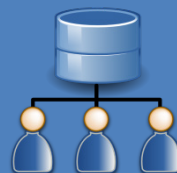




Active Directory Integration Documentation

<http://mid.as/ldap>
v1.00



...making your facilities work for you!

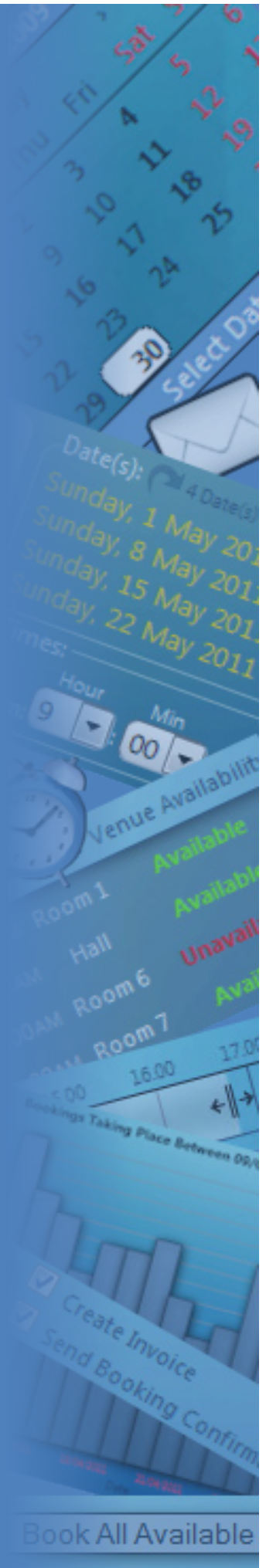




Table of Contents

Table of Contents	1
Overview	2
Pre-Requisites	2
MIDAS.....	2
Server	2
End Users	3
Configuration	3
Configuring Apache.....	3
Configuring IIS.....	4
Configuring IIS 6.0	4
Configuring IIS 7.x	5
Configuring Web Browsers	8
Configuring Microsoft Internet Explorer.....	8
Configuring Mozilla Firefox.....	9
Configuring Google Chrome.....	9
Configuring MIDAS.....	10
Managing Permissions	12
Troubleshooting.....	13
Frequently Asked Questions	15



Active Directory Integration

Overview

The Lightweight Directory Access Protocol (or LDAP) is a method of accessing an Active Directory (AD) over an IP network. It's commonly used to authenticate users on a corporate network when they login to their computer/workstation.

MIDAS (v4.06 or later) offers seamless Single Sign-On (SSO) support through LDAP integration with your Active Directory. This allows users to be automatically logged on whenever they open MIDAS.

The basic process is as follows...


Stage 1	Stage 2	Stage 3	Stage 4	Stage 5
User opens their browser and navigates to MIDAS	The browser sends the logged in user's username to MIDAS	MIDAS queries your AD to retrieve the user's real name, email address and Primary Group	User is added (or update) in MIDAS using permissions from the User Group having a corresponding name as the user's Primary Group in the AD	User is seamlessly logged into MIDAS


Pre-Requisites

In order to be able to use the LDAP integration offered by MIDAS, the following pre-requisites must first be met:

MIDAS

Your must be running MIDAS v4.06 (or later) on your own server (self-hosted), and your MIDAS must be licenced for "Unlimited" users.

 **Tip:** If you need to upgrade your self-hosted MIDAS licence to "Unlimited" users you can do so at <https://mid.as/upgrade>

 **IMPORTANT:** If your MIDAS is "remotely hosted" by us and/or your MIDAS isn't licensed for "Unlimited" users, Active Directory integration is not available

Server

It is assumed that you already have an Active Directory setup and running within your infrastructure. Setting up of an Active Directory itself is beyond the scope of this documentation.

It is also assumed that you're running either an Apache or an IIS web server.

Apache

The module "**mod_auth_sspi.so**" is required on the server where your MIDAS resides. See [Configuring Apache](#)


IIS

Windows authentication needs to be enabled on the server where your MIDAS resides. See [Configuring IIS](#)



Perl

The Perl module **Net::LDAP** is required on the server where your MIDAS resides. This module provides LDAP support to Perl (the language MIDAS is written in) and may be freely obtained via [CPAN](#).

 **Tip:** If you're using ActiveState Perl, this module may be installed via the Perl Package Manager, where it is listed as "perl-ldap"

End Users

End users must be logged on to their computer/workstation through your Active Directory. If they logged onto their device "locally", they may not be able to seamlessly authenticate against your Active Directory when using MIDAS, and may instead be prompted for their system credentials.

User's browsers must also be capable of determining the username of the logged in user. See [Configuring Browsers](#)

Configuration

Configuring Apache

In order for Apache to authenticate against an Active Directory server, the module "mod_auth_sspi.so" must be present and enabled.


