Declan Murphy



The aim of this document is to provide details on how to access the Tango Network remotely when working from home or on site. This is strictly an internal document and strictly confidential.

Tango Telecom Remote Access Setup

Contents

[Remote Access Setup 2](#_Toc408348092)

[Setting Up Public/Private Keys 2](#_Toc408348093)

[Applying the Private/Public Key 3](#_Toc408348094)

[Accessing tangier Remotely 6](#_Toc408348095)

[Accessing other Tango internal Services Remotely 7](#_Toc408348096)

[Twiki 7](#_Toc408348097)

[Tango Contact Page 7](#_Toc408348098)

[DRE Twiki Page 7](#_Toc408348099)

[Meeting Room Booking System 7](#_Toc408348100)

[Accessing Documentation Folder on Tangier 7](#_Toc408348101)

[Accessing PST Folder on Tangier 7](#_Toc408348102)

[PST RFP Responses 7](#_Toc408348103)

[Accessing Marketing Folder on Tangier 8](#_Toc408348104)

# Remote Access Setup

For security reasons access to the Tango internal network is restricted to people outside of the Limerick office LAN. To gain access remotely (e.g: From Home or on Customer Site) Tango personnel will need to have to go through the security firewall which is known as Atlas (Not to be confused with our Travel booking company☺).

The only mechanism to gain terminal access to atlas is via Secure Shell (ssh) or root login with a password from the system console.

Access to the Tango network externally is only allowed using SSH2 1024-bit public/private keys as described below.

## Setting Up Public/Private Keys

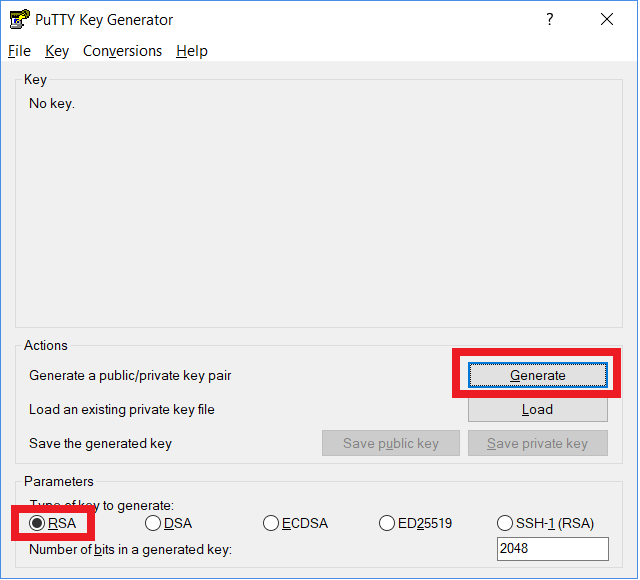
|  |  |
| --- | --- |
| **Note**: | *The following steps will only have to be carried out once off for generating the private/public keys which will be used for all connections in future.* |

1. Download and install a recent version of putty from:

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

|  |  |
| --- | --- |
| **Note**: | *The 5 PUTTY binaries should be installed and it may be necessary to add the target directory*  *to the PATH (click on My Computer/Properties/Advanced/Environment). puttygen is used*  *to generate the keys; putty is used for gaining terminal access; psftp is an ssh ftp client.* |

1. Launch puttygen.exe
2. In the Parameters section at the bottom of the window, select RSA (this is the default).
3. In the Actions section (middle of window), click the Generate button.



1. SET 4096 FOR RHEL8 TARGET MACHINES
2. Shake your mouse pointer in the Key section until the key is generated.
3. In the Key Comment field, type in a name for the key (e.g. “SSH2 key for atlas”).
4. Enter and re-enter a passphrase (between 10 and 30 characters) –

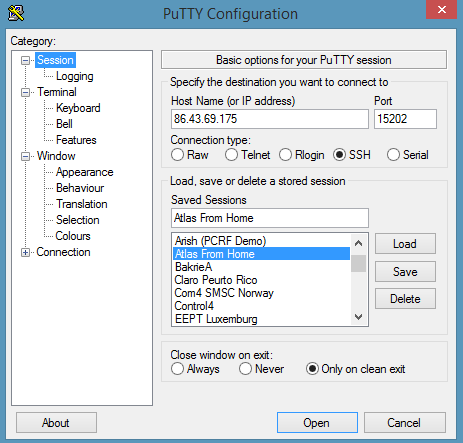
|  |  |
| --- | --- |
| **Note**: | *this passphrase is used to encrypt the file that will be used to store your SSH key on disk. You will be asked for this passphrase every time you need to use the key (e.g. to login).* |

1. Click the “Save private key” button (Actions section) and choose an appropriate location and file name for the private key file (e.g: *C:\Users\YOURNAME\Documents\Tango Stuff\Atlas\Putty Private Key\AtlasKey.ppk*)
2. Select the content of the public key area in the Key section – this needs to be pasted into ***$HOME/.ssh/authorized\_keys2*** on the target server (e.g. atlas).

