

MassTransit® 6

Application Client Manual

Macintosh and Windows

GroupLogic®

Group Logic Inc.
703-528-1555
Fax: 703-527-2567
Email: info@grouplogic.com
Internet: www.grouplogic.com

Copyright (C) 1995-2008 Group Logic Incorporated. All rights reserved. 09150860

This manual, as well as the software described in it, is furnished under license and may only be used or copied in accordance with the terms of such license. The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Group Logic Incorporated. Group Logic Incorporated assumes no responsibility or liability for any errors or inaccuracies that may appear in this book. Printed in the USA.

Except as permitted by such license, no part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Group Logic Incorporated.

The software described in this manual is covered by a license agreement which places restrictions on its export and import to specific countries. This License agreement is expressly made subject to any applicable laws, regulations, orders, or other restrictions on the export of the licensed products, software or information about such licensed products which are in effect or may be imposed from time to time. You shall not export or import the licensed products or information about the licensed products without complying with such laws, regulations, orders, or other restrictions. The licensed products may not be exported or reexported to Cuba, Libya, Iraq, Iran, Sudan, Syria, or North Korea. You agree to indemnify Group Logic, Incorporated, against all claims, losses, damages, liabilities, costs and expenses, including reasonable attorney' fees, to the extent such claims arise out of any breach of this section.

Adobe, the Adobe logo, and PostScript are trademarks of Adobe Systems Incorporated. All references to PostScript on the screen or in this manual are references either to the Adobe PostScript software or to the Adobe PostScript language. Apple, Finder, Macintosh, and Mac OS are registered trademarks of Apple Computer, Inc. Explorer, Internet Information Services, and Windows are registered trademarks of Microsoft, Inc.

All other trademarks are the property of their respective owners.

For defense agencies: Restricted Rights Legend. Use, reproduction or disclosure is subject to restrictions set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013.

For civilian agencies: Restricted Rights Legend. Use, reproduction or disclosure is subject to restrictions set forth in subparagraphs (a) through (d) of the commercial Computer Software Restricted Rights clause at 52.227-19 and the limitations set forth in Group Logic's standard commercial agreement for this software. Unpublished rights are reserved under the copyright laws of the United States.

For detailed license information related to included software, see the Related Licenses folder in the MassTransit installation directory.

The Software contains open source computer programs the copyright to which is owned by MySQL AB, and which may not be used except pursuant to the licensed rights in the Software granted above to you or as otherwise expressly permitted by MySQL AB. MySQL is a trademark of MySQL AB and may not be used without express permission from MySQL AB. Copyright (C) 1995-2008 MySQL AB. All rights reserved.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Portions Copyright (C) 1999-2008 The Apache Software Foundation. All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). Portions Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved. Portions Copyright (C) 1998-2008 The OpenSSL Project. All rights reserved.

Portions written with the MacApp® Application Framework. Copyright (C) 1983-2008 Apple Computer, Inc. MacApp is a trademark of Apple Computer, Inc., registered in the United States and certain other countries."

This product includes software developed by the Fusebox Corporation (<http://www.fusebox.org/>). Copyright (C) 1997-2008 The Fusebox Corporation. All rights reserved.

This product includes software developed by the New Digital Group, Inc. Portions Copyright (C) 2001-2008 New Digital Group, Inc. All rights reserved.

This product includes software developed by Robert A. van Engelen. Portions created by gSOAP are Copyright (C) 2001-2008 Robert A. van Engelen, Genivia inc. All rights reserved.

Portions Copyright (C) 1995-2008 Jean-loup Gailly and Mark Adler.

Introduction: Getting Started	5
ABOUT MASSTRANSIT	5
Application Clients and Servers.....	5
The Navigation Bar	5
Security.....	6
About Job tickets	6
Workflow features	6
MINIMUM REQUIREMENTS.....	6
INSTALLING MASSTRANSIT.....	6
Installing Application Client software	7
Chapter One: Communications	8
SETTING UP COMMUNICATIONS	8
Incoming and Outgoing calls	8
TCP/IP COMMUNICATION METHODS	9
TCP/IP	9
TCP/IP Secure.....	10
SETTING UP SECURE CONNECTIONS.....	11
Encrypting	12
Exporting encryption	12
Setting encryption levels.....	12
Verifying the caller.....	12
Using a MassTransit generated certificate.....	12
Using your own Certificate Authority	13
Using a Trusted Root Certificate Authority.....	13
Obtaining a certificate from a Certificate Authority (CA)	13
Setting up MassTransit to use a certificate.....	14
Chapter Two: Transferring Files	16
TRANSFERRING FILES	16
Setting privileges.....	16
Converting Macintosh file names for Windows file names	17
Viewing the transfer of files.....	17
DESIGNATING FILES TO SEND.....	17
By dragging to the Files window To Send tab.....	17
Using the Files window Add button.....	17
Removing a file's "To Send" status	18
Adding a job ticket.....	18
Modifying and managing job tickets.....	19
Viewing or editing a job ticket	19

Sending files	19
Sending files manually	19
Letting the Server Retrieve Files	19
RECEIVING FILES FROM THE SERVER	19
The Received Mailbox.....	20
Receiving files Automatically.....	20
Retrieving files Manually.....	20
Viewing Received files with the Files window	20
CANCELLING A CONNECTION.....	20
Chapter Three: Tracking Job Information	21
TRACKING FILES WITH THE LOG WINDOW	21
Reordering log entries	21
Managing outdated log entries	22
BACKING UP DATABASE FILES	23
Appendix: Troubleshooting.....	24
GETTING HELP WITH MASSTRANSIT	24
Web Help	24
Index	25

Introduction: Getting Started

Welcome to MassTransit. This introduction covers the following topics.

- About MassTransit
- Requirements
- How to install MassTransit Application Client

About MassTransit

MassTransit lets you transfer files from one location to another with a simple drag and drop. It also enables remote processing.

