Provision & Setup Ubuntu Desktop 22.04

>prøjectsecurity_

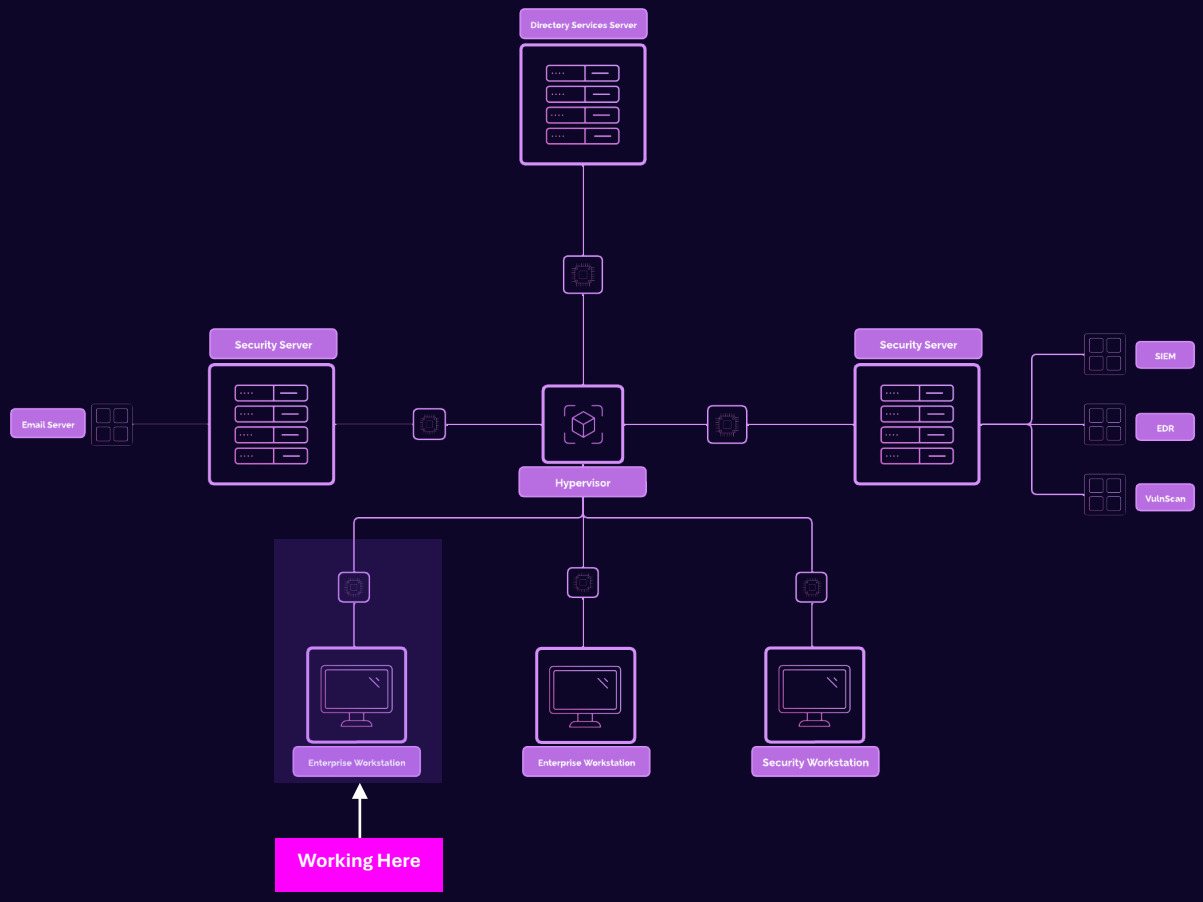
>prøjectsecurity_

Table of Contents

Prerequisites

1. Virtualbox installed.
2. Virtual Machine with Ubuntu 22.04 ISO has been configured and provisioned (the ISO should be attached to the new VM).
3. Windows Server 2025 with AD Directory Services (ADDS) configured.

Network Topology



Ubuntu Overview

What is Linux & Ubuntu?

Linux:
Linux is an open-source operating system kernel that serves as the foundation for various

distributions (distros) like Ubuntu, Debian, Fedora, and CentOS. It is known for its flexibility, stability, and security, making it a popular choice for servers, desktops, and embedded systems.

Ubuntu:
Ubuntu is a Linux distribution based on Debian, developed and maintained by Canonical. It is designed to be user-friendly, making it a go-to choice for beginners while remaining robust enough for advanced users and enterprise environments. Ubuntu is available in various editions: Desktop, Server, and Core (for IoT).

Key Features:

- **Open-Source**: Free to use, modify, and distribute.
- **Wide Compatibility**: Supports a variety of hardware and software.
- **Active Community**: Backed by a vast community and regular updates.

How is Linux used?

Linux, and specifically Ubuntu, is utilized across various fields for diverse purposes:

1. **Servers and Hosting**
    - **Web Servers**: Ubuntu is a leading choice for hosting websites, applications, and databases using services like Apache, Nginx, and MySQL.
    - **Cloud Computing**: Powers major cloud platforms like AWS, Google Cloud, and Azure.
2. **Development and Testing**
    - Popular among developers for its built-in tools, package management (APT), and scripting capabilities.
    - Ideal for DevOps workflows with support for Docker, Kubernetes, and CI/CD pipelines.

Security Implications

While Linux and Ubuntu are inherently more secure than many other operating systems, they are not immune to threats. Understanding their security implications is crucial for safe and effective usage.

Common Threats

1. **Privilege Escalation**

- Misconfigured sudo or excessive permissions can allow attackers to gain root access.

