Overview

Active Data Calendar allows for the use of single authentication for users logging into the administrative area of the application through LDAP/AD. LDAP stands for Lightweight Directory Access Protocol which is an application protocol for querying and modifying directory services running over TCP/IP. A directory is a set of objects with attributes organized in a logical and hierarchical manner.

The benefits of using LDAP/AD to authenticate users in the application include the ability to centrally manage updates to passwords and/or users being placed in an inactive state after leaving an organization. Changing information in the source LDAP/AD system means that the Calendar will not allow a user account to authenticate and login once deactivated in LDAP/AD.

Examples of Various Major Directories

Although there are many implementations of directories by other vendors, these are the most commonly used in conjunction with Active Data Calendar. The Calendar is not specifically coded to work with an exact directory but rather uses LDAP as the standard for interacting with different types of directories. As each vendor is able to implement the standard, there may be variations in how a connection to a directory through LDAP is setup. Some directories are extremely strict with the parameters needed to successfully connect while others are much more relaxed with the parameters needed for a connection through LDAP. The major differences are often the “LDAP Unique Identifier” and the “LDAP Server Path”, which are defined in more detail further below.

As the Calendar is a .NET application, it is optimized to work with Windows Active Directory (AD) and the server path is often more flexible than non-Windows directories which require very precise LDAP paths that can be more difficult to identify in creating a successful connection.

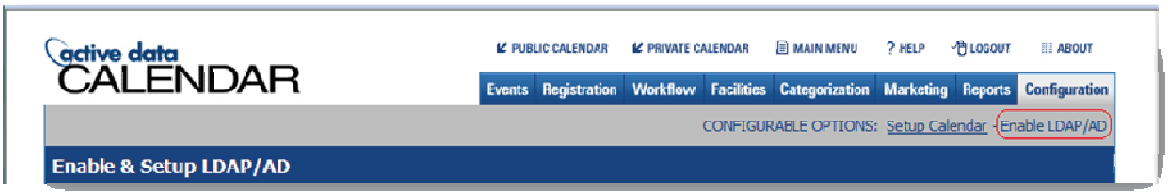
Please contact technical support if you have questions about the directory that your organization uses for user management.

Vendor	Directory
Microsoft	Active Directory
Novell	eDirectory
Sun	Sun ONE

The non-Windows LDAP directories that have successfully connected with Active Data Calendar are as follows: SunOne, Planet LDAP or ATOM.

Super User Account and LDAP/AD

During the installtion of an Active Data Calendar instance a Super User account is created as the first user in the system; it is recommended to not use any credentials that match network credentials but rather set up login information that is unique to the Calendar. The Super User account is the master user account in the system that has global unrestricted rights and is the only account that has access to configure and enable/disable LDAP/AD. This user account is considered native to the application and never validated against Active Directory but rather the database.



Configuring and Enabling LDAP/AD

Once logged in as the Super User, navigate to *Configuration: Enable LDAP/AD*. This screen includes the ability to add an LDAP Server Path and run a test to ensure that the path/connection is working to that LDAP Server. To begin the LDAP/AD Connection setup process, first click the checkbox to "Enable LDAP/AD for Adding User Accounts" and then additional fields will be displayed for completion.

- **Directory Type:** Windows Active Directory or Non-Windows LDAP.
- **LDAP Server Path:** (255 character limit / alpha-numeric)
    - This is an open text field that allows for an LDAP URL to be entered. This URL can point to the ROOT of a directory structure or specific branches of a directory structure.
    - Example value: *LDAP://ldap.mydomain.com:389/dc=mydomain,dc=com*
- **LDAP Filter** (255 character limit - alpha-numeric)
    - **This** is an open text field that allows for a filter to be used when accessing the directory. If only a subset of a directory is to be targeted in the LDAP connection a filter can be entered that narrows any interaction to the objects as defined by the "LDAP Server Path" and the "LDAP Filter".
    - Example value: *(&(objectCategory=person)(objectClass=user))*
- **LDAP Search Base:** There are 3 options for selection: Base, One Level, or SubTree
    - This limits the interaction of LDAP with a directory even further. Applications that modify a directory should be limited in the scope they are allowed to make changes. Limiting scope through these settings can be very helpful in maintaining proper security and limiting negative effects and any possible invalid actions that an application could cause. Additionally, extremely large directories could benefit in limiting the search scope to increase performance when looking through the directory; if it is never needed to search past the base node there is no reason to select OneLevel or SubTree as these would just add unneeded overhead.
        - If "Base" is selected, the search against LDAP will only look through the highest level node in the directory as identified by the "LDAP Server Path".
        - If "OneLevel" is selected, the search against LDAP will only look through the highest level node in the directory and 1 level below the highest node as identified by the "LDAP Server Path".
        - If "SubTree" is selected, the search against LDAP will only look through the highest level node in the directory and all levels below the highest node as identified by the "LDAP Server Path".

