

Understand Catalyst Center 3.x Maglev(SSH) Password Reset Procedure

Contents

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[Requirements for On-prem \(Physical appliance\)](#)

[Requirements for Virtual Appliance \(ESXi\)](#)

[Components Used](#)

[Step 1a: Boot from Live CD \(On-prem\)](#)

[Step 1b: Boot from an Live CD \(VA - ESXi\)](#)

[Step 2a: Loading into the Ubuntu ISO](#)

[Step 2b: Mount Required Partitions](#)

[Use Case 1: Unlock Maglev Account](#)

[Step 1: Verify that maglev user is unlocked](#)

[Use Case 2: Reset Maglev User Password](#)

[Step 1: Reset the Maglev user password](#)

[Step 2: Reboot normally to Cisco Catalyst Center environment](#)

[Step 3: Update Maglev User Password from Cisco Catalyst Center CLI](#)

[Step-by-Step Video Guide](#)

Introduction

This document describes how to unlock and/or reset the password for the Maglev user for Catalyst Center 3.x physical and ESXi virtual appliance nodes.

Background Information

In the case where the Maglev account is locked out, you cannot log in to unlock it. To unlock and/or reset the password for the Maglev user, you must mount an image to the Cisco IMC vKVM for physical appliances or mount a CD ISO to the VM for ESXi virtual appliances. This allows you to access the shell and reset the user and/or password.

Prerequisites

Requirements for On-prem (Physical appliance)

- You need to download an ISO image for Ubuntu 22.04 or newer from <https://ubuntu.com/download/desktop>. This is due to how the filesystem changes in Ubuntu 22.04 with xfs.
- After the ISO has been downloaded to the local system you then need to mount the ISO to the Cisco Integrated Management Controller (CIMC) KVM.
- Once the ISO is mounted to the KVM you then need to boot from the ISO.
- Once you can access Ubuntu, mount the root and var directories to the system.
- After you have mounted the root and var directories, you can unlock and change the Maglev user account.
- Finally, you reboot the appliance, confirm you can login in with Maglev, and reset the password with the configuration wizard.

Requirements for Virtual Appliance (ESXi)

- Download ISO
- Upload ISO to the Datastore ISO File location or the Content Library in vSphere/vCenter
- Add a CD/DVD rom to the VM (virtual machine)
- Change the boot delay to a larger value

Components Used

This operation was run on Ubuntu 25.10 image; a different image produces different times and results.

It has been seen in some environments to take up to 2 hours to reach the Ubuntu desktop but for most customers the process completes within 30 minutes.

This operation is not restricted strictly to the Ubuntu desktop version. All that is required is access to the shell. Any Ubuntu image at version 22.04 or newer that provides shell access works for this operation. Other images can also work such as Gentoo and Linux SystemRescue, however Cisco recommends using Ubuntu 25.10. Any other attempt is at the risk of the user themselves.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.



Note: You can use the same procedure in a DR environment. However, note these points:

***** Ensure that disaster recovery is in a PAUSED state before attempting any password recovery/reset methods *****

In a 1+1+1 DR deployment, the corresponding site is down while this process is completed.

In a 3+3+3, If your passwords are to be updated on all three nodes, do it one node at a time to ensure that the two other nodes are available to avoid an unnecessary DR failover.

lesta

Step 1a: Boot from Live CD (On-prem)

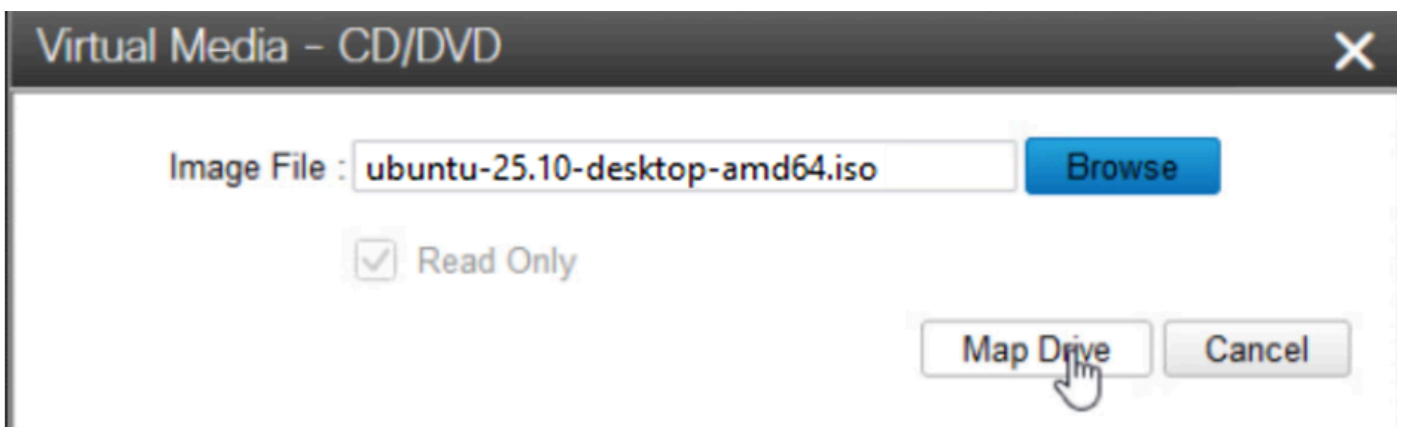
Log in to the Cisco IMC GUI, choose **Launch KVM** and then choose **Virtual Media > Activate Devices**.



