



Active Directory LDAP Configuration

OVERVIEW:

GS-4 incorporates the LDAP protocol to access, (and import into a GS-4 database) Active Directory user account information, such as a student's LoginID, FirstName, LastName, or Card Number to dynamically assign print funds.

This document begins by providing an overview of LDAP functionality to help you become familiar with its many terms and options. The last section, GS-4 Active Directory Integration, guides you through the step by step process of configuring a GS-4 LDAP profile. If you feel comfortable with the LDAP/Active Directory process, you may skip the informational portion and proceed directly to the GS-4 LDAP profile configuration.

What is LDAP

Is a directory service protocol that specifies directory communications. It runs directly over TCP/IP, and it can also run over user datagram protocol (UDP) connectionless transports. LDAP enables clients to query, create, update, and delete information that is stored in a directory service over a TCP connection. LDAP is the preferred and most common means of interacting with Active Directory.

In Active Directory, directory clients use Lightweight Directory Access Protocol (LDAP) to perform searches against the directory. LDAP is defined by Request for Comments (RFC) 3377, "Lightweight Directory Access Protocol (v3): Technical Specification." LDAP is a standards-based protocol that makes it possible for users to query and update information in an LDAP-based directory service, such as Active Directory. To perform Active Directory searches, LDAP-compliant directory clients compose a search query using LDAP syntax and then submit the query to Active Directory for processing.

Distinguished Name

Every object in Active Directory has a distinguished name (also known as DN). A distinguished name uniquely identifies an object by using the name of the object, plus the names of the container objects and domains that contain the object.



Therefore, the distinguished name identifies the object as well as its location in a tree. The distinguished name is unambiguous (that is, it identifies one object only) and unique (that is, no other object in the directory has this name). It contains enough information for an LDAP client to retrieve the object's information from the directory.

For example, a user named Jeff Smith is a graduate student in the school of business for a major university. His user account is created in the grads OU that stores the accounts for graduate students. The root domain of the university is goprint.edu, and the local domain is southcampus.goprint.edu. The distinguished name for this user object is: *cn=Jeff Smith,ou=grads,dc=southcampus,dc=goprint,dc.edu*

Relative Distinguished Name

The relative distinguished name (also known as the RDN) of an object is the part of the distinguished name that is an attribute of the object itself — the part of the object name that identifies this object as unique within a container. For the example in the previous paragraph, the relative distinguished name of the user object:

cn=Jeff Smith,ou=grads,dc=southcampus,dc=goprint,dc=edu

is: *cn=Jeff Smith.*

The maximum length that is allowed for a relative distinguished name is 255 characters, but attributes have specific limits that are imposed by the directory schema. For example, in the case of the common name (cn), which is the attribute type that is often used for naming the relative distinguished name, the maximum number of characters that is allowed is 64.

Searching Active Directory

Searching is the most common directory activity. To complete an LDAP search, a directory client must complete a series of steps, as follows:

- Find an LDAP directory server
- Establish a connection



TECHNICAL WHITE PAPER

- Authenticate against (bind to) the LDAP directory server
- Perform a search

FINDING A SERVER

The first step that a directory client must take in conducting an Active Directory search is to find an LDAP directory server (in other words, a domain controller) to search against. To find a domain controller, directory clients rely on DNS. When a domain controller starts up, it registers service (SRV) records in DNS that indicate that the domain controller provides LDAP directory services. To locate a domain controller, a directory client performs a DNS query for SRV records of hosts that provide LDAP directory services.

ESTABLISHING A CONNECTION

After it finds a directory server, a directory client must next connect to the server. A directory client can connect to an LDAP directory server by opening a session on a TCP port number on which the LDAP directory server is listening. The string that is used to establish the connection includes the fully qualified domain name (FQDN) of the LDAP directory server, along with the TCP port number of the directory server. For standard LDAP searches, directory clients connect to TCP port 389.

AUTHENTICATING - BINDING

After a directory client establishes a communications path to the domain controller, it must bind to the domain controller to establish the logon and authentication credentials and, if necessary for Windows-based computers, set up a secure channel. (A client can also attempt to bind to a domain controller without first establishing a connection.) The bind operation identifies the connecting person, device, or application to the server by providing a distinguished name and some type of authentication credential, such as a password. The exact credentials depend on the authentication method that is being used.

LDAP v3 enables the client to negotiate with the LDAP server to determine the best available security package. If no security package is available, the bind is a simple bind that uses a plaintext password. The Microsoft implementation of the LDAP API uses the NEGOTIATE flag so that the client can discover the best security package



TECHNICAL WHITE PAPER

that is available. For example, a SASL mechanism, such as Kerberos V5 or NTL, might be used.

LDAP BIND REQUEST

The **bind** command initiates a protocol session to the domain controller. After a session is established, a method of authentication is negotiated between the domain controller and the client. By default, Kerberos is used, but other methods can also be used. Finally, the domain controller returns a bind response to the client when the client is authenticated.