Once installed, this module can be enabled by adding the following line to your server's httpd.conf file:

```
LoadModule sspi_auth_module modules/mod_auth_sspi.so
```

Next, you will need to configure the directory on your server where your MIDAS resides to authenticate against your Active Directory. Again, this is done by adding the following to your httpd.conf file:

```
<Location "/midas/">
  AuthName "Intranet"
  AuthType SSPI
  SSPIDomain xxx.xxx.xxx.xxx
  SSPIAuth on
  SSPIOfferSSPI on
  SSPIAuthoritative on
  SSPIUsernameCase lower
  SSPIPerRequestAuth on
  SSPIOmitDomain on
  require valid-user
</Location>
```

Where "/midas/" is the location where MIDAS resides on your server, relative to the root (usually "public_html"). And xxx.xxx.xxx.xxx is the IP address or domain name of your Active Directory server. In the above example, MIDAS resides under /public_html/midas/, and therefore the location to use is "/midas/"

 **Tip:** You will need to restart Apache for changes you make to your httpd.conf file to take affect

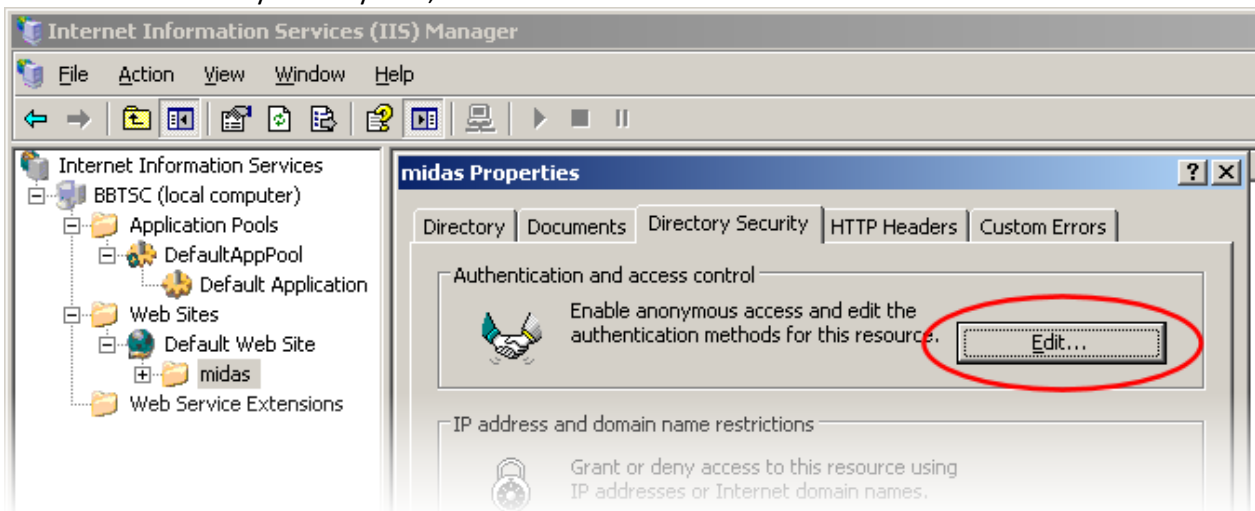


Configuring IIS

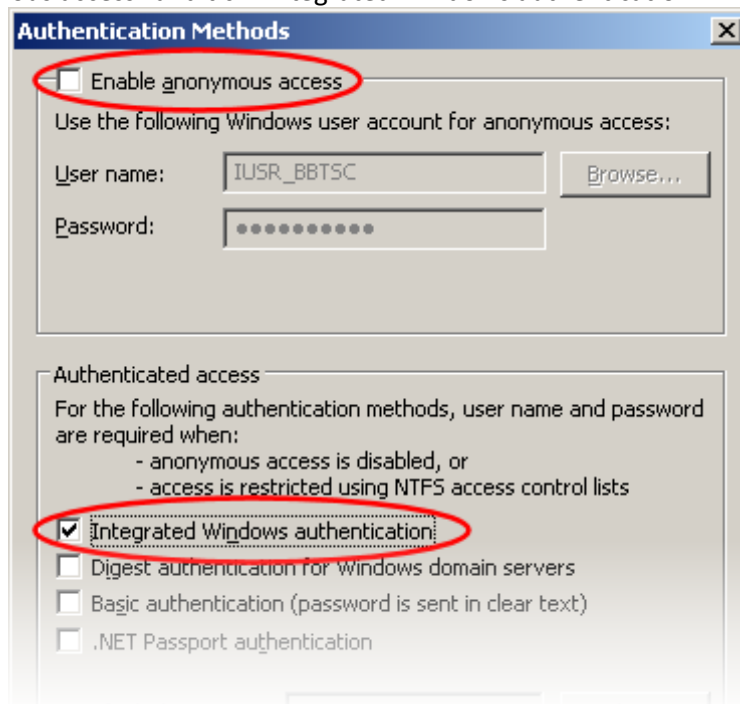
In order for IIS to authenticate against an Active Directory, you must disable anonymous access and enable Integrated Windows authentication for the server (or specific directory) where your MIDAS resides.

Configuring IIS 6.0

1. Open Administrative Tools → Internet Information Services (IIS) Manager.
2. Right-click on the site/directory where your MIDAS resides and select "Properties".
3. Switch to the "Directory Security" tab, and click the Authentication and access control "Edit" button:



4. Untick "Enable anonymous access" and tick "Integrated Windows authentication":



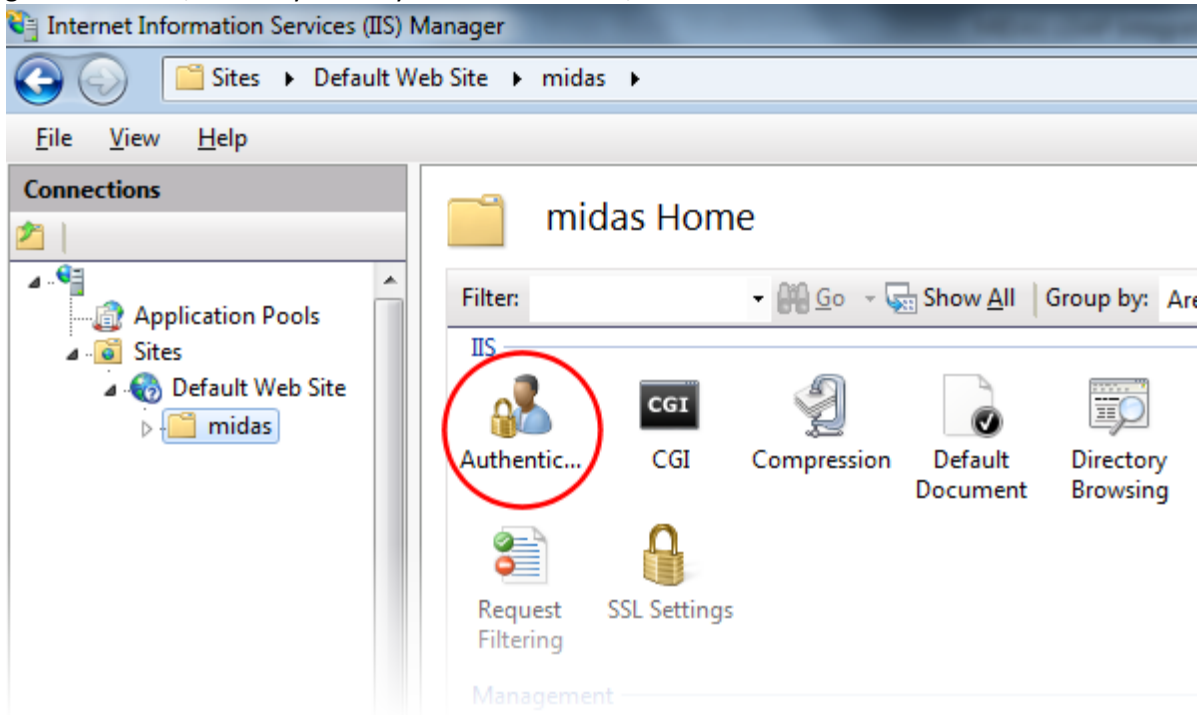
5. Click "OK" then "OK" again to return to the IIS manager.



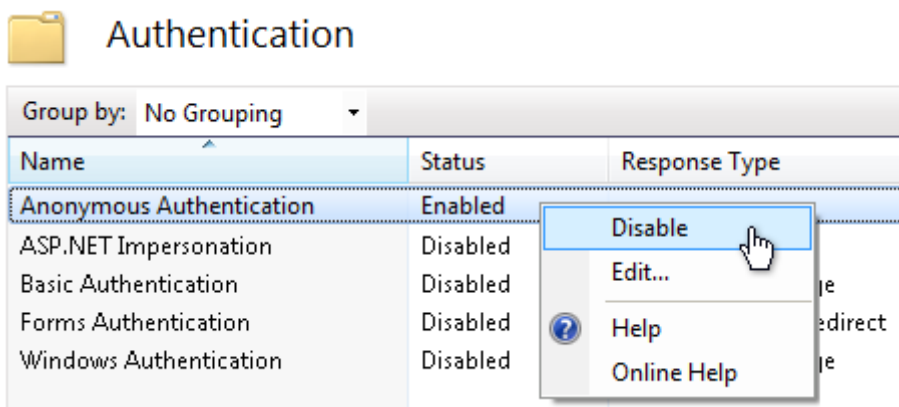
Configuring IIS 7.x

The default installation of IIS 7.x does not include the Windows authentication role service. To use this authentication on IIS 7.x, you must install the role service, disable Anonymous authentication for the server or directory where your MIDAS resides, and finally enable Windows authentication for the directory/site.

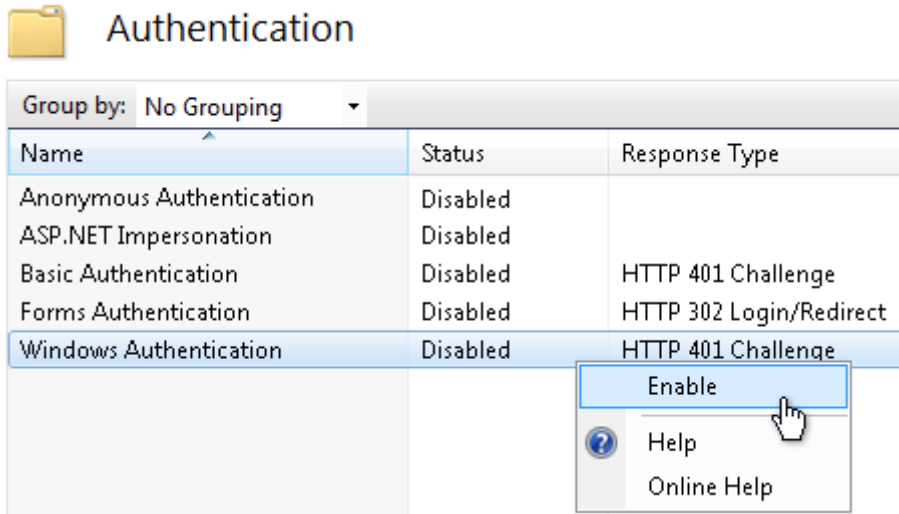
1. Open the Internet Information Services (IIS) Manager.
2. Navigate to the site/directory where your MIDAS resides, and click "Authentication":



