Perform Password Recovery for ISE Command Line Interface (CLI)

Contents

Introduction

This document describes different mechanisms for password recovery for Identity Services Engine (ISE) CLI and GUI 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

This document is not restricted to specific software and hardware versions.

- ISE virtual machine (VMware version 8 (default) for ESXi 5.*x* (5.1 U2 minimum))
- ISE 3500 series appliance (ISE-3515-K9 / ISE-3595-K9)
- SNS-3600 series appliance (SNS-3615-K9 /SNS-3655-K9/SNS-3695-K9)

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.

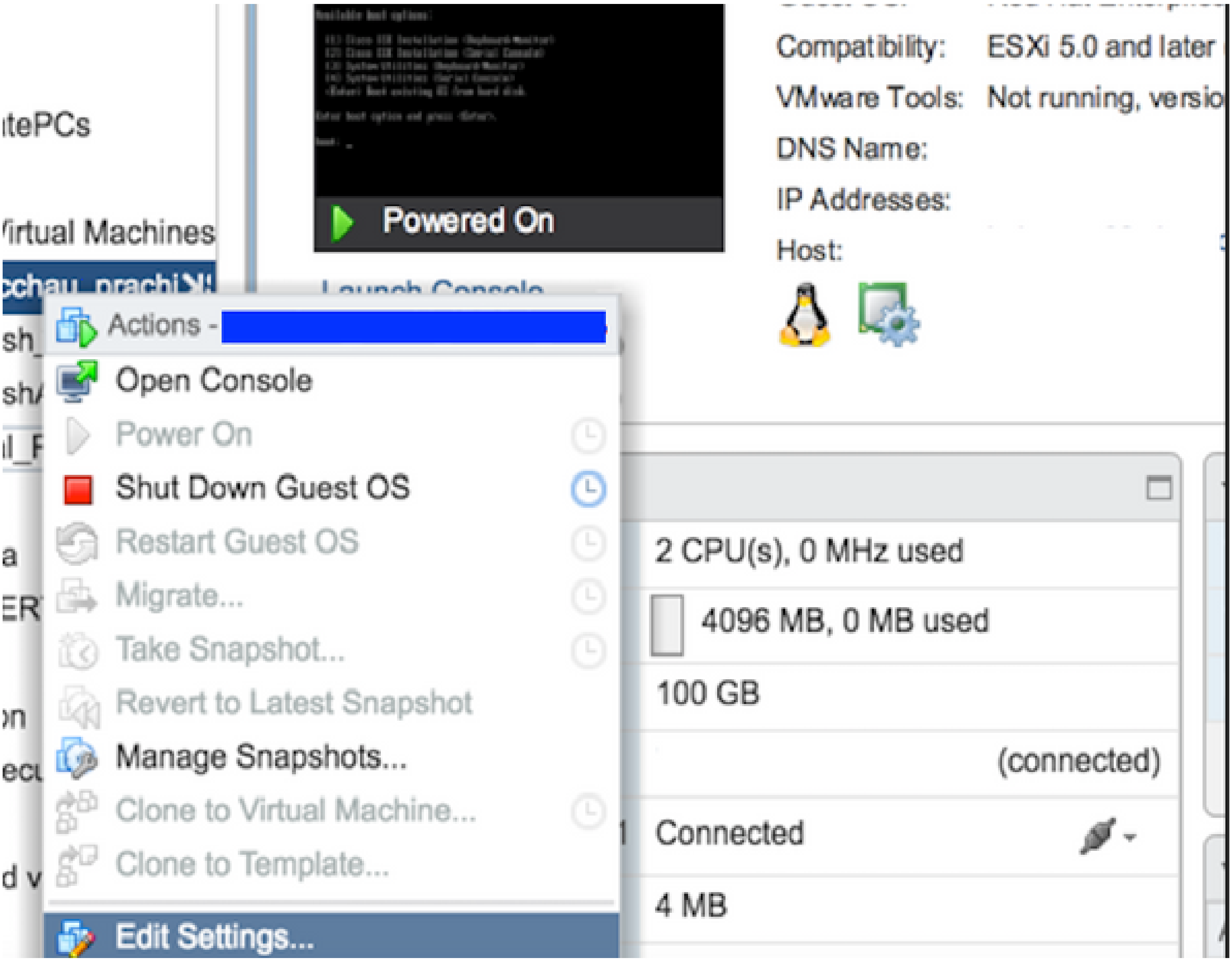
Password Recovery Procedure

Password Recovery for ISE Virtual Machine

Step 1. Download the ISO file of the current ISE version that runs in the environment from the Cisco software download site and upload it to the virtual machine's datastore.

Step 2. Power off the ISE virtual machine.

Step 3. Right-click **ISE VM** from the list and select **Edit Settings**.



Compatibility: ESXi 5.0 and later

VMware Tools: Not running, versio

DNS Name:

IP Addresses:

Host:

2 CPU(s), 0 MHz used

4096 MB, 0 MB used

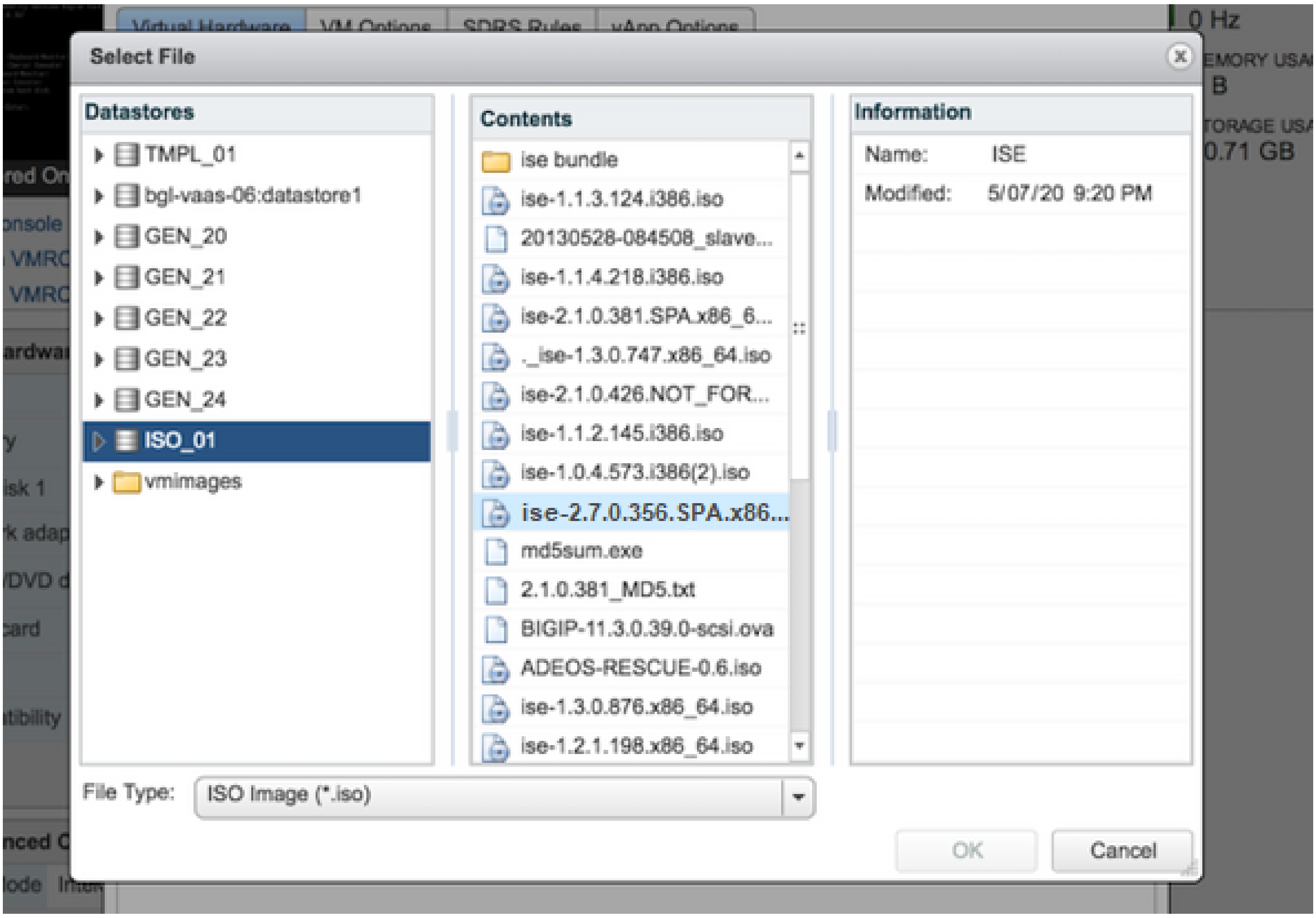
100 GB

(connected)

Connected

4 MB

Step 4. In the dialog box, navigate to **Virtual Hardware > CD/DVD**, browse to the ISE version ISO under datastore **ISO** file.



