x.*

For further informations see manual pages for ssh and its components res. the documentation for putty (<http://www.chiark.greenend.org.uk/~sgtatham/putty/>).

SSHD_PUBLIC_KEY_x Provide the public part of each user's key here who should be able to access fli4l via ssh. The easiest way is cut and paste it from a terminal window. Example:

```
SSHD_PUBLIC_KEY_1='1024 ... username@hostname'
```

Important: *The key does not contain carriage returns. Puttygen will insert those eventually while doing cut-and-paste. They will have to be deleted again.*

SSHD_PUBLIC_KEYFILE_N Default setting: SSHD_PUBLIC_KEYFILE_N='0'

Instead of copying the content of the public part of the key to sshd.txt you could copy it directly to the opt archive. This works like described for SSH_CREATEHOSTKEYS. Copy the public part of the key to the directory <config>/etc/ssh.

SSHD_PUBLIC_KEYFILE_x The file name of the public key in directory <config>/etc/ssh.

```
SSHD_PUBLIC_KEYFILE_1='root@fli4l'
```

SSH_CLIENT_PRIVATE_KEYFILE_N Default setting:

```
SSH_CLIENT_PRIVATE_KEYFILE_N='0'
```

If you want to use private keys for the ssh or plink client for login at a ssh server you could copy them to the directory <config>/etc/ssh. This works the same way as described in SSH_CREATEHOSTKEYS. Copy your private key to the directory <config>/etc/ssh. Private keys in OpenSSH format will be automatically converted to dropbear format on each boot.

SSH_CLIENT_PRIVATE_KEYFILE_x The file name of the private key in directory <config>/etc/ssh.

```
SSHD_PRIVATE_KEYFILE_1='babel@rootserver'
```

1.1.2 Installation Of Dbclient

OPT_SSH_CLIENT Default setting: `OPT_SSH_CLIENT='no'`

To use a pure ssh2/scp client activate dbclient from dropbear by setting `OPT_SSH_CLIENT` to 'yes'. The advantage of this client is that it shares program code with the dropbear ssh server. This saves a lot of space in the OPT archive. Dbclient is more or less compatible with ssh/scp client, its command syntax is similar. A symbolic link to `/usr/bin/ssh` res. `/usr/bin/scp` will be created to make `ssh <host> res. scp <source> <target>` working out of the box.

If dbclient's known hosts should be saved permanently the file `known_hosts` from the directory `/.ssh` on the router has to be copied to `config/etc/ssh`. This works in the same as with a generated host key. In the following example the fli4l directory (fli4l's boot medium is generated there) is found at `/home/babel/fli4l-3.10.5`. All config files are in directory `config.babel`.

```
cd /home/babel/fli4l-3.10.5
mkdir -p config.babel/etc/ssh
scp fli4l:/.ssh/* config.babel/etc/ssh
```

1.1.3 Installation Of A Plink Client

OPT_PLINK_CLIENT Default setting: `OPT_PLINK_CLIENT='no'`

Installs a ssh1/ssh2/telnet client on the fli4l router. plink is the Unix version of the well known PuTTY program for Windows. Executing plink on the fli4l router displays a help page for using plink.

If plink's known hosts should be saved permanently the file `sshhostkeys` from the directory `/.putty` on the router has to be copied to `<config>/etc/plink`. This works in the same as with a generated host key. In the following example the fli4l directory (fli4l's boot medium is generated there) is found at `/home/babel/fli4l-3.10.5`. All config files are in directory `config.babel`.

```
cd /home/babel/fli4l-3.10.5
mkdir -p config.babel/etc/plink
scp fli4l:/.putty/* config.babel/etc/plink
```

1.1.4 Installation Of A Sftp Server

OPT_SFTPSERVER Default setting: `OPT_SFTPSERVER='no'`

Installs a sftp server on the fli4l router.

1.1.5 Literature

Dropbear SSH2 Site: <http://matt.ucc.asn.au/dropbear/dropbear.html>

List of Figures

1.1 Directory structure of fli4l 4

List of Tables

Index

OPT_PLINK_CLIENT, [7](#)

OPT_SFTPSERVER, [7](#)

OPT_SSH_CLIENT, [7](#)

OPT_SSHD, [3](#)

SSH_CLIENT_PRIVATE_KEYFILE_N, [6](#)

SSH_CLIENT_PRIVATE_KEYFILE_x, [6](#)

SSHD_ALLOWPASSWORDLOGIN, [3](#)

SSHD_CREATEHOSTKEYS, [3](#)

SSHD_PORT, [5](#)

SSHD_PUBLIC_KEY_N, [5](#)

SSHD_PUBLIC_KEY_x, [6](#)

SSHD_PUBLIC_KEYFILE_N, [6](#)

SSHD_PUBLIC_KEYFILE_x, [6](#)