Note: If a directory client attempts to bind to a directory server without specifying credentials, an anonymous bind is attempted. Active Directory does not accept anonymous binds by default. However, Active Directory can be configured to accept anonymous binds. For more information, see “Anonymous queries” later in this section.

PERFORMING AN LDAP SEARCH

LDAP searches are the most common LDAP operations that are performed against an Active Directory domain controller. An LDAP search retrieves information about all objects within a specific scope that have certain characteristics.

The following parameters are used in LDAP to accomplish an LDAP search:

- *Search base* (the distinguished name of the search base object). Defines the location in the directory from which the LDAP search begins.
- *Search scope*. Defines how deep to search within the search base:

 - *Base (or zero level)*. Indicates a search of the base object only.
 - *One level*. Indicates a search of objects immediately subordinate to the base object but not the base object itself.
 - *Subtree*. Indicates a search of the base object and the entire subtree of which the base-object distinguished name is the topmost object.

- *Filter*. Allows certain entries in the subtree and excludes others.
- *Selection*. Indicates what attributes to return from objects that match the filter criteria.



Default Active Directory Naming Attributes

Object Class	Naming Attribute Display Name	Naming Attribute LDAP Name
User	Common-Name	cn
organizationalUnit	Organizational-Unit-Name	ou
domain	Domain-Component	dc

Other naming attributes that are described in RFC 2253, "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names," such as o= for organization name and c= for country/region name, are not used in Active Directory.

Common LDAP Search Filters

ObjectCategory - defines the Active Directory Schema category. For example, objectClass = Person

Objectclass - Defines the database schema, specifying which attributes an entry can, and must, include.

objectClass = User. Also used for Computer, organizationalUnit, even container. Important top level container, refers to cn, sn,oid

objectClass vs. objectCategory in a search filter

Sometimes, you might want to search Active Directory for objects of a particular type. For example, you might want to search for Active Directory objects that represent users. You can do this by searching for objects of a particular object class,



using the **objectClass** attribute (objectClass=user). Or, you can search for objects of a particular category, using the **objectCategory** attribute (objectCategory=user). Because of the class inheritance hierarchy in the schema, every object in Active Directory is in fact a member of many classes — four or five, on average. For this reason, searches that use **objectClass** can be less accurate than searches that use **objectCategory**.

For example, a search filter of objectClass=user returns both user and computer objects. On the other hand, **objectCategory** usually refers to the most specific class in the object's class hierarchy. Every Active Directory object has an **objectCategory** attribute whose value is a classSchema object. For example, a search filters of objectCategory=user returns only user objects. Although **objectClass** can have multiple values, the attribute **objectCategory** has only one value.

Subordinate References

When a client requests a search, the domain controller searches all objects at or below the search base in the directory partition that the domain controller holds. If a subtree search has a search base that includes child partitions, the domain controller uses information that is provided by subordinate references to return referrals (called subordinate referrals) to these partitions on other domain controllers.

The search base

Basic root search

Starting a search at the root level of a domain scans the entire directory tree including all subordinate OUs. Using the Active Directory domain "goprint.edu" the base DN may look like: dc=goprint,dc=edu.

Limiting the search

To reduce system overhead and to intentionally exclude or include only a specific group of users you can start the search at the OU level. For example, to start your search at the students OU of the goprint.edu domain you might use a search base as



TECHNICAL WHITE PAPER

follows: **ou=students,dc=goprint,dc=edu**. The AdsPath can use either the LDAP or Global Catalog providers. You would use the GC provider to search for information in other trusted domains, but only attributes replicated to the Global Catalog are available.

The search filter - A clause that specifies the conditions that must be met for records to be included in the resulting recordset. The attribute values for all objects meeting the conditions are included in the recordset.

The syntax of the search filter is explained below. An example to filter for all user objects would be "**(&(objectCategory=person)(objectClass=user))**"

Attributes

By default, the following attributes are members of the ANR attribute set, and are used by the GoPrint GS-4 solution:

- **givenName** (first name)
- **sn** (surname, or last name)
- **displayName** (the name that is given to the object when it is created)
- **RDN** (the relative distinguished name of the object)
- **mail** (email address)

GS-4 Active Directory Integration

To access the GS-4 Active Directory LDAP profile configuration section select:


Accounts – Authentication Connectors






Standard Authentication and the Card Swipe Authentication

GS-4 provides two connector options, Standard Authentication and Card Swipe Authentication. The card swipe authentication is used when the students Login Id is programmed on a university campus card and is used to release print jobs when swiped at a print release station.


Step 1 - Click Add a Standard Authentication Connector

 **Authentication Connectors**
 Authentication connectors are listed below. You may add, edit, or reorder the items in the list. When a user authenticates the active authentication connectors will be attempted in the order listed here, until the user authenticates successfully with one of them or fails to authenticate with all of

Standard Authentication

Name	Type	Active
 Students	LDAP	Active
 Add a Standard Authentication Connector		
 Test Standard Authentication Connectors		

Card Swipe Authentication

Name	Type	Active
No Card Swipe Authentication Connectors have been defined.		
 Add a Card Swipe Authentication Connector		

Select Microsoft Active Directory:

Add a Standard Authentication Connector
 Please select a connector type:



LDAP Server



Microsoft® Active Directory



Novell eDirectory



Step 2 – Enter the Server name and Base DN

LDAP Authentication
Configure user authentication by searching and/or authenticating with LDAP compatible servers. Account attributes can also be loaded from LDAP attributes when the user is authenticated.

