Reset and Recover ISE 3.3 Password

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Password Reset Procedure

- GUI Password Reset
- CLI Password Reset

Password Recovery Procedure

- Password Recovery for SNS physical Appliance
  - Password recovery through the use of CIMC
  - Password recovery through the use of a bootable USB
- Password Recovery for ISE Virtual Machine

Introduction

This document describes CLI and GUI methods for Identity Services Engine (ISE) password reset and recovery based on the type of appliance.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of ISE.
- Basic knowledge of Cisco Integrated Management Controller.

Components Used

- ISE virtual machine (VMware version 13 for ESXi 6.5 (and later))
- ISE 3715 physical appliance

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.

Password Reset Procedure

In Cisco ISE, Web GUI and CLI passwords can be different. Complete these steps to change the password:

GUI Password Reset

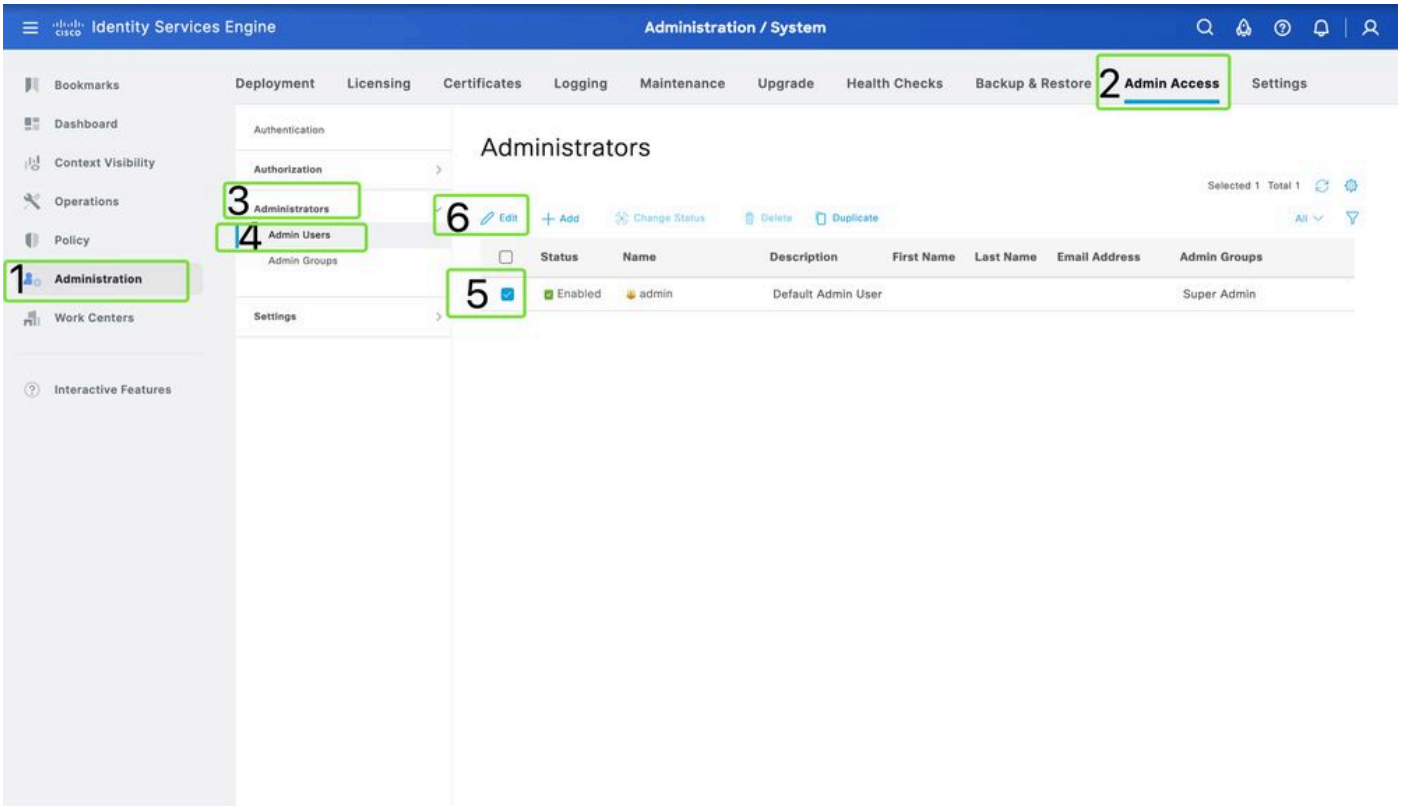
You can change the GUI password either via Web GUI or via CLI.

Using Web GUI Method

1 - 4. Navigate to **Administration > Admin Access > Administrators > Admin Users**.

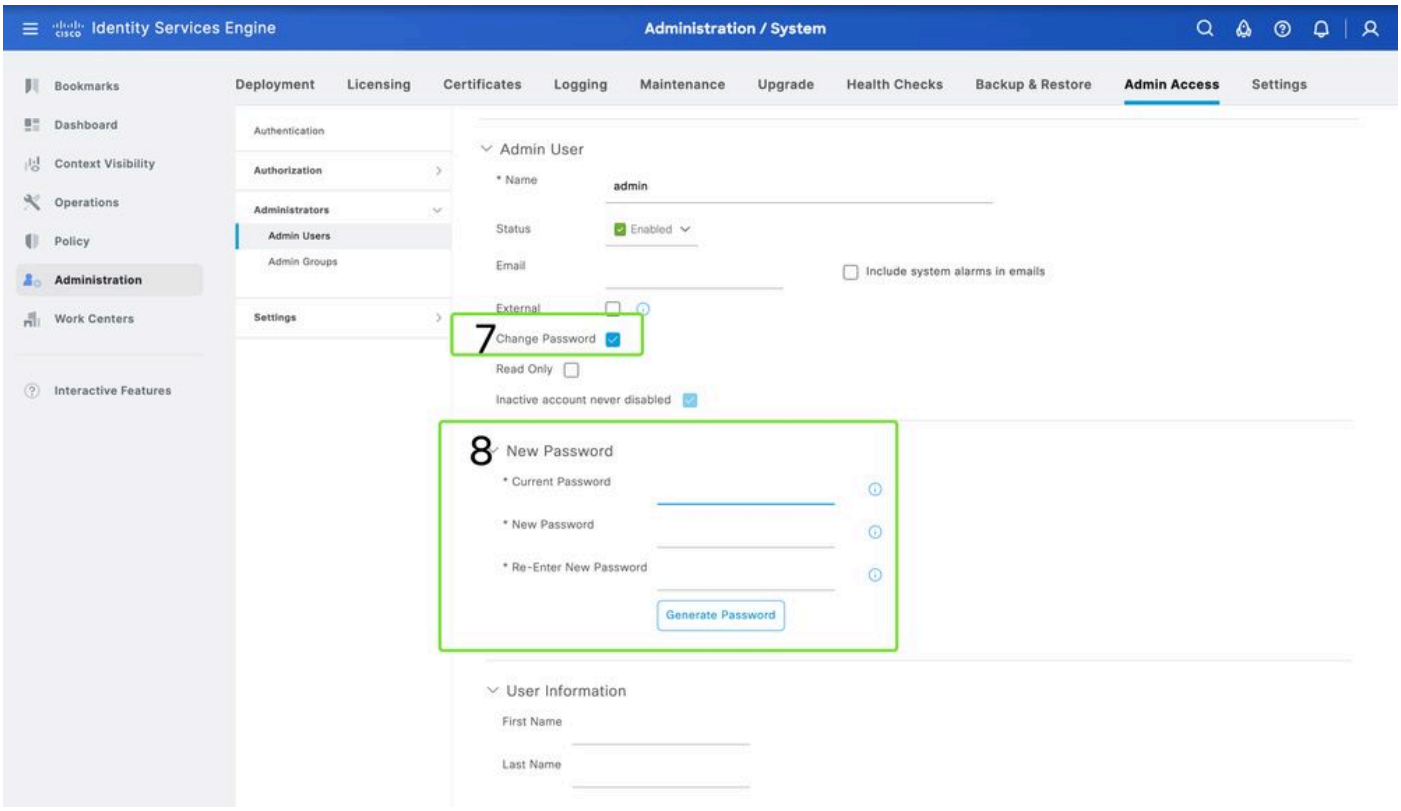
5. Select the user.

6. Click **Edit**.



7.Enable **Change Password**.

8.Enter **Current Password** and **New Password**.



Using CLI Method

In CLI, run the command **#application reset-passwd ise <username>**

This prompts you to enter the new password.

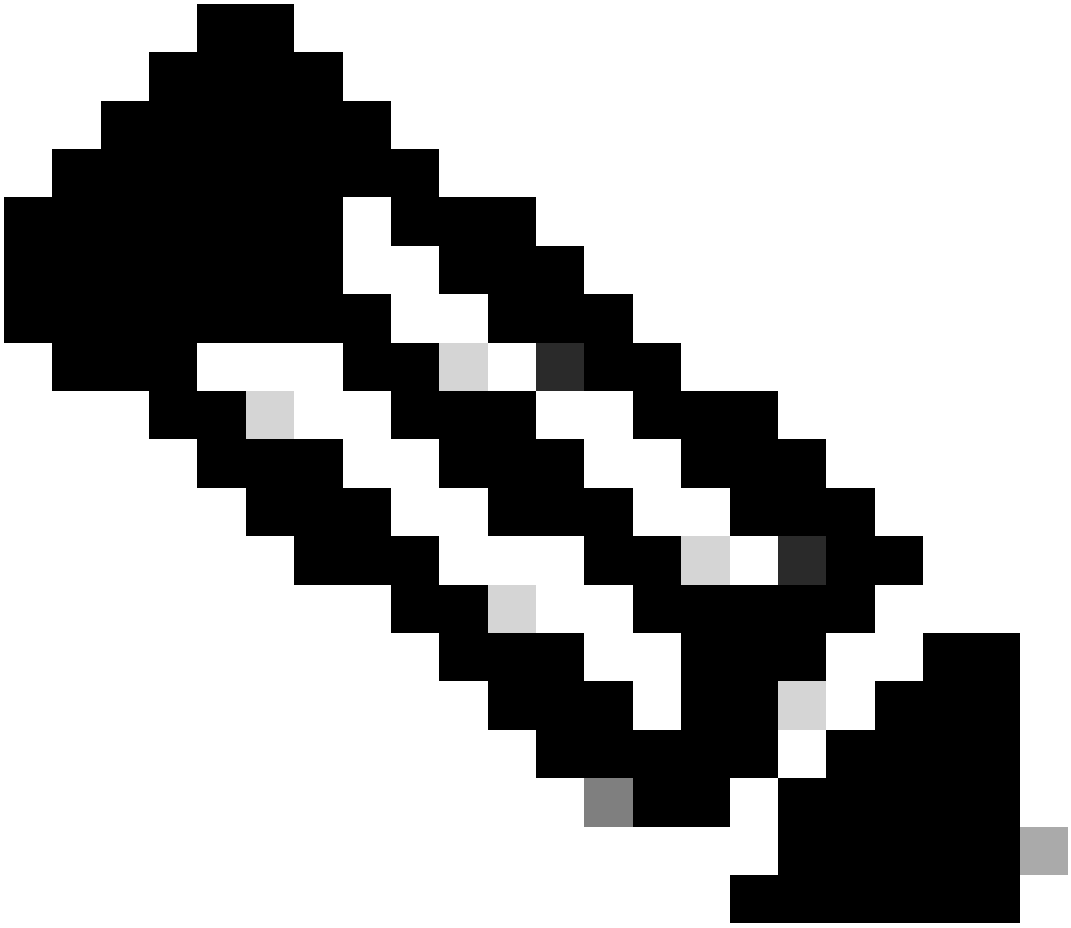
```
ise331/admin#application reset-passwd ise admin
Enter new password:
```

When the new password is entered and confirmed, the password is successfully reset.

```
ise331/admin#application reset-passwd ise admin
Enter new password:
Confirm new password:

Password reset successfully.
```

CLI Password Reset



Note: You cannot change the CLI password of ISE from your GUI. You can either do it via CLI command if you have CLI access. If you do not have CLI access, then you must perform password recovery process.

From CLI, run the command **#password** . You are prompted to enter the current password.

```
ise331/admin#password
Enter old password:
```

After correctly entering the current password, enter the new password to reset it.

```
ise331/admin#password
Enter old password:
Enter new password:
Confirm new password:
```

Password Recovery Procedure

To perform password recovery, download the ISO file from software portal.

This document is demonstrated ISE 3.3 version using **Cisco-ISE-3.3.0.430.SPA.x86_64.iso** .

Password Recovery for SNS physical Appliance

There are two methods to recover password on SNS physical appliances:

- Password recovery through the use of **Cisco Integrated Management Controller (CIMC)**
- Password recovery through the use of a bootable USB

Password recovery through the use of CIMC

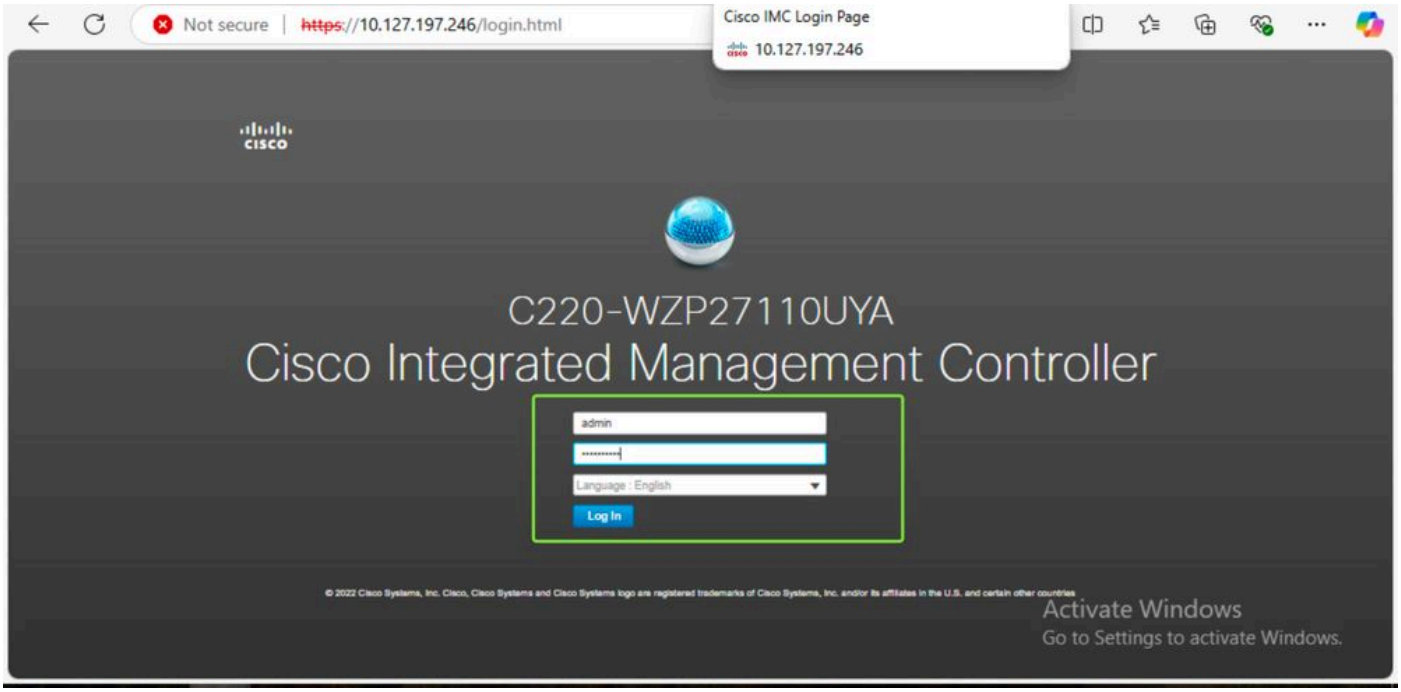
To perform Password Recovery, you need CIMC access.

If you do not have CIMC, refer to Setting Up the System With the Cisco IMC Configuration Utility to know more about CIMC configuration steps.

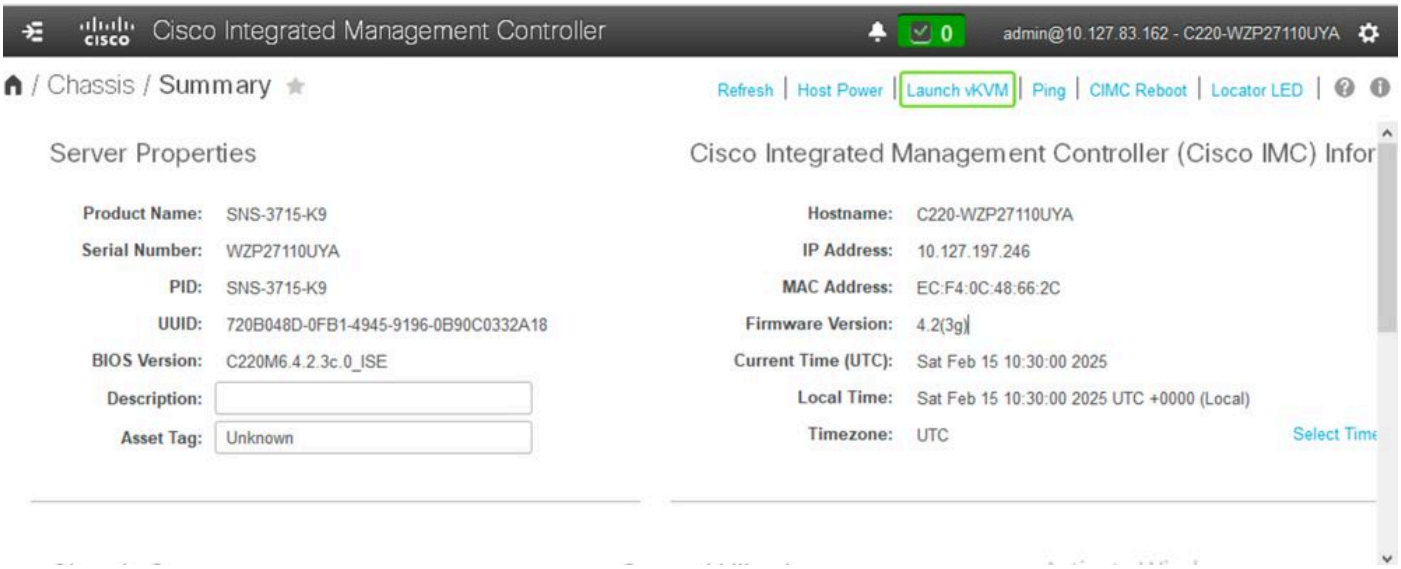
You can use CIMC connection to manage Cisco SNS-36XX, SNS-37XX appliances.

KVM utility through CIMC connection can be used to perform all operations including BIOS configuration on Cisco SNS-36XX or Cisco SNS-37XX appliance.