Select File

Datastores

- TMPL_01
- bgl-vaas-06:datastore1
- GEN_20
- GEN_21
- GEN_22
- GEN_23
- GEN_24
- ISO_01
- vmimages

Contents

- ise bundle
- ise-1.1.3.124.i386.iso
- 20130528-084508_slave...
- ise-1.1.4.218.i386.iso
- ise-2.1.0.381.SPA.x86_6...
- ._ise-1.3.0.747.x86_64.iso
- ise-2.1.0.426.NOT_FOR...
- ise-1.1.2.145.i386.iso
- ise-1.0.4.573.i386(2).iso
- ise-2.7.0.356.SPA.x86...
- md5sum.exe
- 2.1.0.381_MD5.txt
- BIGIP-11.3.0.39.0-scsi.ova
- ADEOS-RESCUE-0.6.iso
- ise-1.3.0.876.x86_64.iso
- ise-1.2.1.198.x86_64.iso

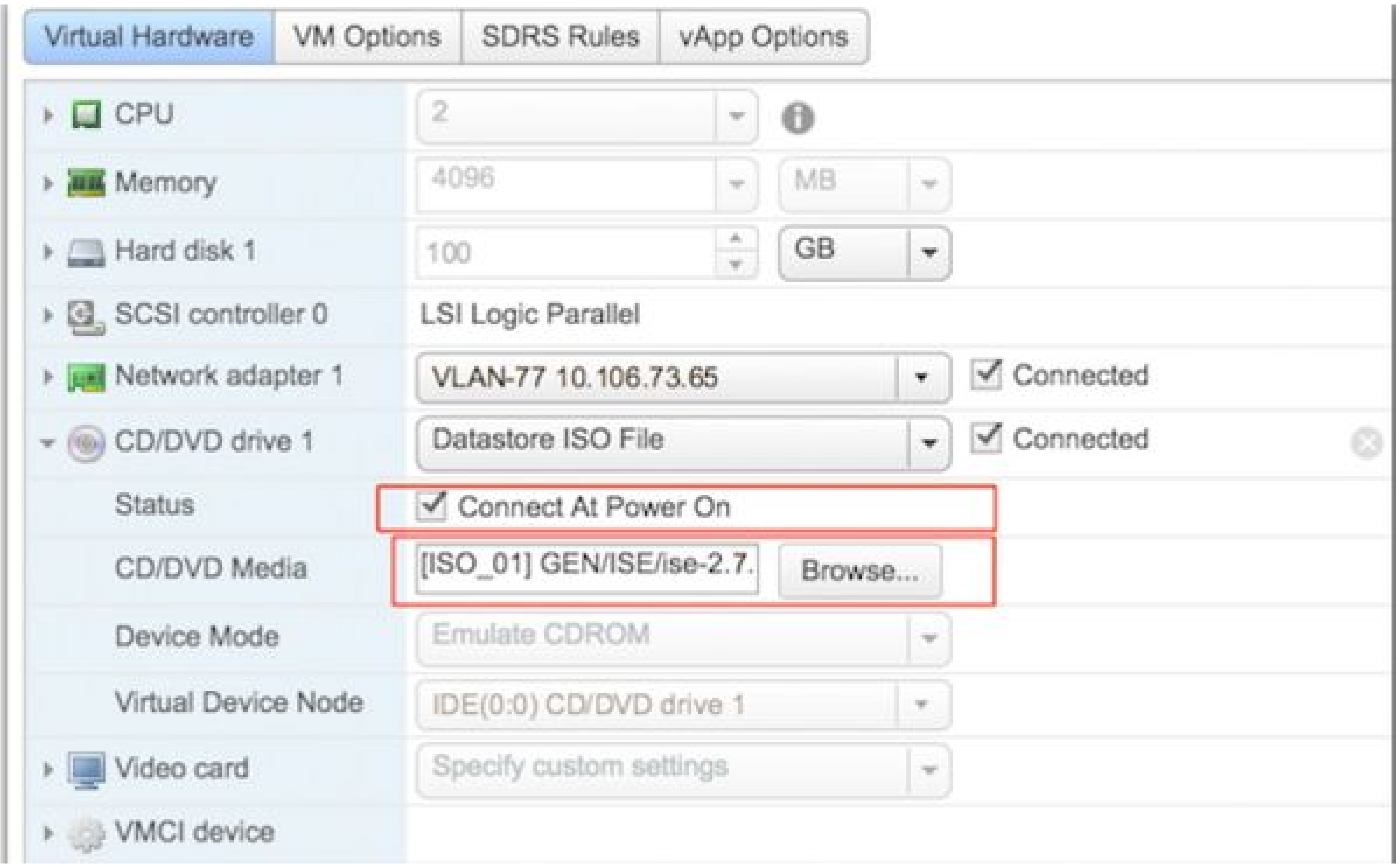
Information

Name: ISE

Modified: 5/07/20 9:20 PM

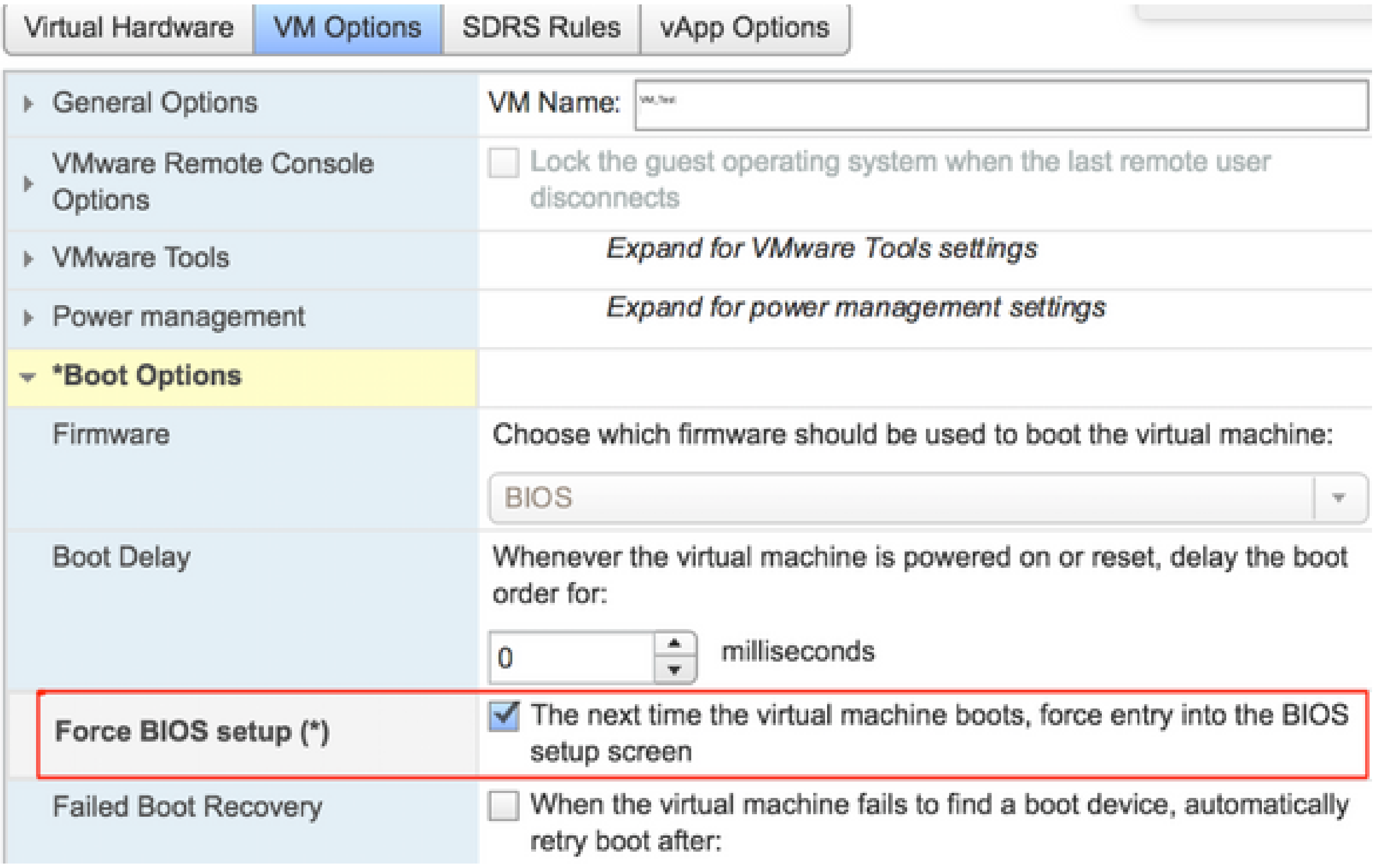
File Type: ISO Image (*.iso)

Step 5. Click **Connect At PowerOn** as shown in the image.



CPU	2	
Memory	4096 MB	
Hard disk 1	100 GB	
SCSI controller 0	LSI Logic Parallel	
Network adapter 1	VLAN-77 10.106.73.65	☑ Connected
CD/DVD drive 1	Datastore ISO File	☑ Connected
Status	☑ Connect At Power On	
CD/DVD Media	[ISO_01] GEN/ISE/ise-2.7.	
Device Mode	Emulate CDROM	
