

Cisco UCS Server Configuration Utility User Guide, Release 6.3

First Published: 2023-10-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2023 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Overview of UCS Server Configuration Utility** 1

Introduction 1

Supported Platforms and Operating Systems 1

Hardware Requirements 1

CHAPTER 2 **Launching UCS Server Configuration Utility** 3

Introduction 3

Obtaining ISO Image From cisco.com 3

Booting UCS-SCU 4

Using vKVM Mapped vDVD 4

Using Cisco FlexMMC vDVD 5

Using CIMC Mapped vDVD 8

Using Physical Media 9

Using Network Boot Support 9

Exiting UCS-SCU 10

CHAPTER 3 **Understanding UCS Server Configuration Utility User Interface** 11

Introduction 11

License Agreement 11

UCS-SCU GUI Home Page 11

Navigation Pane 12

Sync SD Card Button 12

Rebooting a Server 12

CHAPTER 4 **Installing Operating Systems** 13

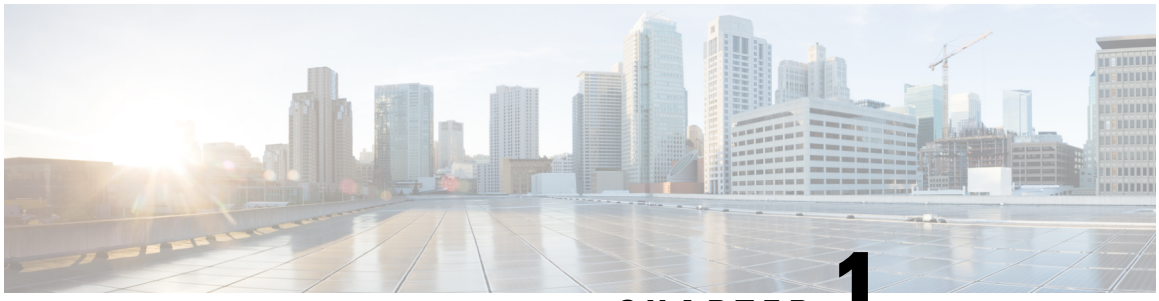
Introduction 13

Quick Install 14
Custom Install 14
ESXi Custom Installation 15
Installing ESXi 15
Windows OS Custom Installation 15
Installing Windows Server Operating System 15
Linux OS Custom Installation 16
Installing Linux Server Series Operating System 16

CHAPTER 5 **Non Interactive Operating System Installation 19**
Non Interactive Operating System Installation 19
Support for Network Boot from PXE, iPXE, HTTP and HTTPS 20
Modifying the nwboot.cfg File 20
Modifying the niscu.cfg File 27
Modifying conf_file 34
Running the Python Script to Start OS Deployment 36
Installing Operating Systems Using Commands 37
Sample nwboot.cfg file 40
Sample conf_file and niscu.cfg files 42

CHAPTER 6 **Configuring RAID Levels 45**
RAID Configuration 45
Storage Configuration 45
Physical Disks Area 46
Logical Disks Area 47
Creating RAID Arrays 47
Configuring Single-Level RAID 47
Configuring Nested RAID 48

APPENDIX A **Common Procedures for OS Installation 51**
Selecting a Installation Disk 51
Network Settings 51
Selecting Installation Drivers 52



CHAPTER 1

Overview of UCS Server Configuration Utility

This chapter includes the following sections:

- Introduction, on page 1
- Supported Platforms and Operating Systems, on page 1
- Hardware Requirements, on page 1

Introduction

The Cisco UCS Server Configuration Utility (SCU) is an application that helps you manage Operating System installation on your server. The utility helps you easily set up the OS from a single application.

Using the SCU, you can install and support an operating system and its associated drivers on a specific server.

Beginning with Release 6.3, you can install Cisco UCS Server Configuration Utility ISO boot through network like HTTP/HTTPS, PXE and iPXE along with the existing vMedia boot medium. For more information on the different network boot options, see Support for Network Boot from PXE, iPXE, HTTP and HTTPS, on page 20.

Beginning with Release 6.1(1a), options provided by Cisco UCS Server Configuration Utility are changed. For more information, refer Understanding UCS Server Configuration Utility User Interface, on page 11.

Supported Platforms and Operating Systems

Supported Platforms and Operating Systems

For details on supported platforms and operating systems, see Intersight OS Install Overview documentation when using SCU with Intersight OS installation or the associated *Release Notes for Cisco UCS Server Configuration Utility* when using SCU as a standalone utility.

Hardware Requirements

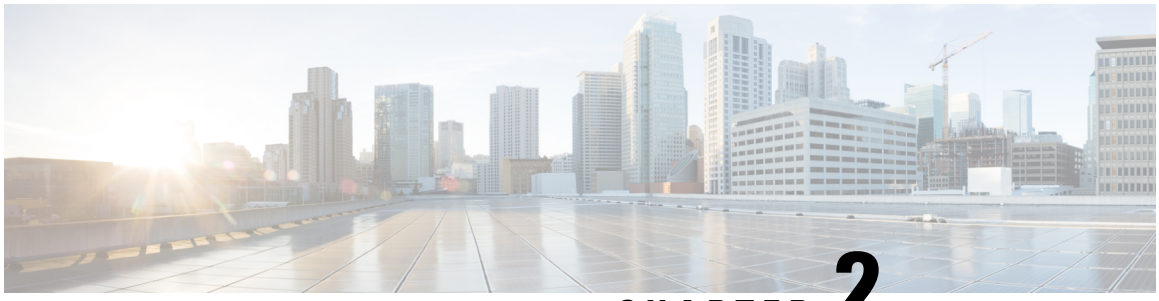
The following are the minimum hardware requirements for UCS-SCU:

- CD-ROM drive—A USB CD/DVD-ROM drive is required to be able to boot and run the UCS-SCU. You can also use the virtual media option in the CMC KVM, CIMC vMedia to boot UCS-SCU.

- Mouse—Some functions require a standard mouse (PS/2 or USB) for navigation.
- USB disk on key device—Functions such as saving UCS-SCU logs require a USB disk on key.
- RAM—A minimum of 1 GB RAM. If the available RAM is less than the minimum recommended value, UCS-SCU will not function properly.
- Network adapter—Some optional functions, such as, downloading the OS drivers from support.cisco.com, require network access. Any single onboard NIC adapter connection is supported.



Note RAID Cards—RAID configuration and OS installation are supported on selected controllers.



CHAPTER 2

Launching UCS Server Configuration Utility

- Introduction, on page 3
- Obtaining ISO Image From cisco.com, on page 3
- Booting UCS-SCU, on page 4
- Exiting UCS-SCU, on page 10

Introduction

UCS Server Configuration Utility (SCU) is a bootable image based on a 64-bit Linux kernel and can be used to perform operations such as configure RAID logical volume, install operating systems on Cisco rack servers. It is designed to run on one server at a time.

Obtaining ISO Image From cisco.com

Perform this procedure to find the ISO file for your server.

Before you begin

You must have valid Cisco login credentials to perform this procedure.

Step 1 Go to Software Download.

Note Log in using your Cisco credentials.

Step 2 Click **Select a Product** > **Browse All**.

Step 3 Click **Servers - Unified Computing** in the first column.

Step 4 Click **Cisco UCS C-Series Rack-Mount Standalone Server Software** in the middle column.

Step 5 Click the name of your server model from the last column.

A new page is displayed with the list of available software.

Step 6 Under **Select a Software Type** list, select **Unified Computing System (UCS) Server Configuration Utility**.

The Download Software page appears listing the release version and the UCS-SCU image.

Step 7 Select the desired release from the left pane.

Step 8 Click the **Download** icon on the right pane.

Step 9 Continue through the subsequent screens to accept the license agreement and browse to a location where you want to save the ISO file.

Booting UCS-SCU

You can launch the UCS-SCU application using one of the following options:

- Using vKVM Mapped vDVD, on page 4
- Using Cisco FlexMMC vDVD, on page 5
- Using CIMC Mapped vDVD, on page 8
- Using Physical Media, on page 9
- Using Network Boot Support, on page 9

Using vKVM Mapped vDVD

Before you begin

Download the UCS-SCU ISO image file from cisco.com. For information on how to download the image, refer Obtaining ISO Image From cisco.com, on page 3.

Step 1 Log in to Cisco IMC.

Step 2 From top right hand menu, click **Launch KVM**.

Note Depending on your browser settings, you may need to accept **KVM server certificate** and click the KVM viewer.

Virtual KVM Console displays the server console.

Step 3 Select **Virtual Media** > **vKVM-Mapped vDVD**.

The **Map Virtual Media - CD/DVD** window is displayed.

Step 4 Navigate to and select the ISO file and click Open to mount the image.

Step 5 Select **Map Drive** from the **Map Virtual Media - CD/DVD** window.

The following message is displayed in the virtual KVM console:

Successfully inserted media into device "vKVM Mapped DVD".

Step 6 Select **Power** > **Power Cycle System**.

Step 7 Press **F6** when the server starts to select a boot device.

The boot selection menu appears.

Step 8 Use the arrow keys to select **vKVM Mapped DVD** and then press **Enter**.

The server boots using the UCS-SCU image and launches the application in the KVM tab.

Using Cisco FlexMMC vDVD

Before you begin

Download the UCS-SCU ISO image file from cisco.com. For information on how to download the image, refer Obtaining ISO Image From cisco.com, on page 3.

Step 1 Log in to Cisco IMC.