Host Info Authentication Attributes

Connector
Name:
 Active

Host Info
Server:

It appears you are setting up a new LDAP Authentication Connector. To get a list of the Base DN's on your LDAP server, enter your LDAP server's name and click the Browse button below. This will work to show your Base DN's as long as your LDAP server supports LDAPv3 and anonymous binds.

Authentication Type: Simple (no network privacy) ▾
Base DN:
 Append Base DN to User DNs

Name: create a user-friendly name to identify the connection type.

Active: click Active

Server: enter the host name of the Active Directory domain controller

Authentication Type: leave default of Simple. To enable SSL authentication the Active Directory schema must be enabled to force secure TLS communication, and the domain SSL certificate must be imported into the GS4\JRE\ keystore. Refer to "Advance Topics" under the GS-4 HELP section for additional information.

SCENARIO 1 – ROOT LEVEL SEARCH

Example domain: **goprint.com**

Base DN: *DC=goprint,DC=com*

Append Base DN to Users DNs:

leaved checked!

Host Info

Server:

Authentication Type: Simple (no network privacy) ▾

Base DN:

Append Base DN to User DNs



Note: Active Directory allows anonymous bind only at the root level. When electing to use any of the Browse options you may receive an error message indicating you must bind before searching is allowed.

Step 3 – Search and Authentication

Method: select Search First, then Authenticate



Caution: The Authenticate Only option does not apply to Windows Active Directory and LDAP under GS-4. The sole goal is to search users and return results. Do not attempt to select Authenticate only

Search Filter: GS-4 provides and recommends using the following default search filter: **(&(objectCategory=person)(objectClass=user)(CN=\${User}))**



Note: you may replace **CN=\${User}** with **sAMAccountName=\${User}** to return the LoginID instead of the Common Name or Display Name.

Host InfoAuthenticationAttributes

Method Authenticate Only Search First, then Authenticate

Search and Authenticate Method

Use an LDAP search filter to perform a search in order to locate the quota account to authenticate with, then a subsequent authentication to verify their password. Substitute \${User} in the filter to indicate where the user's ID should go. The user's ID is what they enter at a PayPoint in order to pay for their print jobs.

Search Filter

Attribute Browser

Some LDAP servers require an authenticated user to perform searching. If yours does, enter a user account that can be used below.

Search User DN

Password Currently Unset



Search User DN

Active Directory requires an authenticated user to perform searching. In the majority of cases, a standard user account has sufficient Read rights to perform a search.



Caution: to ensure a successful bind and directory search, it's important to follow the following examples carefully.

Option 1 - Authenticated User lies within the Built-in Users container

If the authenticated user account is found under the Active Directory built-in "Users" container, (Hint: the Users container is NOT regarded as an OU) then you are required to reference the Users container with the CN attribute.

Example: **cn=goprintldap,cn=Users**

Some LDAP servers require an authenticated user account that can be used below.

Search User DN	<input type="text" value="cn=goprintldap,cn=Users"/>
Password	<input type="text"/> Previously Set

Option 2 - Search User lies within a specific OU

If the search user is located under a specific OU then you must include the OU. In the following example the search user is located in the Library OU

Example: **cn=goprintldap,OU=Library**

Some LDAP servers require an authenticated user account that can be used below.

Search User DN	<input type="text" value="goprintldap,OU=Library"/>
Password	<input type="text"/> Pre

Step 4 - Attributes

GS-4 automatically provides the required attributes you will need to successfully import users:

Account ID: use CN or sAMAccountName

Class Name: optional

Default Class: specify the User Class (refer to the GS-4 Quota section on applying User Classes)

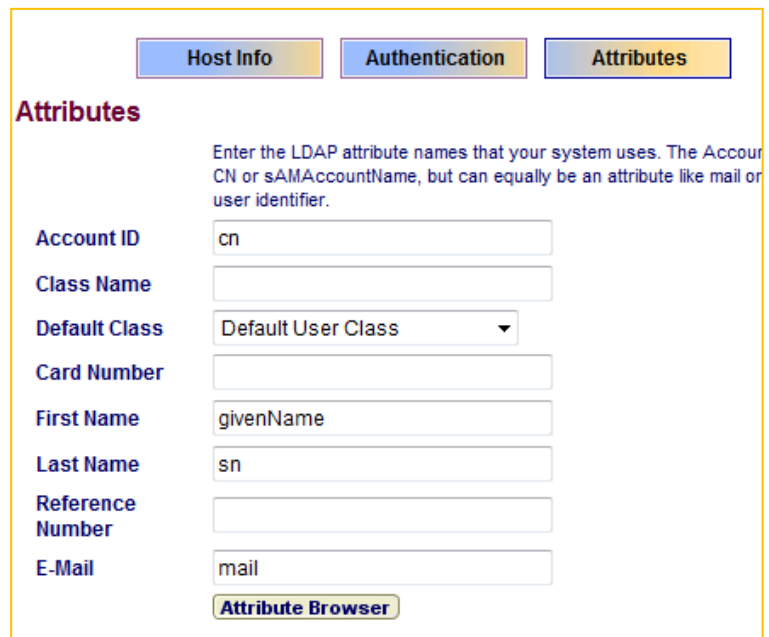
Card Number: optional. Used with 3rd party transaction systems

FirstName: givenName

LastName: sn

Reference Number: optional

E-Mail: Optional



Attribute Browser: Clicking the attribute Browser will return the default system attributes.