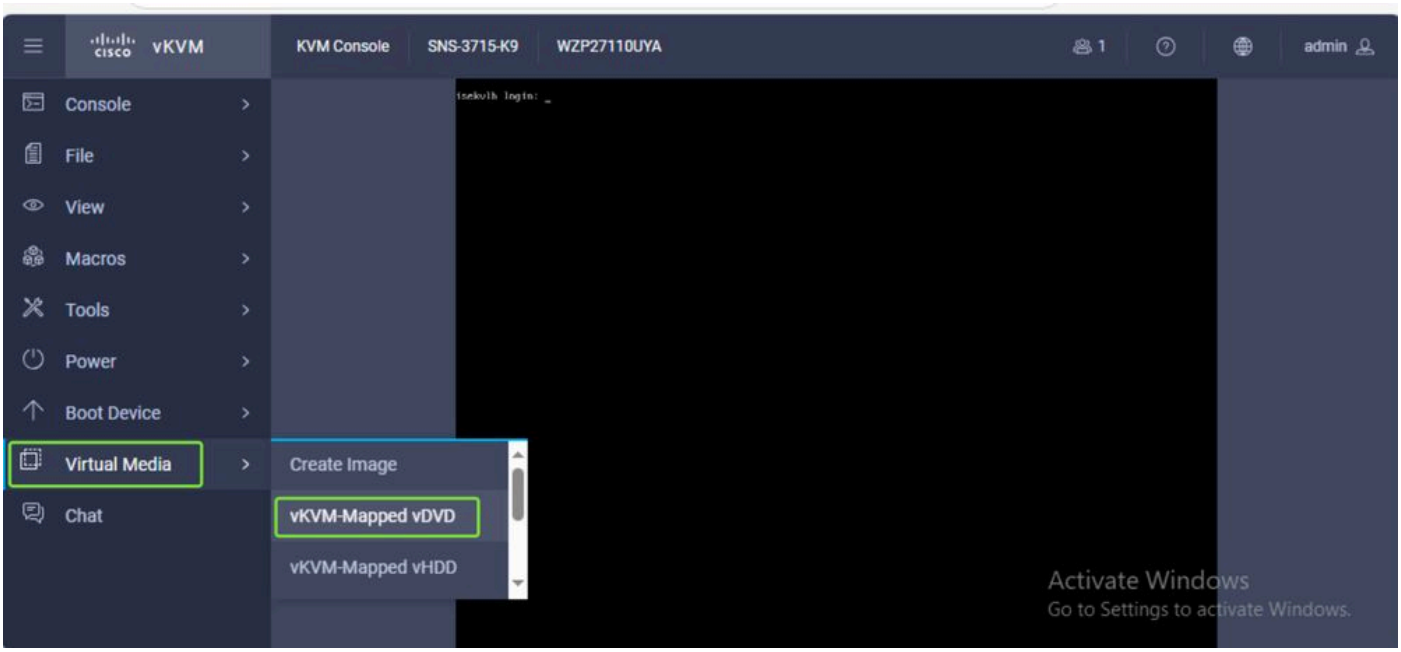
Step 1. Open any browser and search for CIMC ip address andprovide the username and password details in order to log in to the CIMC portal.



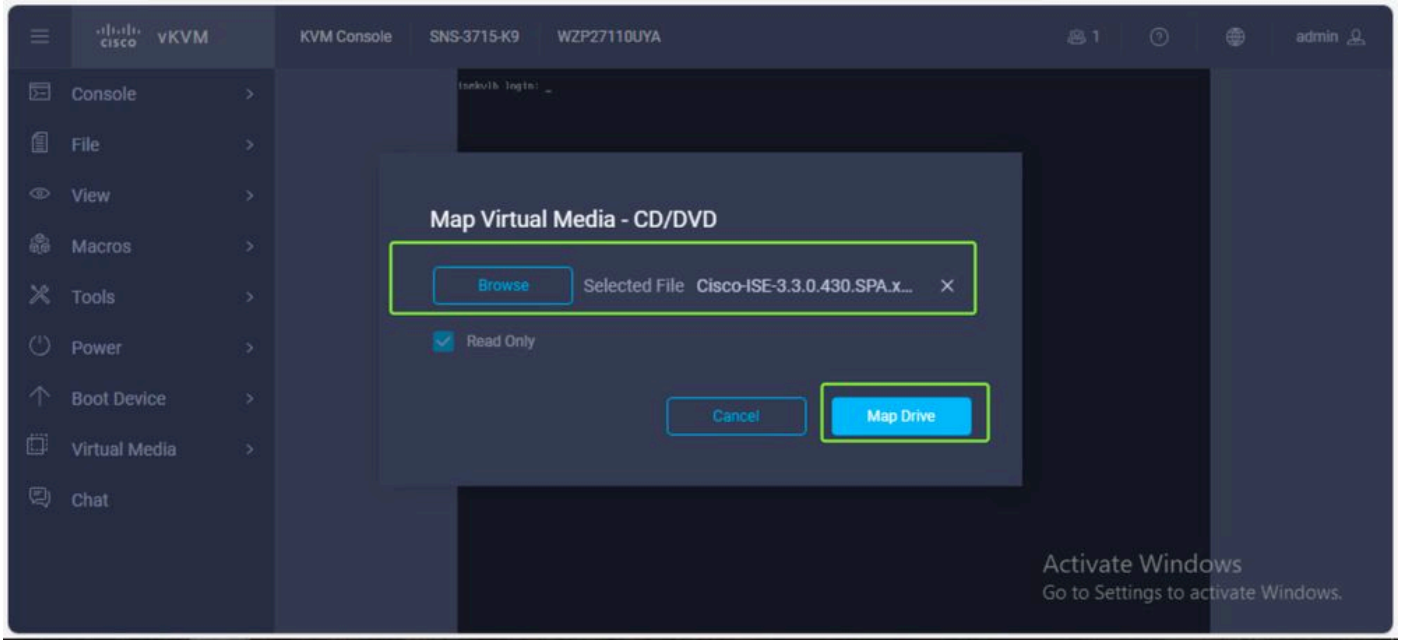
Step 2. Click**Launch KVM Console**.



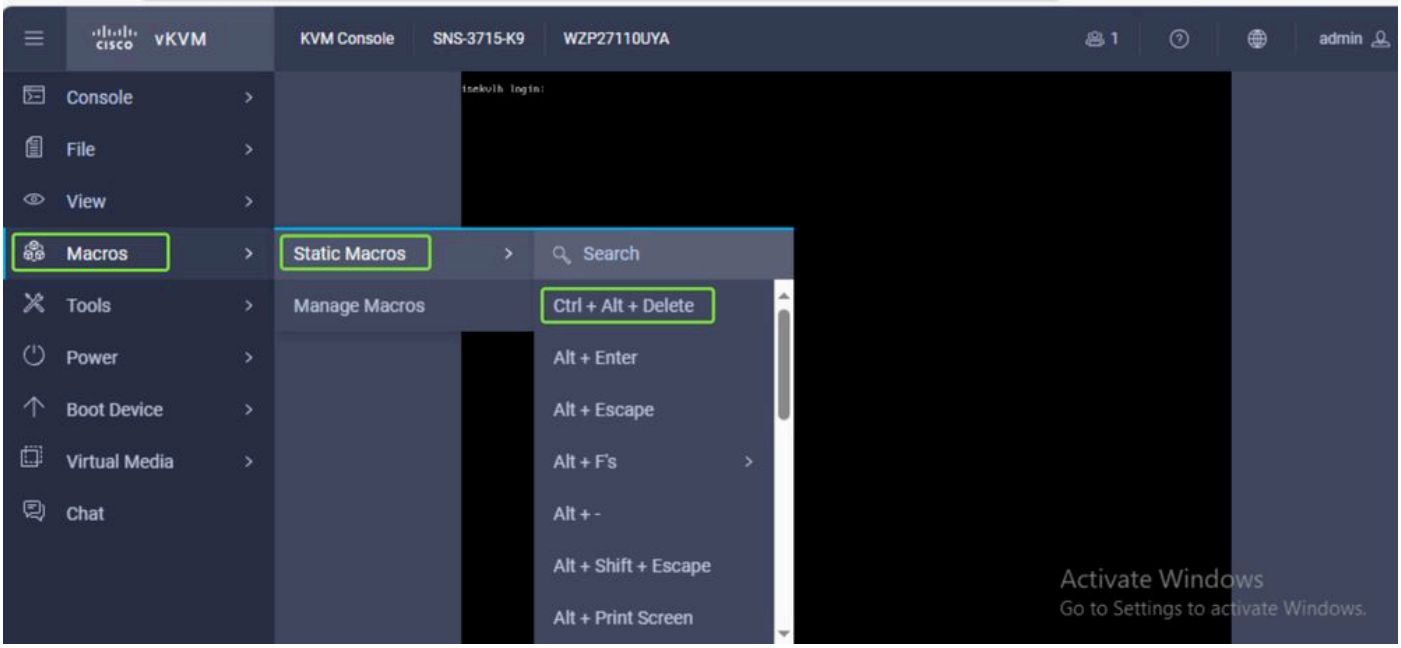
Step 3. Click the **Virtual Media**tab and select **vKVM-Mapped vDVD**.



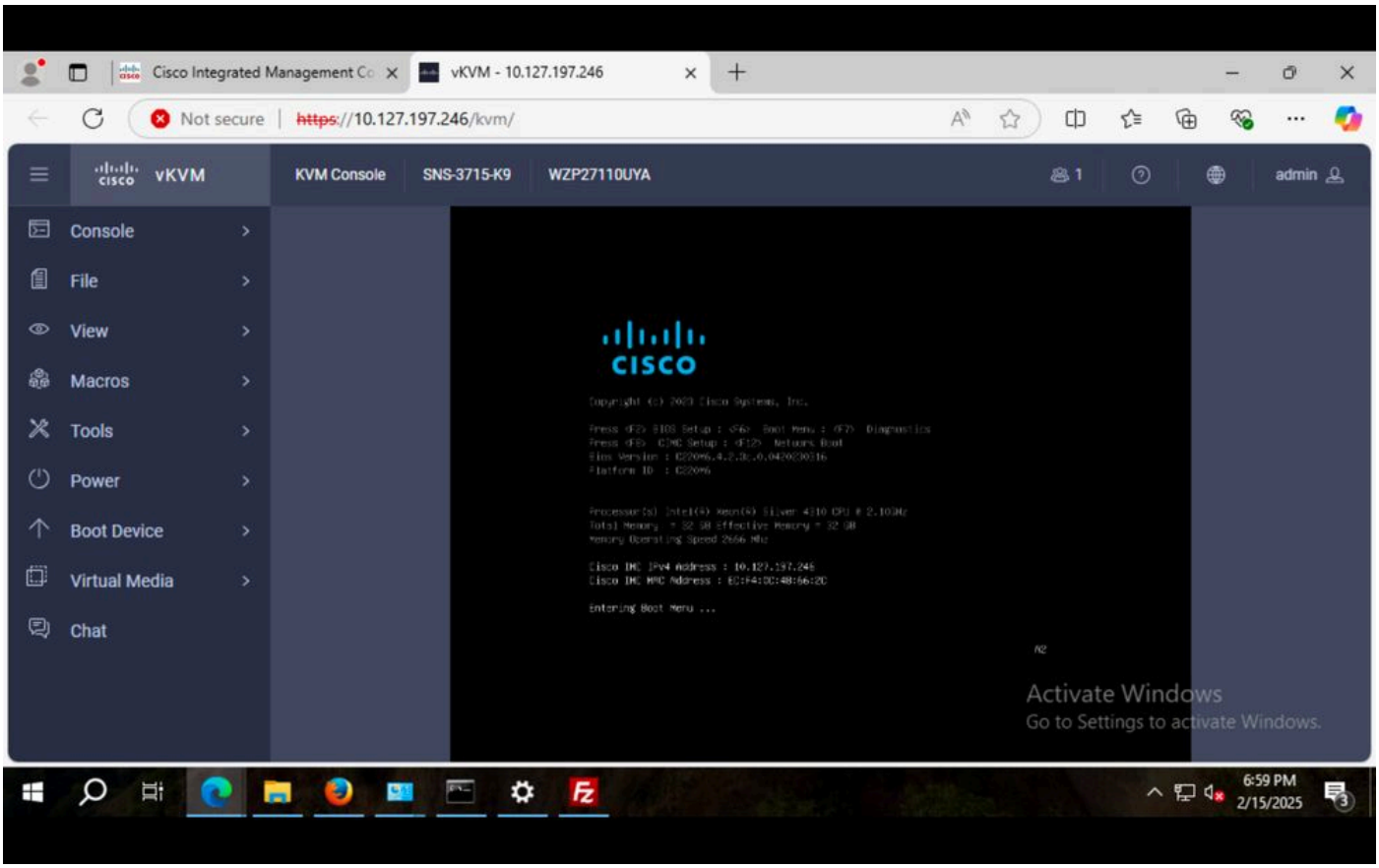
Step 4. Select the ISO file and click **Map Drive**.



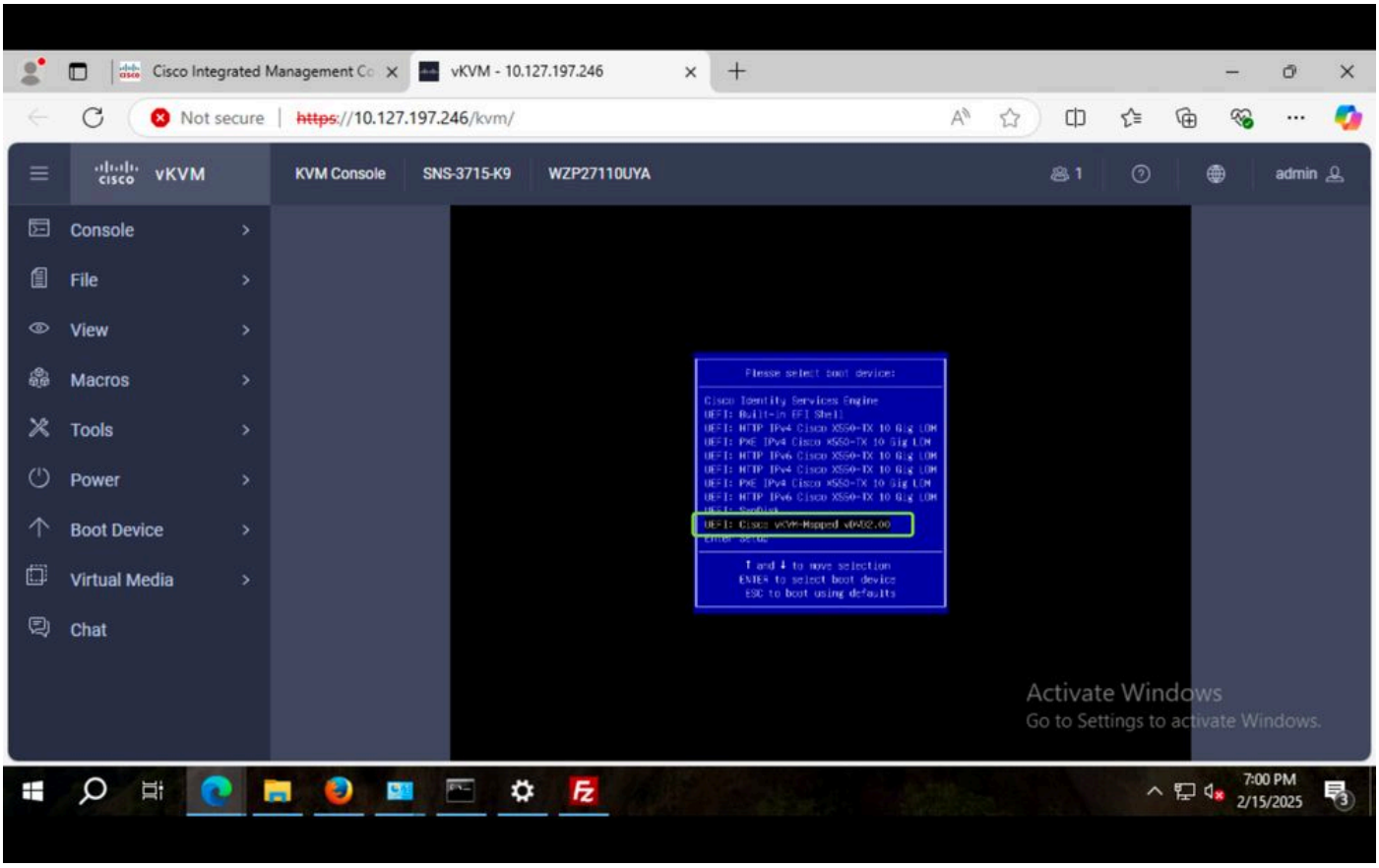
Step 5. Choose **Macros > Static Macros >Ctrl-Alt-Del** to boot the Cisco SNS-36XX or Cisco SNS-37XX appliance through use of the ISO image.



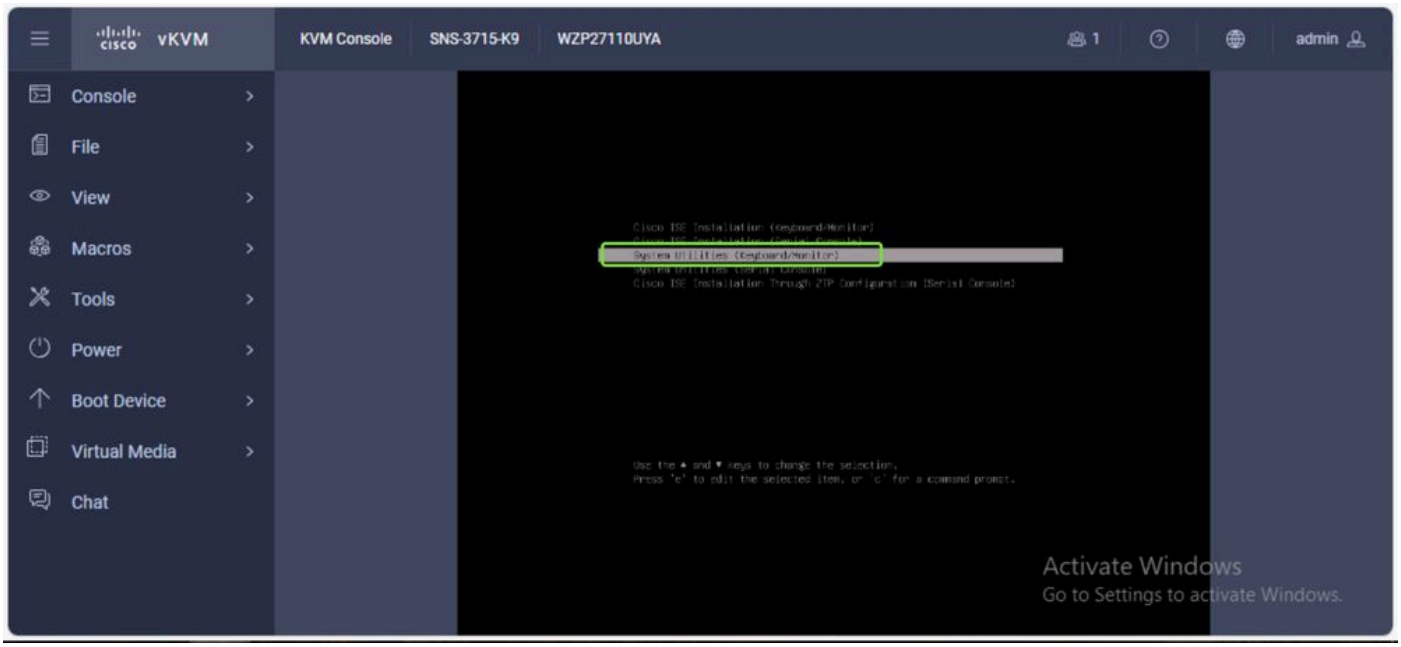
Step 6. Press F6 to bring up the boot menu. Entering boot menu then shows at the bottom of the screen.