- **LDAP Unique Identifier:** (255 character limit - alpha-numeric)
    - When validating user information against a directory the unique value that identifies an object in a directory is needed. This value varies among directories. Note that it is possible for an organization to decide to use a different field as the unique identifier such as an email address. Generally, For windows accounts the login name of a user maps to the directory value of "samAccountName" while in some non-windows implementation the users login name maps to a directory value of "uid".

Type	**Value Used** (**Case Sensitive*)
Windows Active Directory	samAccountName
Non-Windows LDAP	uid

- **Use Secure Sockets (SSL):** There are options for selection: Yes or No
    - If the directory object being validated against has implemented SSL, this value allows for the connection to LDAP to use security. With Windows Active Directory, the "No" value should always be selected even if SSL is required as packets are automatically encrypted through the standard TCP/IP protocol behind the scenes. Other LDAP implementations may or may not need to be explicitly set to the "Yes" value as they may allow for encrypting the LDAP connections through the standard TCP/IP protocol behind the scenes as well. The requirements of this value vary among network setups and implementations and security should be confirmed by using applications that monitor LDAP traffic or by confirming through access logs on the directory server.

Once you have added the all required information on this screen, click the button labeled **SUBMIT**. This button will launch a function window on the right hand side of the screen where you will be prompted to enter:

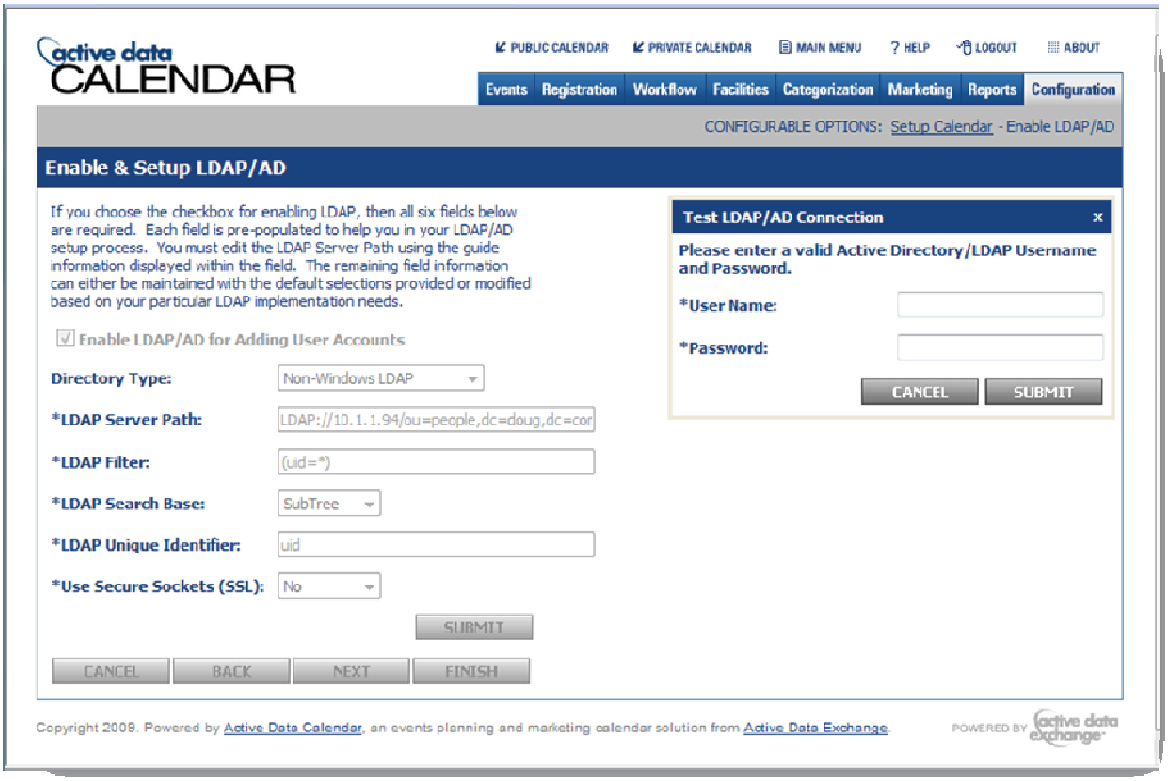
Username: (255 character limit - alpha-numeric) - This is a required field.

