

Active Directory synchronization with AD groups

Configuring Integration with Active Directory

1. Go to **"System settings" - "Auth"** and select the **LDAP** tab.
2. Enter the LDAP server address, an account for connection, and its password.
3. Specify the OU and user search filter. See an example of a filter for a specific group in the screenshot below.

The screenshot shows the 'Auth' settings page for LDAP integration. The left sidebar contains a menu with 'Auth' selected. The main content area has tabs for 'Basic', 'CAS', 'Passkey', 'OIDC', 'SAML2', 'OAuth2', 'WeCom', 'DingTalk', 'FeiShu', 'Slack', and 'Radius'. The 'Basic' tab is active, showing the 'Enable LDAP auth' toggle (checked). Below this are fields for 'LDAP server' (ldap://afidc.afilocal:389), 'Bind DN' (testadmin@afilocal), and 'Password'. The 'LDAP User' section includes 'User OU' (DC=afilocal), 'User search filter' ((&(objectClass=user)(memberOf=CN=AFI_IT,CN=Users,DC=afilocal))), and 'User attr map' (a JSON object mapping LDAP attributes to system attributes).

```
1 {
2   "username": "sAMAccountName",
3   "name": "cn",
4   "email": "mail"
5 }
```

4. Click the **"Submit"** button to save the settings. Note: After changing parameters and settings, always click **"Submit"** to apply changes. Otherwise, the test will run with old parameters.
5. Click the **"Test connection"** button to verify the settings or **"Test login"** to check a specific user's authorization.
6. Click the **"Bulk Import"** button. You should see the users of the group that will be added for PAM authorization. You can select specific users and click **"Import"** or import all users by clicking **"Import all"**.

7. You can also configure automatic user synchronization by clicking the **"Sync setting"** button.

Sync setting [X]

* Organization: Default [x]

Periodic perform: ☒

Regularly perform: */15 * * * *

For example: every Sunday at 03:05 execute <5 3 * * 0>
Using the 5-bit Linux crontab expression <minute hour day month week> ([Online tool](#))
If both regularly perform and cycle perform execution are set, use regularly perform first

* Cycle perform: 1

Unit: hour

Recipient: Select

Reset Submit

Synchronization with Active Directory Groups

Why synchronize with AD groups?

Managing access rights to target systems can be done using familiar Active Directory groups. Adding or removing a user from such groups will automatically synchronize with the permissions matrix in JumpServer, and the user will gain or lose access rights.

Configuring synchronization with AD groups.

1. Go to **System settings - Authentication - LDAP**
2. In the **User attribute** field, add the parameter **groups** to look like this:

```
{
  "username": "sAMAccountName",
  "name": "cn",
  "email": "mail",
  "groups": "memberOf"
}
```

See screenshot:

Basic

LDAP



* Server ?

ldap://afidc.afi.local:389

* Bind DN ?

testadmin@afi.local

Password ?

Password

Search

* Search OU ?

DC=afi,DC=local

* Search filter ?

(&(objectClass=user)(memberOf=CN=AFI_IT,CN=Users,DC=afi,DC=local))

* User attribute ?

1

2

3

4

5

6

"username": "sAMAccountName",

"name": "cn",

"email": "mail",

"groups": "memberOf"

}

3. Click the **Submit** button to save the settings.

4. Click the **User Import** button and then click **Sync Users** in the opened window.

If everything is correct, you will see a list of users and a column with AD group attributes:

Ldap user

Please submit ldap configuration before import

Search

| <input type="checkbox"/> | Username | Name | Email | Groups | Already exists |
|--------------------------|----------|----------------|-------------|---|----------------|
| <input type="checkbox"/> | denis | Морозов Денис | - | CN=TestJS,OU=subOU,OU=TestOU,DC=afi,DC=local CN=AFI_IT... | Yes |
| <input type="checkbox"/> | sergey | Попцов Сергей | - | CN=AFI_IT,CN=Users,DC=afi,DC=local | Yes |
| <input type="checkbox"/> | nlo | Наталия Орлова | no@afi-d.ru | CN=TestJS,OU=subOU,OU=TestOU,DC=afi,DC=local CN=thyc... | Yes |
| <input type="checkbox"/> | Вася | Вася | - | CN=TestJS,OU=subOU,OU=TestOU,DC=afi,DC=local CN=AFI_IT... | Yes |
| <input type="checkbox"/> | testnlo | testnlo | - | CN=AFI_IT,CN=Users,DC=afi,DC=local CN=Domain Admins,CN... | Yes |
| <input type="checkbox"/> | TST_User | TST_User | - | CN=AFI_IT,CN=Users,DC=afi,DC=local | Yes |

Total 6

15/page

< 1 >

Sync users

Import

Import all

Cancel

5. Click **Import all** to add users to the system.

If you go to **Console - User - Groups**, you will see JS user groups with AD group names and the same users in them:

JumpServer

Console

Groups

Dashboard

User

Groups

Assets

Zones

Platforms

Accounts

+ Create

Actions

| | Name | Users |
|--------------------------|-------------------------|-------|
| <input type="checkbox"/> | AD AFL_IT | 6 |
| <input type="checkbox"/> | AD Domain Admins | 2 |
| <input type="checkbox"/> | AD Remote Desktop Users | 1 |
| <input type="checkbox"/> | AD TestJS | 3 |
| <input type="checkbox"/> | AD thycotic | 1 |
| <input type="checkbox"/> | Default | 16 |

Версия #1
Сергей Попцов создал 21 января 2025 11:37:42
Сергей Попцов обновил 21 января 2025 11:40:39