

# **Configuring MassTransit for the Web**

## Using Apache on Mac OS 10.2 and 10.3

Version: 1.1  
Date: 2/18/2004

## Version History

<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Changes</b>
1.0	2/2/2004	Janie Longfellow	Created from MassTransit Web Config doc.
1.1	2/18/2004	Janie Longfellow	Added copyright information.



# Table of Contents

<b><u>CONFIGURING MASSTRANSIT FOR THE WEB</u></b>	<b>4</b>
<b><u>SETUP REQUIREMENTS</u></b>	<b>4</b>
<b><u>BASIC APACHE CONFIGURATION FOR MASSTRANSIT</u></b>	<b>5</b>
BEFORE YOU BEGIN	5
CONFIGURING APACHE FOR MASSTRANSIT	5
TROUBLESHOOTING	10
<b><u>SECURE APACHE WEB CONFIGURATION FOR MASSTRANSIT</u></b>	<b>12</b>
DO I NEED A SECURE CONFIGURATION?	12
BEFORE YOU BEGIN	12
CONFIGURING APACHE FOR SECURE CONNECTIONS	13
TROUBLESHOOTING	16
<b><u>MULTIHOMING FOR APACHE</u></b>	<b>18</b>
DO I NEED MULTIHOMING?	18
BEFORE YOU BEGIN	18
CONFIGURING APACHE FOR MASSTRANSIT	18
TROUBLESHOOTING	19
<b><u>APPENDIX A: USING SECURE SOCKET LAYERS (SSL)</u></b>	<b>20</b>
SSL CERTIFICATES	20
WEB SERVER CERTIFICATES VS. MASSTRANSIT SERVER CERTIFICATES	21
<b><u>APPENDIX B: RUNNING AS ROOT</u></b>	<b>22</b>
ENABLING THE ROOT ACCOUNT	22
LOGGING INTO MAC OS X SERVER AS ROOT	22
SUDO - RUNNING INDIVIDUAL COMMANDS AS ROOT	22
<b><u>APPENDIX C: CONVERTING LINE ENDINGS</u></b>	<b>23</b>



# Configuring MassTransit for the Web

This document describes how to configure the MassTransit Remote Administration and Web Client features under Apache httpd, the default web server in Mac OS 10.2 and Mac OS 10.3. Instructions for configuring unencrypted as well as secure configuration for the web server are included.

## Setup Requirements

These setup instructions only apply to the built-in Apache web server (“Web Sharing”) on Mac OS 10.2 Client and Mac OS 10.3 Client.

**Note: If you are running MassTransit as root, you WILL NOT be able to configure Apache successfully on Mac OS 10.2 Client.**

If you are using a different web server or are on Mac OS X Server, please refer to the appropriate setup document.



# Basic Apache Configuration for MassTransit

## Before You Begin

In order to ensure the successful web setup, MassTransit Enterprise must be installed on Mac OS X. Specifically, you need to ensure:

- MassTransit is installed and running as the appropriate user (see the MassTransit manual for details).
- MassTransit is configured to listen on either TCP/IP or TCP/IP Secure (see the MassTransit manual for details).
- At least one web client is configured who can connect via an active connection method. (see the MassTransit manual for details).

## Configuring Apache for MassTransit

### Configure MassTransit for Web Connections

1. Open `mtadmin.cfg` (in the `MassTransit Remote Admin` directory) in a text editor like TextEdit.
2. Change the line

```
WEB_SERVER_ADDRESS = www.yourdomain.com:80
```

By replacing `www.yourdomain.com` with the DNS name (or IP address) and port clients will use to access the web server, like `serverX.domainname.com`. If you are unsure of what port to use, use the default port, 80.

3. Verify that `WEB_SERVER_SECURE` is set to `FALSE`.
4. Set `APACHE_MODE` to `TRUE`.
5. Ensure that `USE_SEND_PARTIAL_EVENTS = FALSE`.
6. Save `mtadmin.cfg` with Unix line endings.
  1. Save `mtadmin.cfg` and close your text editor.
  2. Run the `Fix Mac Line Endings` script (available at <http://www.groupllogic.com/products/masstransit/scripts/>).
  3. When asked to select a file to convert the line endings on, choose the `mtadmin.cfg` file.

