Quick Note 19

Manage a Router Securely with HTTP over SSH Tunnel

Digi Technical Support

September 2016

Contents

1 INTRODUCTION

1.1 Outline

To securely administer a Digi TransPort router, SSH, VPN or SSL can be used. The document explains how to use SSH to secure the router HTTP (web GUI) management traffic. It is possible to transport HTTP traffic in the SSH tunnel and have ease of management through the web interface without compromising on security. Security can be increased further by using an RSA key pair to handle the authentication of the connection. When using public and private keys, the regular user passwords configured on the router are not used, the client must have the private key configured within the SSH software that can be verified by the public key on the router.

Management of a TransPort via HTTP is used in this Quick Note (QN) by way of an example. It may be that the reader wishes to use an SSH tunnel to connect to some third party equipment on port 80 or some other TCP port via SSH. This can be achieved by following this QN and making changes to the destination IP address and port number in section 2.4.

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. This QN applies only to:

Model: All Digi TransPort routers

Firmware versions: 5.123 and later

> **NOTE**: This QN has been specifically rewritten for firmware release 5.123 and later but the original QN was testing as working for TransPorts running 5.050 and later. TransPorts running earlier firmware may find that the screenshots do not accurately reflect what will be seen.

Configuration: This QN assumes that the TransPort is set to its factory default. Most configuration commands are only shown if they differ from the factory default.

1.3 Corrections

Requests for corrections or amendments to this QN are welcome and should be addressed to: tech.support@digi.com

Requests for new QNs can be sent to the same address.

1.4 Version

Version Number	Status
1.0	Published
2.0	Updated for New Web Gui after 5123
2.1	Updated screenshots and instructions for new web interface, rebranding (Sept 2016)

2 CONFIGURATION

This process involves generating a private key on the TransPort then configuring the SSH to use the key for SSH connections.

All new TransPorts have a factory generated private key named privSSH.pem and SSH access is pre-configured. If you wish to use this key rather than generating a new one, skip to section 2.3

2.1 Generate a New SSH Private Key

ADMINISTRATION > X.509 CERTIFICATE MANAGEMENT > KEY GENERATION

Browse to the link above and enter the following values:

Parameter	Setting	Description
Key Filename	<name_of_key>.pem	Enter a name for the private key that will be generated.
Key Size	<Key_size>	Select a key size in bits.

NOTE: The larger the key, the more secure the connection, but also the larger the key, the slower the connection.

Click on the 'Generate Key' button to start the creation of the private key. After a few seconds, the browser will start updating with the progress of the key generation. When the key has been generated, the information below the 'Generate Key' button in the screenshot below will be shown.

The private key has now been generated and saved to FLASH as "privSSH.pem".

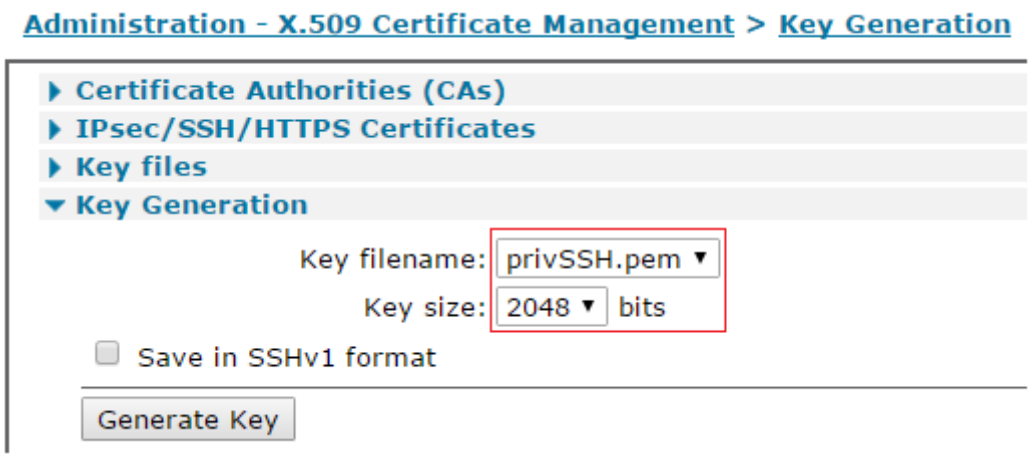

Figure 1: Generate SSH Key

2.2 Configure the SSH Server

CONFIGURATION > NETWORK > SSH SERVER > SSH SERVER 0

Browse to the above link; if the default values are correct, just enter the name of the private key generated in the previous step into the 'Host key 1 filename' field and enable Port Forwarding:

Parameter	Setting	Description
Enable SSH Server	Ticked	Option to enable SSH Server
Host Key 1 Filename	<SSH_Key_File_Name>	SSH Key file name generated in section 2.1
Enable Port Forwarding	Ticked	Allows access through the tunnel to the router

