TELNET CLIENT 5.0 SSL/TLS SUPPORT

This document provides information on the SSL/TLS support available in Telnet Client 5.0

OVERVIEW

- Overview of SSL/TLS Support
- Installing the SSL/TLS support utility
- Deploying the SSL/TLS support utility
- Configuring SSL/TLS
- Configuring certificate verification

This document describes how to install and configure SSL/TLS support and verification certificates in Wavelink Telnet Client 5.0.

OVERVIEW SSL/TLS SUPPORT

Secure Sockets Layer/Transport Layer Security (SSL/TLS) is a protocol developed for transmitting private information over the Internet. SSL/TLS encrypts data that is transferred over the Telnet session.

Verification certificates validate the server with which you are communicating.

The Telnet Client 5.0 has options to enable SSL/TLS support and verification certificates. The Telnet Client supports SSL Version 2, SSL Version 3, and TLS Version 1 protocols and will automatically select the most secure protocol that the Telnet host supports.

This document describes the following:

- Installing the Windows SSL/TLS support utility to the PC.
- Deploying the SSL/TLS support utility to the device through Avalanche.
- Configuring the host profile for SSL/TLS support.
- Enabling and configuring verification certificates.

INSTALLING THE SSL/TLS SUPPORT UTILITY

Installing the SSL/TLS support utility is a two-step process. First, install the Windows SSL/TLS support utility on the PC from which you will deploy the Telnet. Once you install the SSL/TLS support utility on the PC, use Avalanche to deploy the utility to the device.

To install the Windows SSL/TLS support utility on the PC

1. Obtain the installation executable for the Windows SSL/TLS support utility.

Note: To obtain the Wavelink SSL/TLS support utility install, downloading any of the Telnet 5.0 clients from the Wavelink web site or go to http://www.wavelink.com/downloads/files/sslagreement.aspx.

2. Install the SSL/TLS support utility on the PC from which you will deploy the Telnet Client.

DEPLOYING THE SSL/TLS SUPPORT UTILITY

You can use Avalanche to deploy the SSL/TLS support utility to the device.

To deploy the SSL/TLS utility through Avalanche

1. Obtain the Avalanche SSL/TLS support file.

2. From the Software Management menu in Avalanche Management Console, select Install Software Package.

3. Browse to the location of the Avalanche SSL/TLS support package and select the package.

4. Select the software collection where you want to install the SSL/TLS support package.

5. Click Next.

6. Click Yes to agree to the license agreement.

7. Enable the SSL/TLS support package.

8. Perform an Avalanche update on the device to download the SSL/TLS support package to the device.

CONFIGURING SSL/TLS SUPPORT

The SSL/TLS support is configured from the Host Profiles window of the configuration utility.

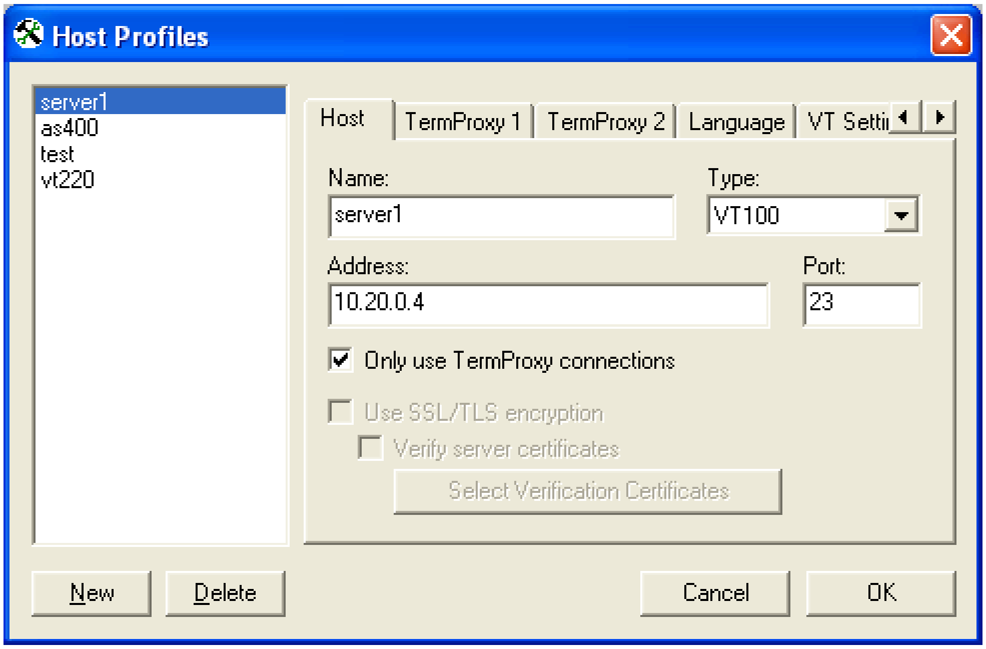
Note: SSL/TLS is only an active option if SSL/TLS support has been installed on the PC running the Telnet Client configuration utility.