Step 2 In the **Navigation** pane, click the **Storage**menu.

Step 3 In the **Storage** menu, select **Cisco FlexMMC**.

Step 4 In the **Files Copied** area of the **Cisco FlexMMC** pane, click the **Upload Files** tab.

The **Cisco FlexMMC Upload File** dialog box is displayed.

Step 5 In the **Cisco FlexMMC Upload File** dialog box, enter the following details:

Field	Description
Partition drop-down list	Type of partition. This can be: • **IMC Images**—Cisco .iso file. • **User Files**—Any .iso, image or any other file format. Only one .iso file can be uploaded. **Note** If you choose any other file format, Cisco IMC converts the file into an image file. In case of any other file format, the file size should be more than 10MB. It also takes extra space due to conversion.

Field	Description
Mount Type drop-down list	The type of mapping. This can be one of the following: **Note** Ensure that the communication port of the mount type that you choose is enabled on the switch. For example, when you are using CIFS as your mount type, ensure port 445 (which is its communication port) is enabled on the switch. Similarly, enable ports 80 for HTTP, 443 for HTTPS and 2049 for NFS when you use them. • **NFS**—Network File System. • **CIFS**—Common Internet File System. • **WWW(HTTP/HTTPS)**—HTTP-based or HTTPS-based system.
Remote Share field	The URL of the image to be mapped. The format depends on the selected Mount Type: • NFS—Use serverip:/share • CIFS—Use //serverip/share. • WWW(HTTP/HTTPS)—Use http[s]://serverip/share.
Remote File field	The name and location of the .iso or .img file in the remote share.

Field	Description
Mount Options field	Industry-standard mount options entered in a comma separated list. The options vary depending on the selected Mount Type. If you are using NFS, leave the field blank or enter one or more of the following: • **ro** • **nolock** • **noexec** • **soft** • **port=VALUE** If you are using CIFS, leave the field blank or enter one or more of the following: • **ro** • **nounix** • **noserverino** • **port=VALUE** • **Ntlm**—NT LAN Manager (NTLM) security protocol. Use this option only with Windows 2008 R2 and Windows 2012 R2. • **vers=VALUE** **Note** The format of the VALUE should be x.x If you are using WWW(HTTP/HTTPS), leave the field blank or enter the following: • **noauto** **Note** Before mounting the virtual media, Cisco IMC tries to verify reachability to the end server by pinging the server. • **username=VALUE** • **password=VALUE**
User Name field	The username for the specified **Mount Type**, if required.
Password field	The password for the selected username, if required.

Step 6 From top right hand menu, click **Launch KVM**.

Note Depending on your browser settings, you may need to accept **KVM server certificate** and click the KVM viewer.

Virtual KVM Console displays the server console.

Step 7 Select **Power** > **Power Cycle System (boot)**.

Step 8 Press **F6** when the server starts to select a boot device.

The boot selection menu appears.

Step 9 Use the arrow keys to select **vKVM-Mapped vDVD** and then press **Enter**.

The server boots using the UCS-SCU image and launches the application in the KVM tab.

Using CIMC Mapped vDVD

Before you begin

Download the UCS-SCU ISO image file from cisco.com. For information on how to download the image, refer Obtaining ISO Image From cisco.com, on page 3.

Step 1 Log in to Cisco IMC.

Step 2 In the **Compute** menu, click **Remote Management** > **Virtual Media**.

Step 3 In the **Virtual Media** tab > **Current Mappings** area, check for the required mapping.

Step 4 From top right hand menu, click **Launch KVM**.

Note Depending on your browser settings, you may need to accept **KVM server certificate** and click the KVM viewer.

Virtual KVM Console displays the server console.

Step 5 Select **Virtual Media** > **CIMC-Mapped vDVD**.

The **Map Virtual Media - Removable Disk** window is displayed.

Step 6 In the **Map Virtual Media - Removable Disk** window, perform the following steps:

a) Enter the desired name for the CIMC-mapped device.

b) Select any of the following protocols:

- NFS
- CIFS
- HTTP/S

By default, HTTP/S is selected.

c) Enter the file location in the format:

```
[http[s]://server-IP|DNS-name:Port/path-to-file.img
```

d) Enter the username and password.
e) Enter the desired name for the CIMC mapped device.
f) (Optional) Select the **Auto-remap**.

Step 7 Click **Save**.

Step 8 Select **Map Drive**.

After the host ejects this media, Cisco IMC will automatically re-map this device.

Step 9 Navigate to and select the ISO file and click Open to mount the image.

The following message is displayed in the virtual KVM console:

Successfully inserted media into device "CIMC-Mapped vDVD".

Step 10 Select **Power** > **Power Cycle System (boot)**.

Step 11 Press **F6** when the server starts to select a boot device.

The boot selection menu appears.

Step 12 Use the arrow keys to select **CIMC-Mapped vDVD** and then press **Enter**.

The server boots using the UCS-SCU image and launches the application in the KVM tab.

Using Physical Media

Before you begin

- Download the UCS-SCU ISO image file from cisco.com. For information on how to download the image, refer Obtaining ISO Image From cisco.com, on page 3.
- Create an .iso CD using an application that burns .iso CDs.

Step 1 Connect the USB DVD drive to the server through the USB port.

Step 2 Insert the physical media on to your DVD drive.

Step 3 Restart the server and press **F6** to enter the boot selection menu. Select **CDROM** drive as the boot device.

The server boots using the UCS-SCU image and starts the application.

Using Network Boot Support

Prerequisites

- A minimum of two systems is required for a PXE installation
- A server - a system running a DHCP server, a TFTP server, HTTP or FTP server to provide boot files. Theoretically, each of the servers can run on a different physical system; procedures in this section assume a single system runs all of them for simplicity

- A client - the system which you are booting SCU ISO. When the installation begins, the client will query the DHCP server, obtain boot files from the TFTP server

PXE Legacy Boot

Note The following files can be obtained from the mounted SCU ISO:

- `initrd`
- `bzImage`
- `rootfs.img`
- `ucs-scu-container-xxx.squash.fs`

1. Copy bootloader `Pxelinux.0` under `/var/lib/tftpboot` directory.
2. Copy `Pxelinux.cfg` under `/var/lib/tftpboot` directory.
3. Copy `initrd` and `bzImage` files from mounted SCU ISO under `/var/lib/tftpboot` directory.
4. Copy `rootfs.img`, `ucs-scu-container-xxx.squashfs` and `drivers` folder under `/var/www/html` directory or `/var/ftp/pub` directory.

PXE UEFI Boot

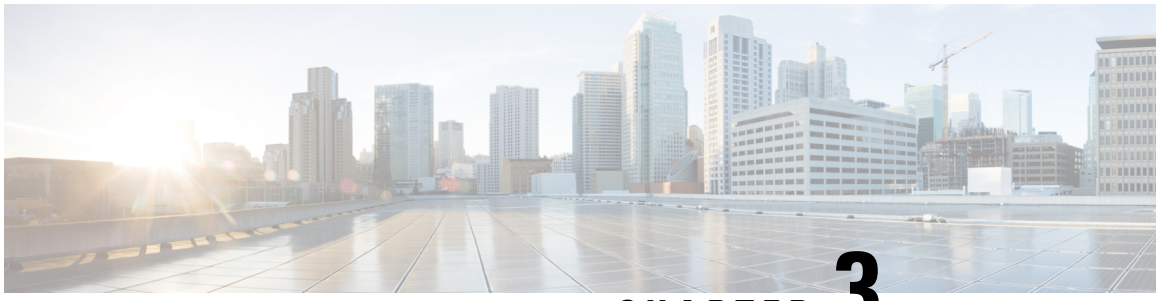
1. Copy `bootx64.efi` under `/var/lib/tftpboot` directory from extracted SCU ISO (which will be found in (`EFI/BOOT`) directory.
2. Copy `rootfs.img`, `ucs-scu-container-xxx.squashfs` and `drivers` folder under `/var/www/html` directory or `/var/ftp/pub` directory.

```
niosscubootmedium=pxe #type of the boot pxe/http/ipxe
```

Exiting UCS-SCU

Step 1 Remove the .iso disk from the disk drive.

Step 2 Click **Reboot** and then click **Yes** to confirm reboot of your server.



CHAPTER 3

Understanding UCS Server Configuration Utility User Interface

- Introduction, on page 11
- License Agreement, on page 11
- UCS-SCU GUI Home Page, on page 11

Introduction

The UCS-SCU GUI is a web-based management interface that allows you to perform tasks such as operating system installation and RAID configuration.

License Agreement

After UCS-SCU boots up, the first interface is the End User License Agreement. Select **I Accept** and click **Next** to agree to this license.

UCS-SCU GUI Home Page

Table 1: UCS-SCU GUI Elements

Element	Description
Navigation Pane	Located on the left side in the UCS-SCU user interface. See for more information.
OS Installation	Located on the right side of the GUI. Different pages appear in the **OS Installation** page depending on what you select in the **Navigation Pane**.
Execution Logs	Located at the bottom of the GUI. Shows the dynamic log of the system.

Navigation Pane

Table 2: Navigation Pane Elements

Element	Description
OS Installation	Installs the RHEL, SLES, Windows, and ESXi operating systems in a fully unattended mode. The most recent drivers for all onboard components are added from the Tools and Drivers CD or from other supported locations during the operating system installation. For more information about OS Install, see Installing Operating Systems, on page 13.
Server Configuration	Configures a RAID volume on attached hard drives of your server. Contains links to the RAID configuration pages: For more information about Server Configuration, see Configuring RAID Levels, on page 45
Help	Opens a window in the application that displays context-sensitive help for the displayed page.

