Cisco Prime Infrastructure 3.10 Appliance Hardware Installation Guide

First Published: 2021-09-24

Last Modified: 2023-04-07

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

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CONTENTS

CHAPTER 1

Installation and Initial Configuration

Overview

This guide provides the information on how to install the Cisco Prime Infrastructure Physical Appliances Gen2, Gen 3, and Digital Network Architecture Center (DNAC1 & DNAC2).

System Configuration

Table 1: System Configuration

Specification	Gen-2 Appliance	Gen-3 Appliance	DNAC Appliance	DNAC 2 Appliance
CPU	1 X 10 core processor (20 threads)	20C/40T	44 C/ 88 T	44 C/ 88 T
RAM	64 GB	64GB	256GB	256 GB
HDD	4 X 900 GB in RAID 10 configuration and 2.5inch drive	4 x 1.2 TB SSD - 900 GB	3.6 TB	2 x 480 GB in RAID 1 2 x 1.9 TB in RAID 1 6 x 1.9 TB in RAID 10
CIMC	Cisco UCS C-Series Integrated Management Controller	Cisco UCS C-Series Integrated Management Controller	Cisco UCS C-Series Integrated Management Controller	Cisco UCS C-Series Integrated Management Controller
NIC	Integrated dual-port Gigabit Ethernet	Integrated dual-port Gigabit Ethernet	Integrated dual-port Gigabit Ethernet	Integrated dual-port Gigabit Ethernet

For scaling information on this server see the *Scaling* Prime Infrastructure section in Cisco Prime Infrastructure Quick Start Guide.

Note When there is a flap time in hard appliance, ensure that the hardware clock (BIOS / CIMC) and the Network Time Protocol time are in sync.

Set the Appliance

This section describes how to set the Prime Infrastructure appliance.

Step 1 Attach a keyboard and monitor to the USB ports on the rear panel of the appliance or by using a KVM cable and connector to access the appliance console.

Step 2 Power on the appliance.

Step 3 To set up CIMC press F8 to enter the CIMC configuration utility and continue with Step 3 to Step 11. Continue with Step 12 in case you do not wish to configure CIMC.

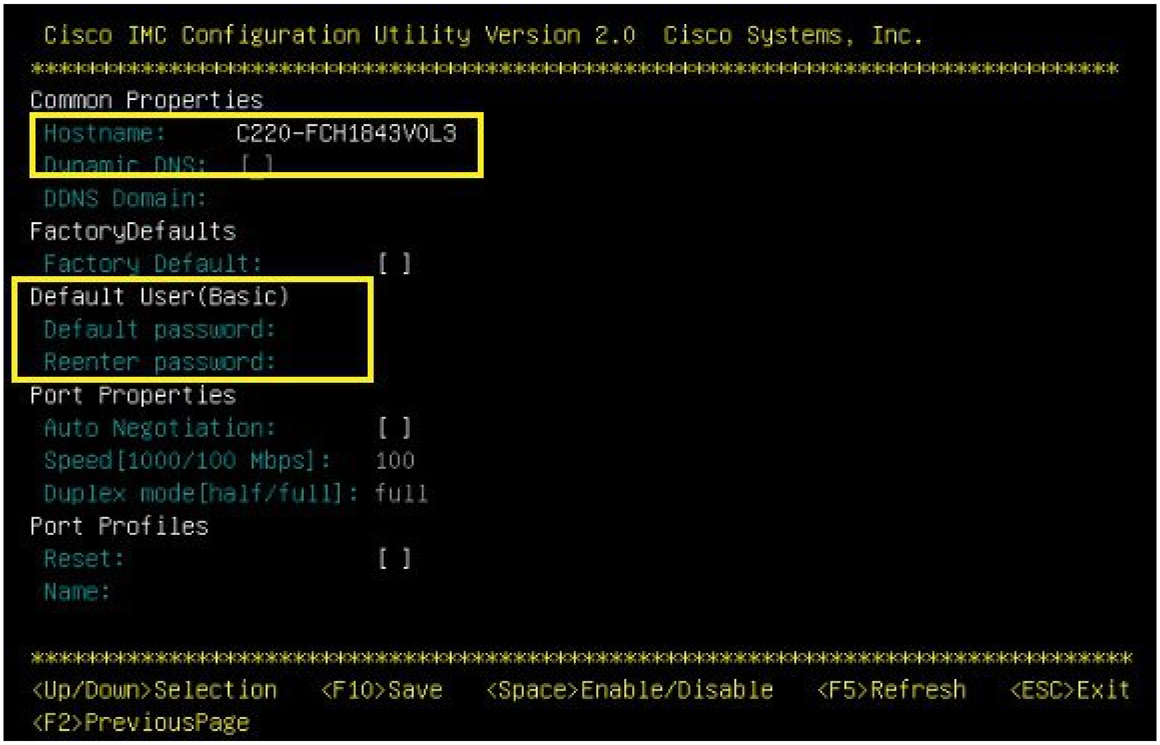
You might need to press the function keys (F8, F6 and F2) more than once until the system responds. If you do not press F8 quickly enough you may enter the EFI shell. Press Ctrl, Alt, Del to reboot the system and press F8 again.