Next, navigate back to **Virtual Media** and choose **Map CD/DVD**.



After that choose **Browse** and then select the Ubuntu ISO image you downloaded to your local system. After you have selected the Ubuntu image, choose the **Map Drive** button.

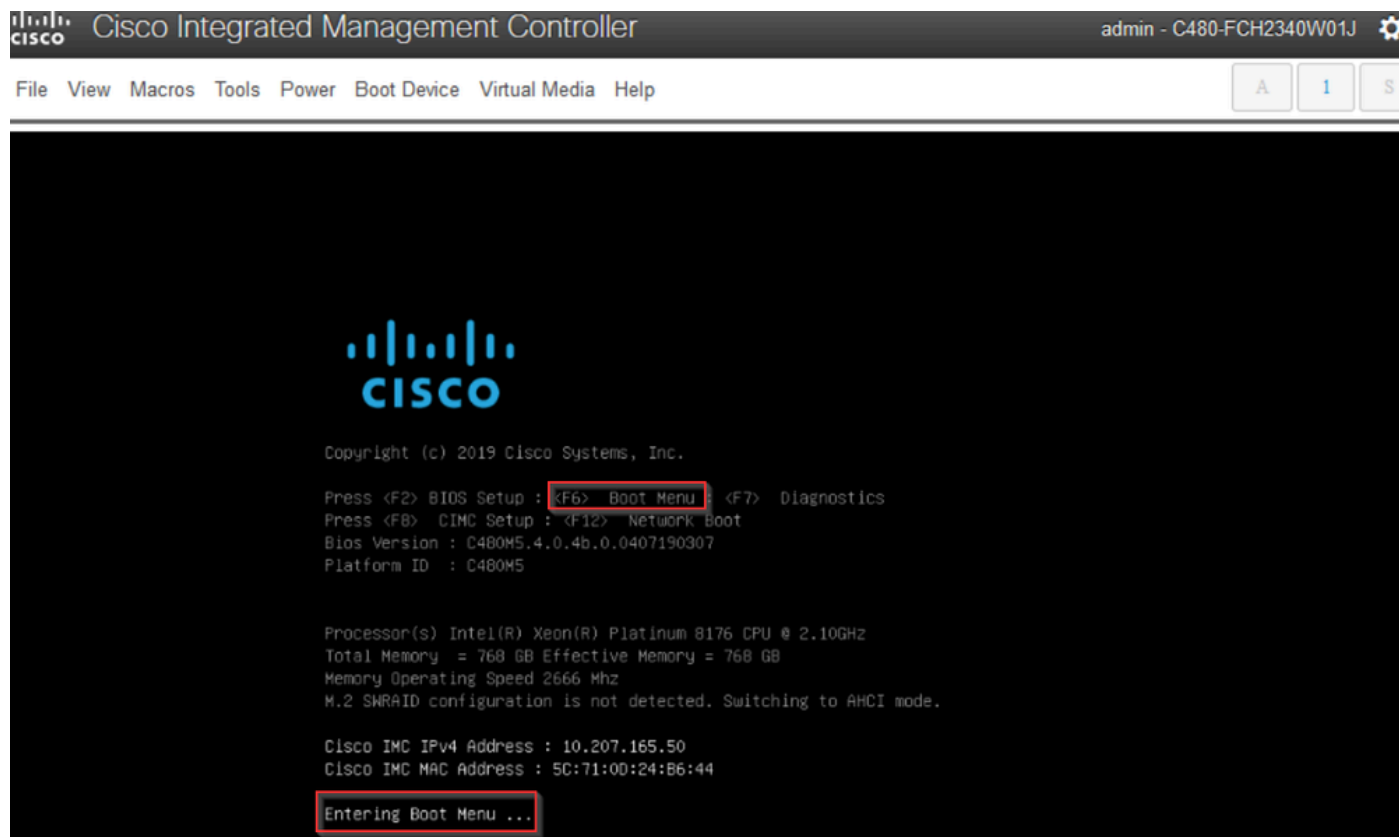


You can confirm that the image is activated and mapped by navigating back to **Virtual Media** and seeing

the ISO mapped as an option.

Next power cycle the appliance with **Power > Reset System (warm boot)**.

After the system has rebooted, press **F6** when the Cisco logo appears.



We know if it works because you see "**Entering Boot Menu ...**" at the bottom of the screen.

But a second screen appears and we can see that it is entering the boot menu. If we forgot to press **F6** on the first Cisco screen, we can press it here.

