Wavelink Software Test Plan

Telnet SSH:

SSH (Secure Shell)
SSH is set of programs which employ public/private key technology for authenticating and encrypting sessions between user accounts on distributed hosts on the Internet.

SSH can also be used as a way to "tunnel" other protocols, such as the X Window System protocol, adding encryption to the channel to improve security against packet sniffing and "man in the middle" attacks. When used, SSH looks like a normal (albeit a proxy) server on the local machine which redirects protocol communication across an encrypted channel to the actual server on the other end.

SSH works by the exchange and verification of information, using public and private keys, to identify hosts and users. It then provides encryption of subsequent communication, also by the use of public/private key cryptography.

Telnet does not include the SSH support by default. To add the SSH support, install SSHInstall_10001.exe or SSH_Support_WIN_10001_AV.ava on your Windows 2000/XP computer.
If you are using a CE device, you will also need to install the ActiveSync, AirBEAM or Avalanche version of SSH to that device.

You can tell if SSH is installed on Windows 2000/XP because the Host Profile editor will have the SSH options available and not grayed out when creating a profile. This is similar to the SSL support.

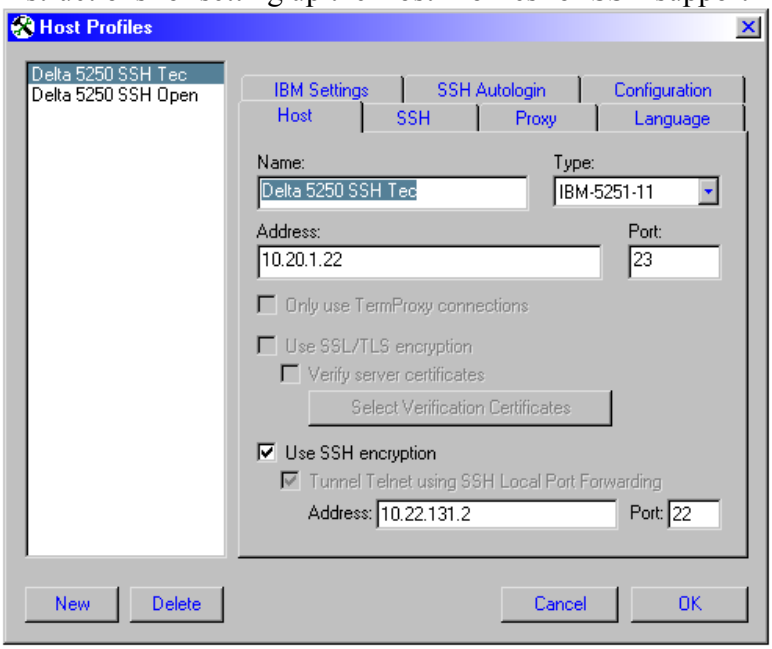
In Telnet, the About Box will show the SSH licensing information if SSH is installed on the device.

Information needed for Testing:

1. Tectia SSH Server is installed to a PC.
    a. IP address: 10.22.131.2 - Port 22
    b. Username: sshuser2 - password: sshpasswd2
2. OpenSSH Server is installed to a PC
    a. IP address: 10.22.131.2 – Port 8022
    b. Username: sshuser2 – password: sshpasswd2
3. There are RSA and DSA SSH-2 private keys located at R:\test\SSH\Tectia for the Tectia server
    a. The user name is: sshuser2