Note The Cisco Integrated Management Controller (CIMC) is the management service that you use to remotely access, configure, administer, and monitor the Prime Infrastructure server.

Step 4 In the Configuration Utility window, change the following fields as specified:

- NIC mode—Select **Dedicated**.
- IP (Basic)—Select **IPV4**.
- DHCP—Disable DHCP if enabled.
- CIMC IP—Enter the IP address of the CIMC.
- Prefix/Subnet—Enter the subnet of the CIMC.
- Gateway—Enter the Gateway address.
- Pref DNS Server—Enter the preferred DNS server address.
- NIC Redundancy—Null

Step 5 Press **F1** to specify additional settings.



```
 Cisco IMC Configuration Utility Version 2.0  Cisco Systems, Inc.
*****************************************************************************
Common Properties
 Hostname:     C220-FCH1843V0L3
 Dynamic DNS:  [ ]
 DDNS Domain:
FactoryDefaults
 Factory Default:         [ ]
Default User(Basic)
 Default password:
 Reenter password:
Port Properties
 Auto Negotiation:        [ ]
 Speed[1000/100 Mbps]:    100
 Duplex mode[half/full]:  full
Port Profiles
 Reset:                   [ ]
 Name:

*****************************************************************************
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F2>PreviousPage
```

Step 6 Make the following changes on the Additional Settings window:

- Enter a hostname for CIMC.
- Turn off Dynamic DNS.
- Enter the admin password. If you leave the password field blank, the default password is **password**.

Step 7 Press **F10** to save the settings.

Step 8 Press escape to exit and reboot the server.

For remote management move to current step 7.

Step 9 After the settings are saved, open a browser and enter the following URL:

https://CIMC_ip_address where *CIMC_IP_address* is the IP address that you entered in Step 3 above.

Step 10 Log in to CIMC web interface using the following credentials:

- Username—admin
- Password—the password configured in Step 6

You will be prompted to reset the password if you did not change the default password in Step 6.

Improve Performance on Physical Appliances

For better performance on the Prime Infrastructure Physical Appliance Gen 2, Gen 3, and DNAC Appliance, make sure you configure the virtual drive Write Policy to Write Back Good BBU. To configure the virtual drive Write Policy, follow these steps:

Step 1 Launch the CIMC web interface.

Step 2 Click the **Storage** tab, click on the SAS Modular Controller name, click the **Virtual Drive Info** tab, select the **Virtual Drive** and then click **Edit Virtual Drive**.

Step 3 Click **OK** on the dialog box that appears.

Step 4 In the Write Policy field, select **Write Back Good BBU** fro the drop-down, then click **Save Changes**.

Migrate from Previous Releases of Cisco Prime Infrastructure

You can restore and back up only on Prime Infrastructure 3.10 from the following versions:

- PI 3.9.x Prime Data Migration Tool Update 02
- Cisco Prime Infrastructure 3.9.1
- Cisco Prime Infrastructure 3.9 Update 01
- Cisco Prime Infrastructure 3.9
- PI 3.8.x Prime Data Migration Tool Update 02
- PI 3.8.x Prime Data Migration Tool Hotfix
- Cisco Prime Infrastructure 3.8.1 Update 01
- Cisco Prime Infrastructure 3.8.1
- Cisco Prime Infrastructure 3.8 Update 02
- Cisco Prime Infrastructure 3.8
- PI 3.7.x Prime Data Migration Tool Update 02
- PI 3.7.x Prime Data Migration Tool
- Cisco Prime Infrastructure 3.7.1 Update 05
- Cisco Prime Infrastructure 3.7.1
- Cisco Prime Infrastructure 3.7 Update 03
- Cisco Prime Infrastructure 3.7

See the section *Before You Migrate Your Data* in the latest Cisco Prime Infrastructure Quick Start Guide before you restore your data from Prime Infrastructure 3.7.x, 3.8.x, or 3.9.x to your newly installed Prime Infrastructure 3.10 server.

