LDAP Groups

Overview

The LDAP Groups Add-on allows you to synchronize your LDAP groups with Artifactory and leverage your existing organizational structure for managing group-based permissions.

Unlike many LDAP integrations, LDAP groups in Artifactory use super-fast caching, and has support for both Static, Dynamic and Hierarchical mapping strategies. Powerful management is accomplished with multiple switchable LDAP settings and visual feedback about the up-to-date status of groups and users coming from LDAP.

LDAP groups synchronization works by instructing Artifactory about the external groups authenticated users belong to. Once logged-in, you are automatically associated with your LDAP groups and inherit group-based permission managed in Artifactory.

> ⚠ **Make sure users log in**
>
> Synchronizing LDAP groups does not automatically create users that are members of those groups. Once the LDAP connection is configured, the LDAP users are only created in Artifactory after they log in to Artifactory for the first time. Automatic creation of users can be controlled by the Auto Create Artifactory Users checkbox in the LDAP Settings screen.

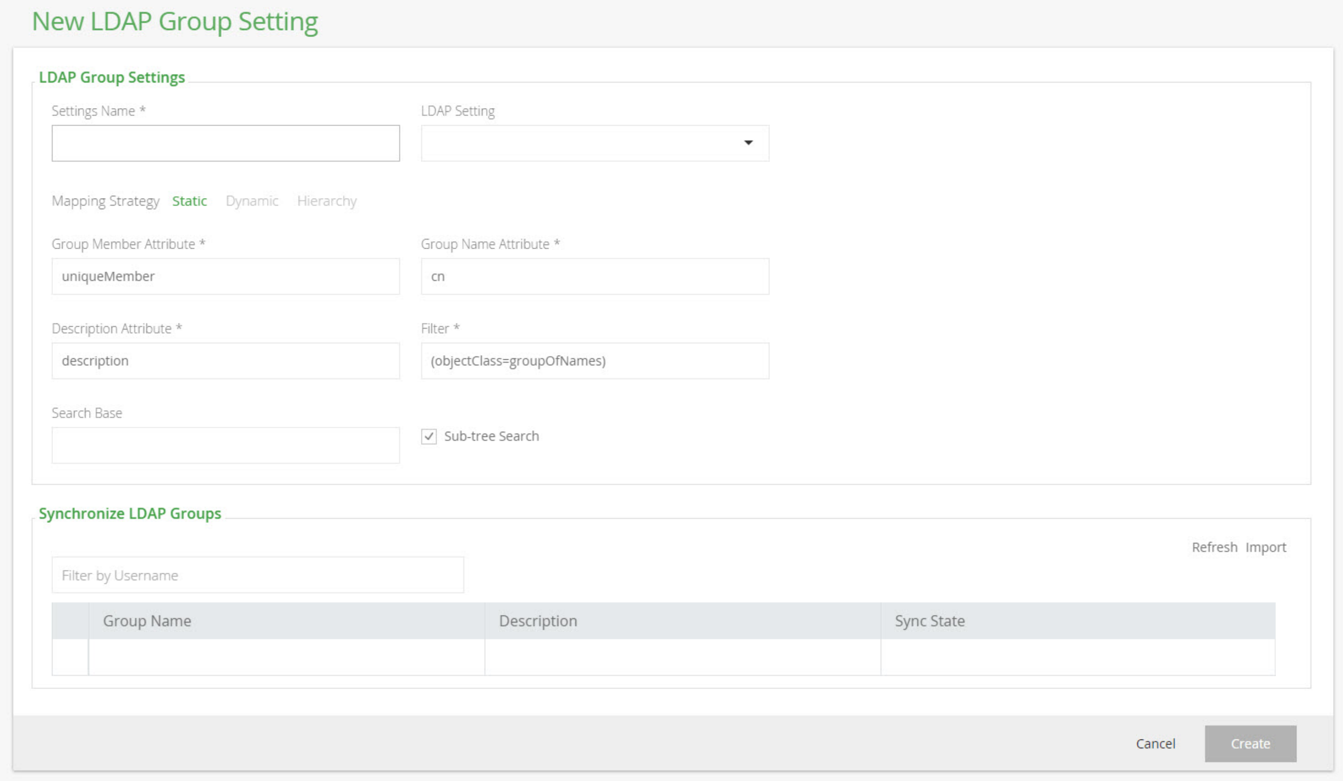
Page Contents

Usage

LDAP Groups settings are available in the **Admin** module under **Security | LDAP.**

To use LDAP groups you must first set up an LDAP server for authentication from the LDAP Settings screen. You must also alert Artifactory about the correct LDAP group settings to use with your existing LDAP schema.