Sync SD Card Button

Allows you to synchronize data written on a disk that is in an out-of sync RAID 1 partition to a replacement disk.



Note This button is available only on Cisco UCS C460 M4 server.

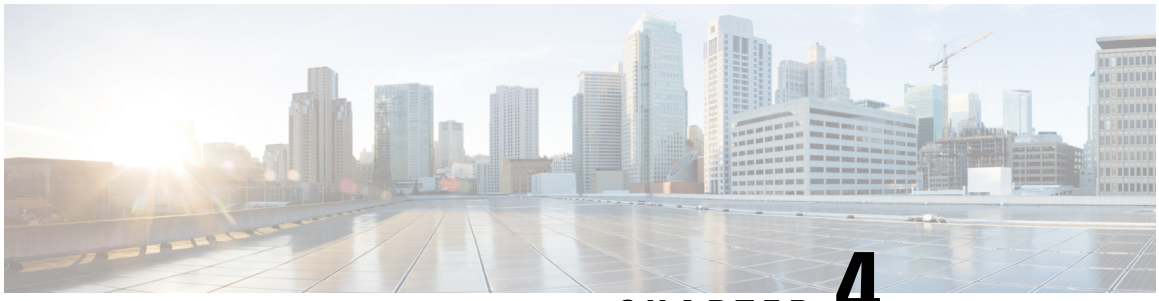
Rebooting a Server

Step 1 Click the **Reboot** button at the bottom of the GUI.

The **Reboot** dialog box appears.

Step 2 Click **Yes** to reboot.

The server is rebooted.



CHAPTER 4

Installing Operating Systems

- Introduction, on page 13
- Quick Install, on page 14
- Custom Install, on page 14
- ESXi Custom Installation, on page 15
- Windows OS Custom Installation, on page 15
- Linux OS Custom Installation, on page 16

Introduction

Cisco UCS-SCU has integrated device drivers including RAID drivers to seamlessly install operating systems on supported RAID logical arrays without additional load driver steps or devices such as the USB.

UCS-SCU supports OS installation on the following:

- Virtual disks
- NVMe device
- M.2 device
- Disks in JBOD mode
- SD Cards
- SW RAID

Note This is available only on Cisco UCS M5, M6 and M7 servers.

Note Before you begin the operating system installation, be sure that you have disabled the Watchdog Timer. If this feature is enabled and the value is set for a time duration that is less than the time needed to install the OS, the operating system installation process is interrupted. This Watchdog Timer feature automatically reboots or powers off the server after the specified time duration.

You can use the following two options to install the operating system:

- Quick Install, on page 14—Use the Quick Install option to install the operating system with the default settings.
- Custom Install, on page 14—Use the Custom Install option to modify the default settings prior to installing the operating system.

Quick Install

The Quick Install option allows you to quickly install the operating system with the default parameters. You can view the OS Install page with the default parameters depending on the target operating system. The Quick Install method does not require any user input and is a one-click operating system installation method.

Before you begin

If you wish to install the OS on a physical/virtual/logical disk, then ensure that virtual/logical disks are created before you install the operating system. If logical disks are not created, the disk details are not displayed under **Default Settings** area.

Step 1 Select **OS Installation** in the left navigation pane.

The **OS Installation** page displays all the OS installation options.

Step 2 From the **OS category** drop-down list, select the desired operating system.

Step 3 From the **OS version** drop-down list, select the desired version.

Step 4 From the **OS edition** drop-down list, select the desired edition.

Note This is available only on Windows operating system.

Step 5 From the **Installing Disk** drop-down list, select the disk where you want to install the OS.

Step 6 Click **Quick Install** to begin installation.

Step 7 Click **Yes** to confirm.

Step 8 Once the installation is complete, login using the default password.

Note Factory default password is `Pa55w0rd@`. Cisco recommends that you change the password after the first login.

Custom Install

The Custom Install option allows you to customize the default settings. Refer the following for custom installation:

- Installing ESXi, on page 15
- Installing Windows Server Operating System, on page 15
- Installing Linux Server Series Operating System, on page 16

ESXi Custom Installation

Installing ESXi

The ESXi Install option allows you to install the operating system and customize the default settings.



Note ESXi installation is also supported on SD cards for Cisco UCS C220 M4/M5 and C240 M4/M5 servers after enabling the virtual drive on the HV partition and rebooting the host.

Step 1 Select **OS Installation** in the left navigation pane.

The **OS Installation** page displays all the OS installation options.

Step 2 From the **OS category** drop-down list, select **VMware**.

Step 3 From the **OS version** drop-down list, select the desired ESXi version.

Step 4 From the **Installing Disk** drop-down list, select the disk location.

Step 5 Click **Custom install** button.

The **VMware ESXi Custom Install** page of the selected ESXi version appears.

Step 6 Perform the following in the **VMware ESXi Custom Install** page:

a) In the **Basic Configuration** area, do the following:

1. From the **Keyboard** drop down list, select the desired language.

   By default, the language is English.

2. In the **Root Password** field, enter the root password.
3. In the **Confirm Root Password** field, re-enter the root password.
4. In the **Product key** field, enter the product license key.

b) For **Installation Disk** area, perform the steps in Selecting a Installation Disk, on page 51.

c) For **Network Settings** area, perform the steps in Network Settings, on page 51.

Windows OS Custom Installation

Installing Windows Server Operating System

Perform this procedure to install Windows Server OS with custom settings.

Step 1 Select **OS Installation** in the left navigation pane.

The **OS Installation** page displays all the OS installation options.

Step 2 From the **OS category** drop-down list, select the **Windows**.

Step 3 From the **OS version** drop-down list, select the desired Windows version.

Step 4 From the **OS edition** drop-down list, select the desired edition.

Step 5 From the **Installing Disk** drop-down list, select the disk location.

Step 6 Click **Custom Install** to begin installation.

The **Windows Custom Install** page of the selected Windows version appears.

Step 7 Perform the following in the **Windows Custom Install** page:

a) In the **Basic Configuration** area, do the following:

1. From the **Time Zone** drop-down list, choose a time zone.
2. From the **Language** drop-down list, choose a language.
3. In the **Administrator Password** field, enter the password.
4. In the **Confirm Administrator Password** field, re-enter the password.
5. In the **Organization** field, enter a name of the organization of the administrator.

   The maximum limit is 15 characters.
6. In the **Workgroup** field, enter a workgroup name.

   The maximum limit is 20 characters.
7. In the **Host name** field, enter a Windows host.
8. From the **Auto logon** drop-down list, select **ON** or **OFF**.
9. In the **Product key** field, enter OS license key.

b) For **Installation Disk** area, perform the steps in Selecting a Installation Disk, on page 51.

c) For **Network Settings** area, perform the steps in Network Settings, on page 51.

d) For **Installation Drivers** area, perform the steps inSelecting Installation Drivers, on page 52.

Linux OS Custom Installation

Installing Linux Server Series Operating System

Perform this procedure to install Linux Server OS with custom settings.

Step 1 Select **OS Installation** in the left navigation pane.

The **OS Installation** page displays all the OS installation options.

Step 2 From the **OS category** drop-down list, select the **Linux**.

Step 3 From the **OS version** drop-down list, select the desired Linux version.

Step 4 From the **Installing Disk** drop-down list, select the disk location.

Step 5 Click **Custom Install** to begin installation.

The **Linux Custom Install** page of the selected Linux version appears.

Step 6 Perform the following in the **Linux Custom Install** page:

a) In the **Basic Configuration** area, do the following:

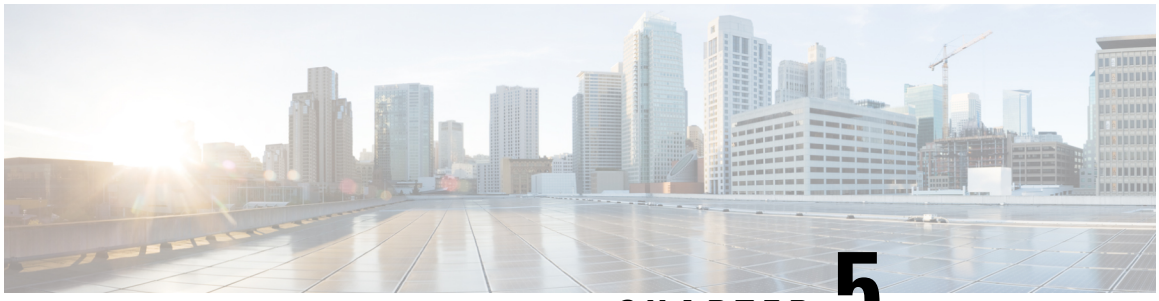
1. From the **Keyboard** drop down list, select the desired language.
2. From the **Timezone** drop down list, select the desired time zone.
3. From the **Language** drop down list, select the desired language.
4. In the **Root Password** field, enter the root password.
5. In the **Confirm Root Password** field, re-enter the root password.

b) For **Installation Disk** area, perform the steps in Selecting a Installation Disk, on page 51.

c) In the **Package Selection** area, select the applicable packages.

d) For **Network Settings** area, perform the steps in Network Settings, on page 51.

e) For **Installation Drivers** area, perform the steps in Selecting Installation Drivers, on page 52.