CHAPTER 2

Install the ISO on the Application

Install the ISO on the Appliance

The appliance is shipped with the software version pre-installed. You do not have to perform these steps during the initial installation of the appliance. However in case you need to re-image the appliance, you can install the software from the ISO file.

To reduce the installation time, choose **Admin** > **Network** > **Network Settings** in the CIMC interface and check the **Auto Negotiation** check box.

Before You Begin

Download the ISO file PI-APL-3.10.0.0.205-1-K9.iso from cisco.com and verify file integrity using the checksum values listed for it on cisco.com.

You can verify the Cisco Signature for the ISO image with the following steps:

1. Download PI-APL-3.10.0.0.205-1-K9.iso, CiscoPI3.10.pem and PI-APL-3.10.0.0.205-1-K9.iso.signature.
2. Copy these file to any Linux server and enter the following command.

```
openssl dgst -sha512 -verify
CiscoPI3.10.pem -signature PI-APL-3.10.0.0.205-1-K9.iso.signature PI-APL-3.10.0.0.205-1-K9.iso
```

The result will be shown as “Verified”.

Note Ensure no storage devices are connected to the USB port of the appliance before upgrading or installing the ISO image. The installation fails if a USB storage device is connected to the USB port of the appliance as the installer selects the USB storage device.

Note When you connect Gen 2 and Gen 3 appliances through serial console connection after reboot, there are chances that you might encounter garbled screen display. To overcome this issue, you can connect through CIMC or VGA console.

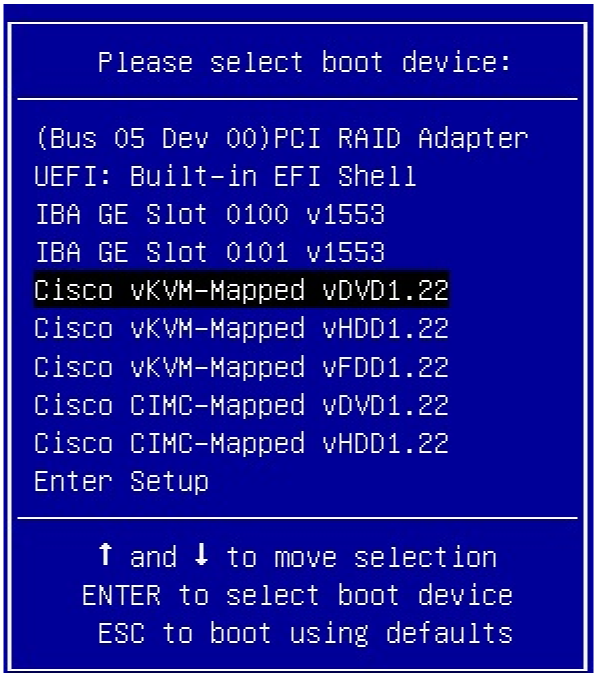
Step 1 Connect to the console using one of the options mentioned in Connect to the Console.

Step 2 Mount ISO using any one of the mounting options. See DVD Mount Options for more details.

Step 3 Reboot the appliance by pressing the power switch or select **Power** > **Reset System(Warm Boot)** if you are using vKVM to restart.

Step 4 After the appliance reboots, press **F6** to enter the boot option.

Step 5 Select one of the DVD mount option with the Cisco Prime Infrastructure 3.10 software image. See DVD Mount Options for more information.



```
    Please select boot device:

 (Bus 05 Dev 00)PCI RAID Adapter
 UEFI: Built-in EFI Shell
 IBA GE Slot 0100 v1553
 IBA GE Slot 0101 v1553
 Cisco vKVM-Mapped vDVD1.22
 Cisco vKVM-Mapped vHDD1.22
 Cisco vKVM-Mapped vFDD1.22
 Cisco CIMC-Mapped vDVD1.22
 Cisco CIMC-Mapped vHDD1.22
 Enter Setup

    ↑ and ↓ to move selection
   ENTER to select boot device
    ESC to boot using defaults
```

