

MC Login Hub Installation Guide

About

The Maintenance Connection Login Hub is used to setup the links and mapping information from a LDAP source such as Active Directory to the Maintenance Connection user list and access group settings. Once the configuration has been completed, a Login Hub service can be installed which will, on a scheduled basis, setup new users for MC access and update existing users with the appropriate access rights.

Contents


About.....	1
Supported Configurations.....	5
Futures:	5
7.x Release notes: (development started).....	5
7.1 Release notes: (version 7.1 is coming soon).....	5
7.0 Release notes:	6
Upgrading From Previous Versions of LDAP	6
Upgrading to Login Hub v7.0 From Versions older than 7.0.....	6
Configuration	6
Pre-Installation.....	7
Maintenance Connection.....	7
Active Directory only: Test Windows Authentication environment.....	7
Additional Pre-installation steps.....	7
Installation Process	7
Summary Installation Process.....	7
Configuring for Novell LDAP Only	8
Starting the Service	9
Configuration Wizards in Detail	9
Launching the Configuration Application	9
Areas that can be Configured	10
Configuring the Connection to Maintenance Connection.....	10



Welcome Screen	10
mc.ini Path	10
Update Registration Database	11
Select License	11
Number of LDAP Connections (optional screen)	11
Map Licenses to Entity Databases	11
Update Entity Database	12
Success Page	12
Configuring the LDAP Directory Type to Connect To	12
Configuring Special Service Options and Sync Timings	12
Welcome Screen	13
Service Timing	13
Service User Account	13
Service Configuration	13
Advanced Capture (optional page)	14
Error Reporting	15
Success Page	16
Configuring Each LDAP Connection	16
Configuring the LDAP Directory Connection	16
Welcome Screen	16
Active Directory Connection (AD Only)	16
Novell Directory Connection (Novell Only)	17
Test Directory Connection	17
Success Page	17
Configuring LDAP Field Mapping (Active Directory Only)	17
Welcome Screen	17
Username & E-mail Address	17
Name Fields	18
Contact Numbers	18
Success Page	18
Configuring LDAP Field Mapping (Novell Only)	18
Welcome Screen	18



Username & E-mail Address	18
Name Fields.....	19
Contact Numbers	19
Advanced Fields	19
Success Page	19
Configuring LDAP Group Mapping	19
Welcome Screen	19
Search For LDAP Groups	20
Map LDAP Groups onto Access Groups	20
Access Group Priority.....	20
Access Group Auto Approval	20
Success Page	20
Scripted Field Import Mapping	21
Select Script.....	21
Script Editor.....	21
Success Page	22
Test Tools	22
Sync	22
Display Users To Sync.....	22
Limited Sync.....	23
Appendix: Q&A	24
Assigning Repair Centers to Labor/Requesters	24
Importing unmapped fields into MC from LDAP	24
Appendix: Environment Setup testing and problem shooting	25
Test 1.....	25
Summary:	27
Some other, less likely, causes of getting the password/id prompt.....	27
Test 2.....	28
Summary	28
Test 3.....	28
Summary	29
Test 4.....	29

Summary	30
Appendix: Install .NET 4.5.2	31
Appendix: Create an Application Pool	32
Appendix: Turn on Windows Authentication Feature Delegation	33
Appendix: Installing Automatic Login Pages into Maintenance Connection	34
Appendix: Initial Configuration of Login Hub	35
Initial Setup: Step 1	35
Initial Setup: Step 2	35
Check and update the Registration Database	35
Check and update each Entity database	36
Appendix: Configure Login Providers	37
Adding a New Login Provider	37
Configuring a Login Provider	37
MC Account	37
Active Directory	38
Active Directory  (Active Directory Forced Login prompt)	38
Active Directory: Generic	39



Supported Configurations

The Login Hub Service is a very flexible integration service and can be setup many different ways. While it is impossible to actually test every possible configuration here are some known good configurations. Some of these configurations may require additional licenses to work.

- Active Directory & Server 2003+ → Single MC Database
- Multiple Active Directory Forests/Domains & Server 2003+ → Single MC Database
- Active Directory & Server 2003+ → Multiple MC Databases
- Multiple Active Directory Forests/Domains & Server 2003+ → Multiple MC Databases
- Novell Groupwise → Single MC Database
- Novell Groupwise → Multiple MC Databases

Futures:

7.x Release notes: (development started)

- Facebook and other social providers
- Azure background synchronization
- HTTPS 'forced' switch. Option to 'force' any logins to use MC in an HTTPS.
- Offline appcache the loginhub
- Directly logging into report (emailed smart reports)
- Profile-less service requester
- Other ways to log in that we aren't aware of?
- Shared workstation features
- Multi-lingual

7.1 Release notes: (version 7.1 is coming soon)

- MC Express (Requires full time internet connectivity)
- *MC Express LE (Only requires internet access during initial login and synchronizing. Aka MC Everywhere) login
- If the browser has JavaScript turned off, we gracefully detect this and give detailed browser by browser instructions on how to turn it on (with screen shots)
- Advanced 'Direct URL Builder' – using the login provider and application. These can then be emailed or sent by means like skype.
- *Azure login
- *Windows Account login option (using any accounts on the Server)
- *Create user accounts (a new MC account, a new account based on Social logins etc..)
- *Forgot password functionality (This is of course for MC account logins only!)
- If database update does not have permissions to function in automatic mode, we create the SQL script file to run 'directly' through a tool like SSMS.
 - * Release builder needs to put the exe into the correct location.



- Login works on any size browser screen. Tested on: Safari on Mac, Safari on iPad iOS 9, Safari on iPhone iOS 9, Various Android on Chrome, Windows 10 with Edge, IE 11 and Chrome.
- *Upgrading the service config file automatically (from 5)

7.0 Release notes:

- Works with MC7
- Tools for detecting system setup errors
- Option in setup to 'force' to use a Windows account that can access MS-SQL Server
- Easy use of MC Account logins as an option.
- Forced 'User name and Password' option for Active Directory

Upgrading From Previous Versions of LDAP

There have been many changes to the LDAP integration service over time. Login Hub Version 7 is a major upgrade to LDAP (and the name of the product changed due to the much wider login options, LDAP is just a small portion of the new Login Hub). Due to these changes upgrading can be different depending upon which version is currently installed. Please ensure you select the most appropriate upgrade process to maximize the efficiency of upgrading.

Upgrading to Login Hub v7.0 From Versions older than 7.0

Many new changes and improvements were added to v7.0 of the Login Hub. Due to the significance of the changes made the configuration and setup of previous versions cannot be automatically imported into the new software.

1. Stop the Maintenance Connection LDAP Service using the Services tool in Windows.
2. Start the configuration program.
3. Click on Service Configuration, Uninstall the service.
4. Close the configuration program.
5. Backup the tool and configuration settings
6. Delete the old tool and software.
7. The old configuration tool can be run (but do NOT save!) from the backup folder to enable easy discovery and transfer of settings from the old tool to the new service.
8. Follow the standard Login Hub installation process

Configuration

Configuring the Login Hub service is explained in detail in the installation process. When making changes to settings the service should be stopped to ensure all settings are properly reloaded. After changes are complete start the service.



Once setup is completed it is unlikely that extensive changes will need to be made. Individual settings can be changed (mostly) without concern for affecting other settings. With the wizard style interface all connected settings will normally be addressed at once to ensure no partial changes are made.

Pre-Installation

Maintenance Connection

Make sure that Maintenance Connection has been installed and is working consistently.

Active Directory only: Test Windows Authentication environment

We have Appendix: Environment Setup testing and problem shooting that we strongly recommend you follow BEFORE anything else. If you are experienced setting up the Login Hub, those steps are optional and you can decide whether to do them or wait until you have problems before doing them (perhaps just run the last one, and if it works, carry on.) Experienced installers will frequently 'recognize' when they need to go back and run those tests. If you are not comfortable that you know how – then run those tests first to make sure your environment is correctly set up.