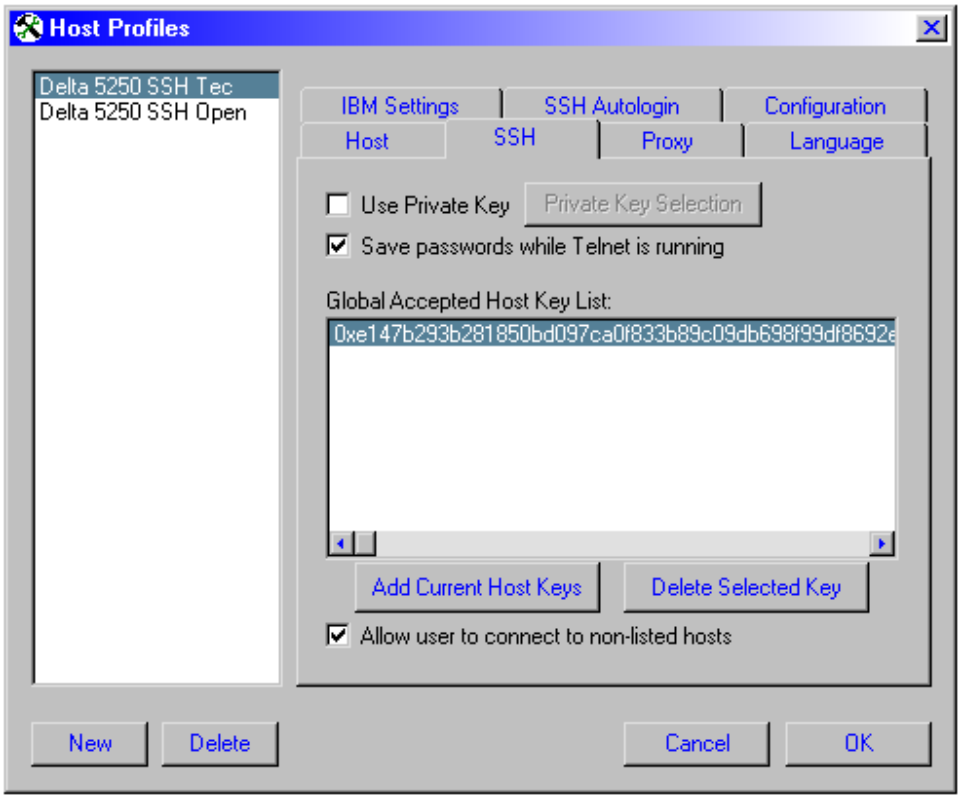
   b. Passwords for the keys are: sshrsa2 for the RSA key and sshdsa2 for the DSA key
4. There are RSA and DSA and Identity(SSH-1 RSA) private keys for the OpenSSH server located at R:\test\SSH\Open
   a. Passwords for the keys are: sshrsa2 for the RSA key and sshdsa2 for the DSA key and for the identity key the password is sshrsa12
5. WebScout server which is used for HHTP and SOCKS 5 Proxy server testing
   a. HTTP: IP address: 10.22.111.4 – Port 8080
   b. SOCKS: IP address: 10.22.111.4 – Port 1080
   c. Username: test – Password: test
6. SocksServ server is a executable server that is used for SOCKS 4 testing and the executable is located at R:\test\SSH\SOCKS4 SERVER
   a. The IP address and port are based on what PC you run the application from

Instructions for setting up the Host Profiles for SSH support



The first listing of "Address" is the IP address of the Host.
The second listing of "Address" is to the SSH server the port listed there is for the SSH server

If the emulation is set to IBM Tunneling is in use automatically and cannot be turned off.