3. Right-Click the "Anonymous Authentication" entry and select "Disable":

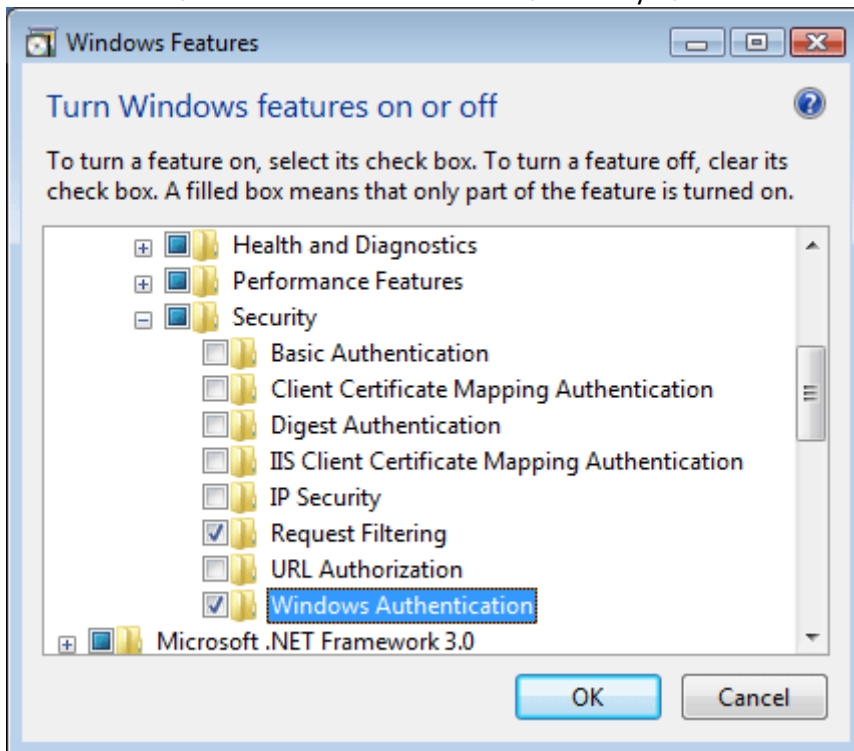


4. Right-Click the "Windows Authentication" entry and select "Enable":



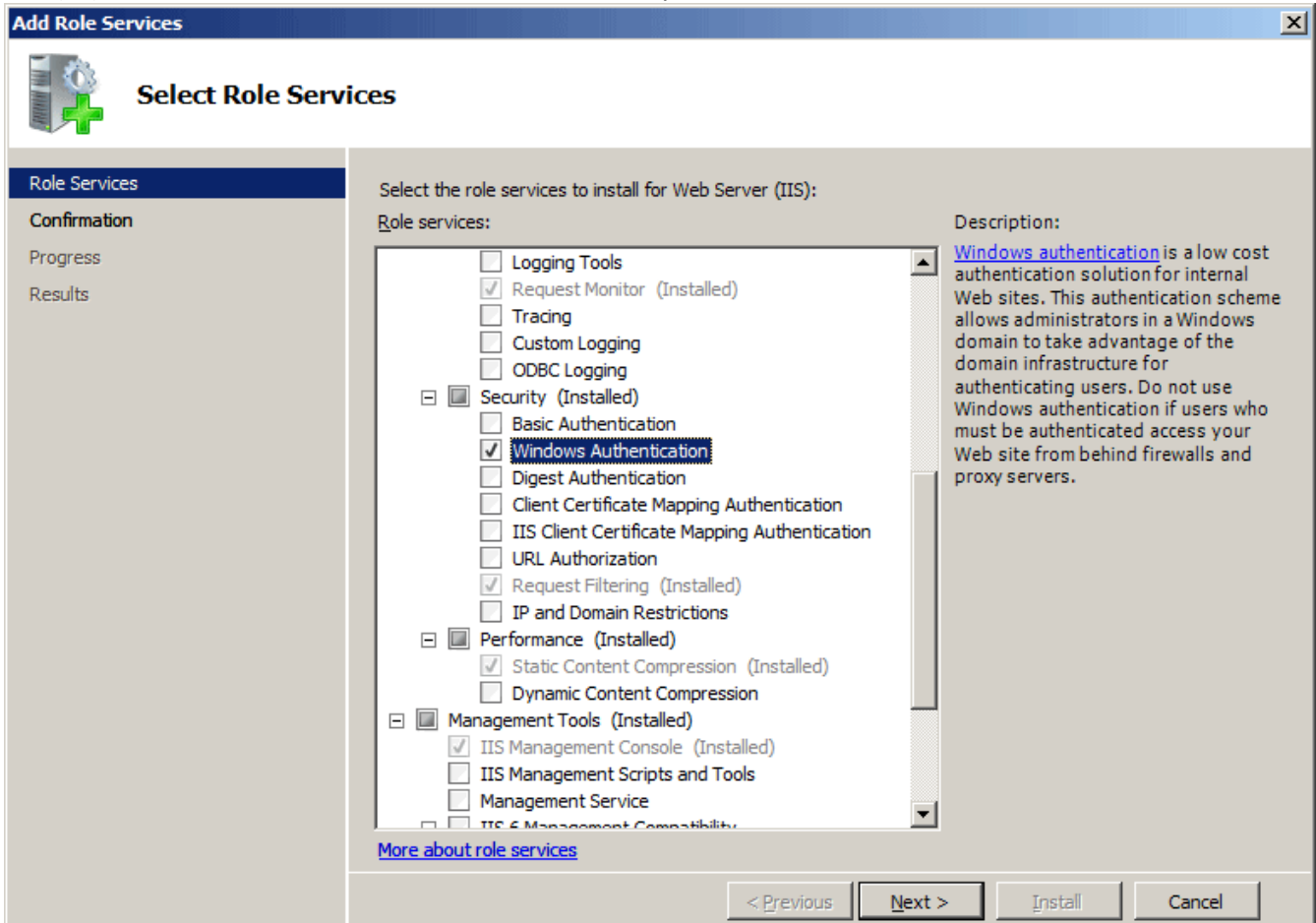
If the "Windows Authentication" option isn't present, you will first need to install the Windows authentication role services.