Additional Pre-installation steps

1. Ensure that appropriate permissions have been granted within the Login Hub directory to have either anonymous querying of the Domain or a user has been setup that has sufficient permissions.
2. **Active Directory Only:** Confirm that the IIS Server has been attached to the Active Directory domain.
3. Download the install files.
4. Ensure the Pre-Installation questionnaire has been filled out.
5. **Active Directory Only:** We recommend you go and run the Environment Setup tests again – if you've already run them above or you are experienced and confident, start with the last one, if it works, you don't need to run the previous ones. This is to make sure nothing you did above 'broke' it accidentally.

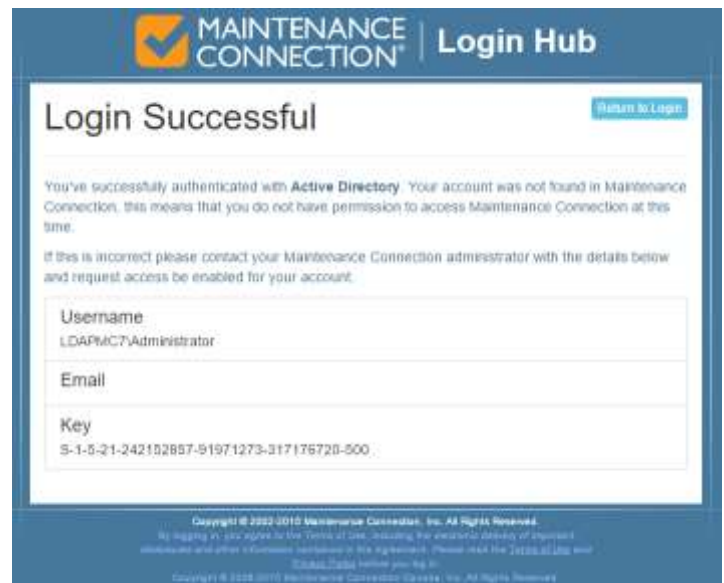
Installation Process

Summary Installation Process

1. You need .NET 4.5.2 installed. See Appendix: Install .NET 4.5.2
2. You need a mcc_loginHub AppPool. See Appendix: Create an Application Pool
3. Create an Application directory in /mc_web/onsite
 - Called loginHub
 - Pointed to /mcc_loginhub/loginHub
 - Use the apppool from previous step



4. Edit the web.connection.config file in /mcc_loginhub/loginHub/. Change line 2 if it doesn't match your system. It should have the path to the mc.ini file. The default is set to "c:/Maintenance Connection/mc_iis/mc.ini"
5. Windows Authentication Feature Delegation needs to be on. See Appendix: Turn on Windows Authentication Feature Delegation
6. Installing Automatic Login. See Appendix: Installing Automatic Login Pages into Maintenance Connection.
7. In a supported browser (IE 11, Edge, Chrome, Safari), go to MC. It should automatically load the login hub pages.
8. Perform the Initial Setup if required. See [Appendix: Initial Configuration of Login Hub](#)
9. Configure the required Login Providers. See [Appendix: Configure Login Providers](#)
 - Once complete, you can select the "Return to Login" button on the top right corner of the page
10. Login via "MC Account" Login to confirm the setup
11. Perform a test login via Active Directory
 - If you have already run the LoginHub Service with a successful sync, you will login
 - If you have not, you will see a "Login Successful" page. This tells you the login process was successful (IIS & Active Directory are communicating properly) but your account was not found in the MC Database.
12. If requiring Active Directory or Novell LDAP sync, setup the Login Hub Service. See Configuration Wizards in Detail for more information.



Configuring for Novell LDAP Only

There are several ways Novell LDAP can be implemented. Contact Maintenance Connection support to create a Login Hub implementation plan for your specific Novell LDAP configuration.

Starting the Service

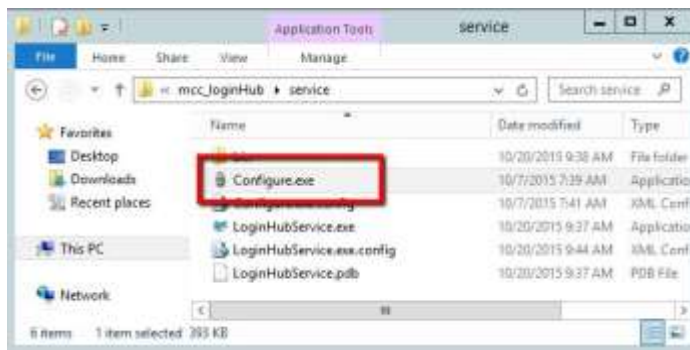
Once the Login Hub service has been successfully configured and tested it can be installed and started. Installing and starting the service is controlled from the Service Information tab in the configuration application. See “Launching the Configuration Application” for a screenshot and details of how to start the configuration application.

Configuration Wizards in Detail

This configuration section applies to existing installations as well as new installs. All configuration steps are the same regardless of if the product is already installed and configured. The only exception to this is an existing installation does not need to re-insert configuration information that is already present.

You cannot change configuration options while the service is running. Always stop the running service (can be done in the configuration application) before performing any changes to the configuration.

Launching the Configuration Application

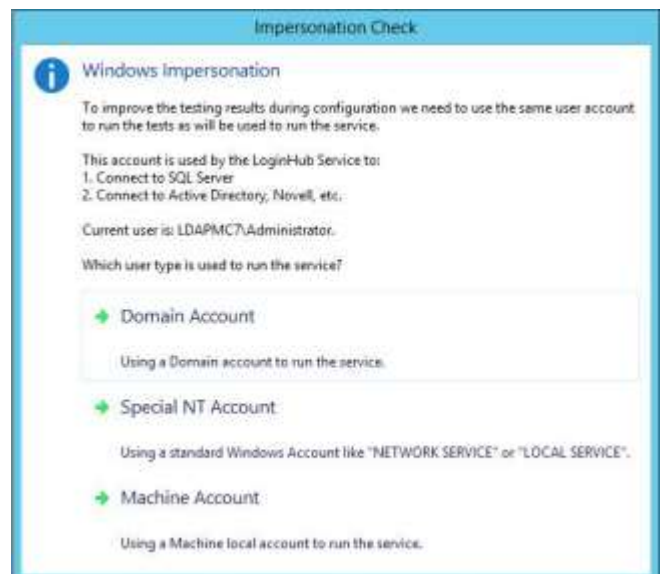


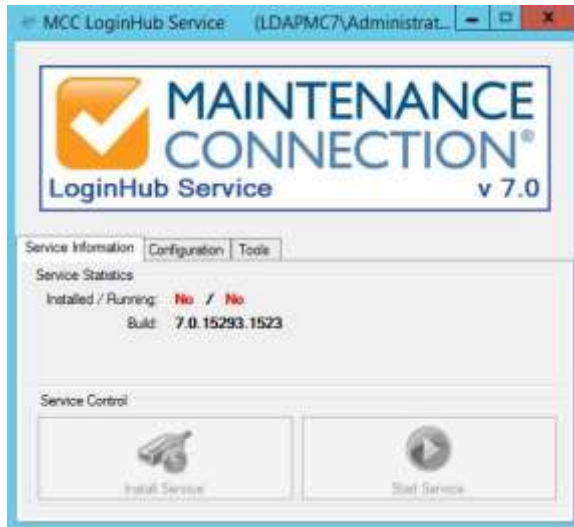
To launch the configuration application, double click on the Configure.exe application.

Launching Configure.exe may display a UAC elevation prompt. Select accept to enable the configuration program to properly launch.

You will then be asked for an Impersonation Check

Make sure you select the correct account type that will be running the Login Hub Service. This will ensure that all test actions are run using the same configuration and provide more accurate test results.





