LDAP Source

- Modes
- Configuration
  - Key Attribute
  - Search Filter
  - UID Attribute
- Supported Attributes
- Constraints
- See Also

The LDAP Organizational Identity Source Plugin is designed to integrate with an LDAP server.

Modes

Org Identity Source Mode	Support
Manual Search and Linking	Supported
Enrollment, Authenticated	Not supported
Enrollment, Claim	Not supported
Enrollment, Search	Supported
Enrollment, Select	Supported

Org Identity Sync Mode	Support
Full	Supported, with restrictions
Query	Supported
Update	Supported
Manual	Supported

Installation

This is a non-core plugin, see Installing and Enabling Registry Plugins for more information.

This plugin requires PHP 5.6 or later (for ldap_escape).

PHP 7.2 or later is recommended when integrating with Active Directory (for `JSON_INVALID_UTF8_SUBSTITUTE`).

Configuration

The LDAP Source Plugin supports both anonymous and authenticated binds.

Key Attribute

An attribute (the *Key Attribute*) containing a unique key is required. The value of this attribute should be persistent and not change under any circumstances. There should only ever be exactly one value for this attribute. While `dn` can be used, many LDAP deployments allow DNs to be changed, for reasons such as being based on a name, or a structural change of the LDAP server itself. If DNs are not persistent, then a different attribute (such as `employeeNumber`, if suitable) should be used.

Search Filter

By default, the Plugin will search for all records under the Base DN. However, under some circumstances it may be desirable to further filter searches, such as to exclude inactive entries. This is done by setting the *Search Filter* configuration. The Search Filter will be AND'd together with any search operation performed by the Plugin. Be sure to include the parentheses in the filter definition, and also to escape any special characters within the filter values.

An example search filter, to constrain searches against Active Directory to active users: `(!(userAccountControl=514))`

UID Attribute

The LDAP Source Plugin can select an arbitrary attribute from the LDAP record to assign to the Org Identity as an Identifier of type UID. This is intended as an interim capability until a more general solution is implemented (CO-1346).

Supported Attributes

The following attributes are currently supported by LdapSource:

LDAP Attribute	Org Identity Source Attribute
edupersonaffiliation	Affiliation
employeenumber	Identifier/identifier, type=Enterprise
givenname	Name/given, type=Official
l	Address/locality, type=Office
mail	EmailAddress/mail, type=Official, verified
o	o
ou	ou
postalcode	Address/postal_code, type=Office
sn	Name/family, type=Official
st	Address/state, type=Office
street	Address/street, type=Office
telephonenumber	TelephoneNumber/number, type=Office
title	title

Constraints

Full syncs are dependent on the LDAP server having sufficiently high search limits to allow the full directory to be read, or for binding to be performed with a Bind DN with unlimited search permission.

Wildcards are not supported in searches (though they are supported in the *Search Filter*). All searches will be prefix searches (ie: foo*).

See Also

- cm_ldap_sources