APPLICATION CLIENTS AND SERVERS

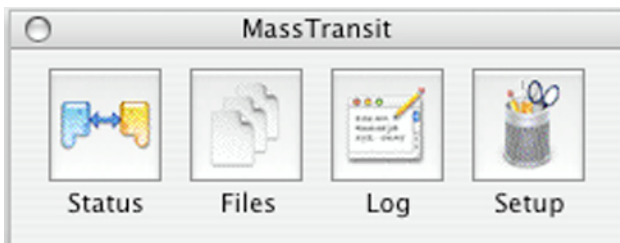
MassTransit consists of two parts: the Application Client version and the MassTransit Server. The MassTransit Server can be either the Professional or Enterprise Server. The Application Client and its Server let you perform the following tasks:

- Send files to and receive files from one another
- Specify whether one user can receive files from or send files to the other
- Specify whether the remote user can overwrite files of the same name on the receiving computer
- Track the status of incoming and outgoing files
- Use a secure connection

The Application Client lets you control the transmission of files to and from a MassTransit Server.

THE NAVIGATION BAR

The quickest way to open MassTransit windows is with the Navigation Bar. This bar includes buttons that represent the windows and dialog boxes you use to set up and monitor file transfers. When you click a button in the bar, MassTransit immediately jumps to that window or dialog box. The Navigation Bar appears when you launch MassTransit.



If you close the Navigation Bar, you can reopen it from the Windows menu or press Command Ø (Macintosh) or Control 1 (Windows).

Use the icons in the Navigation Bar to do the following tasks.

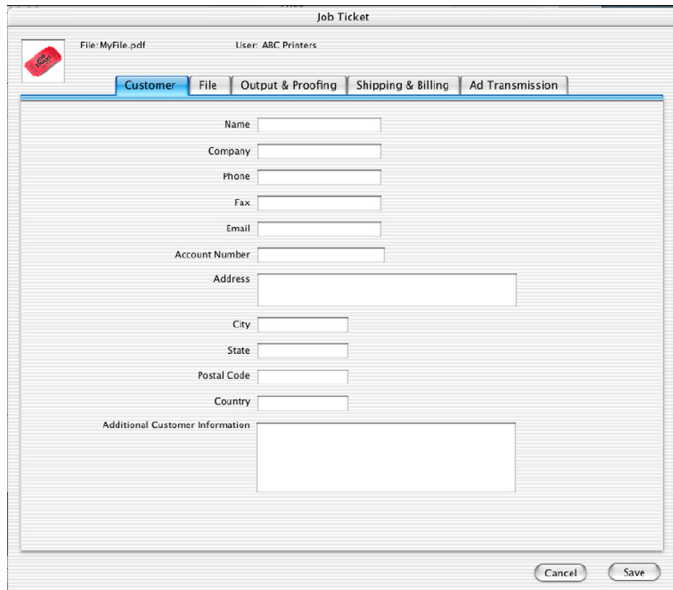
- View the Status window to see what's happening in MassTransit—if you are currently connected to the MassTransit Server and are receiving or transferring files—and to cancel a connection.
- Use the Files window to see the files that are ready to be sent, files that you have already sent, and those that you have received.
- Look at the Log to see a list of all the actions MassTransit has taken. Any problems are explained here.
- Setup allows you to set the way MassTransit works including designating your communications method.

SECURITY

Your server may require you to make secure connections. MassTransit offers a TCP/IP security option, TCP/IP Secure, which uses the Secure Sockets Layer (SSL) protocol to encrypt transferred data, maintain the integrity of data, and authenticate the calling parties. Authentication allows you to verify the identity of the caller to make sure you are sending to or receiving data from the right place. When MassTransit tries to establish a secure connection using SSL, each party provides the other with its certificate. Each party verifies that the other's certificate is valid and, if it is, proceeds with the connection.

ABOUT JOB TICKETS

Like the real-world paper version, the MassTransit job ticket provides a convenient and familiar way for you to communicate with your MassTransit Server. The Job Ticket window lets you enter name, address, shipping, and billing information, as well as instructions and details about the accompanying job.



The screenshot shows a 'Job Ticket' window with a menu bar and a form. The menu bar includes 'Customer', 'File', 'Output & Proofing', 'Shipping & Billing', and 'Ad Transmission'. The 'Customer' menu is selected. The form contains the following fields: Name, Company, Phone, Fax, Email, Account Number, Address, City, State, Postal Code, and Country. There is also a large text area for 'Additional Customer Information'. At the bottom right, there are 'Cancel' and 'Save' buttons.

WORKFLOW FEATURES

MassTransit keeps a log of all actions it performs. You can check the Log window to see if files were received or sent. The Log lists errors that occurred so you can correct a problem. For example, if the MassTransit Server does not have enough room on the computer you're transferring a file to, the log gives the reason why the file is not transferred. You can call the MassTransit Server and transfer the file again when more space is made available to receive the file.

Minimum Requirements

In order to use MassTransit, you need the correct resources. See the ReadMe file in the MassTransit installation directory for the latest requirements.

Installing MassTransit

Install the Application Client software and place the MTClient.cfg file provided by your MassTransit Server in the folder with the MassTransit software. The MTClient.cfg file allows your MassTransit Server to recognize you when you connect to transfer files.

INSTALLING APPLICATION CLIENT SOFTWARE

To install the MassTransit, follow these steps.

1. Double click the MassTransit Application Client icon.
2. Follow the on-screen instructions. When installation is complete, click Finish to close the installer.
3. Obtain the MTClient.cfg file from your MassTransit Server and place the file in the folder with MassTransit. The CFG file allows your MassTransit Server to recognize you.

Chapter One: Communications

Before you can send files to your MassTransit Server, you must tell MassTransit what communications method and settings you are using. The communications methods available with MassTransit include TCP/IP and TCP/IP Secure.

- Setting up communications
- Setting up security

MassTransit lets your MassTransit Server send files to you; for example, files for proofing or trapped graphics to place in a document you are working on.

Setting up Communications

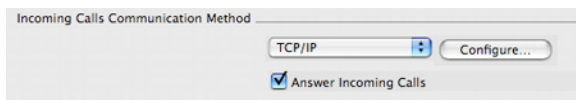
If you want your MassTransit Server to be able to initiate these transmissions, you must set up incoming communications for your MassTransit Application Client.

INCOMING AND OUTGOING CALLS

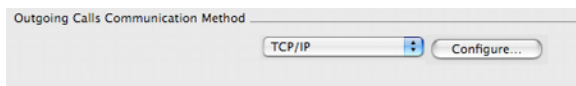
Your server may have preconfigured communications methods for you in the CFG file. You can change these using the Communications tab of the Setup window. Follow these steps to set up or edit a communications method. Then, see the following sections for individual communication methods.