Note: UserPrincipalName attribute is not supported

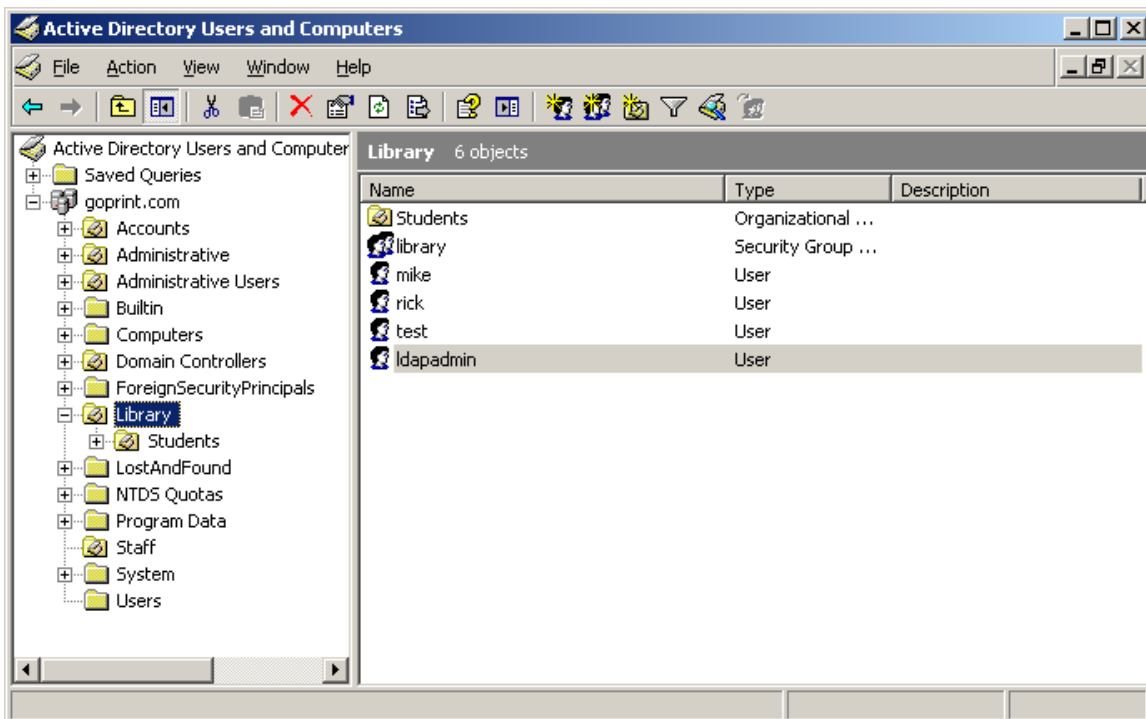
SCENARIO 2 - BASE DN – STARTING A SEARCH AT THE OU LEVEL

When searching extremely large directory trees, to enhance performance, you may want to begin your search at the OU level. Starting a search at a specific OU also grants you the ability to include only a select member of users, beneficial when it's desired to grant different print quota to a select group of users.

In our example, we begin our search at the Library OU:



Note: Starting a search at the OU level also searches ALL subordinate subtrees.



STEP 1 – SET THE BASE DN: OU=LIBRARY,DC=GOPRINT,DC=COM

Host Info

Server:

Authentication Type:

Base DN:

Append Base DN to User DNs

STEP 2- SPECIFY THE AUTHENTICATED USER ACCOUNT



Note: When setting a Base DN at the OU level, for easy management, it's recommended to also have the search user account within the same OU.



TECHNICAL WHITE PAPER

Since the search user account is located in the base OU, (in this example, the library OU) you only need to reference the CN name and not the OU.

Example: `cn=ldapadmin`

a user account that can be used below.

Search User DN	<input type="text" value="cn=ldapadmin"/>
Password	<input type="text" value="Previously Set"/>

When the authenticated user account is located in different OU

If campus security restrictions require placing the authenticated user in a different OU other than what is specified in your Base DN, then you must initiate the following changes.

If your search user is located in a different OU outside your search path, then you MUST:

1. uncheck Append Base DN to Users DNs
2. provide the search user's complete distinguished name

Host Info

Server	<input type="text" value="goprnsrv"/>
Authentication Type	<input type="text" value="Simple (no network privacy)"/>
Base DN	<input type="text" value="OU=Library,DC=goprint,DC=com"/>
	<input type="checkbox"/> Append Base DN to User DNs

In the example the `goprintldap` user is located under the ITS OU, a subtree of the staff OU. The Search User DN field would appear as:

`cn=goprintldap,ou=ITS,ou=staff,dc=goprint,dc.edu`

a user account that can be used below.

