Bitvise Tunnelier Installation Guide

Revised Oct 20th, 2010

CONTENTS

INTRODUCTION

Bitvise Tunnelier is third party software used as a port forwarding client for restaurants who have implemented ASI's On Line Ordering. Limiting access to a server is an important part of PCI Compliance. In the past, DMZ machines with open ports were required to run on a sub-network to insure PCI compliance. The Tunnelier program eliminates the need for a DMZ machine for On Line Ordering and requires no ports to be open. In addition, the Tunnelier program is easier to set up when compared to the effort involved with configuring routers and firewalls needed for sub networks on DMZ machines. An additional benefit is, by replacing a DMZ machine; the Bitvise Tunnelier software reduces extra hardware costs for the end user.

INSTALLATION

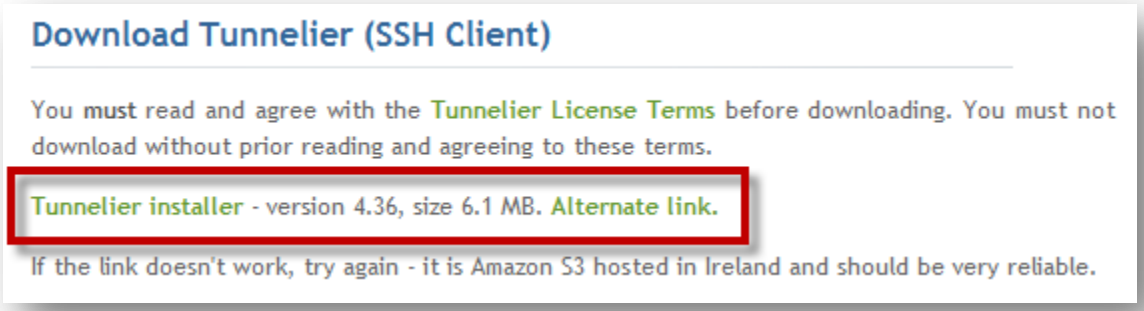
The installation of The Bitvise Tunnelier SSH Client software is a relatively easy process. The following sections outline the installation process at the restaurant site:

- Download Software
- Install Software
- Tunnelier Configuration
- Add Tunnelier to Windows Start Up

Please note there may by a delay during certain steps in installation process. The delay is due to generating a public key within Tunnelier, emailing the key info to ASI, and the registering the public key and restaurants public IP address at ASI.

DOWNLOAD SOFTWARE

The Bitvise Tunnelier is a free program for individual use. The software can be downloaded at the Bitvise website: http://www.bitvise.com/tunnelier-download. Use the "Tunnelier installer" option on the webpage to begin download process:

