Cisco Prime Network Registrar 10.0 Jumpstart Quick Start Guide

First Published: 2019-02-01

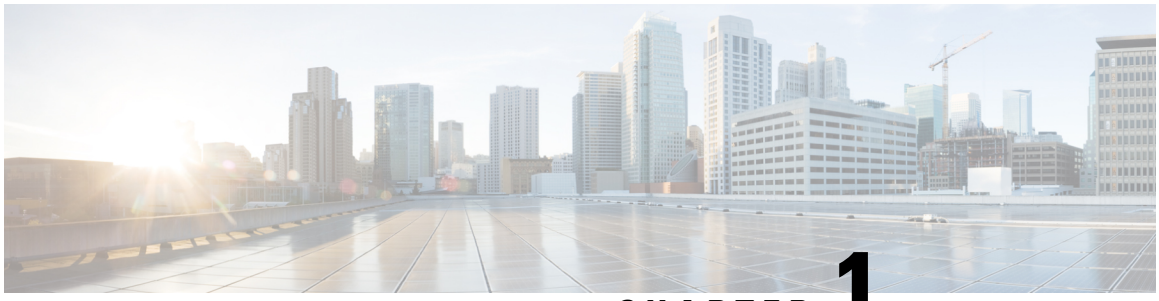
Last Modified: 2019-04-02

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

CONTENTS

CHAPTER 1 **Cisco Prime Network Registrar 10.0 Jumpstart Quick Start Guide** 1

- Introduction 1
- Prerequisites 3
- Configuring the Cisco Prime Network Registrar Jumpstart 4
  - Configuring Cisco Prime Network Registrar Jumpstart 4
  - Configuring Network Information for ESXi 4
  - Configuring Cisco Prime Network Registrar Virtual Appliance 6
- Configuring Network Access on RHEL/CentOS 7.x Using nmcli 7
- Configuring Cisco Prime Network Registrar to Automatically Power Up 10
- Licensing the ESXi Host 11
- How to Recover Cisco Prime Network Registrar Jumpstart 11
  - Prerequisites 11
  - Downloading the Recovery Kit 11
  - Recovery Procedures 12
    - Recovering Cisco Prime Network Registrar Jumpstart 12
- Troubleshooting 14
- Related Documentation 14
- Obtaining Documentation and Submitting a Service Request 15



CHAPTER 1

Cisco Prime Network Registrar 10.0 Jumpstart Quick Start Guide

- Introduction, on page 1
- Prerequisites, on page 3
- Configuring the Cisco Prime Network Registrar Jumpstart, on page 4
- Configuring Network Access on RHEL/CentOS 7.x Using nmcli, on page 7
- Configuring Cisco Prime Network Registrar to Automatically Power Up, on page 10
- Licensing the ESXi Host, on page 11
- How to Recover Cisco Prime Network Registrar Jumpstart, on page 11
- Troubleshooting, on page 14
- Related Documentation, on page 14
- Obtaining Documentation and Submitting a Service Request, on page 15