CHAPTER 5

Non Interactive Operating System Installation

This chapter contains the following sections:

- Non Interactive Operating System Installation, on page 19
- Support for Network Boot from PXE, iPXE, HTTP and HTTPS, on page 20
- Modifying the nwboot.cfg File, on page 20
- Modifying the niscu.cfg File, on page 27
- Modifying conf_file, on page 34
- Running the Python Script to Start OS Deployment, on page 36
- Installing Operating Systems Using Commands, on page 37
- Sample nwboot.cfg file, on page 40
- Sample conf_file and niscu.cfg files, on page 42

Non Interactive Operating System Installation

Non Interactive Server Configuration Utility (NI-SCU) helps deploy operating systems without user intervention.

To install operating systems using NI-SCU, do the following:

- Modify the nwboot.cfg file to include information such as the target server, the SCU ISO file location, and the log collection details.
- Modify the niscu.cfg configuration file to include information such as the target server, the SCU ISO file location, and the log collection details.
- See Modifying the niscu.cfg File, on page 27.
- See Modifying conf_file, on page 34.
- Prepare the answer file for kickstart installation.

  For sample answer files, see the Custom OS Installation Examples chapter.
- Run the `os_install-4.2.yc.yyyymmddab.py` script to begin the installation.

  See Running the Python Script to Start OS Deployment, on page 36.

Support for Network Boot from PXE, iPXE, HTTP and HTTPS

Beginning with Release 6.3, you can perform SCU Network boot from the following network options with IPv4 and IPv6.

- PXE
- iPXE
- HTTP
- HTTPS

The above network boot options are available in addition to the existing boot medium options like CIMC vMedia.

You can perform the SCU ISO boot from the above network options using the NISCU-XML API and NISCU-Redfish interfaces on Cisco UCS M5, M6 and M7 servers.

Beginning with Release 6.3, for non interactive operating system installation using HTTP/HTTPS, PXE and IPXE, you must first configure the `nwboot.cfg` file.

Modifying the nwboot.cfg File

Beginning with Release 6.3, for non interactive operating system installation using HTTP/HTTPS, PXE and IPXE, you must first configure the `nwboot.cfg` file.

The `nwboot.cfg` file consists of the following sections:

Default

The Default section consists of the following parameter:

Table 3: Parameters in the Default Section

Parameter	Description
`Update_Timeout`	The time (in minutes) the python script is active after it has been started. The default value is 240 minutes. The valid range is 30 to 240 minutes.

Example

```
[defaults]
update_timeout=240
```

SCU Repository

The SCU Repository section consists of the following parameters:

Table 4: Parameters in the SCU Repository Section

Parameter	Description
`BootMedium`	The boot medium to install SCU boot. The following types are supported: • vMedia • HTTP • FlexMMC • MicroSD • PXE • IPXE



Note See the below sections for the details of the fields available for the respective boot medium under **SCU Repository**.

Table 5: HTTP Boot Medium

Parameter	Description
`ImageRepository`	Path where SCU ISO resides in the HTTP share
`MACAddress`	The MAC address assigned to the active network interface to SCU
`PCIeSlot`	The name of the PCIe slot in which the controller is located.
`PhysicalPortNumber`	Physical Port Number

Parameter	Description
`IPv4Address` and `IPv6Address`	IP address for IPv4 and IPv6 These are the following parameters for IPv4: • AddressOrigin • Address - Host IP Address for the network interface • Gateway - IPv4 Gateway Address • Subnetmask - IPv4 Subnet Address • Static Name Server These are the following parameters for IPv6: • AddressOrigin • Address - Host IP Address for the network interface • Gateway - IPv6 Gateway Address • Subnetmask - IPv6 Subnet Address • Static Name Server

Table 6: vMedia Boot Medium

Parameter	Description
`ImageRepository`	Path where SCU ISO resides in the HTTP share
`TransferProtocol`	The transfer protocol type.
`Username`	User credentials
`Password`	
`MountOptions`	Mounting options

Table 7: PXE Boot Medium

Parameter	Description
`ImageRepository`	Path where SCU ISO resides in the HTTP share
`MACAddress`	The MAC address assigned to the active network interface to SCU
`PCIeSlot`	The name of the PCIe slot in which the controller is located.
`PhysicalPortNumber`	Physical port number

Parameter	Description
AddressOrigin	Server IP address from which IPv4 or IPv6 origins The value is DHCP.

Table 8: iPXE Boot Medium

Parameter	Description
ImageRepository	Server IP address from which IPv4 or IPv6 origins The value is DHCP.
MACAddress	The MAC address assigned to the active network interface to SCU
PCIeSlot	The name of the PCIe slot in which the controller is located.
PhysicalPortNumber	Physical port number

Example

```
"BootMedium": {
            "VMEDIA": {
                "ImageRepository": "10.10.10.1/home/nfsshare/iso/scu.iso",
                "TransferProtocol": "nfs",
                "Username": "root",
                "Password": "password",
                "MountOptions": ""
            },
            "HTTP": {
                "ImageRepository": "http://10.10.10.1:80/iso/scu.iso",
                "MACAddress": "70:df:2f:86:af:02",
                "PCIeSlot": "L",
                "PhysicalPortNumber": 1,
                "IPv4Address": {
                    "AddressOrigin": "Static",
                    "Address": "10.104.255.179",
                    "Gateway": "10.104.255.129",
                    "SubnetMask": "255.255.255.128",
                    "StaticNameServer": "64.104.76.247"
                },
                "IPv6Address": {
                    "AddressOrigin": "DHCPv6",
                    "Address": "fc00:1234::a:b:c:d",
                    "PrefixLength": 64,
                    "Gateway": "fe80::fe15:b4ff:fe97:90cd",
                    "StaticNameServer": "fe80::fe15:b4ff:fe97:90cd"
                }
            },
            "FLEXMMC": {
                "ImageRepository": "scu.iso"
            },
            "MICROSD": {},
            "PXE": {
                "ImageRepository": "ftp://10.104.255.224/pub/scu",
                "MACAddress": "70:df:2f:86:af:02",
                "PCIeSlot": "L",
                "PhysicalPortNumber": 1,
```

```
            "IPv4Address": {
                "AddressOrigin": "DHCP"
            }
        },
        "IPXE": {
            "ImageRepository": "http://10.10.10.1/iso/scu.iso",
            "MACAddress": "70:df:2f:86:af:02",
            "PCIeSlot": "L",
            "PhysicalPortNumber": 1
        }
    }
```

OS Details

In the OS Details section, provide the OS Repository and Target OS details of the share where the SCU ISO image is located.

The OS Details section consists of the following parameters for OS Repository, vMedia boot medium and Target OS:

Table 9: OS Repository

Parameter	Description
MediaType	Type of media.
BootMedium	The boot medium to install SCU boot. The following types are supported: • vMedia • HTTP • FlexMMC • MicroSD • PXE • IPXE

Table 10: vMedia Boot Medium

Parameter	Description
`ImageRepository`	SCU ISO boot image repository location
`Transfer Protocol`	The transfer protocol type.
`Username`	User credentials
`Password`	
`Mount Options`	Mounting options

Example

```
"OSDetails": {
        "OSRepository": {
            "MediaType": "Local",
            "BootMedium": {
                "VMEDIA": {
                    "ImageRepository":
"10.10.10.1/home/nfsshare/iso/rhel/RHEL-8.5.0-20211013.2-x86_64-dvd1.iso",
                    "TransferProtocol": "nfs",
                    "Username": "root",
                    "Password": "password",
                    "MountOptions": ""
                }
            }
        },
        "TargetOS": {
            "OSName": "rhel8u5x64",
            "OSEdition": "None"
        }
```

Target Disk

In the Target Disk section, provide the type of disk details.

The Target Disk section consists of the following parameters:

Table 11: Target Disk

Parameter	Description
PHYSICALDISK	Enter the Drive Serial Number.
VIRTUALDISK	Enter the following details: • Storage Controller Slot ID • Virtual Drive Number
DISKNAME	Enter the OS Drive details.
VIRTUALDRIVENAME	Enter the virtual drive name.
ONBOARDSATAM2SSD	Enter the slot details for SATAM2SSD.
M2SWVDNAME	Enter the details for M2 SW RAID Name.
FC	Enter the following details: • HostWWPN • TargetWWPN • LUN
iSCSI	Enter the following details: • MACAddress • Primary Target Name • Primary LUN

Example

```
"TargetDisk": {
        "PHYSICALDISK": {
            "DriveSerialNumber": "06VSGVVB"
        },
        "VIRTUALDISK": {
            "StorageControllerSlotID": "MRAID",
            "VirtualDriveNumber": 0
        },
        "DISKNAME": {
            "OSDrive": "/dev/sdk"
        },
        "VIRTUALDRIVENAME": {
            "VirtualDriveName": "Hypervisor"
        },
        "ONBOARDSATAM2SSD": {
            "SATAM2SSD": "slot1"
        },
        "M2SWVDNAME": {
            "M2SWRAIDName": "RAID0"
        },
        "FC": {
            "HostWWPN": "10:00:54:88:DE:A7:32:6F",
            "TargetWWPN": "50:06:01:68:3E:A0:62:22",
            "Lun": 200
        },
        "ISCSI": {
            "MACAddress": "70:DF:2F:86:AE:FD",
            "PrimaryTargetName":
"iqn.2001-05.com.equallogic:0-af1ff6-082b3ebe6-cf2005780845d665-iqn.siva-25.com",
            "PrimaryLUN": 1
        }
```

Remote Log

In the Remote Log section, provide the IP address and access details of the share where the installation logs will be saved.

