

SINGLE SIGN-ON FOR MTWEB

FOR MASSTRANSIT ENTERPRISE WINDOWS SERVERS WITH DIRECTORY SERVICES
INTEGRATION

Group Logic, Inc.
November 26, 2008
Version 1.1

CONTENTS

Revision History	3
Feature Highlights.....	4
Overview	4
Before You Begin	4
Configuring Single Sign-On.....	5
Configuring Internet Browsers	10
Before You Begin	10
Mozilla Firefox	10
Microsoft Internet Explorer	11
Apple Safari.....	13
Additional Information.....	14
Other Browsers	14

REVISION HISTORY

Version	Author	Changes	Date
1.0	JLB/AC	Initial document creation.	9/5/2007
1.1	HVL/AC	Update permissions settings.	9/5/2007

FEATURE HIGHLIGHTS

OVERVIEW

MassTransit 5.1 introduces a new feature that allows Active Directory users connected to an Active Directory-enabled MassTransit Enterprise Server to authenticate to the MassTransit MTWeb interface without typing a username and password. This technology, known as Single Sign-On (SSO), works with popular browsers on Microsoft Windows and Mac OS X when connecting to an IIS web server.

The end result is an environment that is more streamlined and intuitive for end users, and helps administrators better manage their MassTransit systems in a larger computing environment.

BEFORE YOU BEGIN

This document assumes that MassTransit Enterprise 5.1 or higher is installed and running, and is properly configured to access an Active Directory domain or forest for authentication. In addition, it is assumed that the MassTransit instance has been configured to use MTWeb, and that MTWeb has been properly configured for use.

For additional information on configuration MassTransit to integrate with Active Directory, or, for MTWeb Configuration, please see the documentation that came with the product or contact Group Logic Support for assistance.

Group Logic Support

www.grouplogic.com/knowledge

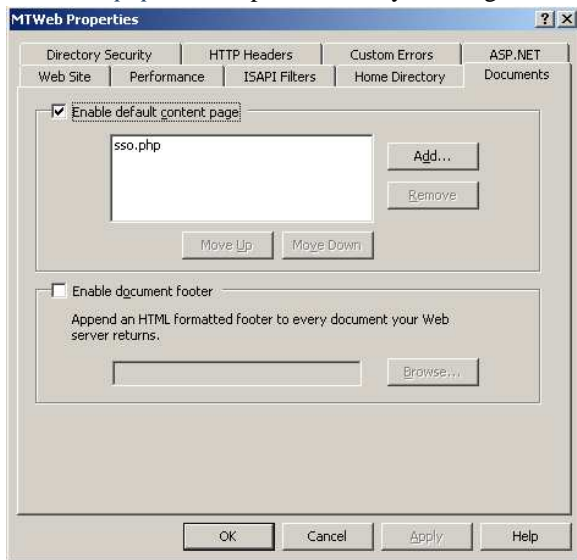
(703) 527-7979

CONFIGURING SINGLE SIGN-ON

The server running the SSO-enabled MassTransit MTWeb components must be bound to the organization's Active Directory domain. This will allow the web server (Microsoft Internet Information Services) to pass credentials received via the web browser to MassTransit and Active Directory for authentication. If the machine is not bound, or if you are unsure, ask your organization's network administrator for assistance.

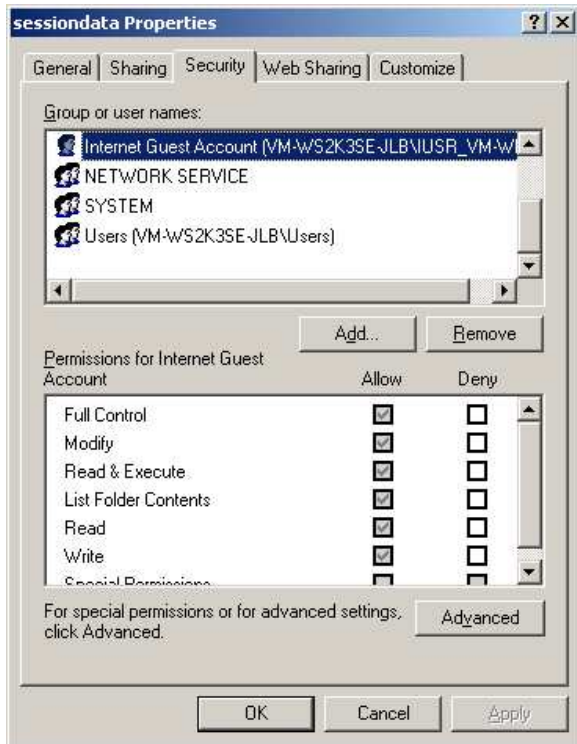
To configure SSO, follow these steps. If you have not previously configured MTWeb for use in your environment, please see the document *MassTransit Enterprise Web Configuration*. These steps will assume you already have MTWeb running.