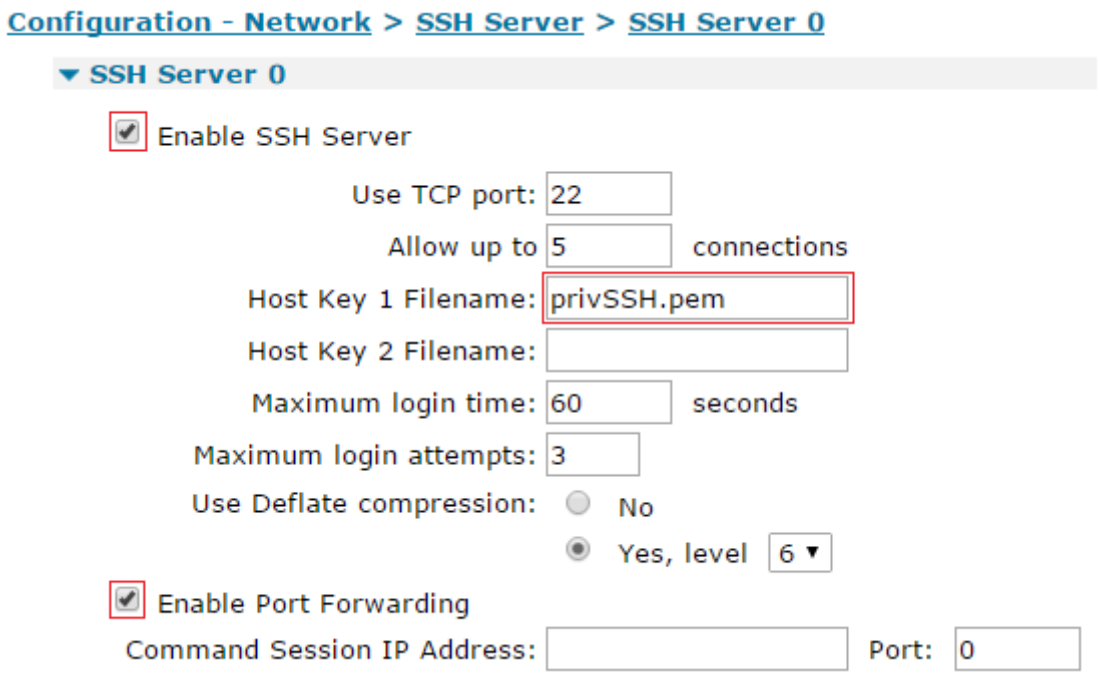

Figure 2: SSH Server Configuration

Then click the '**Apply**' button.

NOTE: Depending on the running TransPort firmware version, these may be the default settings.

2.3 Test SSH Connectivity

A normal SSH connection to the router should now be possible without RSA authentication.

2.4 Configure the SSH Client for Port Forwarding

Configure Putty or any other SSH client to listen on a local port and forward this to the TransPort on port 80.

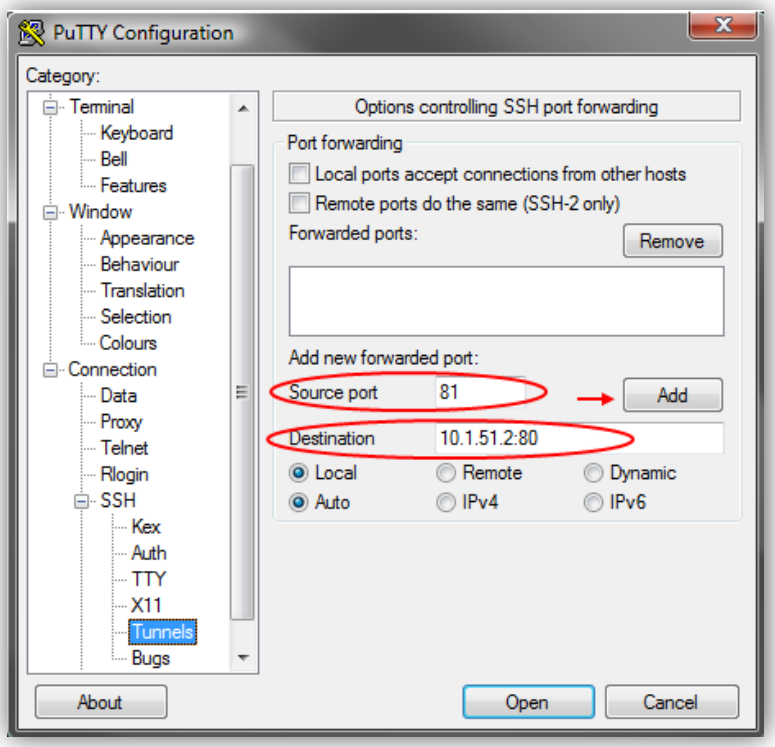

Figure 3: Putty Port Forwarding Configuration

In the Putty menu, expand the menus to **Connection > SSH > Tunnels**

Configure the '**Source port**'; this is the local port that PuTTY will listen on.

