

# Azure AD Plugin

## Plugin Information

View Azure AD [on the plugin site](#) for more information.



Older versions of this plugin may not be safe to use. Please review the following warnings before using an older version:

- [Credentials stored in plain text](#)
- [Client secret transmitted in plain text](#)

A Jenkins Plugin that supports authentication & authorization via Azure Active Directory.

## Setup In Azure Active Directory

1. Make sure your Jenkins server has enabled HTTPS. If your Jenkins instance is created by the [Jenkins Solution Template](#), you can update your NGINX config file at `/etc/nginx/sites-available/default`. More configuration details can be found [here](#).
  2. Open Azure Active Directory, in `Properties`, copy `Directory ID`, it will be used as `tenant` in Jenkins.
  3. Register an application in AAD, copy the `Application ID`, it will be used as `Client ID`.
  4. In Application setting page, add a `Reply URL` `https://{your_jenkins_host}/securityRealm/finishLogin`. Make the variable `jenkinsURL` set as `https://{your_jenkins_host}` for the file `jenkins.model.JenkinsLocationConfiguration.xml` in the `$JENKINS_HOME` folder.
  5. In Application setting page, click `Keys`, generate a new key, copy the value, it will be used as `Client Secret` in Jenkins.
  6. To configure Azure Active Directory Matrix-based security, you have to add your `user/group` value with pattern `userName|groupName` (`principalName`). The pattern `userName|groupName` (`objectId`) still works to make compatible with previous versions. Below two steps are optional since version 1.0.0. Without these steps:
    - You are not able to have autocompletion when adding `user/group` in Azure Active Directory Matrix.
    - You do not have the same privileges as the groups you belonged to.
1. In Application setting page, click `Required Permissions` and select `Windows Azure Active Directory`, then select `Read directory data` permissions in `Application permissions` section.
  2. Click `Grant Permissions`. If you are not an admin in your tenant, please contact admin to grant the permissions which declared as `require admin` in `Enable Access` page. Wait for the permissions taking effects.

## Setup In Jenkins

Click `Manage Jenkins` in the left menu, then click `Configure Global Security`, check `Enable security`

## Enable Azure Authentication

To enable Azure Authentication, check `Azure Active Directory` and fill in the credential.

Click `Verify Application` to make sure your input is valid.

## Enable Azure Authorization

To enable Azure Authentication, check `Azure Active Directory Matrix-based security`

## Version 1.0.0 Migration Instruction

In version 1.0.0, this plugin upgrades from Microsoft identity platform v1.0 to v2.0. Before you upgrade ad plugin to version 1.0.0, please read following items first.

1. Make sure your Jenkins server has enabled HTTPS. Microsoft identity platform v2.0 forces using HTTPS schema in reply uri for its applications. Please update the reply uri for your AAD application. You also need to update the url setting in `jenkins.model.JenkinsLocationConfiguration.xml` file and restart your Jenkins instance. If your Jenkins instance is created by the [Jenkins Solution Template](#), you can update your NGINX config file at `/etc/nginx/sites-available/default`. More configuration details can be found [here](#).
2. Go to your related AAD application, click `Manifest` to open the inline manifest editor. Replace the `optionalClaims` value as below. You can find more information about [this](#).

```
"optionalClaims": {
  "idToken": [
    {
      "name": "family_name",
      "essential": false
    },
    {
      "name": "given_name",
      "essential": false
    },
    {
      "name": "upn",
      "essential": false
    }
  ]
},
```

## Q: How to recovery if Jenkins keeps failing during the login phase?FAQ

A: You can disable the security from the config file (see <https://wiki.jenkins.io/display/JENKINS/Disable+security>)

## Q: Why getting a error "insufficient privileges to complete the operation" even having granted the permission?

A: It takes rather long time for the privileges to take effect, which could be 10-20 minutes. So just wait for a while and try again.

## Change Log

### 1.0.0 (2019-05-30)

**This release includes breaking changes for Azure Identity platform, please follow up wiki to migrate.**

- Bump Jenkins version to 2.138.3
- Upgrade Microsoft identity platform from v1.0 to v2.0
- Add support for configuration as code
- Admin permission for tenant is no more necessary
- Jenkins server must enable HTTPS

### 0.3.4 (2019-04-30)

- [Fix security issue](#)

### 0.3.3 (2019-04-11)

- Support named groups and users

### 0.3.2 (2019-01-18)

- Fix seed authentication issue

### 0.3.1 (2018-09-19)

- Upgrade Azure commons to 0.2.7
- Use UPN as Jenkins user id

### 0.3.0 (2018-02-09)

**Jenkins under version 2.60 is not supported any more!**

- Upgrade the dependency of matrix-auth to 2.2

### 0.2.0 (2018-01-18)

- Support project-based authorization
- Improve security

### **0.1.1 (2017-12-07)**

- Fixed the CSRF protection issue.

### **0.1.0 (2017-12-01)**

- Initial release