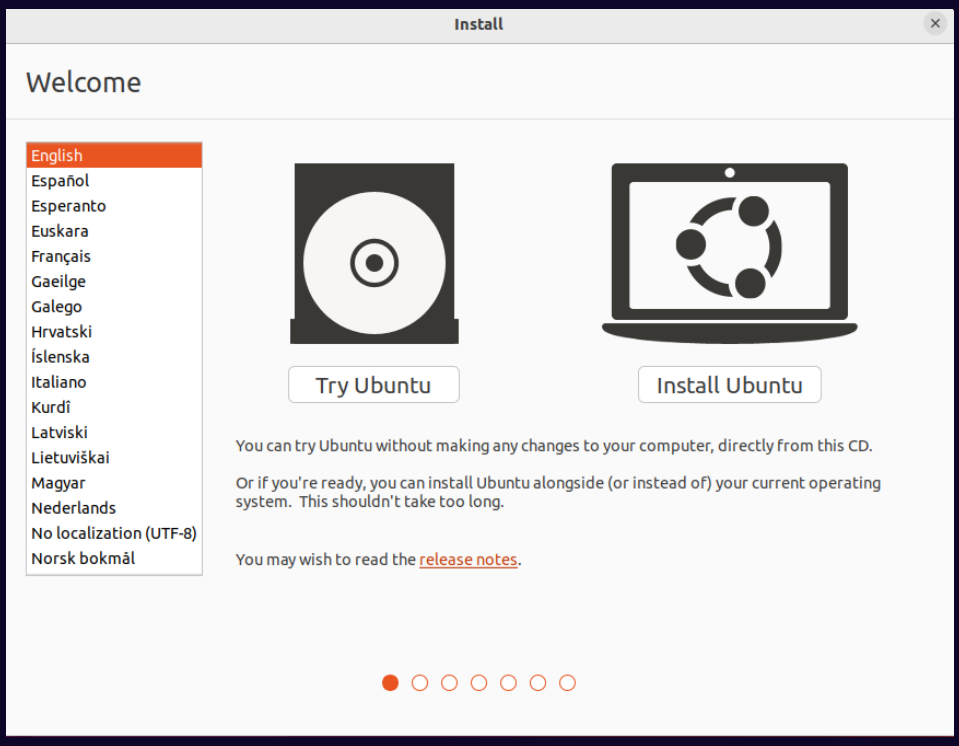
2. **Unpatched Vulnerabilities**
    - Delays in applying updates can leave systems exposed to exploits like kernel vulnerabilities.
3. **Weak SSH Configurations**
    - Using default settings or weak passwords can lead to brute-force attacks.
4. **Malware and Rootkits**
    - Though less common, Linux-specific malware and rootkits exist and can compromise systems.
5. **Supply Chain Attacks**
    - Threats can arise from malicious packages or software downloaded from untrusted sources.

Setup Ubuntu

Step 1

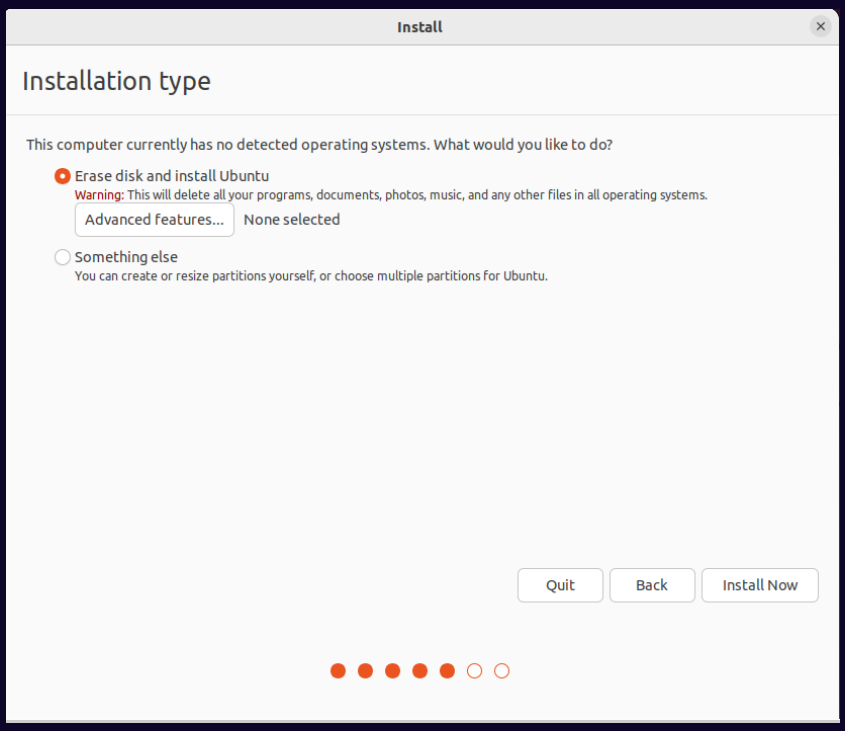
Hit “Enter”.

Choose “Install Ubuntu”.

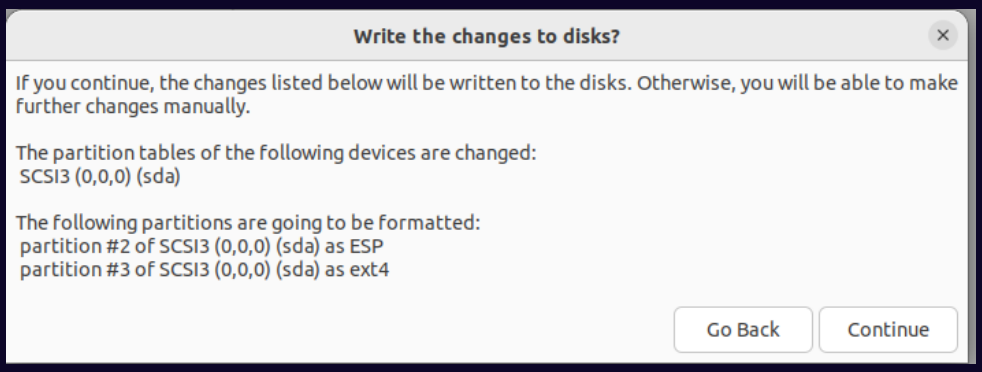


Proceed through keyboard layout. Choose defaults for “Updates and other software”.