The Remote Log section consists of the following parameters:

Table 12: Parameters in the Remote Log Section

Parameter	Description
`ImageRepository`	The IP address of the share where the log file is generated during the installation.
`TransferProtocol`	The protocol type used to access the share. The following protocols are supported: • SCP • SFTP
`Username` `Password`	The user credentials to access the share.

Example

```
"RemoteLog": {
        "ImageRepository": "10.10.10.10/home/nfstest/scu.log",
        "TransferProtocol": "scp",
        "Username": "root",
        "Password": "John123"
```

Answer File

In the Answer File section, provide access details of the share where the answer file is located. The answer file contains details about OS deployment.

Example

```
"AnswerFile": {
        "ImageRepository": "10.10.10.10/home/nfstest/answerfile",
        "TransferProtocol": "scp",
        "Username": "root",
        "Password": "John123"
```

Modifying the niscu.cfg File

Beginning with Release 6.3, for non interactive operating system installation using HTTP/HTTPS, PXE and IPXE, you must first configure the `nwboot.cfg` file.

For non interactive operating system installation using vMedia, you must first configure the `niscu.cfg` file.

Note You do not have to configure `nwboot.cfg` file while installing non interactive operating system using vMedia.

The `niscu.cfg` file consists of the following sections:

- Default, on page 27
- SCU, on page 28
- NIOS Install, on page 29
- Log Collection, on page 30
- OS, on page 31
- Answer File, on page 32
- Target System, on page 33

Each section must have an unique name. The section name is provided by the user.

Default

The Default section consists of the following parameters:

Table 13: Parameters in the Default Section

Parameter	Description
`[section_name]`	Enter a name for the section.

Parameter	Description
use_http_secure=	The HTTP type. The default value is 'Yes'. Type 'No' if the connection is insecure.
update_timeout=	The time (in minutes) the python script is active after it has been started. The default value is 120 minutes. The valid range is 30 to 240 minutes.

Example

```
[defaults]
use_http_secure=yes
update_timeout=120
```

SCU

In the SCU section, provide the IP address and access details of the share where the SCU ISO image is located.

The SCU section consists of the following parameters:

Table 14: Parameters in the SCU Section

Parameter	Description
[section_name]	Enter a name for the section.
isoshareip=	The IP address of the SCU ISO share.
isosharepath=	The location of the ISO image in the share.
imagefile=	The name of the SCU ISO image.
isosharetype=	The share type. The following share types are supported: • NFS • CIFS • WWW (HTTP or HTTPS)
isoshareuser=	The user credentials to access the share.
isosharepassword=	
bootmedium=	The medium to be used to boot from. The following types are supported: • vmedia - To boot from vmedia • flexmmc- To boot from eMMC • microsd - To boot from microsd

Parameter	Description
nios_section=	The nios_install section containing the OS installation process.

Example

```
[scu_iso]
isoshareip=192.0.2.10
isosharepath=/cifsshare
imagefile=ucs-cxxx-scu-5.0.0.39.iso
isosharetype=cifs
isoshareuser=Administrator
isosharepassword=John123
bootmedium=vmedia
```

NIOS Install

The NIOS Install section initiates the OS installation process and consists of the following parameters.

Table 15: Parameters in the NIOS Install Section

Parameter	Description
remoteShareIp=	IP Address of the scuConfigFile remote share
remoteSharePath=	scuConfigFile remote share path.
remoteShareFile=	scuConfigFile in the remote share
remoteShareType=	Remote share protocol. The following are supported: • SCP • SFTP • TFTP • WWW (HTTP or HTTPS)
username=	The user credentials to access the remote share.
password=	
scubootmedium=	The medium to be used to SCU boot from. The following types are supported: • HTTP - To boot from HTTP or HTTPS • PXE - To boot from PXE • IPXE - To boot from IPXE • vmedia - To boot from vmedia • flexmmc- To boot from eMMC • microsd - To boot from microsd

Parameter	Description
`osBootMedium=`	The medium to be used to boot SCU ISO from. vmedia is the supported medium.
`targetDiskType=`	The type of target disk. The following types are supported: • physicaldisk • virtualdisk • microsd

Example

```
[nios_install]
niosremoteshareip=10.10.10.10
niosremotesharepath=/home/nfstest/xyz/config/
niosremotesharefile=scuConfigFile_VMEDIA_VMEDIA_RHEL8_4
niosremotesharetype=scp
niosusername=root
niospassword=Jack123
niosscubootmedium=vmedia
niososbootmedium=vmedia
niostargetdisktype=physicaldisk
```

Log Collection

In the Log Collection section, provide the IP address and access details of the share where the installation logs will be saved.

The Log Collection section consists of the following parameters:

Table 16: Parameters in the Log Collection Section

Parameter	Description
`[section_name]`	Enter a name for the section.
`remshareip=`	The IP address of the share where the log file is generated during the installation.
`remsharepath=`	The location of the log file in the share. The log data generated during the installation is saved in this file. Enter the absolute path of the share.
`remsharefile=`	The file name to store SCU NI-OSI logs on the remote server. The default value is share_file.
`remsharetype=`	The protocol type used to access the share. The following protocols are supported: • SCP • SFTP

Parameter	Description

`remshareuser=`
 	
`remsharepassword=`
	The user credentials to access the share.

Example

```
[log_info]
remshareip=192.0.2.100
remsharepath=PATH
remsharefile=share_file
remsharetype=scp
remshareuser=user
remsharepassword=xxxx
```

OS

In the OS section, provide access details of the share where the config file is located. The config file contains the operating system details that are used in niscu.cfg. The OS section is for a single operating system only. If you want to install a different OS, repeat this section with the corresponding config file. See Modifying conf_file, on page 34 for information about config_file.

The OS section consists of the following parameters:

Table 17: Parameters in the OS Section

Parameter	Description
`[section_name]`	Enter a name for the section. The name provided here should be used as the value for the config_section parameter in the Target Server section.
`ip=`	The IP address of the share where the config file is located.
`path=`	The location of the config file in the share.
`file=`	The config file that contains the operating system details.
`username=`	The user credentials to access the share.
`password=`	
`protocol=`	The protocol used to access the share. The following protocols are supported: • SCP • SFTP • HTTP • TFTP

Example

```
[OS_iso]
ip=192.0.2.200
path=/var/www/html/huu
file=conf_file
username=root
password=Huudefault369
protocol=scp
```

Answer File

In the Answer File section, provide access details of the share where the answer file is located. The answer file contains details about custom OS deployment. This section is optional if you want to install an operating system with default settings (Quick installation).

Table 18: Parameters in the Answer File Section

Parameter	Description
`[section_name]`	Enter a name for the section. The name defined here should be used as the value in the "answerfile_section" parameter in the target server section.
`ip=`	The IP address of the share that contains the answer file.
`path=`	The location of the answer file in the share.
`file=`	The kickstart file. For custom installation, the kickstart file contains the required installation details.
`username=`	The user credentials to access the share.
`password=`	
`protocol=`	The protocol type used to mount the share. The following protocols are supported: • SCP • SFTP • HTTP • TFTP

Example

```
[OS_answerfile]
ip=192.0.2.254
path=/home/SCU/NI_SCU/Files/
file=esxi_ks.cfg
username=root
password=root@123
protocol=scp
```

Target System

In this section, provide details about the target server where the operating system is being installed. This section also contains details about the config file and answer file that are passed to the niscu.cfg file. For deploying operating systems in multiple servers, repeat this section with the details of target server, config file, and answer file.

Table 19: Parameters in the Target System Section

Parameter	Description
`[section_name]`	When naming this section, use this format: `cimc`, followed by an underscore (_), and a number. The number defines the target server instance.
`address=`	The IP address of the target server where the OS is being installed.
`user=`	The user credentials to access the target server.
`password=`	
`imagefile=`	The SCU image file name.
`config_section=`	The name given for the OS section should be provided here. For example, if the OS section name is "rhel_iso", then provide that name here.
`servernode=`	Select the node where you want to install the OS. This option is applicable for only C3260 and S3260 M4 servers. Enter 1 to select node 1. Enter 2 to select node 2. Enter 'all' to select both the nodes.
`[answerfile]`	The name given for the Answer File section should be provided here. For example, if the Answer File section is "OS_answerfile", then provide that name here. This is an optional parameter. The Answer file section is required only for custom installation.

Example

```
[cimc_1]
address=192.0.2.10
user=admin
password=Cisucs891
imagefile=ucs-cxxx-scu-5.0.0.39.iso
config_section=OS_iso
servernode=1
answerfile_section=OS_answerfile

[cimc_2]
address=192.0.2.20
user=admin
```

```
password=Ciscoucs345
imagefile=ucs-cxxx-scu-5.0.0.39.iso
config_section=OS_iso
servernode=2
answerfile_section=OS_answerfile
```

Modifying conf_file

The `conf_file` contains details about the operating system being deployed on the target server. The `conf_file` includes the following parameters:

Table 20: Parameters in conf_file

Parameter	Description
`shareMapType:`	The share type. The following share types are supported: • NFS • CIFS • WWW (HTTP and HTTPS)
`shareIP:`	The IP address of the share where the OS ISO file is saved.
`sharePath:`	The location of the OS ISO file.
`sharefile:`	The name of the OS ISO file.
`username:`	The user credentials to access the share. Enter the user name and password.
`password:`	
`osName:`	The operating system format. See Modifying conf_file for the operating system formats.