1. In the Setup window, select the Communications tab.
2. Use the Incoming Calls Communication Method menu to choose and configure a communication method to receive calls. To answer calls from your MassTransit Server, place a check in the Answer Incoming Calls checkbox.

To edit a method, just click **Configure**.



3. Use the Outgoing Calls Communication Method menu to choose and configure a communication method to receive calls. To edit a method, just click **Configure**.



4. Configure the Privileges settings. For secure connections, set Authentication. See page 16 for information about privileges. See page 11 for secure connections.
5. If you wish, choose a different location for your mailbox location. The default mailbox is located in the same folder with the MassTransit Application Client.

TCP/IP Communication Methods

MassTransit allows you to connect to your server through a TCP/IP network connection. You can use TCP/IP or you can set up secure connections using Secure Sockets Layer (SSL) by choosing TCP/IP Secure as the communication method.

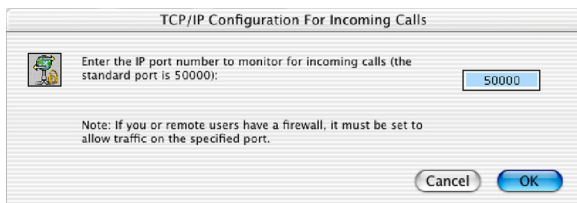
Note The Mac OS X versions of MassTransit cannot listen on any port less than 1024 unless running as root. Due to this limitation, you will need to install and run MassTransit under the Mac OS X root account for SSL listens on the normal 443 port. This limitation will be addressed in an upcoming version of MassTransit. See the ReadMe file for more information.

TCP/IP

To set up TCP/IP communications, follow these steps.

Incoming calls using TCP/IP Follow the steps below to configure TCP/IP to receive calls.

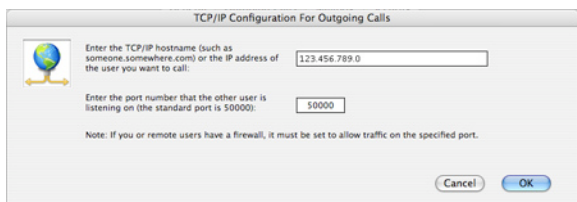
1. In the Setup window, select the Communications tab.
2. For Incoming Calls, choose TCP/IP from the Method menu.
The TCP/IP Configuration for Incoming Calls dialog box appears.



3. If necessary, change the port to one which allows network traffic.
MassTransit uses the standard port 50000 as the default. If your network is protected by an Internet firewall, type the number for the port that allows network traffic.
4. Click OK, then click OK in the Setup window.
You are ready to receive calls over TCP/IP.

Outgoing calls using TCP/IP You must enter the IP address or MassTransit Server hostname of your MassTransit Server.

1. In the Setup window, select the Communications tab.
2. For Outgoing Calls, choose TCP/IP from the Method pop-up menu.



3. Type the IP address or MassTransit Server hostname of the MassTransit Server.
4. If necessary, change the port to one which allows network traffic.
MassTransit uses the standard port 50000 as the default. If your network is protected by an Internet firewall, type the number for the port that allows network traffic.
5. Click Save or OK, then click Save in the Setup window.
You are ready to place calls with TCP/IP.

TCP/IP Secure

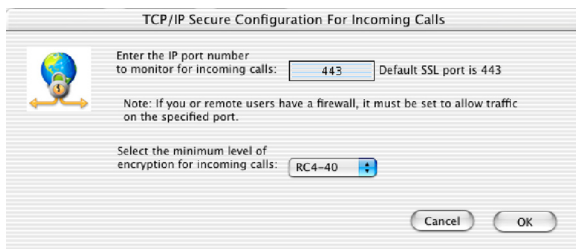
Your server may require you to set up secure TCP/IP communications. Using SSL, MassTransit can require calling parties to verify who they are before allowing a connection. To verify who a calling party is, SSL uses authentication in the form of certificates which are presented at the time MassTransit connects with another user. If a certificate is not valid, MassTransit does not allow a connection. See "Setting Up Secure Connections" starting on page 11 for detailed information on setting up security with SSL.

Certificates MassTransit works with two types of certificates: 1) Self-generated by MassTransit itself (which is the default option), or 2) Issued by a Certificate Authority (CA). Using self-generated certificates allows you to avoid paying fees and maintenance issues. However, no one verifies that the certificate owner is who they claim to be, and you may be susceptible to certain kinds of attacks that allow people to intercept your data. When you have a certificate issued by a CA they verify the identity of the other party you are about to connect to. You can buy a certificate from one of the well known Certificate Authorities, such as VeriSign® or Thawte®, or you can become your own CA and issue certificates for all the MassTransit servers within your organization.

Starting out Your MassTransit Server may have chosen the TCP/IP Secure method of communication when generating your CFG file. If this is the case, your MassTransit Application Client software generates a certificate for you. If your MassTransit server wants you to use a certificate issued by a CA instead, you must first obtain a certificate from a CA and then, use your configuration dialog box to set up MassTransit to use your certificate. For directions on creating or obtaining certificates, see page 12.

Incoming calls using TCP/IP Secure Follow the steps below to configure TCP/IP Secure to receive calls.

1. Click the Setup icon on the Navigation Bar, or press Command 4 (Macintosh) or Control 5 (Windows) and select the Communication tab.
2. For Incoming Calls, choose TCP/IP Secure from the Method menu.



3. If necessary, change the port to one which allows network traffic. MassTransit uses 443 as the default port for TCP/IP Secure. Normally, you should not change this value. However, if your network is protected by an Internet firewall, type the number for a port that allows incoming network traffic.

Note Notify the person who will call you of the port number. They must call the port you have typed here.

4. Select a minimum level of encryption for incoming files. MassTransit uses the selected level as a minimum. If your server sets connection encryption to a higher level, MassTransit accepts the connection. If connection encryption is set to a level lower than your minimum, MassTransit refuses to connect.
5. Click OK, then click Save in the Setup window. You are ready to receive calls over TCP/IP Secure.

Outgoing calls using TCP/IP Secure You must enter the IP address or the MassTransit hostname of your MassTransit Server.

1. In the Setup window, select the Communications tab.

- For Outgoing Calls, choose TCP/IP Secure from the Method menu.