1. Launch *Internet Information Services (IIS) Manager* from *Administrative Tools* on your Windows server.
2. Right-click on the Web Site hosting the MTWeb interface. The default name for this site is *MTWeb*. Click *Properties*.
3. In the resulting dialog, click the *Documents* tab. Ensure *Enable default content page* is selected.
4. Click *Add*, and in the *Add Content Page* dialog, type *sso.php*. Click *OK*.
5. Move *sso.php* to the top of the list by clicking the *Move Up* button. Ensure *sso.php* is listed above *index.php*, if it exists.



6. Click on the *Custom Errors* tab. The *Error messages for HTTP errors* section has a list of HTML documents used when IIS encounters an error. Six (6) 401 errors are listed. For each 401 error, click *Edit*. Ensure *Message type* is *File*, and then click *Browse* to locate the 401.html that is provided in the MTWeb components. This file is generally located in the following location:
C:\Program Files\Group Logic\MassTransit Server 5\MTWeb\webroot\401.html or
C:\Program Files\Group Logic\MassTransit Server 6\MTWeb\webroot\401.html
Apply this new file to all 401 errors.
7. Click *OK* to continue.
8. Next, right-click on the *sso.php* file in the *MTWeb* root inside *Internet Information Services (IIS) Manager*. Click *Properties*.
9. Click the *File Security* tab. In the *Authentication and access control* section, click the *Edit* button.
10. In the *Authentication Methods* dialog that appears, ensure *Enable anonymous access* is not checked and ensure *Integrated Windows authentication*, under *Authenticated access*, is checked.
11. Click *OK*, then click *OK* again.
12. Next, open the PHP configuration file, *php.ini*, located in the Windows installation folder, generally *C:\Windows*.
13. Find the option *session.save_path* and set this to "*C:\php\sessiondata*" (including the quotation marks). If this option is commented out (preceded by a semicolon ';') remove the comment to make it active. Save the file, and close your text editor.
14. The *sessiondata* folder in the previous step may not already exist inside *C:\php*. If this folder does not exist it must be created. Navigate to *C:\php* and right-click, select *New*, then select *Folder*. Name the folder *sessiondata*.
15. Right-click on the *sessiondata* folder and click *Properties*. Click the *Security* tab.
16. Add privileges for the *Internet Guest Account* and the local *Users* group by clicking the *Add* button. Click *Object Types*, and select *Users* and *Groups*. Click *OK*. Click *Locations*, and select the computer in the *Locations* window that appears. Click

OK. In the *Select Users or Groups* window, click *Advanced*. Click the *Find Now* button. Select both the Internet Guest Account (IUSR_MACHINENAME) and the local *Users* group by clicking the first, holding down the CTRL key, and clicking the second. Click OK, then click OK. Inside the *sessiondata Properties* window, click the *Internet Guest Account* user, and, under *Permissions for...*, allow *Full Control*. Next click the *Advanced* button. In the “Advanced Security Settings for sessiondata” window check the box next to “Replace permission entries on all child objects with entries shown here that apply to child objects.” In the Security dialog that appears next click Yes. Repeat for the *Users* group. Click OK.



17. Navigate to the folder where MTWeb is located. This is generally *C:\Program Files\Group Logic\MassTransit Server 5*. Right-click on *MTWeb*, then click *Properties*. Similar to the previous step, allow *Read & Execute* permissions for the *Internet Guest Account* and the local *Users* group. Do not set advanced permissions for the child objects.
18. Inside the *MTWeb* folder set the permissions for the *parsed* and *templates_c* folders. If these folders are not empty, delete their contents prior to completing this step. Apply *Full Control* permissions for the *Internet Guest Account* and the local *Users* group on the *parsed* and *templates_c* folders. Also set the advanced permissions for child objects for the *parsed* and *templates_c* folders, see Step 16.
19. Restart IIS by right-clicking on the machine name in the left-hand pane of the IIS Manager, selecting *All Tasks* and choosing *Restart IIS...* In the *Stop/Start/Restart...* dialog that appears, choose *Restart Internet Services on MachineName*, and click OK. IIS will restart.