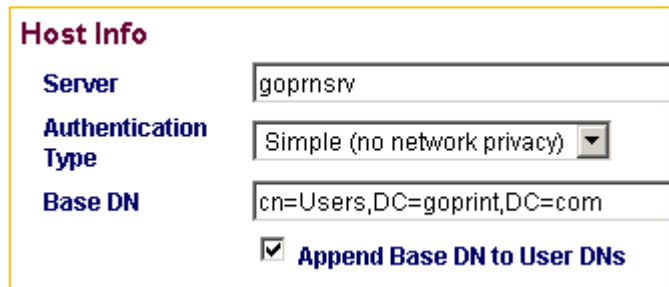
Search User DN	<input type="text" value="rs,DC=goprint,DC=com"/>
Password	<input type="text" value="Previously Set"/>

SCENARIO 3 – SEARCHING ONLY THE DEFAULT USERS CONTAINER

You can also start your Base DN to search only the Default Users container.

The trick is, is to reference the Users container using the CN attribute. Example:

cn=Users,DC=goprint,Dc=com



The screenshot shows a configuration form titled "Host Info". It contains the following fields and options:

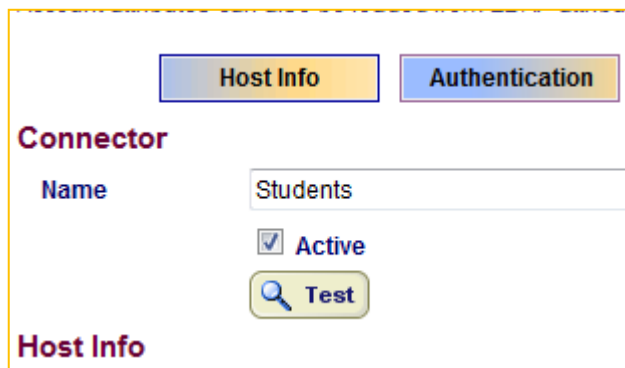
- Server:** goprnsvr
- Authentication Type:** Simple (no network privacy) (dropdown menu)
- Base DN:** cn=Users,DC=goprint,DC=com
- Append Base DN to User DNs**

This scenario is beneficial if numerous LDAP profiles are desired to enable multiple print quotas based on OU level and the Users container.

Testing your LDAP Connection String

You can run a connection test using the connector Test utility to ensure your LDAP settings are correct.

Click the Test button



The screenshot shows a "Connector" configuration window with two tabs: "Host Info" and "Authentication". The "Host Info" tab is active. The form contains:

- Connector Name:** Students
- Active**
- Test** button (with a magnifying glass icon)

Below the form, the "Host Info" section is partially visible.



Authentication Test

Enter a username and password located in the search filter path

Click: Test

Authentication Test
 Here you may test an authentication profile setting. Select which authentication profile to test and enter a username/password to test with.

Authentication Profile:

Username:

Password:

A successful query returns the following results:

Test Result	Successful				
	NOTE: This is only a test. An account has not been created.				
Using Connector	Students				
Connector Type	LDAP				
User ID	steve				
First Name	steve				
Memberships	<table border="1"> <thead> <tr> <th>Class Name</th> <th>Class Type</th> </tr> </thead> <tbody> <tr> <td>Default User Class</td> <td>USERS</td> </tr> </tbody> </table>	Class Name	Class Type	Default User Class	USERS
Class Name	Class Type				
Default User Class	USERS				

Troubleshooting Bind and searching Issues

Whenever an unsuccessful test result is generated, to troubleshoot, it's important to understand how the search and authenticate process is initiated. The best point of reference is the GS-4 **RUN.log** file found under [\\GS4\Logs](#).

A successful Bind and Search

A search attempt first looks for the authenticated user. If successful, the LDAP Auth users Distinguish name is returned as follows:

] LDAP Auth for CN=goprintldap,CN=Users,DC=goprint,DC=com



Once authenticated an attempt is made to find the specific User entered during the test. In this case, a successful attempt was made to find the user Steve under the IT Staff OU.

```
2008-11-17 16:07:28,265      DEBUG      [btpool1-4:ldap.LDAPConnector  
]      LDAP Auth for CN=Steve,OU=IT STAFF,DC=goprint,DC=com
```

Failed to find authenticated user

An error code 525 is returned when the account cannot be found. The results could be caused by a number of things:

- The authenticated user account is not located in the search path
- Authenticated username may be misspelled
- DisplayName may be required
- Incorrect search filter path
- typos exist
- Incorrect servername was provided.

```
] LDAP authentication for
```

```
CN=goprintldap,cn=Users,DC=goprint,DC=com failed: [LDAP: error code 49 -  
80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data  
525, vece ]
```

Wrong password provided by authenticated user

Incorrect passwords are represented by a 52e error

```
LDAP authentication for CN=goprintldap,CN=Users,DC=goprint,DC=com failed:  
[LDAP: error code 49 - 80090308: LdapErr: DSID-0C090334, comment:  
AcceptSecurityContext error, data 52e, vece ]
```

525 - user not found

52e - invalid credentials



Authenticated user and end-user accounts are found but invalid password was entered by the end-user. Note the 52e error below

LDAP Auth for CN=goprintldap,CN=Users,DC=goprint,DC=com

User account Fred is found but an error 52e is returned, representing invalid credentials were entered.