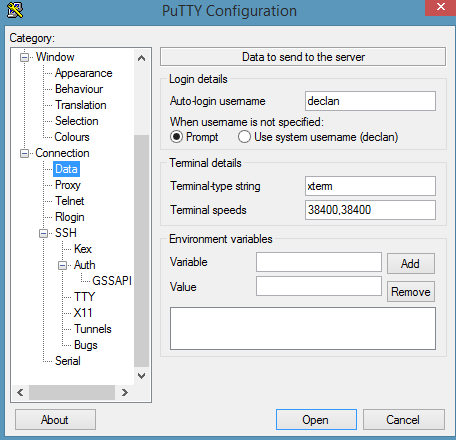
You will need to contact Maurice ([maurice.oconnor@tangotelecom.com](mailto:maurice.oconnor@tangotelecom.com)) with this key as he will have permissions to add it.

## Applying the Private/Public Key

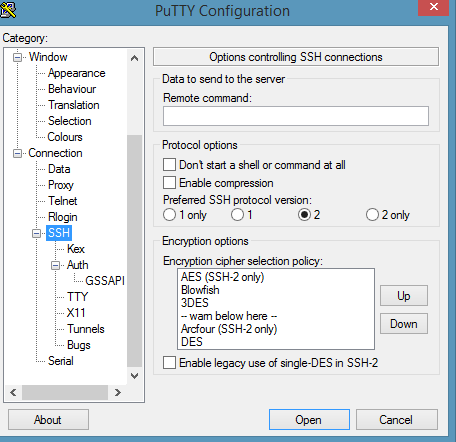
1. Launch putty
2. Create a Saved Session with a suitable name (e.g: Tango Remote Access) – the configuration items necessary are:
   1. Hostname or IP address of target server
   2. Select the SSH protocol



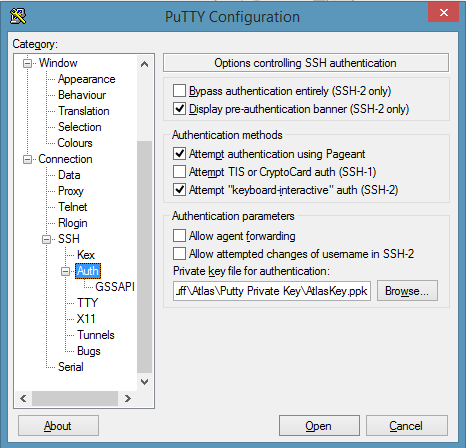
* 1. In the Connection category, enter your username ($HOME) in the “Auto-login username” field.



* 1. In **Connection -> SSH**, select **2** as the preferred SSH protocol version.



* 1. In ***Connection -> SSH -> Auth***, click the browse button to select the filename of the stored private key (item 8 in the “*Setting up Public/Private Keys*” section).

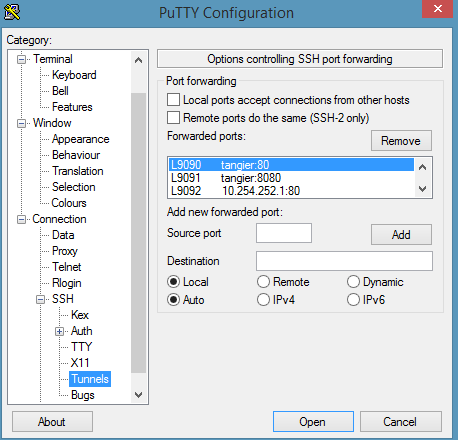


* 1. To set up a tunnel from Atlas to Tangier select: ***Connection -> SSH -> Tunnels***

Source port = 9090

Destination = tangier:80

Select **ADD**



* 1. To set up a tunnel from Atlas to luxof for Meeting Room Booking System access : ***Connection -> SSH -> Tunnels***

Source port = 9095

Destination = 192.168.25.14:80

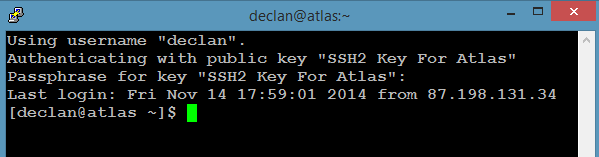
Select **ADD**

* 1. Select the Session category again, enter a name for the session and click the saved button.

# Accessing tangier Remotely

Provided the steps in the “Remote Access Setup“Section have been completed include Tunnel setup the following steps are used to access tangier.

1. Double-click on the saved putty session to launch an SSH2 encrypted session between your computer and the target server – you will be asked for the passphrase you entered in step 7 in the “*Setting up Public/Private Keys*” section. When successfully logged in you will see the following:



1. Open your internet browser and enter the following address:

# Accessing other Tango internal Services Remotely

Provided your Putty session is open to Atlas the following should be accessible via your browser.

## Twiki

<http://localhost:9090/>

## Tango Contact Page

<http://localhost:9090/phonelist.php>

## DRE Twiki Page

<http://localhost:9090/twiki/bin/view/Main/DREProject>

## Meeting Room Booking System

<http://localhost:9095/mrbs>

## Accessing Documentation Folder on Tangier

<http://localhost:9090/documentation/>

## Accessing PST Folder on Tangier

http://localhost:9090/pst/

### PST RFP Responses

<http://localhost:9090/pst/Proposals,%20RFI%20and%20RFP/>

## Accessing Marketing Folder on Tangier

Note: restricted Access to Sales & Marketing

<http://localhost:9090/market>