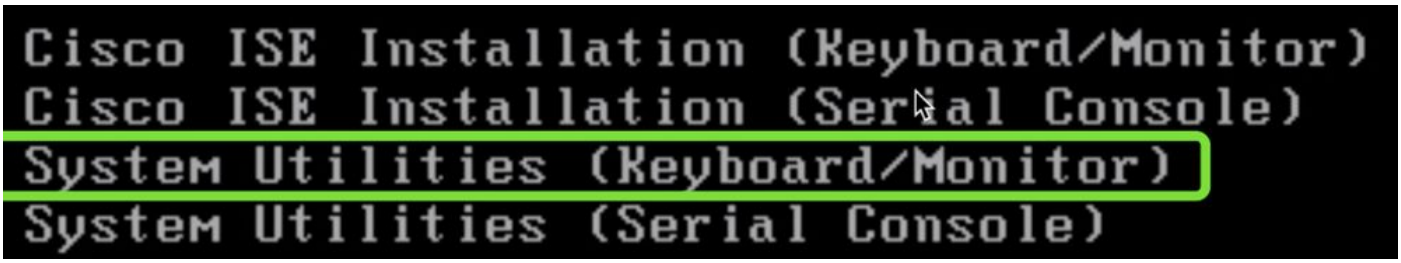


Step 7. Select the CD/DVD that is mapped and click **Enter**.

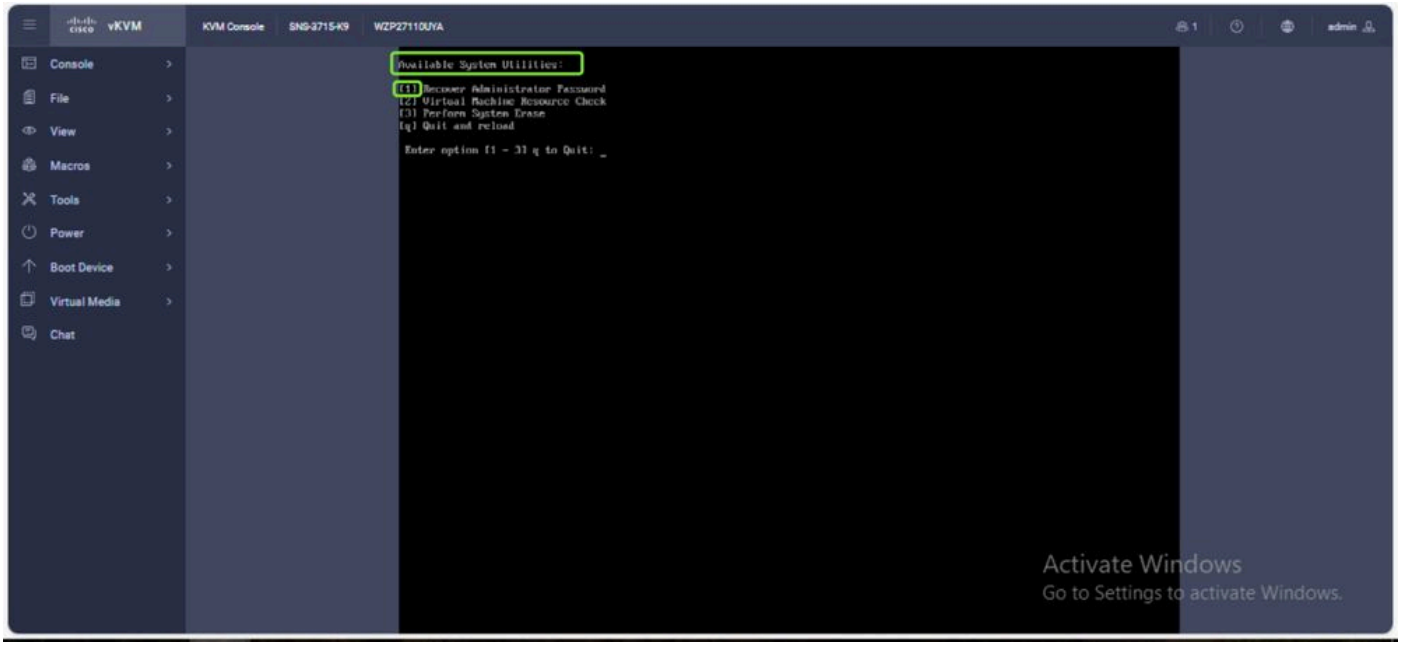


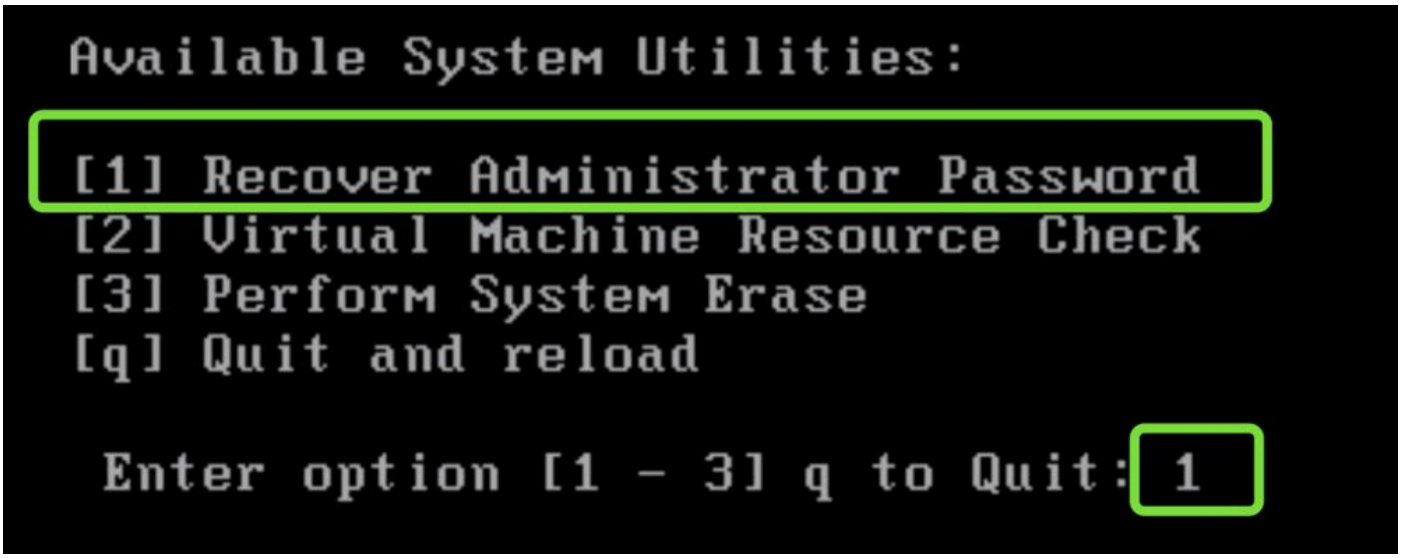
Step 8. Select **System Utilities (Keyboard/Monitor)** or **System Utilities (Serial Console)** if you access through a local serial console port connection):

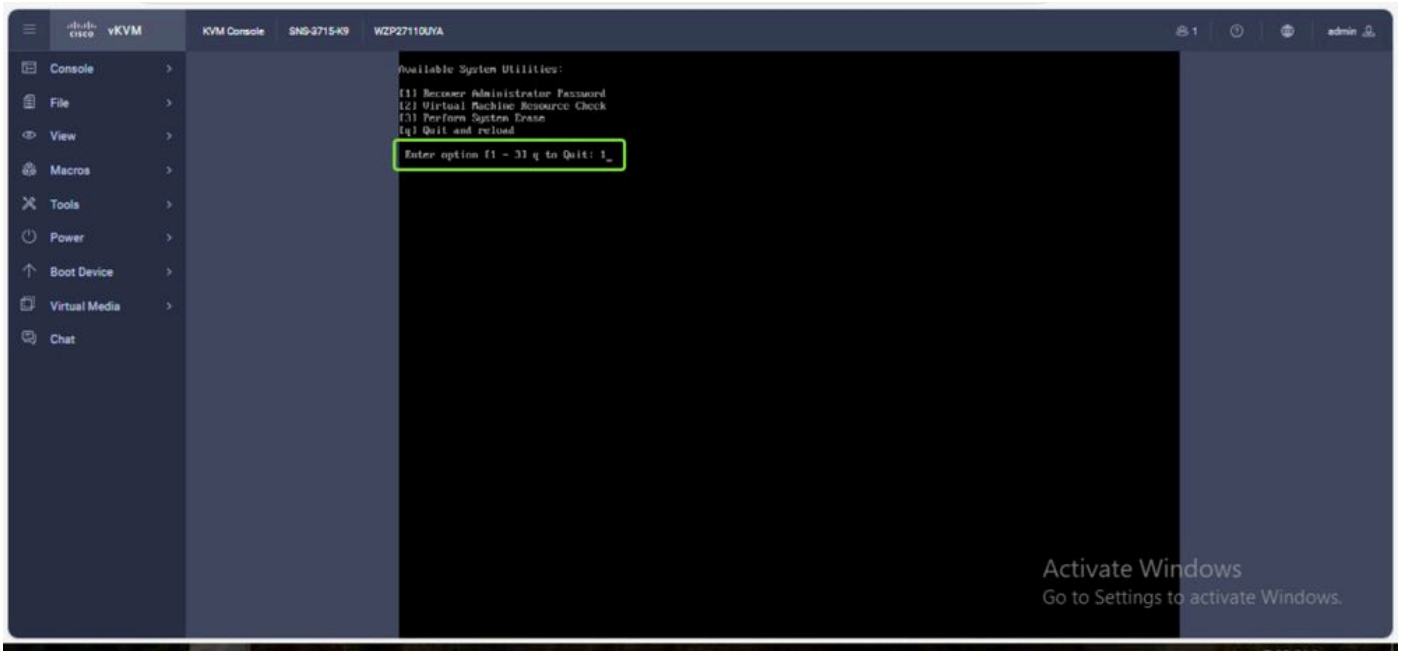




Step 11. From **System Utilities**, choose **Recover Administrator Password** Option 1.

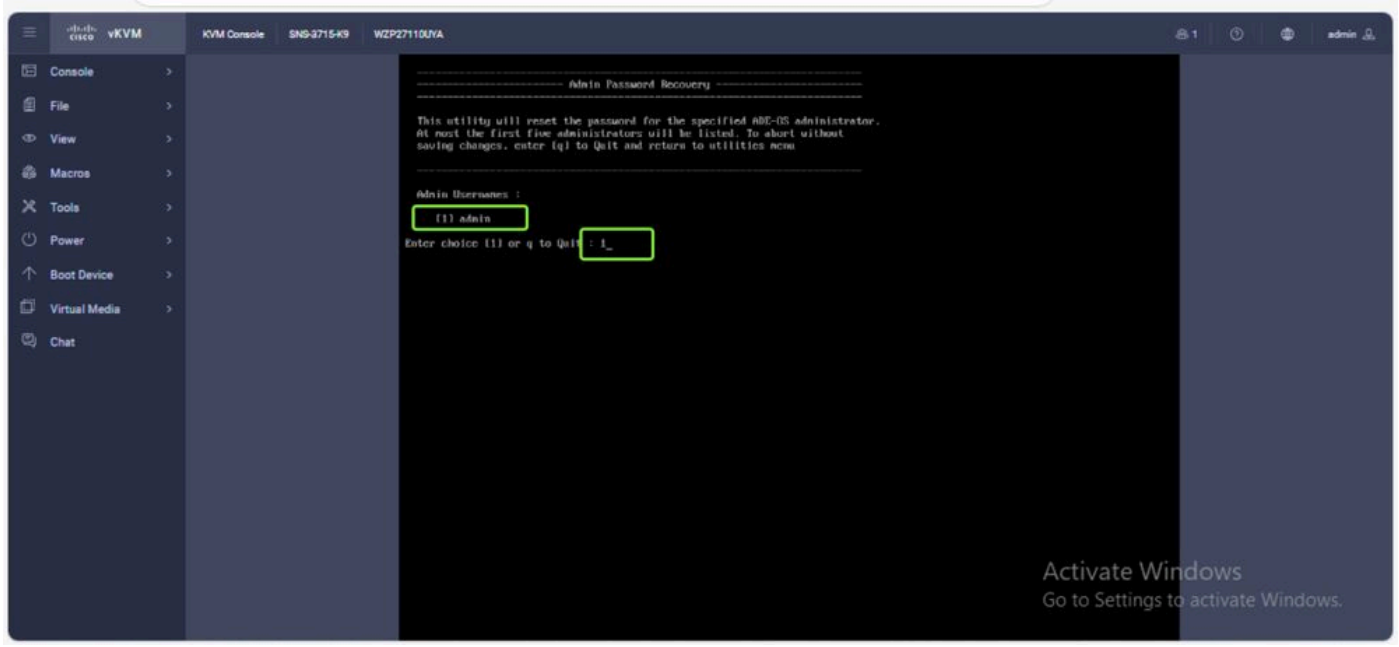






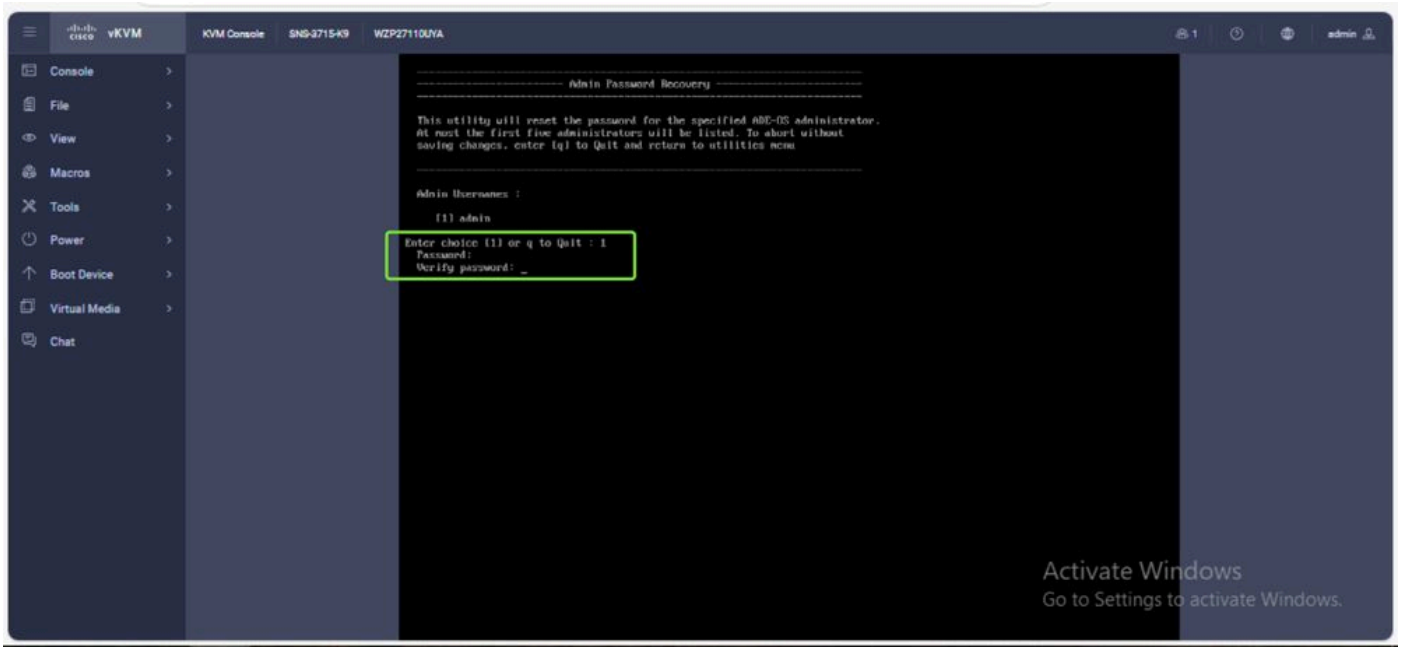
Type option 1 and click **Enter**

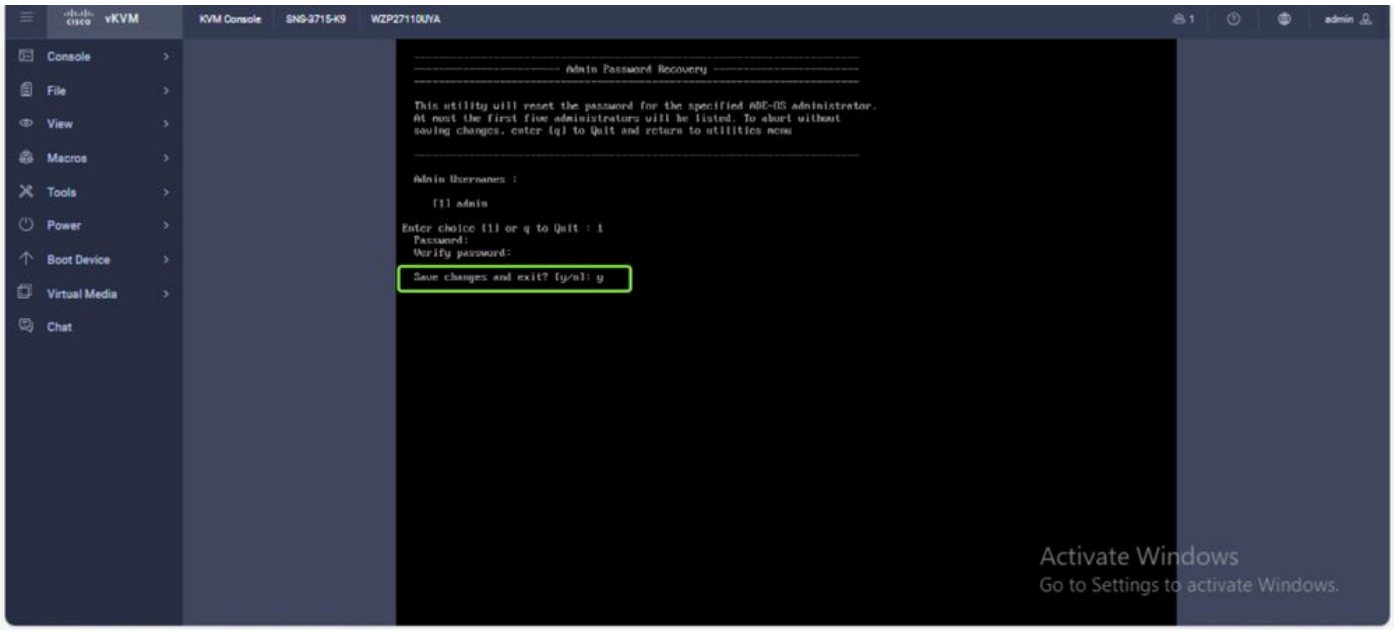
Step 9. Select the required username from the list and press enter to reset the password. The console displays:





Step 10. Type the new password and type **y** to save the changes.