Password: (255 character limit - alpha-numeric) - This is a required field.

*NOTE: The username and password supplied can be any valid, active LDAP/AD username and password.

CANCEL: Can be clicked to cancel out of the function window and be returned to the main screen for Enable & Setup LDAP without performing the test.

SUBMIT: Can be clicked to submit your test account information and be returned to the main screen for Enable & Setup LDAP where you will be presented with a confirmation message of the success or failure of your test.



Testing the LDAP/AD Connection

Once you have submitted your test information the software will run a test of the information entered regarding the LDAP connection. You will then see one of two possible messages depending on the success or failure of your test.

If your test was not successful, please change the LDAP Connection information that you have entered and re-run your account test. Otherwise, if you have received a "success message" you must still click the “FINISH” button on the “Enable LDAP/AD” screen to save the LDAP information and finalize the addition of the connection.

Disabling LDAP/AD

If the checkbox for "Enable LDAP/AD" is deselected at any time (after a connection has already been successfully finalized/saved), then any existing account information that has been imported up to that point will be maintained “as is” in the Calendar database. If usernames, passwords, email addresses, etc. are changed, re-enabling LDAP in the future may cause these accounts to be unusable for association reasons.

For this reason, it is highly recommended that all efforts be made to avoid enabling and disabling LDAP repeatedly. As soon as the “Enable LDAP/AD” checkbox is deselected, then the standard “User” navigation buttons are re-enabled and standard user functions can be used from within the Active Data Calendar system.

LDAP/AD Security and Passwords

When a user account attempts to log into the Calendar and enters a password, the user is validated against Active Directory to authenticate and ensure that they are a valid user account and that the

password is correct. If any authentication methods are required by a client that are not currently supported, please contact the Active Data Exchange Professional Services team to discuss any custom enhancements.

Each time the password is checked in LDAP/AD, the Calendar has a process of re-hashing it and storing it in the database in this secure manner to ease any associated security risks. This is done in case LDAP/AD is ever disabled so that a record of the last login information is stored for accounts to continue to login. The password hash code is a one way process meaning that once hashed it cannot ever be undone and there is no way to determine the actual password values.

An example of a hash code that equals “admin12” is “1844156D4166D94387F1A4AD031CA5FA.” Below is a simple SQL script that is provided in case there is a need to reset the Super User information in the database to this known hashed password.

This can also be done by running a simple SQL script against the database as follows:

```
UPDATE Account

SET acct_idn='admin', acct_password='1844156D4166D94387F1A4AD031CA5FA'

WHERE def_org_unit='*'
```

LDAP/AD Required Data

There are 4 pieces of information that are brought in when users are queried in Active Directory to be brought over into Active Data Calendar.