> ⓘ **Active Directory Users**
>
> For specific help with setting up LDAP groups for an Active Directory installation please see Managing Security with Active Directory.



New LDAP Group Setting

LDAP Group Settings

Settings Name *

LDAP Setting

Mapping Strategy: Static | Dynamic | Hierarchy

Group Member Attribute *: uniqueMember

Group Name Attribute *: cn

Description Attribute *: description

Filter *: (objectClass=groupOfNames)

Search Base

☑ Sub-tree Search

Synchronize LDAP Groups

	Group Name	Description	Sync State

Group Synchronization Strategies

Artifactory supports three ways of mapping groups to LDAP schemas:

- **Static**: Group objects are aware of their members, however, the users are not aware of the groups they belong to.
  Each group object such as `groupOfNames` or `groupOfUniqueNames` holds its respective member attributes, typically `member` or `uniqueMembe`
  , which is a user DN.

- **Dynamic**: User objects are aware of what groups they belong to, but the group objects are not aware of their members.
  Each user object contains a custom attribute, such as `group`, that holds the group DNs or group names of which the user is a member.

- **Hierarchy**: The user's DN is indicative of the groups the user belongs to by using group names as part of user DN hierarchy.
  Each user DN contains a list of ou's or custom attributes that make up the group association.
  For example,
  `uid=user1,ou=developers,ou=uk,dc=jfrog,dc=org` indicates that `user1` belongs to two groups: `uk` and `developers`.

> **Using OpenLDAP**
>
> When using OpenLDAP, you can't apply the **Dynamic** strategy because the `memberOf` attribute is not defined by default (`memberOf` is an overlay), so Artifactory would not be able to fetch it from the LDAP server.

Synchronizing LDAP Groups with Artifactory

Importing Groups Through the UI

Once you have configured how groups should be retrieved from your LDAP server, you can verify your set up by clicking the `Refresh` button on the `Synchronize LDAP Groups` sub-panel. A list of available LDAP groups is displayed according to your settings.

You are now ready to synchronize/import groups into Artifactory. The groups table allows you to select which groups to import and displays the sync-state for each group:

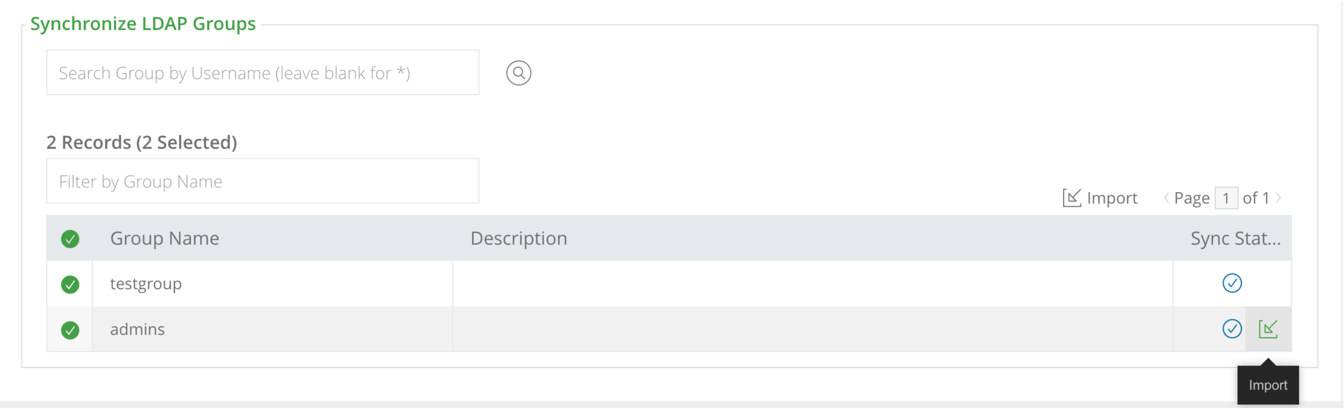
A group can either be completely new or already existing in Artifactory. If a group already exists in Artifactory it can become outdated (for example, if the group DN has changed) - this is indicated in the table so you can select to re-import it.