TCP/IP Secure Configuration For Outgoing Calls

Enter the TCP/IP hostname (such as somewhere.somewhere.com) or the IP address of the user you want to call:

Enter the port number that the other user is listening on (the default port is 443):

Note: If you or the party you are calling have a firewall, it must be set to allow traffic on the specified port.

Remote user's COMMON NAME: ?

Select the level of encryption to use:

- Type the IP address or hostname of your server.
- If necessary, change the port to one which allows incoming network traffic on the remote network. MassTransit uses port 443 as the default. Normally, you should not change the port number. However, if the network you are calling is protected by an Internet firewall, type the number for the remote port that allows incoming network traffic.
- Type the server's identity. This must be the common name the server used when creating a certificate or obtaining a certificate from a Certificate Authority. See step 3 on page 14 in this chapter.
- Choose a level of encryptions from the menu. When you send files to your server, the files are encrypted to this level.

Note Make sure the level you choose is at or above the minimum level of encryption the server has set when configuring TCP/IP Secure as an Incoming Method in the Setup window. Otherwise, you cannot make a connection and a message appears in your log explaining why.
- Click OK. You are ready to place calls with TCP/IP Secure.

Note If you have trouble connecting, make sure you have the correct IP address or hostname and the correct port number entered.

Setting up secure Connections

If you are sending files over a network, you can use security features of MassTransit to secure files from tampering or disclosure (encryption) and verify the contact with whom you are exchanging files (authentication). Security can be set up for TCP/IP connections.

MassTransit uses Secure Sockets Layer (SSL) to provide secure connections for TCP/IP. SSL provides authentication of callers, data encryption and message integrity. These three features keep your data secure while it is travelling across the Internet, and in addition, authenticates the identity of both contacts in the connection. SSL is used widely for secure connections, for example, when web browsers connect to web sites for online shopping or financial institutions.

Once you have set up MassTransit for secure connections, SSL works behind the scenes at the time a connection is requested. First, certificates are exchanged proving who each contact is for verification. Then, SSL checks to make sure the encryption level is agreed upon before exchanging files. This makes the connection secure.

ENCRYPTING

Everything sent over a network from MassTransit including passwords and files are vulnerable to others who may read the files or intercept and change or destroy the files. When you choose the TCP/IP Secure communication method, MassTransit encrypts all transfers before sending them over a network and requires encrypted incoming information.

Exporting encryption

MassTransit products fall under the category of retail encryption items eligible for License Exception ENC. This means that they can be exported, and reexported, to government and non-government end-users alike in any country except, at the time of writing, Libya, Sudan, Iraq, Iran, Cuba, Syria, and North Korea. In addition, they may not be exported, or reexported, to any person, or entity, engaged in the development or use of nuclear weapons, guided missiles or chemical and biological weapons. It does not matter that the software has no utility in such activities. Finally, the Commerce and Defense Departments maintain lists of denied persons and specially designated "nationals" with whom United States persons may not trade. These lists are maintained on the Web.

Setting encryption levels

Using SSL, MassTransit can encrypt files to one of three levels of strength.

- RC4-40, the lowest level of encryption; International transfers between or to other countries may be restricted to this level
- RC4-128
- 3DES
- AES-128
- AES-256

Transferring files Set a minimum encryption level for data received from your server; check with your server to see what encryption level must be used. MassTransit does not accept a connection encrypted to a lower level; a message is logged. For descriptions of setting encryption levels while configuring an incoming communication method, see page 11.

VERIFYING THE CALLER

MassTransit uses SSL to provide a certificate to calling parties to verify who they are. In addition, the certificate provides a public/private key combination that allows files to be encrypted and decrypted. The certificate verifies that the user communicating with you is not an imposter. MassTransit works with two types of certificates: 1) Self-generated by MassTransit itself (which is the default option), or 2) Certificates issued by a Certificate Authority (CA) such as VeriSign or Thawte. Using self-generated certificates allows you to avoid paying fees and maintenance issues. However, no one verifies that the certificate owner is who they claim to be. When you have a certificate, issued by a CA, they verify the identity of the other party you are about to connect to. You can buy a certificate from one of the well known Certificate Authorities, such as VeriSign or Thawte, or you can become your own CA and issue certificates for all the MassTransit servers within your organization.

When a secure connection is selected, MassTransit verifies the certificate presented by you and your server. When MassTransit provides your certificate to your remote MassTransit Server, it contains your identity name and your public key. The remote MassTransit uses the public key contained in the certificate to encrypt files to be transferred. When you receive the encrypted file, MassTransit decrypts it using the private key. Since you are the only one who has the private key, you are the only one who can decrypt files.

Using a MassTransit generated certificate

When your server has selected the TCP/IP Secure communication method for you, MassTransit generates a certificate for you when you open it the first time. You can choose to use this MassTransit created certificate. This certificate includes public and private keys for encrypting files. Creating your own certificates allows you to avoid fees and maintenance issues. However, no one verifies that the certificate owner is who they claim to be and you may be susceptible to some forms of attacks that break encryption called "man-in-the-middle" attacks.

Using your own Certificate Authority

You can create your own certificate authority using the OpenSSL toolkit. Creating your own authority allows you to avoid paying fees. For more information and detailed instructions on how to create your own authority, go to the website www.openssl.org.

Using a Trusted Root Certificate Authority

Trusted Certificate Authorities (CA) verify that the information in a certificate accurately represents who it claims to represent. They charge to provide a certificate, usually by the year. Usually, you contact a CA at their web site and request a certificate. Two popular CAs issuing certificates are VeriSign and Thawte. You may look at their web sites for more information at www.verisign.com and www.thawte.com.

Obtaining a certificate from a Certificate Authority (CA)

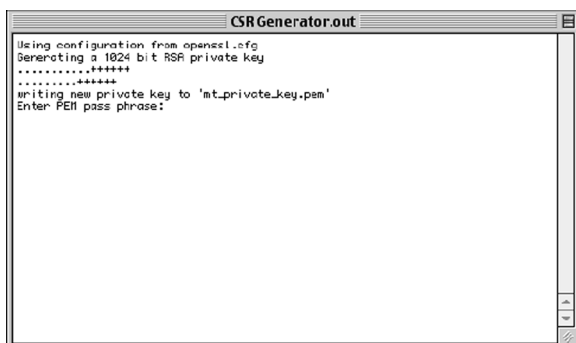
To set up MassTransit to use a trusted root Certificate Authority (CA), read these steps which provide an overview, then, see the next sections for detailed instruction.