Configuration of single sign-on is now complete for your MassTransit MTWeb server.

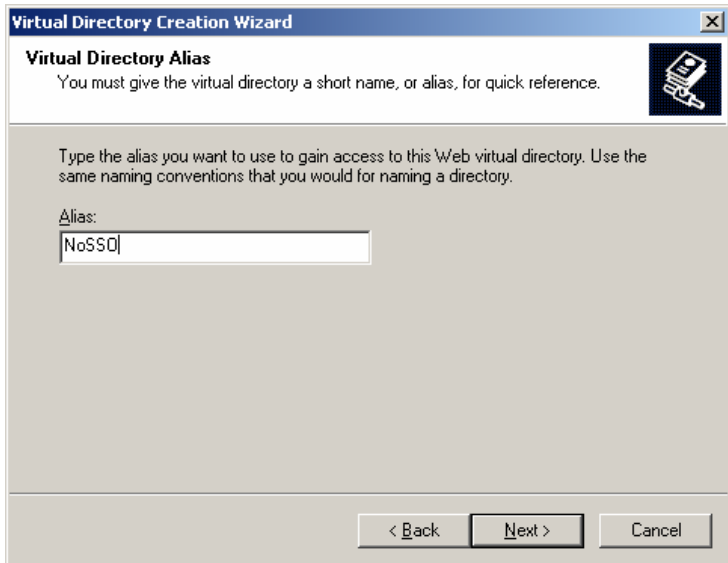
Under certain circumstances it might be necessary to maintain both single sign-on and regular authentication mechanisms for the same MassTransit MTWeb server. If that should be the case, follow the steps below:

1. Configure single sign-on as described above.
2. In the *Internet Information Services (IIS) Manager*, right click on the Web Site hosting the MTWeb interface and select *New ->Virtual Directory...*

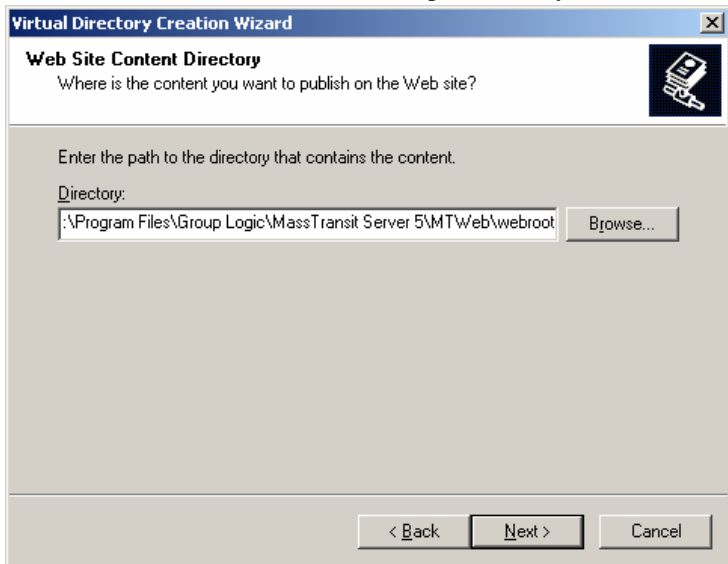
3. The *Virtual Directory Creation Wizard* opens up. Click *Next*.