Virtual Device Node	IDE(0:0) CD/DVD drive 1	
Video card	Specify custom settings	
VMCI device		

Step 6. Navigate to **Options > Boot options**, enable the option **Force BIOS Setup** as shown in the image here, and click **OK** to continue.



General Options — VM Name:

VMware Remote Console Options — □ Lock the guest operating system when the last remote user disconnects

VMware Tools — *Expand for VMware Tools settings*

Power management — *Expand for power management settings*

***Boot Options**

Firmware — Choose which firmware should be used to boot the virtual machine: BIOS

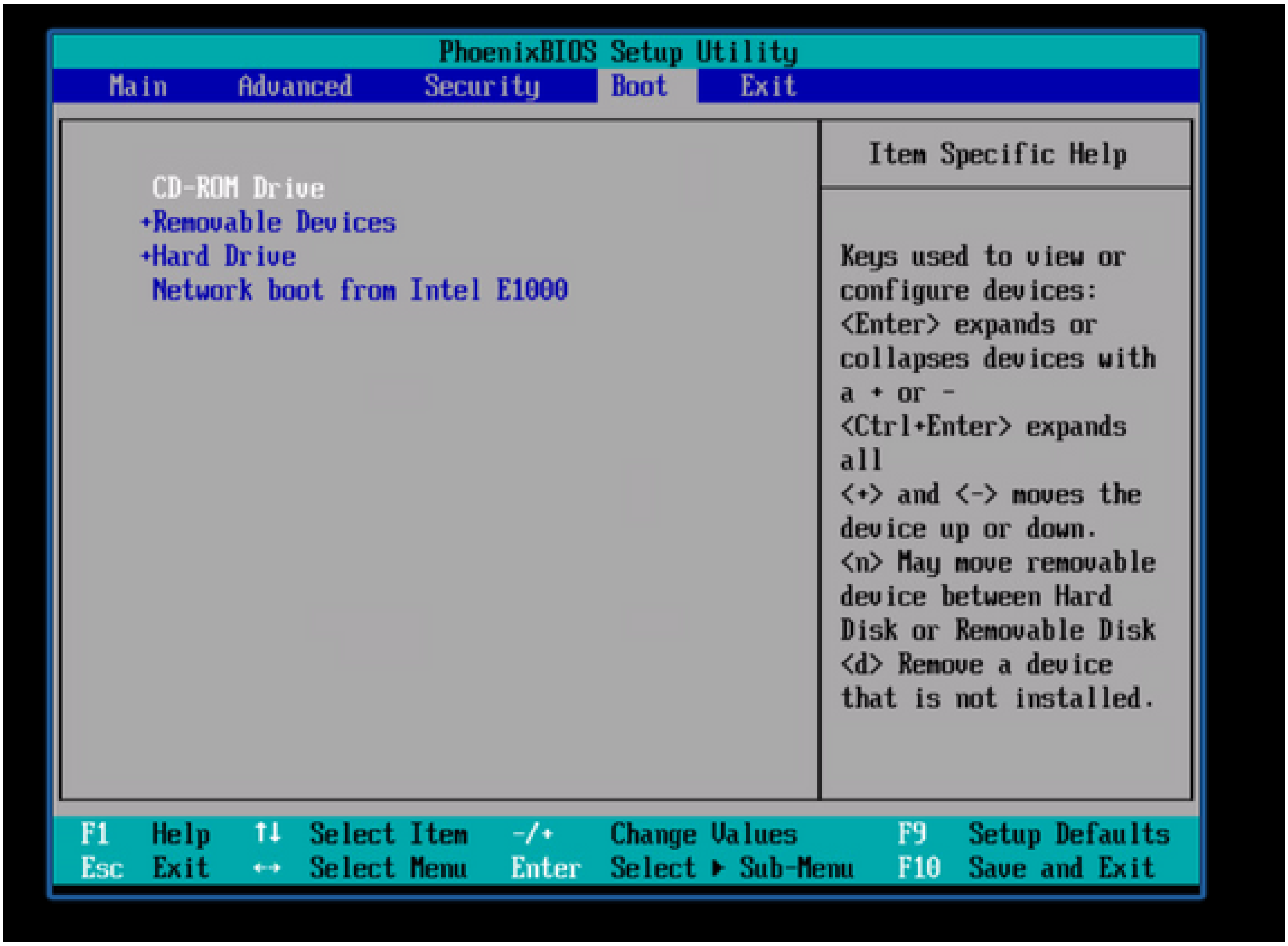
Boot Delay — Whenever the virtual machine is powered on or reset, delay the boot order for: 0 milliseconds

Force BIOS setup (*) — ☑ The next time the virtual machine boots, force entry into the BIOS setup screen

Failed Boot Recovery — □ When the virtual machine fails to find a boot device, automatically retry boot after:

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.