Password reset is complete.

```
  This utility will reset the password for the specified ADE-OS administrator.
  At most the first five administrators will be listed. To abort without
  saving changes, enter [q] to Quit and return to utilities menu

  --------------------------------------------------------------------------

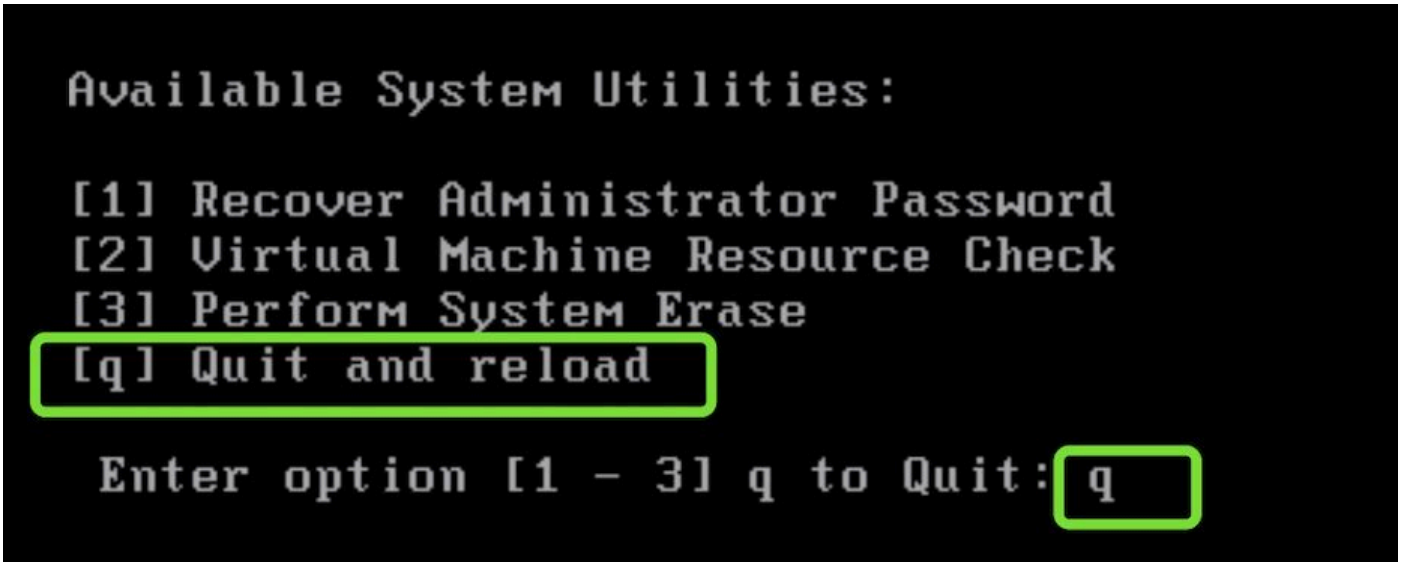
  Admin Usernames :

     [1] admin

 Enter choice [1] or q to Quit : 1
  Password:
  Verify password:

  Save changes and exit? [y/n]: y
[  145.273614] EXT4-fs (sda6): 4 orphan inodes deleted
[  145.273680] EXT4-fs (sda6): recovery complete
[  145.275917] EXT4-fs (sda6): mounted filesystem with ordered data mode. Opts:
(null)
```

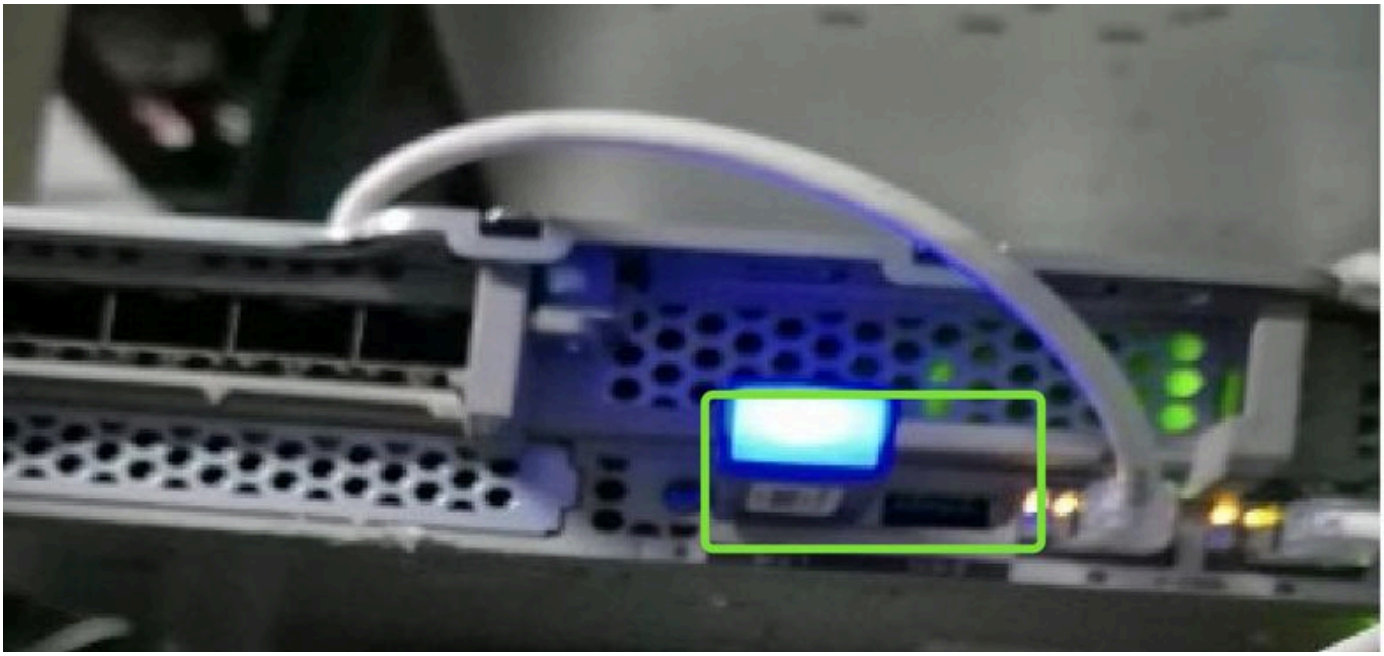
Step 11. To access the CLI, Select **Quit and reload**, type option **q.**



Password recovery through the use of a bootable USB

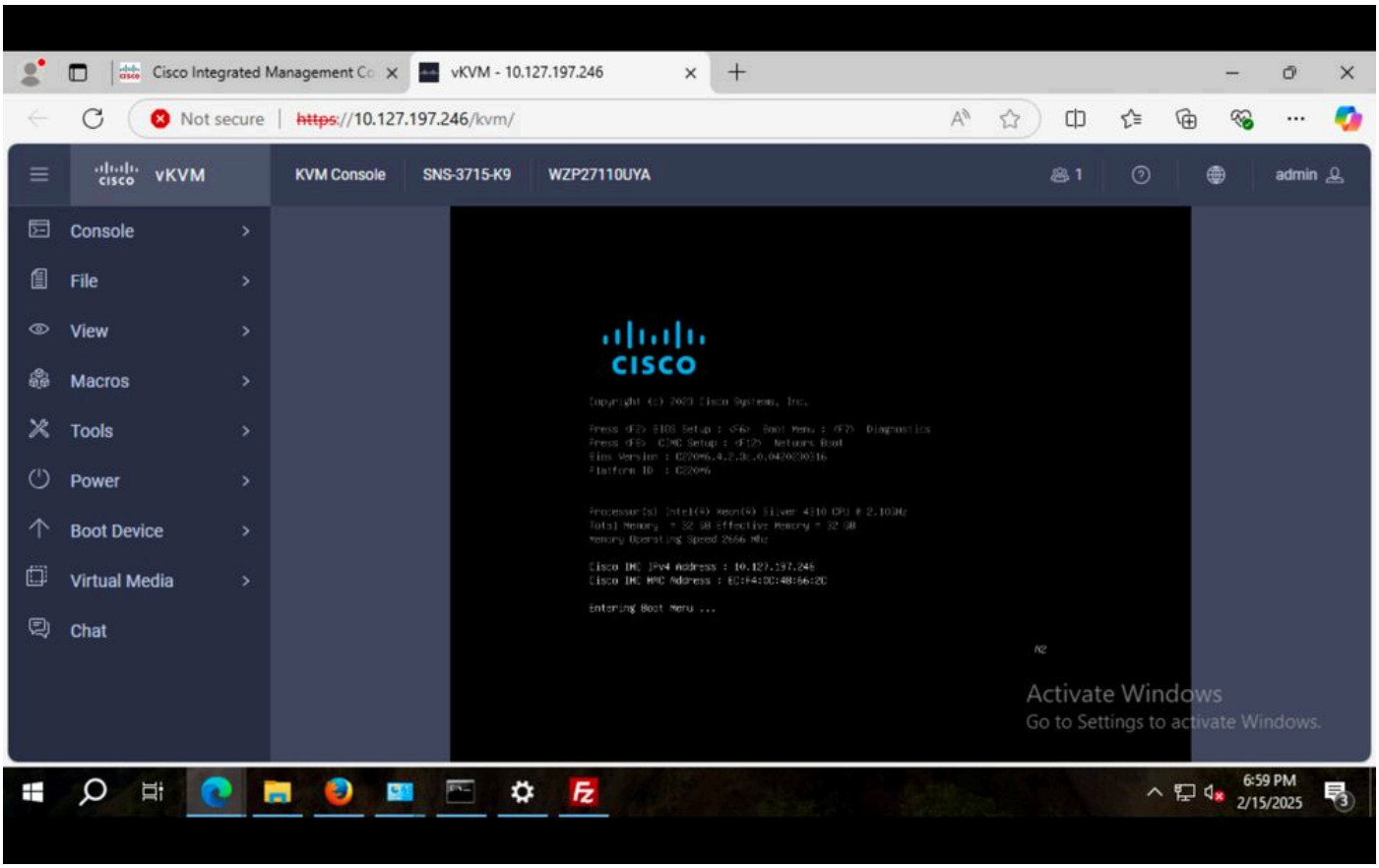
Before You Begin: Create a bootable USB drive. See Create a Bootable USB Device to Install Cisco ISE.

Step 1. Plugin the bootable USB drive that has the bootable Cisco Secure ISE ISO image into the USB port.

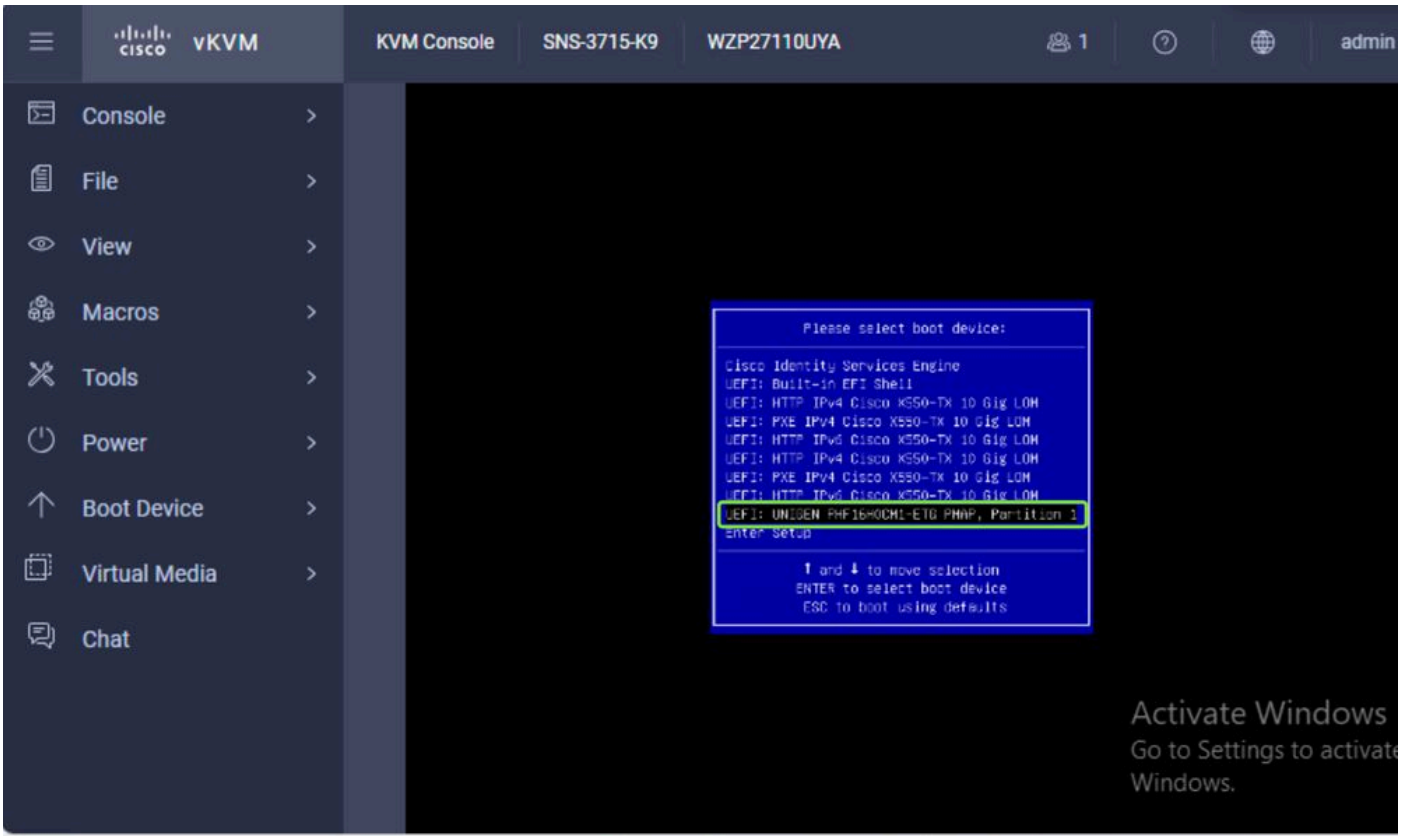


Step 2. Power on the **Cisco SNS-36XX** or **Cisco SNS-37XX** appliance.

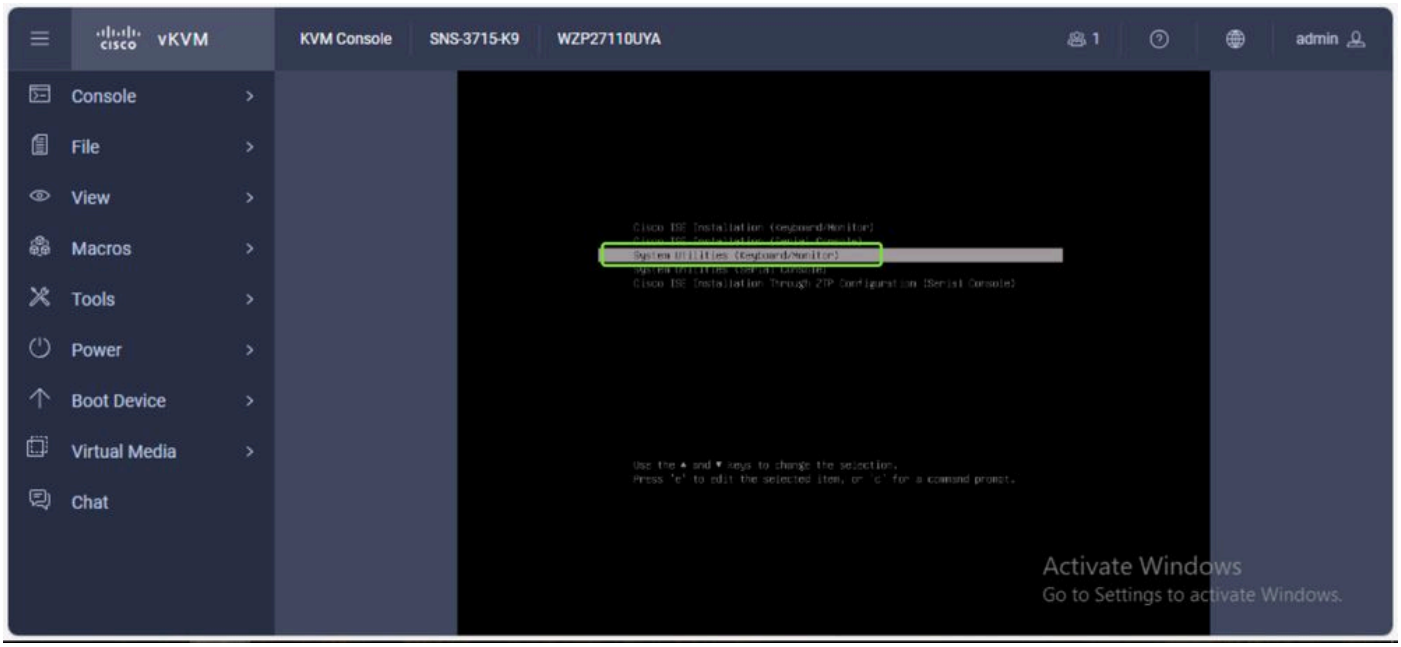
Step 3. Press F6 to enter BIOS menu.

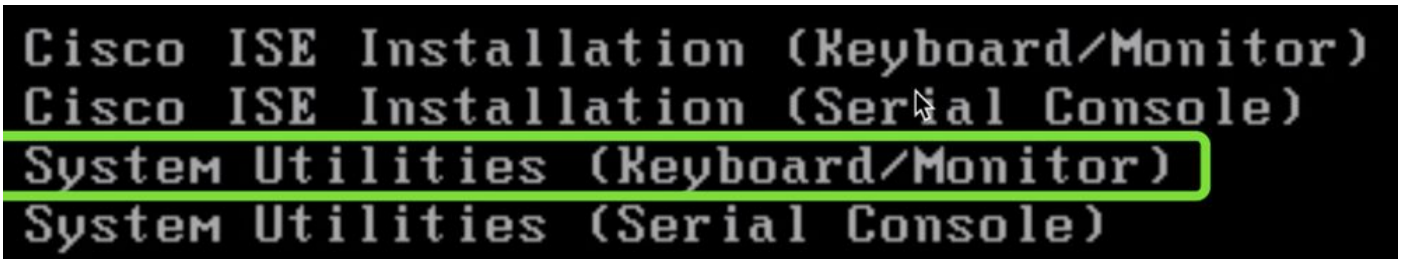


Step 4. Choose **USB** from the boot menu.

