MassTransit 6.0 Enterprise Web Configuration
for Macintosh OS 10.5 Server

GroupLogic

November 6, 2008

Group Logic, Inc.
1100 North Glebe Road, Suite 800
Arlington, VA 22201
Phone: 703-528-1555 Fax: 703-528-3296
E-mail: info@grouplogic.com
Internet: http://www.grouplogic.com

Using This Document

This document is a comprehensive guide to installing and upgrading the MassTransit Web (MTWeb) component provided with MassTransit Enterprise. MassTransit supports the following features via the web interface: file transfer, job tickets, log viewing, password change and reporting. MassTransit 6.0 introduces new reporting features including system based reports and contact based reports; passkey login enabling users to log into the web interface without having to know a username and password; and two new levels of SSL encryption for secure data transfer. To learn more about the new 6.0 features, please go to the "Other MassTransit 6.0 Resources" section of this document.

MTWeb requires four components – MassTransit Enterprise, MySQL 5, a web server (IIS or Apache), and PHP 5. Please view the latest ReadMe for a comprehensive list of the recommended system requirements located at http://www.grouplogic.com/files/glidownload/mtreleases.cfm.

Before You Begin

To configure the MassTransit Web Interface on Mac OS 10.5 Server you will need to have:

- MySQL 5 installed and configured
- MassTransit Enterprise 6.0 installed and configured
- Apache 2 (installed by default on Mac OS 10.5 Server).

NOTE: You MUST install the MassTransit web site files corresponding to your MassTransit engine version. **MassTransit 6.0 requires version 6.0 web files.**

For assistance configuring the MassTransit web interface on other versions of Mac OS X, please contact Group Logic support.

System Requirements

MassTransit Web requires the following components:

- MassTransit Enterprise version 6.0 or higher.
- MySQL version 5.0.42 is required for MassTransit 6.0.
- PHP 5.2.x.
- Apache 2 (installed by default on Mac OS 10.5 Server).

Along with the above components, MassTransit Web requires one of the following web browsers:

Windows

- Internet Explorer 7 or higher
- Firefox 2 or higher

Macintosh

- Safari 3 or higher
- Firefox 2 or higher

For a complete listing of all system requirements, please see the MassTransit ReadMe.

MassTransit Web Setup for New Installations

These instructions will properly configure the MassTransit web interface for new MassTransit installations. If you are upgrading from a previous version of MassTransit that had the web interface configured, please contact Group Logic technical support to ensure a smooth upgrade.

The MassTransit web setup consists of three steps:

1. MassTransit web configuration
2. PHP installation and configuration
3. Web Server setup.

The following sections provide a comprehensive guide to setting up MTWeb on Mac OS 10.5 Server systems with specific instructions for Apache.

MassTransit Enterprise and MySQL must be installed and running before configuring MTWeb. See the Installation Guides for Macintosh and Windows included on the CD or with your download package for assistance.

Apache 2.2 comes pre-installed and is the default web server on Mac OS 10.5 Server. Note that Apache 1.3 is also installed with Mac OS 10.5 Server. You should confirm that you are using Apache 2.2 on the Overview panel of the Web Server section of Server Administration. These instructions require Apache 2.

Step 1: Configuring MassTransit

The following instructions provide steps to configure MassTransit Web. The *MassTransit.cfg* and *mtweb.ini* files must be configured.

1. Navigate to the **Extras** folder within the **MassTransit** directory. Copy the *MassTransit.cfg* file to the **MassTransit Server 6** directory. If there is already a version of *MassTransit.cfg* in the **MassTransit Server 6 directory**, skip this step.

2. Open the *MassTransit.cfg* file and make sure to uncomment (delete the "%%") the ENABLE_SOAP_API and SOAP_API_PORT flags. Set the ENABLE_SOAP_API flag to TRUE. Leave the SOAP_API_PORT set to the default, 50050.

   NOTE: You must restart MassTransit Enterprise Engine for any changes to take affect. To verify that these changes have taken effect, launch the MassTransit Administrator and look at the log; a message appears stating, "SOAP interface enabled on port 50050."