1. Create a Certificate Signing Request (CSR) using the Certificate Generation program that comes with MassTransit. Do this before you request a certificate online. You paste this text into the request.
2. Obtain a certificate online by contacting the Trusted Root CA you wish to use and requesting a certificate.
3. The CA sends you the certificate which you make available to MassTransit.
4. Obtain a certificate of the trusted root authority used by your contact using TCP/IP Secure if it is not already included in MassTransit. These certificates allow you to verify callers. MassTransit comes with many of these certificates. Others can be downloaded from the CAs web site.

Generating a Certificate Signing Request Before setting up MassTransit to use a certificate, generate a Certificate Signing Request (CSR) to give to the Certificate Authority when asked. Later, when you request a certificate online, you copy and paste the text generated.

To create a CSR, follow these steps.

1. Open the CSR Generator program located in the MassTransit: Security: CSR Generator folder.



2. Enter a pass phrase for the private key. You are asked to enter this pass phrase in MassTransit when setting up your certificate and later to authorize use of your private key. So keep the pass phrase in a safe place. Protect it from unauthorized use.

- Type the remaining information.
Give information about the following and press return to go to the next line:
Your Country (use a two letter code; e.g.. US)
Your State (do not abbreviate)
Your Locality
Your Organization name
Your Organizational Unit
Your Common Name (see note below)
Your Email Address

Note Remember the Common Name you type here because your server must use the exact Common Name you enter here for your Certificate. Matching the name is part of the authentication process when you connect.

Later, you can see the Common Name by viewing your certificate.

- Enter extra attributes, if you wish, including a challenge password and an optional company name. Press return.
The CSR generator produces a file called `mt_cert_req.pem` to use when applying for a certificate. In addition, it produces a private key file names, `mt_private_key.pem`. This file is encrypted with the PEM pass phrase you typed at the beginning of the generating process. Protect this key from others.

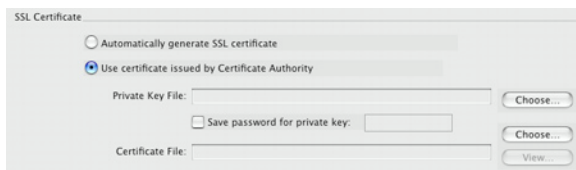
Getting the Certificate Go the CAs web site (for example, www.verisign.com or www.thawte.com) and request a certificate. Depending on your provider, you may apply in a different way.

- Generate a Certificate Signing Request as described in the previous section.
- Request a certificate online from the CA of your choice. When requested, copy and paste the CSR or `mt_cert_req.pem` text from a text editor.
Do not use a word-processing program which might add extraneous formatting.
- The CA sends the certificate to you.
The Certificate Authority sends you two files: a certificate file which contains a public key and a private key file. You may place the files in the MassTransit Security folder for ease in locating them when you set up MassTransit.

Setting up MassTransit to use a certificate

MassTransit uses the certificate to verify who you are when you connect. To set up certificate information, follow these steps.

- In the Setup window, select the Security tab.



- For SSL Certificate, select either Automatically generate SSL certificate or Use certificate issued by Certificate Authority.
If you choose to have MassTransit generate the SSL certificate, MassTransit creates a private key, creates a certificate request, and then signs the certificate request creating the certificate. The pass phrase for the private key file is automatically generated. You can skip the remainder of the steps.

Note This does not guarantee your identity to remote server.

3. If you choose to use a certificate issued by a certificate authority, either a trusted root Certificate Authority or your own certificate authority, click Choose to locate the private key file.
This is the private key generated by the CSR program.
4. If you wish, check Save Password for private key, then type the pass phrase in the text box to the right.
This saves the pass phrase on disk. If you do not save the pass phrase, you are prompted for it every time MassTransit starts.
5. Click Choose to locate the Certificate.
This is the certificate you received from your CA.
6. If you wish, click View to view the Certificate.
When you view the certificate, you see the Common Name assigned to the certificate. This Common Name is the name that must be specified by a server calling you in the TCP/IP Secure Outgoing Calls dialog.
7. After finding out the names of the Certificate Authorities your remote server is using, check to make sure the Trusted Root Certificate Authorities certificates include these names.
When you connect using a secure connection, MassTransit checks the remote server's certificate using a certificate provided for that purpose by the remote server's Certificate Authority. MassTransit comes with a number of the more common trusted root CAs. You may have to download a certificate from the remote server's CA website and import it into MassTransit if it is not included.
8. If the CA for your server's certificate is not on the Trusted Root Certificate Authorities list, click Import to import a certificate you have previously obtained either from a CAs web site or elsewhere.
The CA is added to the list.
9. Highlight the certificate and click Remove if you no longer want the name on the list.
The certificate is removed but is not deleted from your computer.
10. Click OK when you have completed all tasks.
MassTransit is ready to provide secure connections.

Chapter Two: Transferring Files

MassTransit makes it easy to send to and receive files from your MassTransit Server. You can send files to the MassTransit Server's computer, or even to an application or printer at the MassTransit Server's location. And you can receive files from your MassTransit Server. But first you'll have to make sure your MassTransit software has all the right settings. This chapter covers the following topics:

- Transferring files
- Sending files to your Server
- Receiving files from your Server
- Cancelling a connection

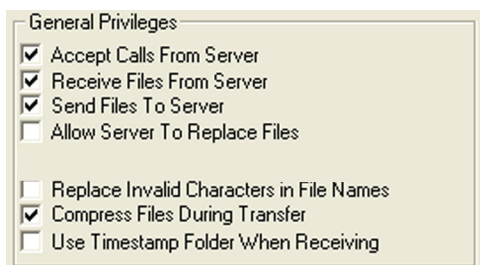
Transferring files

After setting up your communications method you can receive files from and send files to the MassTransit Server. First, set the Privileges in the Communications tab of the Setup window. Make sure you select Receive Files From Server and Send Files to Server. The MassTransit Server must have selected the Answer Incoming Calls option and configured MassTransit to send and receive files from you.

SETTING PRIVILEGES

To set up privileges for sending files, follow these steps.

1. In the Setup window, select the Communications tab.



Accept Calls From Server allows the server to call you.

Receive Files From Server allows the server to send files to you.

Send Files To Server automatically sends files designated for sending each time a connection is made. For more information, see "Designating Files to Send" on page 17.