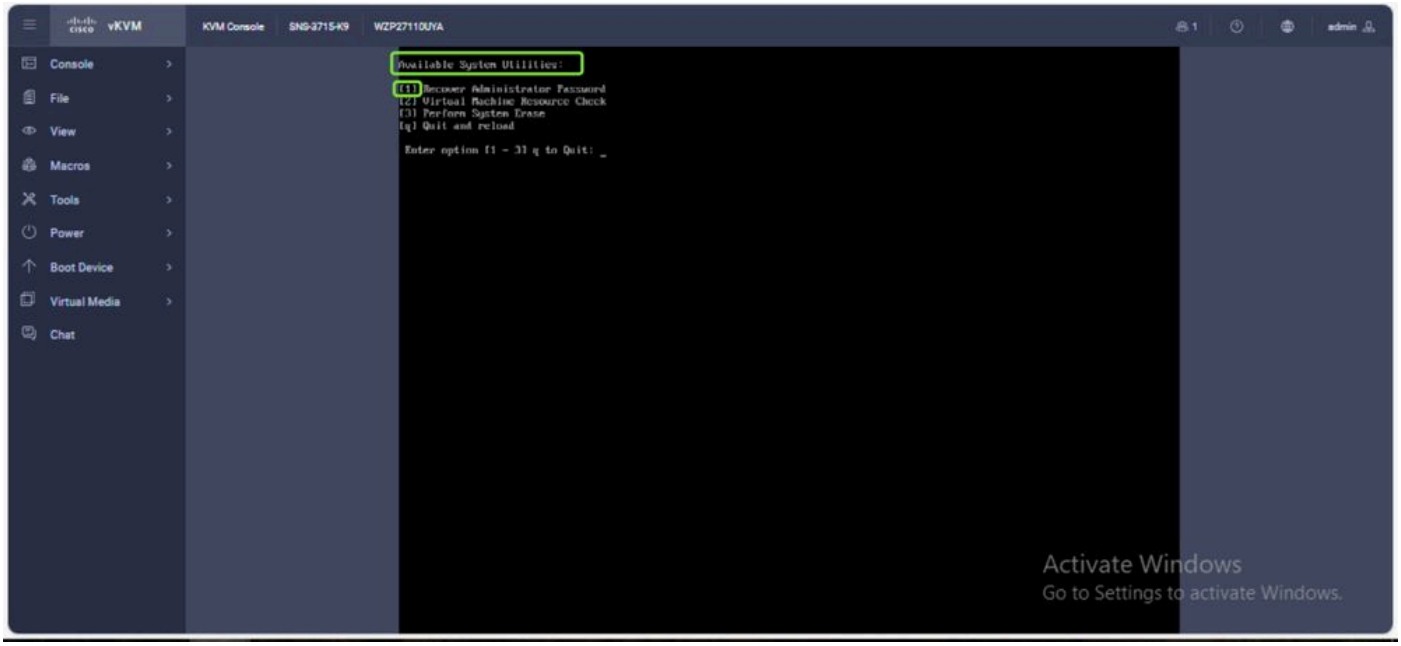


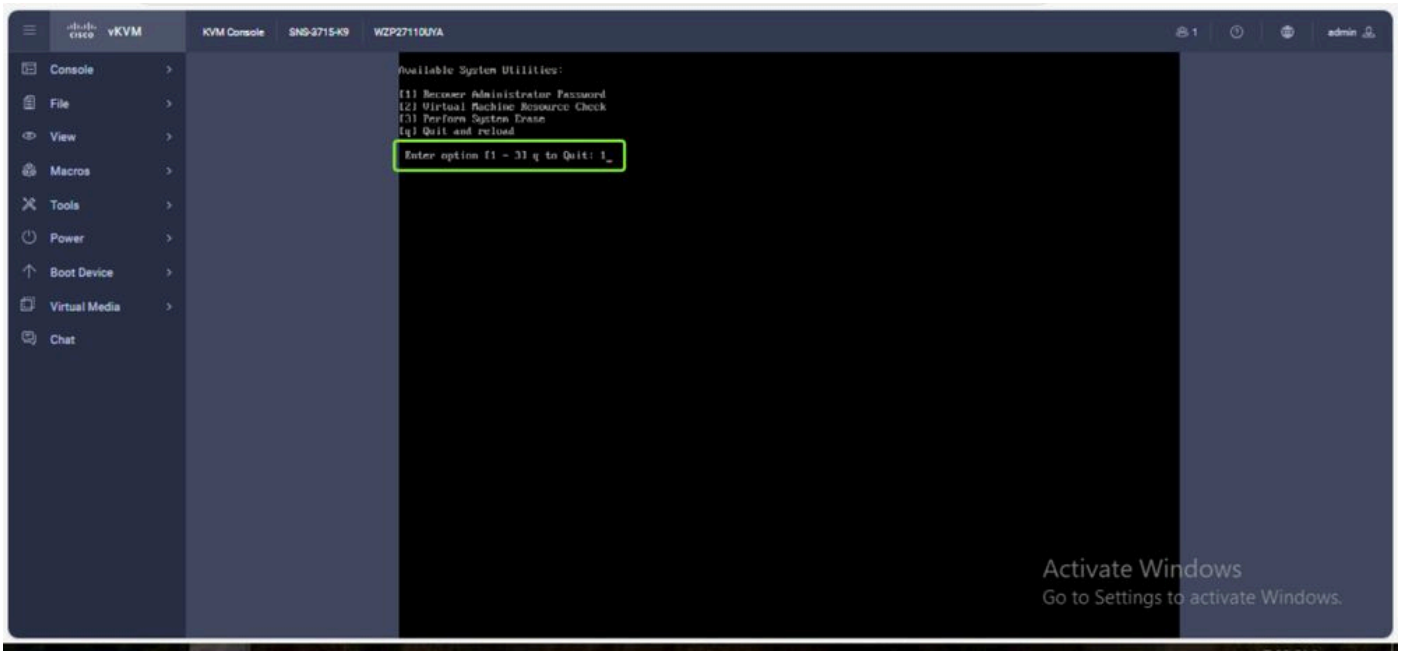
Step 5. Select **System Utilities** (Keyboard/Monitor) or **System Utilities** (Serial Console) if you access is through a local serial console port connection:

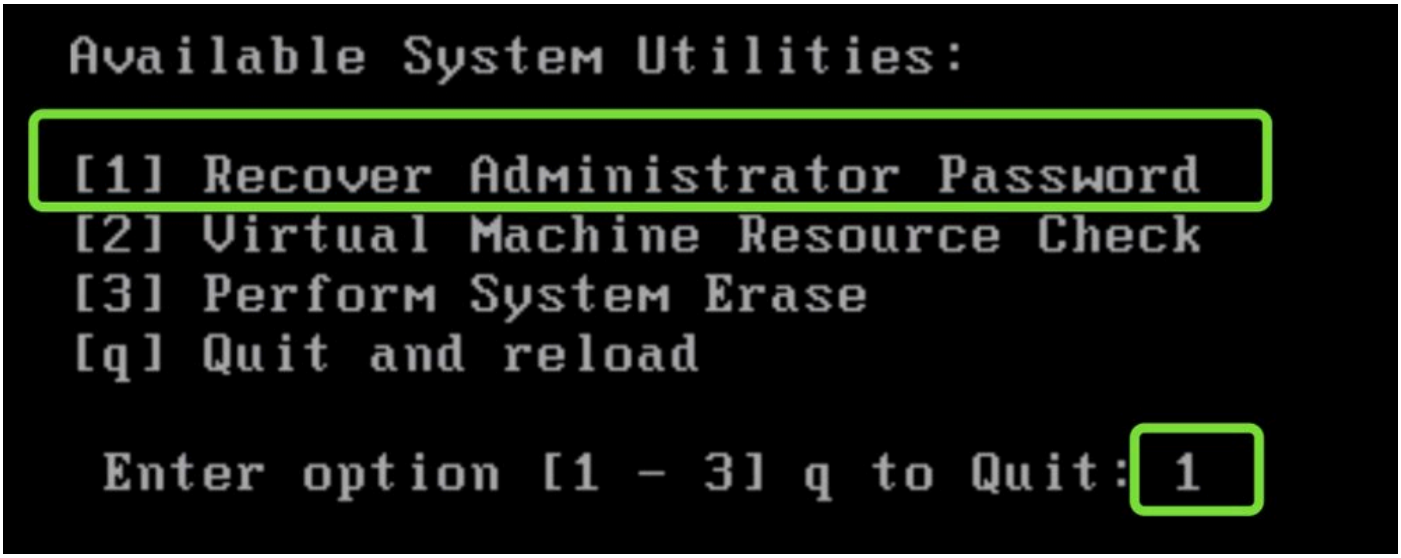




Step 6. From System Utilities, choose **Recover Administrator Password** Option 1.



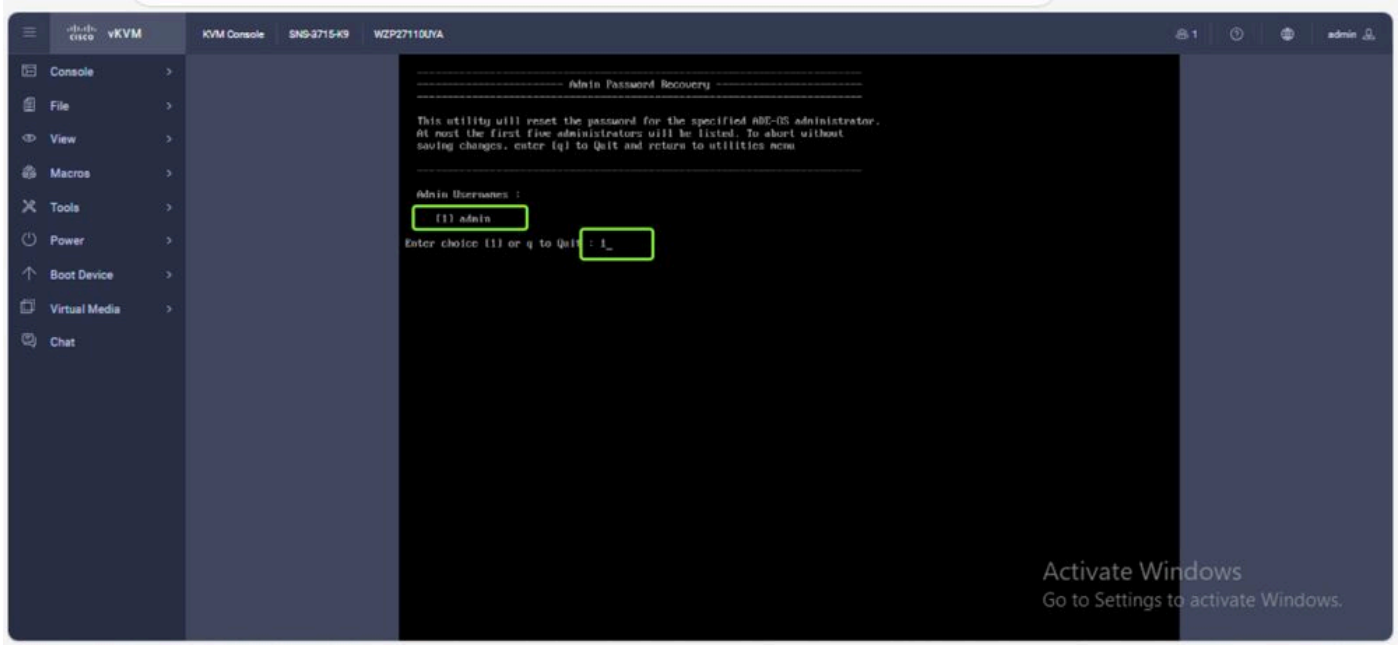




Select option 1 (Recover Administrator Password) .

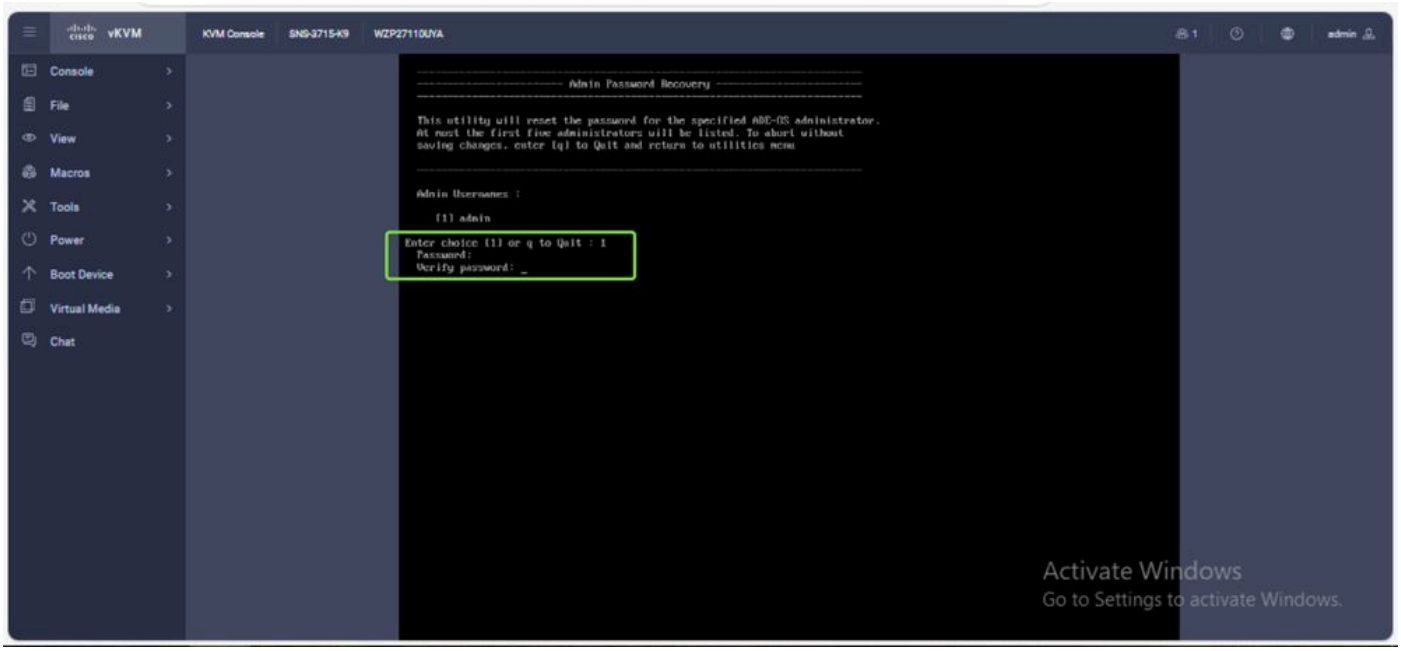
Step 7. Select the required username from the list and press enter to reset the password.

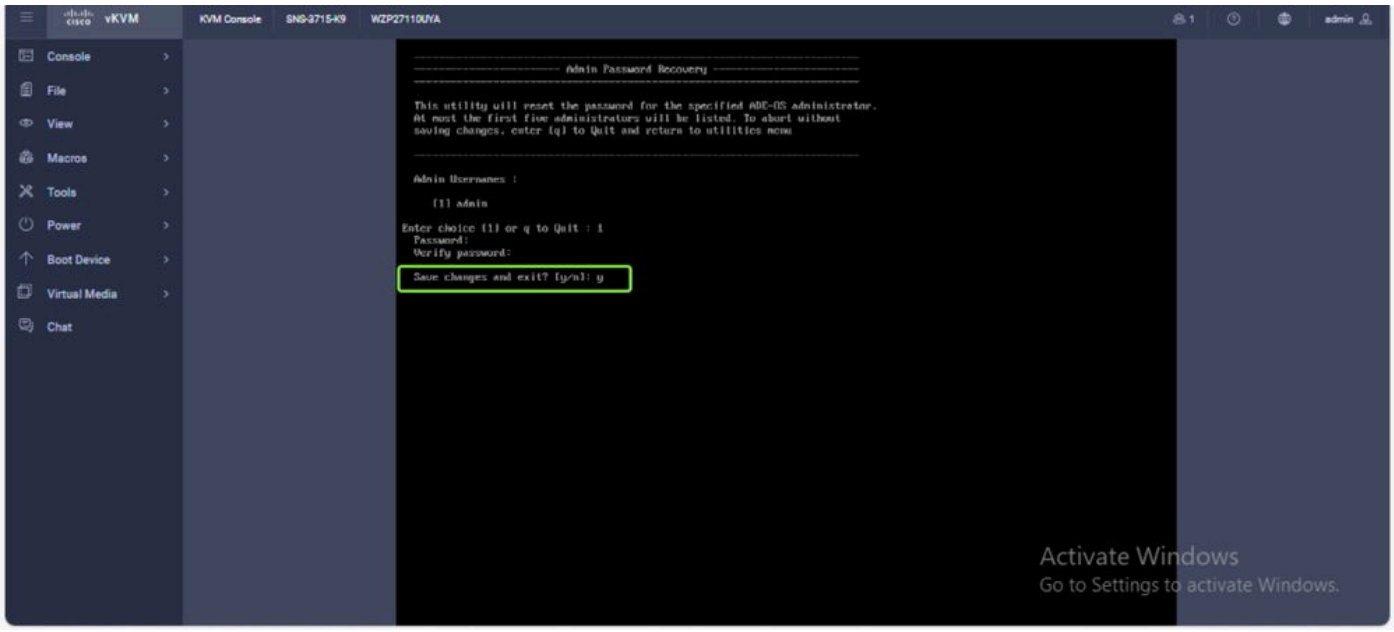
The console displays:





Step 8. Type new password and type 'y' to save the changes.





Password reset is complete.

```
  This utility will reset the password for the specified ADE-OS administrator.
  At most the first five administrators will be listed. To abort without
  saving changes, enter [q] to Quit and return to utilities menu

  --------------------------------------------------------------------------

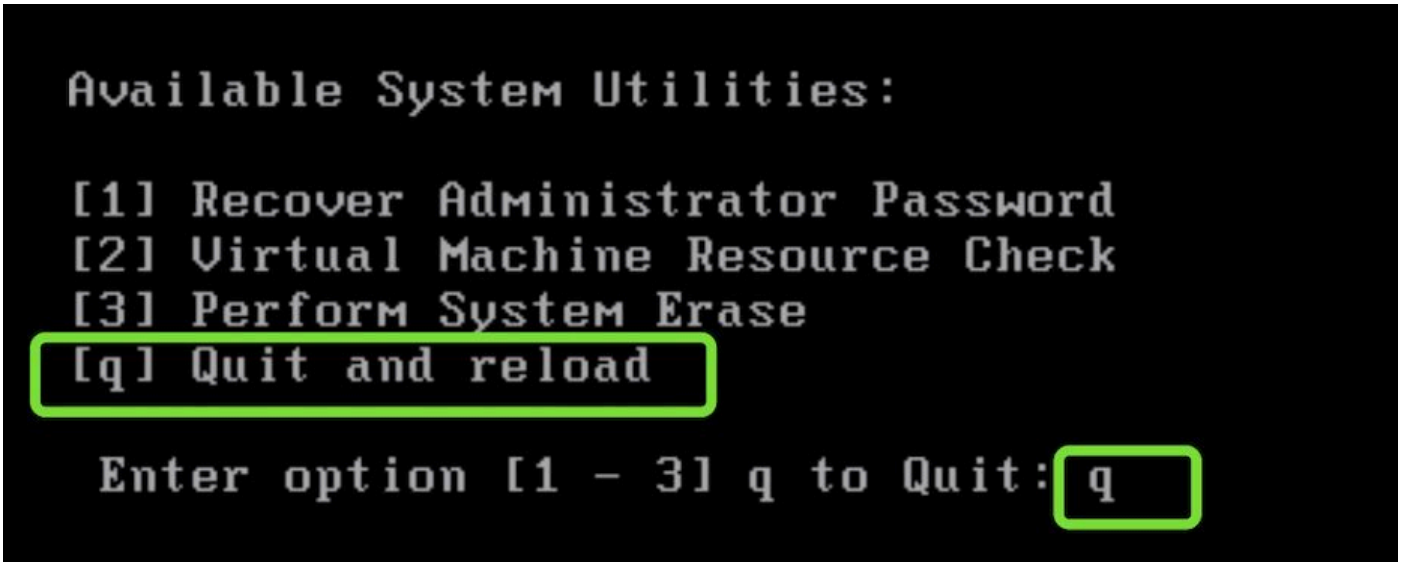
  Admin Usernames :

     [1] admin

 Enter choice [1] or q to Quit : 1
  Password:
  Verify password:

  Save changes and exit? [y/n]: y
[  145.273614] EXT4-fs (sda6): 4 orphan inodes deleted
[  145.273680] EXT4-fs (sda6): recovery complete
[  145.275917] EXT4-fs (sda6): mounted filesystem with ordered data mode. Opts:
(null)
```

Step 9. To access the CLI, Select quit and reload, type option **q**.

