Master Calendar Integrated Authentication Configuration Instructions

Dean Evans & Associates, Inc.

ems
MASTER
CALENDAR
Promote • Share • Engage

Copyright

Dean Evans & Associates, Inc.
6465 Greenwood Plaza Blvd
Suite 600
Centennial, CO 80111

Information in this document is subject to change without notice.

Table of Contents

Integrated Authentication is *Optional* Functionality

The Integrated Authentication module (which includes Integrated Windows Authentication, Portal Authentication and LDAP Integration) is a separately licensed component for the EMS Master Calendar system. ***You must be licensed for Master Calendar and Integrated Authentication in order to configure and use this module.***

If you are unsure whether your organization is properly licensed, or if you would like to learn more about the Integrated Authentication module, please contact your EMS Account Executive (800-440-3994 ext. 863 or sales@dea.com).

Compatible EMS Systems

Integrated Windows Authentication and Portal Authentication are supported on the following Master Calendar versions:

- EMS Master Calendar 1.5 (Build 2.0.40) or later

LDAP integration is supported on the following Master Calendar versions:

- EMS Master Calendar 2.0 or later

You can determine your Master Calendar version by accessing your system and, at the main (i.e., Calendar Selection) window, adding systemcheck.aspx to the end of the website address. For example:

http://[ServerName]/ MasterCalendar/systemcheck.aspx
(*replace [ServerName] with the name of your web server*)

The version number is displayed at the top of the page and can also be found by clicking the Assembly heading.

If you would like to utilize integrated authentication or LDAP integration but are not running a Master Calendar version that supports it, you can (if you have a current Annual Service Agreement) download the latest version of the software from our website (www.dea.com). Click Customer Login, provide your email address and password (or request a password), click on the appropriate download(s) and follow the instructions.

Portal Authentication

The Master Calendar system can, with proper licensing, be configured so that users are automatically signed on when they access your network. This process is sometimes referred to as “single sign-on” since users have already signed on to the network through some other means – usually a portal such as SiteMinder, Plumtree or uPortal.

Using one of several methods, Master Calendar can compare a unique variable captured by your portal/sign-on page (email address, employee ID, network credential, etc.) to a value that has been stored for the user in your database. If the credentials match, the system automatically logs the user into the Master Calendar application.

Configuration Steps

In order to configure portal authentication you must perform the following steps:

1. Confirm or install new license
2. Select portal authentication method
3. Verify portal redirect

These steps are described in detail below.

Confirm or Install New License

In order to use Portal Authentication, your organization must be properly licensed. If you are unsure about whether you have purchased the Integrated Authentication module that enables Portal Authentication, log in to Master Calendar, go to the systemcheck.aspx page (as described under Compatible Systems), click the License Information heading and review the Licensed For list.

If you were not previously licensed for Integrated Authentication but are now, update your registration information by logging in to the Master Calendar, going to Admin – Registration, entering the new information and clicking Save License Data.

After you have entered the registration information, you must have Master Calendar re-read it by going to the systemcheck.aspx page, clicking the License Information heading and then clicking Read License.

Select Portal Authentication Method

To select the portal authentication method to be used, log in to Master Calendar and go to Admin – Default Settings. Select the appropriate entry from the Portal Authentication Method drop-down list. Since almost every “single sign-on” environment and strategy is different, we have provided you with five commonly-supported methods of authentication: server variable, session, form, cookie and query string. The first two methods are the most widely used.

Server Variable Method (Header Variable)

Server Variable/Header Variable is a collection of variables that are set by the Internet Information Server (IIS). Applications like SiteMinder create custom server variables for portal site use.

Code example:
Set the Portal Authentication Method field to Server Variable and type the appropriate entry in the Portal Authentication Variable field. Then redirect users to the Default.aspx page (or to *any* page in the system for Master Calendar) and the server variable will be read.

Session Method

A session is a way to provide/maintain user state information in an inherently stateless environment. It provides access to a session-wide cache you can use to store information.

In order to use the session method, set the Portal Authentication Method field to Session and type the appropriate variable in the Portal Authentication Variable field. Then you must create an asp.net web page and name it with the .aspx extension similar to the example below. The asp.net web page created must be copied into the Master Calendar root web directory. It must be put there in order for Master Calendar to read the session variable.

You will need to pass the user's email address or external reference through to your asp.net web page.

