

SERVICENOW

LDAP INTEGRATION



REVANTH KARRA
ServiceNow Integrations | ITOM

 [revanth-karra](#)
 karrarevanth325@gmail.com
 Hyderabad, India

ServiceNow LDAP Integration

What is LDAP?

Lightweight Directory Access Protocol (LDAP) is a protocol that helps applications find and access information about users, groups, and other resources in a network.

How?

Imagine that you have a large company with hundreds of employees. Each employee has a name, email address, phone number, and other information. You could store this information in a spreadsheet, but that would be difficult to manage and keep up to date. A better solution would be to use a directory service, such as LDAP. LDAP would store all of the employee information in a central location. Any application that needs to access this information could then query the LDAP directory.

Example:

When an employee logs in to their computer, the computer could query the LDAP directory to verify their identity and grant them access to their resources. Similarly, when an employee tries to print a document, the printer could query the LDAP directory to see if the employee is authorized to use it.



Pre-requisites:

- You must have an LDAP server. This can be a commercial LDAP server, such as Microsoft Active Directory, or an open source LDAP server, such as OpenLDAP.
- You must have a network connection between the LDAP server and the applications or services that will be using it.
- You must have the necessary permissions to configure and manage the LDAP server, user, accounts and groups.

TIPS:

- Make sure that your LDAP server is properly configured and secured.
- Use strong passwords for all LDAP user accounts.
- Regularly back up your LDAP server data.
- Have a plan in place for recovering from an LDAP outage.

For this Demo, I'm going to use Public Open Source LDAP (FORUM SYSTEMS)

Link: <https://www.forumsys.com/2022/05/10/online-ldap-test-server/>



- We can get all the LDAP server Information here.
- This is a Public Open Source URL, which we can test in our Instance.

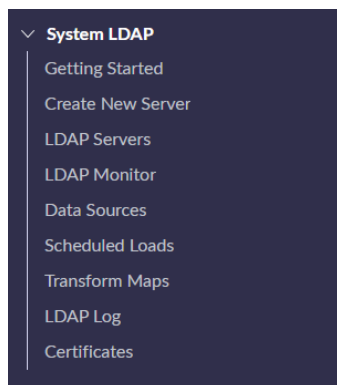
NOTE:

We only have read-only access to this LDAP server.

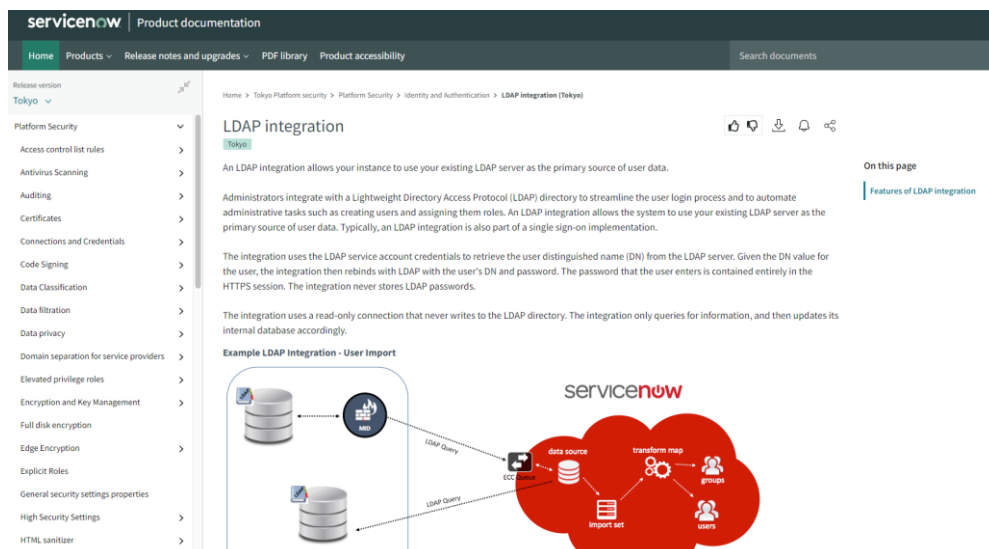
Let's get started!