Choose “Erase Disk and Install Ubuntu”. Then select “Install Now”.



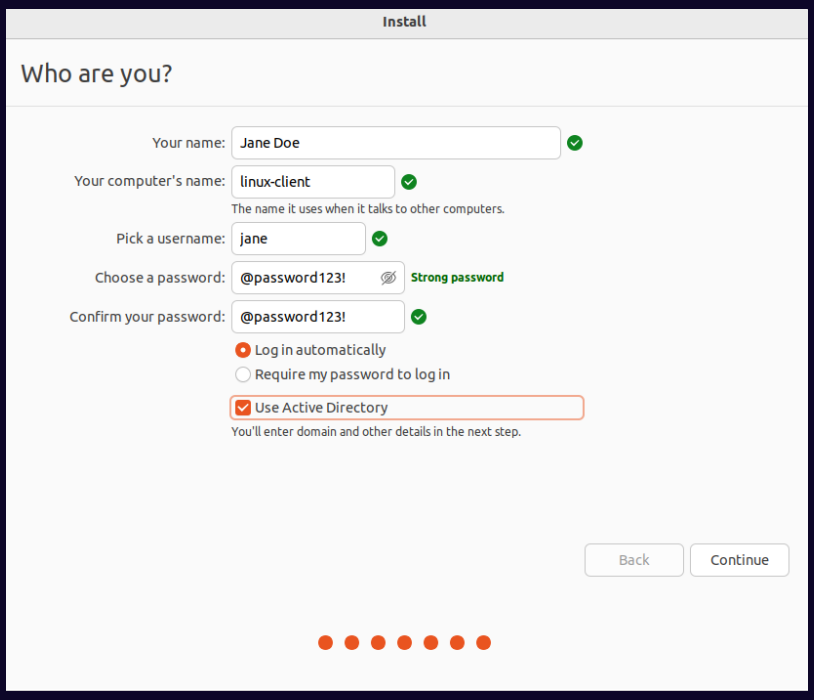
Select “Continue”.



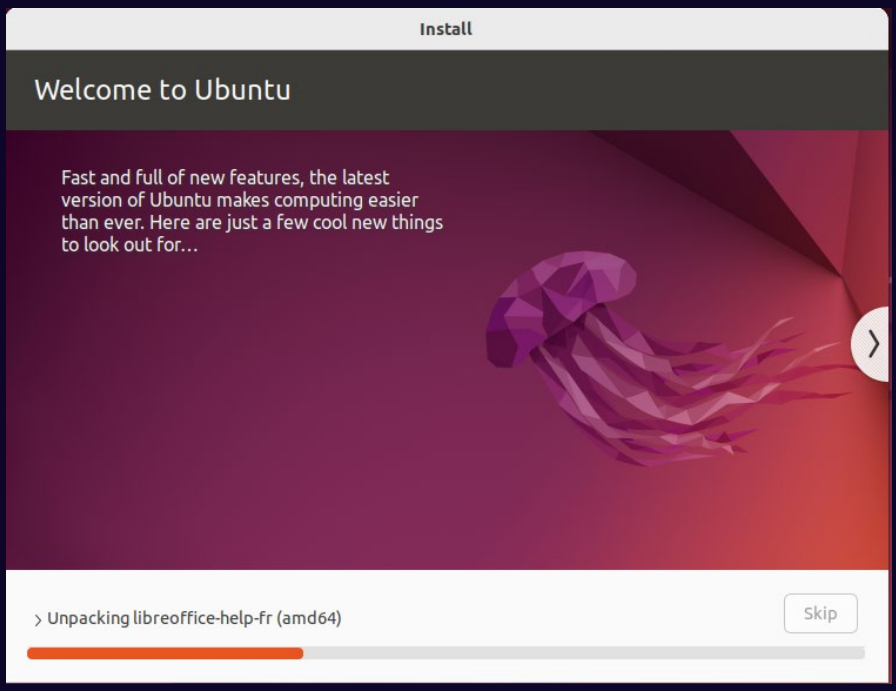
Choose whichever region you live in.

Add the following information.

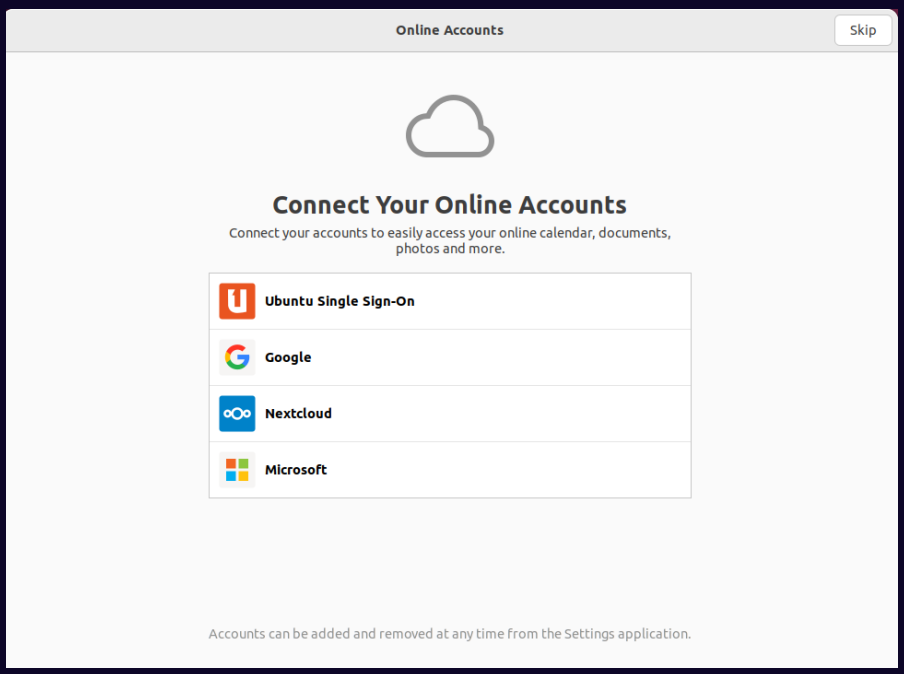
> 👉 You don’t need to Select “Use Active Directory”. (I was playing around while building this guide).



