

This document provides information on the SSH support available in Telnet Client 5.11

OVERVIEW

- Overview of SSH
 Support
- Installing Windows
 SSH Support
- Configuring the host
 profile for SSH
 support
- Deploying Windows
 SSH Support
- Revision History

TELNET CLIENT 5.11 SSH SUPPORT

This document describes how to install and configure SSH support in Wavelink Telnet Client 5.11.

OVERVIEW OF SSH SUPPORT

Secure Shell (SSH) is a protocol developed for transmitting private information over the Internet. SSH encrypts data that is transferred over the Telnet session.

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

This document describes the following:

- Installing Windows SSH support utility
- · Configuring the host profile for SSH support
- Deploying Windows SSH support to the device through Avalanche or ActiveSync

INSTALLING WINDOWS SSH SUPPORT

Installing SSH support is a two-step process. First, install SSH support on the PC from which you will deploy Telnet. Once you install SSH support on the PC, use Avalanche or ActiveSync to deploy the utility to the device.

To install SSH support on your PC:

1. Obtain the installation executable for SSH support.

NOTE: To obtain the Wavelink SSH support utility install, go to http://www.wavelink.com/downloads/files/sshagreement.aspx.

2. Install SSH support on the PC from which you will deploy the Telnet Client.

CONFIGURING THE HOST PROFILE FOR SSH SUPPORT

SSH support is configured from the Host Profiles window of the 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.

NOTE: Telnet must be tunneled using SSH local port forwarding if an IBM emulation type is selected.

VT Settings SSI	H Autologin Configuration
331	
Name: New Host	Type:
Address:	Port:
10.20.131.2	8022
Use SSL/TLS encryptio	in ites
	tion Lettificates
Use SSH encryption	SSH Local Port Forwarding
Address: 10.22.131.	.1 Port: 22

Enabling SSH

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

😵 Host Profiles					×
New Host	VT Calling		u da la sia	Cauffernation	_
	VISettings	55H A	Nutologin	Configuration	_
	Host	SSH	Proxy	Language	
	📃 Use Priva 🔽 Save pas:	te Key Privat swords while Tel	e Key Selectio net is running	in	
	Global Accep	ted Host Key Lis	:t:		
	Add Cur	rent Host Keys	Delete S	elected Key	
		1			
		to connect to n	on-listed hosts		
New Delete			Cancel	ок	

SSH Tab

Use of private keys is optional. For more information on private keys, refer to Configuring Private Keys on page 8.

You can verify that the client will connect with the correct SSH server by using the Global Accepted Host Key List options. For more information, refer to Security Options on page 10.

6. To save your passwords in the current Telnet session, check the Save Passwords while Telnet is running option.

NOTE: The passwords will be erased each time you exit Telnet.

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.

😵 Host Profiles		X
New Host	VT Settings Autologin SSH Autologin Configuration Host SSH Proxy Language Proxy Type: SOCKS 4	
	Iour Host Poit 10.21.0.63 1080 Proxy server handles DNS name lookup: Auto Name:	
	Telnet Command:	
	connect %host %port\n	100
New Delete	Cancel OK	

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.

🛠 Host Profiles				×
New Host	VT Settings Host Proxy Type: SOCKS 4 Proxy Host: 10.21.0.63 Proxy server H Name Password Telnet Comma	Autologin SSH nandles DNS n e: f: f: st %port\n	SSH Autologin Proxy ame lookup: Auto Auto No Yes	Configuration Language Port: 1080
New Delete			Cancel	ОК

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 Suser or Spass 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

SSH Autologin allows you to specify and save the username and/or password to use 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.

🛠 Host Profiles					×
New Host SSH1	Host	SSH	Proxy	Language	
	VT Settings This is to spe connections. for them while Name: Password:	SSH / cify the Name a If they are left b connecting.	Autologin nd/or Passwor plank, the user	Configuration d to use for SSH will be prompted	
New Delete			Cancel	ОК	

SSH Autologin

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.

🛠 Host Profiles				
New Host SSH1	Host VT Settings	SSH Autologin	Proxy SSH Autologin	Language Configuration
	F Name:	Prompts	CFG in terminal Resp	ponses
	Password:	Password:		
	Command:			
				050550555
New Delete			Cancel	ОК

Autologin

CONFIGURING THE SSH PARAMETERS

Use the Configuration tab to modify the emulation parameters for a specific host profile.

🛠 Host Profiles					×
Host Profiles	Host IBM Setting Emulation pa	SSH Is SSH / rameters for this Modify	Proxy Autologin host profile can Reset	Language Configuration be modified.	X
New Delete			Cancel	ОК	

Configuration

When you click Modify, the Emulation Parameters screen opens where you will see that the SSH parameters has been added to the tree view. Clicking Reset will return the parameters to their previous settings.

🛠 hostofg.bin - Emulation Parameters				
File Edit Value View Help				
Í 🗅 📽 🖬 🗄 🗃 🗙 💽				
🖻 🗝 🔁 SSH				
🕸 🗠 🗢 SSH Compression				
👜 🗠 🗢 SSH Preference				
🕸 🗠 🗢 SSH Rekey Data				
👜 🗠 SSH Rekey Time				
👜 🔶 SSH-1 Bug: Chokes on Ignore Messages				
👜 🔶 SSH-1 Bug: Refuses All Password Camouflage				
SSH-1 TIS or CryptoCard Authentication				
💩 🔶 SSH-2 Bug: Fails on Rekey				
💩 🔶 SSH-2 Bug: Miscomputes Encryption Keys				
💩 🔶 SSH-2 Bug: Miscomputes HMAC Keys				
💩 🔶 SSH-2 Bug: Misuses the Session ID				
💩 🔶 SSH-2 Bug: Requires Padding on RSA Signatures				
🖢 🗠 🔶 SSH-2 Change Username				
💩 🔶 SSH-2 Keyboard-Interactive Authentication				
<				
Ready				

SSH Parameters

You can specify the SSH settings that should be applied to all host profiles in the Emulation Parameters utility.