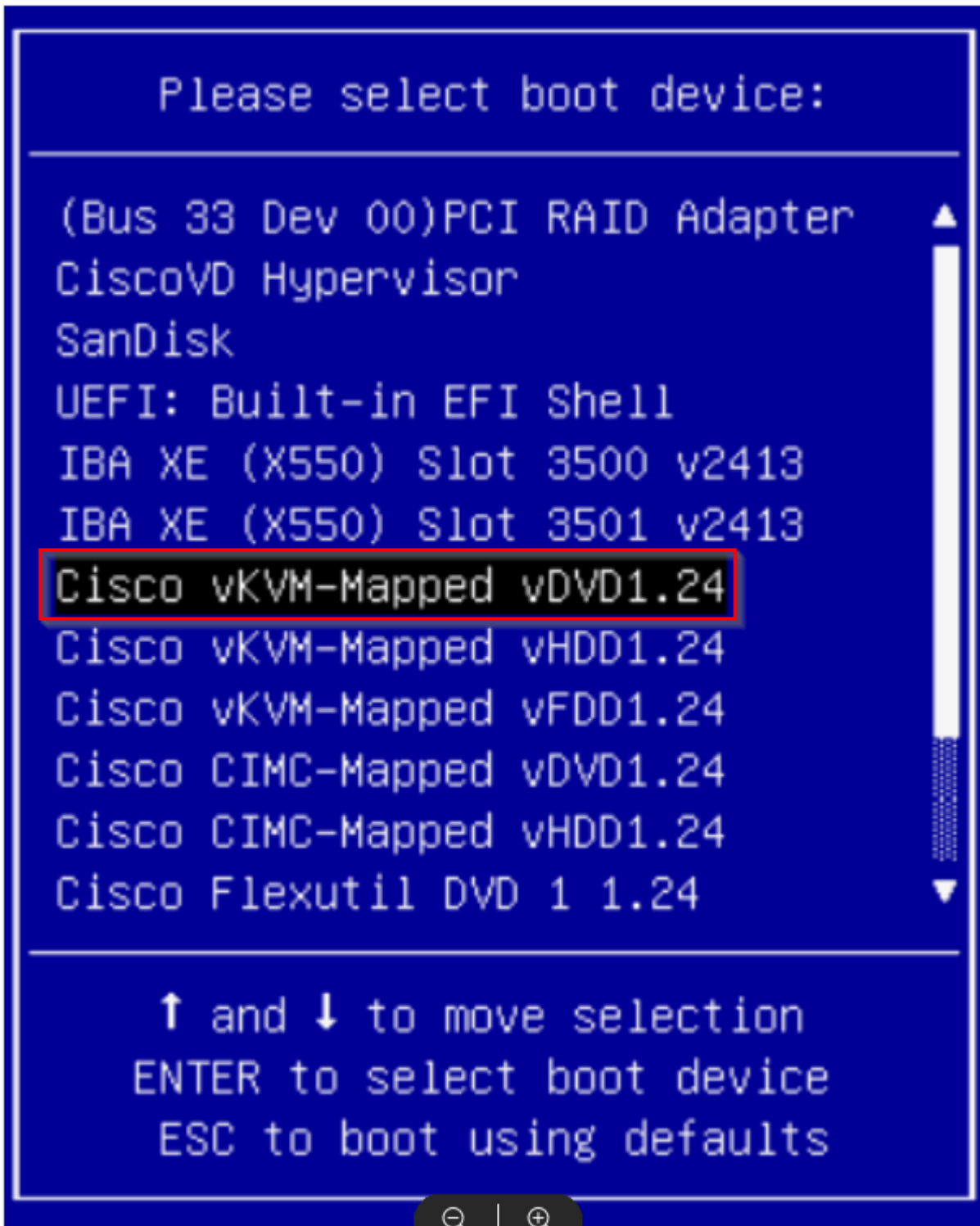
```
File View Macros Tools Power Boot Device Virtual Media Help
A 1 S

ID LUN VENDOR PRODUCT REVISION CAPACITY
-- -- -
6 0 ATA Micron_5200_MTFD U004 1831420MB
7 0 ATA Micron_5200_MTFD U004 457862MB
8 0 ATA Micron_5200_MTFD U004 1831420MB
9 0 ATA Micron_5200_MTFD U004 1831420MB
0 AVAGO Virtual Drive RAID1 456809MB
1 AVAGO Virtual Drive RAID1 1830101MB
2 AVAGO Virtual Drive RAID10 5490303MB

0 JBOD(s) found on the host adapter
3 Virtual Drive(s) found on the host adapter.

0 JBOD(s) handled by BIOS
3 Virtual Drive(s) handled by BIOS.
Press <Ctrl><R> to Run MegaRAID Configuration Utility
```