On Windows Vista/7, this can be done via Control Panel → Programs and Features → Turn Windows features on or off → Internet Information Services → World Wide Web Services → Security → Windows Authentication:





On Windows Server 2008/2008 R2, this can be done via Administrative Tools → Server Manager → Roles → Web Server (IIS) → Role Services → Add Role Services → Security → Windows Authentication:



For more information on enabling Windows Authentication under IIS, please refer to:

<http://www.iis.net/configreference/system.webserver/security/authentication/windowsauthentication>



Configuring Web Browsers

By default web browsers do not supply a user's system credentials to a web server. In order to use MIDAS with Active Directory integration, a modification to your users' browser security settings is required in order to confirm that it is safe to exchange their currently logged in credentials with MIDAS upon request.

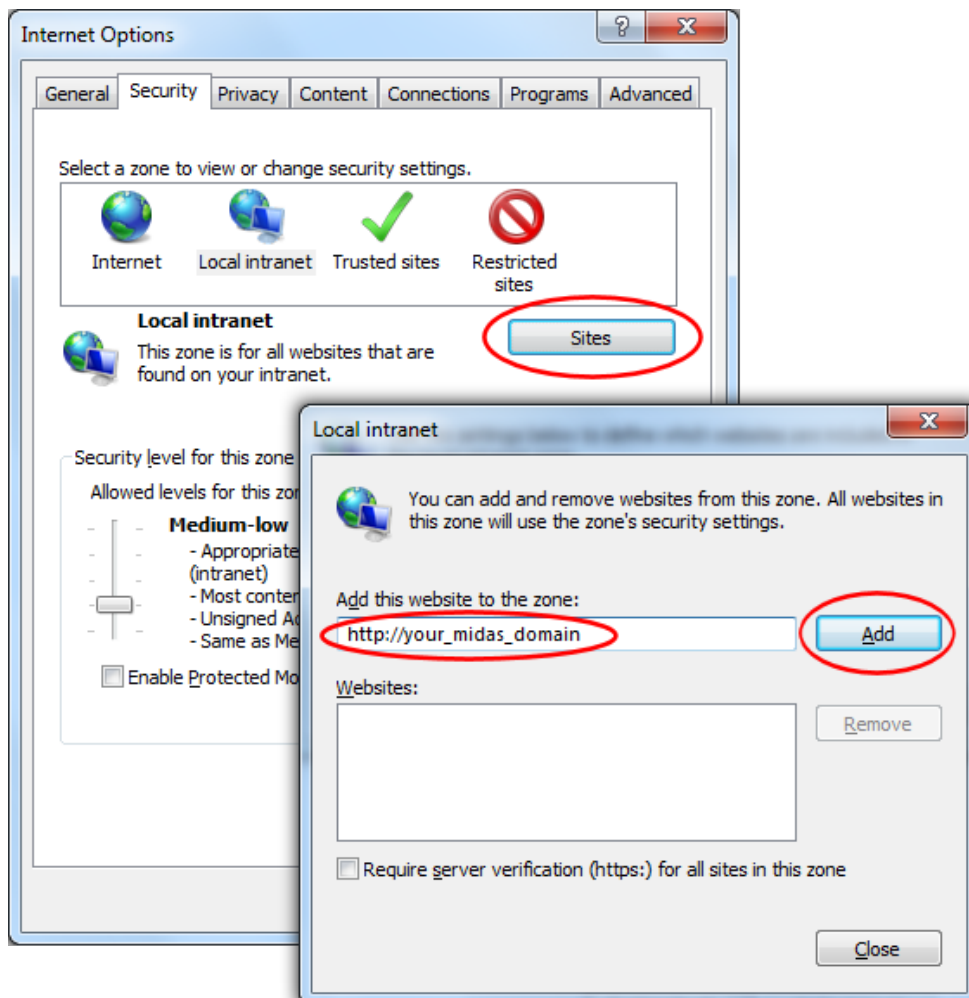
The settings outlined in this section will need to be applied to all user PC's/workstations within your domain. In the case of Internet Explorer, this modification could be pushed out via Group Policy.