3. Give READ & WRITE permissions to the user running the web process for the **parsed** and **templates_c** folders which can be found inside the **MTWeb** directory. On Mac OS X, this is should be the user and group the Apache web server is using. The default user and group are both **www**. Please consult the FAQ section at the end of this document for enabling writable permissions on folders.

   NOTE: Any time the MTWeb files are updated, you must delete the contents of the **parsed** and **templates_c** folders with the exception of the *readme.txt* files.

4. Edit the *mtweb.ini* file in a plain text editor. By default, the file is located inside the **MassTransit**

Server 6\MTWeb directory.

NOTE: All lines beginning with "#" in the *mtweb.ini* file are considered commented and therefore ignored. You must uncomment all lines mentioned in the steps below.

a. Enter a valid username and password in the DB_USER and DB_PASSWORD fields respectively. The username and password created during the MassTransit installation can be used for MTWeb. The default MySQL installation username is "masstransit". Please consult the FAQ for information on creating a new user in MySQL.
b. Verify that the following lines in the *mtweb.ini* file are configured correctly. Please view the file for detailed definitions of each field. In general, the SOAP_PROXY_ADDRESS and DB_HOST will both be localhost; the DB_NAME will be mtdatabase.
   SOAP_PROXY_ADDRESS
   DB_HOST
   DB_NAME

Step 2: PHP Setup

The steps below provide setup instructions for PHP. These steps assume that you do not have a previous version of PHP installed.

1. Copy the INSTALL.sh and gliphp.tar.gz files to the same folder on your server. These files may be found on your CD on or at http://www.grouplogic.com/files/glidownload/mtreleases.cfm.
2. Run the INSTALL.sh script.
   a. Open the Terminal application in Applications->Utilities.
   b. Type "sudo " and then drag-and-drop the INSTALL.sh script from the Finder into the Terminal window. Your command should now look something like this (the path will vary):
      `sudo /Users/username/Desktop/gliphp/INSTALL.sh`
      Press enter to run the command.
   c. Type your Mac OS X administrative password if prompted.

   The installer script will leave a log in /usr/local/gliphp/install.log.

3. Open Server Administration for the web server.
   a. Open Server Admin from /Applications/Server
   b. Enter your administrative password if prompted.
   c. You may receive a dialog that prompts you "Are you sure you want to use Server Admin?" Choose "Use Server Admin".
   d. Click on the triangle next to the server name on the left to expand the list of services.
   e. Click on Web from the list of services.

4. Click on the "Settings" button in Server Admin at the top of the window.
5. Click on the Modules tab.
6. Ensure the "Module Path" for the php5_module is set to /usr/local/gliphp/libphp5.so

   Note: If you need to change the path, you may need to uncheck and check the "Enable" checkbox in order to enable the **OK** button after you change the path.
7. Click "Save" to save the configuration.

8. Close Server Admin.

PHP setup is now complete. You can verify that PHP is running successfully by consulting the FAQ.

Step 3: Apache Web Server Configuration

1. Open Server Administration for the web server.
    a. Open Server Admin from /Applications/Server
    b. Enter your administrative password if prompted.
    c. You may receive a dialog that prompts you "Are you sure you want to use Server Admin?" Choose "Use Server Admin".
    d. Click on the triangle next to the server name on the left to expand the list of services.
    e. Click on Web from the list of services.

2. Click on the "Sites" button at the top of the window.

3. Uncheck the Enabled checkbox next to the existing site to disable it.

4. Click on the "+" button in the Sites pane to add a new site.

5. Set the domain name to the name of your domain (www.yourdomain.com), or leave the field blank.

6. Set the IP field to the IP address you want the web server to listen on. Note that selecting "Any" may cause the web server to behave improperly and is not recommended.

