
WS_FTP Pro

Addendum to User's Guide

Software Version 6.6

Ipswitch, Inc.

Ipswitch, Inc.
81 Hartwell Ave
Lexington, MA 02421-3127

Phone: 781-676-5700
Fax: 781-676-5710
Web: <http://www.ipswitch.com>

The information in this document is subject to change without notice and should not be construed as a commitment by Ipswitch, Inc. While every effort has been made to assure the accuracy of the information contained herein, Ipswitch, Inc. assumes no responsibility for errors or omissions. Ipswitch, Inc. assumes no liability for damages resulting from the use of the information contained in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of that license.

Copyright © 2000 by Ipswitch, Inc. All rights reserved. WS_FTP, the WS_FTP logos, Ipswitch, and the Ipswitch logo are trademarks of Ipswitch, Inc. Other products or company names are or may be trademarks or registered trademarks and are the property of their respective companies.

No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transferred without the expressed prior written consent of Ipswitch, Inc.

Printing History

September 2000 First Edition

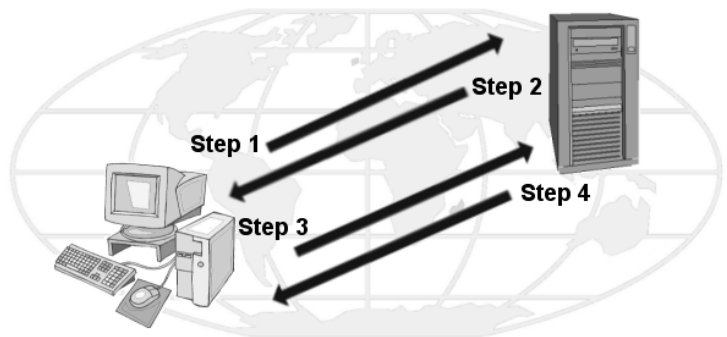
Addendum to WS_FTP Pro User's Guide

This chapter describes what SSL is and how you can configure WS_FTP Pro to make secure (SSL) connections.

What is SSL?

SSL (Secure Socket Layer) is a protocol for encrypting and decrypting data sent across direct internet connections. When a client makes an SSL connection with a server, all data sent to and from that server is encoded with a complex mathematical algorithm that makes it extremely difficult to decode anything that is intercepted.

The following is a step by step illustration of how SSL works.



- Step 1.** The client makes the initial connection with the server and requests that an SSL connection be made.
- Step 2.** If the server is properly configured, the server will send to the client its certificate and public key.
- Step 3.** The client uses that public key to encrypt a session key and sends the session key to the server. If the server asks for the client's certificate in Step 2, the client must send it at this point.
- Step 4.** If the server is set up to receive certificates, it compares the certificate it received with those listed in its trusted authorities database and either accepts or rejects the connection.

If the connection is rejected, a fail message is sent to the client. If the connection is accepted, or if the server is not set up to receive certificates, it decodes the session key from the client with its own private key and sends a success message back to the client, thereby opening a secure data channel.

The key to understanding how SSL works is in understanding the parts that make SSL itself work. The following is a list of these parts and the role each plays.

Client. In this case, the client is the WS_FTP Pro 6.6 software.

Certificate. The Certificate file holds the identification information of the client or server. This file is used during connection negotiations to identify the parties involved. In some cases, the client's certificate must be 'signed' by the server's certificate in order to open an SSL connection. Certificate files have the .crt ending.

Session Key. The session key is what both the client and the server use to encrypt data. It is created by the client.

Public Key. The public key is the device with which the client encrypts a session key. It does not exist as a file, but is a byproduct of the creation of a certificate and private key. Data encrypted with a public key can only be decrypted by the private key that made it.

Private Key. The private key decrypts the client's session key that is encrypted by a public key. The private key file has the .key ending. Private keys should NEVER be distributed to anyone.

Certificate Signing Request. A certificate signing request is generated each time a certificate is created. This file is used when you need to 'sign' a certificate. Once the Certificate Signing Request file is signed, a new certificate is made and can be used to replace the unsigned certificate.

How to make an SSL connection

To make an SSL connection with a server configured for SSL that you have an account on:

- 1 Follow the directions for configuring a site, being sure to select the Secure (SSL) option.