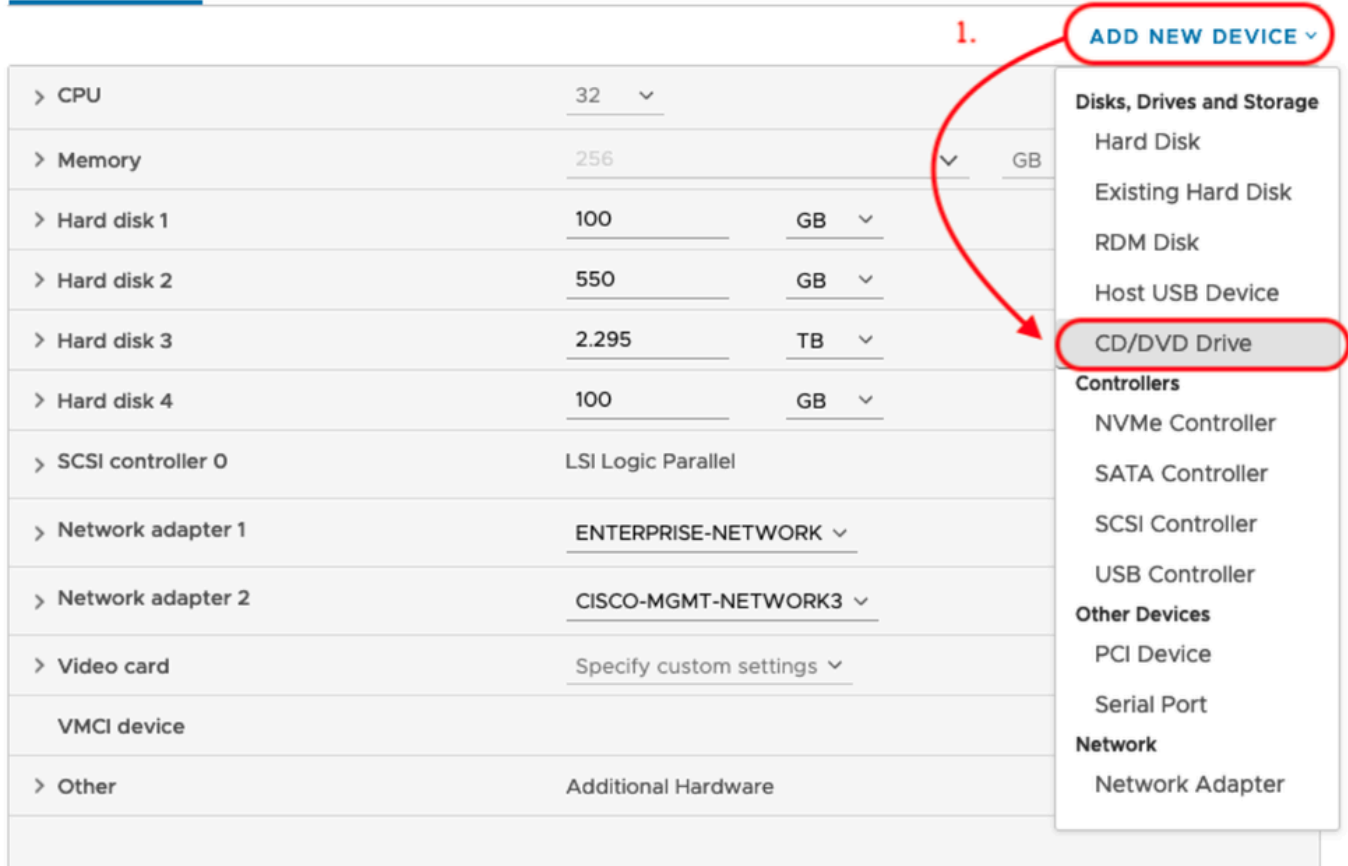
When the boot menu pops up, choose the option that says **Cisco vKVM-Mapped vDVD1.24**. This causes the appliance to boot from the mapped Ubuntu image selected earlier.



Step 1b: Boot from an Live CD (VA - ESXi)

In vCenter/vSphere navigate to where the VM is located, right-click on the VM and click **Edit Settings**. From there, click **ADD NEW DEVICE**, then choose **CD/DVD Drive**.

1.



> CPU	32	▼
> Memory	256	▼ GB
> Hard disk 1	100	GB ▼
> Hard disk 2	550	GB ▼
> Hard disk 3	2.295	TB ▼
> Hard disk 4	100	GB ▼
> SCSI controller 0	LSI Logic Parallel	
> Network adapter 1	ENTERPRISE-NETWORK ▼	
> Network adapter 2	CISCO-MGMT-NETWORK3 ▼	
> Video card	Specify custom settings ▼	
VMCI device		
> Other	Additional Hardware	

- ADD NEW DEVICE ▼
- Disks, Drives and Storage
 - Hard Disk
 - Existing Hard Disk
 - RDM Disk
 - Host USB Device
 - CD/DVD Drive
- Controllers
 - NVMe Controller
 - SATA Controller
 - SCSI Controller
 - USB Controller
- Other Devices
 - PCI Device
 - Serial Port
- Network
 - Network Adapter

The CD/DVD drive now shows in the settings page as **New CD/DVD Drive**. If you have uploaded the ISO to the **Datastore ISO File** then choose that option for the CD/DVD. Otherwise, choose **Content Library ISO File**.