Code example in vb.net:

```
<%@ Import Namespace="System" %>
<script runat="server" language="vb">
        Sub Page_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)
                Session.Item("MCSession") = "test@dea.com"
                Response.Redirect("Default.aspx")
        End Sub
</script>
```

Form Method

Forms enable client-side users to submit data to a server in a standardized format via HTML. The creator of a form designs the form to collect the required data using a variety of controls, such as INPUT or SELECT. Users viewing the form fill in the data and then click Submit to send the data to the server.

To use the form method, set the Portal Authentication Method field to Form and type the appropriate variable in the Portal Authentication Variable field. To create portals through a form, create a web page with a form similar to below. Once the user logs on through the portal, the form below can be submitted to log the user on to the application.

Code example in HTML:

```
<Form name="form1" method="Post" action="http://localhost/virtualdirectory/Default.aspx">
        <input type="hidden" id="MCFORM" name="MCFORM" value="test@dea.com">
        <input type="submit" value="submit">
</form>
```

Cookie Method

A cookie is a small piece of information stored by the browser. Each cookie is stored in a name/value pair called a crumb—that is, if the cookie name is "id" and you want to save the ID's value as "this", the cookie would be saved as id=this.

You can store up to 20 name/value pairs in a cookie, and the cookie is always returned as a string of all the cookies that apply to the page. This means that you must parse the string returned to find the values of individual cookies. Cookies accumulate each time the property is set. If you try to set more than one cookie with a single call to the property, only the first cookie in the list will be retained.

To use the cookie method, set the Portal Authentication Method field to Cookie and type the appropriate variable in the Portal Authentication Cookie Key field. Then create a web page with code similar to below. Once the user logs on through the portal, take their user logon information and create a cookie. After the cookie is created, send the user to the Default.aspx page of the application.

Code example in Active Server Pages 2.0:

```
<%@LANGUAGE="VBSCRIPT" %>
<%
        Response.Expires = -1
        Response.Cookies("MCCookie")("CookVal") = "test@dea.com"
        Response.Cookies("MCCookie").Path = "/"
        Response.Cookies("MCCookie").Expires = DateAdd("m", 3, Now)
        Response.Redirect("http://localhost/virtualdirectory/Default.aspx")
%>
```

Query String Method

A query string is information appended to the end of a page's URL. An example using portal authentication is below

Code example:
http://localhost/virtualdirectory/Default.aspx?MCQS=test@dea.com

To use the query string method, set the Portal Authentication Method field to Query String and type the appropriate variable in the Portal Authentication Variable field.

Verify Portal Redirect

The portal authentication entry page is the page within Master Calendar that processes the portal request. The name of the page is Default.aspx and it is the page where all portal authentication requests should be sent. This page is already installed and included with your Master Calendar software. The location will be the same folder as the EMS product's root web folder. For example, http://localhost/virtualdirectory/Default.aspx

Integrated Windows Authentication

Integrated Windows Authentication is another form of “single sign-on” available as an option with Master Calendar systems.

Configuration Steps

In order to configure Integrated Windows Authentication for Master Calendar, you must perform the following steps *after* installing and configuring Master Calendar:

1. Confirm or install new license
2. Add domain/user account information to user records
3. Configure IIS for authenticated access

These steps are described in detail below.

Confirm or Install New License

In order to use Integrated Windows Authentication, your organization must be properly licensed. If you are unsure about whether you have purchased the Integrated Authentication module that enables Integrated Windows Authentication, log in to Master Calendar, go to the systemcheck.aspx page (as described under Compatible Systems), click the License Information heading and review the Licensed For list and look for a description to state “Integrated Authentication”.

If you were not previously licensed for Integrated Authentication but are now, update your registration information by logging in to the Master Calendar, going to Admin – Site Administration - Registration, entering the new licenses information then click Save License Data. Please note, the licenses information is case sensitive and needs to be entered in exactly how it was provide from Dean Evans & Associates, Inc. If the information that was provided is incorrect, please contact Dean Evans & Associates, Inc.

After you have entered the registration information, you must have Master Calendar re-read it by going to the systemcheck.aspx page, clicking the License Information heading and then clicking Read License. At the very top of the page, it should state “License read successfully”.

Add Domain/User Account Information to User Records

Integrated Windows Authentication functions by comparing the domain/user account used when logging in to your network workstations with the corresponding domain/user account information recorded on your Master Calendar user records.

