LDAP-Driven Accounts Using Group Membership

Authentication and assigning users to User Classes can be filter down to their group membership level. This offers greater flexibility with filtering users when they may exist in the same Organization Unit or Container and allows you to grant users to multiple Class Definitions and their assigned payment methods.

Note: the following steps pertain to managing both end-users, as well as users who can be assigned to Administrative Classes and granted various levels of system administration.

Requirements

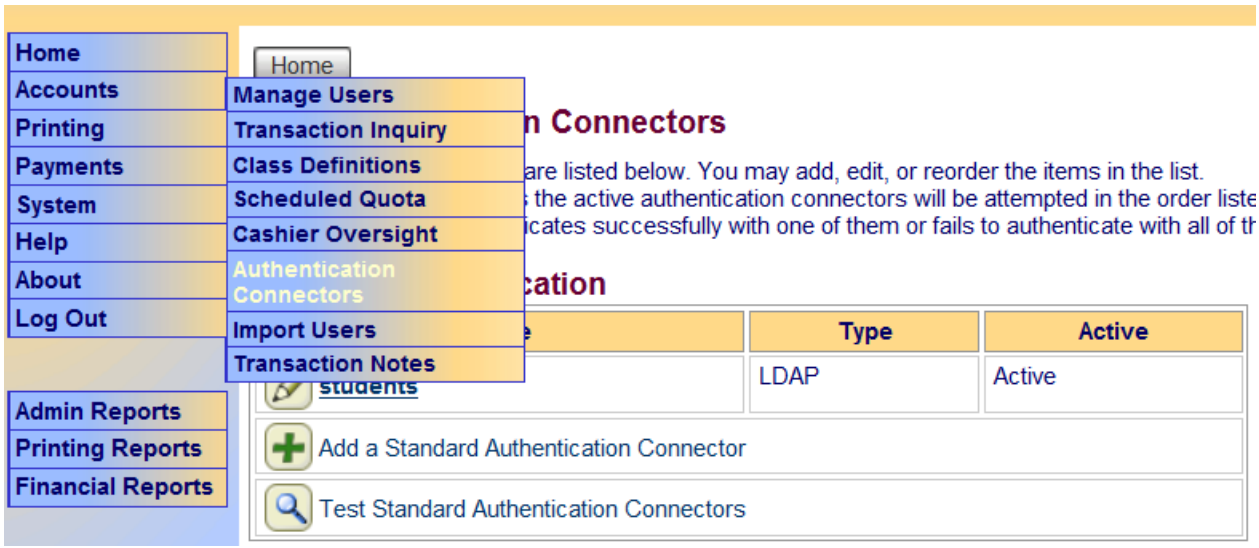
An existing LDAP container must exist and successfully binding. For more information see the section on creating LDAP Authentication Connectors.

For configuration options please refer to the following guides:

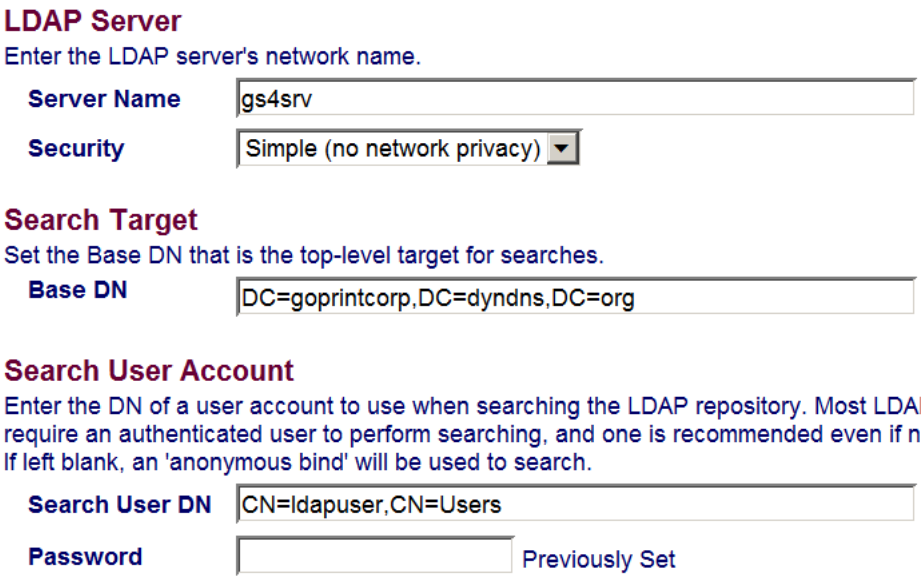
http://www.goprintsupport.com/Active_Directory_LDAP.pdf