Edit Settings



Virtual Hardware | VM Options

ADD NEW DEVICE ▾

> CPU	32 ▾			
> Memory	256	▾	GB ▾	
> Hard disk 1	100		GB ▾	
> Hard disk 2	550		GB ▾	
> Hard disk 3	2.295		TB ▾	
> Hard disk 4	100		GB ▾	
> SCSI controller 0	LSI Logic Parallel			
> Network adapter 1	ENTERPRISE-NETWORK ▾			<input checked="" type="checkbox"/> Connected
> Network adapter 2	CISCO-MGMT-NETWORK3 ▾			<input checked="" type="checkbox"/> Connected
> New CD/DVD Drive *	<input checked="" type="checkbox"/> Client Device			<input type="checkbox"/> Connected
> Video card	2.	<input type="checkbox"/> Datastore ISO File	<input checked="" type="checkbox"/> Content Library ISO File	** Select ISO file from Datastore or Content Library
VMCI device				
New SATA Controller	New SATA Controller			
> Other	Additional Hardware			

Select the ISO file to boot from. For this procedure, use the **Ubuntu 25.10** ISO.

Choose an ISO image to mount



3.

Name	Content Library	Description	Size	Last Modified Date
<input checked="" type="radio"/> CentOS-7-x86_64-DVD-2207-02	Cisco Software - OV A Images		4.42 GB	Oct 2, 2023 11: AM
<input type="radio"/> en-us_windows_11_iot_enterprise_version_23h2_x64_dvd_fb37549c	Microsoft-Content		5.82 GB	Nov 8, 2023 12 AM
<input type="radio"/> en-us_windows_11_business_editions_version_23h2_x64_dvd_a9092734	Microsoft-Content		6.12 GB	Nov 8, 2023 12 AM
<input type="radio"/> en-us_windows_11_consumer_editions_version_23h2_x64_dvd_8ea907fb	Microsoft-Content		6.24 GB	Nov 8, 2023 12 AM

**** Select your desired ISO File to boot from**

CANCEL

OK

Next, make sure to enable the box for **Connected** to the right of the **New CD/DVD Drive**.

Edit Settings



Virtual Hardware | VM Options

ADD NEW DEVICE ▾

> CPU	32 ▾	
> Memory	256 ▾ GB ▾	
> Hard disk 1	100 GB ▾	
> Hard disk 2	550 GB ▾	
> Hard disk 3	2.295 TB ▾	
> Hard disk 4	100 GB ▾	
> SCSI controller 0	LSI Logic Parallel	
> Network adapter 1	ENTERPRISE-NETWORK ▾	<input checked="" type="checkbox"/> Connected
> Network adapter 2	CISCO-MGMT-NETWORK3 ▾	<input checked="" type="checkbox"/> Connected
> New CD/DVD Drive *	Content Library ISO File ▾	4. <input checked="" type="checkbox"/> Connected
> Video card	Specify custom settings ▾	** Click "Connected" and save settings
VMCI device		
New SATA Controller	New SATA Controller	
> Other	Additional Hardware	

Click **VM Options** at the top of the settings screen. Then click the down arrow for **Boot Options** and change the value for **Boot Delay** to a larger value, such as 10000. This gives you time to see the option to enter the boot menu after restarting the VM.

Virtual Hardware **VM Options**

> General Options	VM Name: apic-em-cluster-
> VMware Remote Console Options	<input type="checkbox"/> Lock the guest operating system when the last remote user disconnects
> Encryption	Expand for encryption settings
> Power management	Expand for power management settings
> VMware Tools	Expand for VMware Tools settings
> Boot Options	
Firmware	BIOS (recommended) ▾
Boot Delay	When powering on or resetting, delay boot order by 10000 milliseconds
Force BIOS setup	<input type="checkbox"/> During the next boot, force entry into the BIOS setup screen

CANCEL **OK**

Next, restart the VM so you can access the boot menu to boot from the ISO.

6. Launch the web console so that you can click on the boot settings as the Catalyst Center VA boots up.

At this point, you would select the CD/DVD drive with the mounted ISO file and perform your necessary tasks.