### Configure Apache Settings in the `httpd.conf` file

7. **If you are not running as root**, obtain permission to write to the `httpd` folder.



1. Choose **Go** → **Go to Folder** from the Finder.
2. Enter `/etc/` in the dialog that appears and click **Go**.
3. Select the `httpd` 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.
8. **If you are not running as root**, also obtain permission to write to the `httpd.conf` file.
  1. Double-click on the `httpd` folder.
  2. Select the `httpd.conf` file from the `httpd` 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.
9. Open `httpd.conf` with a text editor like TextEdit. . (If you are running as root and thus skipped steps 7 and 8, you can use steps 7.1 through 7.3 to find the folder in which the file is located.)

## Main Server Configuration

Note that the lines referred to in the following section should all be the in the ‘Main’ server configuration section of `httpd.conf`.

10. Verify that the following line is present:

```
Port 80
```



11. **If, and only if, you are not running MassTransit as root**, change the section of the `httpd.conf` containing the following lines:

```
User www
Group www
```

to

```
User username
Group staff
```

where `username` is the name of the user who MassTransit will run as.

12. Find this line:

```
#ServerAdmin webmaster@example.com
```

and change it to

```
ServerAdmin serveradmin@mycompany.com
```

where `serveradmin@mycompany.com` is the email address of the MassTransit or web server administrator. This email address will be given to users when they encounter unexpected errors occur accessing the web server.

13. Change this line:

```
DocumentRoot "/Library/WebServer/Documents"
```

to

```
DocumentRoot "/Applications/MassTransit Folder/Remote
Administration/MassTransit Remote Admin"
```

where the path specified is the "MassTransit Remote Admin" directory for your MassTransit installation. **DO NOT JUST COPY THE PATH ABOVE**, as the MassTransit folder typically contains a version number.

14. Find this section:

```
# This should be changed to whatever you set
DocumentRoot to.
#
<Directory "/Library/WebServer/Documents">
```

and change it to:

```
<Directory "/Applications/MassTransit Folder/Remote
Administration/MassTransit Remote Admin">
```



where the path specified is the same "MassTransit Remote Admin" path you used for step 11. Again, DO NOT JUST COPY THE PATH ABOVE, as the MassTransit folder typically contains a version number.

15. Immediately following the <Directory> block you changed in step 12, find this line:

```
Options Indexes FollowSymLinks MultiViews
```

and change it to:

```
Options Indexes FollowSymLinks MultiViews ExecCGI
```

16. Change this section:

```
<IfModule mod_dir.c>
    DirectoryIndex index.html index.htm
</IfModule>
```

to

```
<IfModule mod_dir.c>
    DirectoryIndex index.html index.htm default.html
</IfModule>
```

Note that `index.htm` may or may not be on this line.

17. Find this line in `httpd.conf`:

```
<Files ~ "^\.ht">
```

and change the line to read:

```
<Files ~ "^\.ht|^\.cfg">
```

## Enabling CGIs

18. Find this line:

```
#AddHandler cgi-script .cgi
```

and change it to:

```
AddHandler cgi-script .cgi
```



19. Add this line beneath the line you changed in 18:

```
AddHandler cgi-script .acgi
```

## Saving Your Changes

20. Save the file with Unix-style line endings; see “Appendix C: Converting Line Endings” for details.

## Launching Apache

21. **If you are not running MassTransit as root:**

1. Open **System Preferences** (located in `/Applications/Utilities`).
2. Click on “Sharing”
3. Click on “Personal Web Sharing”
4. If “Personal Web Sharing” is on, click **Stop** to stop the web server.
5. Click **Start** to start the web server.

22. **If you are running MassTransit as root:**

1. Open Terminal (located in `/Applications/Utilities`).
2. Type `sudo apachectl stop`.
3. Type `sudo apachectl start`.

If Web Sharing hangs on startup or Apache reports that `httpd` could not be started, consult the Troubleshooting section below for possible solutions.