7. Change the web folder field to the MassTransit webroot folder. (/Applications/MassTransit Server 6 Folder/MTWeb/webroot)

8. Ensure "index.php" is in the list of default index files.

9. Change the administrator email to the appropriate email@your.domain.com.

10. Check the box to enabled the new site you just configured (the name will be the domain name you entered in step 5).

11. Click "Save" to save the site.

12. If the web server is running, click on the Stop Service button to stop it.

13. Click on the Start Service button to start the web server with your configuration.

The Web Server configuration is now complete. At this point, the website should be running. You can verify this by opening up a browser and entering the IP Address of the machine on which MTWeb was configured. The MassTransit Web login page should appear. The MassTransit Engine must be running for the login page to appear. You must create a valid web client account in MassTransit to successfully login.

Restart the machine. This is required to ensure that all new settings for Apache and MassTransit are properly loaded and to remove any cached versions of the old website that may be in memory.

MassTransit Web Setup with SSL File Transfer

Enabling SSL using MTWeb allows for secure data transfer between the MassTransit Enterprise Server and MassTransit web clients.

To setup MassTransit Web with SSL:

1. In the MassTransit Administrator edit a Web Client contact entry by selecting the entry from the Contacts window and clicking the 'Edit' button.
2. Select the Security tab and locate the Web Privileges section.
3. Check the checkbox labeled **Use Secure Connection To Transfer Files.**
4. Select an Encryption Level and click 'OK' to save.

   NOTE: The SSL transfer is enabled in the MassTransit Enterprise Server on a per contact basis. Therefore, this must be followed for all Web Client contacts that require SSL encryption for data transfer.

MassTransit Web Setup Using SSL Certificates or HTTPS

Do I Need A Secure Configuration?

Information sent to and from the web server in a basic configuration is unencrypted. You can configure your web server to use secure sockets (SSL) to encrypt web traffic. Instead of communicating on the default web port (80), your web server will use the default secure port (443).

To simultaneously serve SSL and non-SSL traffic requires two installations of the MassTransit Web folder, each with their own mtweb.ini. This configuration is not officially supported and is not covered by this document.

Note that a using SSL for your web server encrypts your web traffic; encryption of MassTransit file transfers is configured separately in the MassTransit application. See the section "MassTransit Web Setup With SSL File Transfer".

Before you Begin

In order to ensure a successful setup of a secure Apache web server for the MassTransit web interface, first:

- Configure a working basic web configuration (see "MassTransit Web Setup for New Installations" above).
- Determine what port you want to run your secure web traffic over. The default port for secure traffic is 443. Note that MassTransit and the web server must use different ports. If you want to run both on the same port, you will need to follow the instructions in the "MassTransit Web Setup for Multihoming" section.

- Obtain a signed certificate, corresponding private key, and the certificate authority. For information on generating or obtaining these files, see the document "Generating and Signing Certificates."
- Ensure you are logged into the server as a user with administrative privileges.

Configuring Apache for Secure Connections

To configure IIS to run as a secure web server using SSL, follow the steps below.

Configure MassTransit for Secure Web Connections

1. Within MassTransit edit the *mtweb.ini* file located inside the **MTWeb** directory and change the following line:
   WEB_SERVER_SECURE = "true"
2. Save the *mtweb.ini* file.

Install the Server Certificate

3. Open **Server Administration** for the web server:
   a. Open **Server Admin** from /Applications/Server
   b. Enter your administrative password if prompted.
   c. You may receive a dialog that prompts you "Are you sure you want to use Server Admin?" Choose "Use Server Admin".
   d. Click on the triangle to expand the list of services.
   e. Click on **Web** from the list of services.
   f. Click the "Settings" button at the top of the window.
4. Click on the **Modules** tab.
5. Verify that ssl_module is enabled.
6. Click on the **Sites** tab.
7. Click on the site you are configuring for MassTransit to edit it.
8. Verify that you have your domain name entered in the "Domain Name" field. If you are not using DNS, you can enter the IP of your web server.
9. Change the "Port Number" field to 443 (or whatever port you decided to listen on).
10. Click on the **Security** tab.
11. Check the "Enable Secure Sockets Layer (SSL)".
12. From the Certificate pulldown, select "Custom Configuration."
13. Specify the Certificate File, Key File, and Certificate Authority File fields to point to the signed certificate, private key, and certificate authority files you are using to secure your server.