5. ** Restart the Catalyst Center VA

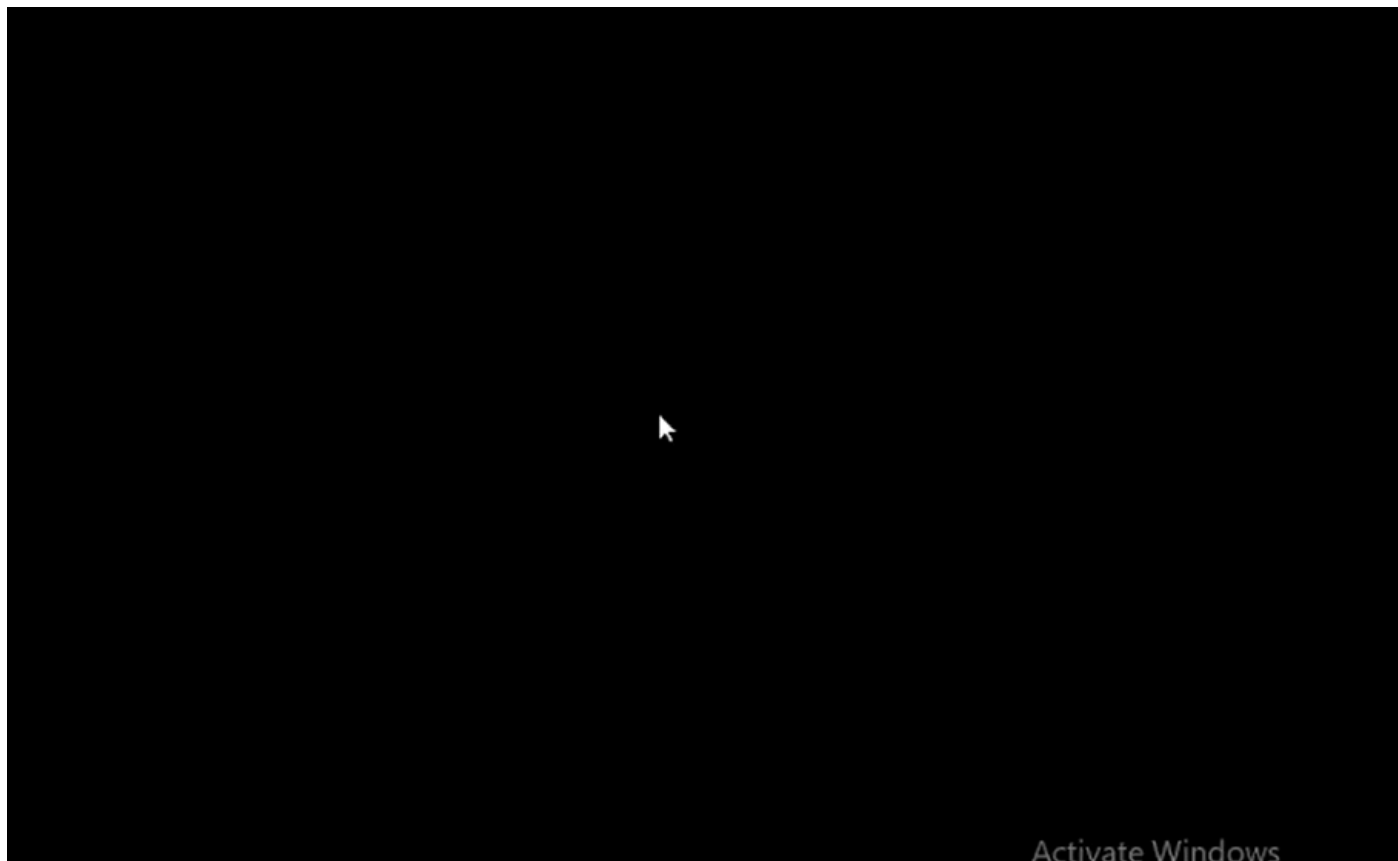
Step 2a: Loading into the Ubuntu ISO



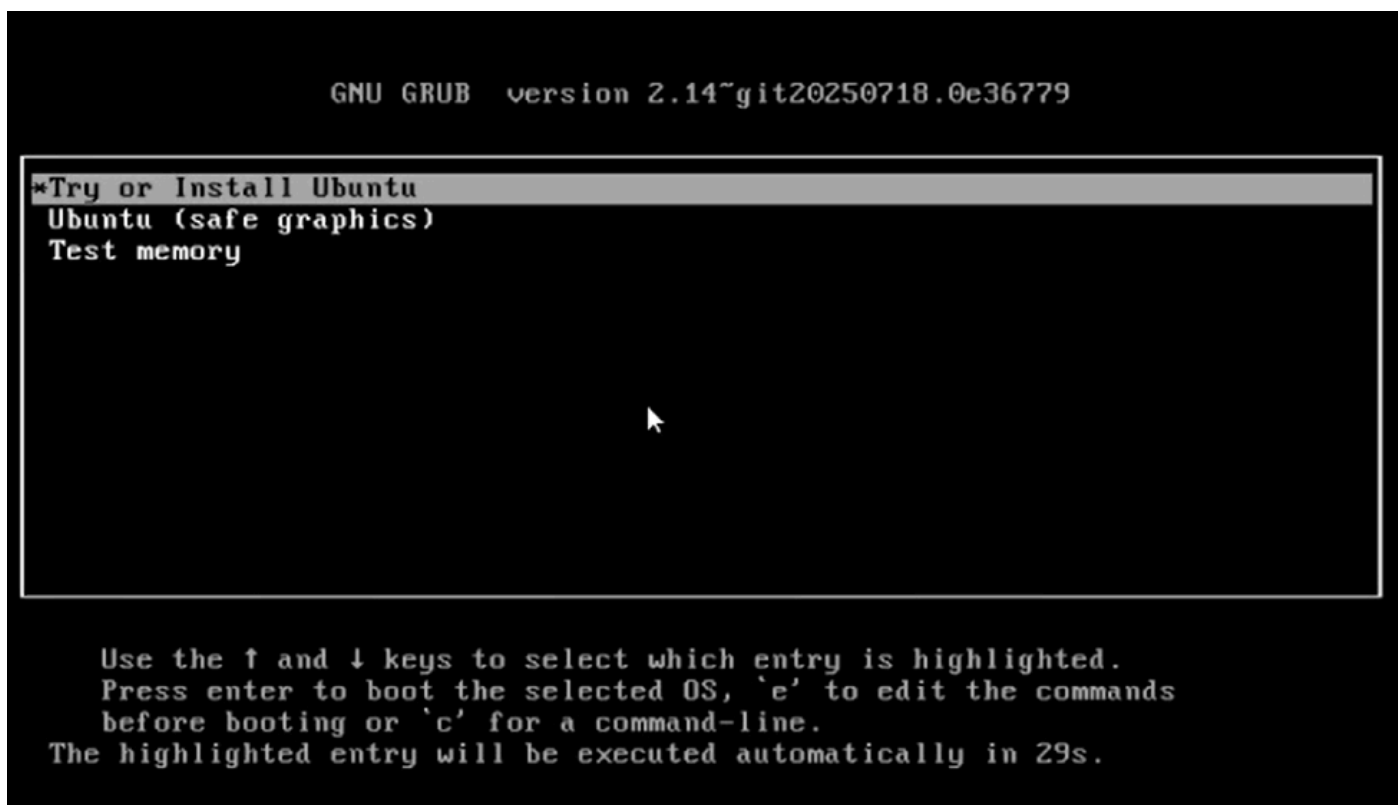
Note: *** The screen shots illustrate how long it takes to reach the Ubuntu desktop in the lab. They differs per environment and image used for recovery ***