Allow Server To Replace Files automatically overwrites files of the same name in the server's Received folder during file transfer. If you don't want to overwrite files, you can use a timestamp folder (see below).

Replace Invalid Characters in File Names for Windows permanently converts filenames from Macintosh computers that have invalid Windows characters (such as `<code>or ?</code>) by substituting dashes`

(-) for invalid characters. See the section below for more information. If this option is not checked, the server does not accept files that have illegal characters in their names.

Compress Files During Transfer compresses files for transfer.

Use Timestamp Folder When Receiving (TCP/IP connections only) places files received from the server in a new folder for each transfer; the folder is named with the date and time.

2. For Privileges, make sure the Send Files To Server option is selected.

3. If you want to receive files from the MassTransit Server, select the Receive Files From Server option.
4. Click OK or Save, if necessary.

CONVERTING MACINTOSH FILE NAMES FOR WINDOWS FILE NAMES

If you are using a Macintosh computer to send files to a Windows MassTransit Server using a hard drive formatted for the FAT file system with either Windows 2000, Windows 2003, or Windows XP, you should create filenames which comply with the Windows naming rules. However, MassTransit for Windows recognizes filenames which are invalid and can change them into valid filenames if you check the privilege Replace Invalid Characters in Filenames. This is true no matter which version of MassTransit for Macintosh you are using. An alternative is if you use Windows 2000, Windows 2003, or XP with a hard drive formatted for NTFS. MassTransit can store the illegal characters on the hard drive. These can be used to maintain the illegal characters when they are on the Windows machine and, then, can be sent to Macintosh clients.

Creating valid filenames To create filenames that are valid on a Windows computer, use any letters or numbers, but check for the validity of symbols. Windows filenames cannot end with a space or a period (.).

To correct invalid file names from a Windows server, follow the steps above for changing Privileges and turn on Replace Invalid Characters in File Names for Windows . To have MassTransit reject files with invalid characters, turn this option off.

Note If you have one or more filenames that are similar except for invalid characters, substituting dashes in the filenames may result in identical filenames when the files are received on a Windows MassTransit Server. In this case, MassTransit only sends the first file. Your log and your MassTransit Server's log explain why the other files were not sent.

VIEWING THE TRANSFER OF FILES

You can watch the transfer of files on the Status window.

TCP/IP	Connected to Cairo (678.456.123.0)
Sending:	Ad Review (file 4 of 4) 420.16K of 420.17K (25209.5 K/min.1)
Receiving:	Photo May cover (file 1 of 2) 900.18K of 1.37M (18003.6 K/min.1)

Designating files to send

Select files you want to send using MassTransit. Use the Add Files button in the Files window to designate files to send. Transmitting the file does not move nor change the original. This is useful if you want to send a file located on a network drive and you don't want to copy it to the mailbox folder on your local system.

Note The To Send tab in the Files window shows all the files designated for sending for either method discussed above.

BY DRAGGING TO THE FILES WINDOW TO SEND TAB

To designate files to send without moving or copying the files, follow these steps.

1. In the Files window, select the To Send tab.
2. Drag Files from the Macintosh Finder® or Windows Explorer® into the To Send tab.
3. Click Connect to send the files.

USING THE FILES WINDOW ADD BUTTON

To designate files to send using the Files window Add Files button, follow these steps.

1. In the Files window, select the To Send tab.

2. Click Add Files in the Files window.
3. Locate the file or files you want to send. Select one and click Add. Repeat for more files. Click Add All to send all files in the currently displayed folder.
4. If you decide that a file you added should not be sent to the server, select it and click Remove.
5. Click Finish.

REMOVING A FILE'S "TO SEND" STATUS

To remove a file's "To Send" status, follow these steps.

1. In the Files window, select the To Send tab.
2. Select the file you no longer want to send in the To Send list, then click Remove.
Press Shift and click to multiple nonadjacent files. You can also press Command (Macintosh) or Control (Windows) and click to deselect an individual file. To select all, choose Select All on the Edit menu, or press Command A (Macintosh) or Control A (Windows).

ADDING A JOB TICKET

Before sending files to the MassTransit Server, you can use the job ticket feature to give your MassTransit Server detailed information about the file and explain what you want done with the file, how to return the results, and how you will pay.

To create a job ticket for a file, follow these steps.

1. Designate a file to send using the To Send folder.
For more information, see "Designating Files to Send" on page 17.
2. In the Files window, select the To Send tab.
3. Select the name of the file from the To Send list and click the Job Ticket Add button (Macintosh) or Add... button (Windows).

The screenshot shows a 'Job Ticket' dialog box with the following fields:

- Name
- Company
- Phone
- Fax
- Email
- Account Number
- Address
- City
- State
- Postal Code
- Country
- Additional Customer Information (text area)

Buttons: Cancel, Save

4. Fill out the job ticket entries and click OK or Save.
For more information, see the descriptions in the following sections.
5. Choose Clear Job Ticket Fields on the Edit menu (Macintosh) to clear all fields in the ticket if required.

Modifying and managing job tickets

After you create a job ticket for a file, you may discover you need to change something in the ticket. Even after saving its settings, you can reopen the job ticket and modify it as long as you have not yet sent its associated file. Once you transmit the file and its job ticket, however, you can not make changes to that ticket. Similarly, you cannot make changes to information in the job tickets attached to files that your MassTransit Server sends to you. The universal "no" symbol over the icon in the Job Ticket window indicates a job ticket that cannot be modified. If you need to send a file with such a job ticket, designate it for sending, then attach a new job ticket.

Viewing or editing a job ticket

MassTransit lets you view and edit job ticket information. To view or edit the job ticket for a file, follow these steps.

1. In the Files window, select the To Send tab.
Any file in the list that displays a job ticket icon in the job ticket icon column has job ticket information associated with that file.
2. Select the name of a file from the list and click Edit to view the job ticket.
If the Job Ticket button is absent, no job ticket is associated with that file. You cannot make changes to job tickets of files that have been sent or received.

SENDING FILES

After designating the files or folders you want to send to the MassTransit Server, you can send them manually or passively. Files designated for sending appear in the Files window To Send tab. After files are sent, they are listed in the Files window Sent tab.

Sending files manually

You can send files manually to the MassTransit Server at any time. Your MassTransit Server must set up MassTransit to accept files and receive calls from you.