Once running you will see a screen similar to the one to the left.

Areas that can be Configured



To the left is a screenshot of the various configuration wizards that can be used to configure the LDAP Integration Service. These configuration wizards are explained in the sections below.

Configuration can only occur when the service is not running.

Configuring the Connection to Maintenance Connection

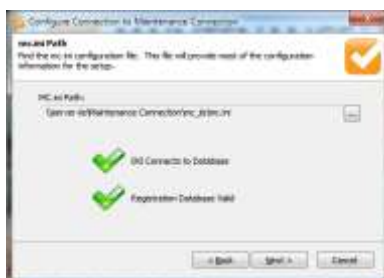


Configuring access to Maintenance Connection is the first step to having the Login Hub Service running. Launch the configuration wizard by selecting the MC Connection Configuration button on the Configuration tab. The wizard will launch and step you through connecting to Maintenance Connection.

Welcome Screen

The first screen of the wizard is the welcome screen. It explains what the purpose of the wizard is. Select next.

mc.ini Path



This page of the wizard will enable you to select the location of the mc.ini file. This file contains the required connection information to connect to the Maintenance Connection databases. Once the file is selected a test will be performed to ensure the INI information can successfully connect to the database and that the database selected is considered a valid Registration database. Select next.

Update Registration Database



The Login Hub engine requires certain API changes to the registration database to operate. This is essential for error free execution of the service.

This should be checked on each upgrade of the service incase new features have been added to the database. If an update is required a red X will be displayed and the Perform Update button will be selectable. Perform the update if required and then select next.

Select License



On this page you will select the license to unlock the Login Hub service. This will allow the Login Hub service to be able to execute properly and display only the most relevant configuration options. If you need assistance with the License Manager please contact your Maintenance Connection administrator. Once the license has been selected it will be validated and you will be able to select next.

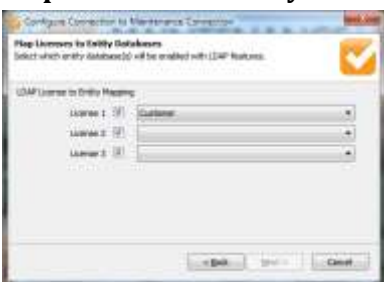
Number of LDAP Connections (optional screen)



This optional page of the configuration wizard will display if you have selected a license that contains 2 or more connections. This enables the user to customize the number of configurable connections without requesting an updated license from Maintenance Connection each time. A connection is defined as the configuration information between 1 LDAP directory and 1 MC database. Unlimited connections can be configured if the proper license has been

purchased and installed.

Map Licenses to Entity Databases



This page enables mapping each connection to a MC database. The same database can be used multiple times if required. If the mc.ini file is configured to use a fixed entity database it will be impossible to change the database references. The check boxes next to each license enables the user to temporarily disable the connection from syncing. This is useful if you want to configure a number of connections and leave them disabled until it is time to roll out the

functionality to the affected users.

Update Entity Database



On this page you will have the ability to upgrade the entity database(s) with the updated LDAP API containing new functions, tables and columns to enable the Login Hub service to run successfully. This is essential to error free execution of the service.

This should be checked on each upgrade of the service incase new features have been added to the database. If an update is required a red X will be displayed and the Perform Update button will be selectable. Perform the update if required and then select next.

Success Page



The last page will enable you to save your changes or cancel. Select finish to save your changes or select cancel to throw out your changes.

Configuring the LDAP Directory Type to Connect To



This allows you to change which type of LDAP directory you will connect to. The three available options are:

- Microsoft Active Directory
- Microsoft Active Directory (Compatibility Mode)
- Novell Groupwise



Select the appropriate option for the LDAP directory you will be using. Active Directory Compatibility Mode is available for instances where Active Directory 2003 is running in compatibility mode with Active Directory 2000, or has some required features disabled. This mode may not offer 100% of available functionality.

Select finish to save your changes.

Configuring Special Service Options and Sync Timings



This wizard allows you to configure how the service will operate in the background. This wizard contains all the global options and settings for the service are set. Keep a careful eye on all the settings as many settings have a direct impact upon the first sync and effectively do nothing after the first sync is complete.

Please consider the following carefully. These settings customize how the LDAP service works at a very base level and will cause completely different results if set differently.

Welcome Screen

The first screen of the wizard is the welcome screen. It explains what the purpose of the wizard is. Select next.

Service Timing



This page will enable you to configure the service interval. This is how often the service will attempt to synchronize between the LDAP directory and Maintenance Connection. Selecting a longer interval will mean that LDAP directory changes will take longer to appear into Maintenance Connection, a shorter interval will cause changes to appear sooner. Select next.

Service User Account



On this page you will be able to configure if the service will prompt for a special user account when installing the service. By default the service will install under the Local Service account, if this account does not have sufficient permissions to access the network (and LDAP) you will need to override the account with a different one. When you install the service it, Windows will prompt for a User Account and Password if this is enabled. Select next.

Service Configuration



On this page you will be able to configure how users are managed in the Login Hub service. The options are explained here:

- **Capture Existing Users into LDAP Integration**

This option is to prevent duplicate Labor/Requester records from appearing after the first sync. It will allow the service to look at user accounts already in MC and attempt to find a valid mapping with a LDAP user account. This will look in the registration database for a user record that exactly matches the LDAP user being synchronized. If existing user names are not “Domain/Username” then advanced capture will be required as well. This is recommended to be enabled.

- **Advanced Capture**

This is an advanced form of the previous option, it will attempt to use more advanced means of capturing existing users, including looking at Labor IDs and e-mail addresses. This will enable a follow up page allowing you to select which advanced methods to use. This is recommended to be enabled. More details in “[Advanced Capture \(optional page\)](#)”



- **Insert Users Only**

This option is for when LDAP directory data is considered out of date. This will keep users Access Group settings matched correctly within Maintenance Connection but will not update any other LDAP sourced information such as Phone, Name and anything else. If this is set user information must be manually maintained within Maintenance Connection. If some LDAP information is considered incorrect but other information is correct this should be left disabled and “LDAP Field Mapping” should be used. This is recommended to remain disabled.

- **Update User Access Groups**

This option controls if the service should keep a users Access Group matched up to the LDAP directories groups. Disabling this allows Access Group changes within Maintenance Connection to be maintained. Enabling this will cause changes to a users Access Group (in MC) to be automatically reverted to the settings in the LDAP directory. This is recommended to be enabled.

- **Assign Repair Center to Requesters**

This option controls if the service should assign a Repair Center to requesters. If the service requester has not been assigned a Repair Center then work orders entered by the service requester will be appear in the default Repair Center. This should be enabled only if requester management uses Repair Centers.

- **Override User Passwords**

This option will automatically erase user passwords contained within Maintenance Connection. Enabling this option will always wipe a user’s password on each sync process. Enable this option for maximum security. If using non-LDAP logins such as Tablet Hybrid or WAP this option should be disabled.

- **Use Blank Password (disable means use “password”)**

This option controls what default password should be used on new accounts as well as what password should be used if the “Override User Passwords” option is set. This is highly recommended to remain checked. If non-LDAP logins are required it is recommended that a user go through the password reset process rather than disabling this option. Leaving this option enabled will ensure maximum security as users without a manually reset password will be unable to login except through the LDAP specific login pages.

Once configuration is complete, select next.

