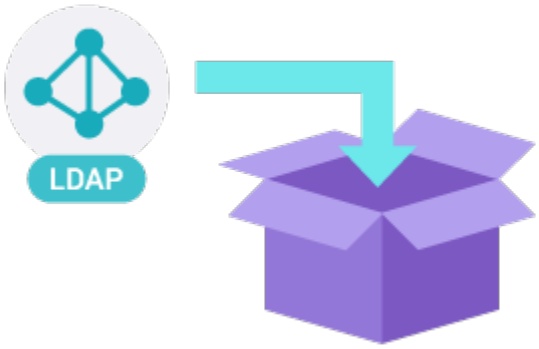
LDAP Import

This import type will import LDAP entries into Insight.



Some use cases could be:

- Your LDAP directory server is full of assets that are stored in your corporate directory.
- When using approval processes, employee and manager relationships are preserved.
- And so much more...

Topics on this page:

Overview

An LDAP directory is a collection of data about users and other assets. LDAP (Lightweight Directory Access Protocol) is an Internet protocol that web applications can use to look up information about those assets from the LDAP server.

We provide a built-in connector for the most popular LDAP directory servers:

- Microsoft Active Directory
- Apache Directory Server (ApacheDS)
- Apple Open Directory
- Fedora Directory Server
- Novell eDirectory
- OpenDS
- OpenLDAP
- OpenLDAP Using Posix Schema
- Posix Schema for LDAP
- Sun Directory Server Enterprise Edition (DSEE)
- A generic LDAP directory server

LDAPS validation

LDAPS (Secure LDAP) is supported and does not have any special requirements from Insight to work.

If you are trying to import from an LDAPS source, you can choose to validate the LDAP server certificate with an imported Certificate Authority (CA) certificate. If you select to validate the LDAP server certificate, you must import the root CA certificate from the CA that signed the LDAP server certificate, so your Jira can use the CA certificate to validate the LDAP server certificate. More information is explained here.

Be sure to change the port to 3269. This is due to the fact that a GC (global catalog) server returns referrals on 389 which refers to the greater AD "forest" , but acts like a regular LDAP server on 3268 (and 3269 for LDAPS) when changing from LDAP to LDAPS.

Import Type Fields

Setting	Description
URL	Protocol, Hostname and Port of the server running LDAP. Example: ldap://ldap.example.com:389
User DN	The distinguished name of the user that the application will use when connecting to the directory server. Examples: • `cn=administrator,cn=users,dc=ad,dc=example,dc=com` • `cn=user,dc=domain,dc=name` • `user@domain.name`
Password	The password of the user specified above.

Base DN	The root distinguished name (DN) to use when running queries against the directory server. Examples: • `o=example,c=com` • `cn=users,dc=ad,dc=example,dc=com` • For Microsoft Active Directory, specify the base DN in the following format: `dc=domain1,dc=local`. You will need to replace the `domain1` and `local` for your specific configuration. Microsoft Server provides a tool called `ldp.exe` which is useful for finding out and configuring the the LDAP structure of your server. If you want specific Base DN in your object type see the Selector value below
Search filter	Defines the scoop of the filter search, default is **(objectClass=*)** which will give you all entries. If you only want Jira Users for example, you can set (objectClass=person). Note that the Users in LDAP need to have the the "objectClass" set to "person". The search filter is important in the way that it can affect the synchronization time.
Search scope when importing	Search scope determines how objects should be fetched from the LDAP. Default setting is ONE_LEVEL while the locators and structure are created with SUBTREE.
Follow Referrals	LDAP functionality to make sure you always get the correct data, even in a distributed LDAP environment.
Include namespace	This option is only applicable when creating an Insight object structure from an LDAP server. The option will append the namespace e.g. *cn=users,ou=company,=dc=examle,dc=com* to the object type description. The value is not used while performing synchronizations.

⚠️ Be sure you test the synchronization in a test environment before doing it in production.

Object Type Mapping configuration

Name	Description
Selector	In the LDAP import type the Selector is prepended to the Base DN value before the search in LDAP is executed. The value is used to narrow down the structured tree in the LDAP to specific nodes. The search filter will be the same as specified in the general configuration but the selector will narrow the scope where the search filter is applied. To examplify: If the Base DN is *dc=ad,dc=example,dc=com* and the Selector is *cn=users* the resulting LDAP search base will be *cn=users,dc=ad, dc=example,dc=com.*

Predefined Structure & Configuration

The structure will be created based on the result from the LDAP server. When creating the predefined structure a query will be sent to the LDAP server with the configuration specified and fetch the result. Based on the result an object type hierarchy will be created. Each node (identified by DN) that has children will be treated as an object type and created. The attributes belonging to the Insight object type will be the attributes found on the node in the LDAP server.