To configure SSL/TLS

1. Access the host profiles configuration utility for the Telnet Client.

2. Select or create a new host profile.

3. Enable the `Use SSL/TLS` encryption option.



server1
as400
test
vt220

Name: server1

Type: VT100

Address: 10.20.0.4

Port: 23

☑ Only use TermProxy connections

□ Use SSL/TLS encryption

□ Verify server certificates

Enabling SSL/TLS

4. Click `OK`.

5. Download the new Telnet Client configuration to the mobile device.

CONFIGURING VERIFICATION CERTIFICATES

Clients use verification certificates to verify that they are communicating with the correct server. Verification certificates are not required but are highly recommended.

ENABLING VERIFICATION CERTIFICATES

Use the *Host Profiles* dialog box to enable verification certificates. Once you enable verification certificates you have options to create, insert, or remove certificates.

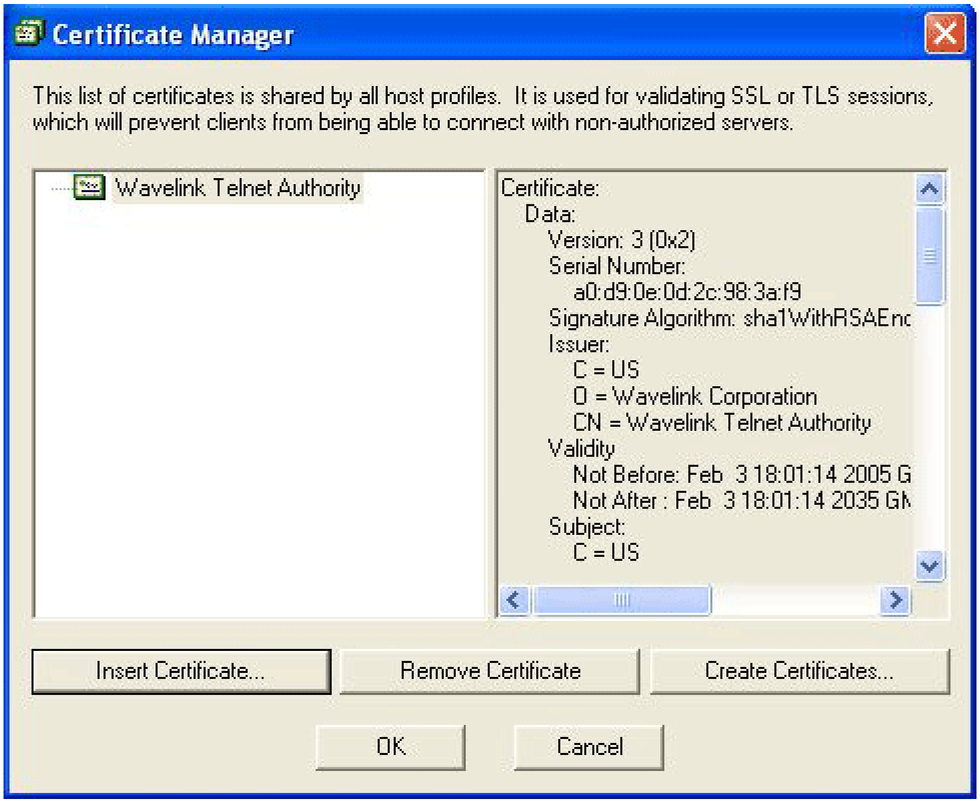
To enable verification certificates

1. Access the host profiles configuration utility for the Telnet Client.

2. In the *Host Profiles* dialog box, enable the `Verify server certificates` option.

3. Click `Select Verification Certificates`.

4. Use the *Certificate Manager* dialog box to create, insert or remove a certificate for use with the Host Profile.



Certificate Manager

This list of certificates is shared by all host profiles. It is used for validating SSL or TLS sessions, which will prevent clients from being able to connect with non-authorized servers.