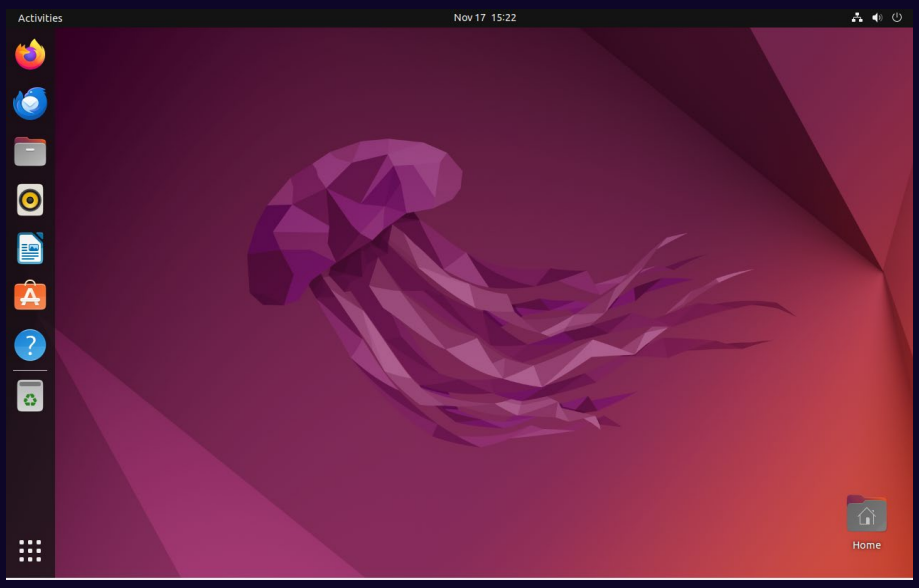
Wait for Ubuntu to install. Let the virtual machine restart and press “Enter” when it says to remove the installation medium.



Go through the wizard. Unselect “Location Services”

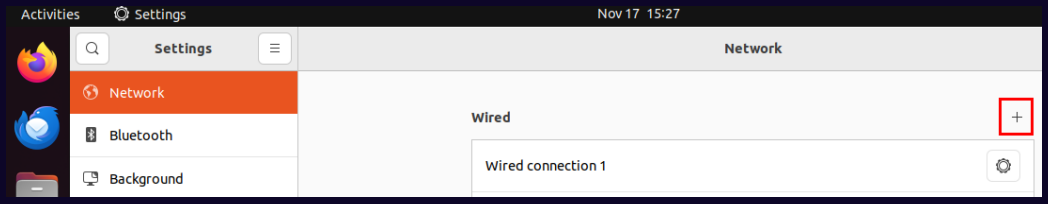


Success!

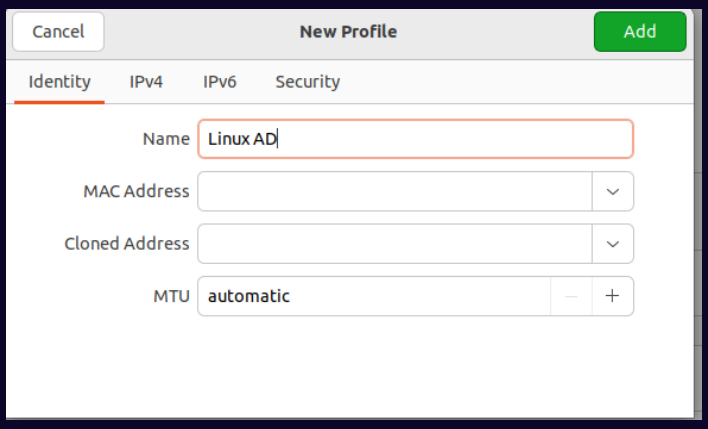


Step 2

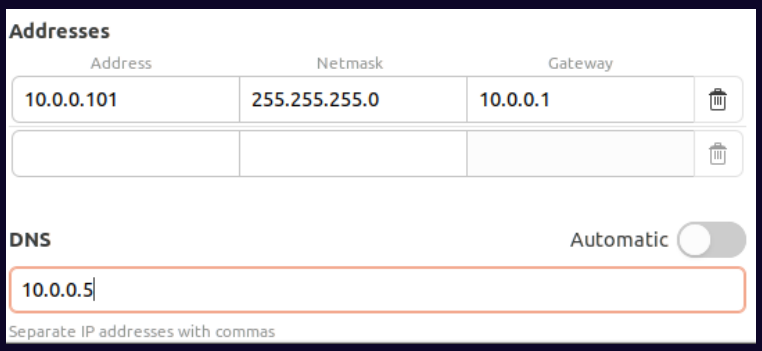
Go to “Settings” → “Network”. Choose “+” symbol to add a new network.



Name the new Wired connection “Linux AD”. Then navigate to “IPv4”.