2008-11-20 01:00:43,609 INFO [btpool1-3:ldap.LDAPConnector] LDAP authentication for CN=fred,CN=Users,DC=goprint,DC=com failed: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data 52e, vece]

End user account does not exist

LDAP Auth for CN=goprintldap,CN=Users,DC=goprint,DC=com

2008-11-20 01:23:06,562 DEBUG [btpool1-3:authentication.AuthenticationManager] Authentication failed: null







javax.naming.PartialResultException [Root exception is javax.naming.CommunicationException: goprint.com:389 [Root exception is java.net.SocketTimeoutException: connect timed

LDAP Advanced Scenario's

Multiple LDAP profiles may be created when necessary to grant different quota amounts based on a user's status such as, credit hours, undergraduate, graduate or department.



Note: GS-4 searches the top most profile first and moves downward until a match is established.

Standard Authentication			
Name	Type	Active	Order
 Utah Law Students	LDAP	Active	
 Utah Law Grad student quota	LDAP	Active	
 Add a Standard Authentication Connector			
 Test Standard Authentication Connectors			



GS-4 Administrator Users and LDAP

Depending on the Base Search filter, you can assign a user to a specific GS-4 Admin Class based on domain group membership using the MemberOf string.

Class Name	<input type="text" value="Library Staff"/>			
Permissions Mark the permissions that you want to allow for this class.	Feature	Permission	Feature	Permission
	System Policy	<input type="text" value="Not Specified"/>	GoPrint Users	<input type="text" value="Read Only"/>
	Admin Users	<input type="text" value="Not Specified"/>	PayStation	<input type="text" value="Not Specified"/>
	Web Client	<input type="text" value="Not Specified"/>	PayPoint	<input type="text" value="Not Specified"/>
	DepositStation	<input type="text" value="Not Specified"/>	Pricing	<input type="text" value="Not Specified"/>
	Rules	<input type="text" value="Not Specified"/>	Agents	<input type="text" value="Not Specified"/>
	Print Job Control	<input type="text" value="Not Specified"/>	Reprint Archive	<input type="text" value="Not Specified"/>
	Journal Entry	<input type="text" value="Not Specified"/>	Non Financial Reports	<input type="text" value="Not Specified"/>
	Financial Reports	<input type="text" value="Not Specified"/>	System Admin	<input type="text" value="Not Specified"/>
	Admin From PayStation	<input type="text" value="All Access"/>	User Quota Refunds	<input type="text" value="All Access"/>
	Printer Catalog	<input type="text" value="Not Specified"/>	Cashier Role	<input type="text" value="All Access"/>
	Payment Connectors	<input type="text" value="Not Specified"/>	NetLink	<input type="text" value="Not Specified"/>

Example: (memberOf=cn=library,OU=Library,DC=goprint,DC=com)

LDAP Filter Build an LDAP filter if you want this class to be automatically assigned to users when they log in, for the duration of that login session.	<input type="text" value="(memberOf=cn=library,OU=Library,DC=goprint,DC=com)"/>
---	---

LDAP Group Membership and Print Rules

Owner Rule

Note: the user name in the Spool file has to match the user name

Reference in the memberOf string under the specific path

Assume Allowed on LDAP Failure

Source of Groups LDAP: Grad student quota ▼

Group Names (&(memberOf=cn=library,OU=Library,DC=goprin'

String





MUST contain reference to: (cn=\${User}))

Example:

(&(memberOf=cn=library,OU=Library,DC=goprint,DC=com)(cn=\${User}))

Make sure to assign the Owner Rule to the Base Pricing Section of the Price Sheet

Pricing

Action	Rule	Price	Time
	Base Price	0.10 per page	Always
 	UCSF	1.00 per page	Always
			



Optionally operators used to refine searches:

Operator	Description
=	Equal to
~=	Approximately equal to
<=	Lexicographically less than or equal to
>=	Lexicographically greater than or equal to
&	AND
	OR
!	NOT

The network ports that are used by Active Directory searches are listed in the following table.

Port Assignments for Active Directory Searches

Service Name	UDP	TCP
LDAP	None	389
LDAP SSL	None	636
Global Catalog LDAP	None	3268
Global Catalog LDAP SSL	None	3269



Additional LDAP Resources

LDAP Query Policy

LDAP v3 supports the definition of client query policy. By default, limits are placed on the server resources that are available to clients requesting LDAP queries, paged result sets, and sorted result sets. These limits constitute the LDAP query policy.