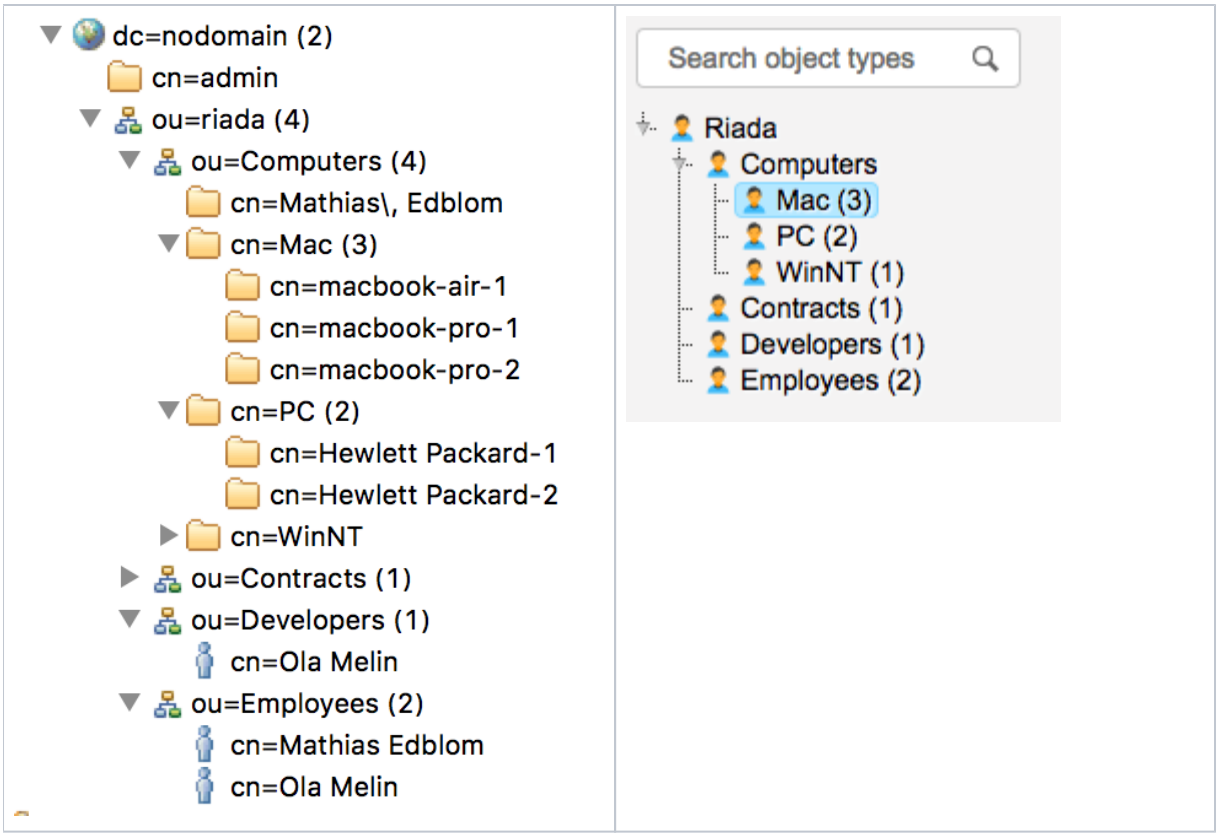
If the result returned by LDAP server retrieves objects that don't have children, then it will be not possible to create a predefined structure automatically and it should be created manually.

The predefined structure will create two additional attributes for each object type. The attribute CN (Common Name) will be used as label and the attribute DN (Distinguished Name) will be set with the property hidden.

All attributes created by the predefined structure in the LDAP import will be of type *Default Text*. If the data represent something else review the attributes and change them accordingly.

Predefined structure example

Example LDAP structure	Resulting Insight Object Type Structure



Predefined Configuration

The predefined configuration will query the LDAP server and create a configuration mapping based on the same criteria as the structure described above. As data locators all attributes found will be choosable with the addition of the CN (Common Name) and the DN (Distinguished Name).

The identifier will be set to DN for each object to uniquely identify each object from the LDAP server.

Since the predefined configuration will be different based on the connected LDAP server the following is one example mapping the Employees as seen in the previous example

Predefined configuration example

Employees

Selector	ou=employees
IQL	"DN" endswith "ou=employees,ou=riada,dc=nodomain"
Missing objects	Ignore
Empty Values	Use default
Unknown Values	Use default

Identifier	Data Locator	Insight Attribute	Object mapping (IQL)
☐	DESCRIPTION	DESCRIPTION	
☐	SEEALSO	SEEALSO	
☐	SN	SN	
☐	TELEPHONENUMBER	TELEPHONENUMBER	
☐	OBJECTCLASS	OBJECTCLASS	
☑	DN	DN	
☐	CN	CN	

If the LDAP import is configured to import users one can use the REGEX configuration to split users in order to create multiple users.