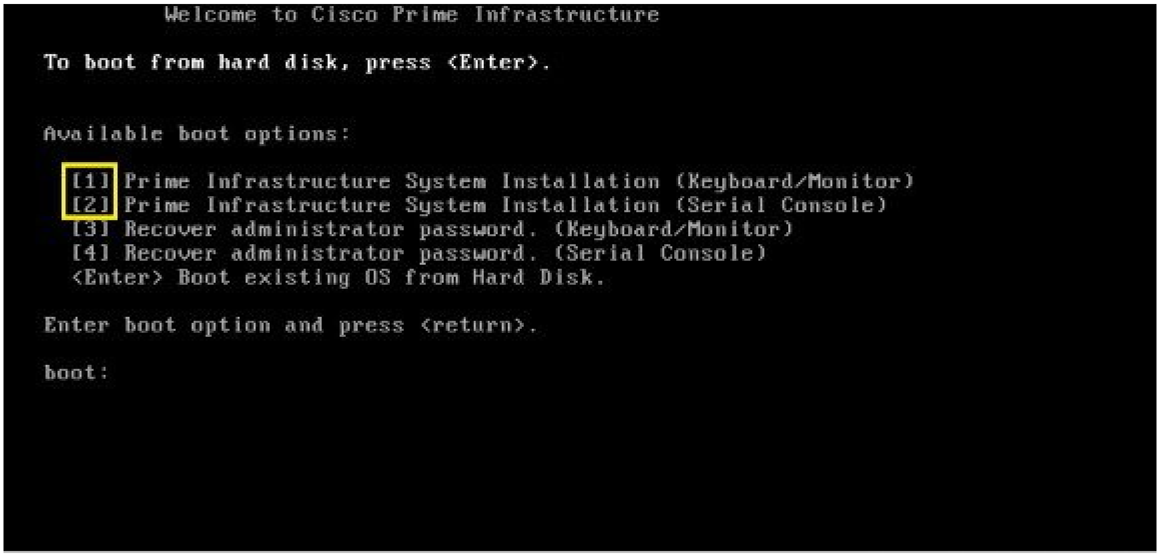
Step 6 From the available boot options, enter **1** or **2** carefully, as all future management messages will be displayed in the selected display.

1—Prime Infrastructure System Installation (Keyboard/Monitor) if you are connected through the VGA port/vKVM (KVM Console).

All console data /information will appear on the VGA port /vKVM (KVM console).

2—Prime Infrastructure System Installation (Serial Console) if you are connected through the serial port or Serial Over Lan. See Connect to the Console Using Serial Over LAN for more information.

All console data/information will appear on the serial port or Serial Over Lan.



```
          Welcome to Cisco Prime Infrastructure

   To boot from hard disk, press <Enter>.

   Available boot options:

     [1] Prime Infrastructure System Installation (Keyboard/Monitor)
     [2] Prime Infrastructure System Installation (Serial Console)
     [3] Recover administrator password. (Keyboard/Monitor)
     [4] Recover administrator password. (Serial Console)
     <Enter> Boot existing OS from Hard Disk.

   Enter boot option and press <return>.

   boot:
```

The time taken to deploy the image will depend on the network speed.

Step 7 Enter **setup** at the login prompt when prompted to initiate the installation.

What to do next

See *Set Up Prime Infrastructure on a Virtual Machine or Physical Appliance* section (Step 3 onwards) in Cisco Prime Infrastructure Quick Start Guide for more information about installing the software.

Note Cisco Prime Infrastructure is installed only using the 1 Gbps ports. To disable the 10 Gbps ports on Cisco DNA Center appliance and use the 1 Gbps ports to install Prime Infrastructure, perform the following steps.

1. Login to **CIMC Console**.
2. Navigate to **Compute** > **BIOS** > **Configure BIOS** > **Advanced** > **LOM and PCle Slots Configuration**.
3. Choose the **Disabled** option from the **PCIeSlot:MLOM OptionROM** and **PCIeSlot:MLOM LinkSpeed** drop-down lists.
4. Click the **Save** button.
5. Navigate to **Host Power**, Power Cycle the machine and then Power ON.

Note In order to Install Prime Infrastructure in DNAC2 Appliance, you need to Disable Virtual Drive option in Cisco FlexFlash link, perform the following steps:

1. Login to **CIMC Server IP** in browser.
2. Navigate to **Storage**, click **Cisco FlexFlash** link.
3. Click **Virtual Drive** tab and click the **Disable Virtual Drive** button.