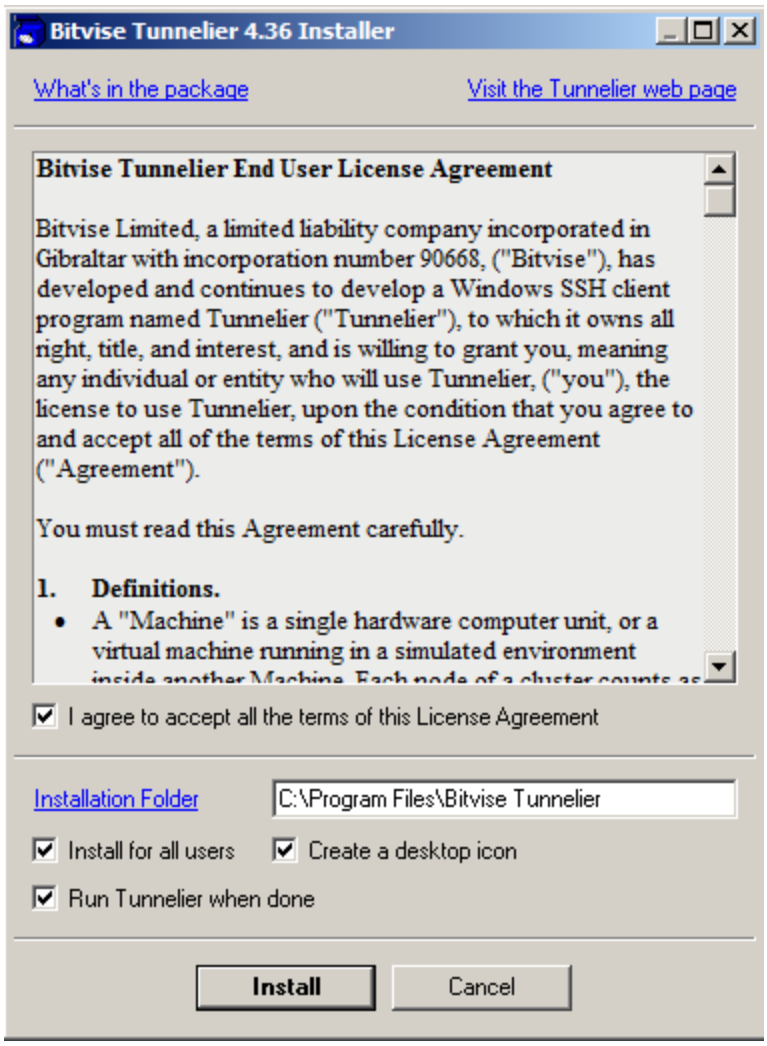


Save the download (Tunnelier-Inst.exe) to a location of your preference on the rmserver.

INSTALL SOFTWARE

Bitvise Tunnelier must be installed on the rmserver (the computer hosting the rmwin directory).After downloading the Tunnelier installer you will need to use the following steps:

1. Begin the installation process by clicking on the Bitvise Tunnelier x.xx Installer
2. Make sure you have the proper installation path and preferred settings enabled/disabled at the bottom of the Installer form before selecting the "Install" button. However, you will want to be careful if you are running more than one user on the rmserver if disabling the "Install for all users" option. The administrator account will be automatically selected if you disable the option. If necessary, you can change the permissions after installation. Once you have the preferred settings configured, have read and agreed to the Agreement terms, you can proceed with the installation by selecting the "Install" button.

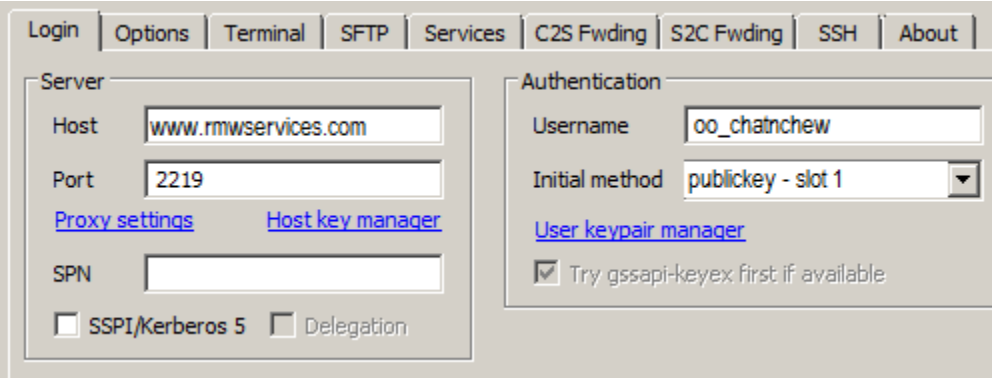


TUNNELIER CONFIGURATION

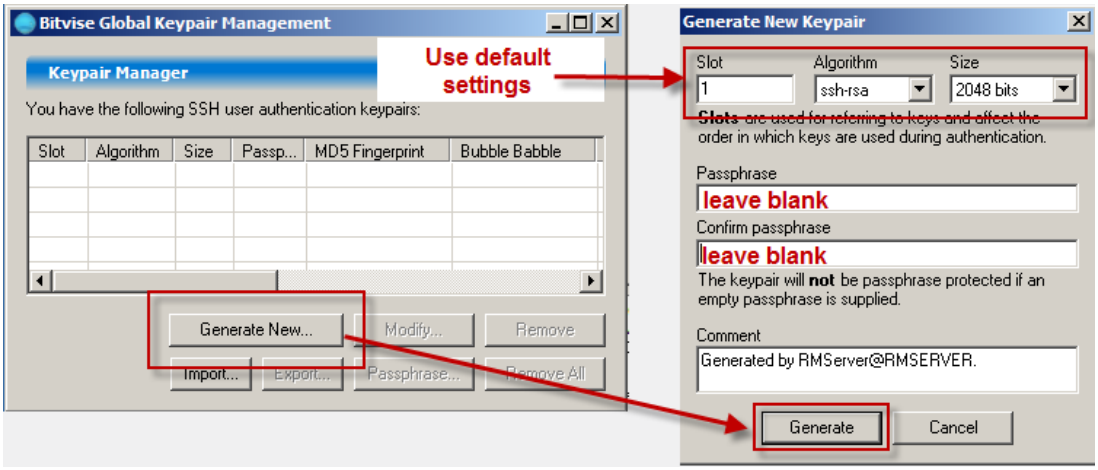
The following steps describe the process of configuring Tunnelier. The steps in this section are critical for the rmserver and cloud computer (hosted by ASI) to communicate. We will begin the configuration process by opening the Tunnelier SSH2 Client program to do the following:

1. Within the Login Tab fill in the following fields with the following information (colored in red):

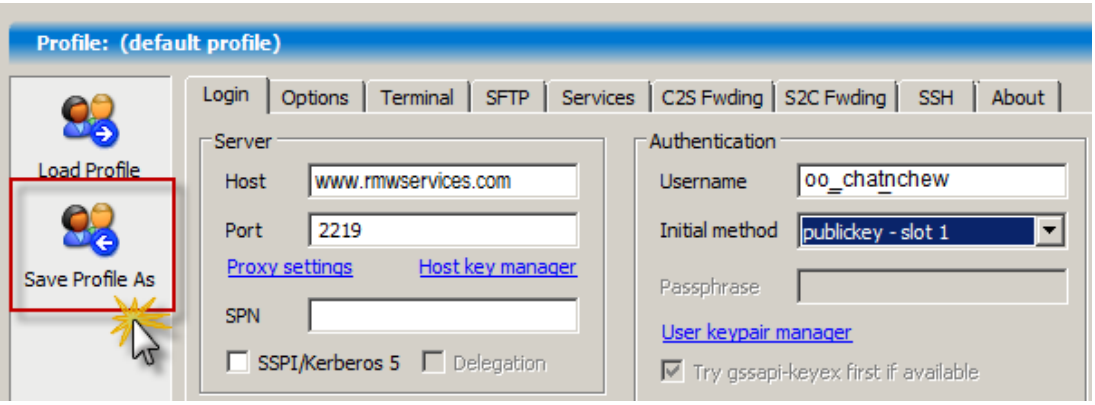
   - **Host:** www.rmwservices.com
   - **Port:** 2219
   - **Username:** oo_chain name. The chain name must be exact. The name is preceded by lower case "oo", then underscore (_), followed by chain name. Example: oo_chatnchew.
   - **Initial method-** none (you will return to adjust this setting after we run the Keypair Manager)



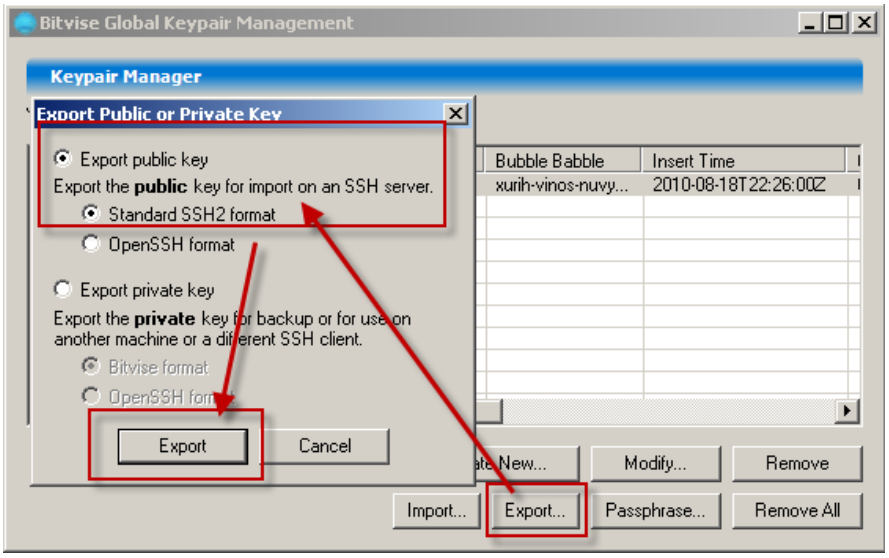
2. Under Authentication, click USER KEYPAIR MGR (pictured above) and then select the “Generate New..” button in the Keypair Management window (pictured on the left below)