The query policy is stored as a multivalue attribute (**IDAPAdminLimits**) of the Default Query Policy object in the configuration directory partition

(cn=Default Query Policy,cn=Query-Policies,cn=Directory Service,cn=Windows NT,cn=Services,cn=Configuration,dc=Forest RootDomain).

Because the workload and resources of a given server can vary, the LDAP query policy is configurable at the server level.

LDAP query policy applies to the following LDAP query–related operations:

- Search. The basic query operation. An LDAP search might cover a small part of a single domain, or it might span every directory partition in the forest. A search can generate a significant amount of disk activity, take a long time, and return a large volume of data.
- Search with Paged Results. Because a search can return a large volume of data, the client can ask the server to hold the result set and return it in “pages” of a specified length. The server must hold the result set until the client releases it or unbinds.
- Search with Sorted Results. A client can request a result set in a particular order. Sorting requires storage and CPU cycles at the server. The resources consumed are directly proportional to the size of the result set.
- Search with Replication. The administrator can specify the maximum number of attribute values that can be returned per request.
- Change Notify. A client can request change notification on particular objects in the directory. The mechanism that is used to post a Change Notify request is the asynchronous LDAP query.



TECHNICAL WHITE PAPER

In the absence of any other assigned policy, all domain controllers use the default query policy. If a site policy is assigned, the domain controller uses the site policy. If a specific policy has been assigned to a domain controller, this policy takes precedence over any site policy.

The following table shows the administrative limits for default query policy.

Default Values for LDAP Administrative Limits

LDAP Administrative Limits	Default Value	Description and Search Behavior
MaxConnIdleTime	900	Maximum Connection Idle Time. The maximum time (in seconds) that the client is allowed to be idle before the connection is closed.
MaxActiveQueries	20	Maximum Active Queries. The maximum number of concurrent search operations allowed on the server. When the stated limit is reached, the LDAP server returns a busy notification.
MaxNotificationPerConn	5	Maximum Notifications per Connection. The maximum number of concurrent notification requests allowed per connection on the server. When the stated limit is reached, the server returns a busy notification.
MaxPageSize	1000	Maximum Page Size. The largest page size allowed by the server (in number of rows). The server returns the number of rows that are specified by MaxPageSize . If paged results are requested, the client can retrieve additional pages until all results are



TECHNICAL WHITE PAPER

		returned.
MaxQueryDuration	120	Maximum Query Duration. The maximum elapsed time (in seconds) that is allowed for a query to complete. If paged results are requested, the client can continue the query if the timer expires before the query completes. When the stated limit is reached, the server returns the timeLimitExceeded error.
MaxReceiveBuffer	10485760	Maximum Receive Buffer. The maximum LDAP request size (in bytes) that the server attempts to process. If the server receives a request that is larger than this value, it closes the connection.
MaxTempTableSize	10000	Maximum Temporary Table Size. The upper limit (in candidate objects) on the temporary table. If the temporary table maximum limit is reached by an "OR" query optimization, the optimization is abandoned and replaced with a direct table scan.
MaxResultSetSize	262144	Maximum Result Set Storage. The maximum storage (in kilobytes (KB)) that the server can hold for all paged result sets. If the stated limit is reached, the oldest result sets are discarded.
MaxPoolThreads	4	Per Processor Asynchronous Thread Queue (ATQ) Threads. The number of threads that are allocated by ATQ per processor. This value is sent as an advisory notification to ATQ. ATQ



TECHNICAL WHITE PAPER

		<p>decides whether to use it or not.</p> <p>Note If it takes a long time to bind, increase the count to 6 or 8.</p>
MaxDatagramRecv	1024	Maximum Receive Datagram Size. The maximum size of datagrams (in bytes) that can be received by the server. The server preallocates datagram buffers and cannot receive datagrams with a size that is larger than the stated limit.
InitRecvTimeout	120	The maximum time (in seconds) that the server waits for the initial request before the connection is dropped.
MaxConnections	5000	The maximum number of concurrent LDAP connections allowed on the server. User Datagram Protocol (UDP) connections do not count toward this limit. If the limit is reached, the LDAP server sends back an LDAP disconnect notification and closes down the connection.
MaxValRange	1500	Maximum Value Range. Controls the threshold at which the server will start returning the range option for attributes with a large number of values. The minimum value for this policy is 30.



Query Limits

To improve the query response time for searches for Active Directory objects, searches are limited to 1,000 objects by default. However, you may want to increase this limit as your organization grows. You can control the buffer size that is allocated for storing the number of objects that are returned by a query search. To control the buffer size, you can either modify the registry on the search client or use Group Policy to set the buffer size on all computers in a domain, site, or OU.

Modifying the registry to change the maximum query limit

You can increase the number of objects that are returned by an Active Directory search on an individual search client by setting the limit in the registry. The **REG_DWORD** value named **QueryLimit** on the registry key **HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Directory** controls the maximum query limit on the local computer.