Once a group is imported (synced) a new external LDAP group is created in Artifactory with the name of the group.

Once you have imported LDAP groups, you can Manage Permissions on them as with regular Artifactory groups. Users association to these groups is external and controlled strictly by LDAP.

> ⚠ Make sure that LDAP group settings is enabled (in the `LDAP Groups Settings` panel) in order for your settings to become effective.

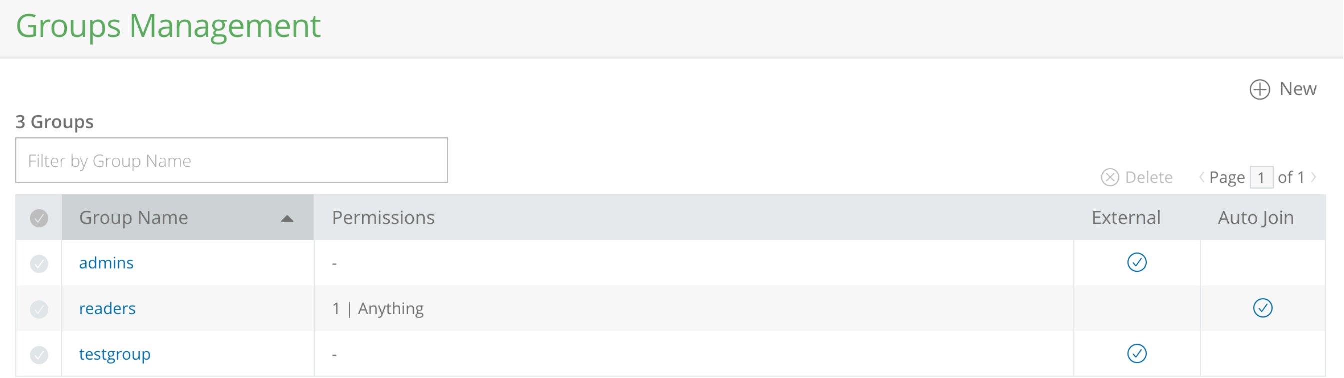
To synchronize a group through the UI, in the **Admin** module, under **Security | LDAP,** select the group you want to synchronize, and search for groups that have been defined under the corresponding group settings. Once groups have been found, select **Import.**



2 Records (2 Selected)

✓	Group Name	Description	Sync Stat...
✓	testgroup		✓
✓	admins		✓

Once the groups are synchronized, you should see them in your list of groups (**Admin** module under **Security | Groups**) indicated as "External".