Manage the Appliance Using CIMC

You can connect to the vKVM console by launching the CIMC and log in using your username and password configured in Set the Appliance. Using the vKVM console you can do the following:

- Remotely power on or off the server.
- Monitor the server and disk status.
- Change the BIOS settings. Following table displays the hardware types and their respective latest firmware and BIOS versions that support the Cisco Prime Infrastructure 3.10 Physical Appliance ISO image:

Hardware Type	Firmware Version	BIOS Version	PID
Gen 2	412(b)	C220M4.4.1.2b.0.0625202204	PI-UCS-APL-K9
Gen 3	413(f)	C220M5.4.1.3k.0.0117220614	PI-UCSM5-APL-U-K9
Gen 3	413(f)	C220M5.4.1.3k.0.0117220614	PI-UCSM5-APL-K9
DNAC	412(b)	C220M4.4.1.2b.0.0625202204	DN1-HW-APL
DNAC2	412(b)	C220M5.4.1.2b.0.0917201934	DN2-HW-APL

- Launch a virtual console on the appliance.
- Mount *iso* files as virtual DVD drives.
- See Cisco Integrated Management Controller documentation for more information.

CHAPTER 3

Additional Functions

Connect to the Console

You can physically connect to the console on the server using the VGA port or the serial port on the server.

The baud rate should be 9600 while connecting to the console using the serial port. See Set the Baud Rate, on page 12.

You can also connect to the console remotely using the following options:

- Serial over LAN
- Using vKVM

Connect to the Console Using Serial Over LAN

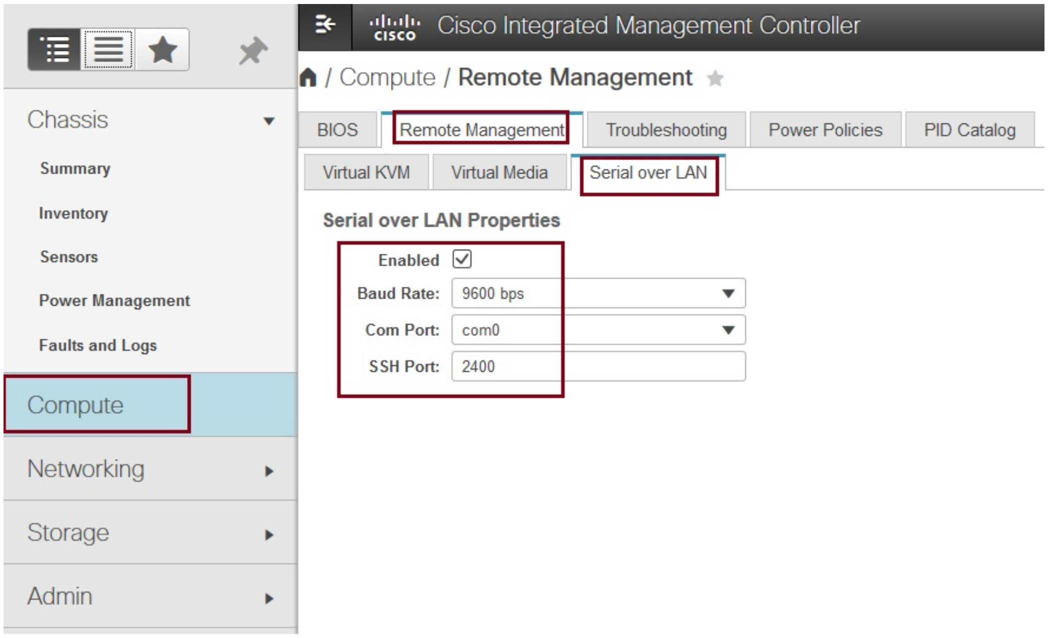
You can use a terminal server to connect to the serial port of the appliance or use Serial over Lan (SOL) to connect to the serial console over the network.

To enable Serial over LAN (SOL):

Step 1 Launch CIMC and log in using your username and password configured in Set the Appliance, on page 2.

Step 2 Select **Compute** > **Remote Management** > **Serial Over LAN.**

Step 3 Check the check box **Enabled.**



Serial over LAN Properties

Enabled ☑

Baud Rate: 9600 bps

Com Port: com0

SSH Port: 2400

Step 4 Connect to CIMC using SSH.