Parameter	Description
`osDrive:`	The drive where the operating system is installed. For example, `sdd` and `sde` might represent the first and second VDs. However, the enumeration of disks depends on the number of JBODs and VDs configured. Suppose a single JBOD has been configured. Then the JBOD is enumerated first and `sde` and `sdf` represent the first and second VDs. • DriveSerialNumber: Z1W4PB480000R610JQWP #Serial Number of the drive connected to LSI/Noe-Valley RAID controller or NVMe disk, on which OS has to be installed. • StorageControllerSlotID: MRAID #Controller Slot ID. This will be ignored, if DriveSerialNumber is present. VirtualDriveNumber: 0 #VD Number of the drive on which OS has to be installed. For LSI/Noe-Valley RAID controllers, VirtualDriveNumber should be specified along with StorageControllerSlotID. • VirtualDriveName: Hypervisor #VD Name on which OS has to be installed. Applicable only for SD Card Drives. **Note** The above options are exclusive. You can provide any one of the above.
`Edition:`	Windows parameter only. This parameter is applicable for both custom and quick installation of Windows. The following editions are supported: • STANDARD • DATACENTER • STANDARDCORE • DATACENTERCORE

Example

```
shareMapType:www
shareIp:192.0.2.100
sharePath:/huu
shareFile:VMware-VMvisor-Installer-5-5-0_update03-3116895_x86_64.iso
userName:root
password:HuuWelcome123
```

```
osName:esxi5u5x64
osDrive:/dev/sde
Edition:STANDARD
MediaType:Local
Interface:eth0
BootProto:static
IP:192.0.2.254
Subnet:255.255.255.0
Gateway:192.0.2.100
DNS:192.0.2.100
```

The following table lists a few examples of operating system formats.

Table 21: Operating System Formats

Operating System	Version	Format

Rocky Linux	Rocky Linux 8 Update 6
	Rocky Linux 8 Update 7
	Rocky Linux 9 Update 1
		`rocky8u6x64`
		`rocky8u7x64`
		`rocky9u1x64`

Oracle Linux	Oracle Linux 7 Update 9
	Oracle Linux 8 Update 6
	Oracle Linux 9
		`oracle7u9x64`
		`oracle8u6x64`
		`oracle9u0x64`

RHEL	RHEL 8.0 RHEL 8.4	`rhel8ux64` `rhel8u4x64`
SLES	SLES 15 SP3 SLES 15.0	`sles15sp3x64` `sles15x64`
Ubuntu	Ubuntu 20.4.2	`ubuntu20042x64`
Esxi	Esxi 7.0U3 Esxi 6.7.3	`esxi7u03x64` `esxi6u73x64`
Windows	Windows Server 2019 and 2022	`w2k19x64` `w2k22x64`

Running the Python Script to Start OS Deployment

Procedure

	Command or Action	Purpose
Step 1	Install the following components on the Linux client system from where you want to run the Python script:	• Python 2.7.x for 4.1.1 and below • Python 3.x for 4.2.1 and above • Open SSL Version 1.0.1e-fips or later

	Command or Action	Purpose
Step 2	On the Linux client system, run the following command:	**python os_install-4.2.yc.yyyymmddab.py -c niscu.cfg** Here, `os_install-4.2.yc.yyyymmddab.py` is the Python script, and `niscu.cfg` is the configuration file that contains information about the SCU ISO image and the OS details. When the Python script is executed, the target server boots to the SCU ISO. After SCU boots, it mounts the OS ISO image that is mapped in the configuration file. SCU then installs the operating system on the target server.

Installing Operating Systems Using Commands

Use the following options to install an operating system on a single server:

Table 22: Options to Install OS on a Single Server

Option	Description
`-a a.b.c.d, --address=a.b.c.d`	The IP address of the target server.
`-u USERNAME, --user=USERNAME`	The admin user credentials to access the target server.
`-p PASSWORD, --password=PASSWORD`	
`-m scu.iso, --imagefile=scu.iso`	The name of the SCU ISO file.
`-i a.b.c.d, --isoshareip=a.b.c.d`	The IP address of the remote share where the SCU ISO image is located.
`-d /data/image, --isosharepath=/data/image`	The location of the ISO file in the share.
`-t cifs/nfs/www, --isosharetype=cifs/nfs/www`	The type of remote share. The following share types are supported: • CIFS • NFS • WWW (HTTP or HTTPS)
`-r ISOSHAREUSER, --isoshareuser=ISOSHAREUSER`	The admin user credentials to access the share where the SCU ISO image is located.
`-w ISOSHAREPASSWORD, --isosharepassword=ISOSHAREPASSWORD`	

Option	Description
`-o BOOTMEDIUM, --bootMedium=BOOTMEDIUM`	The boot medium used to update. The following share types are supported: • vmedia • microsd • flexmmc
`-q TIMEOUT, --timeout=TIMEOUT`	NISCU OS Installation timeout
`-M ISOMOUNTOPTION, --isomountoption=ISOMOUNTOPTION`	Use mount option in case of CIFS share to specify the security option.
`-I a.b.c.d, --remshareip=a.b.c.d`	The IP address of the remote share where the snapshot results will be saved.
`-D /data/image, --remsharepath=/data/image`	The directory to store snapshot results in the share.
`-F REMOTESHAREFILE, --remoteShareFile=REMOTESHAREFILE`	The name of the share file.
`-T scp/sftp, --remsharetype=scp/sftp`	The type of share. The following protocols are supported: • SCP • SFTP
`-U REMSHAREUSER, --remshareuser=REMSHAREUSER`	The user credentials to access the share to save snapshot results.
`-W REMSHAREPASSWORD, --remsharepassword=REMSHAREPASSWORD`	
`-x CONFIGSHAREIP, --configShareIp=CONFIGSHAREIP`	The IP address of the remote share where the config file is located.
`-y CONFIGSHAREPATH, --configSharePath=CONFIGSHAREPATH`	The path to the location of the config file in the share.
`-z CONFIGSHAREFILE, --configShareFile=CONFIGSHAREFILE`	The name of the config file.
`-j CONFIGSHARETYPE, --configShareType=CONFIGSHARETYPE`	The type of share.
`-b CONFIGSHAREUSERNAME, --configShareUsername=CONFIGSHAREUSERNAME`	The user credentials to access the share where the config file is located.
`-e CONFIGSHAREPASSWORD, --configSharePassword=CONFIGSHAREPASSWORD`	

Option	Description
-X ANSWERFILESHAREIP, --answerFileShareIp=ANSWERFILESHAREIP	The IP address of the share where the answer file is located.
-Y ANSWERFILESHAREPATH, --answerFileSharePath=ANSWERFILESHAREPATH	The path to the location of the answer file in the share.
-Z ANSWERFILESHAREFILE, --answerFileShareFile=ANSWERFILESHAREFILE	The name of the answer file.
-J ANSWERFILESHARETYPE, --answerFileShareType=ANSWERFILESHARETYPE	The type of share.
-B ANSWERFILEUSERNAME, --answerFileUsername=ANSWERFILEUSERNAME	The user credentials to access the share where the answer file is located.
-E ANSWERFILEPASSWORD, --answerFilePassword=ANSWERFILEPASSWORD	
-N SERVERNODE, --serverNode=SERVERNODE	Select the node where you want to install the OS. This options is applicable for only C3260 and S3260 M4 servers. Type 1 to select node 1. Type 2 to select node 2. Type ALL to select both the nodes.
-f LOGFILE, --logrecordfile=LOGFILE	The name of the log file that contains the log data.

Table 23: CLI Options for NIOS_Install Section

Option	Description
-A NIOSREMOTESHAREIP, --niosremoteshareip=NIOSREMOTESHAREIP	IP address of remote share for non-interactive OS install
-G NIOSREMOTESHAREPATH, --niosremotesharepath=NIOSREMOTESHAREPATH	Path in remote share for non-interactive OS install
-H NIOSREMOTESHAREFILE, --niosremotesharefile=NIOSREMOTESHAREFILE	Filename in remote share for non-interactive OS install
-K NIOSREMOTESHARETYPE, --niosremotesharetype=NIOSREMOTESHARETYPE	Remote share type for non-interactive OS install
-L NIOSUSERNAME, --niosusername=NIOSUSERNAME	Username of the Cisco IMC admin user
-O NIOSPASSWORD, --niospassword=NIOSPASSWORD	Password of the Cisco IMC admin user
-P NIOSSCUBOOTMEDIUM, --niosscubootmedium=NIOSSCUBOOTMEDIUM	Boot medium for non-interactive OS install
-Q NIOSOSBOOTMEDIUM, --niososbootmedium=NIOSOSBOOTMEDIUM	OS medium for non-interactive OS install

Option	Description
-R NIOSTARGETDISKTYPE, --niostargetdisktype=NIOSTARGETDISKTYPE	Target Disk type for non-interactive OS install

Example

Example 1: Options for Quick Installation

In this example, the command options help in quick installation of Windows on 198.51.100.10. The SCU ISO image is located in 198.51.100.100. The conf_file is placed in 198.51.100.100. The OS installation log files are saved in 198.51.100.254. The NI-SCU script log files are saved in the same client system where the script is executed.

```
python3 os_install.py -a 198.51.100.10 -u user1 -p passwd
-m ucs-cxxx-scu-6.2.xx.iso -o vmedia -i 198.51.100.100
-d /utils_share/scu/kb -t nfs -r user2 -w passwd1 -I 198.51.100.100
-D /niscu/new_TH2U
-F niscu_cli_remsharefile1 -T scp -U user3 -W passwd2 -x 198.51.100.254
-y /niscu/new_TH2U
-z conf_file -j sftp -b abcd -e passwd -f log_latest
```