Note: At time of writing, Opera and Safari browsers do not natively support seamless integration

Warning: If you do not apply these settings to user's PC, users will not be seamlessly logged into MIDAS. Instead, they may be prompted to enter their AD username and password logon each time they access MIDAS

Configuring Microsoft Internet Explorer

In order for Internet Explorer to supply credentials to a site, the site (domain where your MIDAS resides) must be added to IE's "Local Intranet" sites. (Internet Options → Security → Local Intranet → Sites)

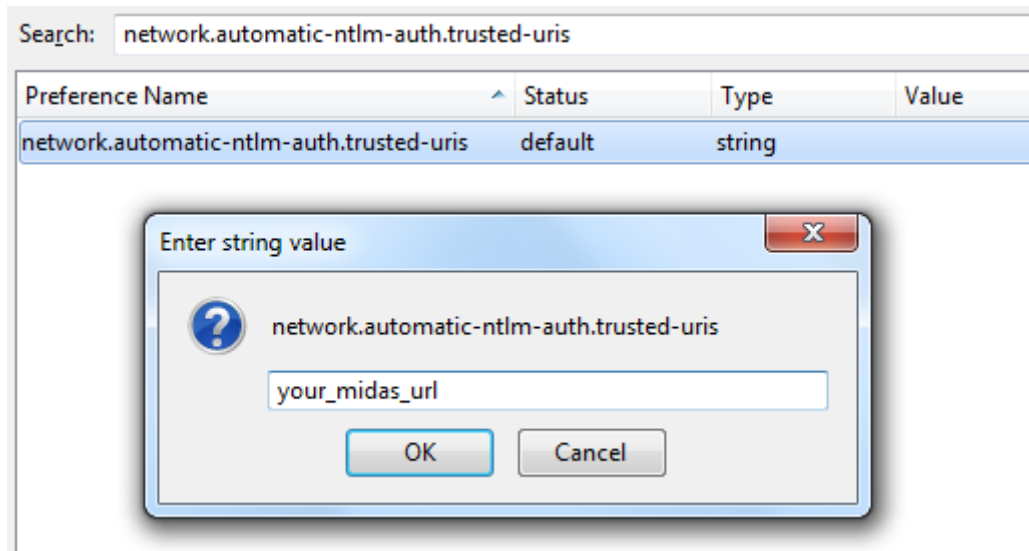




Configuring Mozilla Firefox

To configure Firefox, you will need to add the domain where your MIDAS resides as a "trusted" site for automatic authentication.

To do this, open Firefox and enter "**about:config**" in the address bar. Then locate the "**network.automatic-ntlm-auth.trusted-uris**" setting and add your MIDAS URL to this setting's current value:



i Depending upon your network environment, you may also need to add your MIDAS domain/url to the `network.negotiate-auth.delegation-uris` setting as well

Configuring Google Chrome

Chrome inherits it's from Internet Explorer's Local Intranet Zone. Therefore, please follow the steps outlined in [Configuring Microsoft Internet Explorer](#).

Alternatively, a list of authorized servers may be passed in to Chrome using a comma-separated list of URLs via the "auth-server-whitelist" command-line switch. For example, starting Chrome with the command-line switch:

```
--auth-server-whitelist="*yourdomain.com"
```

...will "white list" "yourdomain.com", allowing for seamless AD integration without prompting the user for additional credentials.

For more information, please see:

<http://dev.chromium.org/developers/design-documents/http-authentication>



Configuring MIDAS

LDAP Integration is configured via MIDAS Admin Options → Manage Users & Permissions → Single Sign On (SSO).

Setting	Description
Enable LDAP Authentication	Enables/Disables LDAP Authentication of users.
Host	The IP/domain of your Active Directory server. This is the server against which users are authenticated within your infrastructure
Bind To	The Distinguished Name binding MIDAS should use to query your Active Directory. Example: CN=Administrator,CN=Users,DC=mydomain,DC=local
Bind Password	The password required by your AD server to bind to the above
Base	The base at which user information may be found in your Active Directory Example: DC=mydomain,DC=local
Update User Permissions upon each login	If selected, the user's MIDAS permissions will be updated with the latest permissions assigned to their "group" each time they access MIDAS. See Managing Permissions
If no matching User Group exists, block access	If the user's Primary Group in the AD does not correspond to a matching user group name in MIDAS, this setting determines what should happen. If selected, SSO access to MIDAS will be denied and the user will see the standard login screen. If unselected, the user will be logged in with a very restrictive set of user permissions (essentially "view only")
Debug	With debugging enabled, failed and successful LDAP authentications will be logged to a "/debug-ldap.dat" file in your MIDAS directory.

Warning: It is recommended to only enable Debug logging whilst troubleshooting integration with your AD. Once up and running, it's strongly advised to disable this logging, otherwise the log file can become very large!

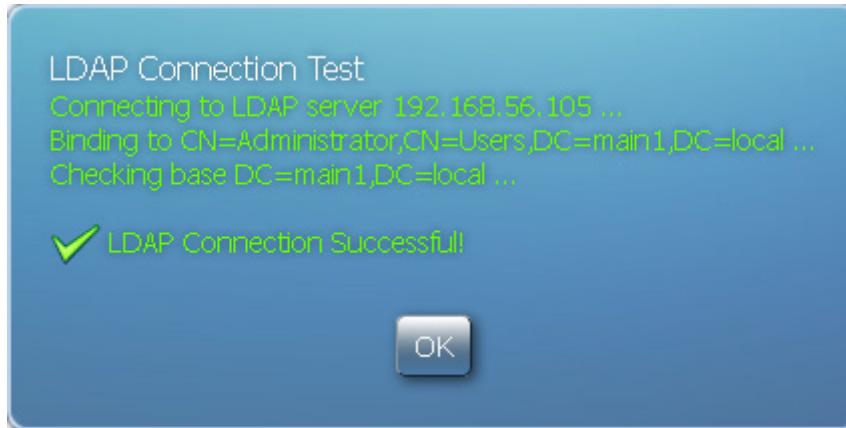
Clicking the "Save Changes" button will apply your settings.