To send files to the MassTransit Server manually, follow these steps.

1. Designate what files you want to send.
See "Designating Files to Send" on page 17.
2. Open the Status or the File window.
3. Click Connect.
The Status window shows the progress of the connection. The Connect button changes to Disconnect. Click it to cancel a transmission. Instead, you may select the Connect button of the Files window.

Letting the Server Retrieve Files

If you prefer, you can let your MassTransit Server initiate a connection to retrieve files from your system. Your system must be set up to send files to the MassTransit Server and answer incoming calls. For more information, see "Setting Up Communications" on page 8. In addition, the MassTransit Server must set up MassTransit to receive files from you.

First, designate what files you want to send. See "Designating Files to Send" on page 17. The transmission will begin as soon as the MassTransit Server connects to your system.

Receiving files from the server

Sometimes, the product you want back from your MassTransit Professional or Enterprise Server is electronic (such as a trapped graphic file) rather than physical (such as pages from a printer). MassTransit is just as handy for receiving files from your MassTransit Server as for sending them. You have two ways to receive files from the MassTransit Server. You can configure MassTransit to wait for incoming calls from the MassTransit Server, or you can actively make a connection.

When a connection is made, all files designated to be sent by you or the MassTransit Server are transferred. As MassTransit receives files, they are placed in the Received folder in the mailbox folder and listed in the Received tab of the Files window. You can watch the transfer process from the Status window.

THE RECEIVED MAILBOX

The first time you start the MassTransit Application Client, it creates a Received folder in the mailbox folder (located in the same folder with the MassTransit Application Client). MassTransit uses this folder to store files your MassTransit Professional or Enterprise Server sends to you.

RECEIVING FILES AUTOMATICALLY

You may want to control when you receive files from the MassTransit Server. You can ask your MassTransit Server to configure MassTransit to transmit files to you at a specific time of day or at a specific interval. Then you would have to make sure MassTransit was ready to receive those calls at the specified days or times.

RETRIEVING FILES MANUALLY

You can manually initiate a connection and retrieve files whenever you want. If the MassTransit Server has designated files to send and each of you has set the proper privileges, all files designated for sending (by either party, either direction) will be transferred when you make the connection.

To connect to the MassTransit Server manually, follow these steps.

1. Open the Status or the File window.
2. Click Connect.
The Status window shows the progress of the transmissions. If no files are designated, the connection is closed. For information on cancelling a transmission in progress, see "Cancelling a Connection" below. Instead, you may select the Connect button of the Files window.

VIEWING RECEIVED FILES WITH THE FILES WINDOW

The Received tab in Files window shows all files received from the MassTransit Server. You can sort the list, and invert it.

In the Files window, select the Received tab.
The received files are listed.

Cancelling a Connection

Whenever your system is connected to the MassTransit Server system, you can terminate that connection at any time. This is useful, for example, if you realize you need to make changes to a file you are sending.

When a transmission is interrupted, whether manually or by accident, any files that were successfully transmitted are no longer designated for sending. Files not completely transferred retain their "To Send" status. Unless you or your MassTransit Server make any changes in settings, the remaining unsent files will be transmitted the next time a connection is made. For information on ways to designate files for sending, see "Designating Files to Send" on page 17.

To cancel a connection, follow these steps.

1. Open the Status window.
2. Under Connection Status, click Disconnect.

Chapter Three: Tracking Job Information

This chapter explains how you can get information about the work you do with MassTransit using the Log window.

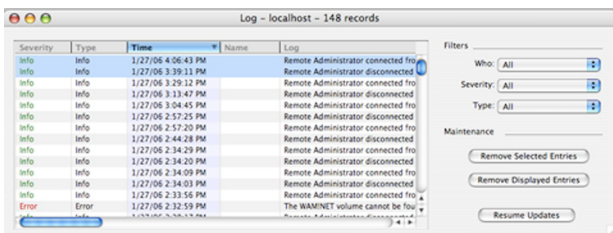
Tracking files with the Log window

Each communication and file transfer event in MassTransit is noted in the Log window. The log records the nature of the event, the time and date, and the user with whom the event is associated. In addition, the log notes the type of each event and ranks it according to one of the following three severity levels.

- Info, a message noting significant events in MassTransit including the shutdown of MassTransit
- Warning, a message noting problems that have arisen or may arise due to current system settings
- Error, a message logging problems beyond the control of MassTransit

In addition to the levels listed above, some of the most common message types the log uses are:

- Connect, indicating the remote MassTransit and user systems successfully initiated a connection
- Transfer, indicating a file was copied from one system to another
- Error, indicating a problem that does not fall into any of the other categories
- Output, indicating a file is being processed by a service
- Summary, giving a summary of files transferred and their size for the preceding transfer



You can change the size of a column by positioning the arrow over the line separating the titles in the title bar. Drag to widen or narrow a column.

While an entry in your Log is highlighted, information is not updated. Click Resume Updates to update the information or close the Log and reopen it.

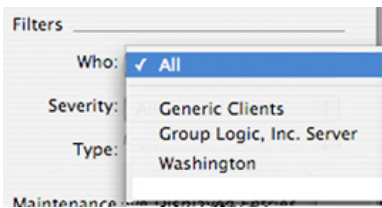
REORDERING LOG ENTRIES

When you first open the Log window, the entries are ordered chronologically with the most recent entry first. There are occasions when it may be more helpful to order the log entries another way. For example, you might want to see all log entries associated with a particular user. Or, when troubleshooting, you may want to view entries by their level (Info, Warning, or Error) or log message. The log window viewing information is easy.

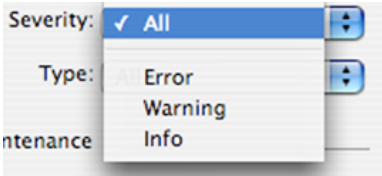
To sort log entries by category, follow these steps.

1. In the Log window, click the Time column heading to invert the order.
2. Under Filters, choose from the three dropdown menus which items you wish to display.

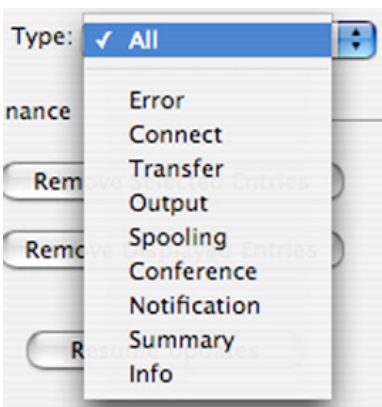
From the Who menu, select the server.