Configure the '**Destination**'; this is the LAN IP address and TCP port of the router that needs to be managed.

Click the **Add** button to confirm the configuration and the data entered will move into the top box titled '**Forwarded ports:**'.

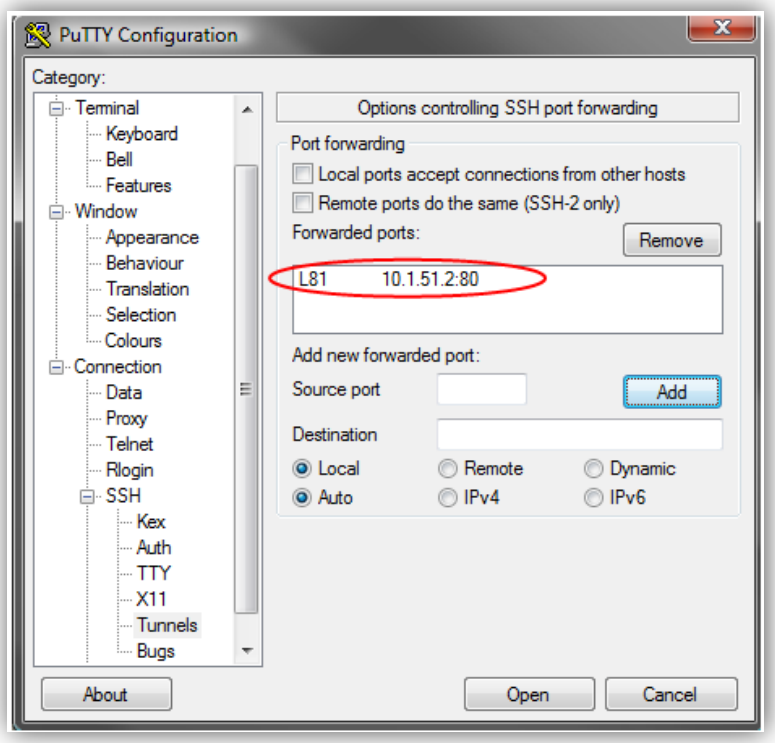

Figure 4: Putty Port Forwarding Configured

In the PuTTY menu, click on '**Session**', enter the public IP address of the router to manage, and select SSH. The port will change to 22.

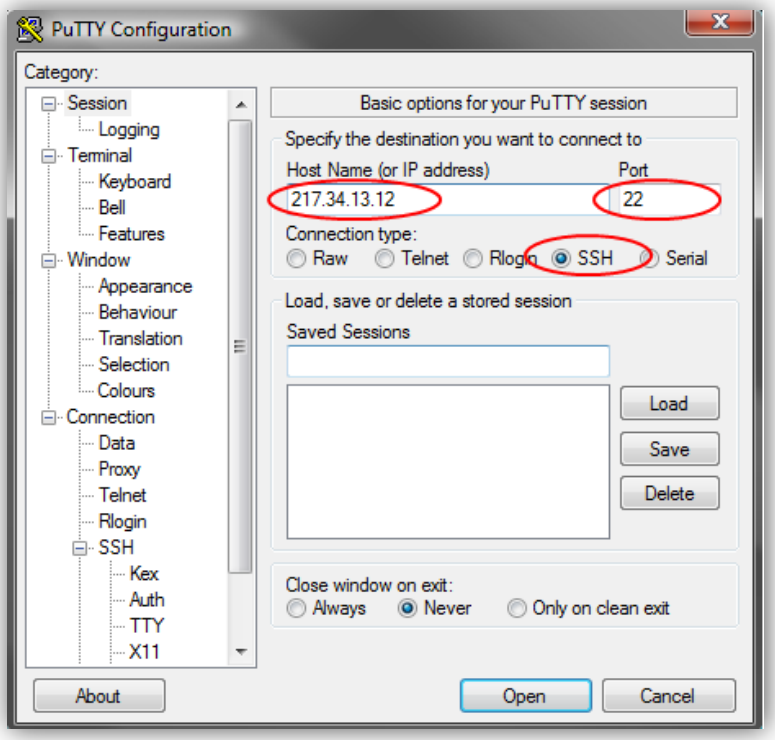

Figure 5: Putty Session Configuration

Click on "**Open**" and log in to the TransPort using SSH, the normal username and password.