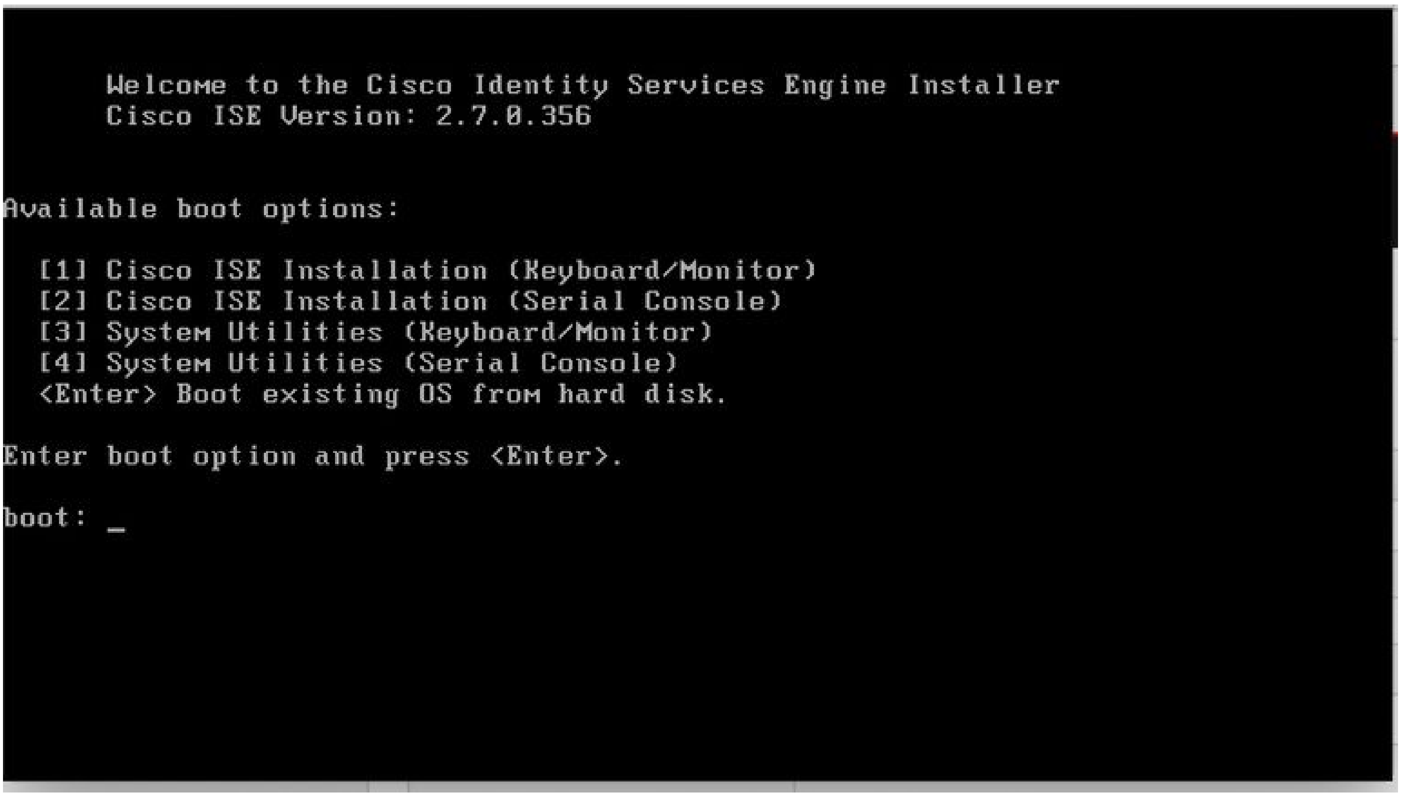
```
 CD-ROM Drive
+Removable Devices
+Hard Drive
 Network boot from Intel E1000
```

Keys used to view or configure devices: <Enter> expands or collapses devices with a + or - <Ctrl+Enter> expands all <+> and <-> moves the device up or down. <n> May move removable device between Hard Disk or Removable Disk <d> Remove a device that is not installed.

Cisco ISE supports these VMware servers and clients:

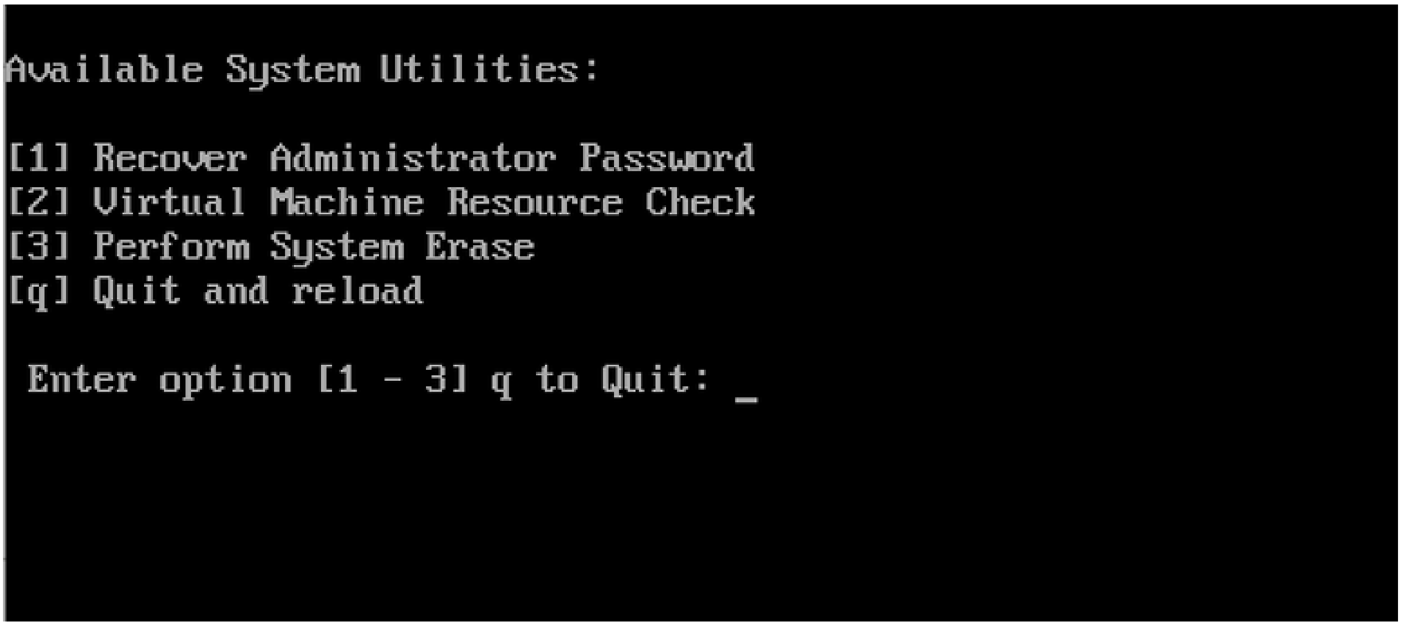
- VMware version 8 (default) for ESXi 5.*x* (5.1 U2 minimum) is the version to 9 or later. RHEL 7 is supported with VMware hardware version 9 and later.
- VMware version 11 (default) for ESXi 6.*x*

Step 9. Hit the **Enter** button to save new boot order settings and exit the BIOS configuration mode. Select option **3** from the ISE Installer page to start **System Utilities (Keyboard/Monitor).**