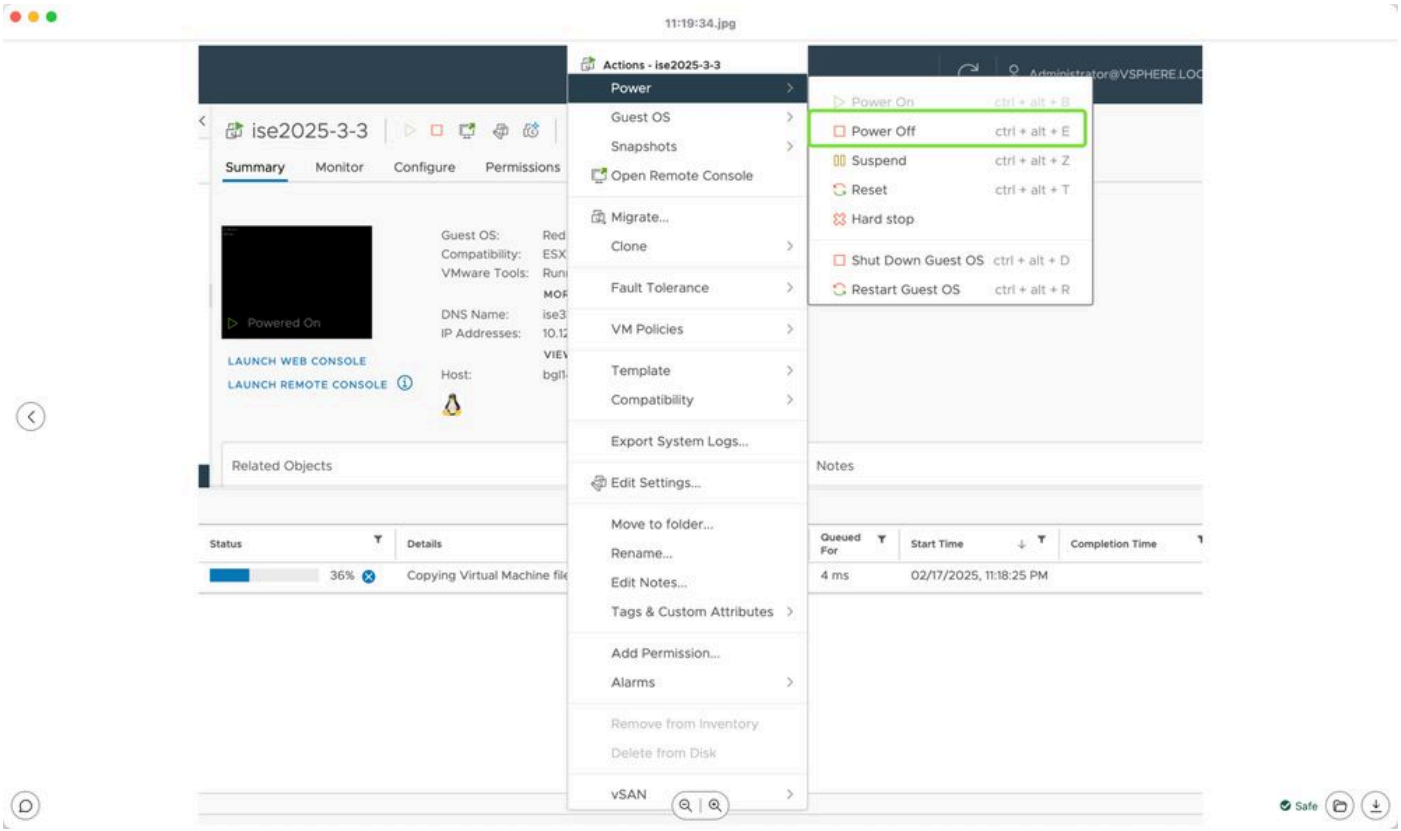


Password Recovery for ISE Virtual Machine

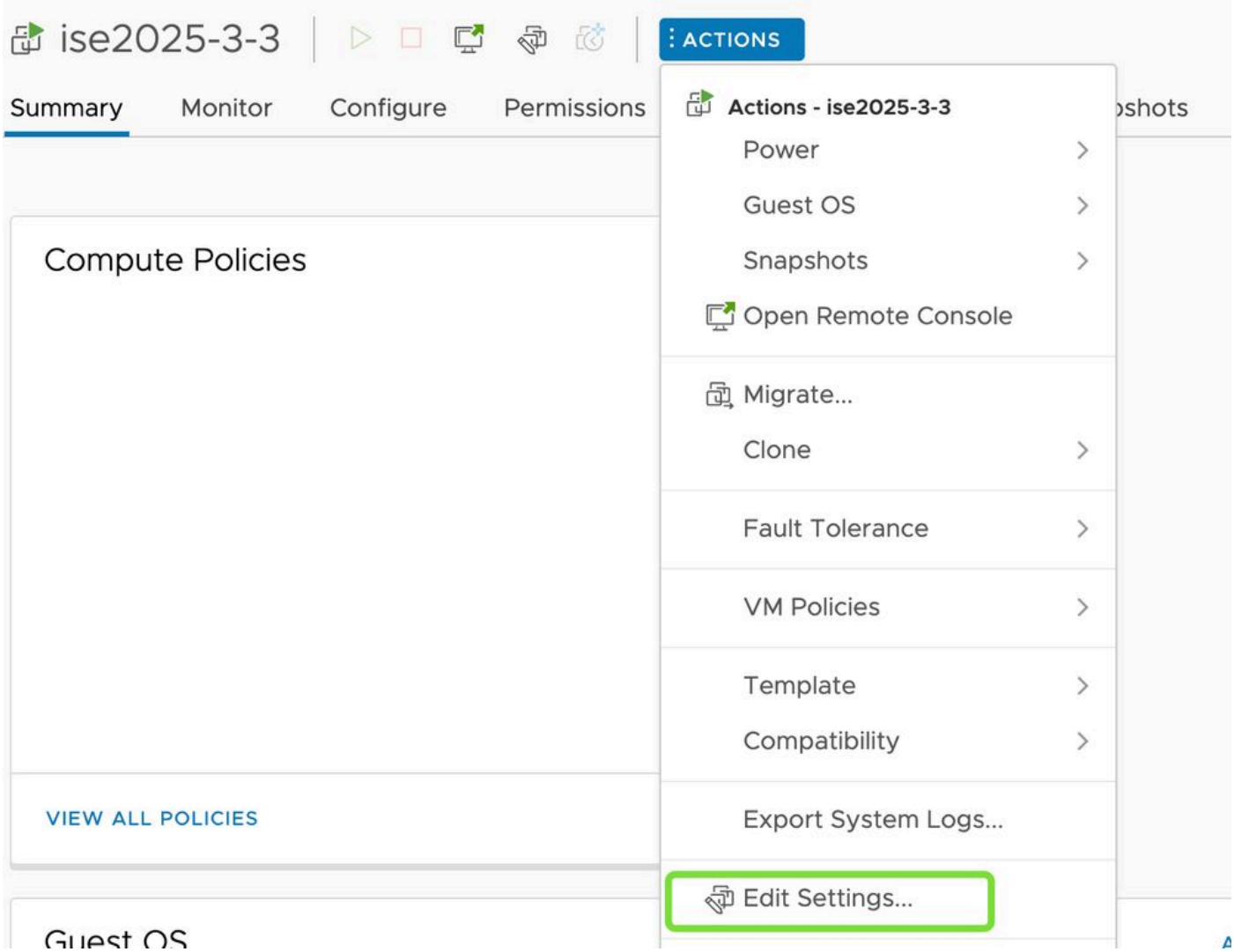
Here, VMWare is the environment used, you can have Vsphere access to perform these steps:

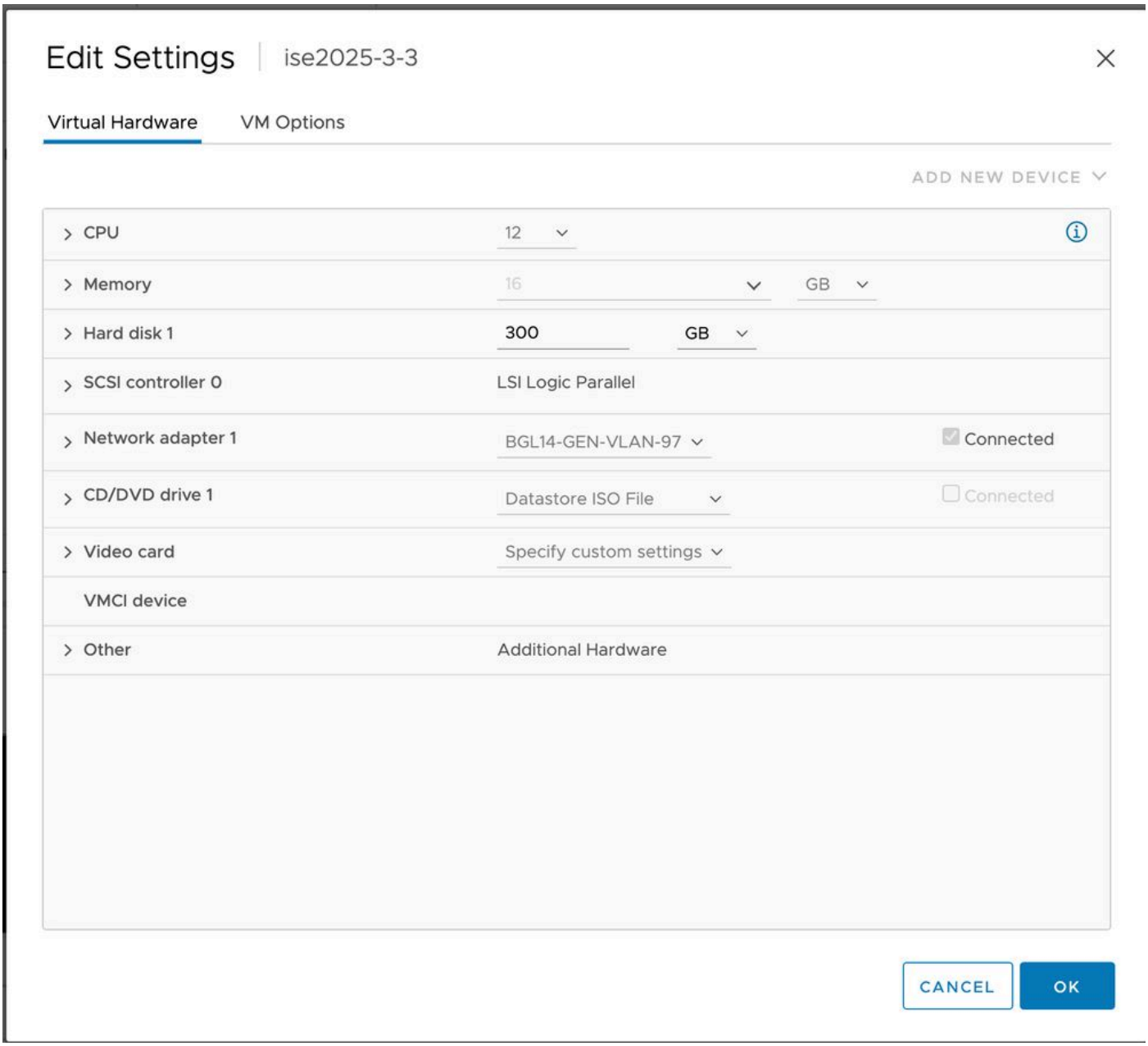
Step 1. Upload the ISO file to the virtual machine datastore.

Step 2. Power off the ISE virtual machine.

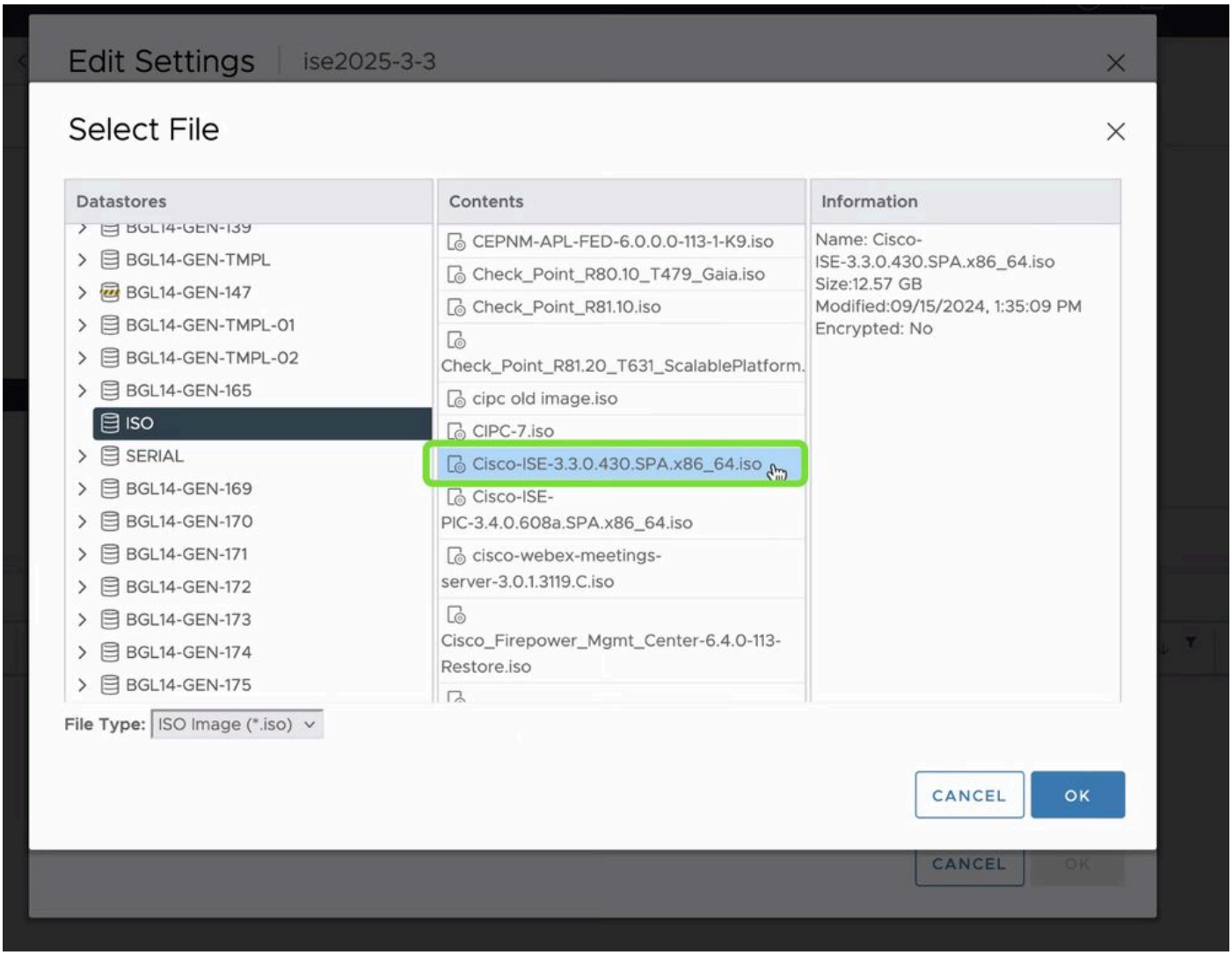


Step 3. Select the VM from the list, Click **Actions** >**Edit Settings.**

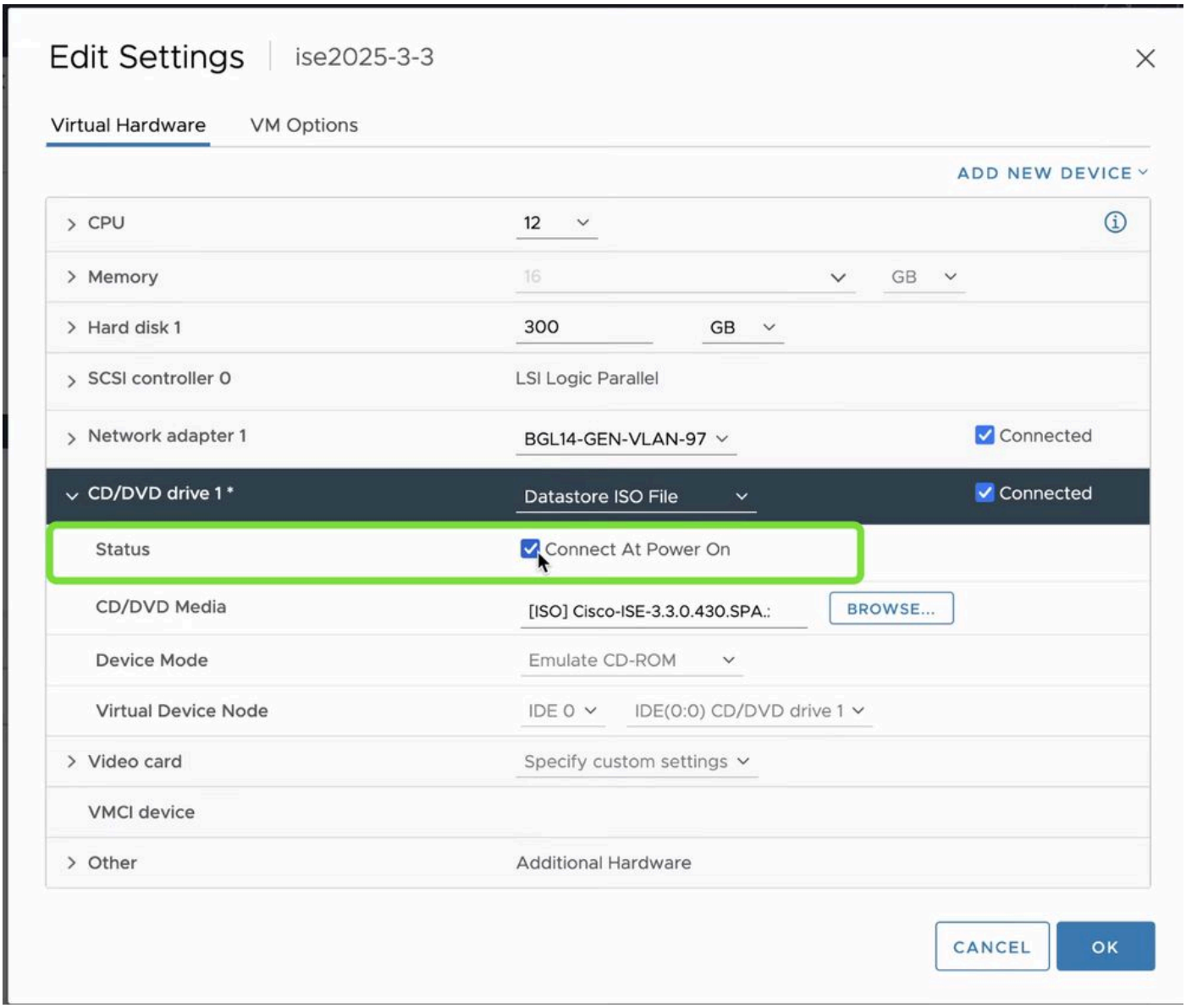

ise2025-3-3
ACTIONS
Summary
Monitor
Configure
Permissions
Actions - ise2025-3-3
Power
Guest OS
Snapshots
Open Remote Console
Migrate...
Clone
Fault Tolerance
VM Policies
Template
Compatibility
Export System Logs...
Edit Settings...
Compute Policies
VIEW ALL POLICIES
Guest OS