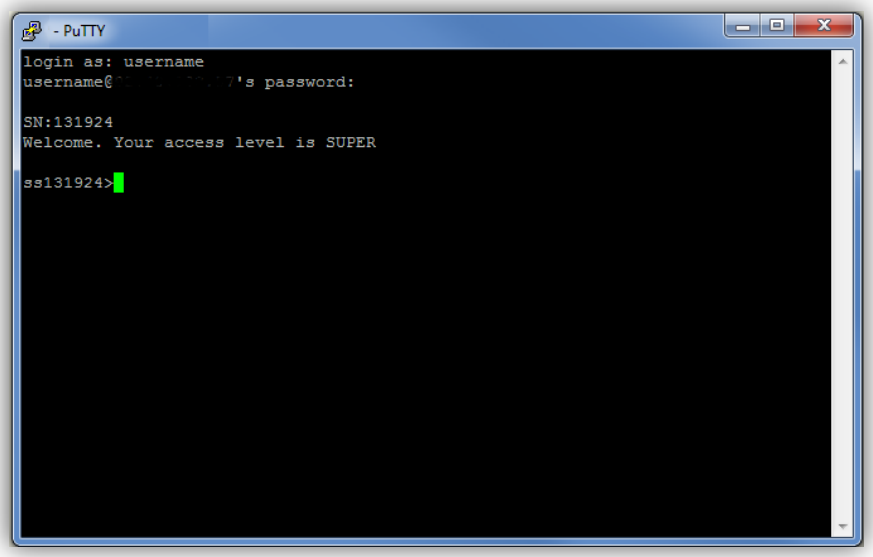

Figure 6: Successful Connection Using Putty

PuTTY is now listening on port 81 for local connections.

2.5 Port Forwarding Test

Open the web browser and enter the following address to manage the router:

```
http://127.0.0.1:81
```

Figure 7: Digi TransPort Configuration via SSH Port Forwarding

HTTP will be forwarded to the router over the SSH tunnel for secure management.

If higher security is required, public and private key pairs can be used. The rest of this QN configures the key pair.

3 GENERATE THE KEY PAIR

Download a copy of PuTTYgen. This will be used to create the public and private keys.

Figure 8: Putty Generate Key

Click on '**Generate'** to start the key generation process:

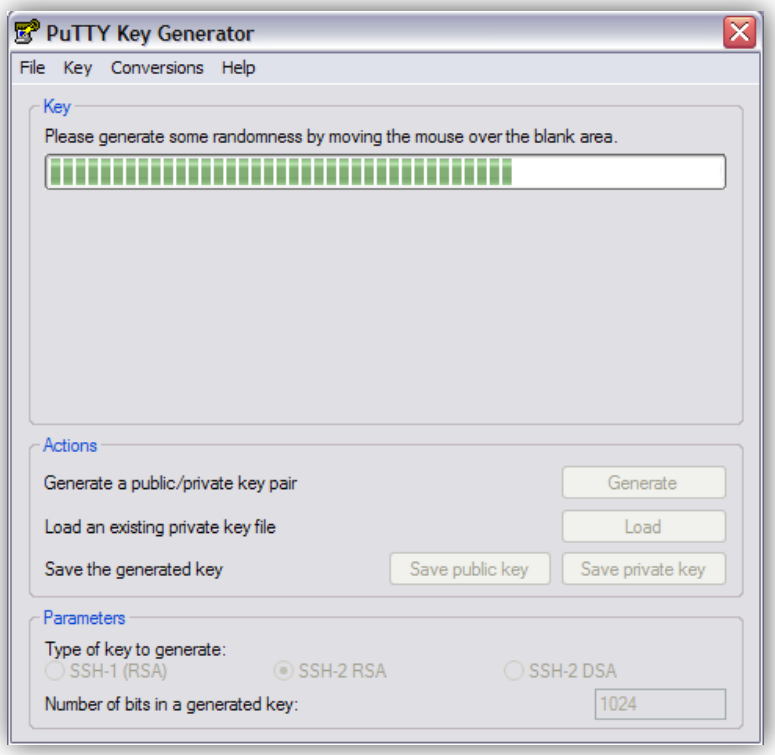

Figure 9: Putty Key Generation in Progress

Move the mouse pointer around below the white bar to generate randomness and the bar will fill up with green blocks. When the process is complete, the following screen will be shown:

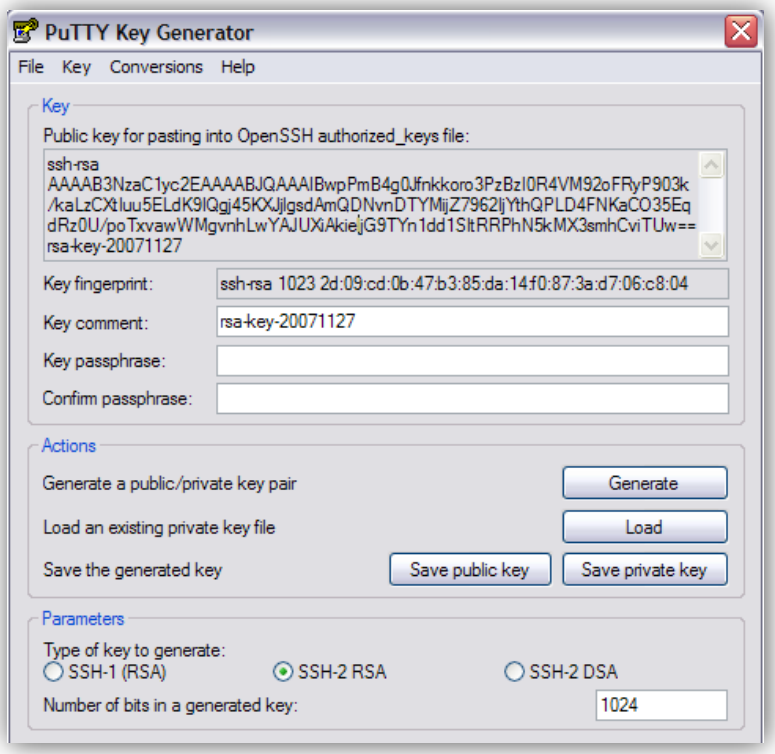

Figure 10: Putty Key Generated

Copy the text in the top part of PuTTYgen, headed "Public key for pasting into OpenSSH authorized_keys file" to the clipboard:

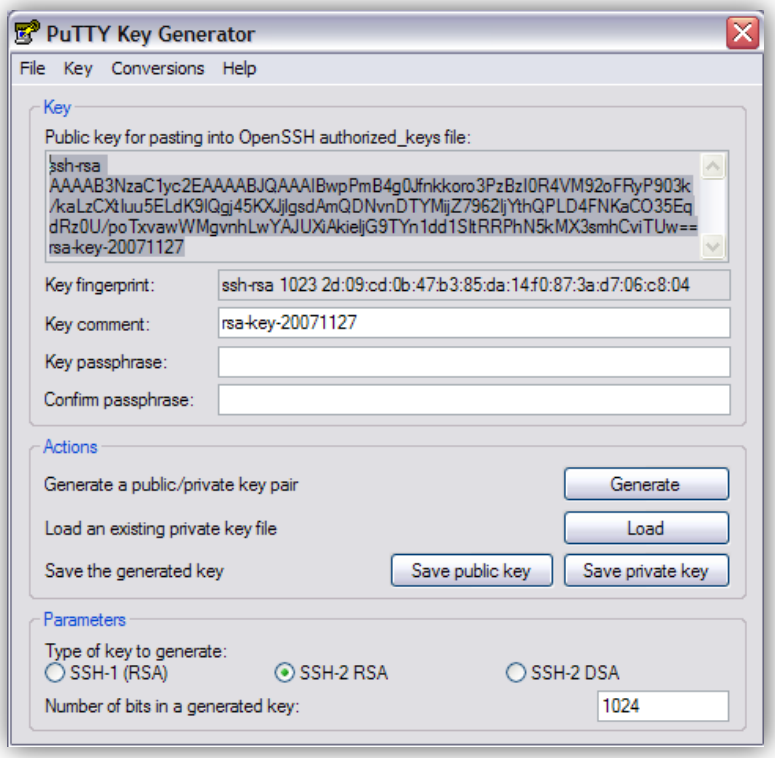

Figure 11: Copy Public Key

Open Notepad; paste the text from the clipboard and save the document as "public.pem":

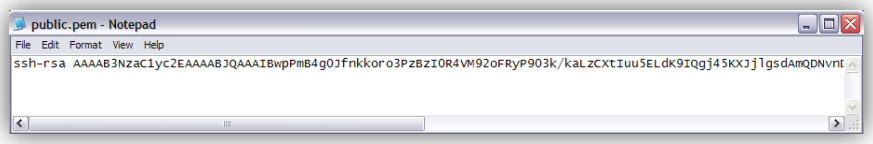

Figure 12: Save Public Key to Text File

NOTE: The pasted text should occupy one (1) line only.

Transfer the public.pem file onto the TransPort using an FTP Client.

Enter a Key passphrase and confirm it in the fields shown, then click the '**Save private key**' button. Save it with the name "private.ppk":

