

USING SSH WITH TERMINAL EMULATION

This document describes how to install and configure SSH support for the Wavelink Terminal Emulation (TE) Client. Secure Shell (SSH) is a protocol developed for transmitting private information over the Internet. SSH encrypts data that is transmitted during the Terminal Emulation session between the Client and the host or proxy server.

The Telnet Client supports SSH version 1 and 2 and will automatically select the most secure protocol supported.

OVERVIEW OF SSH SUPPORT

In order to use SSH with the TE Client, you will need to install a support utility on the computer from which you will deploy the Client configuration, install a support package on the device running the Client, and configure the host profile(s) for the Client. Then you will need to deploy the new configuration to the Client.

- Installing the SSH Support Utility
- Deploying the SSH Package
- Configuring the Host Profile for SSH Support

INSTALLING THE SSH SUPPORT UTILITY

The SSH support utility must be installed on the Windows PC from which you will deploy the Client configuration before you can configure the Client to use SSH.

To install the Windows SSH support utility on the PC:

1. Obtain the installation files for the Windows SSH support utility from the Wavelink Web site and copy them to the system you will use to install the file on your device. You will need the self-extracting support utility and either the Avalanche, ActiveSync, or AirBeam SSH package for the Client.
2. Install the SSH support utility on the PC from which you will deploy the TE Client by double-clicking the `.exe` file.
3. The Installer Setup screen appears. Click **Next**.
4. Read the License Agreement and agree to the terms by clicking **I Agree**.
5. Click **Install** to accept the default installation location or use the **Browse** button to navigate to the location where you want the files installed.
6. The files install locally. Enable the **Show Readme** option if you want to view the release notes. Click **Finish** to close the installer.

DEPLOYING THE SSH PACKAGE

Use Avalanche or ActiveSync to deploy the SSH support package to the device.

NOTE: Wavelink supports some third-party deployment applications. For more information about supported deployments for your device, please see the Wavelink Web site. If you choose to use a third-party application to configure and install the TE Client, please see the documentation for that application for details on this process.

To deploy the SSH package through Avalanche:

1. Ensure you have obtained the SSH package. From the Avalanche Web Console, create a new software profile or select the profile you want to add the package to.
2. In the Software Packages panel, click **New**.
3. Ensure **Install an Avalanche package** is selected and click **Browse**.
4. Navigate to the location of the SSH package, select the package, and click **Open**.
5. Read and agree to the License Agreement, then click **Next**.
6. The software package is extracted locally. When the package is extracted, click **Next**.
7. Enable the software package and click **Finish**.
8. Ensure that the profile is enabled and applied to the correct location(s), then deploy the profile.

To deploy the SSH package through ActiveSync:

1. Establish an ActiveSync connection to the device.
2. From the desktop computer, double-click the `.exe` file to install the SSH support package.
3. The Installer Setup screen appears. Click **Next**.
4. Read the License Agreement and agree to the terms by clicking **I Agree**.
5. Click **Install** to accept the default installation location or use the **Browse** button to navigate to the location where you want the files installed.
6. The files install locally. Enable the **Show Readme** option if you want to view the release notes. Click **Finish** to close the installer.
7. If you enabled the **Run Wavelink SSH ActiveSync Support** option, the package begins to install.

-Or-

If you did not enable that option or if you need to install the package to a different device: from the desktop computer, click **Start > Programs > Wavelink SSH ActiveSync Support > Install to Device**.

8. A prompt appears, asking if you want to install to the default directory. Click **Yes** to install to the default location, or **No** to select a different destination.
9. The package installs, and a prompt appears to instruct you to check the mobile device screen to see if there are any additional steps. Follow the steps, if any, and the package will finish installation.
10. Once the package is installed on the mobile device, you can configure the Client to use SSH.

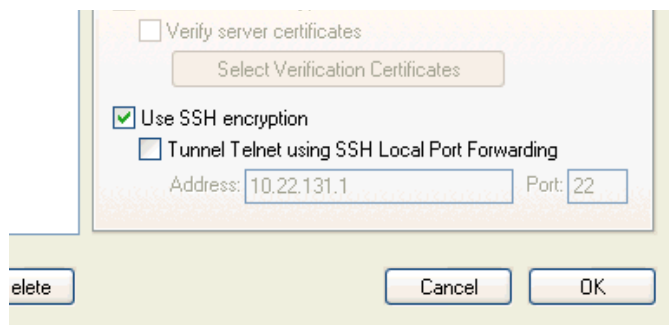
CONFIGURING THE HOST PROFILE FOR SSH SUPPORT

SSH support is configured from the Host Profiles window of the TE Client configuration utility.