Add the following information to set a static IP address and the Domain Controller as the DNS. Select the green “Add” button to save changes.



Make sure the Linux Desktop can reach the Windows Server Domain Controller.

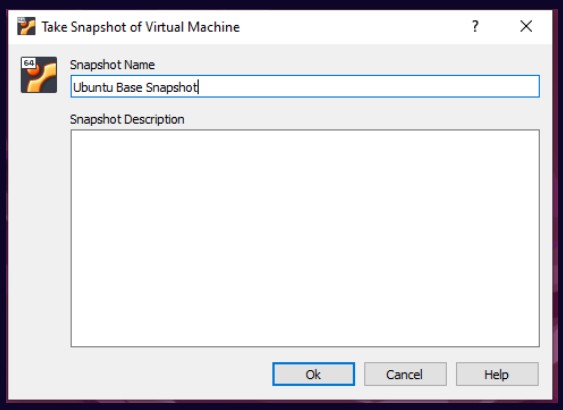
```
jane@linux-client:~$ ping -c4 10.0.0.5
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
64 bytes from 10.0.0.5: icmp_seq=1 ttl=128 time=0.446 ms
64 bytes from 10.0.0.5: icmp_seq=2 ttl=128 time=0.742 ms
64 bytes from 10.0.0.5: icmp_seq=3 ttl=128 time=0.466 ms
64 bytes from 10.0.0.5: icmp_seq=4 ttl=128 time=0.566 ms

--- 10.0.0.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3083ms
rtt min/avg/max/mdev = 0.446/0.555/0.742/0.117 ms
jane@linux-client:~$ ping -c4 corp.project-x-dc.com
PING corp.project-x-dc.com (10.0.0.5) 56(84) bytes of data.
64 bytes from 10.0.0.5 (10.0.0.5): icmp_seq=1 ttl=128 time=0.307 ms
64 bytes from 10.0.0.5 (10.0.0.5): icmp_seq=2 ttl=128 time=0.360 ms
64 bytes from 10.0.0.5 (10.0.0.5): icmp_seq=3 ttl=128 time=0.394 ms
64 bytes from 10.0.0.5 (10.0.0.5): icmp_seq=4 ttl=128 time=0.403 ms

--- corp.project-x-dc.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.307/0.366/0.403/0.037 ms
```

💡 You may not be able to ping `corp.project-x-dc.com`, that is okay at this time.

📸 **Take Snapshot!**



Connect Ubuntu Desktop to Active Directory

Since Ubuntu (and Linux-native operating systems) are not native to the Microsoft ecosystem.
Connecting Ubuntu (and Debian-based systems) to Active Directory can be accomplished in a couple ways. The easiest way is to connect Ubuntu to Active Directory with **realmd** and **SSSD** (System Security Services Daemon). **Samba Winbind** can also be used to join Linux systems if realmd / SSSD is not working.

❗ Currently realmd and SSSD integration do not work for Windows Server 2025 and Debian/Ubuntu-based systems.

About SSSD / Realmd

- **System Security Services Daemon (SSSD):** A service on Linux systems that provides a central access point for identity management and authentication. When connecting a Linux system to Active Directory (AD), SSSD allows for the integration by acting as an intermediary between the Linux system and AD needing to know what files should be edited.
- **realmd**: A tool that simplifies the process of joining Linux machines to AD domains. It automates the discovery, configuration, and enrollment of Linux systems in Active Directory, making it easier to integrate Linux systems into existing AD environments. Realmd is especially useful for administrators because it manages the complexities of setting up Kerberos, configuring LDAP settings, and ensuring proper authentication protocols.
- **realmd** is a tool that automates domain joining and manages configurations for **sssd,** which provides caching, more flexible configuration options, and better performance.

About Samba Winbind

- **Samba Winbind**: A component of the Samba suite that allows Linux systems to authenticate users against Windows Active Directory (AD) and integrate with Windows network environments. Is a more direct integration, especially useful for legacy systems and environments where tight compatibility with Windows protocols is necessary. It's often preferred when working in older Windows Server environments or where native Samba compatibility is crucial.

Realmd + SSSD

Step 1

Open a new terminal session.

Update the system with:

```
sudo apt update
```

Step 2

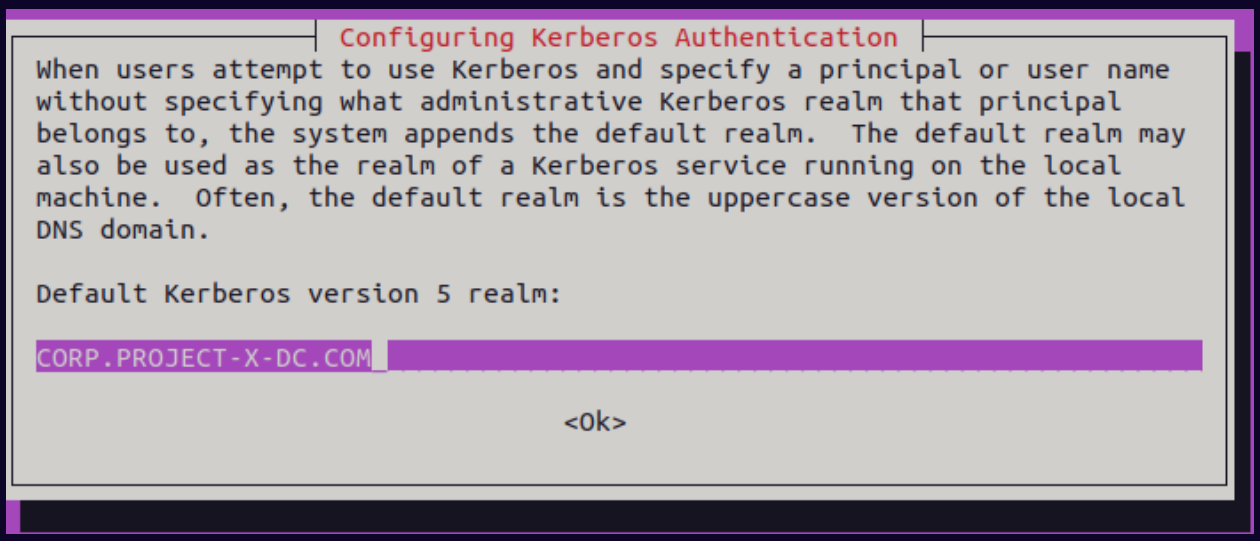
Adding the following under the [Time] block.

```
sudo nano /etc/systemd/timesyncd.conf
```

```
[Time]
NTP=corp.project-x-dc.com
#FallbackNTP=ntp.ubuntu.com
RootDistanceMaxSec=30
```