14. Enter the passphrase for the private key in the “Pass Phrase” field.
15. Save the configuration.
16. If the web server is running, click on the Stop Service button to stop it.
17. Click on the Start Service button to start the web server with your configuration.

Verifying Your Setup

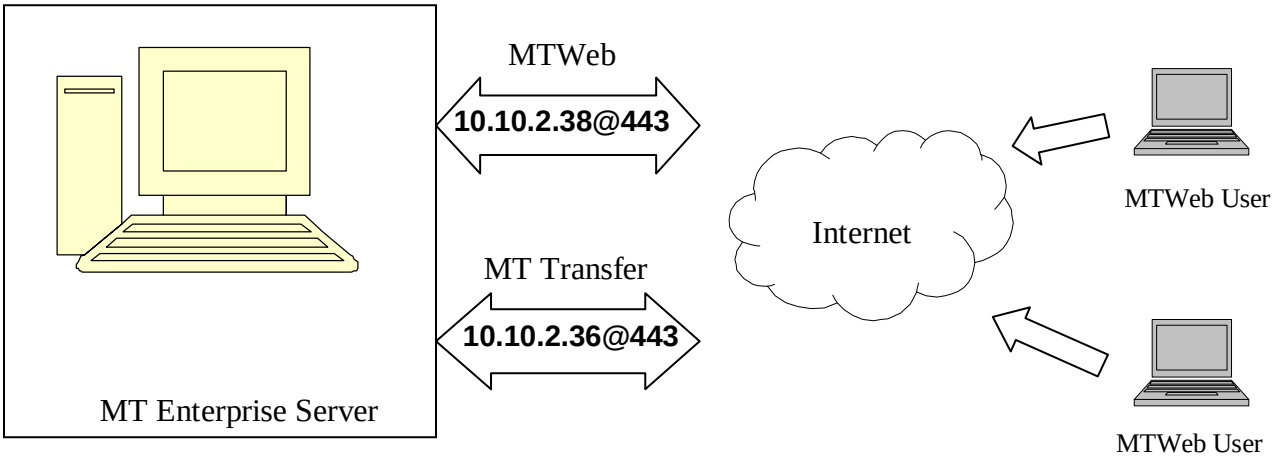
18. Open a web browser.
19. Point the web browser at https://localhost. If you are using a port other than 443, point the web browser at https://localhost:xxx where xxx is the port you are using.

You should see the MassTransit login page and be able to login with a configured web client login and password. After you login, you should be able to upload and download files.

MassTransit Web Setup with Multi-homing

By default MassTransit (MT) listens on all IP Addresses at the specified port. If the machine is configured with multiple IP Addresses, it is often useful to designate an IP Address for MassTransit and the web server. This is especially valuable when both the website and the MassTransit server must run on SSL (port 443). In such cases, you must configure MassTransit with multi-homing.

The figure below provides an example where the MassTransit Server will transfer files using SSL on IP Address 10.10.2.36 on port 443. The website (MTWeb) will be configured on IP Address 10.10.2.38 on port 443.



The setup instructions below are based on the diagram above.

1. Move the *MT IP Addresses.txt* file from the **Extras** folder to the same location as the MassTransit Engine executable.
2. Edit the file and enter the IP Address that MassTransit should listen on. The *MT IP Address.txt* file should look like the following based on the above example:
   ssl=10.10.2.36

   NOTE: Ensure that the line does not start with "%%".

3. Edit the *mtweb.ini* file located in the **MTWeb** directory and change the following line:
   HOST_IP_ADDRESS = "10.10.2.38@443"

The multi-homing setup is now complete. The above setup allows users to access MTWeb via IP Address 10.10.2.38 while the file transfers (communication between MT Server & MT Assistant) will occur on IP Address 10.10.2.36.