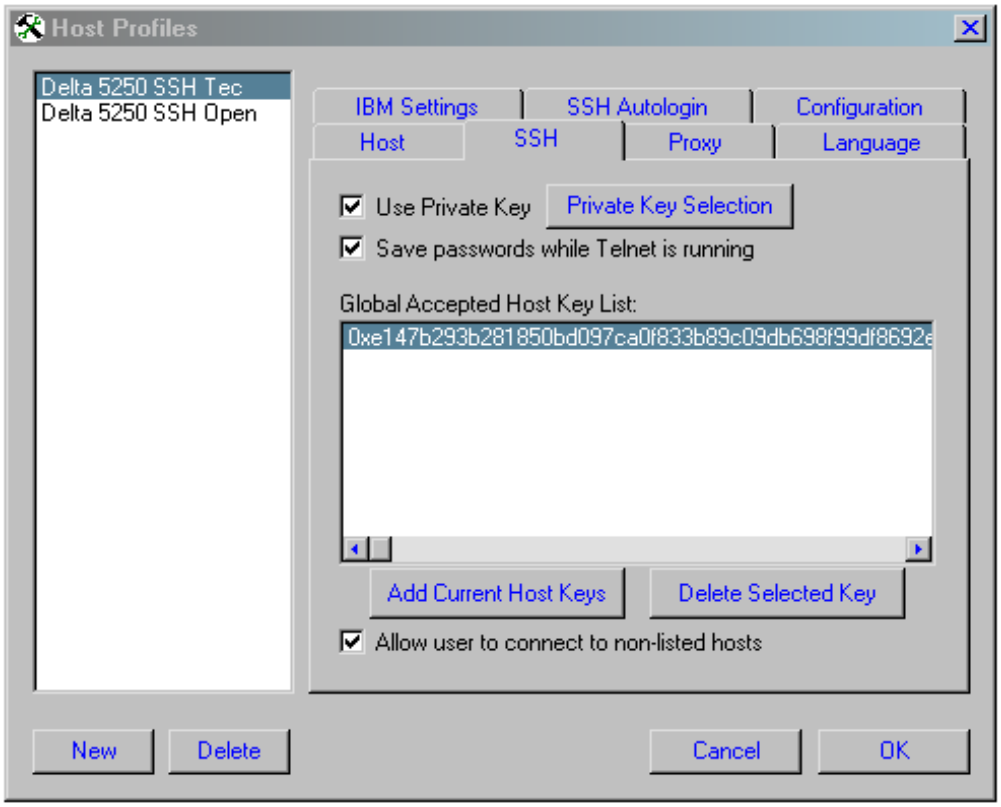


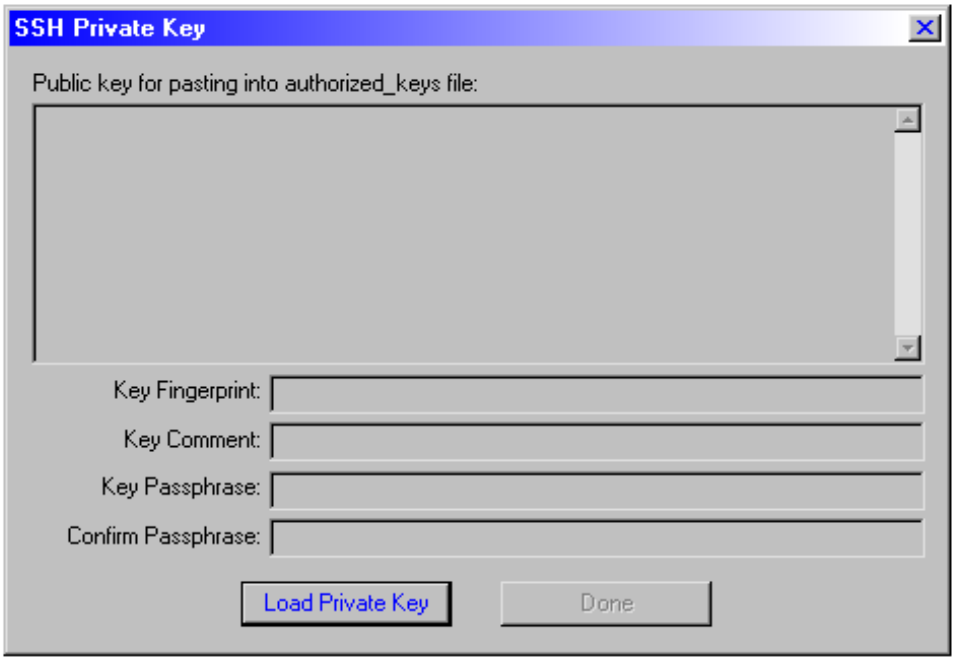
Clicking the “Add Current Host Keys” initiates a connection to the listed SSH server from the Host config screen, it receives the keys and adds them to the Global Accepted Host Key List. (Tectia returns an SSH-2 key; OpenSSH returns an SSH-1 and SSH-2key)

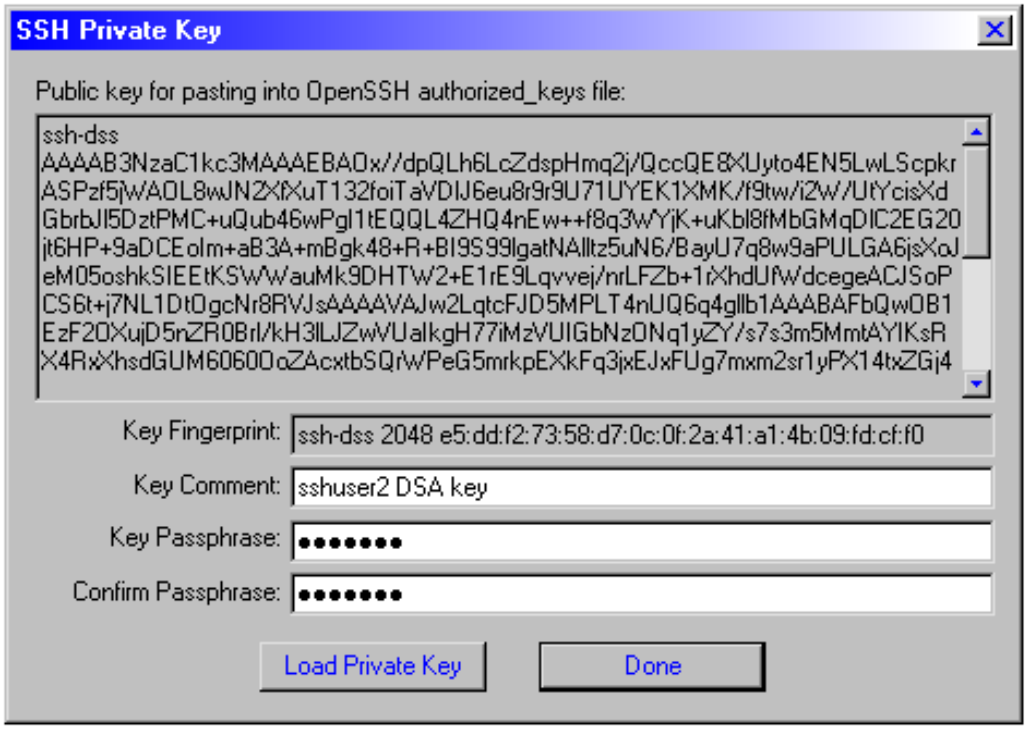
Un-checking the “Save passwords while Telnet is running” will cause the user on the device to enter in the login and password at every session connection.