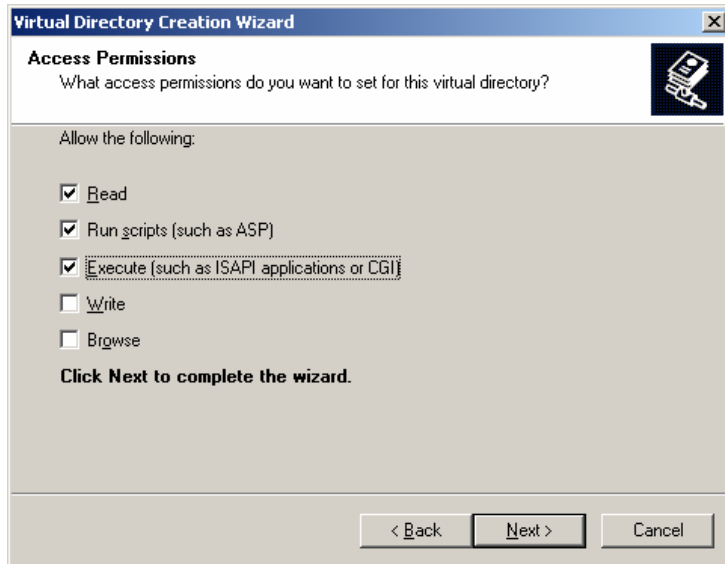
4. Assign an alias to the virtual directory, such as *NoSSO*, and click *Next*.



5. Browse to the same location on disk as pointed to by the web site hosting the MTWeb interface and click *Next*.



6. Make sure *Read*, *Run Scripts (such as ASP)* and *Execute (such as ISAPI applications or CGI)* checkboxes are checked and click *Next*.

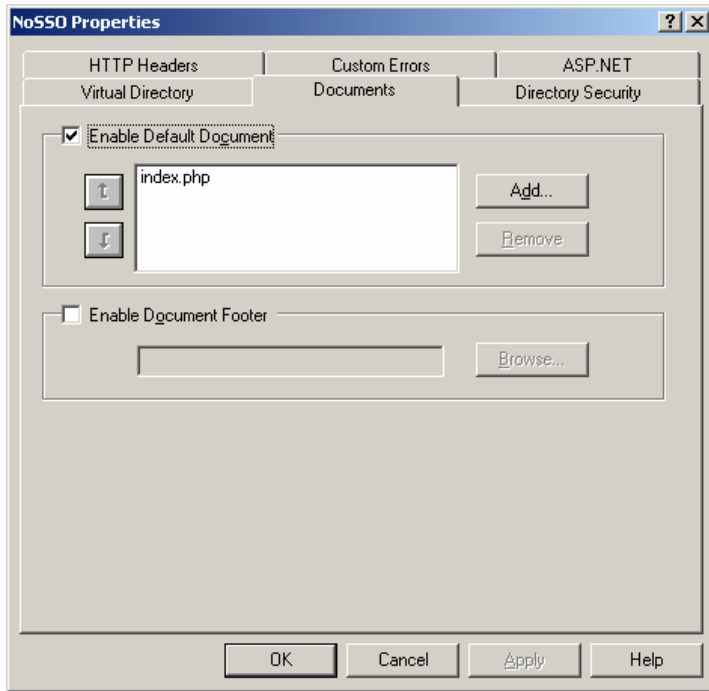


7. Click *Finish*.



8. In the *Internet Information Services (IIS) Manager*, right click on the newly created virtual directory, select *Properties* and in the resulting dialog, click the *Documents* tab. Ensure *Enable default content page* is selected.
9. Click *Add*, and in the *Add Content Page* dialog, type *index.php*. Click *OK*.

10. Move *sso.php* to the top of the list by clicking the *Move Up* button. Ensure *index.php* is listed above *sso.php*, if it exists.



Configuration of the regular authentication entry point to the MTWeb web site is done now. Users not wishing or not being able to use the single sign-on mechanism will be able to navigate to the MassTransit authentication page directly by appending the web site's URL in their browser with */NoSSO*.

CONFIGURING INTERNET BROWSERS

Due to security considerations, modern web browsers will not automatically provide authentication information to web sites unless they are part of your local intranet or explicitly defined within the browser's configuration parameters. This ensures that authentication information isn't sent to a malicious web site inadvertently, which could compromise organizational security.

These next sections will assist you in configuring various browsers to use the single sign-on feature with your SSO-enabled MassTransit Enterprise MTWeb instance.

BEFORE YOU BEGIN

The client machine must be bound to Active Directory in order for this feature to function properly. The current logged-in user must have a valid Active Directory account, and this account must be associated with a contact within MassTransit. For Mac OS X, Kerberos must be properly configured and a valid ticket granting ticket (TGT) must be active for the logged-in user.