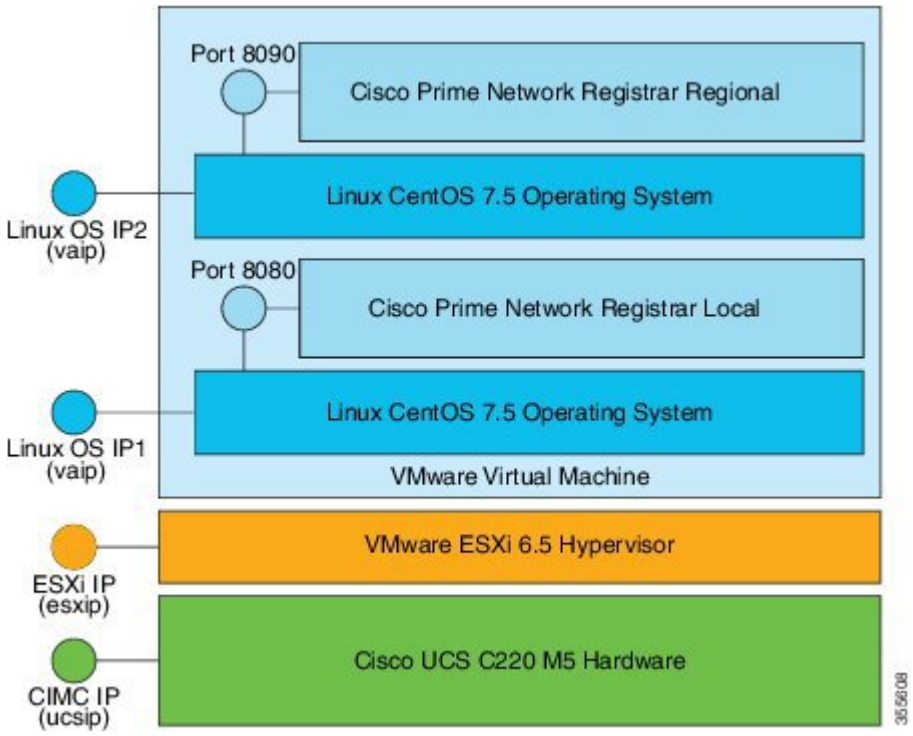
Introduction

The Cisco Prime Network Registrar Jumpstart product is a complete solution for using the Cisco Prime Network Registrar application to manage DHCP, DNS, and Caching DNS servers. It includes the following components:

- Cisco Prime Network Registrar 10.0 application software
- Linux CentOS 7.5 Operating System
- VMware ESXi 6.5 Hypervisor
- Cisco UCS C220 M5 Hardware

These components are integrated together into a single flexible and easy to use appliance (see Figure 1).

Figure 1: Cisco Prime Network Registrar Jumpstart Configuration



Above figure shows the three primary layers in the Cisco Prime Network Registrar Jumpstart appliance. Each of these layers has its own capabilities. Each of these layers can be controlled independently as well as remotely, and each requires its own independent connection to the network. Thus, three unique IP addresses are required.

You may only need to connect to the Cisco Prime Network Registrar Web UI to perform IP address management tasks, but you may also need to connect to one of the other layers to perform system management or troubleshooting tasks related to the appliance. You can connect to each layer as described below:

- Connecting to Virtual Appliance (Open Virtual Appliance) Layer—You can connect to the Cisco Prime Network Registrar application layer using the web browser. Use http://vaip:8080 for local and http://vaip:8090 for regional, where vaip is the virtual appliance IP address (which is also the IP address of the Linux Operating System). For a secure connection to the Cisco Prime Network Registrar Web UI, use https://vaip:8443

  To access the Cisco Prime Network Registrar Command Line Interface (CLI), you can use an SSH connection to the virtual appliance IP address using ssh -l root vaip.

  You can manage the Linux OS by connecting to it using ssh -l root vaip. There is no Windows system installed on the Cisco Prime Network Registrar virtual appliance, but the standard Linux commands necessary to manage a networking application are all present on the Linux OS.

- Connecting to ESXi Hypervisor Layer—Connect to the ESXi hypervisor, identified by the IP address esxip (or its DNS name), using the web browser. esxip is the IP address designated to the ESXi hypervisor.

- Connecting to Cisco Integrated Management Controller (CIMC) UCS Management Console—This allows you to configure and manage the ESXi layer. You can connect to the CIMC by using a browser using https://ucsip/. ucsip is the IP address assigned to the Jumpstart. After you log in to CIMC, you can start the KVM console to get access to the ESXi configuration screen and manage hardware (power, temperature, fan RPM).

Prerequisites

- The IP address or DNS name of the ESXi installation on which you intend to deploy the virtual appliance.
- The IP address or DNS name of any vCenter server associated with the ESXi installation, above.
- Netmask associated with the IP address for the virtual appliance.
- Gateway address appropriate to the IP address and netmask.
- IP addresses of up to two DNS servers for the virtual appliance to use.