Groups Management

3 Groups

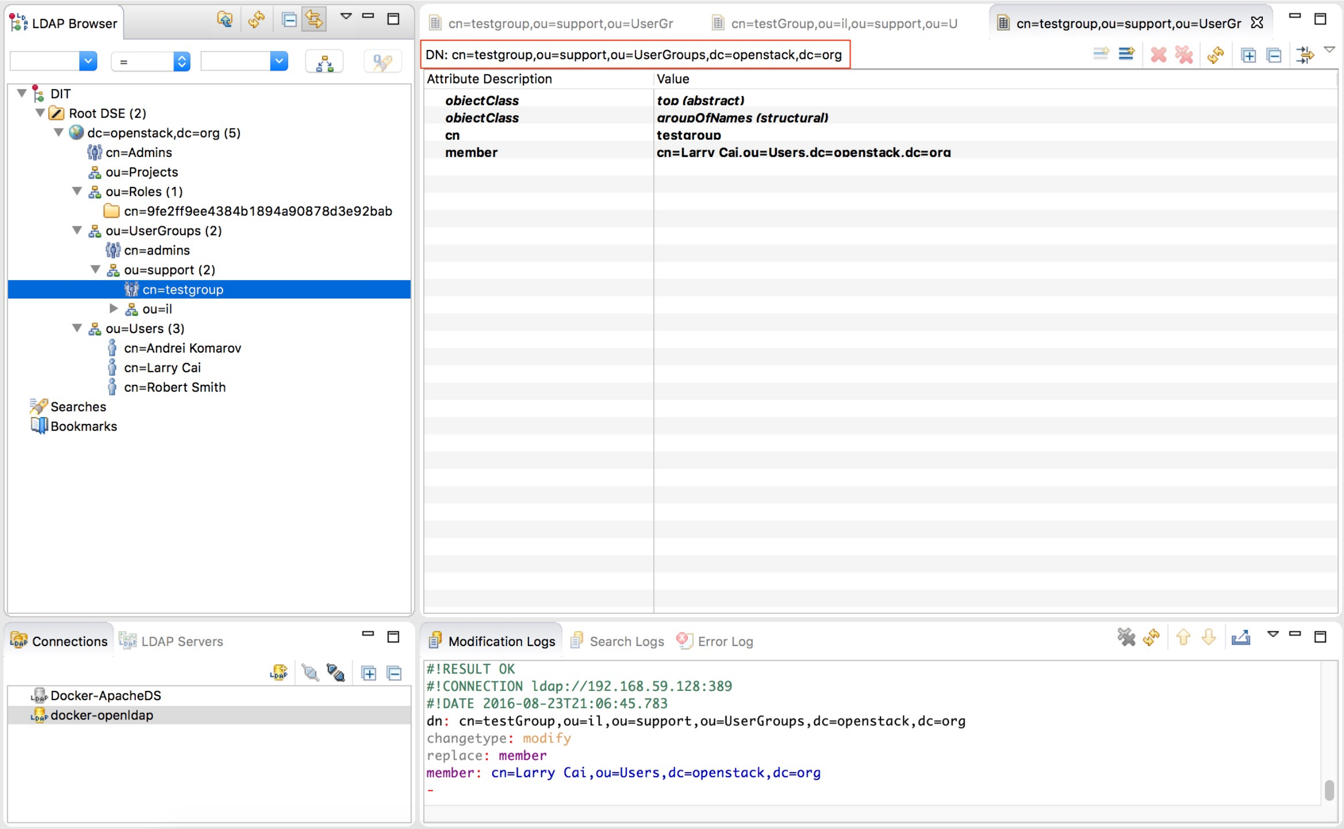
	Group Name	Permissions	External	Auto Join
	admins	-	✓	
	readers	1 | Anything		✓
	testgroup	-	✓	

Using the REST API

You may also synchronize LDAP groups by using the Create Group REST API to create groups with the 'ldap' realm and full DN path to the group object under your LDAP server.

> ⚠ **Limitation**
>
> Make sure to use lower case only when creating LDAP groups through the REST API. Using upper or mixed case will prevent synchronization of groups.

When using the REST API to synchronize LDAP groups, you need to specify the exact and full Group DN path to the group on your LDAP server. The example below shows the JSON payload you would use to synchronize the "testgroup" group displayed in the below LDAP server:



DN: cn=testgroup,ou=support,ou=UserGroups,dc=openstack,dc=org

Attribute Description	Value
objectClass	*top (abstract)*
objectClass	*groupOfNames (structural)*
cn	testgroup
member	cn=Larry Cai,ou=Users,dc=openstack,dc=org

```
#!RESULT OK
#!CONNECTION ldap://192.168.59.128:389
#!DATE 2016-08-23T21:06:45.783
dn: cn=testGroup,ou=il,ou=support,ou=UserGroups,dc=openstack,dc=org
changetype: modify
replace: member
member: cn=Larry Cai,ou=Users,dc=openstack,dc=org
-
```

```
Sample JSON:
{
        "name": "testgroup",
        "description" : "This groups already exists in ldap",
        "autoJoin" : false,
        "realm": "ldap",
        "realmAttributes": "ldapGroupName=testgroup;groupsStrategy=STATIC;groupDn=cn=testgroup,ou=support,
ou=UserGroups,dc=openstack,dc=org"
}
```

Watch the Screencast