MIDAS

Active Directory Integration

Clicking the "Test" button will perform a basic connection test to your Active Directory server using the details you've entered, and will display the results:



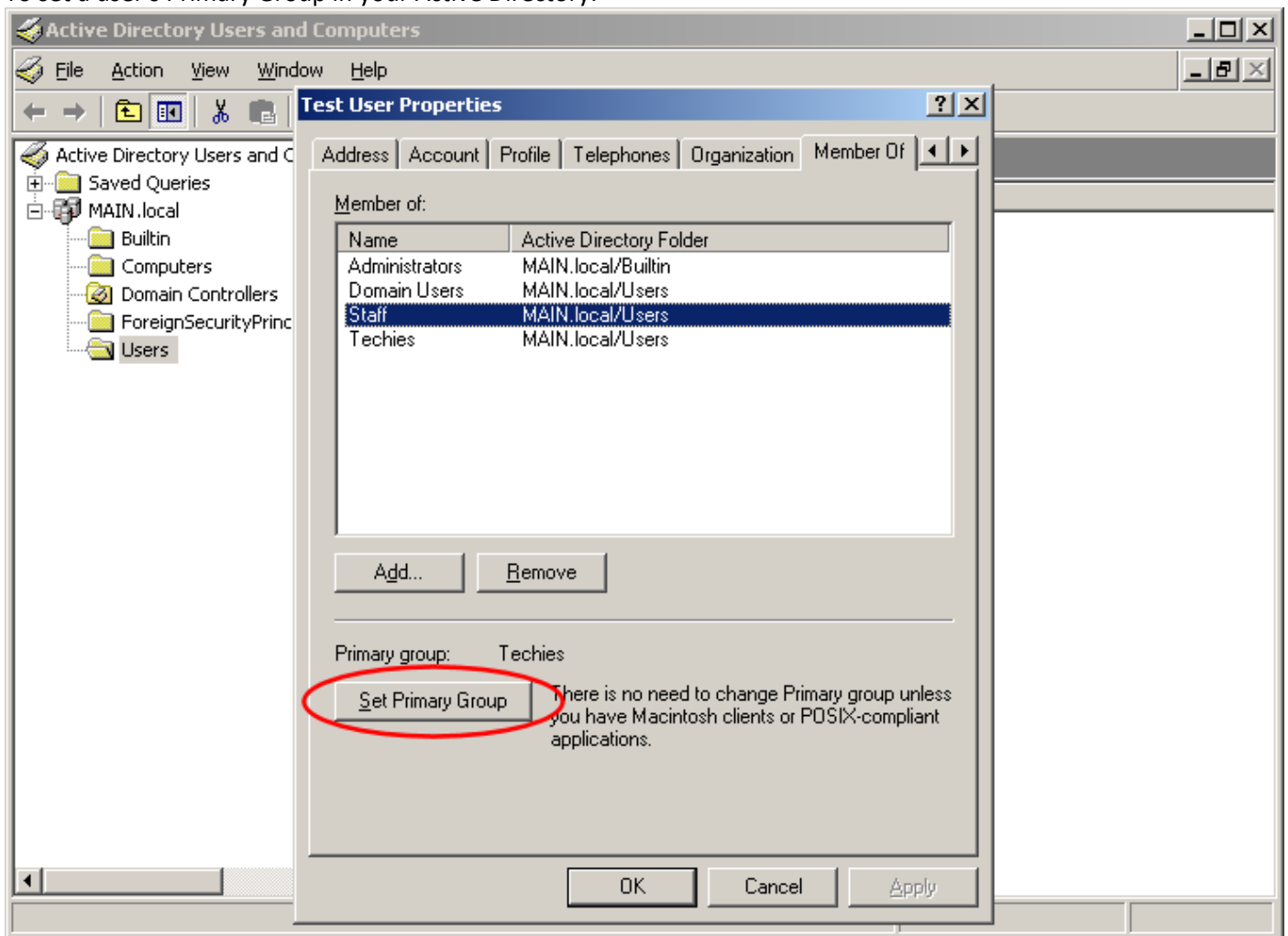
In addition, when you perform an LDAP Connection Test, MIDAS will attempt to retrieve a list of User Groups from your Active Directory, and add these names to the User Group list in MIDAS.



Managing Permissions

The user permissions assigned to each MIDAS user who authenticates against your Active Directory are derived from the name of Primary Group the user is a member of within your Active Directory, and the permissions associated with the corresponding MIDAS User Group with the same name.

To set a user's Primary Group in your Active Directory:



In the above example, the user's Primary Group in the Active Directory is "Staff".

This user's MIDAS permissions will therefore be derived from the permissions you've specified for a User Group within MIDAS with the same name (i.e. "Staff") (You can setup MIDAS user groups via MIDAS Admin Options → Manage Users & Permissions → Groups)

If the "Update User Permissions upon each login" option is enabled (MIDAS Admin Options → Manage Users & Permissions → Single Sign On (SSO)) then each time the user opens MIDAS, their MIDAS user permissions will be updated to reflect the current permissions associated with their User Group.

If the "Update User Permissions upon each login" option is not selected, the user's MIDAS permissions will be set based upon the group permissions at the time of their first access of MIDAS via Active Directory authentication.



