
# Join Ubuntu / Debian To Active Directory (AD) domain

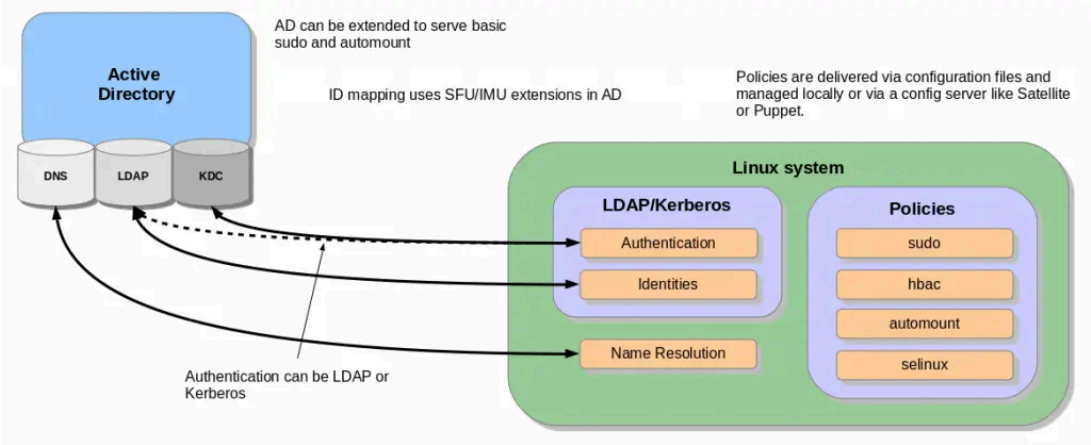
By **Josphat Mutai** - November 22, 2023

**Question**: How can I join Ubuntu 22.04|20.04|18.04 to Windows domain?, can I join Debian to Active Directory domain?. This article has been written to show you how to use **realmd** to join Ubuntu / Debian Linux server or Desktop to an Active Directory domain. Active Directory domain is the central hub for user information in most corporate environments.

For example, in my Company's infrastructure, it is a key requirement that all users are authenticated to all Linux systems with the Active Directory credentials. This should work for both Debian and Red Hat based Linux distributions. I had earlier written a guide for RHEL / CentOS, check it from the link below.

- How To Join CentOS 8 / RHEL 8 System to Active Directory (AD) domain

This guide will illustrate how to configure SSSD to retrieve information from domains within the same Active Directory Resource Forest. if you're working with more than one AD forest, this guide may not work for you. We'll also go further and configure sudo rules for the users logging in through AD. Here is a diagram depicted the setup and how the setup works.




So follow below steps to join Ubuntu / Debian To Active Directory (AD) domain.

## Step 1: Update your APT index

Start by updating your Ubuntu / Debian Linux system.

```
sudo apt -y update
```

This is essential as installations may fail if the server is a freshly installed.

For **Ubuntu 18.04**, add the following repositories to your *sources.list* file.

```
sudo tee -a /etc/apt/sources.list <<EOF
deb http://us.archive.ubuntu.com/ubuntu/ bionic universe
deb http://us.archive.ubuntu.com/ubuntu/ bionic-updates universe
EOF
```

## Step 2: Set server hostname & DNS

Set a proper hostname for your server with correct domain component.

```
sudo hostnamectl set-hostname myubuntu.example.com
```

Confirm your hostname:

```
$ hostnamectl
   Static hostname: myubuntu.example.com
         Icon name: computer-vm
           Chassis: vm
        Machine ID: 5beb7ac3260c4f00bcfbe1088f48b8c7
           Boot ID: b2a0d9abe43b455fb49484dbaa59dc41
    Virtualization: vmware
  Operating System: Ubuntu 18.04.1 LTS
            Kernel: Linux 4.15.0-29-generic
      Architecture: x86-64
```

Confirm DNS ia configured correctly:

```
cat /etc/resolv.conf
```

## Step 3: Install required packages

A number of packages are required for joining an Ubuntu 20.04|18.04 / Debian 10 system to Active Directory (AD) domain.

```
sudo apt update
sudo apt -y install realmd libnss-sss libpam-sss sssd sssd-tools
adcli samba-common-bin oddjob oddjob-mkhomedir packagekit
```

Only after a successful installation of dependencies can you proceed to discover Active Directory domain on Debian 10 / Ubuntu 20.04/18.04.

## Step 4: Discover Active Directory domain

The *realm discover* command returns complete domain configuration and a list of packages that must be installed for the system to be enrolled in the domain.

```
$ sudo realm discover example.com
example.com
  type: kerberos
  realm-name: EXAMPLE.COM
  domain-name: example.com
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
```

Replace *example.com* with your valid AD domain.