There are three ways to add the domain/user information to user records. The first method, manually entering information through the Master Calendar interface, is less technical and can be managed with little knowledge of SQL. The second method while more efficient assumes some degree of experience with SQL and database administration. The third method has your Master Calendar users enter the appropriate information when they first use the application.

Manually entering information through the Master Calendar

1. Log on to EMS Master Calendar and navigate to Admin – Security - Users.
2. Click the icon in the Update column for the user record that you want to edit.
3. In the External Reference field, type the domain\user account used by this person to log in to your network.

   In a single domain environment, only the user account is necessary.

4. Click Update to save your entry.

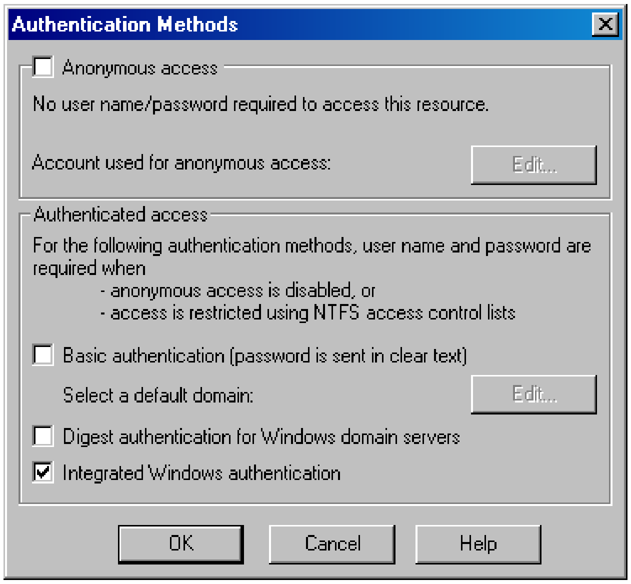
5. After editing all users, continue to the Configuring IIS step below.

Configure IIS for Authenticated Access

To configure IIS for authenticated access, do the following:

1. Open the Microsoft Internet Information Services (IIS) Manager.
2. Navigate to the appropriate virtual directory and right-click to reach Properties.
3. Go to the Directory Security tab and edit the Anonymous Access and Authenticated Access sections as follows: Clear the Anonymous Access check box and check the Integrated Windows Authentication box.

Figure 1-1: The Authentication Methods Window (IIS 6.0)



Authentication Methods

☐ Anonymous access

No user name/password required to access this resource.

Account used for anonymous access:

Authenticated access

For the following authentication methods, user name and password are required when
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

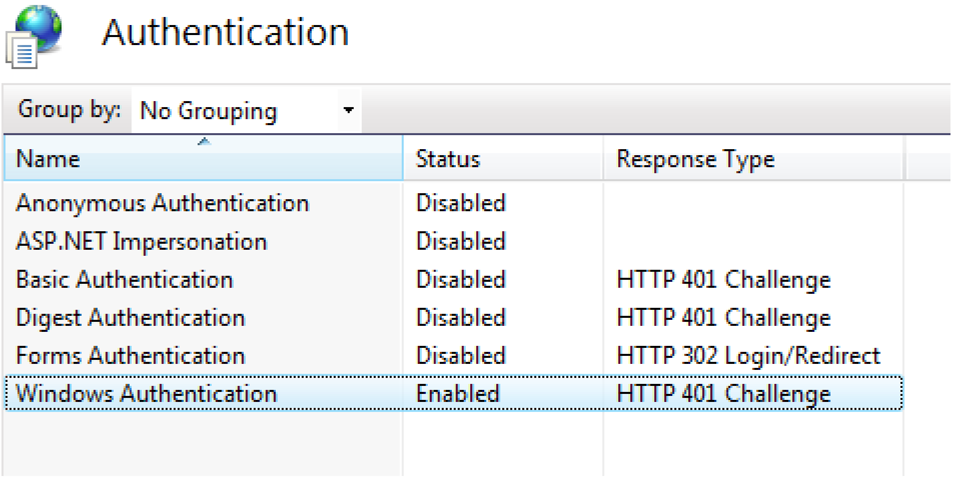
☐ Basic authentication (password is sent in clear text)

Select a default domain:

☐ Digest authentication for Windows domain servers

☑ Integrated Windows authentication

Figure 1-2: The Authentication Methods Window (IIS 7.0)



Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

4. Click OK. Integrated Windows Authentication is now enabled.

Frequently Asked Questions

- *Why is it necessary to put account information into tblUser to authenticate a user?*

We need to know the Master Calendar security template assignment (among other preferences) for the user to authenticate. For licensing purposes we also need to know how many users are active in the system.