Install the necessary packages:

```
sudo apt install realmd sssd sssd-tools samba-common krb5-user
packagekit libnss-sss libpam-sss adcli samba-common-bin
```



Step 3

Use the realm command to discover the domain.

```
jane@linux-client:~$ sudo realm discover corp.project-x-dc.com
corp.project-x-dc.com
  type: kerberos
  realm-name: CORP.PROJECT-X-DC.COM
  domain-name: corp.project-x-dc.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
```

Step 4

Enter the following command, enter the Administrator password:

```
sudo realm join --verbose --user=Administrator corp.project-x-dc.com
```

Step 5

If no output is shown in the console, then the VM has been connected.

Enter the following command to confirm:

```
realm list
```

Samba Winbind

Source

Step 1

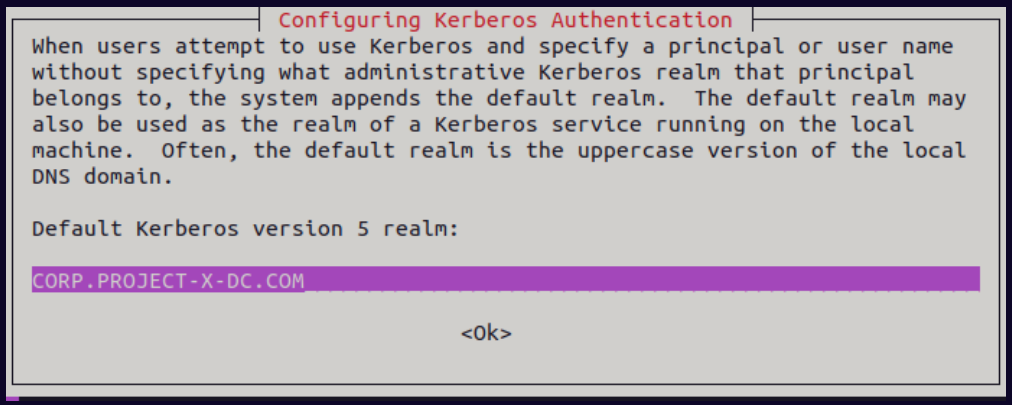
Open a new terminal session.

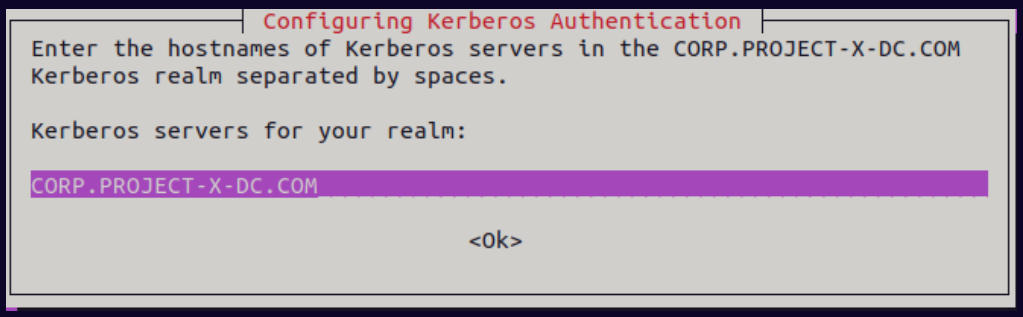
Update the system with:

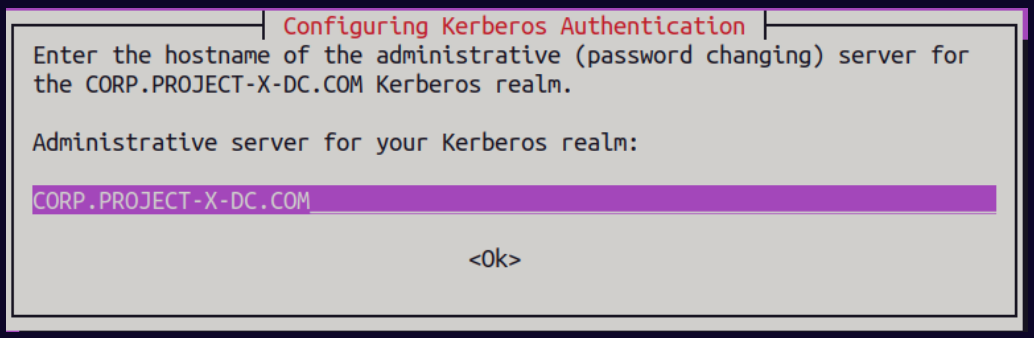
```
sudo apt update
```

Install the necessary packages:

```
sudo apt -y install winbind libpam-winbind libnss-winbind krb5-config samba-dsdb-modules samba-vfs-modules
```







Step 2

Move the smb.conf.org file:

```
sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.org
```