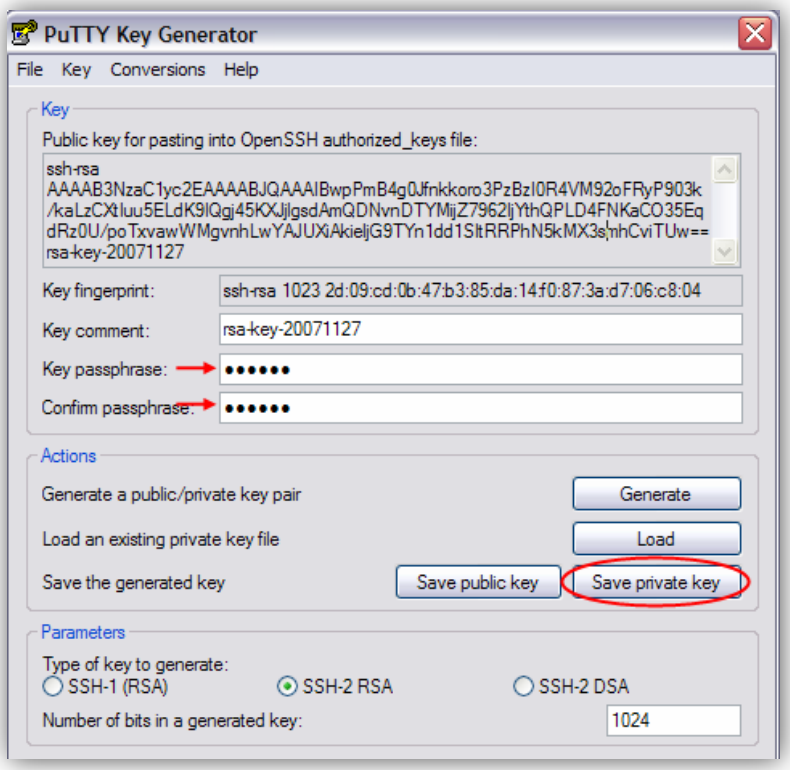

Figure 13: Save Putty Private Key

3.1 Configure a User with the Public Key File

CONFIGURATION - SECURITY > USERS > USER 0 - 9 > USER <N>

Navigate to the above link; enter a name for the user in the '**Username**' field.

Enter a random, non-dictionary based password into the **Password** fields. This password will not be used, but should the RSA authentication fail, the user will be displayed a password prompt.

Select the Public Key from the dropdown list. This is the one that was created and FTP'd onto the TransPort in the previous steps.

Parameter	Setting	Description
Username	<User_name>	Login username for the user to access the router
Password	<User_Password>	Password for user to use if the SSH public private key authentication fails
Confirm Password	<User_Password>	Confirm password for user to use if the SSH public private key authentication fails
Public Key file:	<key_file_name>.pem	Name of the public key file for this user generated above and FTP'd to the TransPort

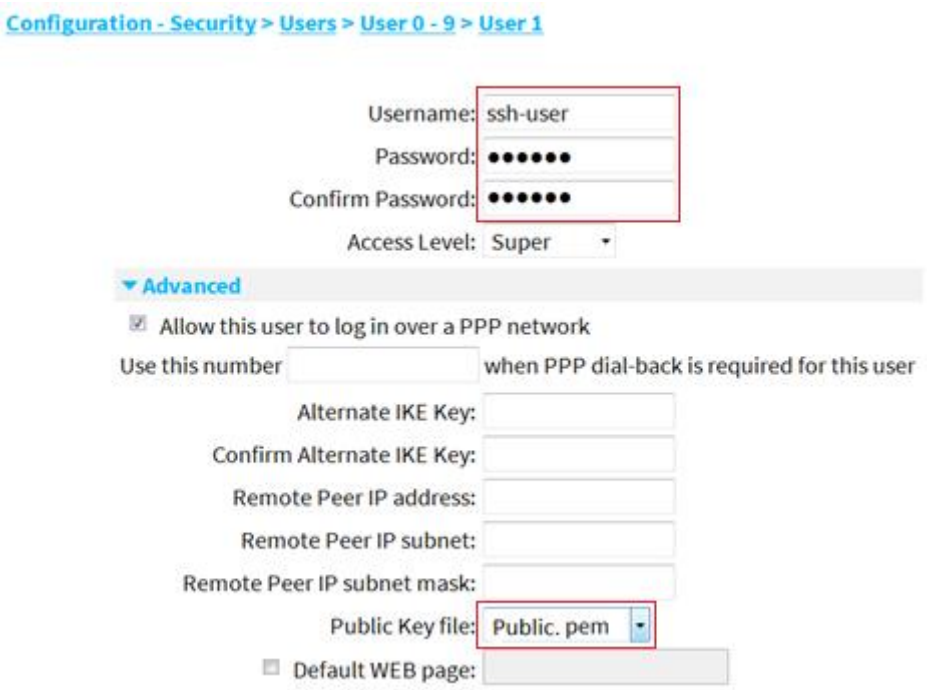

Figure 14: Configure User to Authenticate with Public Key

Click the '**Apply**' button.

3.2 Configure the SSH Client Software

The SSH client software (e.g. PuTTY) will need to be configured to use the private key generated in the previous steps.

In PuTTY, this is done by expanding **Connection > SSH > Auth** and entering the location of the private key file in the field titled 'Private key file for authentication':