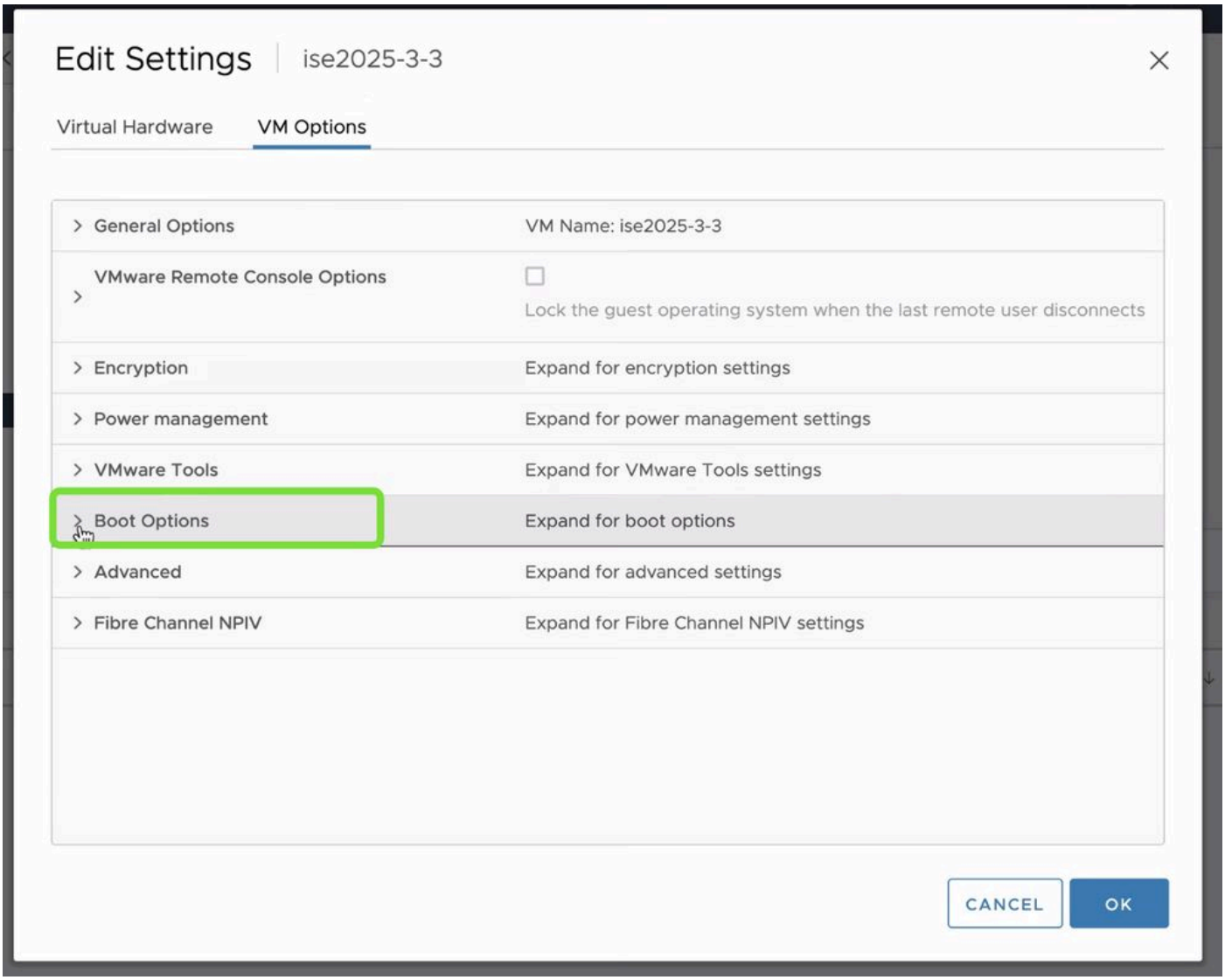
Step 4. Under**Virtual Hardware** > **CD/DVD**, check for ISE 3.3 ISO file "Cisco-ISE-3.3.0.430.SPA.x86_64.iso" and click **OK.**

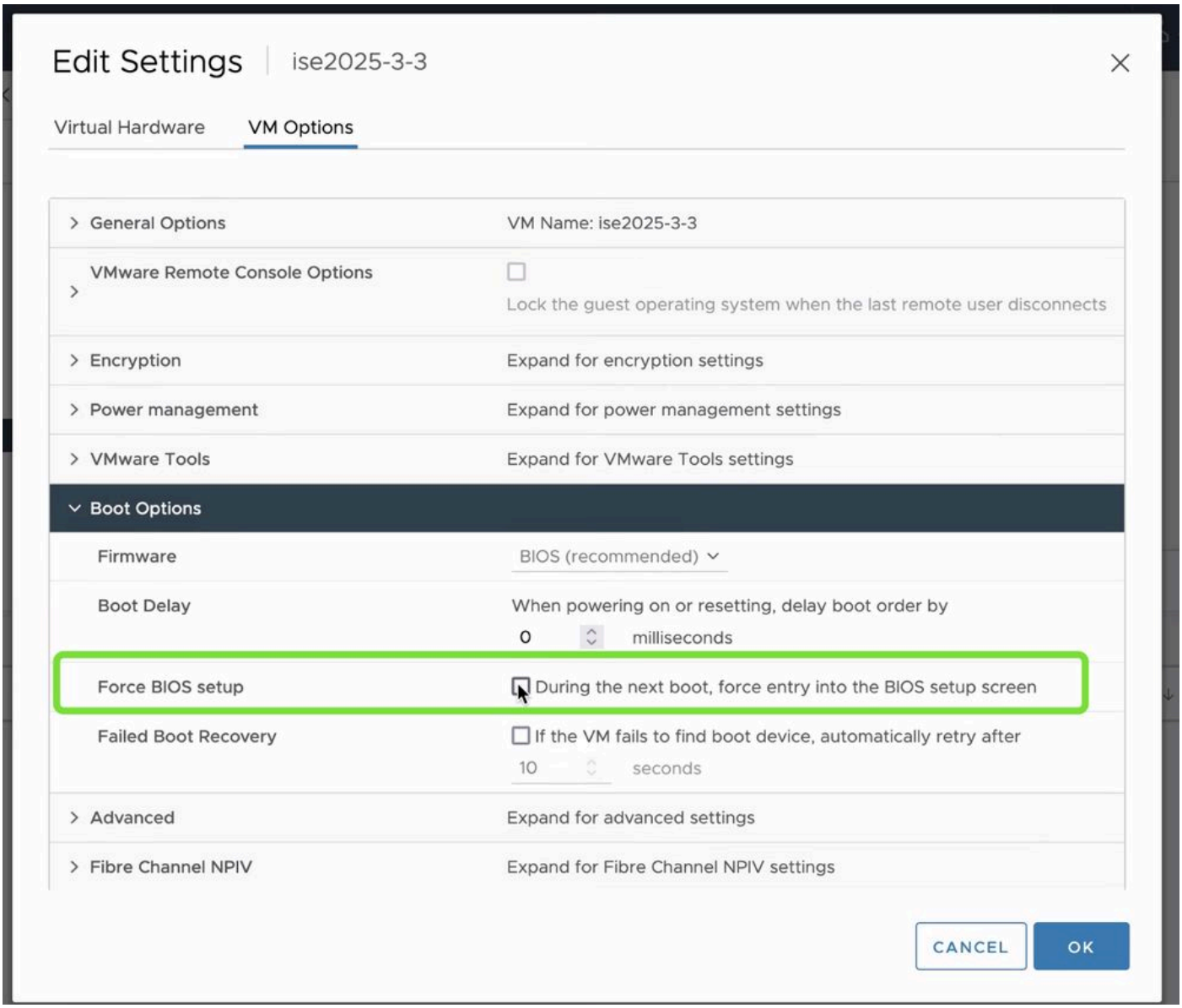


Step 5. Under **CD/DVD** settings, enable**Connect At PowerOn** and click **OK**.

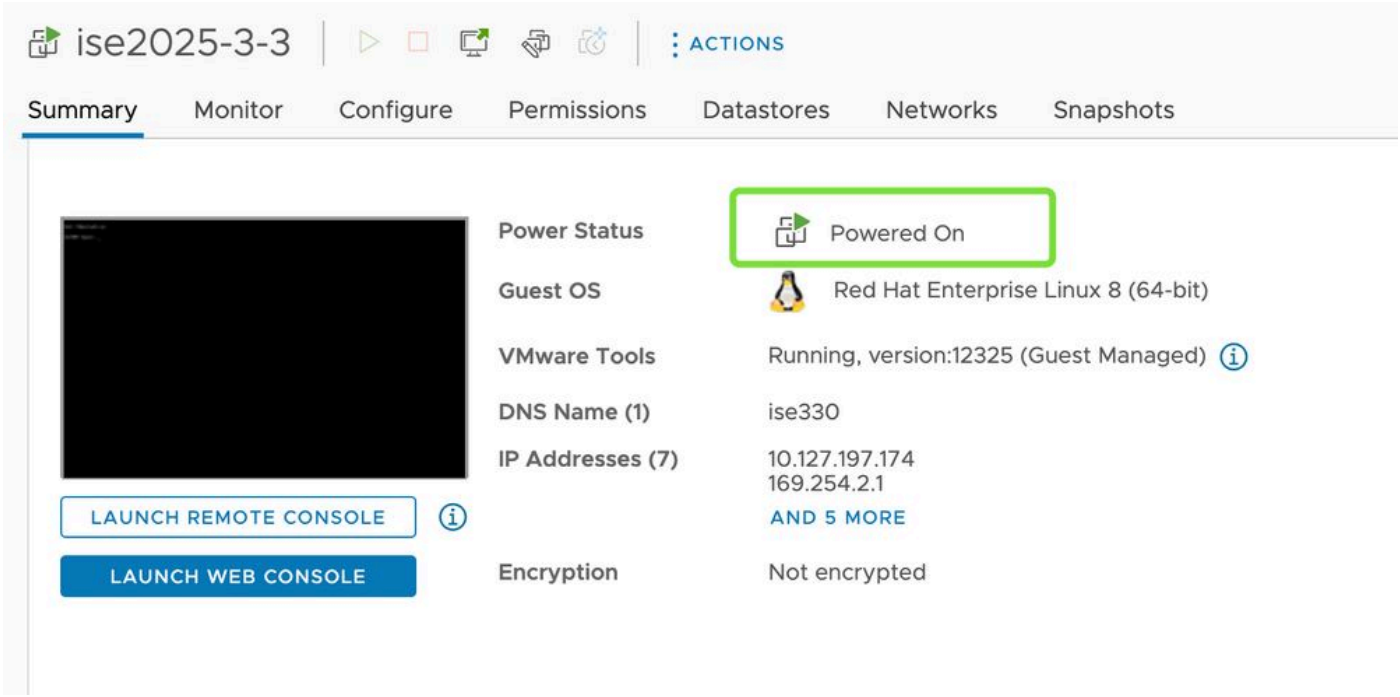


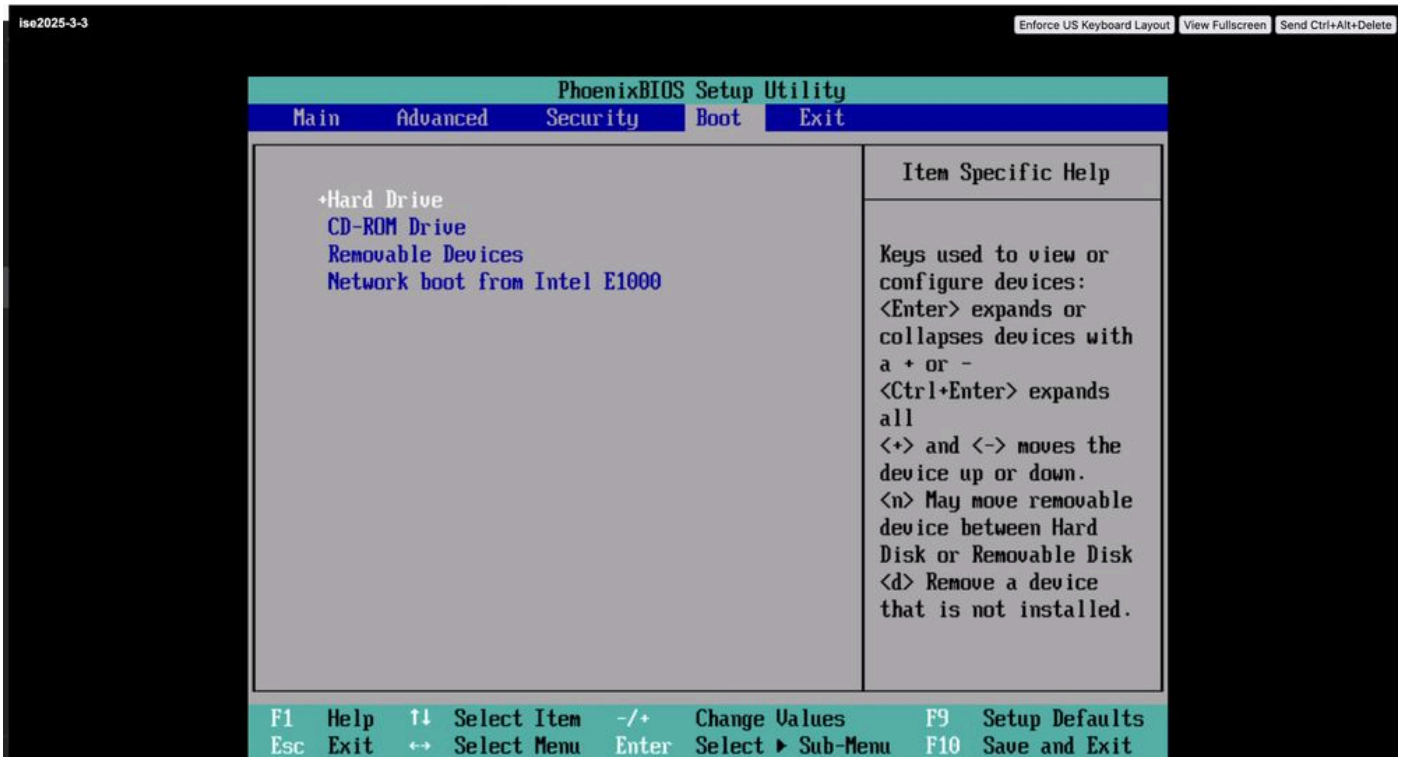
Step 6. Under **VM Options** > **Boot options**, enable **Force BIOS Setup** and click **OK.**


Edit Settings
ise2025-3-3
Virtual Hardware
VM Options
General Options
VM Name: ise2025-3-3
VMware Remote Console Options
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
Expand for boot options
Advanced
Expand for advanced settings
Fibre Channel NPIV
Expand for Fibre Channel NPIV settings
CANCEL
OK

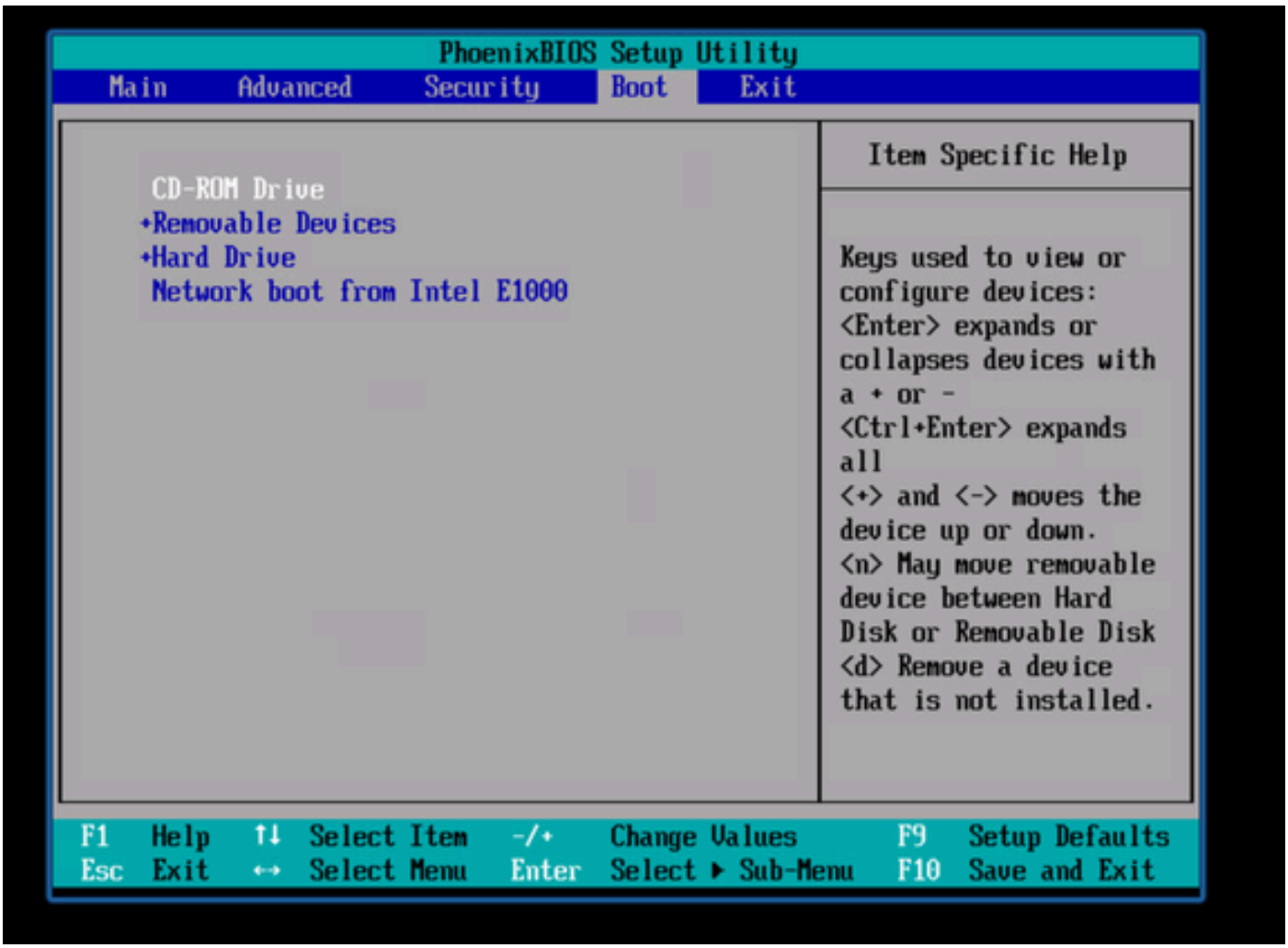


Step 7. Power on the ISE VM and monitor the VM console for BIOS prompt.

