USING SSL/TLS WITH TERMINAL EMULATION

This document describes how to install and configure SSL or TLS support and verification certificates for the Wavelink Terminal Emulation (TE) Client. SSL/TLS support is available with the TE Client version 5.0 or newer.

Secure Sockets Layer and Transport Layer Security (SSL/TLS) are protocols developed for transmitting private information over the Internet. SSL/TLS protocols encrypt data that is transferred over the emulation session. The TE Client supports SSL Version 2, SSL Version 3, and TLS Version 1 protocols and will automatically select the most secure protocol that the emulation host supports.

Verification certificates validate the server with which you are communicating. The certificates that you import and/or create are available for all of the host profiles that you configure. The certificates are added to a list which the Client will check when initiating a session with a host. If the host does not have a certificate that is in the list, then the Client will not establish a connection with the host.

OVERVIEW OF SSL/TLS SUPPORT

In order to use SSL or TLS 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 Client configuration to the device.

If you plan to use verification certificates, you also need to create or import the certificates for the Client to use. If you create certificates using the TE Certificate Manager, you will need to save the certificates in the appropriate location so that the server can use them.

This document describes the following:

- Installing the SSL/TLS Support Utility
- Deploying the SSL/TLS Support Package
- Configuring SSL/TLS Support
- Configuring Verification Certificates

INSTALLING THE SSL/TLS SUPPORT UTILITY

The SSL/TLS 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 SSL/TLS.

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

1. Obtain the installation files for the Windows SSL/TLS 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 SSL/TLS package for the Client.

2. Install the SSL/TLS support utility on the desktop computer from which you will deploy the package 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 SSL/TLS SUPPORT PACKAGE

Use Avalanche or ActiveSync to deploy the SSL/TLS 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 SSL/TLS package through Avalanche:

1. Ensure you have obtained the SSL/TLS 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 SSL/TLS 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 SSL/TLS package through ActiveSync:

1. Establish an ActiveSync connection to the device.
2. From the desktop computer, double-click the .exe file to install the SSL/TLS 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. If you want to deploy immediately, enable the **Run Wavelink SSL/TLS ActiveSync Support** option. Click **Finish** to close the installer.

7. If you enabled the **Run Wavelink SSL/TLS 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 SSL_TLS 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 SSL or TLS.

CONFIGURING SSL/TLS SUPPORT

The TE Client is configured to use SSL/TLS support in the host profile. To access host profiles from the ActiveSync installer, click the **Host Profiles** button. To access host profiles from Avalanche, select the package and click **Configure**.

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

To configure SSL/TLS:

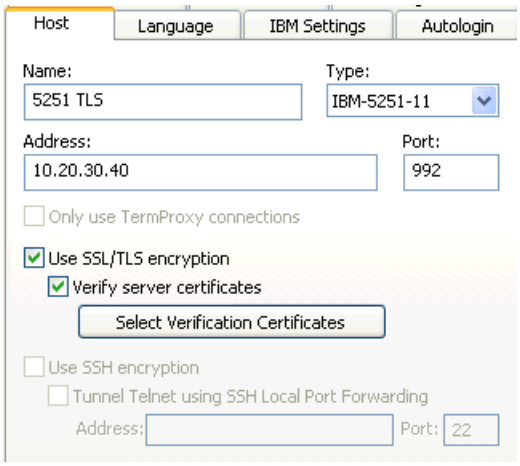
1. Access the Host Profiles configuration utility for the TE Client.

2. Select an existing host profile or create a new host profile.

3. Depending on the connection requirements for the host profile, select one of the following:

   - If the host profile specifies a direct connection to a server, then enable the **Use SSL/TLS Encryption** option in the **Host** tab.

   - If the host profile specifies a connection to a Wavelink ConnectPro or TermProxy server, then enable the **Use SSL/TLS Encryption** option in the **TermProxy** tab. You will not be able to enable the **Use SSL/TLS Encryption** option in the **TermProxy** tab until you select an option from the **TermProxy Server** menu list.



Enabling SSL/TLS

4. If you plan to use server certificates, enable the **Verify server certificates** option and follow the instructions for *Configuring Verification Certificates*.