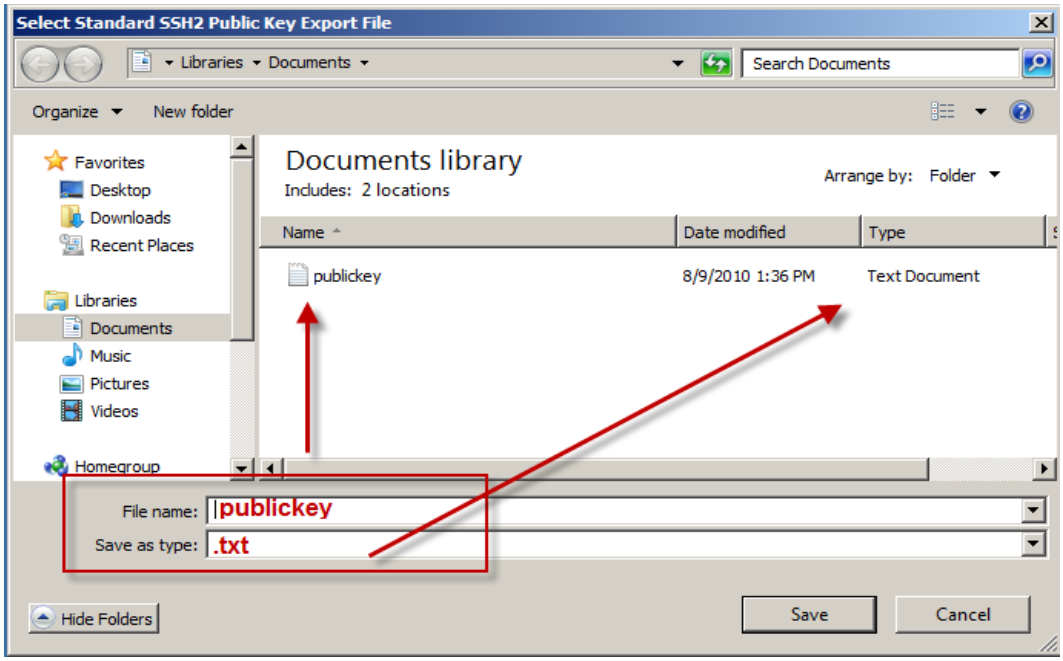
3. Under the Generate New Keypair form select the “Generate” button (pictured on right above). The passphrase settings should be left blank and default settings should be used for the following fields:
    - Slot=1
    - Algorithm= ssh-rsa
    - Size= 2048 bits
4. Under the Authentication section on the Login Tab (Tunnelier SSH2 Client default screen) use the Drop down menu on the “Initial method” field and select the “Public Key-slot 1” option



5. In the next step we will export the public key. While under the Authentication section on the Login Tab select the User Keypair Manager link and then:
    a. Click on the “Export” button in the Keypair Manager.
    b. Verify the Standard SSH2 format is selected (default setting) in the “Export Public or Private Key” window. Next, select the “Export” within the same window.



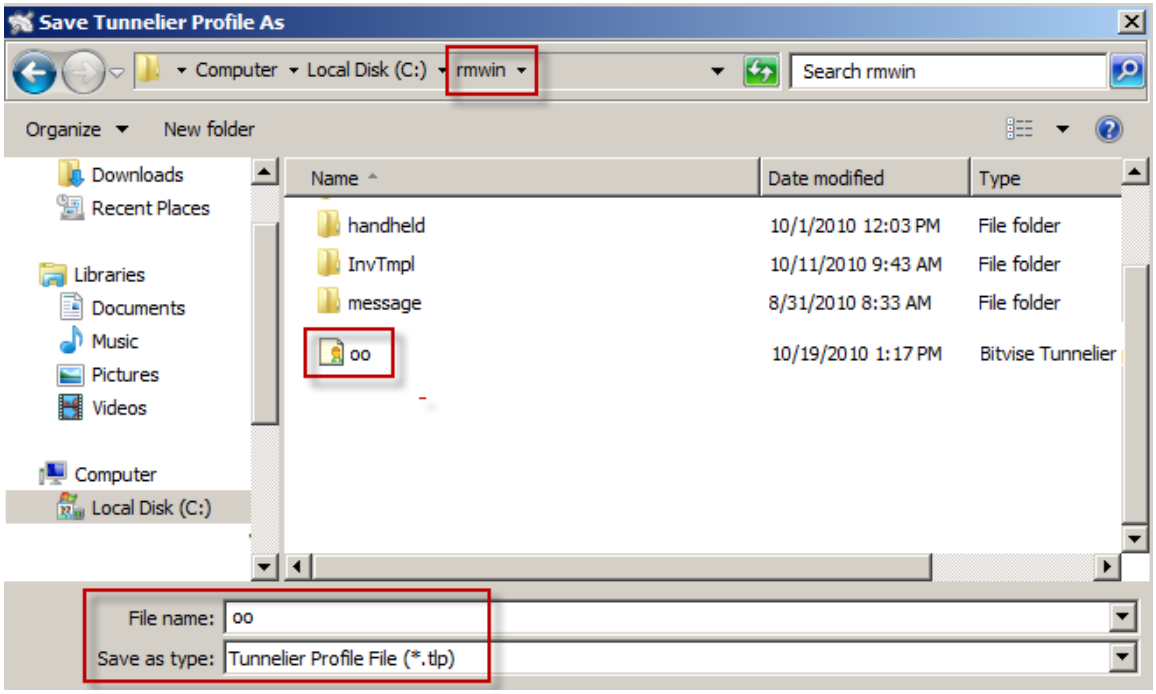
    c. Choose a location where you want to save the profile. It is recommended that you create a special folder to store the document. Name the document “publickey” and save as a text file (.txt). Remember the location of the document: you will need to email (in form of attachment) this to ASI.