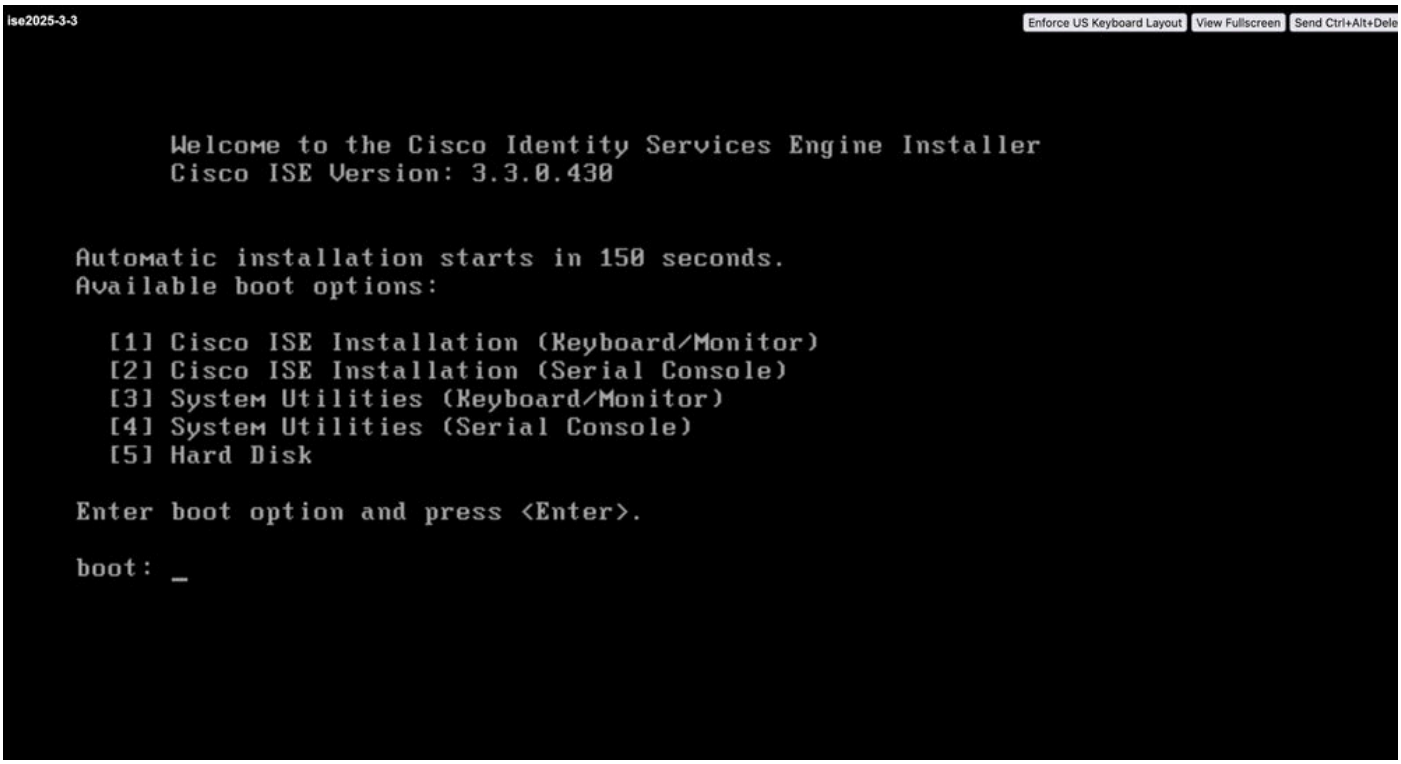


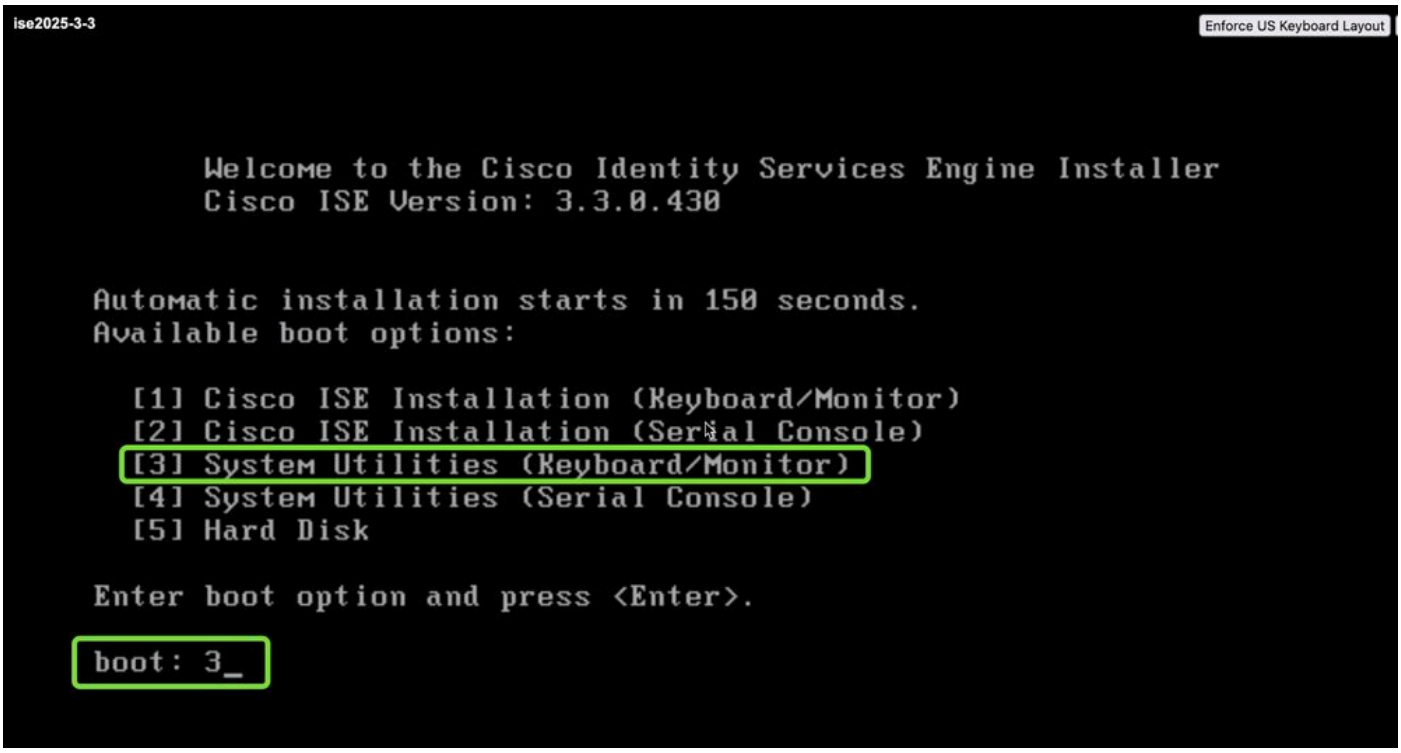


Step 8. Change the boot order of **CD-ROM Drive** and bring it to the first position.



Step 9. Click**Enter**. It prompts a list of available boot options, Select**System Utilities** (Keyboard/Monitor)option **3.**



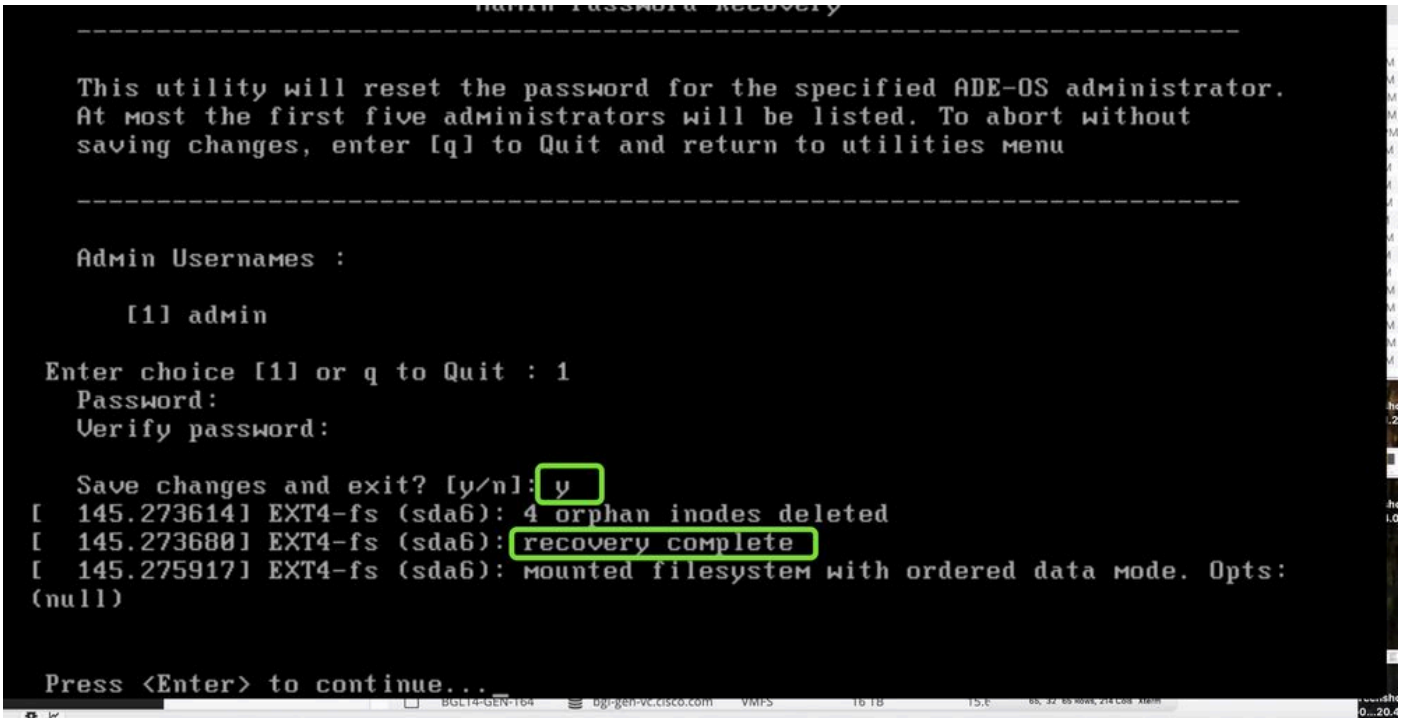


Step 10. On available System Utilities, chose the **Recover the Administrator Password**. Option **1** provides the list of administrators accounts configured on ISE device.



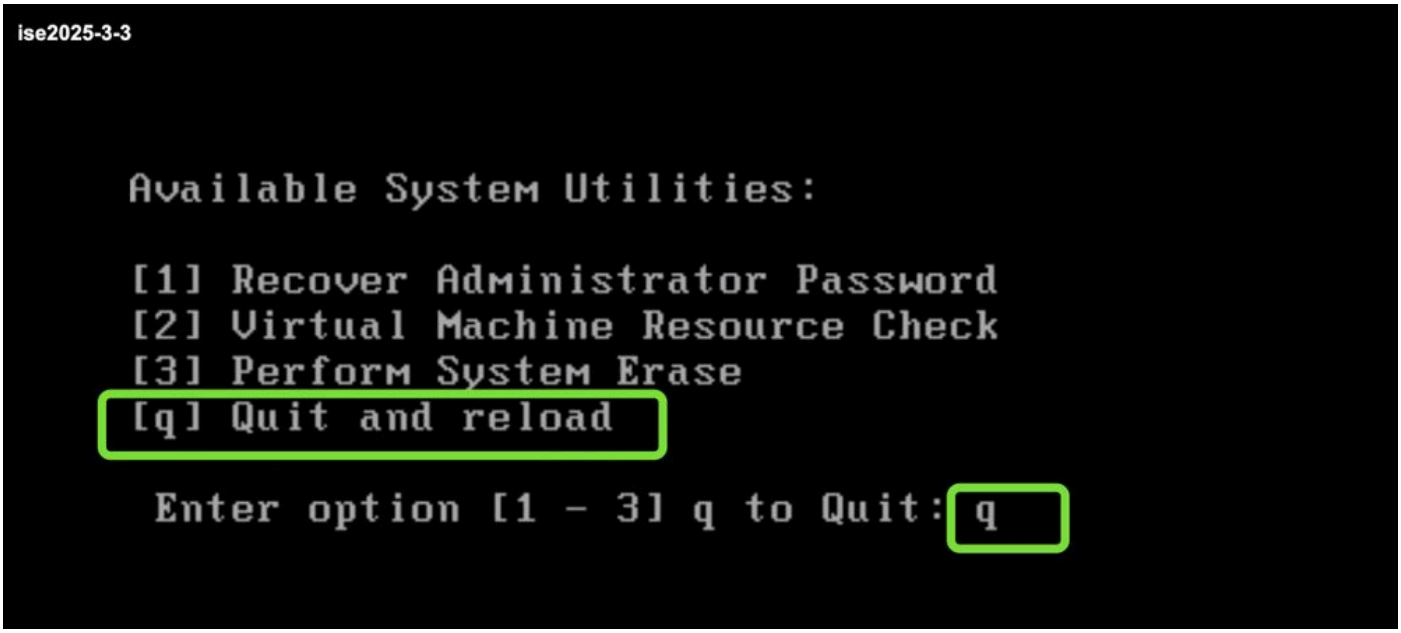
Step 11. Type Option **1** to change the password of user **admin** and enter new password. Enter **y** to save the new password.



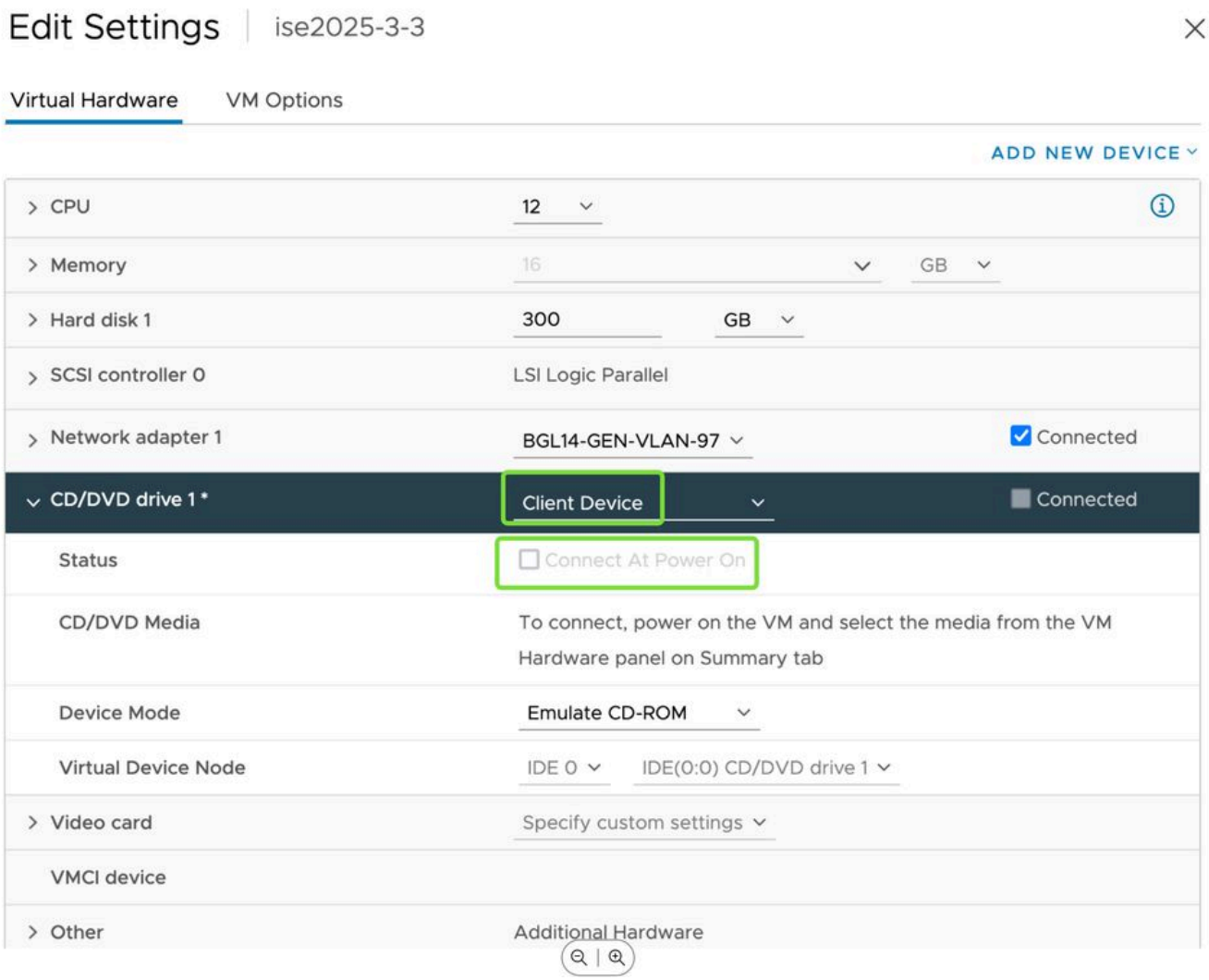


Password Recovery is completed

Step 12. Enter **q** to exit the **System Utilities** page.



Step 12. Change the CD/DVD settings to before and disable connect at Power On


Edit Settings
ise2025-3-3
Virtual Hardware
VM Options
ADD NEW DEVICE
CPU
12
Memory
16
GB
Hard disk 1
300
GB
SCSI controller 0
LSI Logic Parallel
Network adapter 1
BGL14-GEN-VLAN-97
Connected
CD/DVD drive 1 *
Client Device
Connected
Status
Connect At Power On
CD/DVD Media
To connect, power on the VM and select the media from the VM Hardware panel on Summary tab
Device Mode
Emulate CD-ROM
Virtual Device Node
IDE 0
IDE(0:0) CD/DVD drive 1
Video card
Specify custom settings
VMCI device
Other
Additional Hardware