Initially, let us check all the modules present in this System LDAP

- For LDAP server, we have module in ServiceNow known as System LDAP



- If we click on Getting Started, we will redirect to LDAP product documentation by ServiceNow.



- If we click on Create New Server, we can see new LDAP Server record.

New LDAP Server

Create a new LDAP server record

Provide the basic information below and we will create the LDAP configuration records to get you started.

Type of LDAP server

☒ Active Directory

☐ Other

Server name

More information

Server URL

More information

ldap://host-name:389/

Starting search directory

More information

Submit

- If we click on LDAP Servers, it will show us all the LDAP Servers configured in our instance.

LDAP Servers				
Name	Server URL	Login distinguished name	Login password	Starting search directory
Search	Search	Search	Search	Search

- If we click on LDAP Monitor, which shows the status of our LDAP whether it is connected or down or not connected. At present I don't have any active LDAP Server.

No active LDAP servers to monitor

- If we click on Data Sources, we can see Data Sources in this record and these data sources are for Import.

Data Sources		
Name	Type	Format
Search	=LDAP	Search
Example LDAP Users	LDAP	
Example LDAP Groups	LDAP	

- Basically, LDAP is being used to import Users and Groups of your organization. So, in your AD if you want to import some of your users and groups. You can use LDAP.
- Now let's go to schedule loads, if we need to run our scheduled imports. We can do it from here.

Scheduled Data Imports			
Name	Run	Data source	Active
Search	Search	Search	Search
Example LDAP Group Import	Daily	Example LDAP Groups	false
Example LDAP User Import	Daily	Example LDAP Users	false

Let's Create a new LDAP Server record

< New LDAP Server

Create a new LDAP server record

Provide the basic information below and we will create the LDAP configuration records to get you started.

Type of LDAP server

☒ Active Directory

☐ Other

Server name

More Information

Server URL

More Information

ldap://host-name:389/

Starting search directory

More Information

Submit

- Let's make Active Directory option as default, Give a server name (example.: Test Server for Demo)
- For Server URL, let's go to our Online LDAP Test Server website. Our Server URL is *ldap.forumsys.com*

LDAP Server Information (read-only access): Server: *ldap.forumsys.com* Port: *389* Bind DN: *cn=read-only-admin,dc=example,dc=com* Bind Password: *password*

All user passwords are *password*. You may also bind to individual Users (uid) or the two Groups (ou) that include: *ou=mathematicians,dc=example,dc=com*

- Make sure our Server URL is in this format. (Example.: *ldap://ldap.forumsys.com*)
- In the Starting search directory column, we need to mention where exactly our LDAP will look for the Users.

All user passwords are *password*. You may also bind to individual Users (uid) or the two Groups (ou) that include: *ou=mathematicians,dc=example,dc=com*

- From above credentials from our FORUM SYSTEMS website, let's take *dc=example,dc=com* details and Insert it into our Starting search directory column.
- Click on Submit, it will create LDAP server record.

LDAP Server Test Server for Demo

Enter a login distinguished name

Name: Test Server for Demo

Application: Global

Active: ☒

Login distinguished name:

Login password:

Starting search directory: dc=example,dc=com

MID Server:

LDAP Server URLs

URL	Order	Active	Operational Status
ldap://ldap.forumsys.com	100	true	true

Attributes:

Make sure to specify which LDAP Attributes to import to avoid exceeding the row size limit during the import process

Advanced Options

Connect timeout: 10

Read timeout: 30

SSL: ☐

Listener: ☒

Listen interval: 5

Paging: ☒

Update Delete

Related Links

Test Connection

LDAP Listener Status

Search

LDAP OU Definitions

Name	Search	Actions on selected rows...	New
Server: Test Server for Demo			
Groups	Group [cn, user, group]	(objectClass=group)	
Users	User [cn, user]	(objectClass=person)(cn=*)	

- We need to provide Login distinguished name.