## Verifying Your Setup

23. Open a web browser on the machine you just configured.
24. Point the web browser at `http://localhost`.

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. See the MassTransit manual for information on how to transfer files using the web client.



If you do not see the MassTransit login page or cannot transfer files, please consult the Troubleshooting section.

## Troubleshooting

Consult the list below for possible solutions to common setup problems as well and places to look for more information on your errors. Note that the web server must be restarted for most changes to take effect.

### Apache Logs

It may be useful to access the Apache error and access logs to get more information about problems that may be occurring.

To access the Apache error log:

1. Open a Terminal window.
2. Type `tail /var/log/httpd/error_log`.
3. The terminal will display the last several lines of the Apache error log.

To access the Apache access log:

1. Open a Terminal window.
2. Type `tail /var/log/httpd/access_log`.
3. The terminal will display the last several lines of the Apache error log.

### **Symptom: Running `sudo apachectl start` reports “httpd could not be started.”**

Consult the Apache error log (see instructions above). The error log should give more information on what is keeping Apache from starting.

### **Symptom: When launched from the Mac OS X System Preferences UI, Apache never completes startup.**

There may be a syntax error in `httpd.conf` or another of Apache’s configuration files. Try launching Apache from a terminal window using `sudo apachectl start` as described above. You should get an error message indicating exactly what line is preventing Apache from starting. You can also consult the Apache error log.

### **Symptom: “Page Not Found” is displayed in the web browser when a user tries to access the MassTransit login page.**



There may be an error in `httpd.conf` or another of Apache's configuration files. Double check the changes specified in this document, especially the path specified in the `DocumentRoot` and `Directory` settings in `httpd.conf`.

**Symptom: "Internal Server Error" is displayed in the web browser when a user tries to log in to the MassTransit web interface.**

This error indicates the CGI cannot communicate with MassTransit. One common cause of this is that Apache was launched using the GUI in a scenario where it must be launched from a terminal window. Ensure that you followed the right instructions in the "Launching Apache" section.

Another common cause is that in `mtadmin.cfg` `APACHE_MODE` is not set to `TRUE`.

**Symptom: "Can't find a server. Code: 42" is displayed in the web browser when a user tries to log in to the MassTransit web interface.**

This error indicates that MassTransit is not running; launch it and try to login again.

**Symptom: Plugin tab does not display or stays perpetually in the "Initializing" state, but the rest of the web interface works.**

This indicates that the `WEB_SERVER_ADDR` field in `mtadmin.cfg` is not set correctly. Verify that you have the proper URL or IP address followed by a `:80` (or whatever port your web server is running on).

**Symptom: Clients can log in and the plugin tab displays properly, but file transfer fails**

This behavior indicates that the client can communicate successfully with the web server and the CGI is successfully communicating with the MassTransit server, but the MassTransit Assistant running alongside the client's web browser cannot communicate directly to MassTransit.

Verify that no firewalls are blocking traffic and that the MassTransit server is listening for traffic. The MassTransit server must listen on a port that is not in use by the web server.



# Secure Apache Web Configuration for MassTransit

## 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 Remote Admin folder, each with their own mtadmin.cfg and CGI executable. 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 MassTransit manual for details.

## 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 “Basic Apache Configuration for MassTransit” 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.
- Obtain a signed certificate and corresponding private key. 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.
- **If you are running on Mac OS 10.2:** One of the OpenSSL security patches issues by Apple rendered Apache incapable of serving SSL traffic in a CGI environment. There are three options:
  1. Upgrade to Mac OS X 10.3 (Panther).



2. Downgrade the affected file, `libssl.so`, to the old version. (Note that this old version will be missing the security fixes of the new version!). See [http://ganter.dyndns.org/misc/apple\\_ssl.php](http://ganter.dyndns.org/misc/apple_ssl.php) as well as <http://www.macintoshhints.com/article.php?story=20030402004719491&query=ssl+apache>.
3. Install a fresh copy of Apache instead of using Mac OS X Personal Web Sharing. This document does not explicitly cover that approach, but the information supplied here should be applicable.