1. First Name
2. Last Name
3. Email
4. Login Name

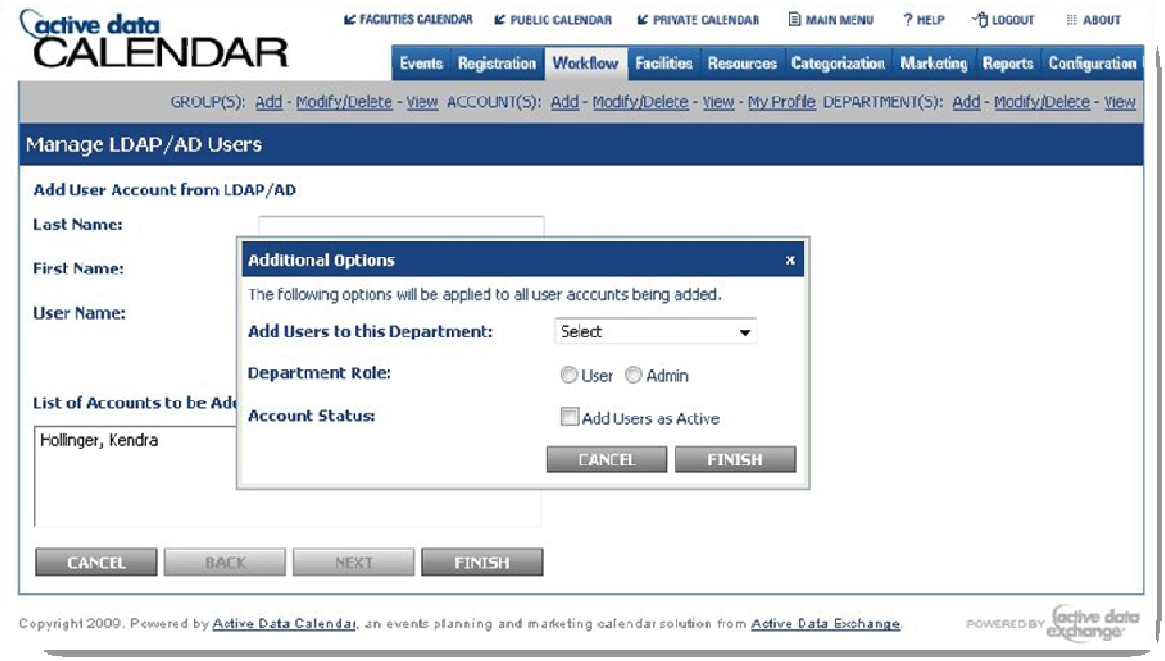
LDAP/AD User Accounts

The application allows for the import of single users from Active Directory into the Calendar. Once you have successfully established a test connection in the LDAP/AD configuration area, you can then go to *Workflow: Accounts: Add* to search for users in Active Directory and copy the users found into the Calendar application.

Please note that bringing users over from LDAP/AD requires a valid and authenticated LDAP/AD account. The authenticated account must have the ability to query Active Directory and pull back user information to be stored in the calendar database. Actually adding the users in Calendar requires the ability to have an LDAP/AD account with proper read permissions.

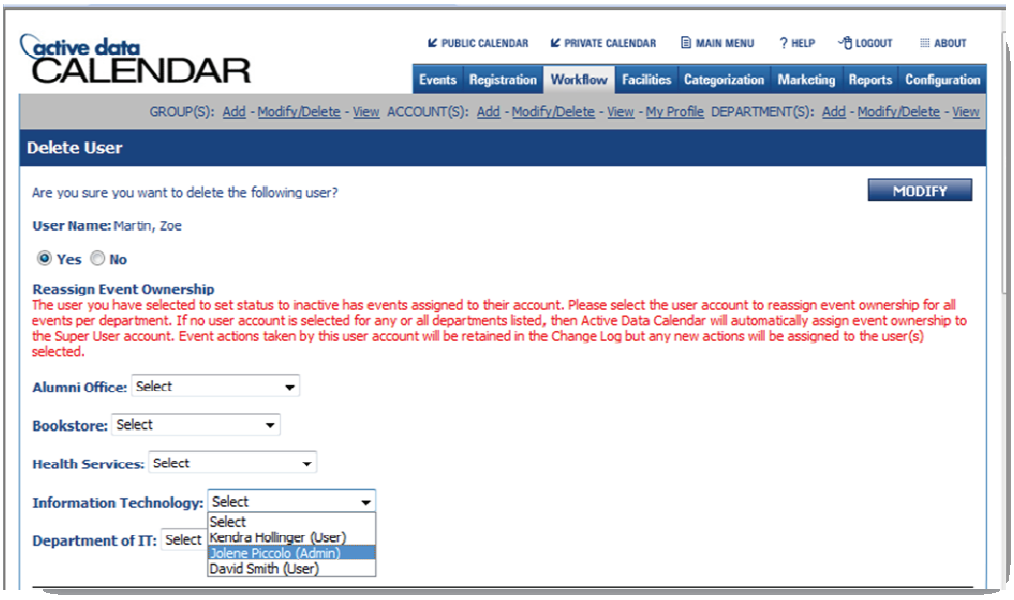
The following occurs when importing users from LDAP/AD:

- The 4 pieces of information noted above are copied from Active Directory and an account is created in the Calendar application.
    - Department permissions and role and account status can then be automatically applied to users as they are brought over to Calendar. A form will be presented at the time of bringing the account over to allow initial assignments to the account which can be modified later by selecting to the modify account process. The same form and process is also presented when adding groups in the Calendar.