Application: Global

Login distinguished name:

Login password:

Starting search directory: dc=example,dc=com

MID Server:

- For this we need to go to our FORUM SYSTEMS website and Copy Bind Distinguished Name (DN) and Password (Bind DN: *cn=read-only-admin,dc=example,dc=com* Bind Password: *password*)
- Now right click on the LDAP Server header and hit Save.

Application: Global

Login distinguished name: cn=read-only-admin,dc=example,dc=com

Login password:

Starting search directory: dc=example,dc=com

MID Server:

- Now we can see connected successfully prompt on the top.

Connected Successfully

- If we need to test the connection again, just scroll little bit down and we can see Test Connection option under related links.

Related Links

[Test Connection](#)
[LDAP Listener Status](#)
[Browse](#)
[Stop Listener](#)
[Certificate List](#)
[Advanced View](#)

- We have configured our LDAP Server. Now if we can see, it also updated few settings under Advanced Options like connect timeout, Read timeout, Listen interval, Listener and paging.
- Listener option monitors LDAP server for changes and updates the ServiceNow user and group tables accordingly.
- Paging option allows ServiceNow to import large numbers of LDAP users and groups in manageable chunks.

Advanced Options

Connect timeout	<input type="text" value="10"/>	Listener	<input checked="" type="checkbox"/>
Read timeout	<input type="text" value="30"/>	Listen Interval	<input type="text" value="5"/>
SSL	<input type="checkbox"/>	Paging	<input checked="" type="checkbox"/>

- LDAP, basically has lot of attributes that means it has lot of columns like email, userid, account status etc.,

Attributes

Make sure to specify which LDAP Attributes to import to avoid exceeding the row size limit during the import process

- We can mention what ever fields we want to import.
- If we can see, it automatically created 2 OU Definitions. One is for Groups and one is for Users.

LDAP OU Definitions				
Name	RDN	Query field	Table	Filter
Groups	CN=Users	sAMAccountName	Group [sys_user_group]	(objectClass=group)
Users	CN=Users	sAMAccountName	User [sys_user]	(&(objectClass=person)(sn=*)(!(objectCla...

1 to 2 of 2

- If we go to our LDAP Server on FORUM SYSTEMS, this particular website provided us these user details.

ou=mathematicians,dc=example,dc=com

- *riemann*
- *gauss*
- *euler*
- *euclid*

ou=scientists,dc=example,dc=com

- *einstein*
- *newton*
- *galileo*
- *tesla*

- If we can see the above image, these are the list of users present in this particular organizational unit (FORUM SYSTEMS).
- Here in our FORUM SYSTEMS, we have 2 OUs. One OU is for mathematicians and one is for scientists.
- Now let's check whether we are able to see all of these Users (mathematicians and scientists)

Name	RDN	Query field	Table	Filter
Groups	CN=Users	sAMAccountName	Group [sys_user_group]	(objectClass=group)
Users	CN=Users	sAMAccountName	User [sys_user]	(&(objectClass=person)(sn=*)(!(objectClass=computer))(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

- Click on Users under LDAP OU Definitions,

LDAP OU Definition: Users

Name: Users

RDN: CN=Users

Query field: sAMAccountName

Application: Global

Active: ☒

Server: Test Server for Demo

Table: User [sys_user]

Filter: (&(objectClass=person)(sn=*)(!(objectClass=computer))(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

Update Delete

Related Links

[Test connection](#)

[Browse](#)

Data Sources for text Search

LDAP target = Users

Name	Import set table name
Test Server for Demo/Users	ldap_import

- Now, let's test the connection again in our LDAP OU definition Users record. We can see a prompt saying Invalid RDN specified. 'CN=Users' does not exist within 'dc=example,dc=com'

Invalid RDN specified, 'CN=Users' does not exist within 'dc=example,dc=com'

Name: Users

RDN: CN=Users

Query field: sAMAccountName

Application: Global

Active: ☒

Server: Test Server for Demo

Table: User [sys_user]

Filter: (&(objectClass=person)(sn=*)(!(objectClass=computer))(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

Specify a relative distinguished name for starting search directory <get dn from ldap server record>

- Basically, it is saying that this CN=User, RDN doesn't exist. For now, let's make RDN column as blank.