Example 2: Options for Custom Installation

In this example, the command options help in custom installation of Windows on 198.51.100.10. The SCU ISO image is located in 198.51.100.100. The conf_file is placed in 198.51.100.100. The answer file required for custom installation is located in 198.51.100.110, and is named win_answer_file. The OS Installation log files are saved in 198.51.100.254. The NI-SCU script log files are saved in the same client system where the script is executed.

```
python3 os_install.py -a 198.51.100.10 -u user1 -p passwd
-m ucs-cxxx-scu-6.2.xx.iso -o vmedia -i 198.51.100.100
-d /utils_share/scu/kb -t nfs -r user2 -w passwd1 -q 120 -I 198.51.100.100
-D /niscu/new_TH2U
-F niscu_cli_remsharefile1 -T scp -U user3 -W passwd2 -x 198.51.100.254
-y /niscu/new_TH2U
-z conf_file -j sftp -b abcd -e passwd -X 198.51.100.254
-Y /niscu/answer_files
-Z rhel.cfg -J sftp -B user4 -E passwd-f log_latest
```

Sample nwboot.cfg file

Sample `nwboot.cfg` file

```
{
    "Update_Timeout": 240,
    "SCURepository": {
        "BootMedium": {
            "VMEDIA": {
                "ImageRepository": "10.10.10.1/home/nfsshare/iso/scu.iso",
                "TransferProtocol": "nfs",
                "Username": "root",
                "Password": "password",
                "MountOptions": ""
            },
            "HTTP": {
```

```
                    "ImageRepository": "http://10.10.10.1:80/iso/scu.iso",
                    "MACAddress": "70:df:2f:86:af:02",
                    "PCIeSlot": "L",
                    "PhysicalPortNumber": 1,
                    "IPv4Address": {
                        "AddressOrigin": "Static",
                        "Address": "10.104.255.179",
                        "Gateway": "10.104.255.129",
                        "SubnetMask": "255.255.255.128",
                        "StaticNameServer": "64.104.76.247"
                    },
                    "IPv6Address": {
                        "AddressOrigin": "DHCPv6",
                        "Address": "fc00:1234::a:b:c:d",
                        "PrefixLength": 64,
                        "Gateway": "fe80::fe15:b4ff:fe97:90cd",
                        "StaticNameServer": "fe80::fe15:b4ff:fe97:90cd"
                    }
                },
                "FLEXMMC": {
                    "ImageRepository": "scu.iso"
                },
                "MICROSD": {},
                "PXE": {
                    "ImageRepository": "ftp://10.104.255.224/pub/scu",
                    "MACAddress": "70:df:2f:86:af:02",
                    "PCIeSlot": "L",
                    "PhysicalPortNumber": 1,
                    "IPv4Address": {
                        "AddressOrigin": "DHCP"
                    }
                },
                "IPXE": {
                    "ImageRepository": "http://10.10.10.1/iso/scu.iso",
                    "MACAddress": "70:df:2f:86:af:02",
                    "PCIeSlot": "L",
                    "PhysicalPortNumber": 1
                }
            }

        },
        "OSDetails": {
            "OSRepository": {
                "MediaType": "Local",
                "BootMedium": {
                    "VMEDIA": {
                        "ImageRepository":
    "10.10.10.1/home/nfsshare/iso/rhel/RHEL-8.5.0-20211013.2-x86_64-dvd1.iso",
                        "TransferProtocol": "nfs",
                        "Username": "root",
                        "Password": "password",
                        "MountOptions": ""
                    }
                }
            },
            "TargetOS": {
                "OSName": "rhel8u5x64",
                "OSEdition": "None"
            }
        },
        "TargetDisk": {
            "PHYSICALDISK": {
                "DriveSerialNumber": "06VSGVVB"
            },
```

```
        "VIRTUALDISK": {
            "StorageControllerSlotID": "MRAID",
            "VirtualDriveNumber": 0
        },
        "DISKNAME": {
            "OSDrive": "/dev/sdk"
        },
        "VIRTUALDRIVENAME": {
            "VirtualDriveName": "Hypervisor"
        },
        "ONBOARDSATAM2SSD": {
            "SATAM2SSD": "slot1"
        },
        "M2SWVDNAME": {
            "M2SWRAIDName": "RAID0"
        },
        "FC": {
            "HostWWPN": "10:00:54:88:DE:A7:32:6F",
            "TargetWWPN": "50:06:01:68:3E:A0:62:22",
            "Lun": 200
        },
        "ISCSI": {
            "MACAddress": "70:DF:2F:86:AE:FD",
            "PrimaryTargetName":
"iqn.2001-05.com.equallogic:0-af1ff6-082b3ebe6-cf2005780845d665-iqn.siva-25.com",
            "PrimaryLUN": 1
        }
    },
    "RemoteLog": {
        "ImageRepository": "10.10.10.10/home/nfstest/scu.log",
        "TransferProtocol": "scp",
        "Username": "root",
        "Password": "john123"
    },
    "AnswerFile": {
        "ImageRepository": "10.10.10.10/home/nfstest/answerfile",
        "TransferProtocol": "scp",
        "Username": "root",
        "Password": "john123"
    }
}
```

Sample conf_file and niscu.cfg files

Sample `conf` file

```
shareMapType:www
shareIp:10.10.10.10
sharePath:/path/to/iso
shareFile:rhel66.iso
userName:www
password:www
osName:rhel6u6x64
osDrive:/dev/sdk

DriveSerialNumber:Z1W4AC480000Z610ABCD

StorageControllerSlotID:MRAID

VirtualDriveNumber:0
```

```
VirtualDriveName:Hypervisor
SATAM2SSD:slot1
M2SWRAIDName:RAID00
Edition:STANDARD
```

Sample `niscu.cfg` file

```
#
# This file is just a template file and suggest user not to use this file directly without
 deleting comments and other info
#
# User has to create their own config file instead of using this.
#
#
[defaults]
use_http_secure=yes
update_timeout=120

[scu_iso]
isoshareip=10.10.10.10
isosharepath=/path/to/file
imagefile=ucs-cxx-scu.iso
isosharetype=www
isoshareuser=root
isosharepassword=password
mountoption=noauto   # Multiple mount options shall be passed as a comma separated list.
Example - nolock,rw
bootmedium=vmedia    # Value shall be vmedia - to boot from vmedia  or flexmmc- to boot
from eMMC or microsd - to boot from microsd

#################  Section to store SCU NI-OSI logs on Remote Server ##########################

[output_location]
remshareip=10.10.10.10
remsharepath=/path/to/file
remsharefile=share_file
remsharetype=scp/sftp
remshareuser=root
remsharepassword=password

###############Section for one server starts here#############

[rhel_iso]
ip=10.10.10.10
path=/path/to/conf_file
file=conf_file
username=root
password=password
protocol=scp  # supports scp, sftp, tftp and www

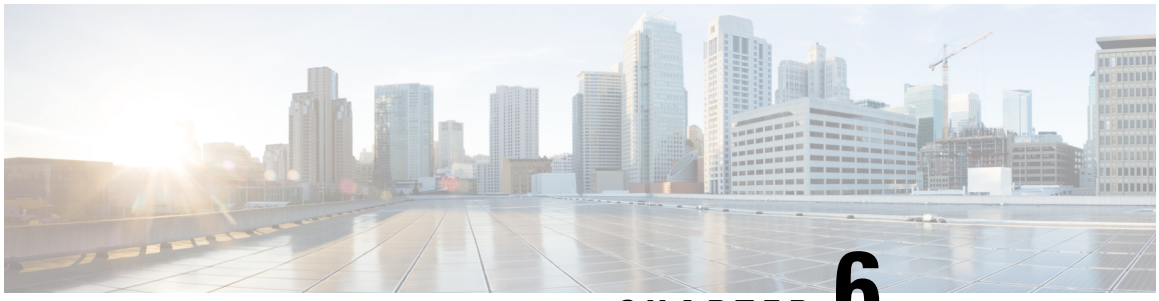
[rhel_answerfile]
ip=10.10.10.10
path=/path/to/answer_file
file=rhel66_custom.ks#Keep this field blank for quick install else give name of kickstart
file to perform Custom install for RHEL,CENT, SLES, Ubuntu
username=root
password=password
protocol=scp # supports scp, sftp, tftp and www

######## Section for Network Boot Support starts here ##########
[nios_install]
niosremoteshareip=10.10.10.10
niosremotesharepath=/home/nfstest/config #config templete file path for scu boot from network
 location
```

```
niosremotesharefile=nwboot.cfg #config template file for scu boot from network location
niosremotesharetype=scp
niosusername=root
niospassword=Ucsrack4All
niosscubootmedium=pxe #type of the boot pxe/http/ipxe
niososbootmedium=vmedia #currently only vmedia is supported
niostargetdisktype=physicaldisk #target disk details

[cimc_1]
address=10.10.10.10
user=admin
password=password
imagefile=ucs-cxx-scu.iso
config_section=rhel_iso
answerfile_section=rhel_answerfile #Mandatory for Custom Install for RHEL,CENT, SLES and
Ubuntu. Remove this line, to perform Quick install.
nios_section=nios_install #nios_install section, if this section is present then it takes
the priority over scu_iso section.
servernode=1/2/all # For Colusa2 .

#servernode option to be passed only in case of colusa2 For other server dont specify this
 option
###############Section for one server ends here#################
################################################################
##### To trigger os installation for multiple servers simply repeate above section with
details for other server
##### and OS, also define separate conf_file for other server
################################################################################
```



CHAPTER 6

Configuring RAID Levels

- RAID Configuration, on page 45
- Storage Configuration, on page 45
- Creating RAID Arrays, on page 47

RAID Configuration

You can use the RAID Configuration functionality to configure the on-board or PCIe supported RAID controller cards.