Advanced Capture (optional page)



On this page you will be able to select which advanced capture methods to enable. Enabling all options will maximize the chance that existing users (from before the LDAP service was installed) will be captured into being managed by the LDAP service. Disable any options that do not make sense or will cause issues. Any capture action that results in more than 1 user being found will be discarded as a bad capture action. The available options are:



- **User = User w/o Domain**
This option will attempt to match a record in the registration database that matches LDAP username without the domain attached.
- **User E-mail = LDAP E-mail**
This option will attempt to match a record in the registration database using the LDAP account's e-mail address.
- **Labor ID = Domain\User**
This option will attempt to match a record in the entity database by matching the LDAP username against the Labor/Requester IDs looking for "Domain\Username".
- **Labor ID = User w/o Domain**
This option will attempt to match a record in the entity database by matching the LDAP username against the Labor/Requester IDs looking for the LDAP username without the domain.
- **Labor E-mail = LDAP E-mail**
This option will attempt to match a record in the entity database using the LDAP account's e-mail address.

Ensure that you disable any capture methods that specifically make no sense for the installed Maintenance Connection environment. For instance if many users use the same e-mail address, disabling matching via e-mail address would prevent a random match from occurring.

Once the methods to perform advanced mappings with have been selected, select next.

Error Reporting



This page configures e-mail error reporting features. It is recommended to enable error reporting so that errors can be monitored by e-mail.

Regardless of the settings here errors are automatically logged to the mccErrorLog table in the registration database and full logs (max 5 days) are stored in the \log subdirectory located in the installation folder (logging to the \log directory is prevented when insufficient permissions are granted to the service user account). No reporting or logging is performed when manually executing sync procedures in the configuration UI.

Auto Report Errors To MC

This feature will automatically e-mail Maintenance Connection when Error level or above conditions occurs during the sync. E-mail reports are delivered to: errorReports@maintenanceconnection.ca. This should only ever be disabled if privacy regulations prevent sending error logs or the e-mail server is unable to deliver to outside e-mail addresses.

E-mail Destinations

This allows for entering an additional 3 e-mail destinations that can be alerted when an error occurs. Typically this should be filled in with a monitored IT support address so that if errors are related to new configuration or changed LDAP directory settings IT will be notified when the error occurs.

Success Page

Click the finish button to save your changes and close the wizard.

Configuring Each LDAP Connection

Each installed LDAP connection must be configured independently to connect to LDAP. This enables the ability to connect to multiple domain servers and/or have multiple databases or types of specific group mappings.



As shown above the bottom half of the configuration tab is headed by a second set of tabs. Each tab represents a configured connection and displays the name of the Entity database each license has been configured to connect to. To change these mappings see the instructions in [“Configuring the Connection to Maintenance Connection”](#).

Configuring the LDAP Directory Connection

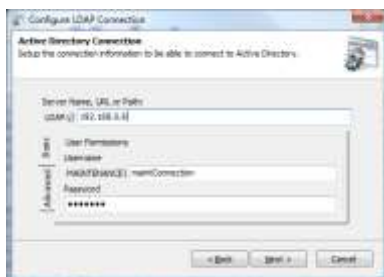


Ensuring a properly setup connection to the LDAP directory is integral to having the entire integration service work.

Welcome Screen

The first screen of the wizard is the welcome screen. It explains what the purpose of the wizard is. Select next.

Active Directory Connection (AD Only)



You will see the primary configuration for connecting to an Active Directory domain server. Fill in the LDAP path and a username & password for the connection. The username & password are optional though may be required depending upon the configuration of the domain server.



The advanced tab is used to change a few advanced settings for connecting to the domain server. If the domain server does not report usernames with the domain included uncheck the “Use Domain in Username”. If the domain name being reported is not the domain name the server uses, for example a multi-domain environment, override the domain name and type in the correct name. Once finished select next to continue.

Novell Directory Connection (Novell Only)



This is where you set the primary configuration for connecting to a Novell LDAP directory. Fill in the directory path and port number. Connecting to a LDAP directory also requires a fully qualified user distinguished name and the user's password. Once finished select next to continue.

Test Directory Connection



This is the wizard screen that allows you to test the connection to the LDAP directory. A connection attempt is made immediately upon going to the page. If the attempt fails a red X will appear; if it succeeds a green checkmark will be displayed. To receive a popup with error results select the Test Connection button. Once a connection is achieved select next.

Success Page

Click the finish button to save your changes and close the wizard.

Configuring LDAP Field Mapping (Active Directory Only)



Configuring the field mappings ensure that the correct information flows from Active Directory into Maintenance Connection. Due to many fields in Active Directory being predefined by the system, several fields have fixed defaults.

Welcome Screen

The first screen of the wizard is the welcome screen. It explains what the purpose of the wizard is. Select next.

Username & E-mail Address



This is the page for configuring the default e-mail address of a user to be synchronized into Maintenance Connection. It is possible to insert users into Active Directory that do not have an e-mail addresses specified. Maintenance Connection does not allow this behavior and all users must have an e-mail address pre-defined. To allow for syncing users without a configured e-mail address you must setup a fallback e-mail to use. Any e-mail addresses, including invalid ones

are acceptable. Select next.

Name Fields



This is the page to configure how user's names will be added into Maintenance Connection. By default names in Active Directory are stored "Firstname Lastname". This can sometimes be undesirable behavior making it hard to look up users in Maintenance Connection (for instance using various address book functions). The Labor/Requester name can be overridden here with a custom name format. Allowed custom format fields are described on the screen.

Select next.

Contact Numbers



This is the page for configuring user phone numbers. If a field is configured and it does not contain any data the corresponding information in Maintenance Connection will not be overwritten. Any fields that have the checkmark next to the field unselected or are left non-configured (no value in the field) will not be synchronized. Select next.

Success Page

Click the finish button to save your changes and close the wizard.

Configuring LDAP Field Mapping (Novell Only)

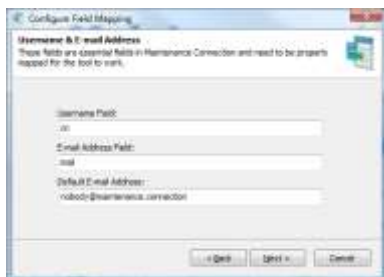


Configuring the field mappings ensure that the correct information flows from LDAP into Maintenance Connection. Since standard LDAP directories do not have a long list of pre-defined fields there are many fields that need to be configured for a successful sync.

Welcome Screen

The first screen of the wizard is the welcome screen. It explains what the purpose of the wizard is. Select next.

Username & E-mail Address



This is the page where you will configure the LDAP fields for the Maintenance Connection username, the e-mail address and the default e-mail address to use in Maintenance Connection if an e-mail address is not available in the LDAP directory. Once configured select next.

Name Fields



This is the page where you configure what fields give a user their name. A full name format can be used instead of a field from the directory; anything can be hardcoded into the format. Available dynamic fields are: {firstName}, {middleName} and {lastName}. Select next when finished.

Contact Numbers



This is the page for configuring user phone numbers. If a field is configured and it does not contain any data the corresponding information in Maintenance Connection will not be overwritten. A non-configured field will not be synchronized. Select next.

Advanced Fields



This is the advanced fields wizard page. This page leads to special advanced fields configuration pages. Each advanced field needs to be correctly configured for full operation. Once finished change the setting to None and click next.

Success Page

Click the finish button to save your changes and close the wizard.

Configuring LDAP Group Mapping

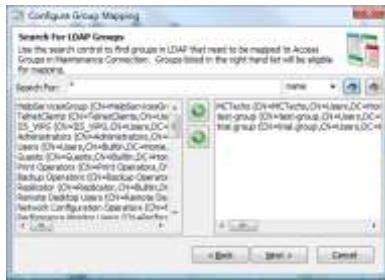


The group mapping wizard enables mapping groups from LDAP to a matching access group in Maintenance Connection.


Welcome Screen

The first screen of the wizard is the welcome screen. It explains what the purpose of the wizard is. Select next.

Search For LDAP Groups



This is the search for LDAP groups screen. This screen allows you to filter through the entire directory of LDAP groups to select a few groups that should be mapped to Maintenance Connection. Wildcard searches are allowed. Search results appear on the left, select a result to map and select the right pointing arrow to add it to the mapped groups list.