d. After saving the document you can return to the default Tunnelier SSH2 Client program screen by closing the Export File and Keypair Manager screens.

At this point you need to email with the "publickey.txt" document attached (do not copy and paste) to support@actionsystems.com. Make sure you identify the restaurant name, contact name, and the Tunnelier username (oo_chain name).

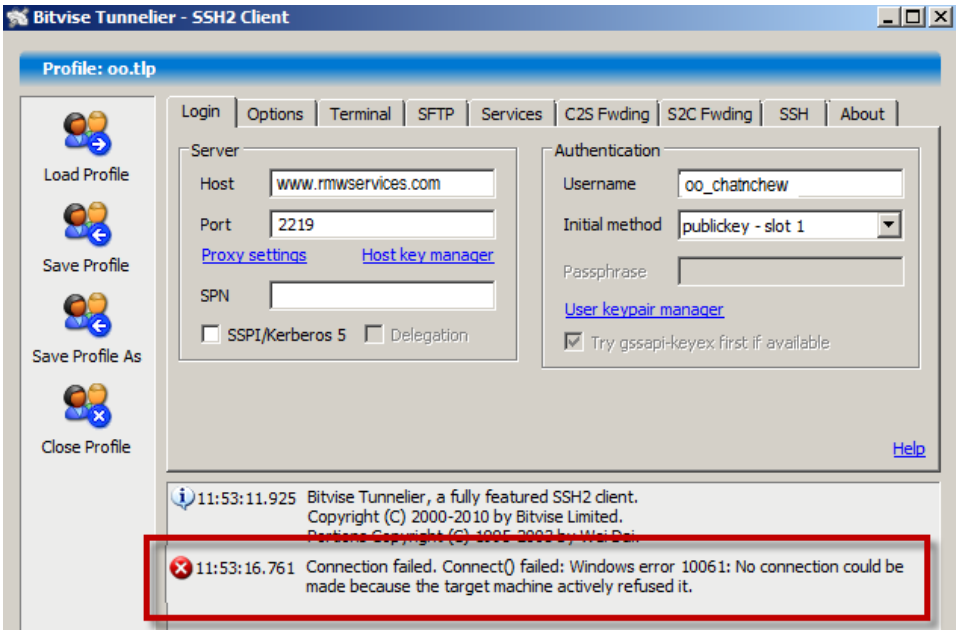
6. Continuing the process we must now create a user profile by:
   a. Select the "Save Profile As" icon in The Profile pane located on the Tunnelier SSH2 Client default screen
   b. Choose a location where you want to save the profile. You can store this anywhere, but a convenient place is in your RMWIN directory. Type "OO" in the File name filed of the "Save Tunnelier Profile As" window. Use the default setting of ".tlp" in the "Save as type" field. Click "Save" after all fields have been successfully entered.



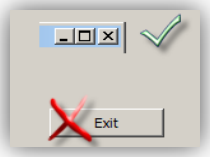
The Bitvise Tunnelier SSH2 Client default screen should look similar to the image below after the profile has been added. Notice the addition of two new icons: Save Profile Ss and Close Profile.

7. Click “Login” at the bottom of the Login tab at the bottom of the Bitvise Tunnelier SSH2 Client default screen and proceed with the following steps:
   a. In the Host verification window click on the Accept and SAVE options
   b. Verify the Public-Slot option in the “Small user authenticate” window.