NOTE: SSH is only an active option if SSH support has been installed on the PC running the Telnet Client configuration utility.

To configure SSH:

1. Access the host profiles configuration utility for the Telnet Client.
2. Select a host profile from the list or click **New** to create a new host profile.
3. Enter the information of the Telnet host to connect to.
4. Enable the **Use SSH encryption** option.



Enabling SSH

5. If you are using IBM emulation, type the address that will be used for port forwarding in the text box.

NOTE: SSH local port forwarding is required if an IBM emulation type is selected.

6. Click the **SSH** tab to configure private keys and security options.

SSH Tab

7. To save your passwords during a Telnet session, check the **Save Passwords while Telnet is running** option. This stores the passwords so they do not have to be re-entered.

NOTE: The passwords will be erased each time you exit the TE Client.

The following sections provide instructions for configuring proxy settings, autologin, SSH parameters, and private keys. When you have configured the Client, deploy the new configuration to the device.

CONFIGURING PROXY SETTINGS IN SSH

You may need to go through a proxy server in order to connect to the SSH server. Proxy settings allow you to get your data through a firewall, if one is present.

To configure proxy settings:

1. From the Host Profile window, select the **Proxy** tab.

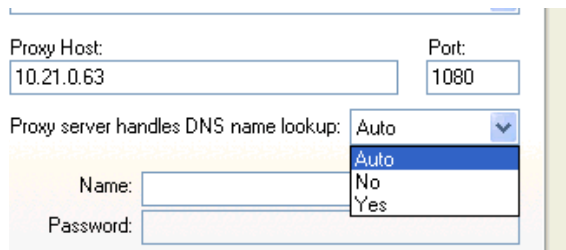
Proxy Settings

2. In the **Proxy Type** drop-down list, select the proxy type.

- Selecting **HTTP** allows you to proxy your connections through a web server.
- Selecting **SOCKS 4** or **SOCKS 5** allows you to proxy your connections through a SOCKS server.
- Selecting **Telnet** allows you to make a Telnet connection directly to the firewall machine in order to connect through to an external host.

3. Enter the proxy host address and port number.

4. From the drop-down list, select the method by which want the proxy server to perform the DNS name look-up if your host name is a string instead of an IP address.



DNS Name Lookup

- If you select **No**, the SSH client will always do its own DNS, and will always pass an IP address to the proxy.
 - If you select **Yes**, the SSH client will always pass host names straight to the proxy without trying to look them up first.
 - If you select **Auto** (default), the SSH client will handle the proxy based on the type: Telnet and HTTP proxies will have the host names passed straight to them; SOCKS proxies will not.
5. Enter a name and password if your proxy requires authentication. Username and password authentication is supported for HTTP proxies, SOCKS 5 and Telnet proxies. SOCKS 4 proxies support the username but not passwords.
6. Enter the Telnet command the proxy will use, if using Telnet proxy.

If you are using the Telnet proxy type, the usual command required by the firewall's Telnet server is `connect` followed by a host name and a port number. If your proxy needs a different command, you can enter an alternative here.

In this string, you can use `\n` to represent a new-line, `\r` to represent a carriage return, `\t` to represent a tab character, and `\x` followed by two hex digits to represent any other character. `\\` is used to encode the `\` character itself. Also, the special strings `%host` and `%port` will be replaced by the host name and port number you want to connect to. The strings `%user` and `%pass` will be replaced by the proxy username and password you specify in step 5. To get a literal `%` sign, enter `%%`.

If the Telnet proxy server prompts for a name and password before commands can be sent, you can use a command such as:

```
%user\n%pass\nconnect %host %port\n
```

This will send your username and password as the first two lines to the proxy, followed by a command to connect to the desired host and port.

NOTE: If you do not include the %user or %pass tokens in the Telnet command, then the **Name** and **Password** configuration fields will be ignored.