This is the first screen we are presented with. It looks like nothing is happening but just wait. In the lab we

are on this screen for 40 seconds



After that, we were presented with these options. Choose **Try or Install Ubuntu** to proceed.



Next, the process took approximately 3 minutes to reach this screen.



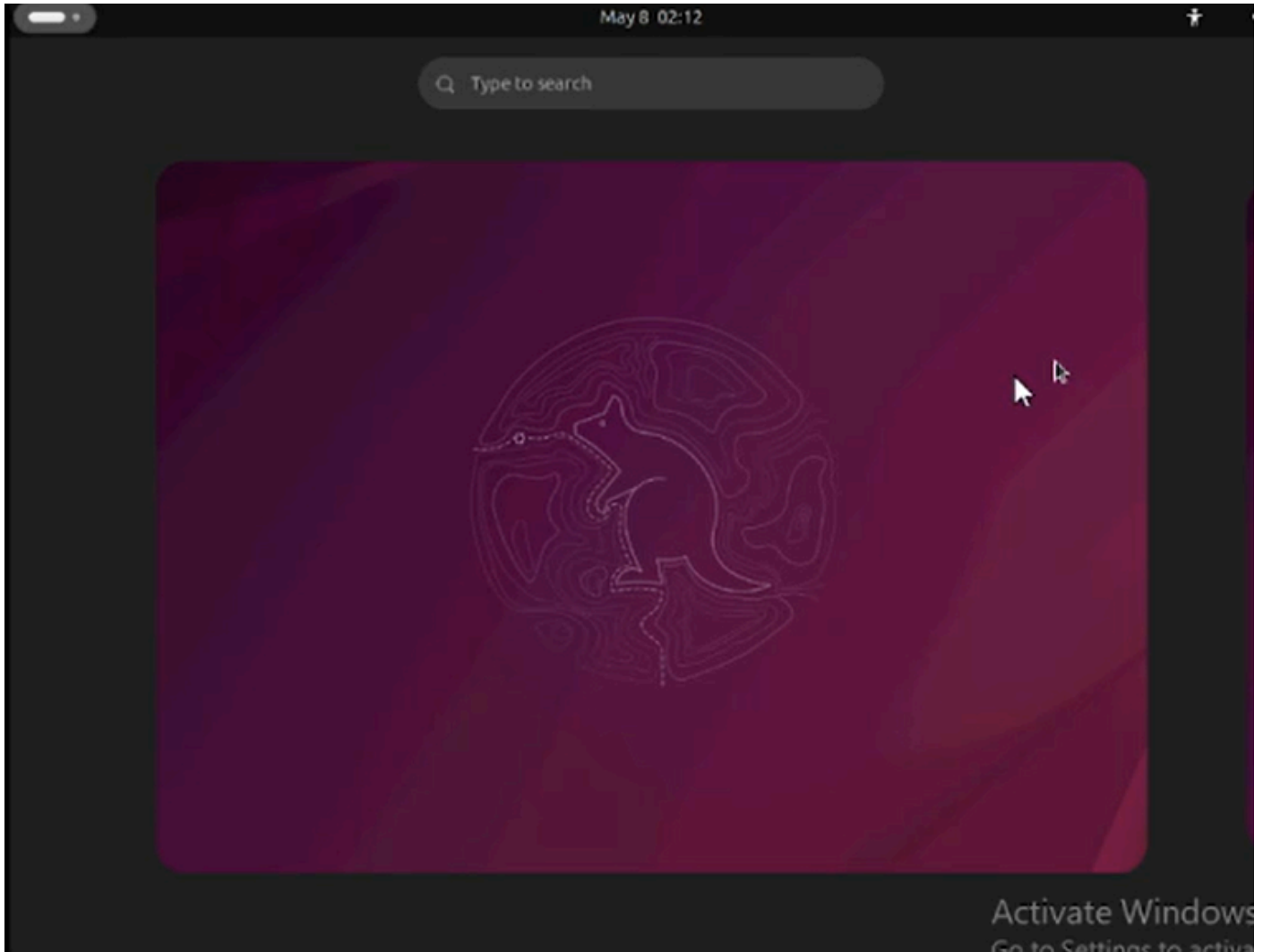
After an additional 11 minutes, the screen was still showing the Ubuntu 25.10.



