Application Guide

Configure a ConnectPort LTS to accept DSA keys for SSH user authentication

Digi Technical Support

13 September 2016

Contents

1 INTRODUCTION

1.1 Outline

Since firmware version 1.4.x the ConnectPort LTS will only accept key in SSH RSA format. This document will describe how to modify the ssh deamon to accept keys in DSA format for backward compatibility.

1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product and of the requirements for their specific application. It also assumes a basic ability to access and navigate a ConnectPort LTS and the Linux command line interface.

This application note applies to:

Model: DIGI ConnectPort LTS

Firmware versions: 1.4.0 and later

Configuration: This document assumes that the devices are set to their factory default configurations. Most configuration commands are shown only if they differ from the factory default.

Please note: This application note has been specifically written for firmware release 1.4.0 and later. Please contact tech.support@digi.com if your require assistance in upgrading the firmware of the ConnectPort LTS device.

1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: tech.support@digi.com Requests for new application notes can be sent to the same address.

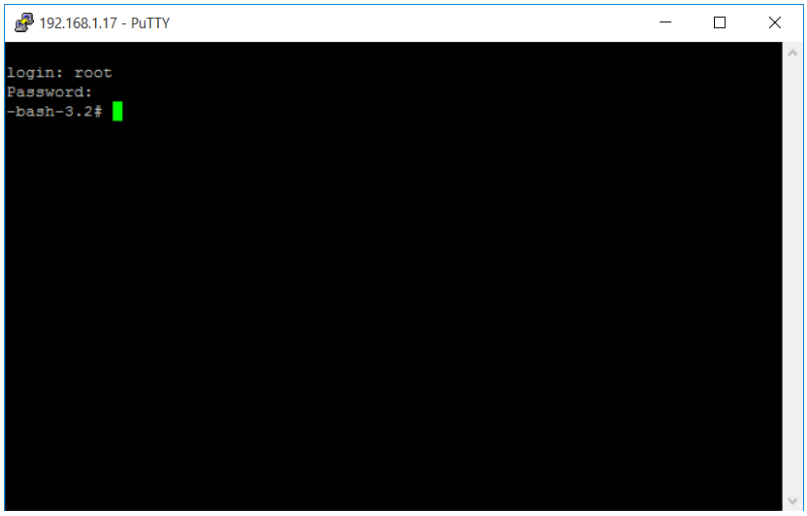
2 VERSION

Version Number	Status
1.0	published

3 MODIFY THE SSHD CONFIGURATION

Open a Command Line Interface connection via Telnet or SSH to the unit using a terminal application such as puTTy: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

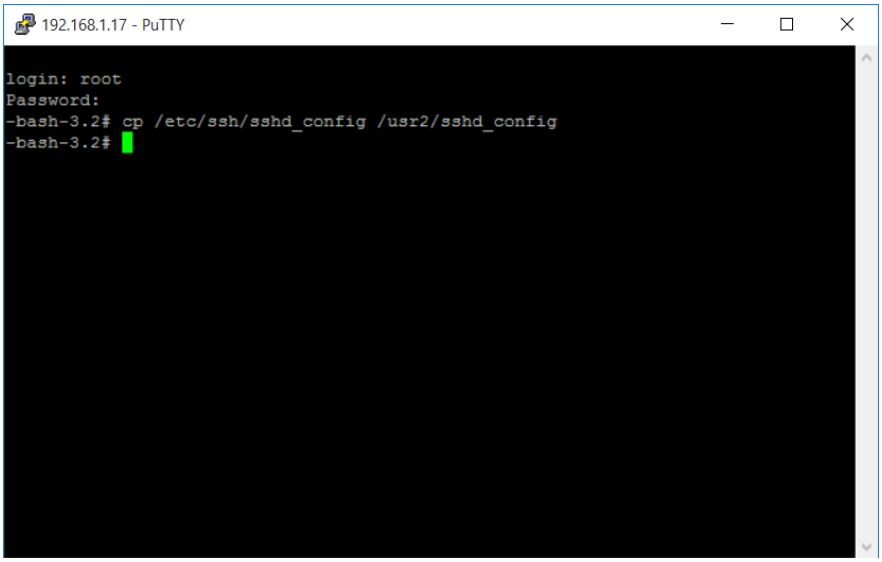
Connect using a super user such as the default **root** user as this will require access to the linux bash.