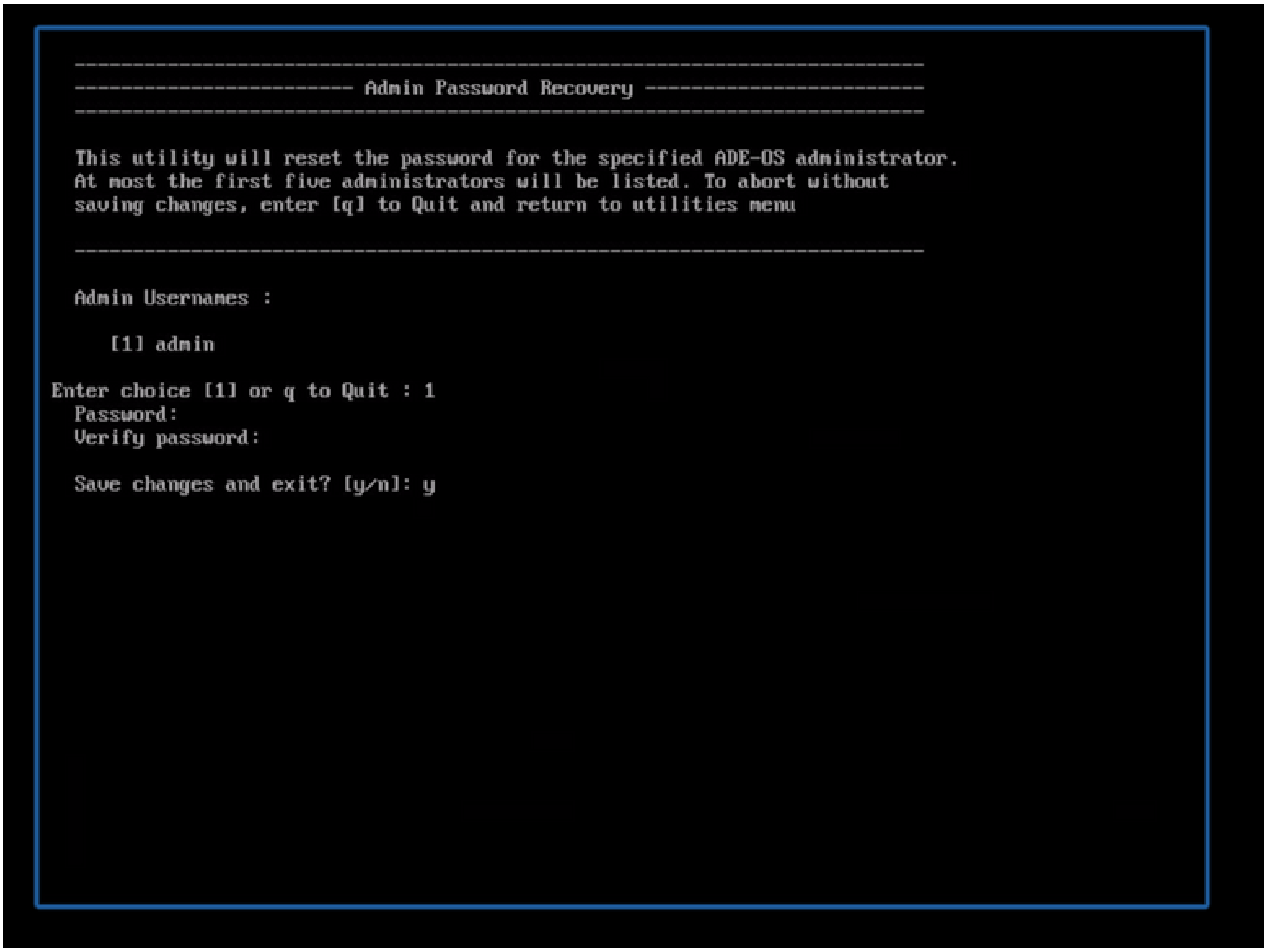
```
      Welcome to the Cisco Identity Services Engine Installer
      Cisco ISE Version: 2.7.0.356


Available boot options:

  [1] Cisco ISE Installation (Keyboard/Monitor)
  [2] Cisco ISE Installation (Serial Console)
  [3] System Utilities (Keyboard/Monitor)
  [4] System Utilities (Serial Console)
  <Enter> Boot existing OS from hard disk.

Enter boot option and press <Enter>.

boot: _
```

Step 10. Select Option **1** from **System Utilities** to recover the Administrator Password. Option **1** provides the list of administrators accounts configured on ISE device.



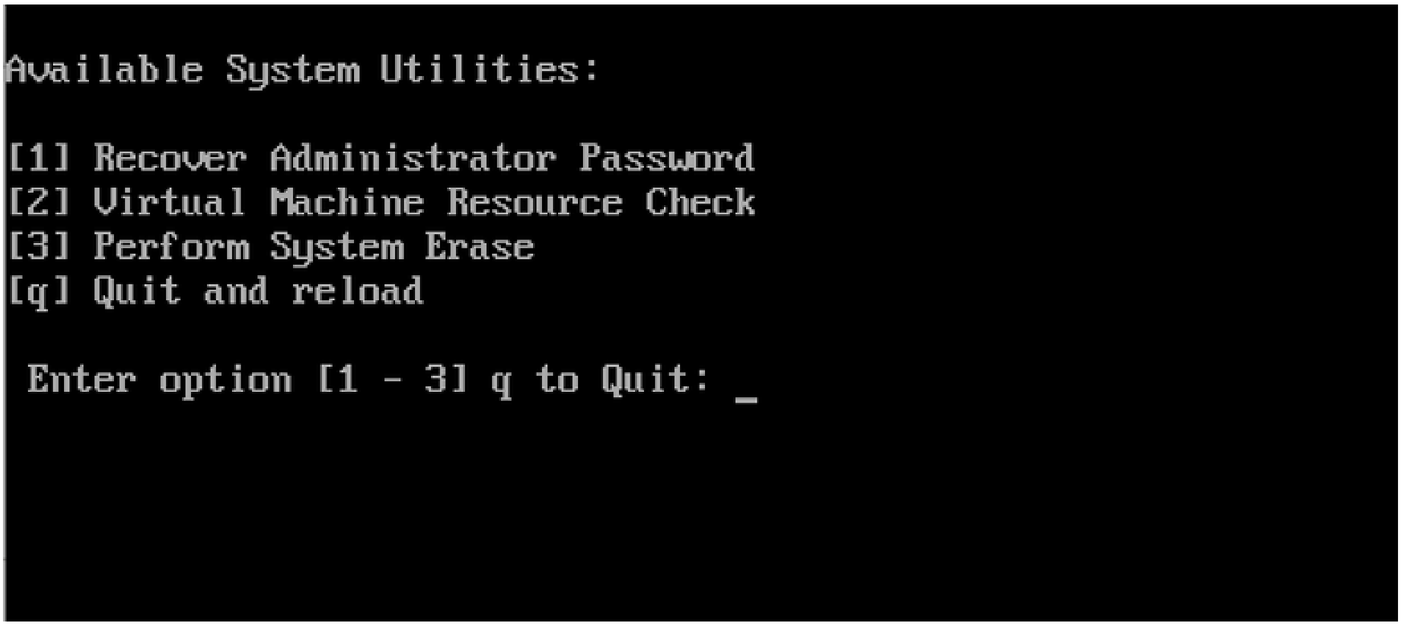
```
Available System Utilities:

[1] Recover Administrator Password
[2] Virtual Machine Resource Check
[3] Perform System Erase
[q] Quit and reload

 Enter option [1 - 3] q to Quit: _
```

Step 11. Select Option 1 for username **admin** and enter a new password. Enter **y** to save the new password and continue to **System Utilities** page.



```
-----------------------------------------------------------------------------
------------------------ Admin Password Recovery ------------------------
-----------------------------------------------------------------------------

   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
```

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



```
Available System Utilities:

[1] Recover Administrator Password
[2] Virtual Machine Resource Check
[3] Perform System Erase
[q] Quit and reload

 Enter option [1 - 3] q to Quit: _
```

Step 12. Click **Enter** to boot the ISE from the current hard disk.

Step 13. (Optional). Execute steps 6-8 in order to restore boot order to the hard drive as the first option after successful password recovery. This step is required so that you do not have to enter the admin password recovery prompt every time an ISE VM is rebooted.

> **Note:** If the new password does not work after you have followed the aforementioned steps, wait for 15-30 minutes before you attempt to sign in to the ISE CLI.

Password Recovery for SNS-36XX Series Appliance

There are three types of SNS 3600 series appliances which support ISE:

- SNS-3615
- SNS-3655
- SNS-3695

There are two methods to recover password on SNS 3600 Series 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

This Password Recovery method requires CIMC configuration setup on 36XX series hardware. Refer to Setting Up the System With the Cisco IMC Configuration Utility to know more about CIMC configuration steps.