At this point the user information stored in Calendar matches the information stored in LDAP/AD. Please note that a user account's username is the unique identifier in LDAP/AD and cannot be modified in the Calendar application since it is authenticated from another system. There is also no longer an ability to modify any of the information on Step 1 of a user account's profile, such as the first name, last name, email, password, etc. Once this information is populated from LDAP/AD, it is recommended to proceed through the rest of the process of setting up application specific permissions for a user account such as department permisions and roles, overall system privleges, category ownership and/or facility ownership (if applicable to a client's installation).

Since the username is a unique identifier for the Calendar, if it has changed for any reason in LDAP/AD then the account will need to be re-added to the Calendar. Once deleted the accounts event ownership will be automatically transferred to the Super User account. In order to continue to maintain the connection of the user's event ownership status, it is recommended to inactivate the account first and then bring in the new user account from LDAP/AD and activate it. Once activated, you can choose to delete the user account and you will be presented with an option to transfer event ownership to any accounts in the system. Please see an example of this below.



LDAP/AD Groups

The application allows for the import of groups from Active Directory into the Calendar. Once you have successfully established a test connection in the LDAP/AD configuration area, you can then go to *Workflow: Groups: Add* to search for groups in Active Directory and then select to import a group into Calendar. This is the only area in Calendar where groups and Active Directory interact.

Please note that bringing groups over from LDAP/AD requires a valid and authenticated LDAP/AD account. The authenticated account must have the ability to query Active Directory and pull back group information to be stored in the calendar database. Actually adding the groups in Calendar requires the ability to have an LDAP/AD account with proper read permissions.

The following occurs when importing groups from LDAP/AD:

1. A group with a name matching the Active Directory group is created in the Calendar application.
2. All user accounts in the Active Directory group are imported into the Calendar
3. All Active Directory users imported are assigned to the group created in the Calendar application.

At this point there is a group name in the Calendar application that matches the group name in Active Directory. Group names can be modified in the Calendar application to be different than the group name stored in Active Directory for business requirement purposes.

Once groups and users are in the Calendar system, it is recommended to proceed through the rest of the process of setting up application specific permissions for the group such as department permisions and roles, overall system privleges, category ownership and/or facility ownership (if applicable to a client's installation). The benefit of using groups is that you can easily apply, modify or remove these application specific permissions in mass to the group. Please note that all of the individual user accounts imported into the group from LDAP/AD can also be modified separately by going to *Workflow: Accounts: Modify*.

Persistent Active Directory Interaction

As of Active Data Calendar v. 3.9.x and all previous versions, there is no persistent interaction between the Calendar application and Active Directory once a user/group is brought into the Calendar from LDAP/AD. If a user is deleted from LDAP/AD they will need to be manually removed in the Calendar.

The Calendar application only checks the following information regarding users attempting to authenticate.

1. The user login name as entered on login must be a valid Calendar account.
2. The user login name as entered on login must validate against Active Directory.

Group assignments in Active Directory do not affect the validity of an Active Directory account. These are only for setting up permissions and associated options on an organization domain. As this sits outside of the scope of the Calendar there is no connection to these account permissions and privileges inside of the Calendar as an application.

For example, a user in Active Directory may be a part of 5 groups when they are first brought into the Calendar application and later on are removed from all 5 groups and assigned to 3 unique, new groups through Active Directory. Although this account is valid inside of Active Directory, the Calendar has no notion of the changes made at the group level and therefore there will be no changes reflected on account/group information in the Calendar application. The original assignments will be retained.

Support

Please contact Product Support at (610)-997-8100 or support@activedatax.com for further assistance.