3.1 Copy the sshd_config to the user folder

To retain settings after a reboot, it is necessary to make the changes to a file inside the usr2 directory (user folder). This directory can contain custom user files and is only erased after a factory reset.

```
cp /etc/ssh/sshd_config /usr2/sshd_config
```



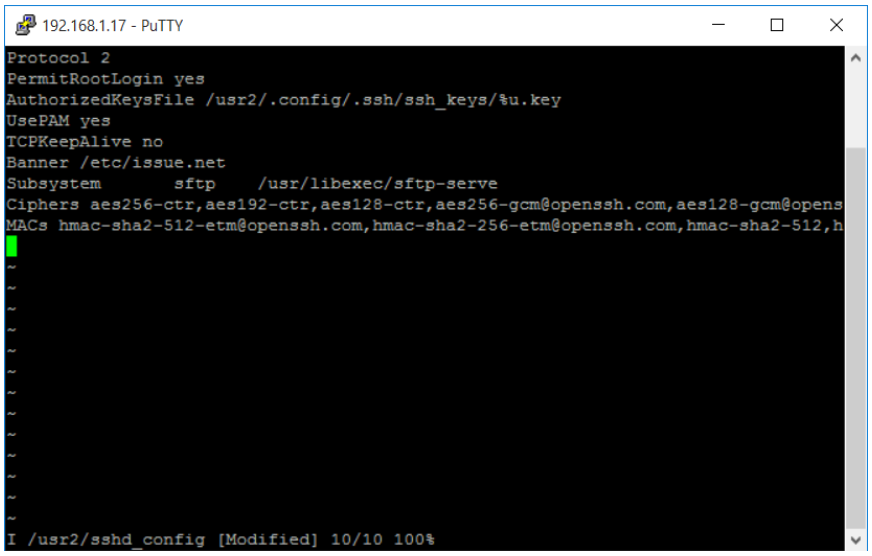
3.2 Add DSA keys support to sshd_config

Add the following extra line to the copied sshd_config file to add DSA keys support.

To do this, use VI:

```
Vi /usr2/sshd_config
```

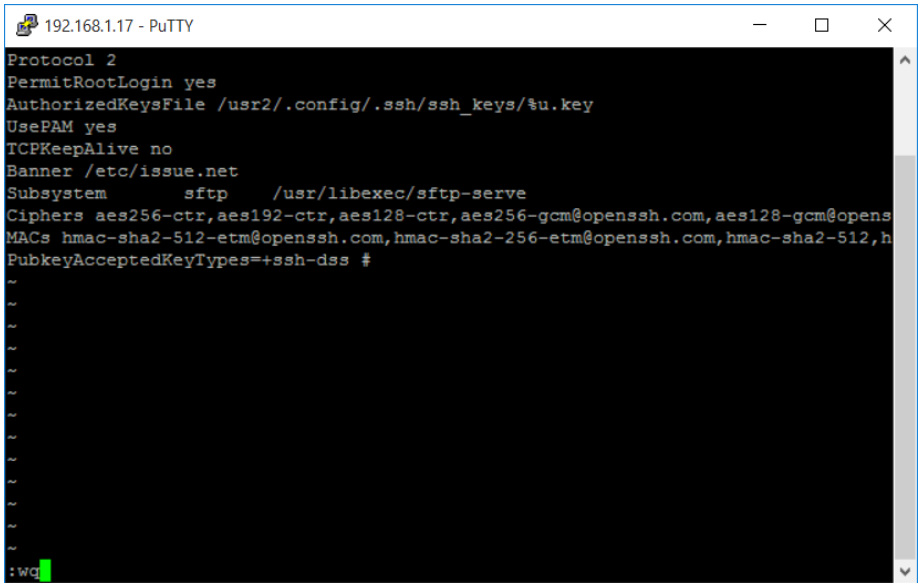
Place the cursor at the end of the last line and press **I** to enter edit mode:



Press **enter** to add a new line and enter

```
PubkeyAcceptedKeyTypes=+ssh-dss #
```

Press **escape** and type **:wq** to write and quit the changes.



3.3 Create a script to copy sshd_config

It is now required to create a script that will copy the customer sshd_config file from the /usr2 folder to the system's ssh folder.

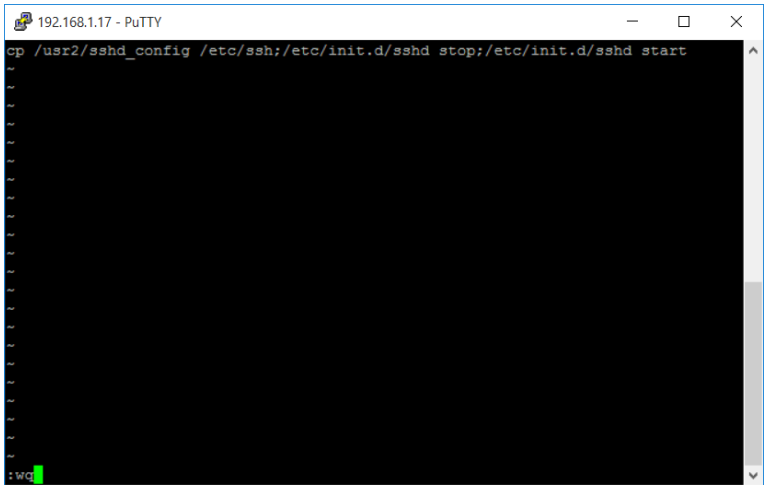
Use **vi** to create a script called **ssh.user**:

```
vi /usr2/ssh.user
```

press **I** to enter edit mode and add the following:

```
cp /usr2/sshd_config /etc/ssh;/etc/init.d/sshd stop;/etc/init.d/sshd start
```

Press **escape** and type **:wq** to write and quit changes

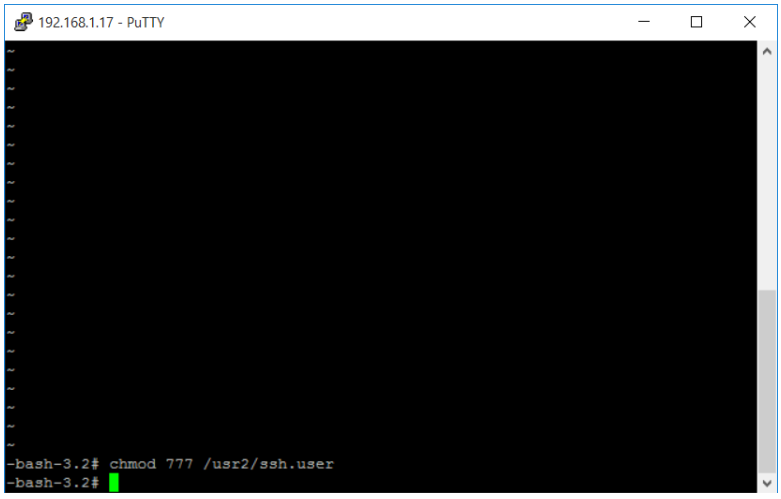


3.4 Set the script rights

The script needs to have write and execute permissions to run properly.