Name	<input type="text" value="Users"/>
RDN	<input type="text"/>
Query field	<input type="text" value="sAMAccountName"/>

- These are the configuration details, which we need to confirm with our AD Team.
- Because in LDAP, we have different directories. So, we have to confirm with our AD Team like what kind of distinguished name, we have to mention or what kind of RDN we have to mention.
- This is LDAP filter, it will decide what users you need to pick and put it into your ServiceNow.

Filter

- In LDAP, you might find different kinds of user may be a user who is just a computer account or user which is a real user. This is the reason why we need to use the filter.
- As we are using Public LDAP Server, it already mentioned the list of uid's and ou's list in Online LDAP Test Server website.

```

cn=read-only-admin
ou=mathematicians
ou=scientists
uid=einstein
uid=euclid
uid=euler
uid=galileo
uid=gauss
uid=newton
uid=riemann
uid=tesla

```

- For now, let's update uid in the filter column like (uid=*)

Filter

- Now if we can see, it says connected successful prompt on top.

Connected Successfully

- That means, now our filter and RDN is working.
- Let click on browser under related links in LDAP OU Definition Users

Related Links

[Test connection](#)
[Browse](#)

- Let's go to Browse,

LDAP Browse

Filter: LDAP details for:

RDN: Distinguished Name:

☒ LDAP Nodes

Attribute Name	Attribute Value
----------------	-----------------

- This is really helpful during troubleshooting LDAP, now let's click on LDAP Nodes.

LDAP Nodes

- uid=newton
- uid=einstein
- uid=tesla
- uid=galileo
- uid=euler
- uid=gauss
- uid=riemann
- uid=euclid
- uid=test
- uid=curie
- uid=nobel
- uid=boyle
- uid=pasteur
- uid=nogroup

- We can see the list of uid's under LDAP Nodes. If we can compare both of the uid's in FORUM SYSTEMS and LDAP Nodes in Services both are same.

ou=mathematicians,dc=example,dc=com

- *riemann*
- *gauss*
- *euler*
- *euclid*

ou=scientists,dc=example,dc=com

- *einstein*
- *newton*
- *galileo*
- *tesla*

- Now, let's click on uid=newton under LDAP Nodes. We can see all the information regarding newton.

LDAP Nodes

- uid=newton
- uid=einstein
- uid=tesla
- uid=galileo
- uid=euler
- uid=gauss
- uid=riemann
- uid=euclid
- uid=test
- uid=curie
- uid=nobel
- uid=boyle
- uid=pasteur
- uid=nogroup

Attribute Name	Attribute Value
cn	Isaac Newton
dn	uid=newton,dc=example,dc=com
mail	newton@ldap.forumsys.com
objectClass	InetOrgPerson
objectClass	organizationalPerson
objectClass	person
objectClass	top
sn	Newton
source	ldap:uid=newton,dc=example,dc=com
uid	newton

- Let's troubleshoot, copy the email id from the attribute value, which is newton@ldap.forumsys.com
- Let's compose a filter with the email id as ([mail=newton@ldap.forumsys.com](mailto=newton@ldap.forumsys.com))

- Make sure the attribute name is same as mentioned in Attribute Naming convention.

Filter: (mail=newton@ldap.forumsys.com)

RDN:

LDAP details for: uid=newton

Distinguished Name: uid=newton,dc=example,dc=com

LDAP Nodes

- uid=newton

Attribute Name	Attribute Value
cn	Isaac Newton
dn	uid=newton,dc=example,dc=com
mail	<u>newton@ldap.forumsys.com</u>
objectClass	inetOrgPerson
objectClass	organizationalPerson
objectClass	person
objectClass	top
sn	Newton
source	ldap:uid=newton,dc=example,dc=com
uid	newton

- Now click Filter, and in the LDAP Nodes we can see uid=newton gets populated.
- This is because the filter that we mention is related to this user(uid=newton)
- We can troubleshoot our LDAP server like this using filters.
- Let's go to LDAP Server Test Server for Demo record
- In order to import our users using MID server. We need to select our MID Server.