## Configuring Apache for Secure Connections

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

### Configure MassTransit for Secure Web Connections

1. Open `mtadmin.cfg` (in the `MassTransit Remote Admin` directory) in a text editor.
2. Change

```
WEB_SERVER_ADDR = www.yourdomain.com:80
```

to

```
WEB_SERVER_ADDR = www.yourdomain.com:443
```

Do not change the domain name, only the value after the colon. If you are listening on a port other than 443, enter that port number after the colon.
3. Set `WEB_SERVER_SECURE = TRUE`.
4. Save the `mtadmin.cfg` file with Unix line endings; see “Appendix C: Converting Line Endings” for details.

### Configure Apache Settings in the `httpd.conf` file

25. Open `httpd.conf` with a text editor.
  1. Choose **Go** → **Go to Folder** from the Finder.
  2. Enter `/etc/httpd`
  3. Double-click on `httpd.conf` to open the file in a text editor.
26. Find the line:

```
#LoadModule ssl_module libexec/httpd/libssl.so
```

and remove the `#` symbol so it reads



```
LoadModule ssl_module libexec/httpd/libssl.so
```

27. Find the line:

```
#AddModule mod_ssl.c
```

and remove the '#' symbol so it reads

```
AddModule mod_ssl.c
```

28. Find the line:

```
Port 80
```

and change it to

```
Port 443
```

29. Find the line:

```
#ServerName Rambo
```

Note that the '#' symbol may or may not be present and 'Rambo' may be replaced with another name. Change this line to

```
ServerName www.mydomain.com
```

Where [www.mydomain.com](http://www.mydomain.com) is the domain name or IP address of the Apache server. Specifically, set the ServerName to the URL users are going to use in their browsers that matches the Common Name (CN) set for the SSL certificate.

30. Add the following lines after the last line of the file:

```
<IfModule mod_ssl.c>
# Some MIME-types for downloading Certificates and CRLs
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl .crl

# Initial Directives for SSL
SSLProtocol all -SSLv3
SSLPassPhraseDialog builtin
SSLSessionCache dbm:/var/run/ssl_scache
SSLSessionCacheTimeout 300
SSLMutex file:/var/run/ssl_mutex
SSLRandomSeed startup builtin
SSLLog /var/log/httpd/ssl_engine_log
SSLLogLevel info

# Enable/Disable SSL for this virtual host.
```



```
SSLEngine on
SSLProtocol all -SSLv3
SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

# Path to your certificates and private key
SSLCertificateFile /etc/httpd/ssl.key/server.crt
SSLCertificateKeyFile /etc/httpd/ssl.key/server.key
</IfModule>
```

31. Find the lines:

```
SSLCertificateFile /etc/httpd/ssl.key/server.crt
SSLCertificateKeyFile /etc/httpd/ssl.key/server.key
```

Change `/etc/httpd/ssl.key/server.crt` to the path of your certificate file. Change `/etc/httpd/ssl.key/server.key` to the path of your private key file.

32. Save the file with Unix-style line endings; see “Appendix C: Converting Line Endings” for details.

## Launching Apache

33. Open Terminal (located in `/Applications/Utilities`).

34. Type `sudo apachectl stop`.

35. If you are not running as root, enter your password when prompted.

36. Type `sudo apachectl start`.

37. If you are not running as root, enter your password when prompted.

38. Enter the private key passphrase for the server key you configured when prompted.

If Apache reports that `httpd` could not be started, consult the Troubleshooting section below for possible solutions.

## Verifying Your Setup

39. Open a web browser.

40. 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.

If you do not see the MassTransit login page or cannot transfer files, please consult the Troubleshooting section.

## Troubleshooting

Consult the list below for possible solutions to common setup problems as well and places to look for more information on your errors. Note that the web server must be restarted for most changes to take effect.

### Apache Logs

It may be useful to access the Apache error and access logs to get more information about problems that may be occurring.

To access the Apache error log:

1. Open a Terminal window.
2. Type `tail /var/log/httpd/error_log`.
3. The terminal will display the last several lines of the Apache error log.

To access the Apache access log:

1. Open a Terminal window.
2. Type `tail /var/log/httpd/access_log`.
3. The terminal will display the last several lines of the Apache error log.