http://www.goprintsupport.com/Scheduled_Quota_LDAP_Users.pdf

Accounts – Authentication Connectors:



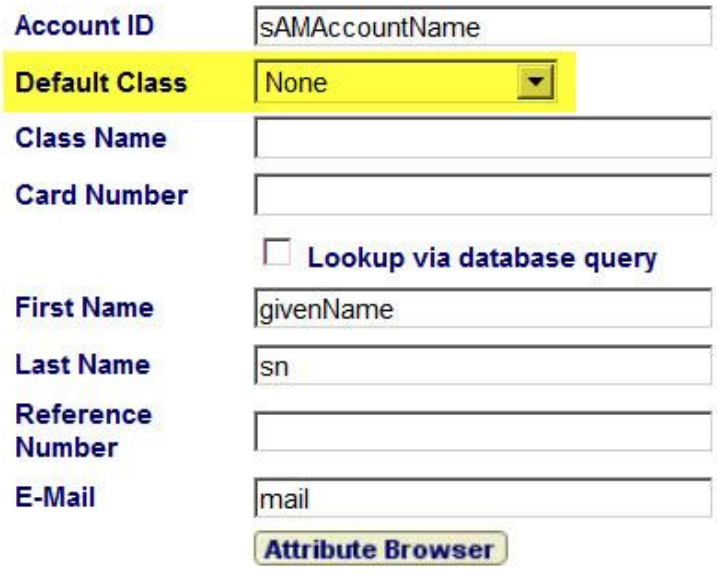
Sample: LDAP Connector



Step 1 – Select **NONE** at the LDAP Connector Attribute section

From the Default Class drop down menu select **NONE**

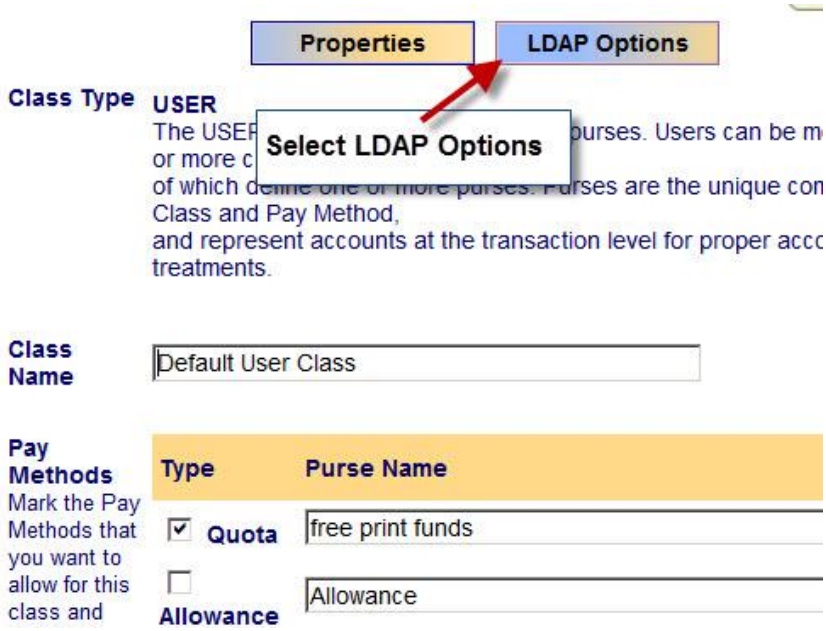
Important: Setting the Default Class level to None forces the LDAP search to first authenticate Users then if a group membership exists at the Class Definition level, then users are granted access to the payment method.