Step 5 Enter these commands in the following sequence:

- **scope sol**
- **show**

Serial over LAN must be enabled. If it is not enabled, use the user interface to enable it.

- **connect host**

Step 6 Launch Cisco Integrated Management Controller server using SSH .

```
# ssh admin@(server IP)
Enter the admin password
```

Step 7 Map the ISO image.

```
# scope vmedia
# map-www <VOLUME NAME> <http-location> <PI_ISO_FILE>
where - <http-location> is http location of iso image

Press Enter
# Server Username:<username>
# Server Password:<password>
# Confirm Password:<renter the password>
        # show mappings
        Volume          Map-Status       Drive-Type         Remote-Share               Remote-File
           Mount-Type
       ------------- ------------------   ----------    -------------------------
------------------------  -------------
        vol1                 OK              CD          http://nmtgre-sjc.cis...
PI-APL-3.10.0.0.205-SNA...     www

# exit
```

Step 8 Reboot the server:

```
# scope chasis
# power off
 This operation will change the server's power state.
 Do you want to continue?[y|N]y
#
#
# power on
  This operation will change the server's power state.
  Do you want to continue?[y|N]y
# exit
```

Step 9 Connect to Serial Over Lan Console.

```
# scope sol
# show detail
Serial Over LAN:
 Enabled: yes
 Baud Rate(bps): 9600
 Com Port: com0
# set enabled yes
# set baud-rate 9600
# commit

# connect host // to connect sol cosole
```

Step 10 The machine reboots and prompts to enter F6 for boot option. Press the function-key **F6**.

You may need to press F6 multiple times to see **Enter boot selection menu...** in the screen. You must wait for a few minutes to get the boot device option.

Step 11 Select the desired DVD mount option and in this case, you must select **Cisco CIMC-Mapped vDVD1.22**.

Step 12 From the available boot options, enter option 1.

Step 13 Enter setup at the login prompt when prompted to initiate the installation.

Step 14 Close Network Connection to Exit.

Connect to the vKVM Console

Step 1 Launch CIMC and log in using your username and password configured in Set the Appliance, on page 2.

Step 2 Choose **Chassis** > **Summary**.

Step 3 Click **Launch KVM** link and select **Java based KVM or HTML based KVM** to open KVM Console .

The Security Warning dialogue box opens.

Step 4 Click **Continue**.

The vKVM console is downloaded and the credentials are verified.

Step 5 Click **Run** to install the KVM console.

Set the Baud Rate

Step 1 Launch CIMC.

Step 2 Select **Compute** > **BIOS** .

Step 3 Click **Configure BIOS.**

The **Configure BIOS Parameter** dialog box opens.

Step 4 Click **Advanced** Tab

Step 5 Expand **Serial Configuration**.

Step 6 Select 9600 from the **Bits Second field** drop-down list.

Step 7 Click **Save**.

DVD Mount Options

To re-image the appliance from an *iso* file the DVD mount options available are:

The following DVD mounting options are available:

- Physical DVD Mount

  Burn the *iso* file to a DVD and mount it through a physical DVD drive connected to the USB port of the appliance. A physical DVD mount is used when CIMC remote management is not configured. This is the fastest option.

- CIMC mapped vMedia

- The *iso* file is on the HTTPS, CIFS or NFS server and the speed depends on the Prime Infrastructure Server and File-Server bandwidth. The client server must remain connected till the installation is completed. This is the preferred mode for mounting the *iso* file.

- vKVM DVD mount

- The *iso* file can also be mounted using a virtual console. The *iso* file is on client machine and the speed depends on server appliance bandwidth.

Mount vKVM DVD

The virtual KVM console (vKVM) is an interface accessible from CIMC that emulates a direct keyboard, video, and mouse connection to the server.

To mount an *iso* file from the desktop client using the vKVM DVD mount:

Step 1 Connect to the vKVM console. See Connect to the vKVM Console for more details.

Step 2 Click **Continue** in the **Warning-Security** dialog box to launch the v**KVM Console**.

Step 3 Select **Virtual Media > Activate Virtual Devices**.

The **Uncrypted Virtual Media Session** dialogue box opens.

Step 4 Select the radio button **Accept this session**.

Step 5 Click **Apply**.

The Virtual Device is activated.

Step 6 Select **Virtual Media > Map CD/DVD** and browse to the Prime Infrastructure 3.10 ISO image on your computer.