Use CIMC connection to manage Cisco SNS-35XX and SNS-36XX appliances. KVM utility through CIMC connection can be used to perform all operations including BIOS configuration on Cisco SNS-35XX or Cisco SNS-36XX appliance.

Step 1. Use the ports that were selected in NIC Mode setting to connect Ethernet cables from the LAN to the server. The Active-active and Active-passive NIC redundancy settings require to connect to two ports. Detailed information is provided in CIMC configuration guide.

Step 2. Use a browser and the IP address of the CIMC to log in to the CIMC Setup Utility. The IP address is based upon CIMC config settings which were made during CIMC configuration steps(either a static address or the address assigned by your DHCP server).

> **Note**: The default user name for the server is admin. The default password is password.

Step 3. Enter the username and password in order to log in to the CIMC portal.

Step 4. Click **Launch KVM Console.**

Step 5. Click the **Virtual Media** tab.

Step 6. Click **Create Image** to select the current ISE version ISO from the system that runs your client browser.

Step 7. Check the **Mapped** check box against the virtual CD/DVD drive which is created.

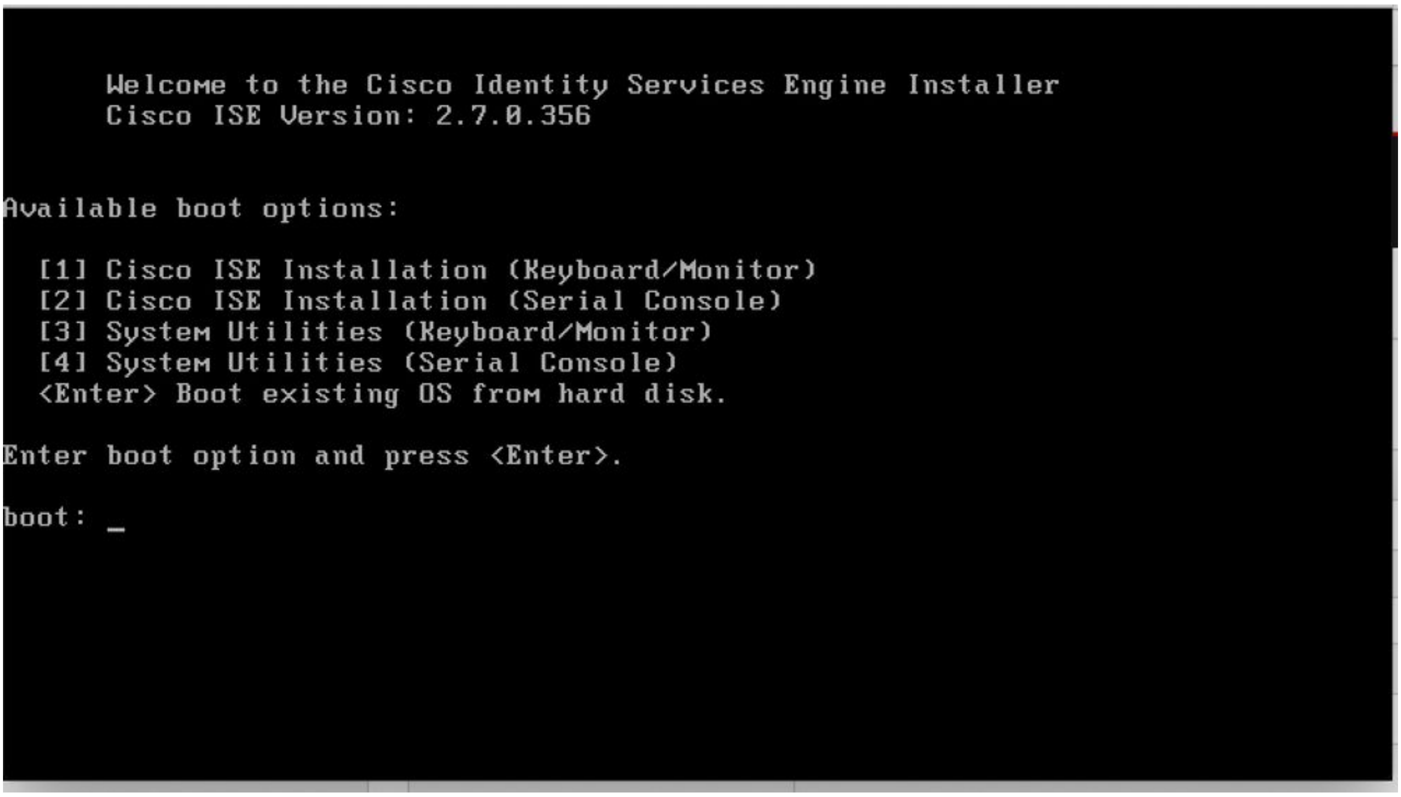
Step 8. Choose **Macros > Ctrl-Alt-Del** to boot the Cisco SNS-35XX or Cisco SNS-36XX appliance through use of the ISO image.

Step 9. Press F6 to bring up the boot menu. A similar screen appears as shown in this image.

Step 10. Select the CD/DVD that is mapped and press **Enter**. The message is displayed here.

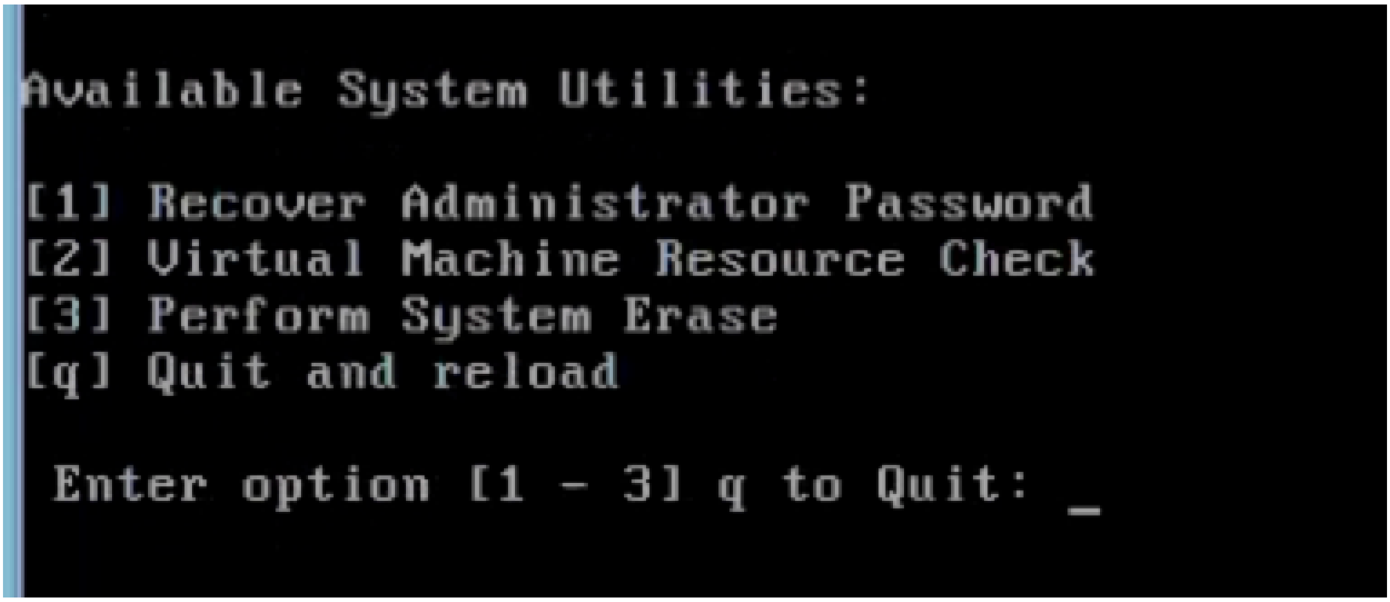
```
Welcome to the Cisco ISE 2.x Recovery
Available boot options:

[1] Cisco Secure ISE Installation (Keyboard/Monitor)
[2] Cisco Secure ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor
[4] System Utilities (Serial Console)
<Enter> Boot existing OS from hard disk. Enter boot option and press <Enter> boot:
```