Once set, these permissions will not be automatically updated again (i.e. subsequent changes to the user group's permissions within MIDAS will not be applied to existing users who have previously authenticated with MIDAS via Active Directory integration).

Leaving this option unselected can be useful if you wish to "tweak" specific individual user's permissions.

➔ Please refer to the main MIDAS documentation for details of the available User Permissions

Troubleshooting

If you encounter an issue configuring MIDAS to authenticate against your Active Directory, a good place to start is the "Test" button on the MIDAS Admin Options → Manage Users & Permissions → Single Sign-On (SSO). This button will test whether MIDAS is able to connect to and query the Active Directory using the settings you've specified.

If this test fails, these settings are the first thing to check.

You can also enable debug logging by selecting the "Debug" option and clicking "Save Changes". With debugging enabled, failed and successful LDAP authentications will be logged to a "/debug-ldap.dat" file in your MIDAS directory.

Warning: It is recommended to only enable Debug logging whilst troubleshooting integration with your AD. Once up and running, it's strongly advised to disable this logging, otherwise the log file can become very large!

Common issues, their causes and resolutions are outlined in the table below...



Active Directory Integration

Symptom	Possible Cause(s)	Resolution
After configuring and enabling LDAP integration, when I access MIDAS, I still see a login screen	If MIDAS is unable to successfully connect to and query your Active Directory, it will fall back to the standard login screen.	Go to MIDAS Admin Options → Manage Users & Permissions → Single Sign-On (SSO) and check your Active Directory settings are correct using the "Test" button
	If there is no email address in your Active Directory for your username, the user will see the standard MIDAS login screen.	If you've enabled debug logging, this cause will be indicated in the debug log. An email address should be entered in your Active Directory for each user who will be accessing MIDAS.
	If there is no User Group in MIDAS with a name matching the name of the user's Primary Group setting in your Active Directory, and the "If no matching User Group exists, block access" option in MIDAS is selected, the user will see the standard MIDAS login screen.	If you've enabled debug logging, this cause will be indicated in the debug log. <ol style="list-style-type: none">1. Ensure that a User Group has been created in MIDAS (MIDAS Admin Options → Manage Users & Permissions → Groups) with the same name as the user's Primary Group from your Active Directory. or... <ol style="list-style-type: none">2. Untick the "If no matching User Group exists, block access" option (MIDAS Admin Options → Manage Users & Permissions → Single Sign-On (SSO)). The user will then be able to access MIDAS using a very limited set of "view only" permissions.
	If a user's MIDAS user account has been "suspended" in MIDAS, they will be returned to the login screen rather than seamlessly logged in.	If you've enabled debug logging, this cause will be indicated in the debug log. Go to MIDAS Admin Options → Manage Users & Permissions → Users and check that the user account in question hasn't been suspended.
A dialog prompting for credentials is shown when accessing MIDAS	Your browser has not been configured to present the username of the currently logged in user to the server where your MIDAS resides.	See Configuring Web Browsers



Frequently Asked Questions

Why is LDAP integration only available for "self hosted" editions of MIDAS?

In order for a web server to support LDAP integration, the server has to be specifically configured to do so. With our "remotely hosted" edition of MIDAS, we do not permit or provide you with access to change/reconfigure the web server in order to support your LDAP server.

Why must my MIDAS be licensed for "Unlimited" users in order to use LDAP integration?

If your MIDAS is licensed to a finite number of users, then LDAP integration would potentially exclude some of your Active Directory users from accessing access MIDAS - defeating the point of the seamless "single sign-on" ability offered by LDAP integration. For example, if your MIDAS is only licensed for 10 users, then whichever 10 users from your Active Directory login to MIDAS first, they would then be the only 10 users who could continue to access MIDAS in the future - all others would be rejected.

Therefore, to avoid this, we have restricted LDAP integration to self-hosted customers with an "Unlimited" user MIDAS license.

Generally speaking, organizations that utilize an Active Directory tend to have dozens, if not hundreds, of users so would likely have or require an "Unlimited" user license for MIDAS anyhow.

Does MIDAS "write" anything back to or update my Active Directory?

No. MIDAS only reads data from your Active Directory. It won't write anything back or make any changes to your Active Directory.

I can't change user's Primary Groups in my Active Directory, yet I need to assign different users different permissions!

By default, MIDAS will assign permissions based upon each user's Primary Group which corresponds to a user group in MIDAS with the same name. If you are unable to change a user Primary Group in your Active Directory to allow them to inherit different permissions within MIDAS, there is a solution!

1. Export a list of users from your AD (including full names and email addresses)
2. Open this exported data in a spreadsheet and add an additional "User Group" column
3. Populate this new user group column with the names of existing User Groups you've previously defined in MIDAS
4. Save your modified spreadsheet as a .CSV file
5. Import this file (MIDAS Admin Options ? Manage MIDAS → Database → Database Tools → Import Data), ensuring you assign the correct fields to the correct columns

This will setup user accounts in MIDAS for all your current AD users, and assign each account the permissions from the relevant existing MIDAS User Group.

Finally, untick the "Update User Permissions upon each authentication" option (MIDAS Admin Options → Manage Users & Permissions → Single Sign-On) Then once you've setup & enabled LDAP authentication, users will be able to seamlessly authenticate and will have the appropriate user permissions.

 The most up-to-date version of this documentation may be found online at <http://mid.as/ldap>