The “Allow user to connect to non-listed hosts” option by defaults allows the host profile to connect to any host that the device does not have keys for. Unchecking this should be tested and then try to connect to a different SSH server that the keys for that server are not listed. What should happen is the connection should be refused.

The “Use Private Key” option when checked and “Private Key Selection” pressed will open the following dialog

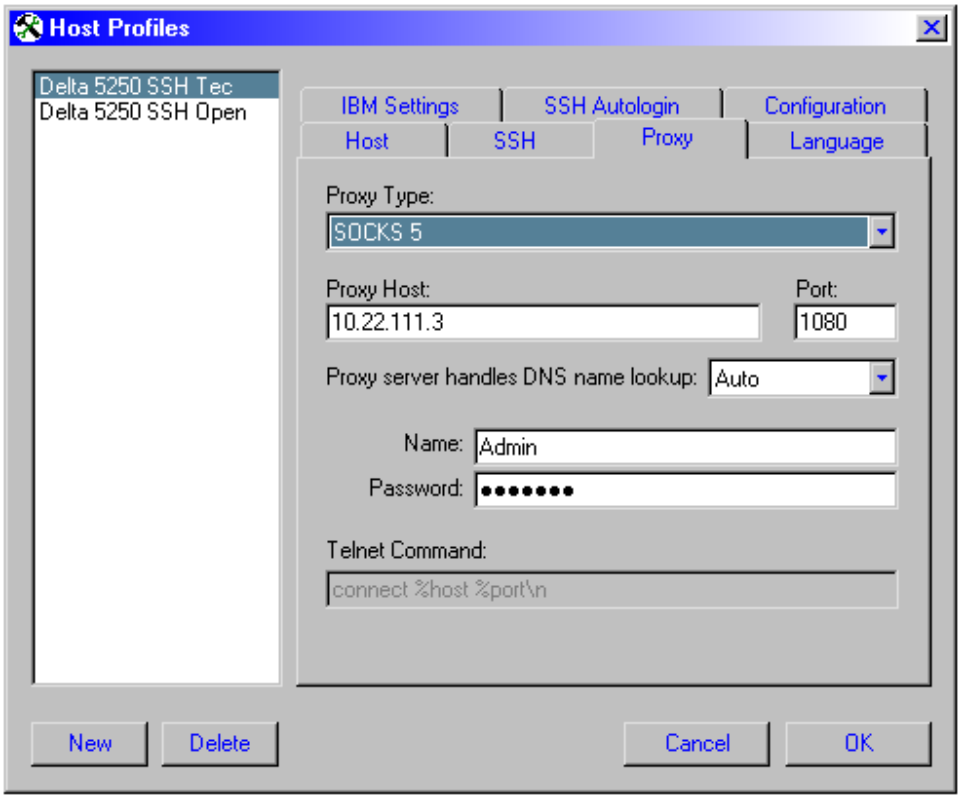

Host Profiles
Delta 5250 SSH Tec
Delta 5250 SSH Open
IBM Settings
SSH Autologin
Configuration
Host
SSH
Proxy
Language
Use Private Key
Private Key Selection
Save passwords while Telnet is running
Global Accepted Host Key List:
0xe147b293b281850bd097ca0f833b89c09db698f99df8692e
Add Current Host Keys
Delete Selected Key
Allow user to connect to non-listed hosts
New
Delete
Cancel
OK


SSH Private Key
Public key for pasting into authorized_keys file:
Key Fingerprint:
Key Comment:
Key Passphrase:
Confirm Passphrase:
Load Private Key
Done



You add the private key from .dat key files. These are the key files located in the R:\test\SSH folder. There is specific keys for which SSH server you are connecting to.

There is a password associated with the keys, but once they are loaded you can change the password the user needs to enter to access the Host. An empty password is valid.



This is the area for Proxy setup. There are 4 different types of Proxy that can be used. SOCKS 4, SOCKS 5, HTTP and Telnet.