To access the SSL error log::

1. Open a Terminal window.
2. Type `tail /var/log/httpd/ssl_engine_log`.
3. The terminal will display the last several lines of the Apache error log.

### **Symptom: Running `sudo apachectl start` reports “httpd could not be started.”**

Consult the Apache error log (see instructions above). The error log should give more information on what is keeping Apache from starting.



**Symptom: When launched from the Mac OS X System Preferences UI, Apache never completes startup.**

You should not launch Apache from the System Preferences UI when using a secure configuration. Please refer to the “Launching Apache” instructions above.

**Symptom: “Internal Server Error” is displayed in the web browser when a user tries to log in to the MassTransit web interface.**

This error indicates the CGI cannot communicate with MassTransit. One common cause of this is that Apache was launched using the GUI in a scenario where it must be launched from a terminal window. Ensure that you followed the right instructions in the “Launching Apache” section.

Another common cause is that in `mtadmin.cfg` `APACHE_MODE` is not set to `TRUE`.

**Symptom: “Can't find a server. Code: 42” is displayed in the web browser when a user tries to log in to the MassTransit web interface.**

This error indicates that MassTransit is not running; launch it and try to login again.

**Symptom: Plug-in tab does not display or stays perpetually in the “Initializing” state, but the rest of the web interface works.**

This indicates that the `WEB_SERVER_ADDR` field in `mtadmin.cfg` is not set correctly. Verify that you have the proper URL or IP address followed by a `:443` (or whatever port number you are listening on).

**Symptom: Clients can log in and the plugin tab displays properly, but file transfer fails**

This behavior indicates that the client can communicate successfully with the web server and the CGI is successfully communicating with the MassTransit server, but the MassTransit Assistant running alongside the client’s web browser cannot communicate directly to MassTransit.

Verify that no firewalls are blocking traffic and that the MassTransit server is listening for traffic. The MassTransit server must listen on a port that is not in use by the web server.



# Multihoming for Apache

## Do I Need Multihoming?

If your server has two network cards or is otherwise configured to use more than one IP addresses, you have a IP multihoming setup. A multihoming setup is useful because you can use one IP address for the web server and another IP address for MassTransit. This division allows you to run all traffic over the default ports, 80 and 443.

## Before You Begin

In order to have MassTransit and your web server listen use different IP addresses, you must first:

- Set up your server with two different IP addresses
- Restrict MassTransit to listen only on certain IP addresses. See the Knowledge Base article “Configuring MassTransit for Multihoming” at <http://www.grouplogic.com/knowledge/index.cfm/fuseaction/view/docID/56> for details on how to accomplish this.

## Configuring Apache for MassTransit

1. Open `httpd.conf` with a text editor.
  - a. Choose **Go → Go to Folder** from the Finder.
  - b. Enter `/etc/httpd`
  - c. Double-click on `httpd.conf` to open the file in a text editor.
2. Find the line:

```
#Listen 443
```

change this line to:

```
Listen 123.456.7.8:80
```

where 123.456.7.8 is the IP address that Apache should use. If you are listening on SSL, change the `:80` to `:443` (or whatever SSL port you are listening on).

Note that you can use multiple lines to allow listening on multiple ports or IP addresses:

```
Listen 123.456.7.8:80
```

```
Listen 123.456.7.9:8000
```



3. Find the line:

```
Port 80
```

and comment it out with a '#' so it reads

```
#Port 80
```

Note that if you are listening on a different port, the 80 may be replaced by a different value.

## Launching Apache

4. **If you are not running MassTransit as root and you are not using SSL:**
  - a. Open **System Preferences** (located in `/Applications/Utilities`).
  - b. Click on “Sharing”
  - c. If the “Web Sharing” is checked, uncheck it to stop the web server.
  - d. Check “Web Sharing” to start the web server.
5. **If you are running MassTransit as root or you are using SSL:**
  - a. Open Terminal (located in `/Applications/Utilities`).
  - b. Type `sudo apachectl stop`.
  - c. If you are not running as root, enter your password when prompted.
  - d. Type `sudo apachectl start`.
  - e. If you are not running as root, enter your password when prompted.