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.

Host Profiles					×
New Host	VT Setting	s SSH A	utologin	Configuration	
	Host	SSH	Proxy	Language	_
	📃 Use Priva	ate Key Privat	e Key Selectio	on	
	🔽 Save pas	swords while Tel	net is running		
	Global Acce	pted Host Key Lis	:t:		
	Add Cu	rrent Host Keys	Delete 9	Selected Key	
	Allow use	er to connect to n	on-listed hosts	\$	
New Delete			Cance	н ок	

Private Key Encryption

5. Enable the Use Private Key option, then click Private Key Selection.

The SSH Private Key dialog box appears.

SSH Private Key	×
Public key for pasting into OpenSSH authorized_keys file:	
sshrisa AAAAB3NzaC1yc2EAAAABIwAAAQEAw0Yz25iKH3hBmMk0TIPSPmFuN6mqFMMwJw w2SRoS1xhEoiM9b7KCjb7/hmvaF7uLh8zXMeUJH7vYg20wiyUZ/NLQBgl3gUfQdxbT3q w29KXHgW+AwUnh1106nI5+yrdYR0EiLrvdLV6kfR0aSdDqpFD2NU+UKVImcz4oY9T ZwwmFkiGG9TUowVwuaYtFYjcmbaLVYuyynGkKJAcava3KWUPF1qon8EH1388etCGA cJZH7EV0n5EL60jRPz70jysYphgH5Gd/xKkQGaTw85YkxX17/952FCZbh19e0LxVTLV BsvtHs7FG1n6frwNi7ixUwDk0YgDku6NN+htIP+g9w== imported-openssh-key	
Key Fingerprint: ssh-rsa 2048 7a;f0:08:72:48:3b;51:34:89:cf:18:06:31:d1:49:d1	-
Key Comment: imported-openssh-key	
Key Passphrase:	
Confirm Passphrase:	
Load Private Key Done	

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.

Enter Passphrase	×
Enter passphrase for key C:\Temp\id_rsa	
OK Cancel	

Enter Passphrase

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 guaruntees 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.

🛠 Host Profiles	
New Host	VT Settings SSH Autologin Configuration Host SSH Proxy Language
	Use Private Key Private Key Selection
	Global Accepted Host Key List:
	Add Current Host Keys Delete Selected Key Allow user to connect to non-listed hosts
New Delete	Cancel OK

Global Accepted Host Key List

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.

🛠 Host Profiles			×
New Host	VT Settings Host SSI Use Private Key Save passwords v Global Accepted Hos 0x23,0xc7re8436268 Add Current Hos Add Current Hos	SSH Autologin H Proxy Private Key Selecti vhile Telnet is running t Key List: 0d56ef146136423d85 7acf7c0fa680c865es t Keys Delete	Configuration Language
New Delete		Canc	el OK

Public Keys Added to 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.

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:

Wavelink SSH Secu	rity Alert	×
The server's The server's ssh-rsa 2048 If you trust t If you want t If you do not	host key is not saved. You have no guarantee that the server is the computer you think i rsa2 key fingerprint is: 147:90:8b:77:35:fa:34:8c:9f:5f:4f:7f:d1:53:86:8c this host, hit Yes to save the key and carry on connecting. to carry on connecting just once, without saving the key, hit No. t rust this host, hit Cancel to abandon the connection. <u>Y</u> es <u>No</u> Cancel	it is.

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:

Wavelink SSH Security Alert		
The server's host key is not in the list of approved host keys. No connection is possible.		
The server's rsa2 key fingerprint is: ssh-rsa 2048 47:90:8b:77:35:fa:34:8c:9f:5f:4f:7f:d1:53:86:8c		
ок		

Connection Refused

DEPLOYING WINDOWS SSH SUPPORT

You can use Avalanche or ActiveSync to deploy SSH support to the device.

To deploy SSH support through Avalanche:

- 1. Obtain the Avalanche SSH support file.
- 2. Open Avalanche Manager and connect to an agent.
- 3. From the Software Management menu in Avalanche Management Console, select Install Software Package.
- 4. Browse to the location of the Avalanche SSH support package and select the package.
- 5. Select the software collection to which you want to install the SSH support package and click Next.
- 6. Click Yes to agree to the license agreement.
- 7. Enable the SSH support package by right-clicking the package and selecting Enable Package.
- 8. Perform an Avalanche update on the device to download the SSH support package to the device.

If you use ActiveSync to install SSH support, you will need to install the package to each device separately.

To install SSH support using ActiveSync:

- 1. Obtain the Wavelink SSH support install from http://www.wavelink.com/downloads/files/sshagreement.aspx.
- 2. In the Wavelink welcome screen, click Next.
- 3. Click I Agree to accept the license agreement.
- 4. Click Yes to install using the default application install directory.
- 5. Click OK to complete the install.

You will need to run the application again to install to other CE devices.

REVISION HISTORY

•

02/16/2006. Document created.



Wavelink Corporation 11335 NE 122nd Way, Suite 200 Kirkland, WA 98034 Main: 425.823.0111

www.wavelink.com