Step 3

```
sudo nano /etc/samba/smb.conf
```

Replace realm and workgroup with the following:

```
[global]
   kerberos method = secrets and keytab
   realm = CORP.PROJECT-X-DC.COM
   workgroup = CORP
   security = ads
   template shell = /bin/bash
   winbind enum groups = Yes
   winbind enum users = Yes
   winbind separator = +
   idmap config * : rangesize = 1000000
```

```
idmap config * : range = 1000000-19999999
idmap config * : backend = autorid
```

Step 4

Confirm `passwd` and `group` have `winbind` set as a value.

```
sudo nano /etc/nsswitch.conf
```

Add if needed.

```
passwd:         files systemd sss winbind
group:          files systemd sss winbind
shadow:         files sss
gshadow:        files
```

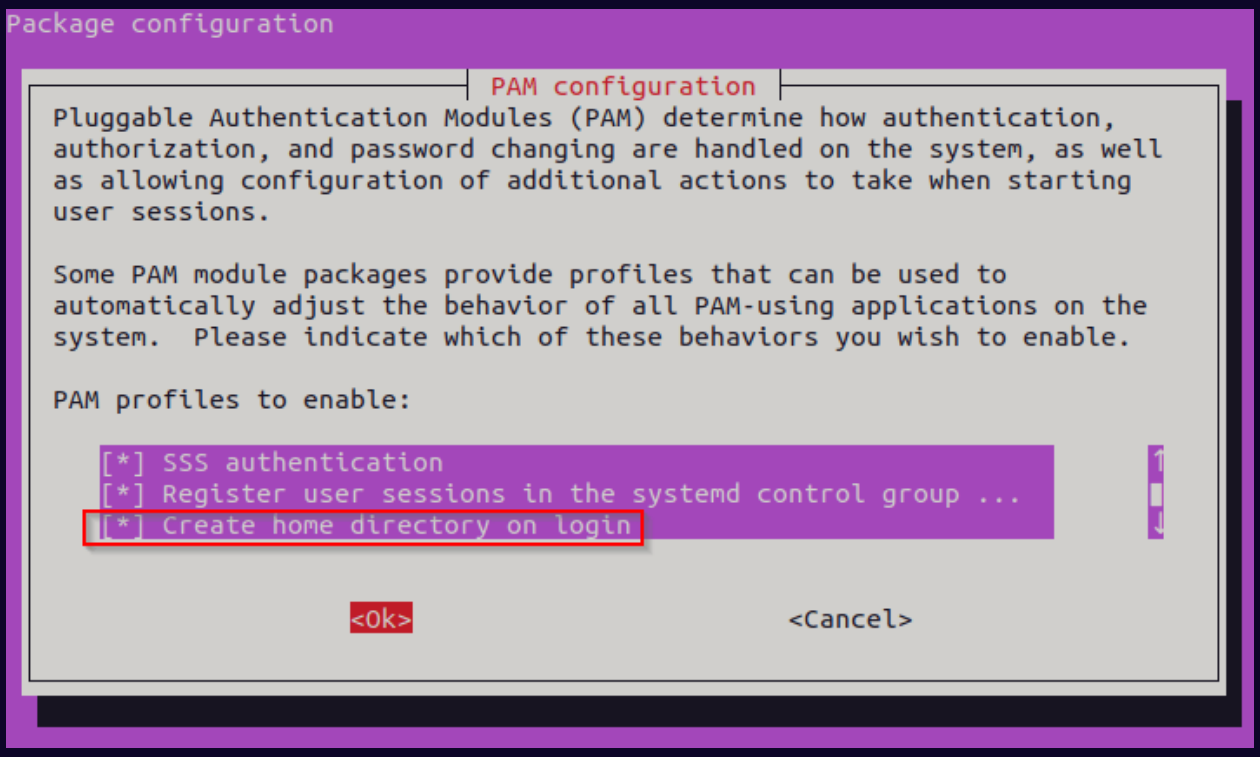
Step 5

On Ubuntu, every user that has an interactive logon to the system needs a home directory. For domain users, we need to set this before a user is able to successfully logon and start working.

Issue the following command

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

Scroll down up to the point where it states:" Create *home directory on login*". Use the space bar to select, tab to "*OK*" and hit enter.



Kudos to Michael Waterman for the screenshot!

Step 6

Change DNS settings to refer to AD.

```
sudo nano /etc/resolv.conf
```

```
nameserver 10.0.0.5
nameserver 127.0.0.53
options edns0 trust-ad
search .
```

Step 7

Join the domain with Administrator:

```
sudo net ads join -U Administrator
```

Step 8

Restart winbind:

```
systemctl restart winbind
```

Step 9

Get Active Directory services information listing.

```
net ads info
```

Step 10

List all available users.

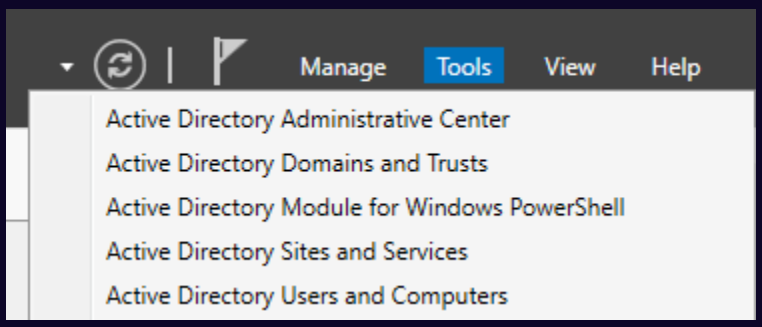
```
wbinfo -u
```

```
jane@linux-client:~$ wbinfo -u
CORP+administrator
CORP+guest
CORP+krbtgt
CORP+johnd
```