7. Click **OK** to save the proxy configurations.

SSH AUTOLOGIN

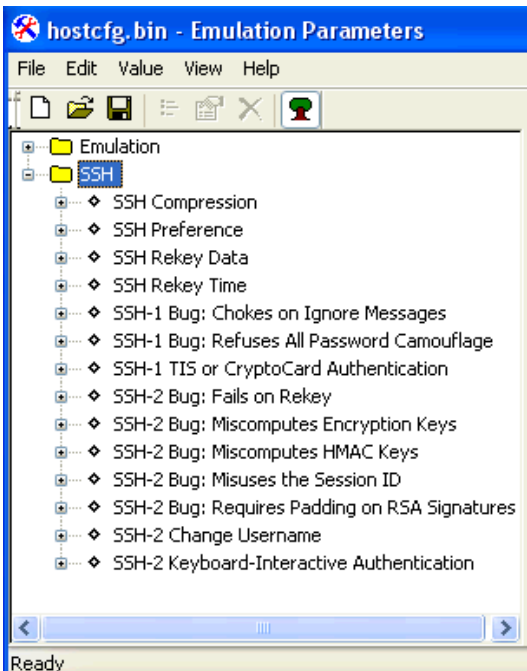
The Host Profiles window has an SSH Autologin tab that allows you to specify and save the username and/or password for SSH connections so that you won't be prompted for them each time you login. If the username or password fields are left blank, you will be prompted for them each time you connect.

If you are tunneling VT, HP or XTERM over SSH, the Autologin tab will also be available for you to enter the Telnet username and password. If you are using IBM emulation, the Autologin tab will not be available.

CONFIGURING THE SSH PARAMETERS

Use the Configuration tab of the Host Profiles window to modify the emulation parameters for a specific host profile.

When you click **Modify**, the Emulation Parameters screen opens where you will see that the SSH parameters have been added to the tree view. Each parameter has a description that appears in the right pane when you click on the name of the parameter.



SSH Parameters

From this screen, you can specify the SSH settings to be applied to all host profiles for the Client.

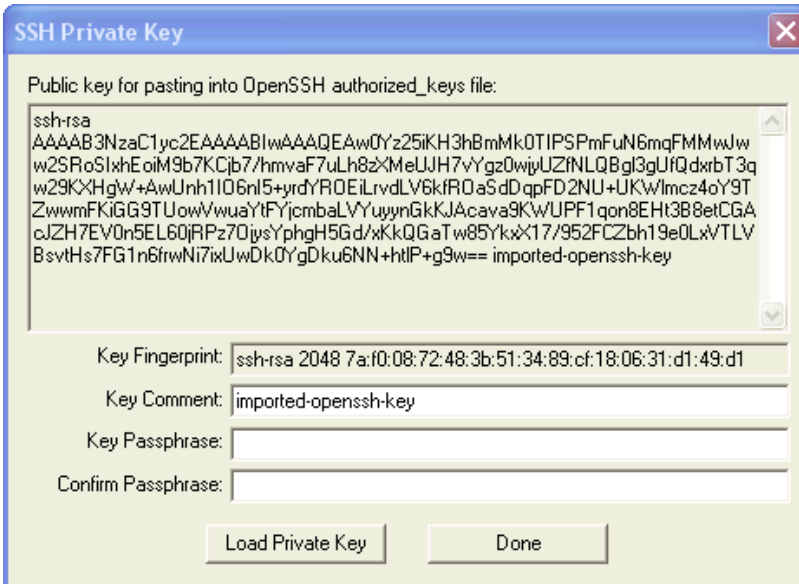
CONFIGURING PRIVATE KEYS

Private keys are an optional way of allowing you to authenticate to the SSH server. Refer to the documentation for your SSH server for instructions on how to create and install user-specific private keys on the SSH server.

To configure private keys:

1. Access the host profiles configuration utility for the Telnet Client.
2. Select a host profile.
3. Enable the **Use SSH encryption** option.
4. Click the **SSH** tab to configure private key encryption.
5. Enable the **Use Private Key** option, then click **Private Key Selection**.

The *SSH Private Key* dialog box appears.



Load Private Key

6. Click **Load Private Key** to open a window where you can browse for the private key file.
7. Locate the file and click **Open**.

Private keys from OpenSSH, SSH.com (Tectia), and PuTTY are recognized. Other private keys will need to be converted to one of these formats before they can be loaded.

The *Enter Passphrase* dialog box appears.

8. Enter the passphrase for the private key.

The passphrase is whatever was specified at the time the private key was created.

9. Click **OK** to return to the **SSH Private Key** dialog box.

10. Change the **Key Comment** and **Key Passphrase** values, if desired.

NOTE: A blank passphrase is allowed but not recommended.

11. Click **Done**.

You will need to re-enter the passphrase for the private key in order to view or edit it.