From the Severity menu, choose the severity level of items you want to display.



From the Type menu, select the Type of information you want to display.



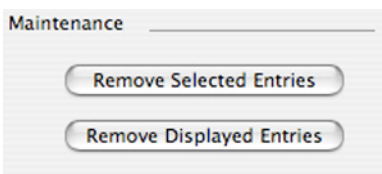
MANAGING OUTDATED LOG ENTRIES

Because the Log window records all significant MassTransit events, the list can become long and unwieldy. A long log list may slow MassTransit down. You can remove log entries that no longer have any relevance to you. You can either delete selected entries manually or set MassTransit to remove entries automatically once they reach a certain age. You can also remove entries using AppleScripts.

While MassTransit Enterprise Servers can have unlimited log size, Application Clients are limited to 32,000 entries. Entries are purged daily as they exceed this number.

To remove log entries manually, follow these steps.

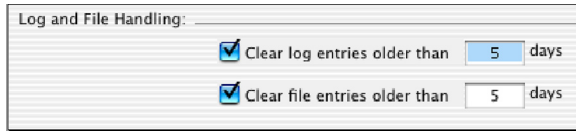
1. In the Log window, view the Maintenance area of the log window.



2. Select the log entry or entries you want to remove and click Remove Selected Entries. Press Shift and click to select multiple nonadjacent entries. You can also press Command (Macintosh) or Control (Windows) and click to deselect an individual entry. To select all, choose Select All on the Edit menu, or press Command A (Macintosh) or Control A (Windows).
-OR-
Display the log entry or entries you want to remove using the filters, then click Remove Displayed Entries.

To remove log entries automatically, follow these steps.

1. In the Setup window, select the Special tab.
2. For Log and File Handling, select Clear Log Entries Older Than <Number> Days and type an age in days. Then click Save.



Backing up Database files

Database files are created in the Databases Folder as you send and receive files. You should back up this folder and store the backups in a safe place.

Note You must quit MassTransit before you copy the contents of the Databases Folder. When MassTransit is running, files you copy may be incomplete causing problems should you use these copies.

Appendix: Troubleshooting

If you or your MassTransit Professional or Enterprise Server have difficulty initiating a connection, the checklist below may help you determine the cause to correct it.

- If your MassTransit Server is unable to initiate a connection with you, choose Setup on the Windows menu, select the Communications tab, and make sure you have selected Answer Incoming Calls.
- If your MassTransit Server is unable to send files to you, choose Setup on the Windows menu and make sure you have selected the Receive Files from Server option.
- If you are unable to send files to your MassTransit Server, choose Setup on the Windows menu and make sure you have selected the Send Files to Server option.
- If you have not given your MassTransit Server permission to replace files and you cannot receive files from your MassTransit Server, check the Received folder to make sure it does not contain files using the same names as the files the MassTransit Server is trying to send. Conversely, if your MassTransit Server has not given you permission to replace files and you cannot send files to the MassTransit Server system, have your MassTransit Server check the Received folder on the MassTransit Server system to make sure it does not contain files with the same names as the files you are trying to send.
- If you are using a TCP/IP connection and have recently changed your machine name or IP address, make sure your MassTransit Server knows this and changes settings accordingly. Similarly, find out whether your MassTransit Server has changed the MassTransit Server machine name or IP address.

Getting Help with MassTransit

Users with active maintenance contracts can call Group Logic at 1-703-528-1555 Monday through Friday, 8:00 am to 5:00 pm EST.

WEB HELP

You can visit our web site, for the latest technical information and releases. On the web site, Group Logic provides help on various information, scripts and resources. The Knowledge Base is available at <http://www.grouplogic.com/knowledge>. Various MassTransit scripts can be downloaded from <http://www.grouplogic.com/products/masstransit/scripts>.

- A**
 - access privileges 16
 - Allow User To Replace Files 16
 - authentication 12
- C**
 - Certificate Generation program 13
 - certificates 11
 - generating a CSR 13
 - obtaining 14
 - self-generated 12
 - setting MassTransit to use 12
 - using a trusted root authority 13
 - Certificate Signing Request 13
 - Client version
 - compared to Server version 5
 - communications
 - setting up 8
 - countries, banned from export of MassTransit 12
- D**
 - date and time on received folder 16
 - disconnecting 19
 - drag & drop
 - files to send
 - to the Files window 17
 - duplicate filenames 17
- E**
 - encryption 11, 12
 - exporting encryption 12
 - export list on the Web 12
- F**
 - filenames
 - invalid characters 17
 - files
 - designating to send 17
 - removing to send status 18
 - sending manually 19
 - sending passively 19
- Files window
 - designating files to send with 17
 - dragging files to 17
- firewall
 - bypassing 9, 11
- H**
 - help with MassTransit 24
- I**
 - incoming communications
 - setting up 8
 - Internet firewall 9, 10
 - invalid filenames
 - sending 17
- J**
 - job ticket
 - adding to a file 18
 - viewing 19
- L**
 - levels
 - encryption 12
- M**
 - MassTransit
 - installing Client software 6
 - Server and Client versions 5
- N**
 - Navigation Bar 5
- O**
 - outgoing communications, setting up 8

P

- port
 - restrictions for TCP/IP 9
- private key 12
- privileges
 - checking for problems 24
 - requirements for receiving files 20
 - requirements for sending files 16
 - setting 16
- program
 - Certificate Generation 13
- public key 12

R

- receiving files
 - requirements for 19
 - stamp with date and time 16
- retrieving files
 - from the Server 20

S

- Secure Sockets Layer (SSL) 11
- security 11
- Send Files To User 16
- sending files
 - automatically 17
 - requirements for 16
- Server version 5
- setting privileges 16
- Setup window
 - Communications
 - incoming & outgoing calls 8
 - Special
 - log and file handling 23
- slow performance
 - too many log files 22
- Status window
 - cancelling a connection 20
 - disconnecting 19
 - viewing files being transferred 17
- support 24

T

- TCP/IP 8
 - restrictions on port 9
- TCP/IP Secure 10
- Timestamp Folder When Receiving 16
- troubleshooting 24
- Trusted Certificate Authorities 13

V

- verifying a caller 12