5. Click **OK**.

6. Download the new TE Client configuration to the mobile device using either Avalanche or ActiveSync.

CONFIGURING VERIFICATION CERTIFICATES

Clients use verification certificates to ensure that they are communicating with the correct server. Verification certificates are not required but are highly recommended. The certificates that you import and/or create are available for all host profiles on the Client. Import existing certificates or create your own with the Certificate Manager.

IMPORTING EXISTING VERIFICATION CERTIFICATES

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

To import a certificate:

1. From the *Host Profiles* dialog box, click **Select Verification Certificates**.

2. In the Certificate Manager, click **Insert Certificate**.

3. Browse to the certificate file and click **Open**.

   The certificate is imported and the Client will recognize and communicate with a server using the certificate.

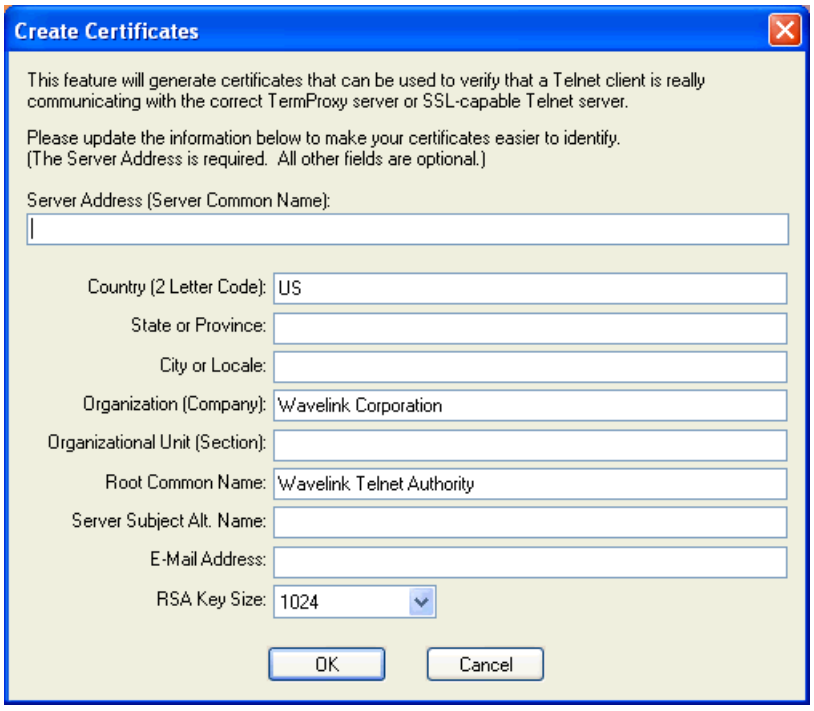
CREATING NEW VERIFICATION CERTIFICATES

If you are using ConnectPro or TermProxy, the **Create Certificates** button in the *Certificate Manager* will generate verification certificates you can use and gives you the option of copying the server certificates to the appropriate location so that the ConnectPro/TermProxy server can use them.

NOTE: ConnectPro/TermProxy should already be installed before you create certificates.

To create a new verification certificate:

1. From the *Host Profiles* dialog box, click **Select Verification Certificates**.
2. In the Certificate Manager, click **Create Certificates**. The *Create Certificates* dialog box appears.



Creating a certificate

3. Enter the certificate information.
4. Click **OK**.
5. A dialog box appears, prompting you to add the certificate to the storage for the local computer. Click **Yes** if you plan to use the local computer as a host for WEB emulation.
6. A dialog box appears, prompting you to copy the certificate and key to the TermProxy (or ConnectPro) installation folder. Click **Yes** to copy these files, or click **No** if you choose to move the files later. You will need to restart the ConnectPro or TermProxy server after copying these files.
7. The created certificate appears in the Certificate Manager.

The certificates need to be saved in the appropriate location(s) so that the Client will recognize and communicate with the server.

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

- 13/05/2005. Document created.
- 16/05/2005. Revised to include TLS information.
- 23/11/2010. Updated.

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