SECURITY OPTIONS

Every server identifies itself by means of a host key. Once the Telnet client knows the host key for a server, it will be able to detect if a malicious attacker redirects your connection to another machine. Host key checking guarantees that you are communicating with the correct server.

To add a host key to the **Global Accepted Host Key List**:

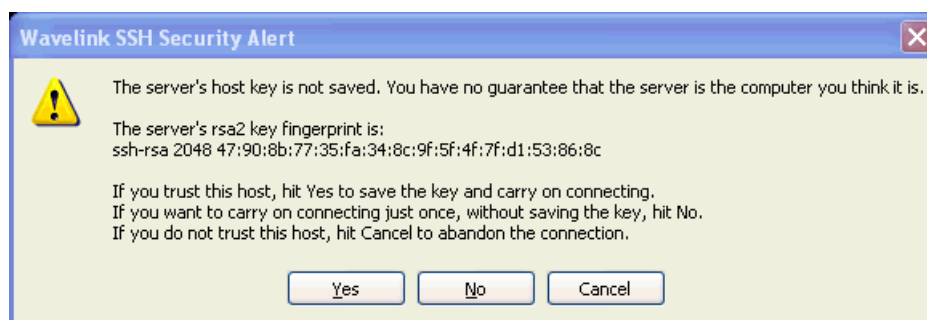
1. Access the host profiles configuration utility for the Telnet Client.
2. Select a host profile.
3. Enable the **Use SSH encryption** option.
4. In the *Host Profiles* window, click the **SSH** tab.
5. Click **Add Current Host Keys**.

A dialog box appears telling you that the public keys for the SSH server, specified on the host page, were detected and added to the list.

6. Enable **Allow user to connect to non-listed hosts** to allow connections to a host whose key is not listed in the **Global Accepted Host Key List**.

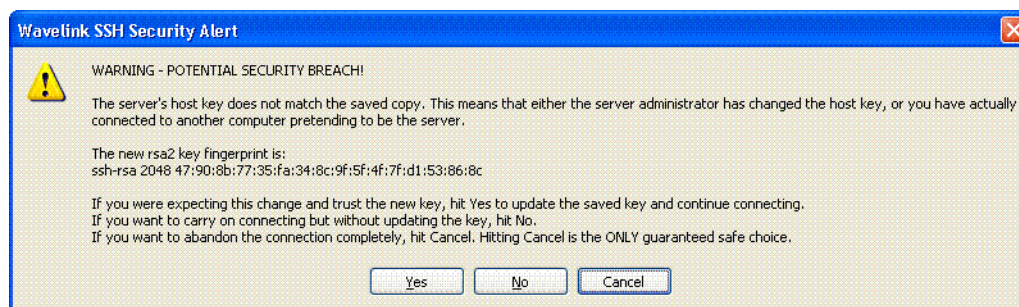
TROUBLESHOOTING HOST KEY ERROR MESSAGES

If no keys are listed or if all the keys you have are different than the ones provided by the server you want to connect to, the following error message appears:



SSH Security Alert

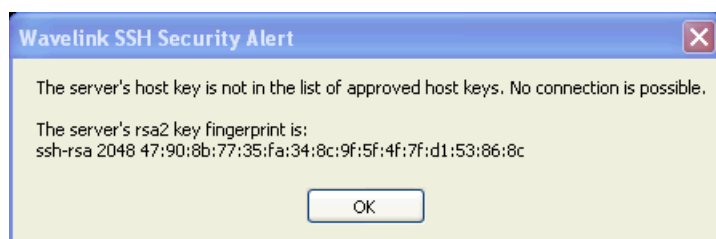
If you connect to the server and the key on the server has been changed, the following error message appears:



Security Breach

This message also appears if you are connecting to a different server than the one to which you previously connected. This could be an indication that someone is attempting to duplicate your server.

If the SSH server returns a key that is not in the **Global Accepted Host Key List** and the **Allow user to connect to non-listed hosts** option is disabled, the Telnet client will not be allowed to connect to that server and the following error message appears:



Connection Refused

OTHER RESOURCES

For more information on using the Terminal Emulation Client or for instructions on how to deploy the Client configuration to the device, see the *Terminal Emulation Client User Guide* on the Wavelink Web site.

DOCUMENT HISTORY

- 02/16/2006. Document created.
- 22/11/2010. Document updated.



Wavelink Corporation
USA and Canada: 1.888.697.WAVE (9283)
Outside the USA and Canada: + 800 WAVELINK (9283 5465)
CustomerService@wavelink.com