To search for all LDAP groups instead of just a few use the find button with a lightning bolt on it ().

Once all the groups that need to be mapped are selected, click next.

Map LDAP Groups onto Access Groups



This is the screen for mapping the previously selected LDAP groups to a Maintenance Connection access group. The LDAP groups that were selected are listed on the left and a dropdown list offering available Maintenance Connection access groups are on the right. Once all the mappings have been set, click next.

Access Group Priority



This is the screen for setting Maintenance Connection access group priority. A user in Maintenance Connection can only be assigned 1 access group, due to this if a user happens to be in 2 or more mapped LDAP roles the highest priority mapped Access Group will be the one selected. Once the Access Group priorities are ordered correctly, click next.

Access Group Auto Approval



This is the screen for setting auto approvals in Maintenance Connection. This will configure if certain access groups will need manual intervention before the users assigned to them are fully approved for use in Maintenance Connection. The default is to approve everything. Once configured, click next.

Success Page

Click the finish button to save your changes and close the wizard.



Scripted Field Import Mapping



The scripted field import mapping wizard enables importing custom configured fields from LDAP into Maintenance Connection. This allows for custom logic to be implemented without requiring custom features to be implemented in the LDAP tool. Any field that is not available for mapping in the regular import (through “[Configuring LDAP Field Mapping \(Active Directory Only\)](#)”) can be filled using this method. Also delayed processing can be performed if calculations must be performed across several imported records.

Select Script



This page allows for selecting which script should be customized. Currently there are 10 available scripts that can be customized, 5 each of 2 different types. The types are:

Text String

This script type stores data for change tracking and long term use in a column of the Labor table called “LDAPCustomFieldText#”. The field is a varchar(50) field allowing for any type of data up to 50 characters

in size to be stored.

Hash Field

This script type stores data for change tracking hashed in a column of the Labor table called “LDAPCustomFieldHash#”. The field is a varchar(32) field and due to storing data hashed can contain data of any type and length without limit.

Script Editor

This page allows for editing the script.

First a LDAP source field must be entered. This is the official LDAP field name in LDAP. Presently this field can be of any type excepting special fields such as array or object reference fields.

Second when the script executes must be selected. The script can be executed on change of the LDAP field or every time the LDAP service executes.



Lastly the script must be entered. This field is of unlimited length and can contain as many SQL statements as required to perform the custom logic required. “GO” and other special SQL Manager commands are not supported. 4 SQL variables will be passed into the script as parameters:

- @SourceValue
The value retrieved from the LDAP directory. This is in its original form. When using Hashed fields this is how you will retrieve the original unchanged value.
- @LaborPK
The PK of the Labor/Requester record being changed.



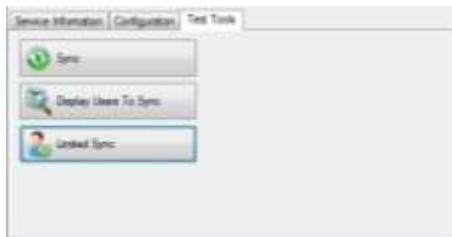
- @UserGuid
The Guid of the user record. Used as an alternative lookup method for the Labor/Requester record or a method to lookup the user in the Registration database.
- @MemberID
The member ID of the user being synchronized. This will take the form of "Domain\Username"

Once the script has been entered and checked over for errors, select next to continue.

Success Page

Click the finish button to save your changes and close the wizard.

Test Tools





To the left is a screenshot of the available test tools. These tools are used to perform various actions between the LDAP directory and Maintenance Connection. Some of these processes can be destructive processes and should be used with caution; backing up of the database is recommended.

Sync



This test tool performs a full and complete sync. This is used to confirm that the tool is fully setup correctly or if a change has been made to the configuration and you do not wish to wait for a sync cycle to occur.

The play button () executes the sync. In the case of issues occurring during the sync the clipboard button () is available to copy the entire sync log to the clipboard for easier identification or



for sending in an e-mail.

Display Users To Sync



This test tool performs what might be considered "sync light". This is a non-destructive process that will execute a standard sync to simply identify which users are expected to be synced. Standard Maintenance Connection database operations are not performed.

This is used to confirm that all the users that are expected to be found are actually being found.


The play button () starts the users search. The clipboard button () will copy the search results to the clipboard.



Limited Sync



This test tool performs a limited version of the standard sync. It will search for a single user in the LDAP directory and attempt to sync that user into Maintenance Connection. In the case of multiple connections, you will first need to select the connection to use.

Type the name in the search box and select the find button to begin the search. Wildcard searches are acceptable and multiple users can be synced at a time using this tool. The clipboard button () will

copy the sync results to the clipboard.



Appendix: Q&A

In this area are various questions and answers that may not be covered in the rest of the installation guide.

Assigning Repair Centers to Labor/Requesters

Repair Centers are often an important part of being able to properly manage service requests and the access to work orders. Repair Centers are assigned based upon the following priorities:

1. If a Repair Center ID has been entered in User Defined field UDFChar1 of the assigned Access Group for the user.
2. The default Repair Center
3. Blank by default if the user is a Requester (MC will assign service requests to the default repair center)

Importing unmapped fields into MC from LDAP

If there is no option in “[Configuring LDAP Field Mapping \(Active Directory Only\)](#)” for importing a field into MC then importing those fields into MC can be accomplished by using “[Scripted Field Import Mapping](#)”. Simple SQL UPDATE scripts can be used to import these fields.

An example script for importing a custom LDAP field as a Craft is presented below:

```
UPDATE [Labor]
SET [CraftID] = @SourceValue,
[CraftName] = (SELECT LaborName FROM Labor WHERE LaborID = @SourceValue AND LaborType = 'CR'),
[CraftPK] = (SELECT LaborPK FROM Labor WHERE LaborID = @SourceValue AND LaborType = 'CR')
WHERE
LaborPK = @LaborPK
```

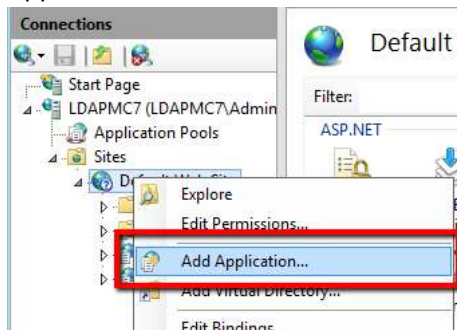



Appendix: Environment Setup testing and problem shooting

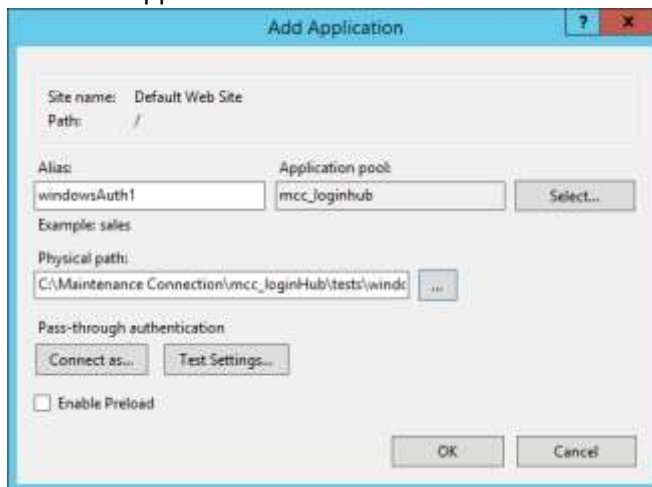
You need the Application Pool setup to run these tests. See Appendix: Create an Application Pool.