- 2 After you click **Connect**, WS_FTP 'tells' the server that you want to make an SSL connection. The server then transmits to you an identifying certificate, letting the client know who the server is. If that certificate is already listed in your Trusted Authority database, the connection is made.
- 3 If that certificate is not listed as a trusted authority, the Non-Trusted Authority dialog box appears.
- 4 Select the option you need and click **OK**. If the server does not require a certificate to be returned, the secure connection will be established. All data transmitted between you and the server will be encrypted.

If the server you are attempting to make a connection to asks WS_FTP to send back a certificate, follow the direction for Client Certificate Verification.

Client Certificate Verification

If the server you are attempting to make a connection to requires your client to send an identifying certificate back to the server, you must:

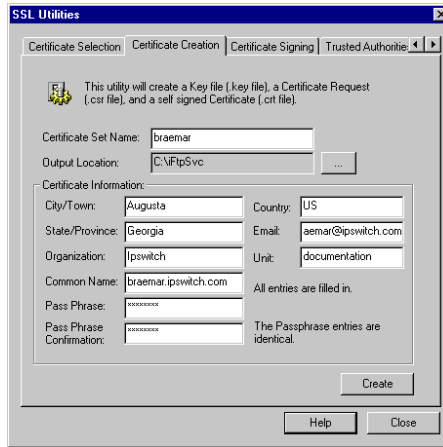
- 1 Configure the site with the Secure (SSL) option selected.
- 2 Create a certificate. Refer to the section “generating a certificate” for more information.
- 3 Send the Certificate Signing Request file to your server administrator.
- 4 Once the server administrator signs the Certificate Signing Request, it will be sent back to you.
- 5 When you receive the file, follow the directions for “Selecting a Certificate” on page 5, selecting the new certificate to go in the **Certificate** box.
- 6 Connect to the server.

Generating a Certificate

To create an SSL certificate:

- 1 From the File menu, select Configure SSL. The SSL Utilities window appears.

- 2 Click the Certificate Creation tab.



- 3 Enter a name in the **Certificate Set Name** box. This will be the name of the certificate that is generated by WS_FTP.
- 4 Click the **Browse (...)** button in the **Output Location** box to select the folder you want the certificate created in.
- 5 Enter information in all of the Certificate Information boxes:
 - City/Town.** City or town where you are located. (Ex. Augusta)
 - State/Province.** State or Province where you are located. (Ex. Georgia)
 - Organization.** Company or individual user name.
 - Common Name.** This can be either the name of the person creating the certificate or the fully qualified domain name of the server associated with the host.
 - Pass Phrase.** Pass phrase that is to be used to encrypt the private key. It is important to remember this pass phrase. The pass phrase can be any combination of words, symbols, spaces, or numbers.
 - Pass Phrase Confirmation.** Re-enter the same pass phrase as above.
 - Country.** The country you are in. This must be a valid two letter country code. (Ex. US)
 - Email.** E-mail address of the person the certificate belongs to.

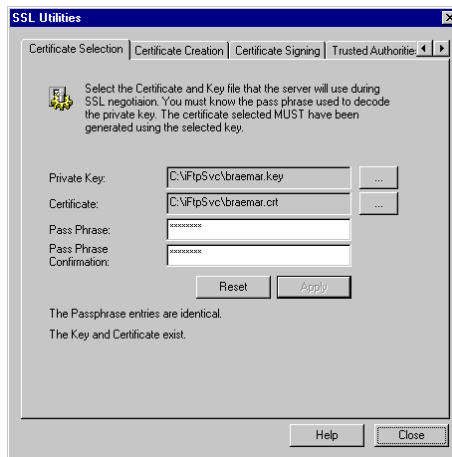
Unit. Name of organizational unit. (Ex. Research and Development)

- 6 After all of the boxes are filled in correctly, click **Create** to generate the keys, certificate, and certificate signing request. If all of the boxes are not filled in, you can not create the certificate.

If you are creating a certificate to be used by WS_FTP Pro, you should send the certificate signing request (by e-mail) to your server administrator. If they require it, they will sign the certificate and return it to you. The returned certificate should be the one you identify in the Certificate Selection tab.

Selecting a Certificate

The Certificate Selection tab is used to choose which private key and certificate you want to use during SSL connection negotiations. If a new certificate has not been created, follow the directions for “Generating a Certificate” on page 3.