To change the script rights, do the following:

```
chmod 777 /usr2/ssh.user
```



3.5 Set the script to autorun on boot

The ConnectPort LTS has a rc.user script that will automatically run at boot of the device. This file can be edited and will keep its changes until a factory reset of the unit is done.

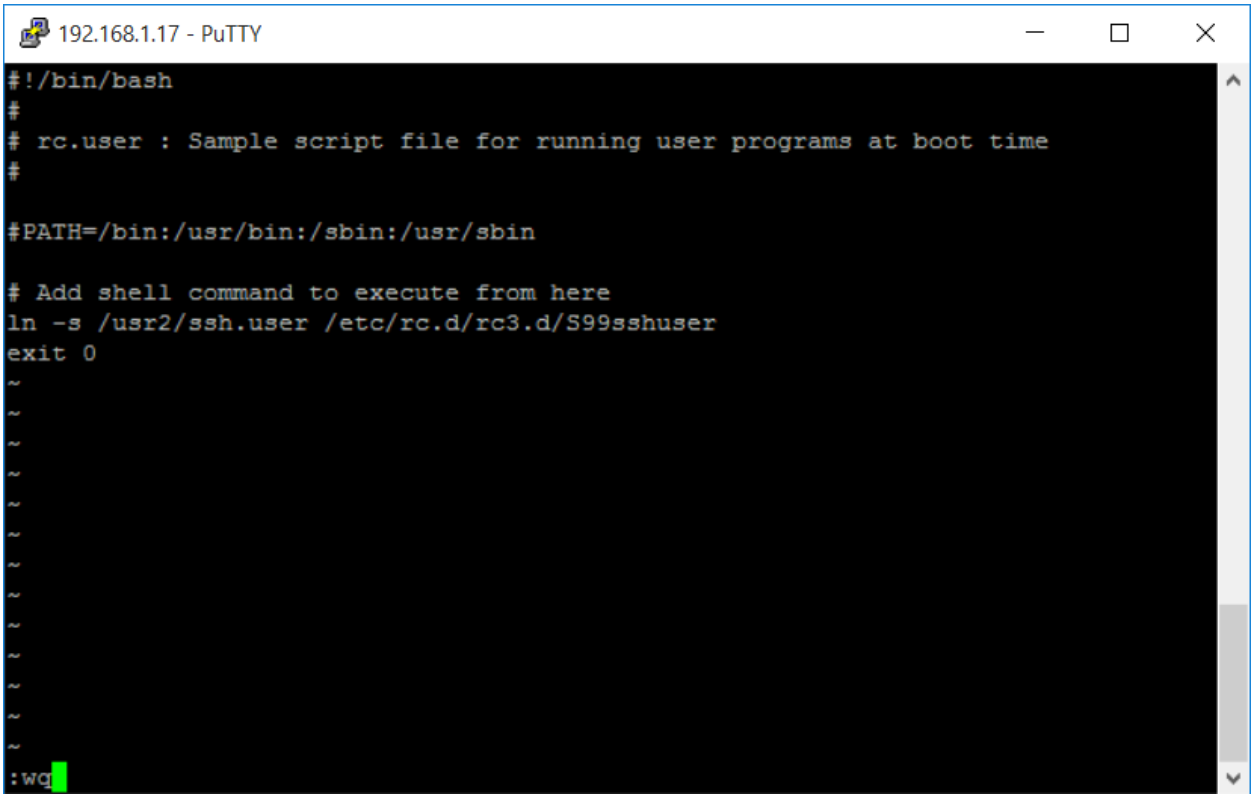
The rc.user script is located under /usr2/rc.user. Using VI, add the following line **ABOVE** "exit 0":

```
vi /usr2/rc.user
```

Add:

```
ln -s /usr2/ssh.user /etc/rc.d/rc3.d/S99sshuser
```

The file should look like this:



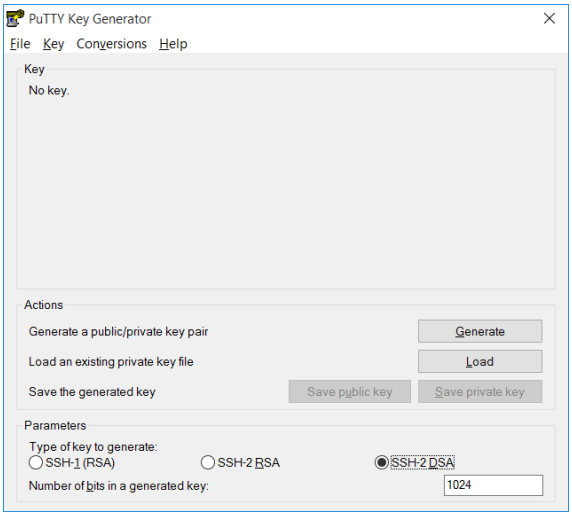
Press **escape** and type **:wq** to write and quit changes.

An SSH Key in DSA format can now be uploaded onto the unit, used for User Authentication and will be kept after a reboot.

4 TESTING

4.1 SSH DSA Key

PuTTy comes with a utility (puttygen) that allows generating SSH DSA keys. This can be used to proceed with the test below or else use an already existing key.



Make sure to save the associated private key for the authentication with a client.

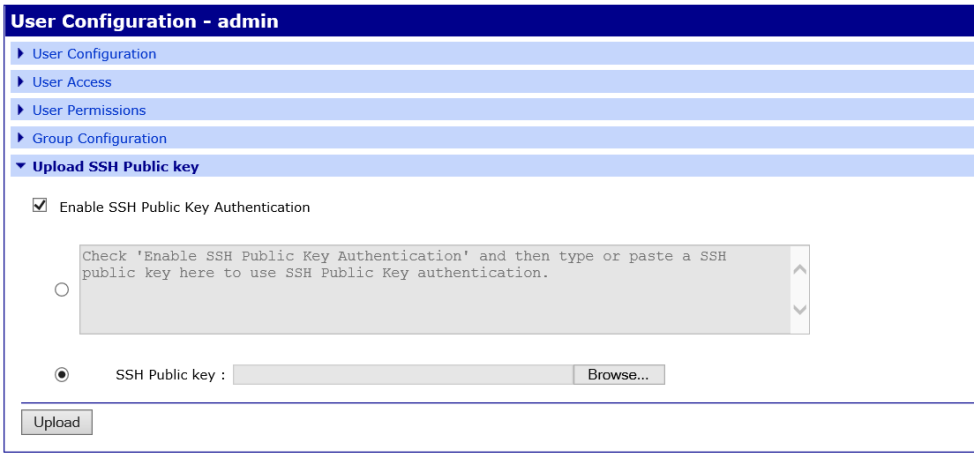
4.2 Upload SSH DSA Key

Open a web browser to the IP address of the ConnectPort LTS. Login using the appropriate username/password that will allow editing user access and rights.