Step 11. Select option 3 or option 4 (enter 3 for keyboard and video monitor connected to the appliance, or enter 4 if access is through a local serial console port connection):



```
      Welcome to the Cisco Identity Services Engine Installer
      Cisco ISE Version: 2.7.0.356

Available boot options:

  [1] Cisco ISE Installation (Keyboard/Monitor)
  [2] Cisco ISE Installation (Serial Console)
  [3] System Utilities (Keyboard/Monitor)
  [4] System Utilities (Serial Console)
  <Enter> Boot existing OS from hard disk.

Enter boot option and press <Enter>.

boot: _
```

Select Option 1 from the screen here and proceed.



```
Available System Utilities:

[1] Recover Administrator Password
[2] Virtual Machine Resource Check
[3] Perform System Erase
[q] Quit and reload

 Enter option [1 - 3] q to Quit: _
```

Step 12. Select the required username from the list and press enter to reset the password.

The console displays:

```
Admin username:
[1]:admin
[2]:admin2
[3]:admin3
[4]:admin4
Enter number of admin for password recovery:2
Password:
Verify password:
Save change and reboot? [Y/N]:y

Password reset is completed.
```

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. Power on the Cisco SNS-35XX or Cisco SNS-36XX appliance.

Step 2. Plugin the bootable USB drive that has the bootable Cisco Secure ISE ISO image into the USB port.

Step 3. Restart SNS-35XX appliance and navigate to the BIOS mode on console.

Step 4. In the BIOS mode, choose boot from USB.

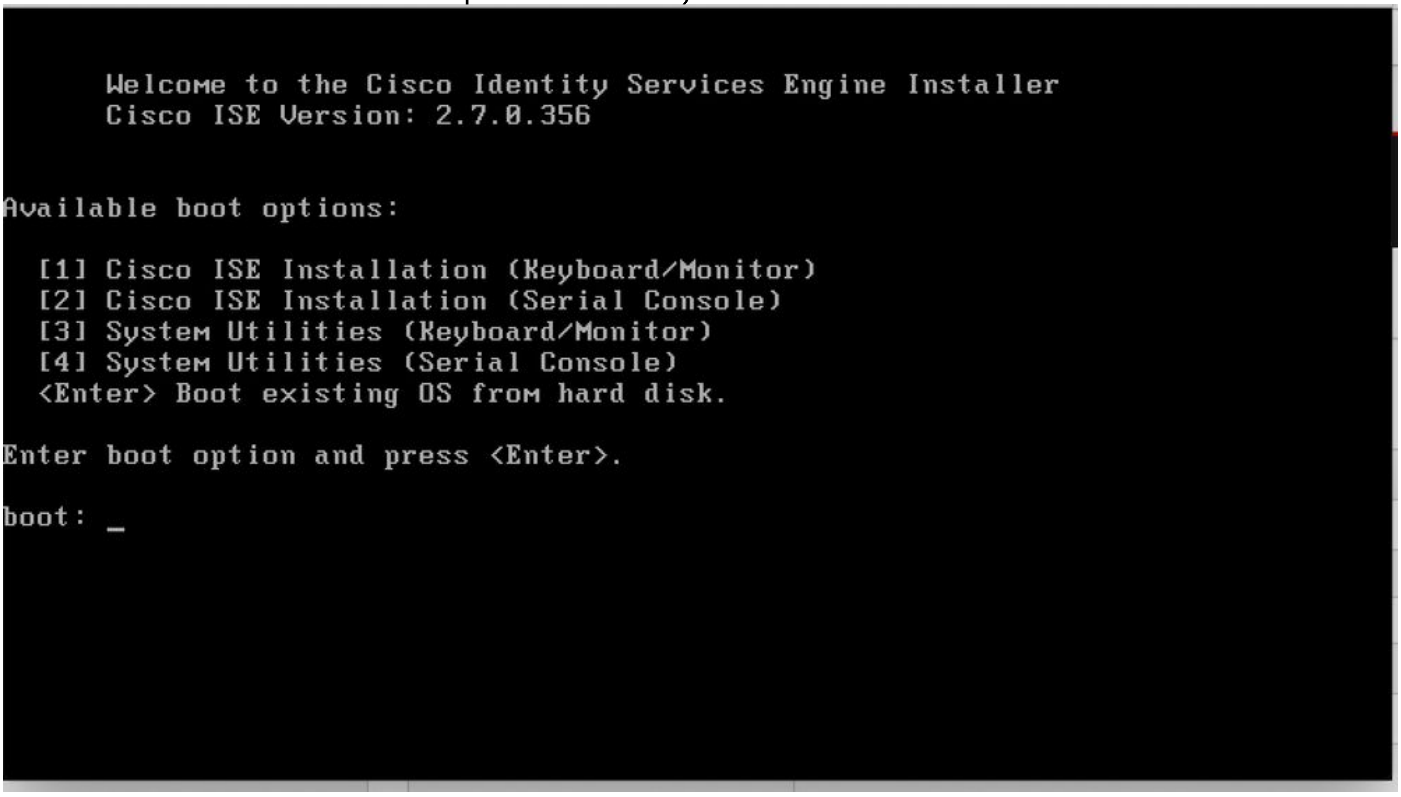
Step 5. Exit from the BIOS mode and click **Save**.

Step 6. Restart ISE appliance and boot from USB.

The message is displayed here.

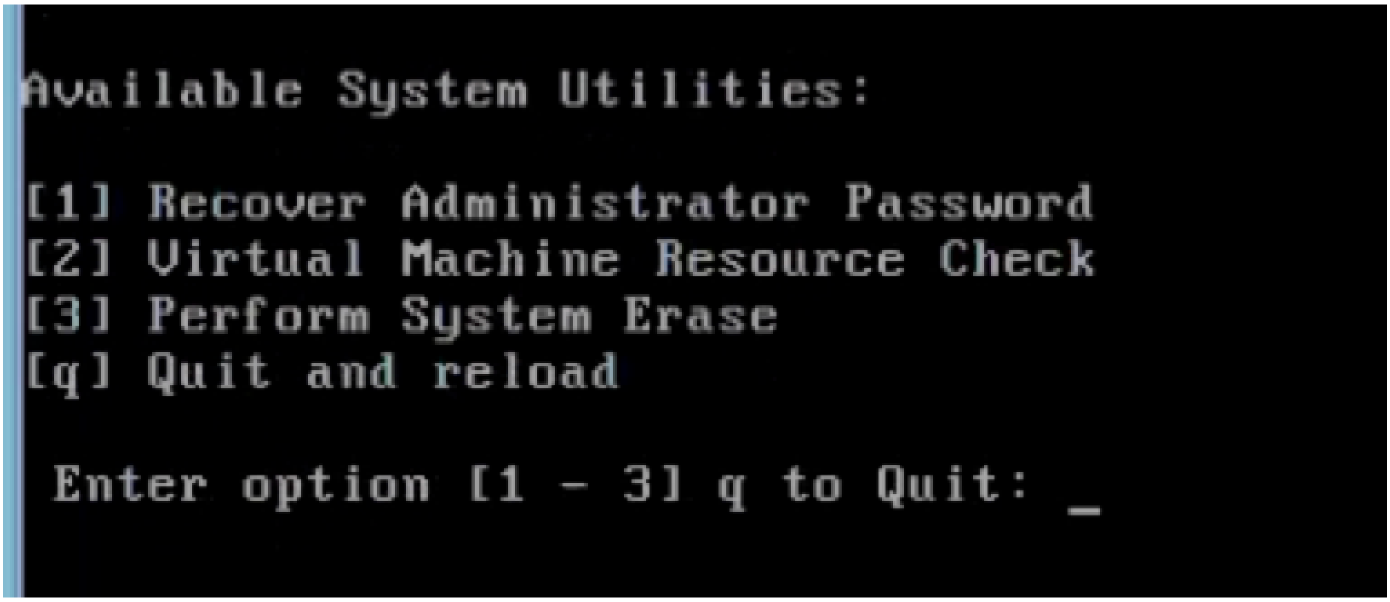
```
Welcome to the Cisco ISE 2.x Recovery
To boot from hard disk press <Enter>
Available boot options:
[1] Cisco Secure ISE Installation (Keyboard/Monitor)
[2] Cisco Secure ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor
[4] System Utilities (Serial Console)
<Remove USB key and reboot to boot existing Hard Disk>
Please enter boot option and press <Enter>
boot: 3
```