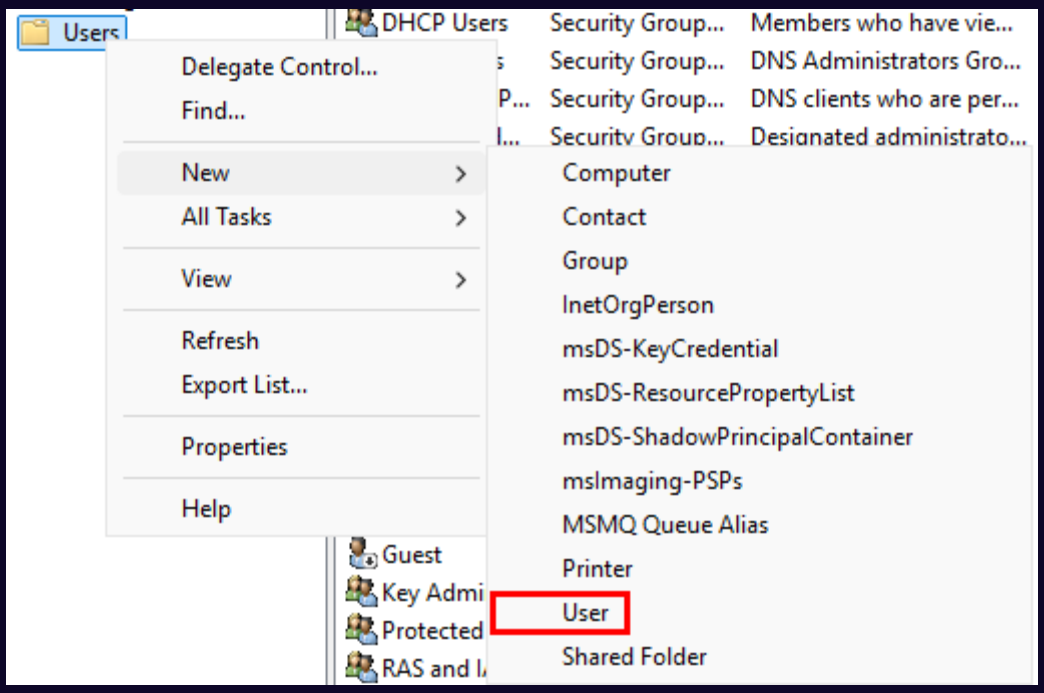
Step 11

Let's create Jane's AD account in our Domain Controller.

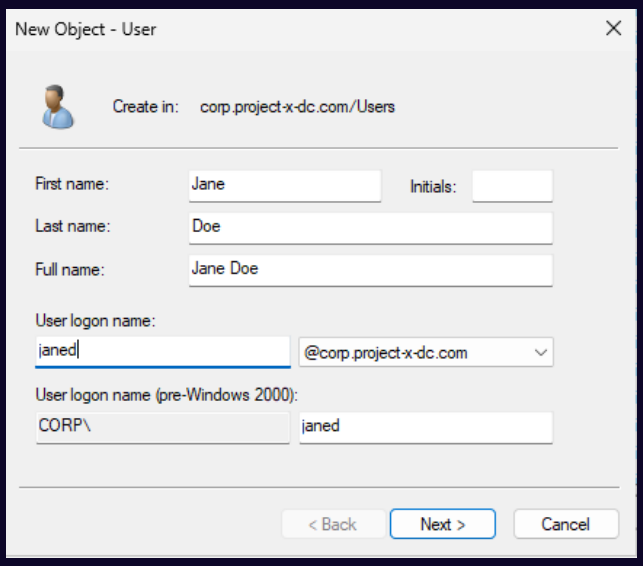
Go to Server Manager, then on the top right "Tools" → "Active Directory Users and Computers"



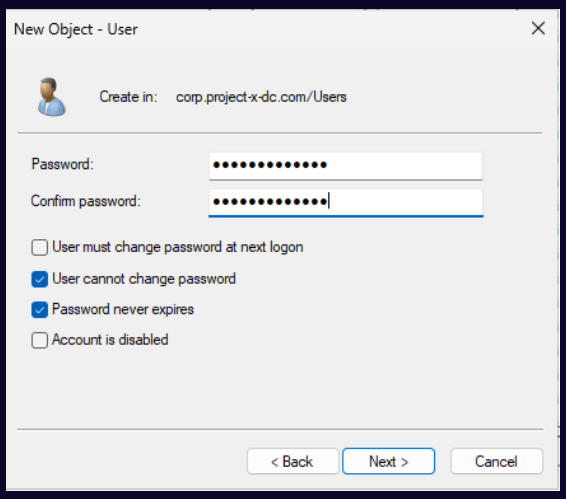
Navigate to the "Users" folder. Right-click, then go to "New" → "User"



Add the following information. Make sure Jane's username is `janed@corp.project-x-dc.com`.



Set Jane's password (`@password123!`). Refer to the Project Overview for default passwords if needed.



Clear the winbind cache by restarting the service, then see the changes reflected.

```
sudo systemctl restart winbind
```

```
wbinfo -u
```

```
jane@linux-client:~$ sudo systemctl restart winbind
jane@linux-client:~$ wbinfo -u
CORP+administrator
CORP+guest
CORP+krbtgt
CORP+johnd
CORP+janed
```

Step 12

Login as `janed`:

```
sudo login
```

```
jane@linux-client:~$ sudo login
linux-client login: CORP+janed
Password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-48-generic x86_64)
```

Step 13

Issue an `id` command to view status:

```
id
```

Success!

```
CORP+janed@linux-client:~$ id
uid=2001117(CORP+janed) gid=2000513(CORP+domain users) groups=2000513(CORP+domai
n users),2001117(CORP+janed)
```

Going back to the Server Manager, we should see “LINUX-CLIENT” under the “Computers” folder.