## Step 5: Join Ubuntu / Debian To AD domain

An AD administrative user account is required for integrating your Linux machine with Windows Active Directory domain. Check and confirm AD admin account and the password.

The *realm join* command will set up the local machine for use with a specified domain by configuring both the local system services and the entries in the identity domain. The command has a number of options which can be checked with:

```
$ realm join --help
```

A basic command execution is:

```
$ sudo realm join -U Administrator example.com
Password for Administrator:
```

Where:

- **Administrator** is the name of admin account used to integrate machine to AD.
- **example.com** is the name of AD domain

The command first attempts to connect without credentials, but it prompts for a password if required.

View current realmd details.

```
$ realm  list
example.com
  type: kerberos
  realm-name: EXAMPLE.COM
  domain-name: example.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
  login-formats: %U@example.com
  login-policy: allow-realm-logins
```

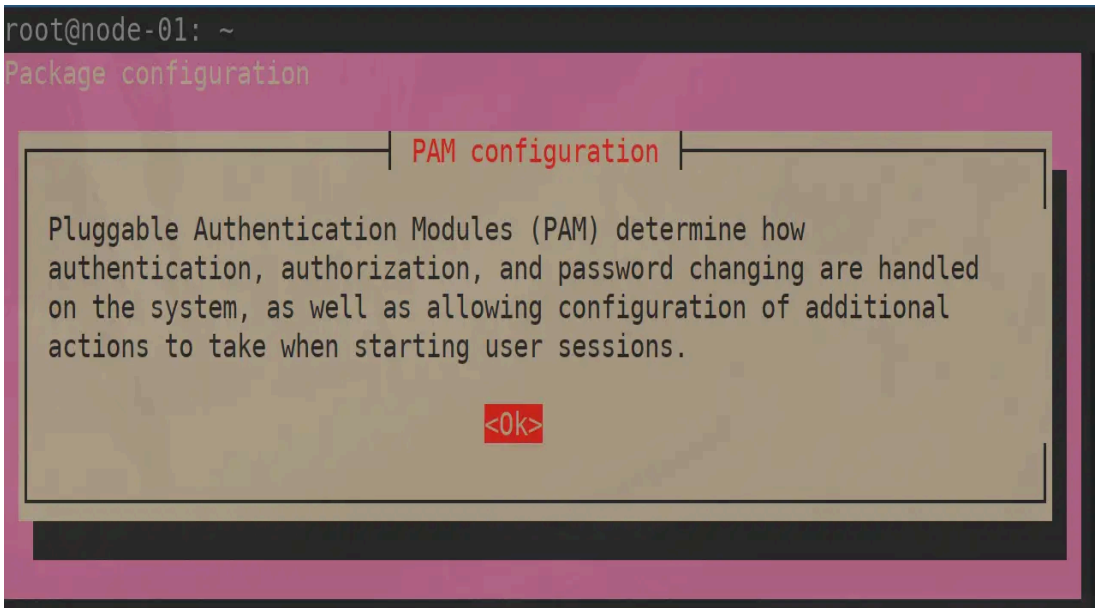
On RHEL based systems, user's home directory will be created automatically. On Ubuntu / Debian, you need to enable this feature.

```
sudo bash -c "cat > /usr/share/pam-configs/mkhomedir" <<EOF
Name: activate mkhomedir
Default: yes
Priority: 900
Session-Type: Additional
Session:
        required                        pam_mkhomedir.so umask=0022
skel=/etc/skel
EOF
```