If your system has multiple RAID controllers, UCS-SCU displays a list of all available RAID cards, and physical and logical disks on the RAID Configuration page.

The following RAID configuration options are available:

- Single RAID levels—RAID 0, RAID 1, RAID 5 and RAID 6
- Nested RAID levels—RAID 10, RAID 50 and RAID 60

Storage Configuration

RAID Configuration page contains the following components:

Table 24: RAID Configuration Page

Component	Description
Physical Disks Area	Contains the list of physical disk available in the server in table format. See Physical Disks Area, on page 46.
Logical Disks Area	Contains the list of virtual disk available in the server in table format. See Logical Disks Area, on page 47.
Create RAID button	You can use this feature to create new RAIDs. See Configuring Single-Level RAID, on page 47 and Configuring Nested RAID, on page 48.

Component	Description
Delete RAID button	You can use this feature to delete an existing RAID. To delete an existing RAID, select it from the **Logical Disks** area and click **Delete**.
Refresh button	You can use this feature to refresh the RAID list.

Physical Disks Area

The Physical Disks table in the RAID Configuration page lists the following:

Table 25: Physical Disks

Column	Description
Enc ID	The identifying number of the physical disk.
Slot ID	The slot in which the physical disk belongs.
Device Node	The devide node in which the physical disk belongs.
Size (MB)	The size of the physical disk.
Serial No	The status of the disk. For more information see .
State	The status of the disk. For more information, see Table 26: Disk State Condition, on page 46.
Block Size	The block size of the physical disk.
Type	Type of physical disk.

Table 26: Disk State Condition

Status	Description
Online	The drive is already used in another array.
Global Hotspare	The drive will be used to repair any array in the system that had a drive failure, if the failed drive is equal to, or smaller than the hot spare drive.
Un-configured Good	The drive is unused or available.
Ready	The drive is online and operating correctly.
Offline	The drive is offline or absent. No actions can be performed on the drive until it is back online.
Un-configured Bad	The drive is not operational and needs to be replaced. Disks with a status of "Unconfigured bad" cannot be used for RAID configurations.

Status	Description
Foreign	The drive is part of an array created on a different controller, or created within one enclosure and moved to another on the same controller. It can be used to create a new array after clearing the configuration.

Logical Disks Area

The Logical Disks table in the RAID Configuration page lists the following:

Table 27: Logical Disks

Column	Description
Select check box	**Select** check box is used to select one or more disk.
VD No	The identifying number of the VD.
Name	Name of the VD.
Device Node	The device node in which the VD belongs.
Size (MB)	Logical drive size. The maximum value depends on RAID level selected and the physical disks size involved.
RAID Level	RAID 0 (Data striping), 1 (Disk Mirroring), 5 (Data Striping with Striped Parity), 6 (Distributed Parity and Disk Striping).
RAID PDs	Physical disk to which the VDs belong.

Creating RAID Arrays

Configuring Single-Level RAID

Step 1 Select **Server Configuration** > **Storage Configuration** from the navigation pane

The **RAID Configuration** window is displayed.

Step 2 Click **Create RAID**.

The **Configure RAID** page is displayed.

Step 3 From the **RAID** drop-down list, select a RAID level (0 or 1 or 5 or 6).

Step 4 From the Physical Disks list on the left side, select the physical disks that you want to include in the Drive Groups list.

Table 28: Minimum Number of Required Physical Drives

RAID Level	Number of Physical Disks Required
RAID 0	1
RAID 1	2
RAID 5	3
RAID 6	4

Step 5 Enter the following information:

Field	Description
Name field	Enter a name of the RAID.
Read Policy drop-down list	From the Read Policy list, choose a read policy for the RAID level.
Disk Cache Policy drop-down list	From the Disk Cache Policy list, choose a disk cache policy for the RAID level.
Stripe Size (KB) drop-down list	From the Stripe Size list, choose a stripe size for the RAID level.
Access Policy drop-down list	From the Access Policy list, choose an access policy for the RAID level.
Cache Policy drop-down list	From the Cache Policy list, choose a cache policy for the RAID level.
Write Policy drop-down list	From the Write Policy list, choose a write policy for the RAID level.
Size field and **Unit** drop-down list	In the Size text field, enter the size of the logical disk and from the unit drop-down list, select the unit.

Step 6 Click **OK**.

Note The Create Drive Group button remains disabled until the minimum number of physical disks for a RAID level is selected.

The selected physical disks are included in the Drive Groups list.

Configuring Nested RAID

Nested RAID levels have primary and secondary RAID levels. You should create a minimum of two drive groups in nested RAID levels and the drive groups should have the same number of physical disks.

Step 1 Select **Server Configuration** > **Storage Configuration** from the navigation pane

The **RAID Configuration** window is displayed.

Step 2 Click **Create RAID**.

The **Configure RAID** page is displayed.

Step 3 From the **RAID** drop-down list, select a nested RAID level (10 or 50 or 60).

Step 4 From the **Physical Disks** list, select the physical disks that you want to include in the Drive Groups list.

Table 29: Minimum Number of Required Physical Drives and Data Groups

RAID Level	Minimum Number of Physical Disks	Minimum Number of Data Groups
RAID 10	4	2
RAID 50	6	2
RAID 60	8	2

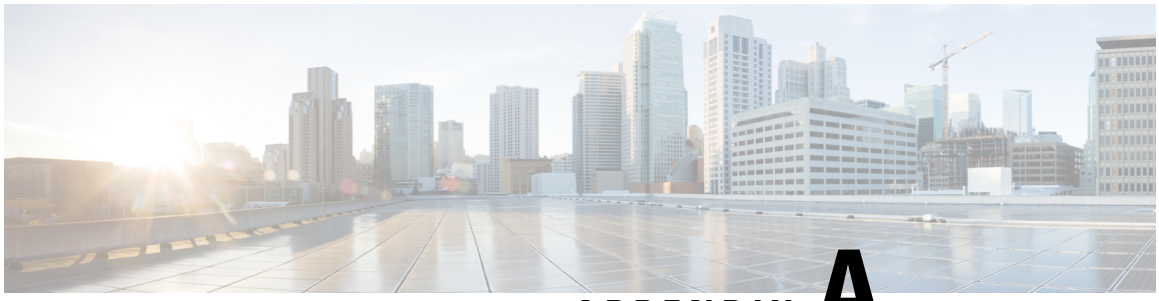
Step 5 Enter the following information:

Field	Description
Name field	Enter a name of the RAID.
Read Policy drop-down list	From the Read Policy list, choose a read policy for the RAID level.
Disk Cache Policy drop-down list	From the Disk Cache Policy list, choose a disk cache policy for the RAID level.
Stripe Size (KB) drop-down list	From the Stripe Size list, choose a stripe size for the RAID level.
Access Policy drop-down list	From the Access Policy list, choose an access policy for the RAID level.
Cache Policy drop-down list	From the Cache Policy list, choose a cache policy for the RAID level.
Write Policy drop-down list	From the Write Policy list, choose a write policy for the RAID level.
Size field and **Unit** drop-down list	In the Size text field, enter the size of the logical disk and from the unit drop-down list, select the unit.

Step 6 Click **OK**.

Note The Create Drive Group button remains disabled until the minimum number of physical disks for a RAID level is selected.

The selected physical disks are included in the Drive Groups list.



APPENDIX A

Common Procedures for OS Installation

- Selecting a Installation Disk, on page 51
- Network Settings, on page 51
- Selecting Installation Drivers, on page 52

Selecting a Installation Disk

In the **Installation Disk** area, do the following:

Select the radio button of the installation disk you wish to use.

Network Settings

Network Settings allows you to enter the network configuration settings for the onboard network adapters that are detected by the operating system during installation. These settings do not affect the network settings for the CMC. We recommend that you set different IP addresses for the operating system and CMC. The network interface column lists each network adapter detected by the UCS-SCU. Your operating system may have a different name for the interface after you install the operating system.

Note Only one of the active network should be configured, and this network interface becomes ESXi management network.

In the **Network Settings** area, do the following:

Step 1 Select the **IPv4 Settings** or **IPv6 Settings** tab.

These tabs display the link status of available network interfaces and the corresponding MAC address, Link Status, IP address, Subnet Mask, Gateway, and DNS.

Step 2 To edit the any of the network setting value, double-click the corresponding row and column.

This activates the field for editing.

Step 3 After editing the field, press **Enter**.

Selecting Installation Drivers

UCS-SCU displays all available drivers downloaded from the driver source. Deselect the drivers that you do not want to install. If you want to install an operating system on a RAID volume, select the driver for the appropriate RAID controller.

In the **Installation Drivers** area, do the following

Select the check box for the drivers that you want to install from the table.

Note Use the arrow keys to browse the list.