After mounting the vKVM DVD continue with Installing the ISO on the Appliance

Step 7 Click **Map Device** to mount the ISO image.

Mount a CIMC vMedia DVD

To mount an iso file from CIFS, NFS, HTTP server as a virtual DVD drive on the appliance:

Step 1 Launch CIMC and log in using your username and password configured in Set the Appliance.

Step 2 Select **Compute** > **Remote Management**.

Step 3 Click **Virtual Media** and expand **Cisco IMC-Mapped vMedia**.

Step 4 Click **Add New Mapping** under **Current Mappings**.

Step 5 Enter the following parameters:

- Volume
- Remote Share
- Remote File
- Mount Options
- User Name
- Password

Step 6 Click **Save**.

Password Recovery

You can recover (that is, reset) administrator passwords on Prime Infrastructure physical appliances. See *How to Recover Administrator Passwords on Physical Appliances* in the Cisco Prime Infrastructure Administrator Guide for more information.

How to Recover Administrator Passwords on Gen 3 Appliance

You can recover (reset) administrator passwords on Prime Infrastructure Gen 3 appliances.

Before You Begin

Ensure that you have an current version of ISO image

You can reset the password using:

- **Console:** CIMC Console (Other console options are KVM Console, VGA Console and Serial Console/Serial Over Lan-SOL)
- **DVD mount option:** KVM mapped DVD (Other mount options are CIMC mapped DVD and Physical External DVD)

To recover the password using Serial Console/Serial Over Lan-SOL, follow these steps:

Step 1 Launch Cisco Integrated Management Controller server using SSH .

```
# ssh admin@(server IP)
Enter the admin password
```

Step 2 Map the ISO image.

```
# scope vmedia
# map-www <VOLUME NAME> <http-location> <PI_ISO_FILE>
where - <http-location> is http location of iso image

Press Enter
# Server Username:<username>
# Server Password:<password>
# Confirm Password:<renter the password>
        # show mappings
        Volume          Map-Status       Drive-Type         Remote-Share               Remote-File
           Mount-Type
       ------------- ------------------   ----------    -------------------------
------------------------  -------------
        vol1                 OK              CD          http://nmtgre-sjc.cis...
PI-APL-3.10.0.0.205-SNA...     www

# exit
```

Step 3 Reboot the server:

```
# scope chasis
# power off
 This operation will change the server's power state.
 Do you want to continue?[y|N]y
#
#
# power on
  This operation will change the server's power state.
  Do you want to continue?[y|N]y
# exit
```

Step 4 Connect to Serial Over Lan Console.

```
# scope sol
# show detail
Serial Over LAN:
 Enabled: yes
 Baud Rate(bps): 9600
 Com Port: com0
# set enabled yes
# set baud-rate 9600
# commit

# connect host // to connect sol cosole
```

Step 5 The machine reboots and prompts to enter F6 for boot option. Press the function-key **F6**.

You may need to press F6 multiple times to see **Enter boot selection menu...** in the screen. You must wait for a few minutes to get the boot device option.

Step 6 Select the desired DVD mount option and in this case, you must select **Cisco CIMC-Mapped vDVD1.22**.

Step 7 The vSphere client displays a list of boot options. Enter **4** to select the **Recover administrator password (Serial Console)** boot option.

Note **To recover administrator password for Gen 3 appliances, it is recommended to use Serial Over Lan (Serial console)**

Step 8 The vSphere client displays a list of administrator user names. Enter the number shown next to the administrator user name for which you want to recover (reset) the password and press **Enter**.

Step 9 Enter the new password and verify it with a second entry.

Step 10 Enter **Y** to save your changes and reboot the system.

Step 11 Login to the admin CLI with the new administrator password.

Related Documentation

- Cisco Integrated Management Controller documentation: http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-integrated-management-controller/tsd-products-support-series-home.html
- Cisco UCS C220 M4 Rack Server Specifications Sheet: http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m4-sff-spec-sheet.pdf
- Cisco UCS C220 Server Installation and Service Guide: http://www.cisco.com/c/en/td/docs/unified_computing/ucs/hw/C220/install/C220.html
- Cisco UCS C220 M5 Rack Server Specifications Sheet:https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m5-sff-specsheet.pdf
- Cisco UCS C220 Server Installation and Service Guide:https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C240M5/install/C240M5.html