- *Why do we need to put account information in the External Reference field for a user?*

Integrated Windows Authentication works by comparing credentials on the user record to those being supplied by Windows authentication. Without the account information, there is no way to cross reference a Master Calendar user with their Windows credentials.

- *We also need our non Windows-authenticated users to access Master Calendar. What can we do?*

You can install another Master Calendar anonymous access directory to your web server and point that installation to the same database. Public users may access the database via this second directory.

LDAP Integration

LDAP integration allows the system to use security group information maintained on your network to determine the appropriate permissions for Master Calendar users.

Configuration Steps

In order to configure LDAP integration for the Master Calendar system, you must perform the following steps *after* installing and configuring Master Calendar:

1. Confirm or install new license
2. Configure Master Calendar to call your LDAP Server
3. Add LDAP security groups to Master Calendar

These steps are described in detail below.

Confirm or Install New License

In order to use LDAP Integration, your organization must be properly licensed. If you are unsure about whether you have purchased the Integrated Authentication module that enables LDAP Integration, log in to Master Calendar, go to the systemcheck.aspx page (as described under Compatible Systems), click the

License Information heading and review the Licensed For list and look for a description to state “Integrated Authentication”.

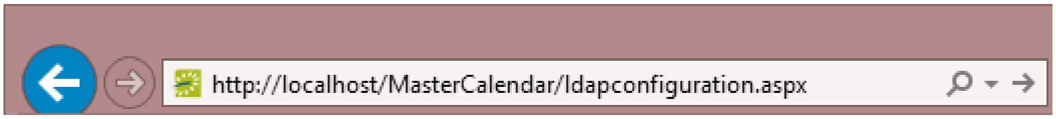
If you were not previously licensed for Integrated Authentication but are now, update your registration information by logging in to the Master Calendar, going to Admin – Site Administration - Registration, entering the new licenses information then click Save License Data. Please note, the licenses information is case sensitive and needs to be entered in exactly how it was provide from Dean Evans & Associates, Inc. If the information that was provided is incorrect, please contact Dean Evans & Associates, Inc.

After you have entered the registration information, you must have Master Calendar re-read it by going to the systemcheck.aspx page, clicking the License Information heading and then clicking Read License. At the very top of the page, it should state “License read successfully”.

Configure Master Calendar to call your LDAP server.

1. Log in to Master Calendar as the site system administrator and click on the Admin menu item. Manually type “LDAPConfiguration.aspx” to the URL in the address bar to access the LDAP Configuration page.

   Figure 1-3: Accessing the LDAP configuration page

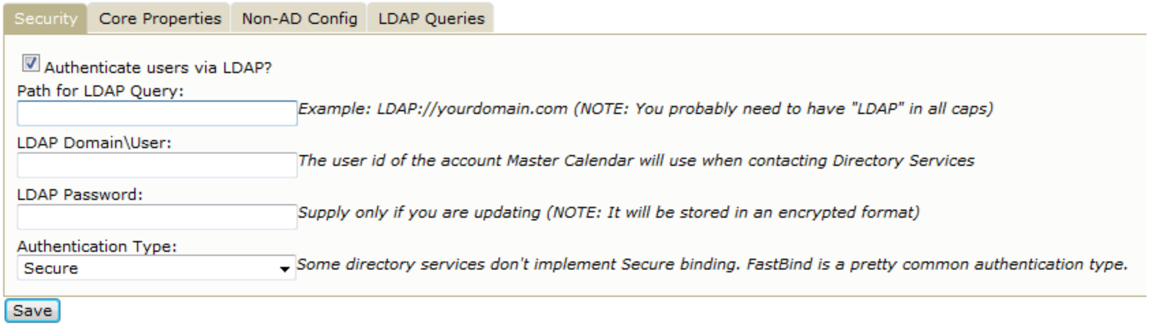


http://localhost/MasterCalendar/ldapconfiguration.aspx

2. Configure your LDAP Settings. Please note:

   - Master Calendar only utilizes read-only queries to the organizations directory services.
   - The Domain\User account does not need to have any special privileges. All that is required is that it be an active account in your directory services.
   - Be aware, in some environments, passwords expire at scheduled intervals. If the password in LDAP settings is not updated when this occurs, Master Calendar/LDAP connectivity will be lost until the new password has been re-entered. It is recommended to consider using a generic account and a password that does not expire.