Next the screen transitioned back to a black screen for about 30 seconds before showing Ubuntu 25.10 on it.



After 10 additional minutes, the screen transitioned to the Ubuntu loading screen.



The Ubuntu desktop takes roughly 5 minutes to load from here. The installer is automatically loaded and can be exited safely by clicking the X at the top-right of the installer window.



After the iinstaller is closed, open a terminal window and proceed with step 2b.

***** REMINDER: It has been seen in some environments to take up to 2 hours to get to this point. In this demonstration, it took roughly 35 minutes to reach. *****

Step 2b: Mount Required Partitions

Once you have access to the Ubuntu desktop GUI environment you need to open the terminal application and perform these steps

- Create a temporary mount point.
- Mount the root and var partitions to the system.
- Mount the pseudo filesystems to the temporary mount point.

First create the temporary mount point with the command:

```
<#root>
```

```
sudo mkdir /altsys
```

Next, we need to find the root and var partitions to mount. We can use the **lsblk -fm | egrep "var|install1"** command to find the partition to mount for "install1" (root) and "var". Make note of the partition we have identified for the mount commands in the next step

For **var**, we found a match with the **120G** partition. We can see in this case it is **sdb2**

For the **install1** (root), we found a match with the **335.6G** partition. In this example, it is **sda5**

```
ubuntu@ubuntu:~$ lsblk -fm | egrep "var|install1"
└─sda5 xfs          install1          a4d195e1-0451-4b99-b5e0-736a7f1410c6
    335.6G root    disk    brw-rw----
└─sdb2 xfs          var              2fc8657a-c41a-435e-b0d0-5359ae9b788d
    120G root     disk    brw-rw----
ubuntu@ubuntu:~$
```

Once you have identified the var and root partitions mount them:

<#root>

```
sudo mount /dev/sda5 /altsys
```

```
sudo mount /dev/sdb2 /altsys/var
```

Once root and var have been mounted, mount the psuedo filesystems:

<#root>

```
sudo mount --bind /proc /altsys/proc
```

```
sudo mount --bind /dev /altsys/dev
```

```
sudo mount --bind /sys /altsys/sys
```

The last step before you change the password or unlock the Maglev account is to change to the temporary mount environment:

<#root>

```
sudo chroot /altsys
```

Use Case 1: Unlock Maglev Account

Step 1: Verify that maglev user is unlocked

```
<#root>
```

```
grep maglev /etc/shadow
```

```
<#root>
```

```
maglev:
```

```
!
```

```
$6$jvRGoDihpcsr8X1$RUFs.Lb.2Abbgv0DfJsw4b2EnpSwiNU1wJ6NQIjEnv0tT5Svz4ePHZa4f0eUvLH17VAFca46f2nHxqMWORY
```

Check if there is an exclamation mark in front of the password hash or not. If there is, that indicates the account is locked. Type in the command to unlock the user:

Unlock the maglev user with the command:

```
<#root>
```

```
usermod -U maglev
```

Use Case 2: Reset Maglev User Password

Step 1: Reset the Maglev user password

```
<#root>
```

```
#
```

```
passwd maglev
```

Enter new UNIX password: #Enter in the desired password

Retype new UNIX password: #Re-enter the same password previously applied

Password has been already used.

passwd: password updated successfully #Indicates that the password was successfully changed

Step 2: Reboot normally to Cisco Catalyst Center environment

Click on **Power** in the KVM window and then **Reset System (warm boot)**. This causes the system to reboot and boot with the RAID controller so that the Cisco Catalyst Center software boots up.



You probably see this image stuck loading for approximately 5 to 10 minutes. This is normal. The screen eventually transition to the login screen.

Step 3: Update Maglev User Password from Cisco Catalyst Center CLI

Once the Cisco Catalyst Center software boots and you have access to the CLI, you need to change the Maglev password with the command **sudo maglev-config update**. This step is required to ensure that the change takes affect across the whole system.

Once the config wizard has been launched, you need to navigate completely through the wizard to screen that allows us to set the Maglev password in step 6.



Once the password has been set for both fields **Linux Password** and **Re-enter Linux Password**, choose **next** and complete the wizard. When the wizard finishes the configuration push, the password is

successfully changed. You can create a new SSH session or enter in the command **sudo -i** in the CLI to test that the password has been changed.

Step-by-Step Video Guide

Please use the link to access the step-by-step video created for this workflow.

Images provided by Tomas De Leon and Faisal Mehmood