To select an SSL Certificate:

- 1 Click the **Browse (...)** button next to the **Private Key** box to select the private key you want to use during SSL negotiation.

- 2 Click the **Browse (...)** button next to the **Certificate box** to select the certificate you want to use during SSL negotiation. The certificate you use must have been created using the key you selected for the **Private Key** box.
- 3 Enter the pass phrase associated with that certificate in both the **Pass Phrase** and the **Pass Phrase Confirmation** boxes. A pass phrase can be any combination of words, symbols, or numbers. It is case sensitive and must be written exactly the same way each time it is used.

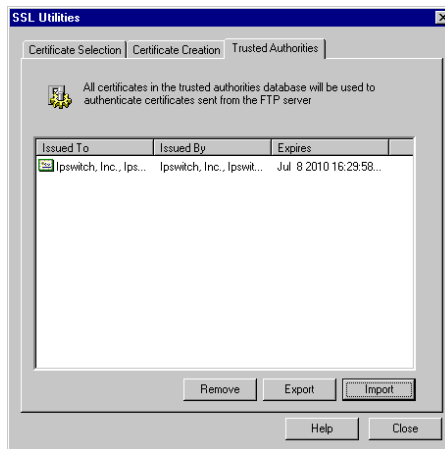
Without the correct pass phrase in both boxes, the certificate and private key cannot be verified and the selection cannot be saved.

- 4 Click **Apply** to save your entries.

Clicking the **Reset** button erases what you have done since the last time new settings were applied.

Trusted Authorities

The Trusted Authorities tab stores a list of certificate names that are recognized by WS_FTP Pro.



Certificate Display

Issued To. Who the certificate was issued to.

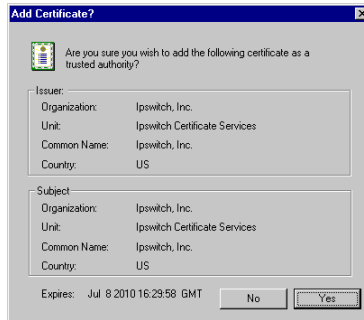
Issued By. Who the certificate was signed by.

Expires. Date on which the certificate expires.

Adding a Certificate

To add a certificate to the database:

- 1 Click the **Import** button and select the path and file name for the certificate. The Add Certificate? dialog box appears.



- 2 Review the information on that dialog box and click **Yes** to add the certificate to the database.

Exporting a Certificate

To export a certificate from the Trusted Authorities database:

- 1 Select the certificate you want to copy out of your database.
- 2 Click the **Export** button.
- 3 Select the folder you want to copy the certificate to and enter the name you want to save the certificate file as.
- 4 Click **OK**.

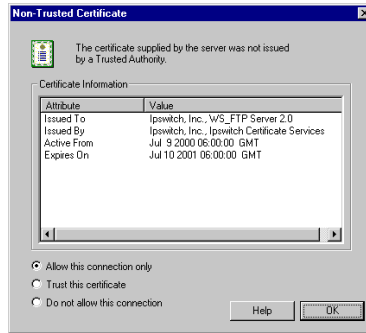
Removing a Certificate

To remove a certificate:

- 1 Select the certificate to be removed.
- 2 Click **Remove**.
- 3 A warning appears advising you to export the certificate before you remove it. Removing the certificate deletes the certificate file.
- 4 Click **OK** to remove the certificate.

Non-Trusted Certificate

When you connect to a server using the SSL connection option, that server sends you a certificate. If that certificate is not listed on the Trusted Authority tab, or if it was not signed by a certificate on this list, this dialog box appears.



Certificate Information

Issued To. Name of the person or company who the certificate belongs to.

Issued By. Name of the person or company who signed the certificate.

Active From. The date on which this certificate was activated.

Expires On. The date the displayed certificate will no longer be a valid certificate.

Options

Allow this connection only. If this option is selected, the connection will be made, but WS_FTP will still not recognize the certificate as a trusted authority. The next time you attempt to connect to this server, this dialog box appears once again.

Trust this certificate. If this option is selected, the connection will be made and the certificate will be added to the trusted authority database in the Trusted Authority tab, so future connections can be made without you being prompted.

Do not allow this connection. If this option is selected, the connection will be terminated.