Figure 1-4: LDAP Security Settings



☑ Authenticate users via LDAP?

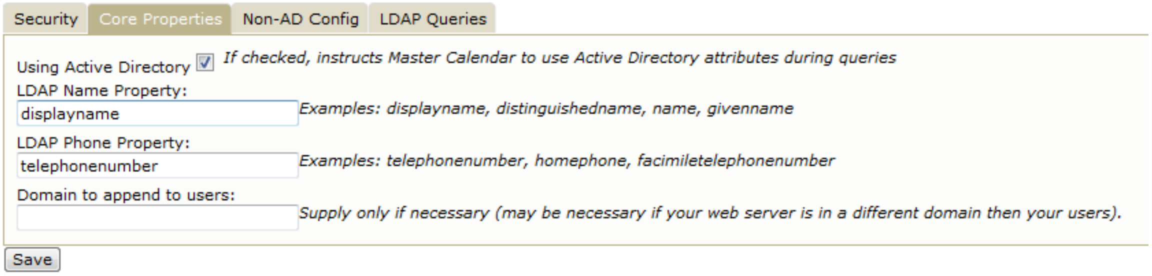
Path for LDAP Query: *Example: LDAP://yourdomain.com (NOTE: You probably need to have "LDAP" in all caps)*

LDAP Domain\User: *The user id of the account Master Calendar will use when contacting Directory Services*

LDAP Password: *Supply only if you are updating (NOTE: It will be stored in an encrypted format)*

Authentication Type: Secure *Some directory services don't implement Secure binding. FastBind is a pretty common authentication type.*

Figure 1-5: Core Properties



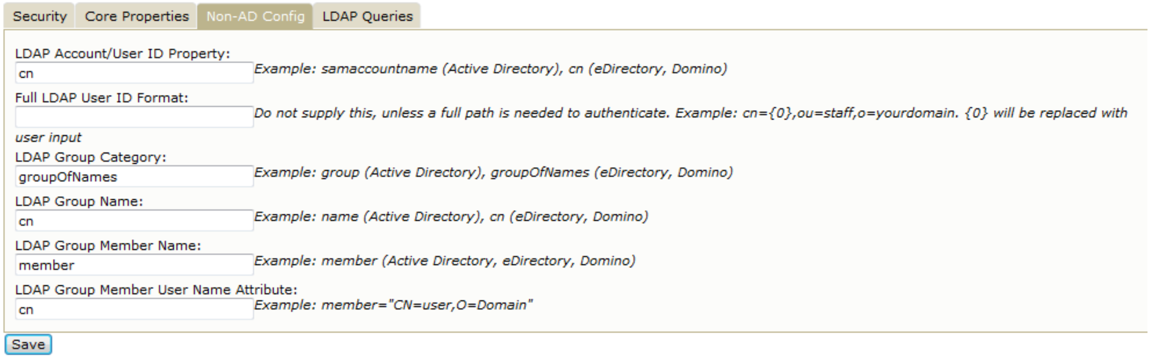
Using Active Directory ☑ *If checked, instructs Master Calendar to use Active Directory attributes during queries*

LDAP Name Property: displayname *Examples: displayname, distinguishedname, name, givenname*

LDAP Phone Property: telephonenumber *Examples: telephonenumber, homephone, facimiletelephonenumber*

Domain to append to users: *Supply only if necessary (may be necessary if your web server is in a different domain then your users).*

Figure 1-6: Non-AD Configuration



LDAP Account/User ID Property: cn *Example: samaccountname (Active Directory), cn (eDirectory, Domino)*

Full LDAP User ID Format: *Do not supply this, unless a full path is needed to authenticate. Example: cn={0},ou=staff,o=yourdomain. {0} will be replaced with user input*