Step 7. Select option 3 or option 4 (enter 3 if connected through keyboard and a video monitor or enter 4 for a local serial console port connection):



```
     Welcome to the Cisco Identity Services Engine Installer
     Cisco ISE Version: 2.7.0.356

Available boot options:

  [1] Cisco ISE Installation (Keyboard/Monitor)
  [2] Cisco ISE Installation (Serial Console)
  [3] System Utilities (Keyboard/Monitor)
  [4] System Utilities (Serial Console)
  <Enter> Boot existing OS from hard disk.

Enter boot option and press <Enter>.

boot: _
```

Step 8. Select option 1 to start the administrator password recovery menu.



```
Available System Utilities:

[1] Recover Administrator Password
[2] Virtual Machine Resource Check
[3] Perform System Erase
[q] Quit and reload

 Enter option [1 - 3] q to Quit: _
```

Step 9. Select the correct username from the list and press enter to reset the password.

```
Admin username:
[1]:admin
[2]:admin2
[3]:admin3
[4]:admin4
Enter number of admin for password recovery:2
Password:
Verify password:
Save change and reboot? [Y/N]:y

Password reset is completed.
```

Additional Content

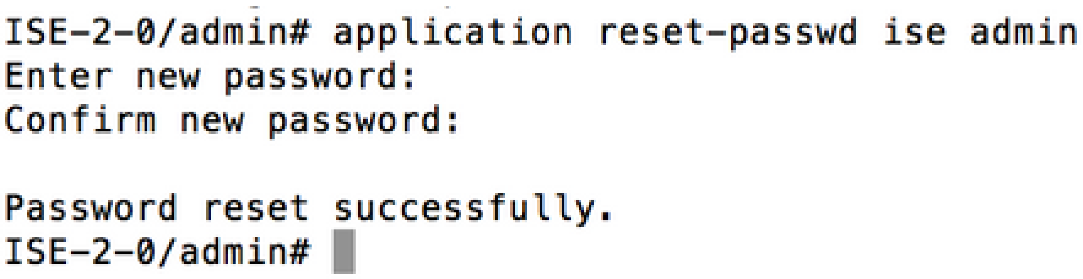
ISE GUI Password Recovery Mechanism

Step 1. Use the CLI admin account to log in on the console.

> **Note**: Remember that the console admin account is different than the web UI admin account. They have the same username but can have different passwords.

Step 2. From the command prompt, use the **application reset-passwd ise admin** command to set a new web UI admin password.

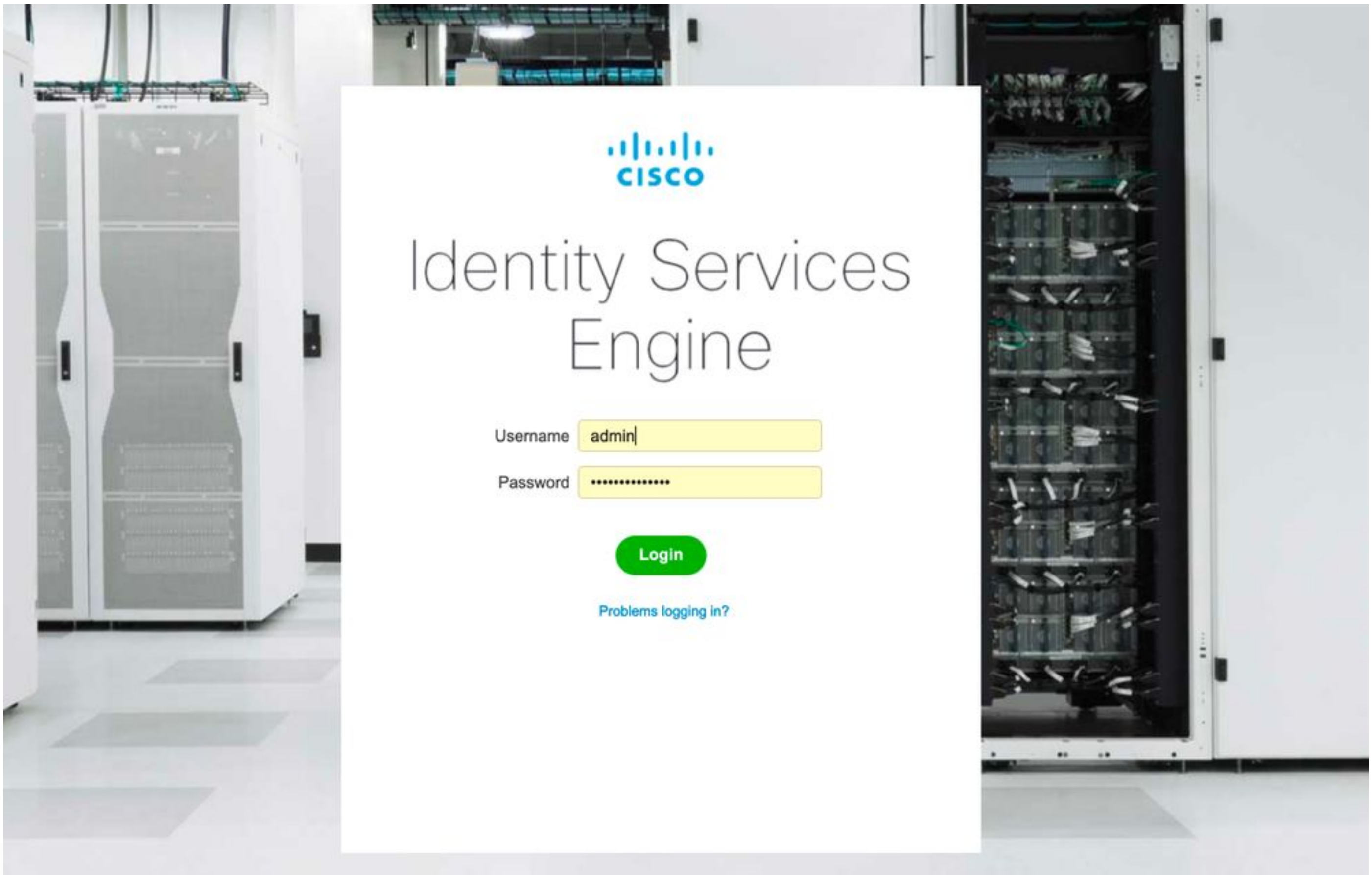
Step 3. Prompt to reset password appears as shown in this image.



```
ISE-2-0/admin# application reset-passwd ise admin
Enter new password:
Confirm new password:

Password reset successfully.
ISE-2-0/admin#
```

Step 4. Enter the new password as required.

Step 5. To confirm that the new password works, use the new password to log in to GUI.



Identity Services Engine

Username admin

Password ••••••••••••••