Wavelink Telnet Authority

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      a0:d9:0e:0d:2c:98:3a:f9
    Signature Algorithm: sha1WithRSAEnc
    Issuer:
      C = US
      O = Wavelink Corporation
      CN = Wavelink Telnet Authority
    Validity
      Not Before: Feb  3 18:01:14 2005 G
      Not After : Feb  3 18:01:14 2035 GN
    Subject:
      C = US
```

Certificate Manager Dialog Box

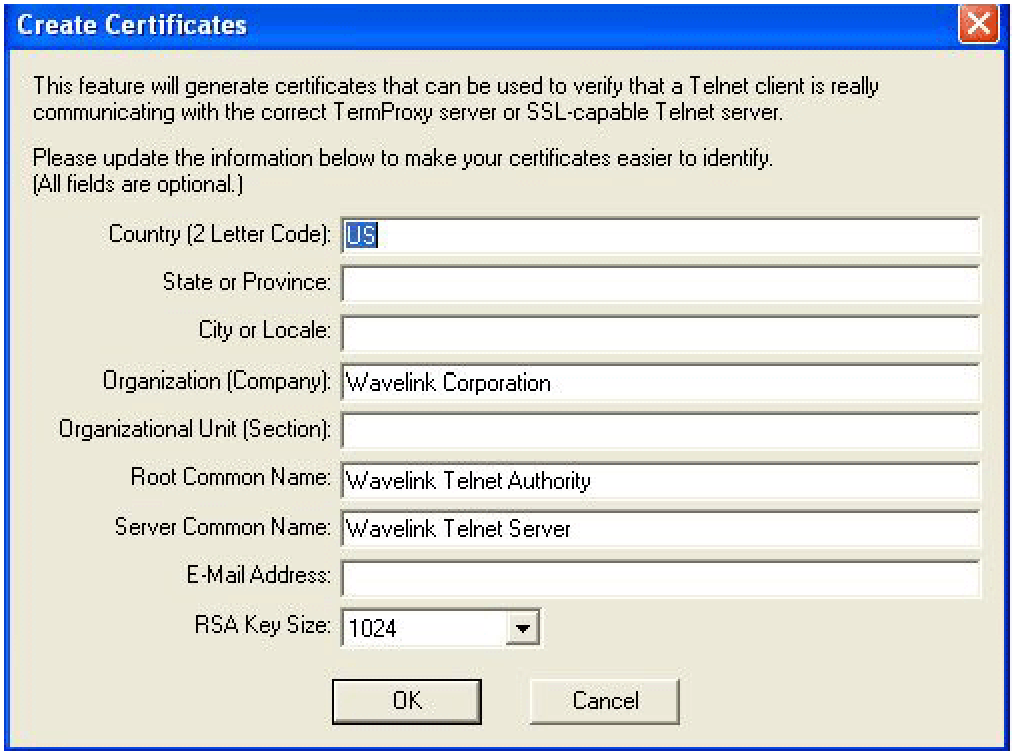
CREATING NEW VERIFICATION CERTIFICATES

If you are using TermProxy, the `Create Certificates` option in the *Certificate Manager* dialog box will generate verification certificates you can use and give you the option of copying the server certificates to the TermProxy installation folder.

Note: TermProxy should already be installed before you create certificates.

To create a new verification certificate

1. Access the *Certificate Manager* dialog box.
2. Click `Create Certificates`.
3. Enter the certificate information.
4. Click `OK`.



Create Certificates

This feature will generate certificates that can be used to verify that a Telnet client is really communicating with the correct TermProxy server or SSL-capable Telnet server.

Please update the information below to make your certificates easier to identify.
(All fields are optional.)

Country (2 Letter Code):	US
State or Province:	
City or Locale:	
Organization (Company):	Wavelink Corporation
Organizational Unit (Section):	
Root Common Name:	Wavelink Telnet Authority
Server Common Name:	Wavelink Telnet Server
E-Mail Address:	
RSA Key Size:	1024

Creating a certificate

INSERTING VERIFICATION CERTIFICATES

If your Telnet host is configured for SSL/TLS, use the `Insert Certificate` option in the *Certificate Manager* dialog box to select the root certificate or certificate chain that can verify the certificate used by the Telnet host.

To insert a certificate

1. Access the *Certificate Manager* dialog box.
2. Click `Insert Certificate`.

3. Browse to the certificate file.
4. Click `Open`.

REMOVING VERIFICATION CERTIFICATES

You can remove a verification certificate if you no longer want to use it.

To remove a certificate

1. Access the *Certificate Manager* dialog box.
2. Select the certificate you want to remove.
3. Click `Remove Certificate`.

DOCUMENT HISTORY

- 05/13/2005. Document created.
- 05/16/2005. Revised to include TLS information.

wavelink
wireless comes together

Wavelink Corporation
11332 NE 122nd Way, Suite 300
Kirkland, WA 98034
Main: 425.823.0111