Step 2 – Select LDAP Options

Navigate to Accounts – Class Definitions

Select the desired User Class and select LDAP Options



Step 3 – Enter the corresponding group membership syntax

Option 1 - Group membership Accounts Using Distinguished Names

Every entry in the directory has a distinguished name (DN). The DN is the name that uniquely identifies an entry in the directory. A DN is made up of attribute=value pairs, separated by commas. This is the easiest way to drive Class membership based on data in the LDAP

Simply provide the full DN of the group container that is associated with this Class of users.

Example: When it's not necessary specify a complex memberOf string; you can use the built-in distinguished name of the group. Note: Nestled OU's are supported.

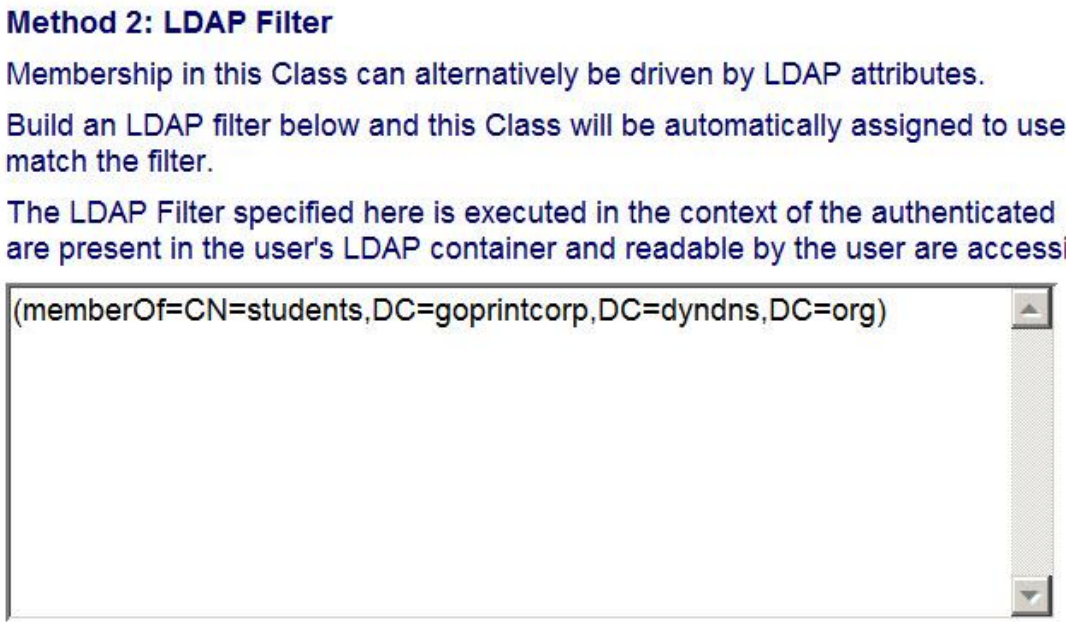
CN=it,OU=staff,DC=goprint,DC=edu
CN=Students,OU=Campus,OU=Groups,OU=Managed,DC=goprint,DC=edu

Option 2 –Group Membership LDAP String using MemberOf Attribute

Note: Each argument must exist in its own set of parentheses. The entire LDAP statement must be encompassed in a main set of parentheses.