Test 1

- 1) Open “Internet Information Services (IIS) Manager”
- 2) On the website that MC is installed (usually “Default Web Site”) right click and select “Add Application”



- 3) Create an application:



Alias:

windowsAuth1

Application Pool: mcc_loginhub

Physical Path:

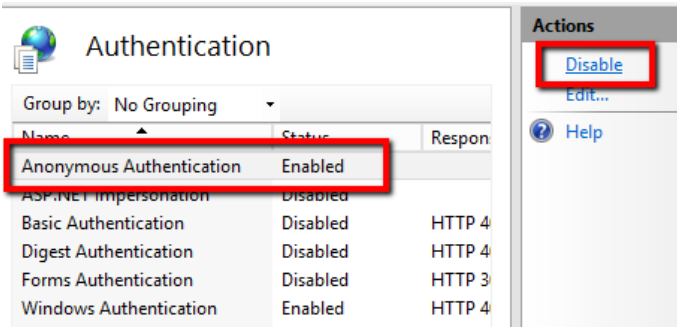
(Your MC install folder)

\mcc_loginHub\test\windowsAuth1\

- 4) Configure “Authentication” on the new Application



- 5) Disable “Anonymous Authentication”, so that *only* one is Enabled: The Windows Authentication.



Note: if Windows Authentication says Disabled, it means something went wrong getting to this point. You will have to Enable Windows Authentication, but make a note that it wasn't set, in case there are problems as you continue that may making finding out why it was wrong important.

- 6) In a browser open [http://\[servername\]/windowsAuth1/](http://[servername]/windowsAuth1/)
- On the server,
 - And on a normal 'client' computer.
 - If you have multiple Active Directory Domains – open it on one normal 'client' computer in every Active Directory domain.
- 7) If everything is setup correctly you should see on every browser you opened the text: If you are looking at this in a browser – the Windows Auth1 page loaded.



If this test shows a Username prompt, there is likely a problem that needs to be resolved.



It should NEVER prompt from a 'client' machine. If it prompts from a 'client' machine then the server is not able to understand your logon details, and there is a problem with the server's setup and connection with Active Directory or there is a 'network' problem.

If it is prompting from the 'server', it could be because you logged in as a local user account (not a network account). In this case, enter in the user name and password of a network account, hit OK, then hit F5 to refresh the page to verify that you are not being asked 'every' time.

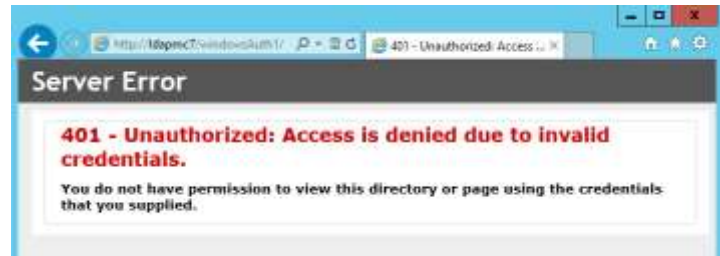
If you still get this prompt, then the server is not able to understand your logon details, and there is a problem in the server's setup and connection with Active Directory.

Summary:

If prompting always on the server and always on the client: then the server is not able to understand your logon details, and there is a problem with the server's setup and connection with Active Directory (and there may also be a 'network' problem as below).

If prompting once or never on the server and always on the client would be the same problem or a network problem.

If you see a 401 error (shown to the right), this means that the credentials that you supplied (or your browser supplied for you) are considered to be invalid by the server. This may show that you either entered the credentials incorrectly, or that the server is not setup to understand your credentials.



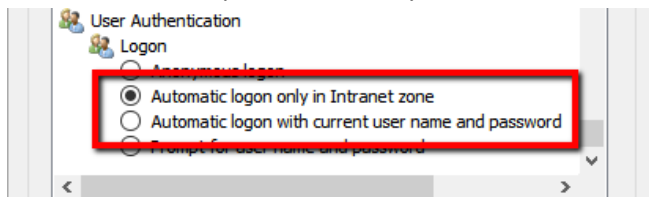
Some other, less likely, causes of getting the password/id prompt

An article you may want to read if you get this is: <http://clintboessen.blogspot.ca/2013/09/ie-10-prompting-for-credentials-windows.html>

Here is a discussion about it if you want to deal with it on a browser by browser case.

For IE: If the website is being detected by Internet explorer as not an Intranet site, then IE will not send credentials "by default". This can be changed by setting the below setting (for more details, read the above linked article).

Tools > Internet Options > Security > Custom level... > User Authentication



For Mozilla Firefox: The Firefox browser does not offer any trusted sites settings in the properties dialog; however it does provide a configuration string which can be modified to enable this functionality. Enter about:config into the address bar, enter and confirm the safety check. Search or create the preference string network.automatic-ntlm-auth.trusted-uris. Afterwards enter trusted site names as list separated by comma and space. For example like this: intra, intranet, localhost

For Chrome: Chrome takes its trusted sites settings from the same Internet Options as Internet Explorer. You can access the dialog from Chrome here:

Properties -> Show advanced settings -> Change proxy settings -> Security -> Trusted sites

Please note: you will be asked to log in the first time you access the trusted site.

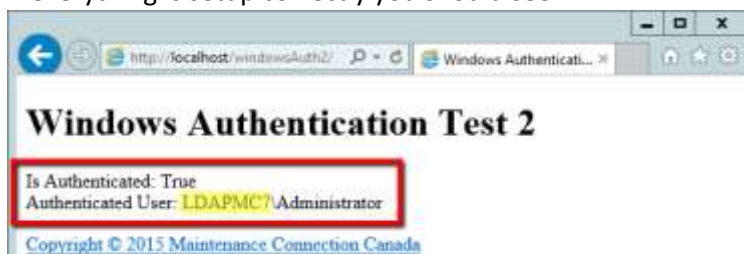


None of those worked? PLEASE ... when you find the solution, let us know HOW you fixed it so we can include it in this manual. That way you will help others AND the next time you run into it and forgot how you fixed it - we will have documented it for you in the perfect location.

Test 2

This test (and all following tests) assumes that any login prompt issues that may exist have already been fixed before attempting the tests. See Test 1 directly above. If login prompts occur during the tests that are not expected, you should go back and look at the settings for Test 1 to confirm that “Anonymous Authentication” is correctly disabled. If any special IIS settings were required in order to get Test 1 to pass, then those settings need to be noted as they may be incompatible (or need to be applied in a special way) with the setup of further tests.

1. Follow the instructions for steps 1-5 from Test 1, but substitute windowsAuth2 instead.
6. In a browser open <http://{servername}/windowsAuth2/>
 - a. On the server,
 - b. And on a normal ‘client’ computer.
 - i. If you have multiple Active Directory Domains – open it on one normal ‘client’ computer in every Active Directory domain.
7. If everything is setup correctly you should see:



“Is Authenticated: True” and your username.
You should also see in the highlighted are below, your NT style domain name.

Summary

If you are not seeing “Is Authenticated: True” you should recheck step 5 from Test 1.

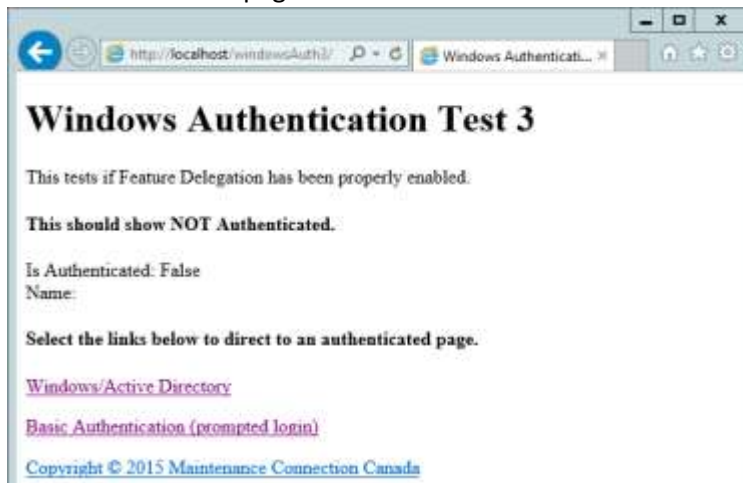
If you are seeing some other username, or not your domain listed, you should recheck what domain/user was used to log into the computer performing the test.