If Web Sharing hangs on startup or Apache reports that `httpd` could not be started, consult the Troubleshooting section below for possible solutions.

## Troubleshooting

At this time, there are no troubleshooting tips for multihoming setups.



# 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 3<sup>rd</sup> 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. For explanations of both how to create CA signatures as well as how to self-sign certificates, see the “Generating and Signing SSL Certificates” document.

## Web Server Certificates vs. MassTransit Server Certificates

Generally speaking it is possible, and desirable, to have the web server and the MassTransit server use the same certificate. However, some web servers, such as WebSTAR and IIS, maintain strict control over the CSR generation process and hide the server’s private key. In this situation the MassTransit server has to have a separate certificate.

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.



## Appendix B: Running as root

### Enabling the Root Account

1. Open the NetInfo app in `/Applications/Utilities/NetInfo Manager`
2. Go to the security menu and select "Enable root user". You will be prompted to enter a password.

The root account is now enabled. Note that most programs (including MassTransit) installed as root will have unexpected results when run by other users. It is therefore best to not use root to install programs unless specifically instructed to do so.

### Logging into Mac OS X Server as Root

1. Go to `System Preferences -> Accounts`
2. Switch to the `Login Options` tab
3. Select "Display Login Window as: Name and password"
4. Log out of your current user
5. The login screen should now allow you to type a username (`root`) and the password you selected.

Note that most programs (including MassTransit) installed as root will have unexpected results when run by other users. It is therefore best to not use root to install programs unless specifically instructed to do so.

### sudo - Running Individual Commands as Root

In a Mac OS X terminal window, the command `sudo` can be used by any administrative user to run any command as root.

So entering:

```
sudo mycommand -myparameter
```

is equivalent to running

```
mycommand -myparameter
```

when logged in as root.

When you enter the `sudo` command, you will be prompted for your administrative password. After you enter the password, the command you entered will be run as root.



## Appendix C: Converting Line Endings

Mac OS 9 indicates the end of a line with a carriage return (often written as CR or \r). Mac OS X, like other UNIX operating systems, instead uses line feeds (often written LF or \n).

Use the `Convert Mac Line Endings` script distributed with MassTransit to convert files to use Unix style line endings. This script is available at <http://www.grouplogic.com/products/masstransit/scripts/>. The script asks you to select a file and then will change all the line endings in that file to the Unix style.

Alternatively, many text editors, such as BBEdit, can convert line endings from one format to another.



© 2004 Group Logic Incorporated. All Rights Reserved.

This document, 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 document. 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 document 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 MacOS are registered trademarks, and Communications Toolbox is a trademark of Apple Computer, Inc. Explorer, Internet Information Services, and Windows are registered trademarks of Microsoft, Inc. Webstar is a trademark of 4D, Inc. All other trademarks are the property of their respective owners.

APPLE COMPUTER, INC. ("APPLE") MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE APPLE SOFTWARE. APPLE DOES NOT WARRANT, GUARANTEE OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE APPLE SOFTWARE IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS OR OTHERWISE. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE APPLE SOFTWARE IS ASSUMED BY YOU. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME JURISDICTIONS. THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. IN NO EVENT WILL APPLE, ITS DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS BE LIABLE TO YOU FOR



Configuring MassTransit for the Web  
Apache on Mac OS 10.2 and 10.3

ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, AND THE LIKE) ARISING OUT OF THE USE OR INABILITY TO USE THE APPLE SOFTWARE EVEN IF APPLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

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 reserved under the copyright laws of the United States.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright (c) 1999-2004 The Apache Software Foundation. All rights reserved. THIS SOFTWARE IS PROVIDED ``as is" and any expressed or implied warranties, including, but not limited to, the Apache Software Foundation or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Support for Rendezvous includes software developed by the Rendezvous Project (<http://developer.apple.com/darwin/projects/rendezvous/>)

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>) Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved. This software is provided by the Open SSL Project "as is" and any expressed or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the Open SSL project or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; losses of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise).