Scenario #1 – Single group membership

(MemberOf=CN=students,DC=goprintcorp,DC=dyndns,DC=org)

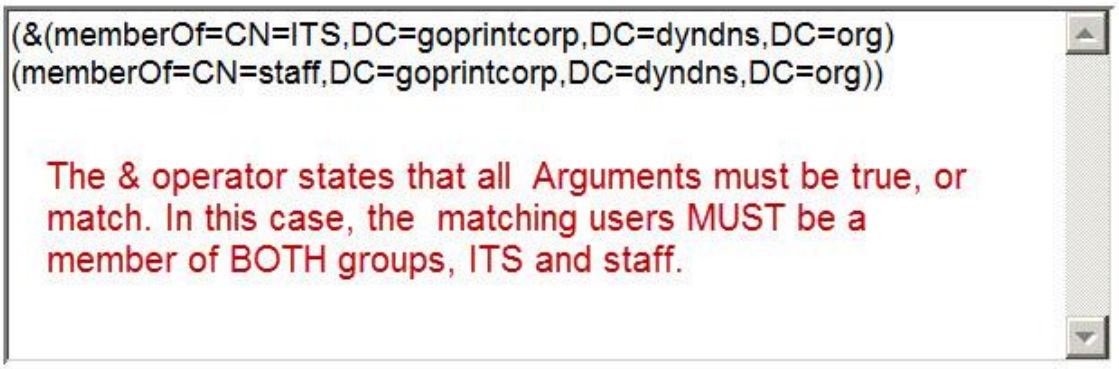


Scenario #2 – Matching Multiple Groups

& (logical AND) - More than one condition, and you want all conditions in the series to be true.

(|(memberOf=CN=medstudents,DC=goprintcorp,DC=dyndns,DC=org)(memberOf=CN=law students,DC=goprintcorp,DC=dyndns,DC=org))

The & operator states that all Arguments must be true, or match. In this case, the matching users MUST be a member of **BOTH** groups, ITS and staff.

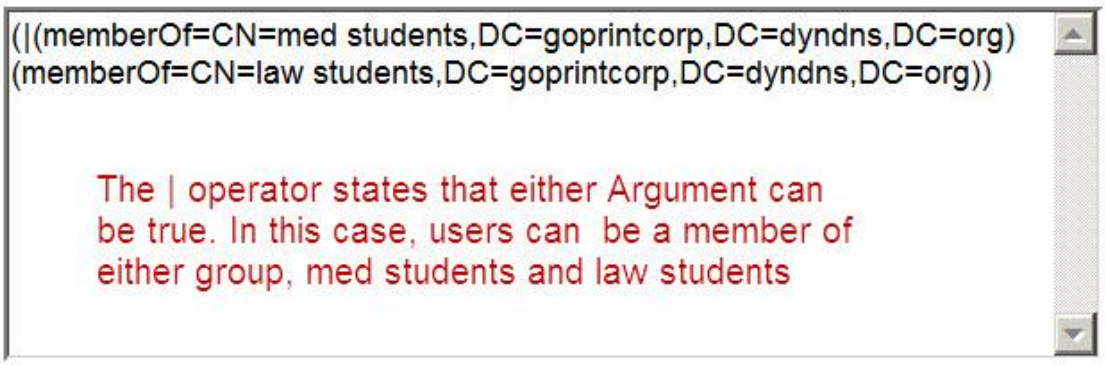


Scenario #3 – Matching Multiple Groups

| (logical or) – either condition is true

(|(memberOf=CN=med students,DC=goprintcorp,DC=dyndns,DC=org)(memberOf=CN=law students,DC=goprintcorp,DC=dyndns,DC=org))

The | Operator states that EITHER Argument can be true. In this case, users can be a member of either group med students or law students.



Scenario #4 – Excluding Multiple Groups

! (logical NOT) - exclude objects that have a certain attribute

(!(memberOf=CN=med students,DC=goprintcorp,DC=dyndns,DC=org)(memberOf=CN=law students,DC=goprintcorp,DC=dyndns,DC=org))

The ! Operator states that the first Argument must be true and NOT the second. In this case, the Argument MUST match the users in the group med students, and exclude users in the group students.