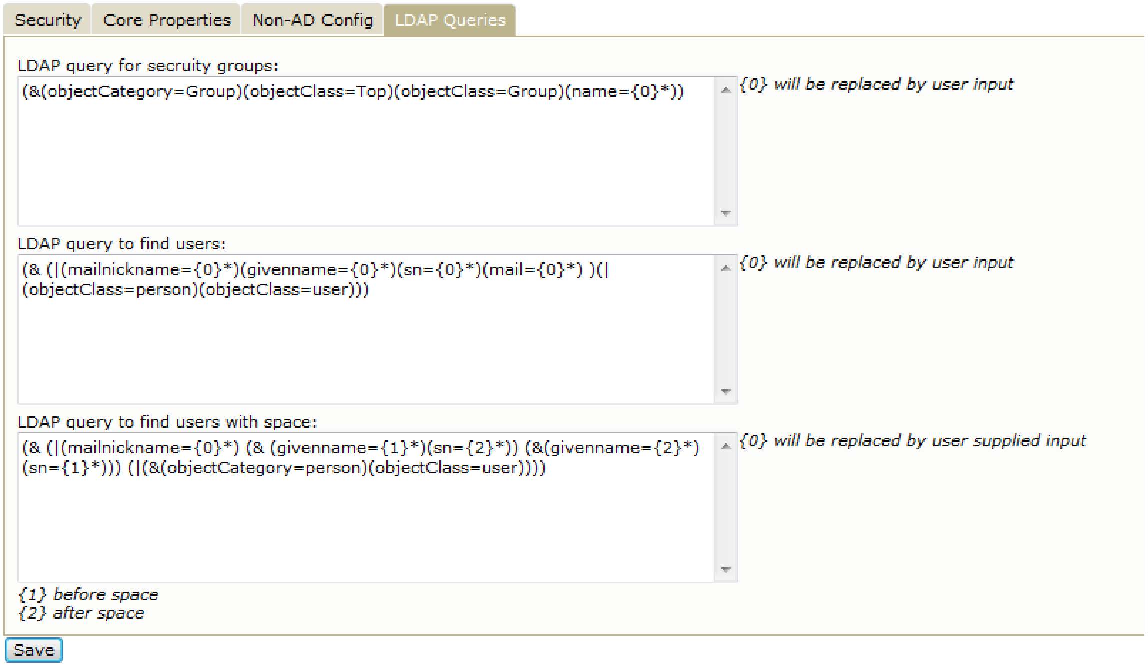
LDAP Group Category: groupOfNames *Example: group (Active Directory), groupOfNames (eDirectory, Domino)*

LDAP Group Name: cn *Example: name (Active Directory), cn (eDirectory, Domino)*

LDAP Group Member Name: member *Example: member (Active Directory, eDirectory, Domino)*

LDAP Group Member User Name Attribute: cn *Example: member="CN=user,O=Domain"*

Figure 1-7: LDAP Queries



LDAP query for secruity groups:

```
(&(objectCategory=Group)(objectClass=Top)(objectClass=Group)(name={0}*))
```

{0} will be replaced by user input

LDAP query to find users:

```
(& (|(mailnickname={0}*)(givenname={0}*)(sn={0}*)(mail={0}*) )(|
(objectClass=person)(objectClass=user)))
```

{0} will be replaced by user input

LDAP query to find users with space:

```
(& (|(mailnickname={0}*) (& (givenname={1}*)(sn={2}*)) (&(givenname={2}*)
(sn={1}*))) (|(&(objectCategory=person)(objectClass=user))))
```

{0} will be replaced by user supplied input

{1} before space
{2} after space

Add LDAP Security Groups to Master Calendar

In the course of setting up LDAP integration within the Master Calendar system, you pair security “templates” defined there with security groups from your network. In order to make groups available for this pairing, you must “add” them to the Master Calendar. To do so, perform the following steps (which are also covered in the *Master Calendar Setup Guide*):

1. Log in to the Master Calendar site as the sites system administrator and select under Admin – Security - User Templates.
2. Click Assign LDAP Groups, and then click Add.
3. Use the Search By to search all LDAP groups or filter by Global Group or Universal Groups. Use the Grouping text box to search a particular string of characters from the list.
4. From the list of LDAP Groups, feel free to use Microsoft Windows multi-select function to highlight group(s). All of the LDAP Groups that are highlighted from the list will be added to Master Calendar once “Add” is selected on the bottom of the Security Group Lookup screen.
5. If a user is in multiple groups, their Master Calendar permissions are based on the template associated with the highest priority group that is assigned. Highlight one or more of the security groups that are listed and use the Move Up ++ / Move Down -- buttons to order the groups in a top – down order.
6. Click Save to save the Security Groups order.

Customer Support

Customer support is available to customers who have a current Annual Service Agreement (ASA). If after reading this document you have questions about configuring your system, contact us at:

Email:	**support@dea.com**
Web:	**www.dea.com**
Phone:	**(800) 288-4565**
Fax:	**(303) 796-7429**

Please have the following information available:

- Name of the organization to which the software is licensed (typically your company).
- Information on any recent problems with, or changes to, your computer or network.