Other MassTransit 6.0 Resources

Go to http://www.grouplogic.com/files/mt/60/OtherMassTransit60Resources.html for additional articles to help you set up, configure, and use MassTransit 6.0 and its new features. The Group Logic Knowledge Base contains many articles that provide detailed information on MassTransit 6.0 and its features and components. The HTML version of this file, "OtherMassTransit60Resources.html", is provided with your MassTransit 6.0 CD or with your download package.

Frequently Asked Questions

Q: How do I give writable permissions to a folder?
A: Follow the steps below to give writable permissions to a folder on Mac:

1. Select a folder from the Finder and press Apple + I to open the **Get Info** dialog.
2. The Group that is configured in the Apache httpd.conf file must be granted "Read & Write" permissions to the "templates_c" and "parsed" folders (located within MassTransit's "MTWeb" folder). To determine which group account Apache HTTP server is using, go to the /etc/apache2 folder and open the httpd.conf file and search for "Group". The default setting for User and Group is normally www.
3. Enable the Read & Write permissions for the Apache Group. In the Get Info dialog under Ownership & Permissions, click Details to view the current settings for Owner, Group and Others. To change permissions choose from the drop down menus. If necessary, click the lock icon and, when prompted, enter the name and password of an administrator user on your computer. Set the permissions and then close the Get Info window.

   NOTE: For further information please consult the following Article:
   http://docs.info.apple.com/article.html?path=Mac/10.4/en/mh669.html

Q: How do I obtain permission to write to the apache2 folder when running as a non-root user?
A: Follow the steps below:

1. Choose **Go → Go to Folder** from the Finder.
2. Enter **"/etc/"** in the dialog that appears and click **Go**.
3. Select the **apache2** folder in the finder window that appears.
4. Choose **File → Get Info** from the Finder.
5. Click the triangle in the "Ownership & Permissions" section to expand the details.
6. Click the lock to allow yourself to change the permissions.
7. Select the user you are logged in as from the "Owner" pulldown.
8. Authenticate by entering your password.
9. Close the Get Info window.

If you are not running as root**,** also obtain permission to write to the *httpd.conf* file.

1. Double-click on the **apache2** folder.
2. Select the *httpd.conf* file from the **apache2** folder.
3. Choose **File → Get Info** from the Finder.
4. Click the triangle in the "Ownership & Permissions" section to expand the details.
5. Click the lock to allow yourself to change the permissions.
6. Select the user you are logged in as from the "Owner" pulldown.
7. Authenticate by entering your password.
8. Close the Get Info window.

Q: How do I create a user for MTWeb in MySQL?
A: You can use the MySQL Administrator to create a user.

1. Launch the MySQL Administrator and sign on with **root** privileges.

2. Select the **Accounts** option from the top and click the 'New User' button located at the bottom left corner.
3. Enter the username and password under the Login Information group of the **General** tab.
4. Select the **Schema Privileges** tab.
5. Click on the **mtdatabase** schemata from the left and apply SELECT privileges by selecting the row labeled "SELECT" and clicking the '<' (left arrow) button.

NOTE: In order to setup MTWeb with this username and password, the above created username and password must be entered in the *mtweb.ini* file.

Q: How do I verify if PHP is installed and configured correctly?
A: Copy the *test.php* test file from the **Extras** folder, and place within your web root directory. In your browser, navigate to the test.php file, which is included in the **MTWeb** folder. If configured with MTWeb as the default site, you can just go to localhost/test.php. If PHP is configured correctly, you should see a listing of the PHP configuration settings. Once you have verified that PHP is set up correctly, you should put the *test.php* file back in the Extras folder for security reasons.

Q: Where are the error messages logged?
A: Error messages are logged to the webserver's default error log. For Apache, this log can be accessed through the console at /var/log/apache2/error_log.

Q: Upon login, I get a "Server Connection error".
A: There may be several factors causing this error. Verify following settings:

- Make sure the user specified in the mtweb.ini file has the correct MySQL privileges.
- Make sure ENABLE_SOAP_API = TRUE is uncommented (delete "%%") in *MassTransit.cfg*

Q: How do I view the php.ini file configuration?
A: Copy the *test.php* test file from the **Extras** folder, and place within your web root directory. In your browser, navigate to the test.php file, which is included in the **MTWeb** folder. If configured with MTWeb as the default site, you can just go to localhost/test.php. This will display the configuration information about PHP. One useful thing is to look at is the "Configuration File (php.ini) Path" to make sure you know where the active php.ini file is.