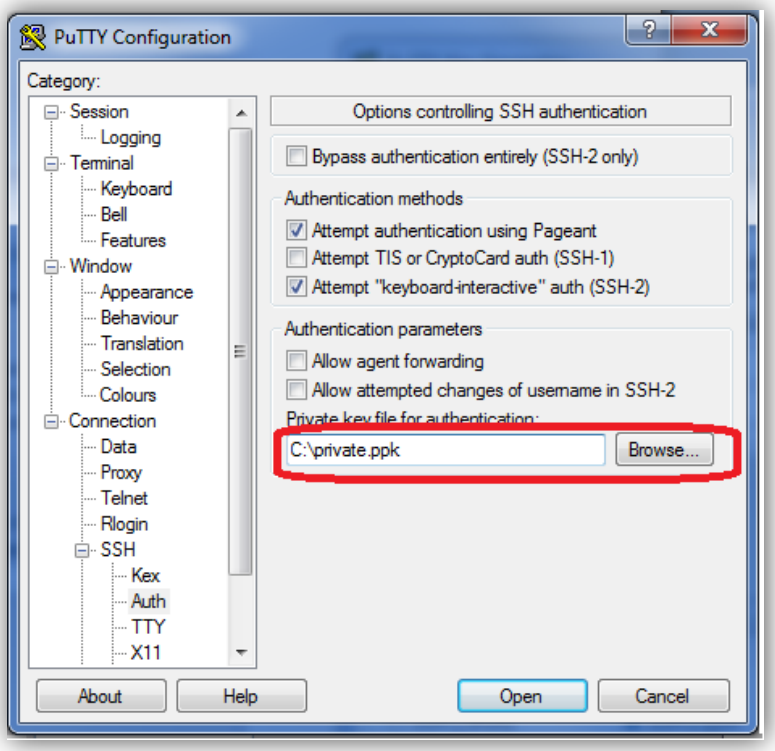

Figure 15: Configure Putty to use the Private Key

Expand **Connection > Data** and enter the username to be used for this connection:

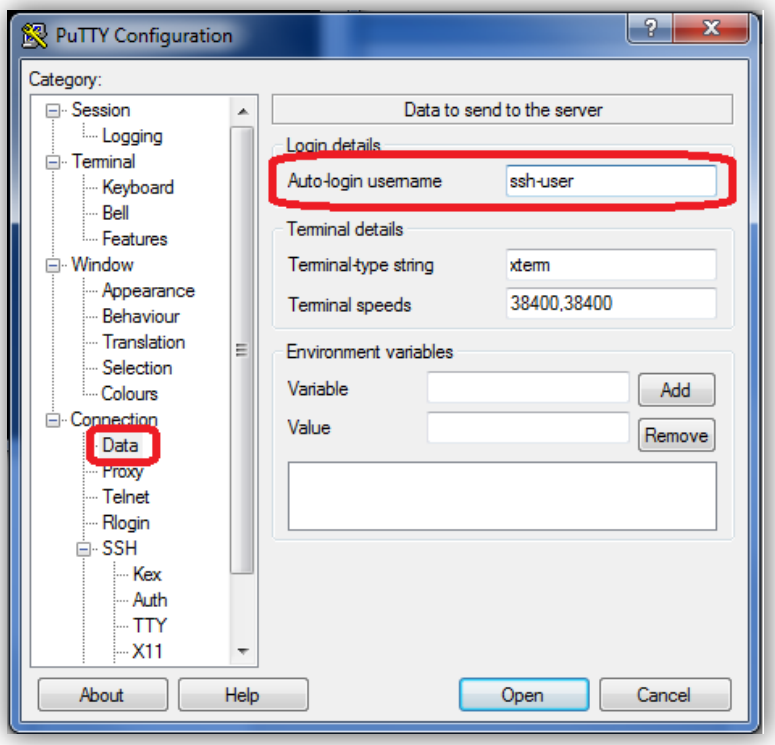

Figure 16: Configure Putty to Automatically Use the Correct Username for this Connection

Return to **Session** and name the connection by typing something meaningful into the blank text box below 'Saved Sessions' and click 'Save':

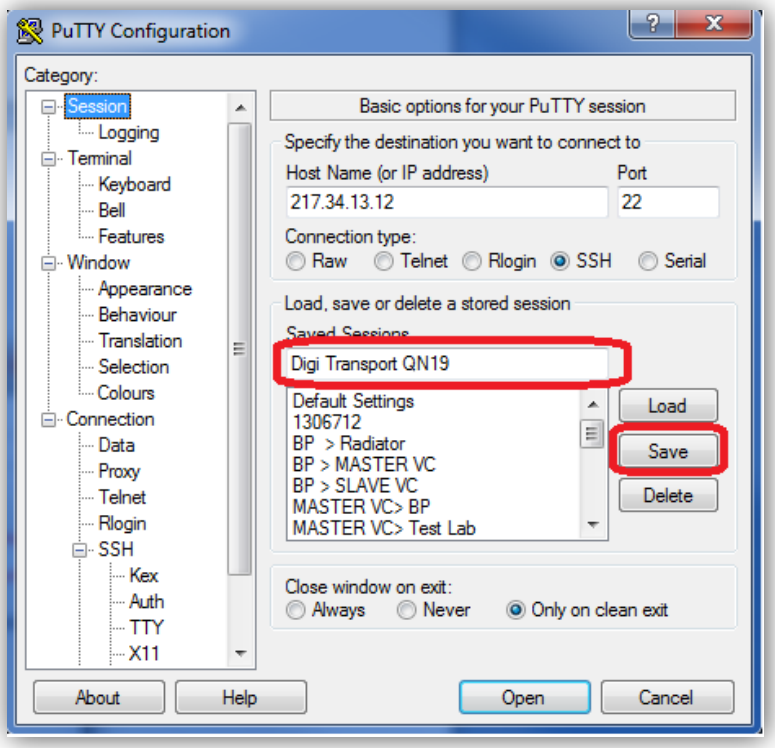

Figure 17: Save the Putty Setup for Future Connection to Remote Router

4 TEST SSH ACCESS

Click the '**Open**' button in PuTTY to connect:

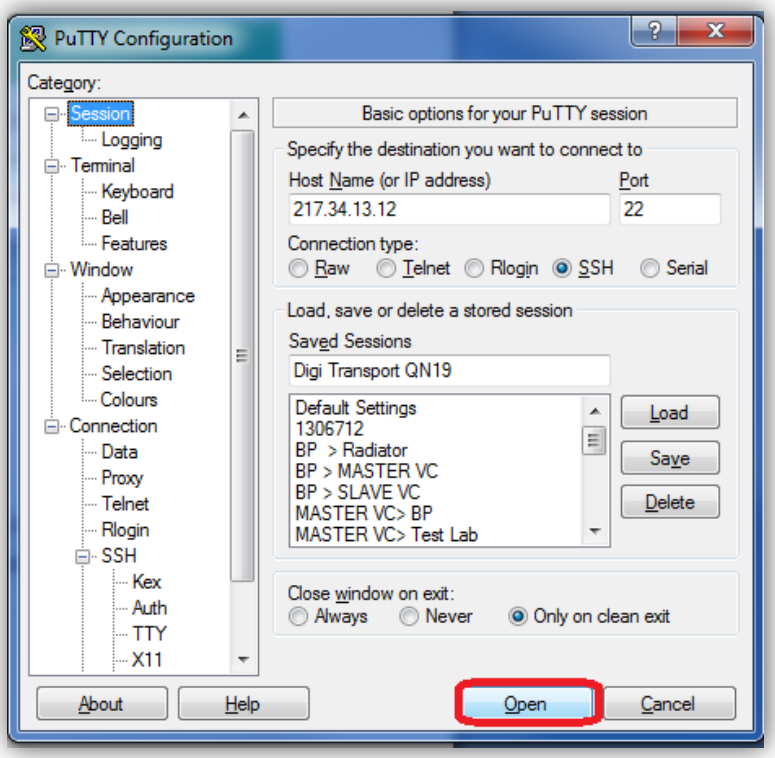

Figure 18: Use Saved Configuration to Connect to Remote Digi TransPort

The first time you connect to the remote router and the private key is loaded into PuTTY, you will be prompted to enter the passphrase that was configured for the private key previously in PuTTYgen. Access to the CLI will now be granted.

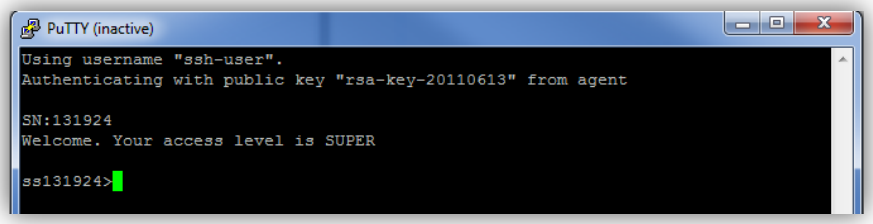

Figure 19: Successful Connection to Remote Digi TransPort Router

5 SAVE CONFIGURATION

ADMINISTRATION > SAVE CONFIGURATION

Browse to the link above and then click '**Save**'.

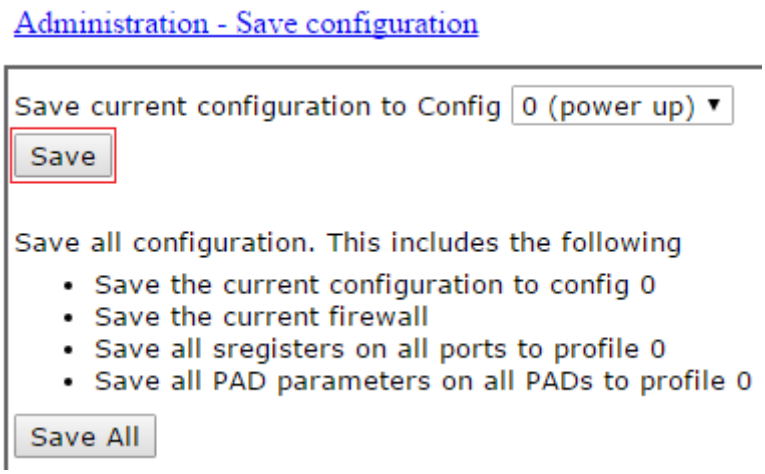

Figure 20: Save TransPort Configuration