Note: you will receive an error message similar to the one below if the public key has not been entered by ASI:



8. Select the “S2C Fwrding” tab at the top of the Bitvise Tunnelier SSH2 Client default screen , click the “Add” in the S2C Fwrding form and proceed with the following steps:
    - In the List. Port column enter the port number supplied by ASI Tech Support (e.g. 5099)
    - In the Dest. Port column enter the appropriate port number (9644 for default ver 17 installations. Port 80 is used as the default port on ver 16 installations.)
    - Click “Add” to exit screen
9. Select the “Options” tab at the top of the Bitvise Tunnelier SSH2 Client default screen. Uncheck the following options in the “On Login” pane.
    - Open Terminal
    - Open SFTP
10. Select the radio button “Always reconnect automatically” in the “Reconnection” pane. Close the screen by clicking on the “X” in the upper right hand corner. Do not use the “Exit” button: this will close the program and On Line Orders will not be processed.



ADD TUNNELIER TO WINDOWS START UP

The Tunnelier Client program is necessary to process On Line Orders. This program is one of the key elements that aids in passing data through the rmserver computer to the ASI host computer. For this reason, it is extremely important the Tunnelier Client program be running at all times. The Tunnelier executable (Tunnelier.exe) should be placed in the Windows Start Up folder to insure it is running in the event a computer reboot is necessary (i.e. anti-virus updates requiring computer re-boot).

You will need to do an additional adjust in the Windows Startup menu after the computer restarts. Use the following steps to complete the start up process:

1. Open the Windows Start Up Menu

2. Right-click on the shortcut in the Start Up folder, and add the following to the end of the Target field:

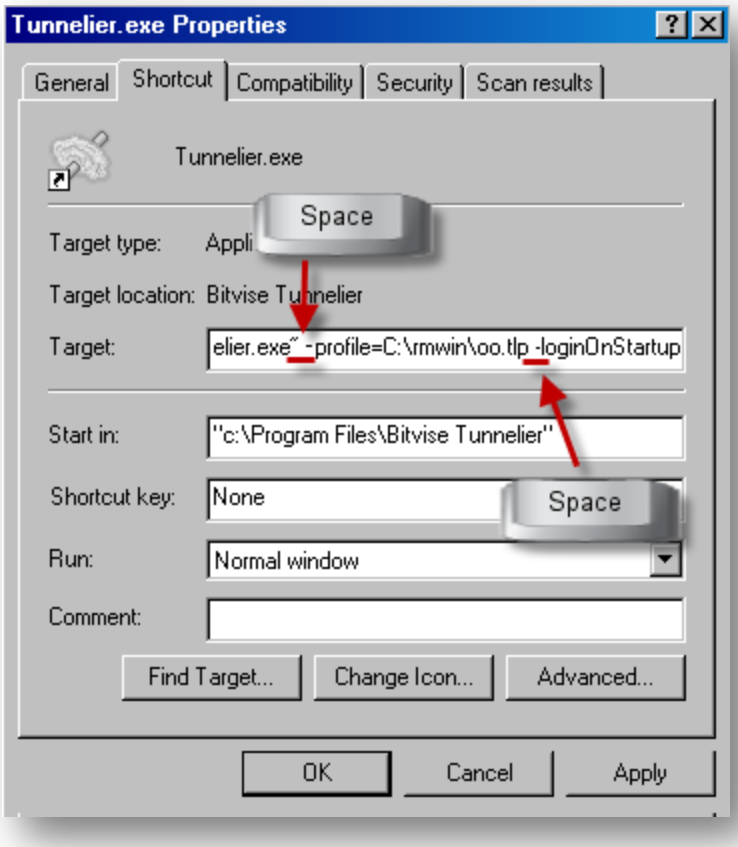
    -profile=c:\rmwin\oo.tlp –loginOnStartup

    The entire target should read like this:

    “c:\Program Files\Bitvise Tunnelier\Tunnelier.exe” –profile=C:\rmwin\oo.tlp -loginOnStartup

The oo.tlp is the user profile we created and saved earlier. The path must be where you saved the user profile (i.e. the rmwin directory in our example would be C:\rmwin).

Note: there is a space between Tunnelier.exe” and –profile and oo.tlp and –loginOnStartup.



TESTING THE CONNECTION

To test that the connection to OO is set up correctly, exit Tunnelier completely (using the Exit button in the lower right of the screen). The system tray icon should disappear. No, launch Tunnelier from the shortcut in the Start Up folder. It should make a connection to the OO Server with no errors (i.e. no little red circle with a white X in it). Then, log into the OO control panel, and click the "test" button on the remote routing configuration page, to verify connectivity.