If the client machine is not presently bound, or, is accessing from a remote location where authentication to the Active Directory infrastructure is not possible, or, if the connecting user has a valid MassTransit account that is not associated with Active Directory, MTWeb users will be presented with a NTLM authentication dialog on Microsoft Windows and Mac OS X. Users in these circumstances can “fall back” to the legacy MTWeb login page by dismissing the dialog by clicking the Cancel button, or pressing Escape. Due to the way these NTLM authentication dialogs work they will not accept login names for MassTransit contacts that are not associated with Active Directory. Instead you must use the “fall back” feature and login from the legacy MTWeb login page.



NTLM Dialog for Microsoft Internet Explorer



NTLM Dialog for Firefox (similar on Mac OS X and in Apple Safari)

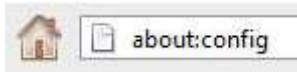
Apple Safari on Mac OS X does not directly support this ability to “fall back” and therefore, in order to use the standard MTWeb login page, the user must append *index.php* to the MTWeb address, which then bypasses the single sign-on component.

For example, if you are connecting to *http://masstransit.company.com*, the user should append *index.php* to this address, and then click Go or press Enter in their web browser to connect to *http://masstransit.company.com/index.php*.

MOZILLA FIREFOX

Firefox allows you to define “trusted” sites using hostnames, IP addresses or combinations - including wildcards - that authentication data should be automatically passed to. These steps apply for Firefox versions 1.0 through 2.0 running on both Microsoft Windows and Mac OS X.

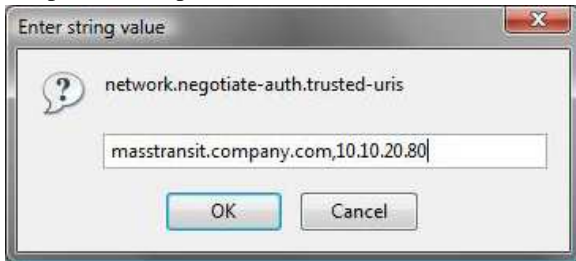
1. Launch Firefox.
2. In the Address Bar, enter *about:config* and then press Enter. A very long list of configuration parameters for Firefox will be displayed.



- Using the *Filter* textbox, type *network.negotiation*. 5 options will be returned.



- Double-click on *network.negotiate-auth.trusted-uris*.
- In the resulting dialog, enter the hostname or IP address of the SSO-enabled MTWeb host. Acceptable inputs are as follows:
 - IP address (i.e. 10.10.20.80)
 - Hostname (i.e. masstransit.company.com)
 - Wildcards (i.e. *.company.com or 10.10.20.*)
 - Separate multiple entries with a comma (i.e. masstransit1.company.com,10.10.20.*)



- Once entered, click OK.
- Restart Firefox.

Single sign-on configuration for Firefox is now complete. You may test the functionality by visiting your MTWeb installation when bound to Active Directory and authenticated as a user associated with a MassTransit contact. If working properly, Firefox will not prompt you to login. Instead, you will be automatically navigated to the MassTransit File Transfer page. Your Active Directory login, in the form of `DOMAIN\USERNAME`, will appear in the upper-left-hand corner of the MTWeb interface.

MICROSOFT INTERNET EXPLORER

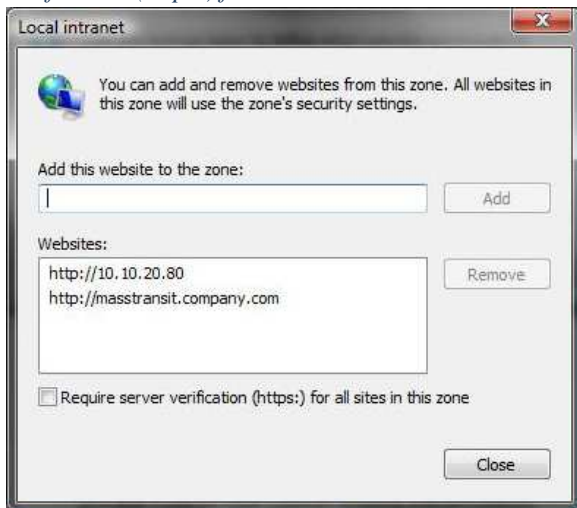
Internet Explorer, by default, will automatically provide authentication credentials to sites defined as being part of the Local Intranet. Internet Explorer contains logic that automatically attempts to identify sites on the intranet network. However, due to network layouts and other factors, this may not always work reliably. Therefore, we need to instruct Internet Explorer to consider your MTWeb installation as part of the Local Intranet zone.