Application: Global

Login distinguished name: cn=read-only-admin,dc=example,dc=com

Login password:

Starting search directory: dc=example,dc=com

MID Server:

- We do not need to have a MID server to import users using LDAP. However, using a MID server can offer some advantages like Improved security, performance and simplified configuration.
- As of now, I don't have any MID server Installed on my Instance. So, I cannot select it.
- Now, let's go to our Test Server for Demo/Users record under Data Sources in LDAP OU Definition Users.

Data Sources: for text Search

LDAP target = Users

Test Server for Demo/Users

Import set table name: ldap_import

1 to 1 of 1

- We can also get this Data Source for Test Server for Demo/Users record from System LDAP module.

- Now click on Test Server for Demo/Users, we can see our Test Server for Demo/Users record here.
- Let's click Test Server for Demo record under Transforms table.
- Now we will be redirected to Table Transform Map LDAP User Import record.

Source field	Target field	Coalesce
u_samaccountname	user_name	true
u_userprincipalname	email	false
u_l	location	false
u_source	source	false
u_givenname	first_name	false
u_sn	last_name	false
u_title	title	false

- Make sure Target table field is set to User [sys_user]
- As we can see, under the Field Maps. All the Source fields and Target fields are not mapped correctly in Field Map.
- Let's map them using Mapping Assist under Related Links.

Related Links

[Auto Map Matching Fields](#)

[Mapping Assist](#)

[Transform](#)

[Index Coalesce Fields](#)

- Map the source field and target field data correctly and dump them in Field Map column.

source	Source	Target
cn	User ID	
sn	Name	
mail	Email	
telephonenumber	Mobile phone	

- Now click on Save.
- Now, if we can see. All of our Source Field and Target Field under Field Maps got loaded correctly and successfully.

Field Maps (5) Transform Scripts (3)		
Source field	Target field	Coalesce
u_mail	email	false
u_telephonenumber	mobile_phone	false
u_cn	user_name	false
u_source	source	false
u_sn	name	false

- Now let's click Transform under Related Links.
- Now we will be redirected to Specify Import Set and Transform map.
- Under Specify Import Set and Transform map, click Transform.
- Now we can see the records got successfully inserted in our sys_user table.

Progress	
Name	ImportProcessor
State	Complete
Completion code	Success
Message	Processed: 14, Inserts 14, updates 0, errors 0, empty and ignored 0, Ignored errors 0 (0:00:01.000)

- Message is showing Processed:14, Inserts: 14, Updates: 0, errors 0, empty and ignored errors 0 (0:00:01.000)
- Now, Let go to our sys_user.list table and let's verify the count under sys_user table before and now.

BEFORE:

1 to 20 of 727

AFTER:

1 to 20 of 741

NEWLY LOADED USERS:

User ID	Name	First name	Email	Active
Albert Einstein	einstein	einstein	einstein@ldap.forumsys.com	true
Carl Friedrich Gauss	gauss	gauss	gauss@ldap.forumsys.com	true
Marie Curie	curie	curie	curie@ldap.forumsys.com	true
No Group	nogroup	nogroup	nogroup@ldap.forumsys.com	true
Bernhard Riemann	riemann	riemann	riemann@ldap.forumsys.com	true
Alfred Nobel	nobel	nobel	nobel@ldap.forumsys.com	true
Nikola Tesla	tesla	tesla	tesla@ldap.forumsys.com	true
Robert Boyle	boyle	boyle	boyle@ldap.forumsys.com	true
Galileo Galilei	galileo	galileo	galileo@ldap.forumsys.com	true
Euclid	euclid	euclid	euclid@ldap.forumsys.com	true
Isaac Newton	newton	newton	newton@ldap.forumsys.com	true
Leonhard Euler	euler	euler	euler@ldap.forumsys.com	true
Test	test	test		true
Louis Pasteur	pasteur	pasteur	pasteur@ldap.forumsys.com	true