Q: How do I find out the version of MTWeb I'm running?
A: Login to MTWeb using a browser. Click on the System Information link in the top right hand corner. This page will display information on the MTWeb Version and Build Number, PHP Version, Plugin version and other relevant system information.

Q: Why do I see a blank page when attempting to load a PHP page in my browser?
A: Check the Apache error log file. This log can be accessed through the Console at /var/log/apache2/error_log. If this doesn't reveal anything, temporarily turn on display_errors and/or display_startup_errors in the php.ini to see what's happening.

Appendix A: Using Secure Socket Layers (SSL)

SSL Certificates

To use SSL, a PEM format x509 certificate is required. A certificate consists of a certificate file and a key file. The certificate is used both to encrypt data being sent and as a form of identification. There are three steps to obtaining a certificate. These three steps are carried out differently for each web server, but the purpose of each step remains the same.

1. Generate a private server key. This key is later used to encrypt the outgoing data.
2. Generate a CSR (certificate signing request). The CSR is linked to the key, the identity of the server's owner, and the URL of the server. **The server URL is stored in the common name (CN) field of the certificate.**
3. Obtain CA (certificate authority) signature. The CA signs the CSR after verifying that the holder of the CSR and private server key matches the identity specified in the CSR. **The signed CSR is the certificate**. Because the receiving party trusts the CA, the CA signature proves to the receiving party that the certificate holder really is the party named in the certificate.

There are three ways to sign the CSR. The first is to have it signed by a publicly known Root CA such as Verisign or Thawte. This is optimal, since these Root CAs are known and trusted.

The second alternative is to have another CA, such as an in-house IT department or a lesser known 3rd party CA, sign the CSR. When using a CA that is not well known, it is necessary to distribute the CA's certificate to clients. Keep in mind that the CA's certificate is independent of the server's certificate! Without the CA's certificate, the receiving party cannot trust the CA and therefore cannot assign any validity to the CA's signature on the server certificate.

CA certificate distribution can be done easily via the web server itself or with MassTransit, but to guarantee security the fingerprint of the certificate must be communicated securely and verified. If the receiving party is able to verify the fingerprint of the CA certificate, then the recipient knows she or he has an authentic CA certificate and not a spoof. The task of distributing CA certificates to web browsers is complicated by the fact that different browsers expect the CA certificate to be distributed in different formats. The default format for keys, requests, and certificates is PEM. Some older versions of Internet Explorer, including IE 5.1 Mac, will only accept CA certificates in DER format. The process of distributing a CA certificate is similar for all web servers; see the "Distributing CA Certificates" section for more information.

The final method of signing the CSR is to self-sign it with the private server key. **A self-signed certificate allows encrypted communication but provides no guarantee whatsoever that the holder of the certificate has any connection to the identity specified in the certificate.** Without proof of identity the client cannot distinguish between communications with the true server and a spoof. As such, self-signed certificates do not offer true security and should only be used for testing purposes. Microsoft IIS cannot use a self-signed certificate.

All web server sections below refer to obtaining a CA signature as a single-step process.

Web Server Certificates vs. MassTransit Server Certificates

The MassTransit certificate serves a somewhat different purpose than the web server certificate. Because the web server and the MassTransit server cooperate closely when communicating with web clients, there is no need for the MassTransit Assistant to verify the identity of the MassTransit server: the MassTransit server is

automatically known to be the same entity as the web server. For communication with web clients it therefore is inconsequential whether the MassTransit server uses a CA signed certificate or an automatically generated, self-signed one.

In communication between two MassTransit servers, however, the web server is not involved and cannot act as a proof of identity. To have truly secure communication here requires that the MassTransit servers use CA signed certificates.