- Launch Internet Explorer.
- From the *Tools* menu, click *Internet Options*.

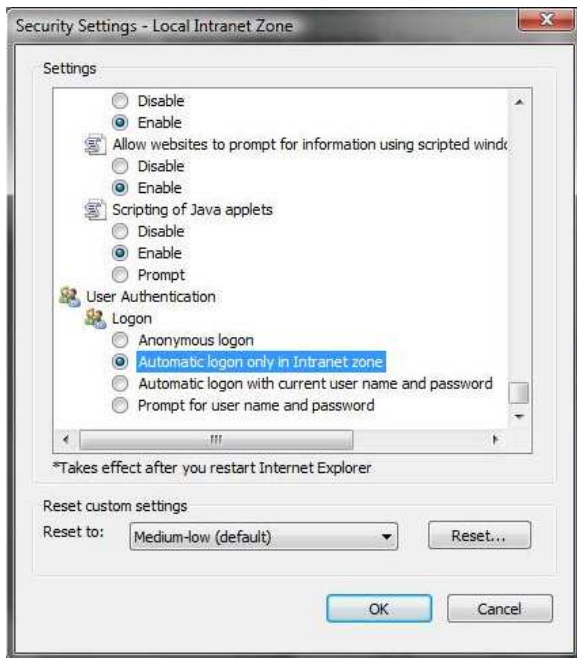
3. Click the *Security* tab. Then, click *Local intranet*.



4. Click the *Sites* button.
5. In the *Local intranet* dialog, click *Advanced*. In the resulting dialog, add the URLs for your SSO-enabled MTWeb installation. You should provide both the DNS hostname and the IP address for the server. Uncheck *Require server verification (https:) for all sites in this zone*.



6. Click Close.
7. Verify that Internet Explorers options have not deviated from the default by clicking *Custom level...* on the *Security* tab.
8. Scroll to the bottom of the *Settings* list. Under *User Authentication – Logon*, ensure that the radio button for *Automatic logon only in Intranet zone* is selected. Optionally, you can reset IE to the zone defaults, which are Medium-low.



9. Click OK. Then click OK in *Internet Options* to apply your changes.
10. Restart Internet Explorer.

Single sign-on configuration for Internet Explorer is now complete. You may test the functionality by visiting your MTWeb installation when bound to Active Directory and authenticated as a user associated with a MassTransit contact. If working properly, Internet Explorer will not prompt you to login. Instead, you will be automatically navigated to the MassTransit File Transfer page. Your Active Directory login, in the form of `USERNAME`, will appear in the upper-left-hand corner of the MTWeb interface.

APPLE SAFARI

Safari supports single sign-on out of the box, and requires no configuration to use this feature. Safari relies on Mac OS X's support for the MIT Kerberos standard for authentication to connect to single sign-on-enabled services. Active Directory uses Kerberos version 5 for authentication by default.

The Mac OS X machine needs to be bound to the Active Directory domain to allow for single sign-on to be used. This feature works with the built-in Active Directory plug-in and optional third party software, such as ADmit Mac from Thursby Software.

When logging in with an Active Directory user account, Mac OS X will be assigned a Kerberos ticket that dictates the services the user is allowed to use. Safari uses this ticket to connect to the SSO-enabled MTWeb server.

You may test the functionality by visiting your MTWeb installation when bound to Active Directory and authenticated as a user associated with a MassTransit contact. If working properly, Safari will not prompt you to login. Instead, you will be automatically navigated to the MassTransit File Transfer page. Your Active Directory login, in the form of `DOMAIN\USERNAME`, will appear in the upper-left-hand corner of the MTWeb interface.

ADDITIONAL INFORMATION

OTHER BROWSERS

Other browsers may work, but have not been tested and may not provide the higher levels of security when using SSO. It is recommended that you use the browsers mentioned in this document when accessing your SSO-enabled MTWeb instance.

Copyright © 2008, Group Logic, Inc. All Rights Reserved.