Test 3

1. Follow the instructions for steps 1-4 from Test 1, but substitute windowsAuth3 instead.
NOTE: Do not follow step 5, only steps 1-4.
5. If you have not previously enabled “Feature Delegation” for “Windows Authentication” then please follow the instructions for enabling that feature. ??? (See Step 5 of the initial Installation process)
6. In a browser open <http://{servername}/windowsAuth3/>
 - a. On the server,
 - b. And on a normal ‘client’ computer.
 - i. If you have multiple Active Directory Domains – open it on one normal ‘client’ computer in every Active Directory domain.



7. You should see this page:



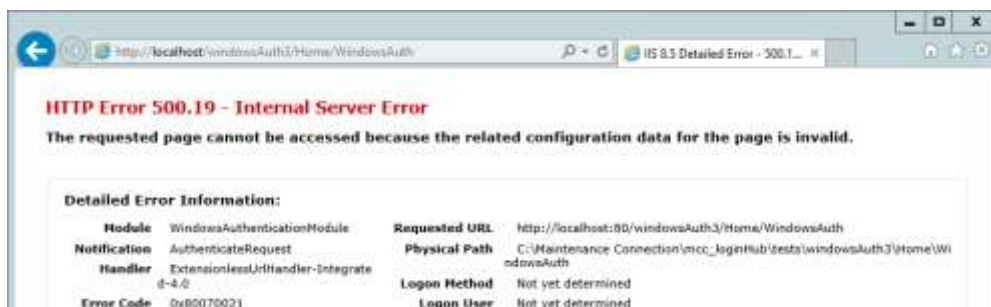
8. Select the “Windows/Active Directory” link
9. If everything is setup correctly you will see:



Summary

This test is testing if IIS Feature Delegation is correctly working on your server.

If instead of the success page, you see an error page much like this:



The above error page means feature delegation has not been properly enabled. This may be at the server root or at any web.config file setup between the server root and the application directory.

Test 4

1. Follow the instructions for steps 1-3 from Test 3, but substitute windowsAuth4 instead.



4. You should see this page:



5. Select the “Windows/Active Directory” link
6. If everything is setup correctly you will see:



Summary

This tests if advanced authentication is working. Confirming that Windows authentication and basic information queries like email & SID are returning correct information.



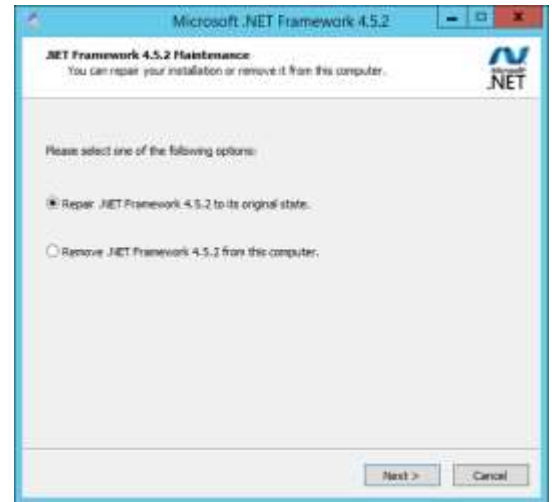
Appendix: Install .NET 4.5.2

You need to have .NET 4.5.2 installed on the server.

If you do not have it already installed 2 options are:

1. Use the web installer we provide in the /mcc_loginHub/preReq directory.
2. .NET can also be installed via Windows Update if you prefer.

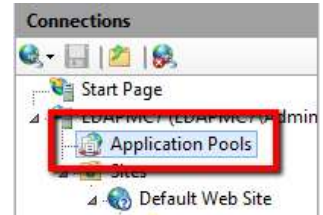
If you do not know if .NET 4.5.2 is already installed, please run the web installer provided in the /mcc_loginHub/preReq directory and it will offer to “Repair” the installation if .NET 4.5.2 is already installed.



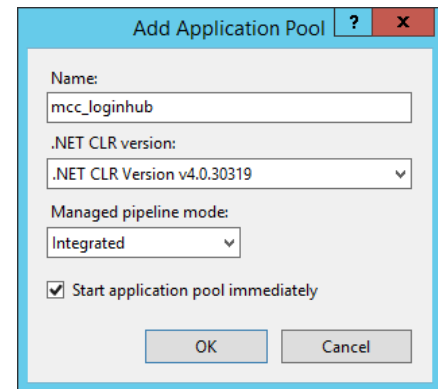


Appendix: Create an Application Pool

- 1) Open "Internet Information Services (IIS) Manager"
- 2) Select the "Application Pools" node (far left panel)
- 3) In the "Actions" bar (far right panel), select "Add Application Pool..."



- 4) Create an "Application Pool" with:
Name: mcc_loginhub (strongly recommended)
.NET CLR version: v4.0.*
Pipeline mode: Integrated



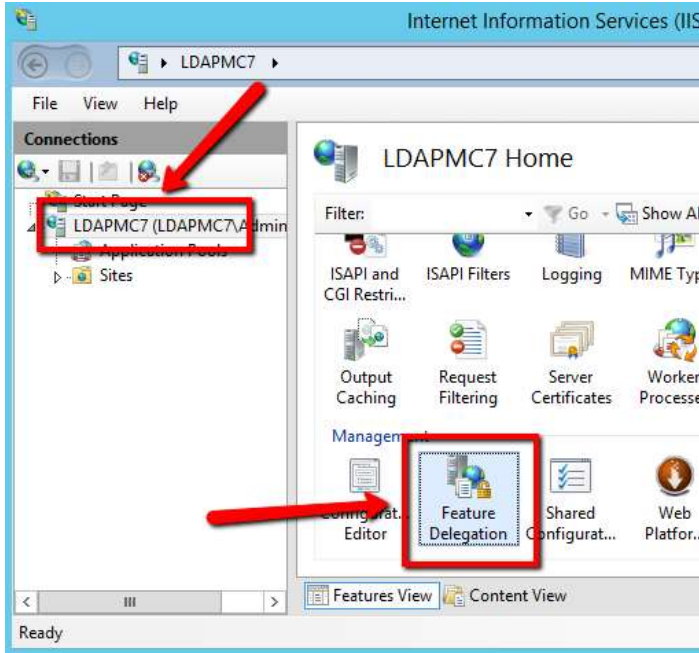
- 5) If using Windows Authentication to log in SQL Server, you need to change the Application Pool Identity to match the account that has been setup for accessing SQL Server.



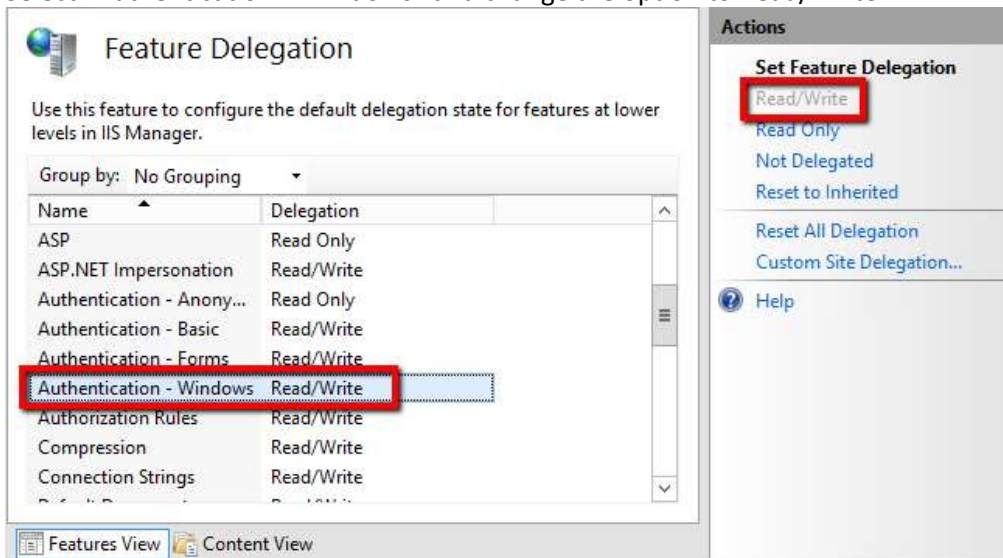



Appendix: Turn on Windows Authentication Feature Delegation

1. Go to the Server node in IIS



2. Open Feature Delegation (bottom center option)
3. Select "Authentication – Windows" and change the option to Read/Write



4. If you wish use the "Active Directory  login provider (what we call the 'Active Directory forced login' provider) to force Username/Password prompts for every login you also want to enable Feature Delegation for "Authentication – Basic".