Using Group Policy to change the maximum query limit

You can use Group Policy to increase the maximum query limit on objects that are returned in response to a command to browse or search Active Directory when the command is issued from an operating system in the Windows 2000 Server family or the Windows Server 2003 family. In the User Configuration section of Group Policy, the setting is found in \Administrative Templates\Desktop\Active Directory\Maximum size of Active Directory searches. You can edit this setting with Group Policy Management Console (GPMC).

Note

- Because this query limit policy is a user-based policy, it is not enforced until the user has logged off the system and then logged on again. Also, the policy only applies to default Active Directory tools, such as Active Directory Users and Computers. Any query limits that are set through Group Policy do not apply to LDAP queries that are performed programmatically

Global Catalog Searches

The global catalog enables searches for Active Directory objects in any domain in the forest, without the need for subordinate referrals. Users can find an object of interest quickly without having to know which domain holds the object.

Global catalog servers

A global catalog server is a domain controller that stores extra information. The database on the global catalog server stores information about every object in the forest, instead of information for the objects in only one domain. The information about objects that occur in directory partitions for domains other than the local domain includes only a subset of attributes for each object. In this way, the global catalog enables forest-wide searches without requiring replication of the entire contents of Active Directory to every domain controller. The Knowledge Consistency Checker (KCC) process creates a replication topology that ensures delivery of the partial contents of every directory partition to every global catalog server in the forest.

Note

- A global catalog server stores full copies of the schema and configuration directory partitions, which is the same as for any domain controller.

By default, the server on which you install Active Directory to create the first domain in a new forest is a global catalog server. Thereafter, you must designate additional global catalog servers if you need them.

Searching the domain vs. searching the global catalog

The decision whether to search the domain or the global catalog is based on the scope of the search:

- When the scope of a search is the domain or an OU, the query can be resolved in the domain directory partition by using an LDAP search.
- When the scope of a search is the forest and the attributes that are being searched against are part of the global catalog, the query can be resolved in any directory partition by using a global catalog search.



TECHNICAL WHITE PAPER

Searches that use the global catalog by default

To search the global catalog, instead of the local domain partition, you must specify port 3268 in the search tool that you are using, instead of port 389, the standard LDAP port. Anytime that you specify port 3268, you are searching in the global catalog. In addition, the global catalog is searched by default under the following conditions:

- During the logon process, when a user principal name (UPN) is presented. The global catalog is searched to find the domain and account name on the basis of the UPN.
- During the logon process, to expand universal groups. Universal group membership can span domains. It is possible, therefore, that a user has a membership in a universal group that is not in the logon domain. For this reason, the global catalog is contacted to search the membership of universal groups. If a membership is found, the group is attached to the user's logon credentials.
- When you select **Entire Directory** in a search-scope list in an Active Directory tool, such as Active Directory Users and Computers.
- When you write the distinguished name value for a property, where the distinguished name represents a nonlocal object. For example, if the member that you are adding is from a different domain, the global catalog is used to verify that the user object that is represented by the distinguished name actually exists.

Global catalog search base

For an LDAP search, you must supply a valid search base. For a global catalog search, the search base can be any value, including the value NULL (). A search base of NULL effectively scopes the search on the search computer to the global catalog. If you use a NULL search base with a scope of one level or subtree and specify port 389 (the default LDAP port), the search fails. Therefore, if you submit a NULL search to the global catalog port and then change the port to the LDAP port, you must change the search base for the search to succeed.



Characteristics of a global catalog search

The following additional characteristics differentiate a global catalog search from a standard LDAP search:

- A global catalog search crosses directory partition boundaries. The extent of an LDAP search is the directory partition.
- A global catalog search does not return subordinate referrals. If you use port 3268 to request an attribute that is not in the global catalog, you do not receive a referral to it. Subordinate referrals are an LDAP response. When you query a server over port 3268, you receive global catalog responses, which are based solely on the contents of the global catalog. If you query the same server over port 389, you receive referrals for objects that are in the forest but whose attributes are not referenced in the global catalog.

Anonymous queries

By default, anonymous LDAP operations to Active Directory, other than rootDSE searches and binds, are not permitted in Windows Server 2003. (Active Directory in Windows 2000 Server accepts anonymous requests; a successful result depends on objects having correct user permissions in Active Directory.)

To enable anonymous binding to Active Directory in Windows Server 2003, you must change the seventh character of the **dsHeuristics** attribute on the following directory object:

CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,Root domain in forest

Valid values for the **dsHeuristics** attribute are **0** and **2**. By default, the **dsHeuristics** attribute does not exist, but its internal default is **0**. If you set the seventh character to **2**, anonymous clients can perform any operation that is permitted by the access control list (ACL). If the attribute is already set, do not modify any bits in the **dsHeuristics** string other than the seventh bit. If the value is



not set, make sure that you provide the leading zeros up to the seventh bit. You can use Adsiedit.msc to make the change to the **dsHeuristics** attribute.

After you set the **dsHeuristics** attribute, if you want anonymous users to be able to query Active Directory, you can enable anonymous access to specific directory objects. Users gain anonymous access to Active Directory objects through Anonymous Logon, which is a special security identifier (SID) that is used to represent anonymous network callers that perform an LDAP bind with NULL credentials.