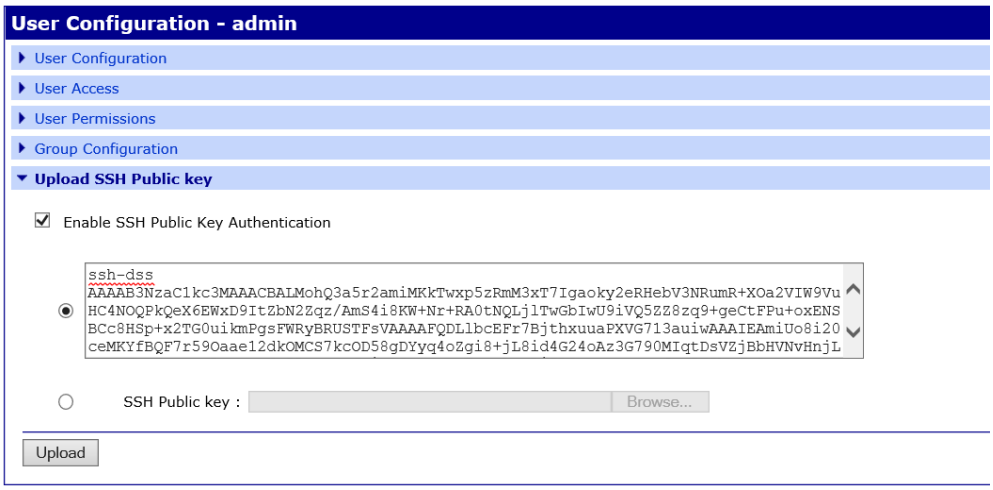
Navigate to **Configuration > Users**

Select the user that will be used for SSH Authentication

Under **Upload SSH Public key**, check **ENABLE SSH Public Key Authentication**, select SSH Public key and browse to the location where the SSH DSA Public key was saved. Click **OK**



Once uploaded, the key will be visible in the window:



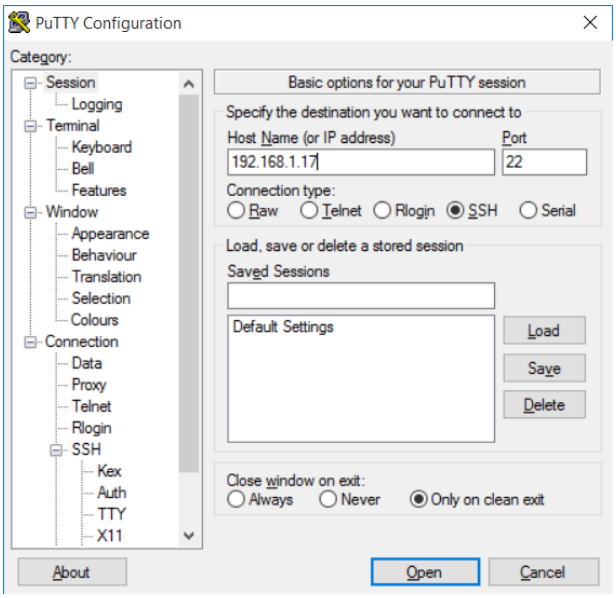
Click **Upload** to save the changes.

4.3 Connect with PuTTy

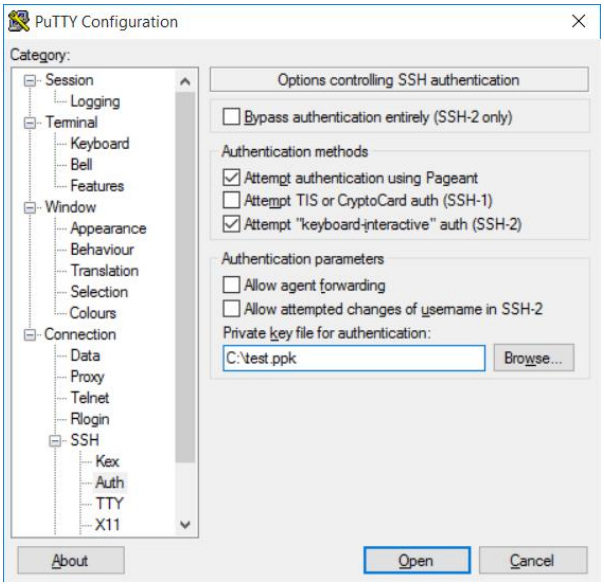
Open PuTTy.

In the **Host Name** field, type the IP address of the ConnectPort LTS.

Select **SSH** as the connection Type



Under **Connection > SSH > Auth** under **Authentication parameters**, browse to the location of the private key file (.ppk)



Click **Open**

The user name will be required to log in. Once entered, the server will use the key to authenticate and not require the password (it is also possible to input the user straight from the connection menu and nothing will be asked):