Appendix: Installing Automatic Login Pages into Maintenance Connection

Once the Login Hub is enabled the standard Maintenance Connection login pages do not function as a login page anymore. Login Hub specific login pages need to be inserted to enable automatic login.

1. Open the file browser.
2. Navigate to the Login Hub tool install folder.
3. Copy all the files located in the “mcPages” folder.
4. Paste the files into the “\Maintenance Connection\mc_iis\onsite” folder.
5. Select “Yes” to overwrite when prompted.

This should be done for each upgrade as well (these files may contain bug fixes)



Appendix: Initial Configuration of Login Hub

1. Open a supported web browser (IE 11, Edge, Chrome, Safari Mac)
2. Browse to http://{servername}/mc_web/onsite/loginHub/diagnostic/
3. If the initial configuration has not been completed, you will be forwarded automatically to the “Initial Setup” pages.

Initial Setup: Step 1

1. If the path to the mc.ini file is incorrect this will display a red X error.
2. If required change line 2 of /loginHub/web.connection.config to point to the correct path of the mc.ini file (usually C:\Maintenance Connection\mc_iis\mc.ini).

Database Connection Retest Connection

MC INI Path: Save

INI File Exists: ✖

3. Once the mc.ini file exists then the test will check if the information within the file allows for a successful connection to the mcRegistrationSA database.

Connection String: Data Source=Idapmc7;Initial Catalog=MCRegistrationSA;Integrated Security=False;User ID=mczar;Password=mczar;Network Library=dbmssocn

Connects to DB: ✔

Test Performed: Thu Oct 29 2015 12:43:35 GMT-0600 (Mountain Daylight Time)

Next

Errors in this step may be corrected by changing the Application Pool identity, or by editing the SQL User ID/Password in the mc.ini file.

Initial Setup: Step 2

Check and update the Registration Database

Database Update Retest Database(s)

Registration Database

Up To Date: ✖ Details: (✔ 4 , ✖ 1 , ⚠ 4)

Perform Update: Automatic Manual

In most cases the “Automatic” update should work to update the database with required tables and stored procedures. If security settings prevent the use of the Automatic update, then use the “Manual” update process. This process is clearly documented in the UI which provides instructions for how to save the SQL Script and run it against the database.



Manual Database Update MCRRegistrationSA

In order to manually update the selected database:

1. Download the SQL script listed below.

2. Open the script in SQL Management Studio.

3. Run the script against the specified database.

Note: The SQL script is database specific and may contain actions unique to each database.

4. Select the **Retest Database(s)** button in order to confirm a correctly applied update.

Download:

Download Script

Script Preview:

```
/*=====
 * BEGIN: RegLoginHubCreate
 *=====*/
/* This SQL script is used to create (or update if already existing) the
tables and views used by the Asset Pro Solutions Inc. LoginHub.
```

Check and update each Entity database

Entity Database(s)

ABFAC ENTABFAC

Up To Date: Details: (0 , 0 , 0)

If any updates need to be run the same process as was performed for the Registration database will need to be repeated. Please note that if using the “Manual” update process, you will need to generate a SQL script for each database individually as the script is customized for each database.



Appendix: Configure Login Providers

Login Providers control which way(s) a user is allowed to login to Maintenance Connection.

A typical install will include the MC Account provider and 1 of the Active Directory providers.

Adding a New Login Provider

Login Providers Add Provider Save All

1. Select Add Provider

Add Provider ×

<input checked="" type="checkbox"/>	MC Login The standard/normal Maintenance Connection Login option.
	Active Directory Active Directory integrated 1 click login. Uses Windows login context information provided via the browser to automatically login.
	Active Directory Active Directory integrated forced prompt login. Prompts the user to enter Active Directory credentials on every login attempt, useful in public/shared computer environments.
	Active Directory: Generic Experimental: Generic login provider for testing LDAP logins.

2. Select from the list of available Login Providers
3. Configure the login provider as required for your environment

Configuring a Login Provider

Login Providers can login through many different potential sources. Due to this the configuration options presented will vary.

When you have finished configuring the provider(s) make sure to select “Save” or “Save All” to ensure your settings will be used the next time a user logs in.


Login Providers Add Provider Save All

<input checked="" type="checkbox"/> MC Login	Remove Provider Save
---	---

MC Account

This provider offers basic Maintenance Connection login options.



 MC Login

Remove Provider Save

The standard/normal Maintenance Connection Login option.

☒ Enabled


Display Order:

100

The only options offered are to “Enable” the provider and to change the order that the provider will be displayed.

Active Directory

This provider is used to make a Single Sign On (SSO) experience with Active Directory possible. If errors are experienced while using this provider see [Appendix: Environment Setup testing and problem shooting](#) for assistance in discovering the server setup issues that may result in SSO not working.

 Active Directory

Remove Provider Save

Active Directory integrated 1 click login. Uses Windows login context information provided via the browser to automatically login.

☒ Enabled

Direct Login URL:

http://ldapmc7/mc_web/onsite/loginHub/loginDirect?provider=ActiveDirectory

Display Order:

200

This provider can be directly logged in with. Entering the provided “Direct Login URL” into the browser will allow a User to be able to login without seeing a login page.

The only options offered are to “Enable” the provider and to change the order that the provider will be displayed on the login page.

Active Directory (Active Directory Forced Login prompt)

This provider is used to provide Active Directory login with a forced credentials entry prompt EACH time a user goes to login to Maintenance Connection. This is a very useful provider for environments where users may share their computers with other users.



Active Directory integrated forced prompt login. Prompts the user to enter Active Directory credentials on every login attempt, useful in public/shared computer environments.

☒ Enabled

Direct Login URL:

`http://ldapmc7/mc_web/onsite/loginHub/loginDirect?provider=ActiveDirectory-Forced`

Display Order:

300

This provider can be directly logged in with. Entering the provided “Direct Login URL” into the browser will allow a User to be able to login without seeing a login page.

The only options offered are to “Enable” the provider and to change the order that the provider will be displayed on the login page.

Active Directory: Generic

This provider is largely an experimental provider used for testing if LDAP logins are working correctly. It operates very similarly to “Active Directory” except it allows for a high degree of customization. This provider does not rely upon IIS to perform the actual user authentication action, instead it communicates with Active Directory directly.

Active Directory: Generic

Experimental Generic login provider for testing LDAP logins.

☒ Enabled

Direct Login URL:

`http://ldapmc7/mc_web/onsite/loginHub/loginDirect?provider=ActiveDirectory-Generic`

Display Order:

400

Context Type

Domain

☒ Use Impersonation

Domain

Domain

Username

Username

Password

Password

Login Type

Network

☐ Debug Mode

This provider provides a large number of configuration choices. If using this provider to test the communication between the IIS server and Active Directory these options should either be clear, or you should coordinate configuration with a Maintenance Connection support representative.