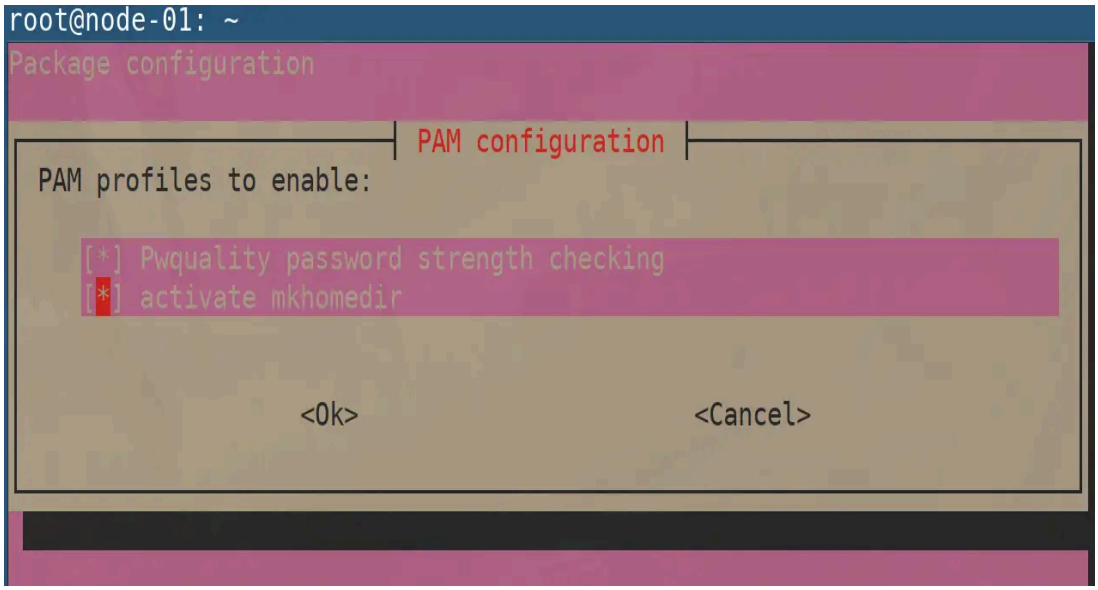
Then activate with:

```
sudo pam-auth-update
```

Select **<OK>**




Ensure **"activate mkhomedir"** is selected, it should have **[*]**




Then Select **<Ok>** to save changes.

Your **sssd.conf** configuration file is located at */etc/sssd/sssd.conf*. Whenever there is a change in the file, restart is required.

```
sudo systemctl restart sssd
```

Status should be running.

```
systemctl status sssd
```

If the integration is working, it should be possible to get an AD user info.

```
$ id jmutai
uid=1783929917(jmutai@example.com) gid=1784800513(domain
users@example.com) groups=1783870513(domain users@example.com)
```

## Step 6: Control Access – Limit to user/group

Access to the server enrolled can be limited by allowing only specific users/ and groups.

**Limit to users**

To permit a user access via SSH and console, use the command:

```
sudo realm permit user1@example.com
sudo realm permit user2@example.com user3@example.com
```

**Permit access to group – Examples**

```
sudo ream permit -g sysadmins
sudo realm permit -g 'Security Users'
sudo realm permit 'Domain Users' 'admin users'
```

This will modify *sssd.conf* file.

If instead you like to allow all users access, run:

```
sudo realm permit --all
```

To deny all Domain users access, use:

```
sudo realm  deny --all
```

## Step 7: Configure Sudo Access

By default Domain users won't have permission to escalate privilege to root. Users have to be granted access based on usernames or groups.

Let's first create sudo permissions grants file.

```
sudo vim /etc/sudoers.d/domain_admins
```

Add single user:

```
user1@example.com        ALL=(ALL)       ALL
```

Add another user:

```
user1@example.com     ALL=(ALL)   ALL
user2@example.com     ALL=(ALL)   ALL
```

Add group

```
%group1@example.com     ALL=(ALL)   ALL
```

Add group with two or three names.

```
%security\ users@example.com       ALL=(ALL)       ALL
%system\ super\ admins@example.com ALL=(ALL)       ALL
```

## Step 8: Test SSH Access

Access the server remotely as user on AD allowed to login.

```
$ ssh user1@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is
SHA256:wmWcLi/lijm4zWbQ/Uf6uLMYzM7g1AnBwxzooqpB5CU.
ECDSA key fingerprint is
MD5:10:0c:cb:22:fd:28:34:c6:3e:d7:68:15:02:f9:b4:e9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known
hosts.
```

This is a confirmation that our configuration was successful. Visit realmd and sssd wiki pages to learn more.

Tags:

- Join Ubuntu 22.04|20.04|18.04 to Windows domain
- Join Ubuntu 22.04|20.04|18.04 to AD
- Join Ubuntu 22.04|20.04|18.04 to Active directory
- Join Ubuntu 22.04|20.04|18.04 to Samba domain
- Join Debian to Windows domain
- Join Debian to AD
- Join Debian to Active directory
- Join Debian to Samba domain

Related guides:

- Set Default Login Shell on SSSD for AD trust users using FreeIPA
- Configure FreeIPA Client on Ubuntu / CentOS 7
- Install and Configure OpenLDAP Server on Debian
- Install and configure OpenLDAP Server on Ubuntu LTS

**Josphat Mutai**

*https://computingforgeeks.com/*

Founder of Computingforgeeks. Expertise in Virtualization, Cloud, Linux/UNIX Administration, Automation,Storage Systems, Containers, Server Clustering e.t.c.