  Any proxy values necessary for the virtual appliance to access the Internet. The items concerning the networking environment are as follows. These are not unique to the virtual appliance, but are instead values that are determined by the environment in which you will deploy the virtual appliance:

Note Ensure that you have the Cisco Prime Network Registrar licenses from Cisco.com before you get started. For details, see the License Files section of Cisco Prime Network Registrar 10.0 Installation Guide.

Cisco Prime Network Registrar Jumpstart

Be ready with the following information when configuring the Cisco Prime Network Registrar Jumpstart:

- IP address for the CIMC port on the Cisco Prime Network Registrar Jumpstart.

  Note This IP address must be unique for this appliance.

- Netmask (subnetmask) for the CIMC port address.
- Gateway for the CIMC port address.

Network information for ESXi

Be ready with the following information when configuring network information for ESXi:

- IP address for the ESXi installation on the Cisco Prime Network Registrar Jumpstart.

  Note This IP address must be unique for this appliance.

- Netmask for the IP address for the ESXi installation.
- Gateway address for the ESXi installation on the Cisco Prime Network Registrar Jumpstart.
- VLAN (if any) for the ESXi installation on the Cisco Prime Network Registrar Jumpstart.

Cisco Prime Network Registrar Virtual Appliance

Be ready with the following information before you deploy the virtual appliance. These items are unique to the installation of this particular virtual appliance.

- A virtual machine name for the deployed virtual appliance.
- A root password for the operating system on the virtual appliance. You will be prompted to enter and configure the root password during your first boot.
- IP address for the Cisco Prime Network Registrar virtual appliance.
- DNS name (hostname) for the virtual appliance. It should be placed into DNS using the IP address you selected for the virtual appliance.
- Username and password for the administrator of the Cisco Prime Network Registrar installation.

Configuring the Cisco Prime Network Registrar Jumpstart

Configuring Cisco Prime Network Registrar Jumpstart requires you to do the following configuration steps to connect it to the network:

- Configuring Cisco Prime Network Registrar Jumpstart
- Configuring Network Information for ESXi
- Configuring Cisco Prime Network Registrar Virtual Appliance

Configuring Cisco Prime Network Registrar Jumpstart

To configure the Cisco Prime Network Registrar Jumpstart:

1. Configure the UCS CIMC Network Connection. To configure this, follow the steps in the *Connecting and Powering On the Server (Standalone Mode)* chapter of the enclosed *Cisco UCS C220 Server Installation and Service Guide* or you can see the document available online at:

   https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C220/install/C220.html You have to configure NIC Mode as **None** in the Connecting and Powering On (Standalone Mode) procedure.

The CIMC gives you insight into the hardware as well as support for a virtual KVM console allowing remote management of the ESXi layer. For details on CIMC, see the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide* available online at:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/4_0/b_Cisco_UCS_C-series_GUI_Configuration_Guide_40/b_Cisco_UCS_C-series_GUI_Configuration_Guide_40_preface_00.html

Configuring Network Information for ESXi

After configuring the network information for the UCS CIMC console, use the virtual KVM console that the CIMC console provides to configure the network information for the ESXi hypervisor.

1. Use a browser to connect to the IP address of the CIMC console.
2. Log in to the CIMC console.

Note The default username is **admin** and default password is **password**, but you should change the password at your earliest convenience.

3. On the **Chassis Summary** page, click **Launch KVM**. Choose Java or HTML. You will be asked to approve the running of the application, as this operation downloads code to run on your system. After some delay, the KVM Console window is displayed.

Note If login fails, it may be either that someone else already has a virtual KVM console already active for this UCS C220 server or that your browser is not configured to run Java Web Start.

The initial screen on the KVM console displays VMware ESXi 6.5.0.

4. Press **F2** to customize the system.

Note The virtual KVM console needs to capture the mouse to accept input. It may be necessary on some systems to use the mouse to select the **Single Cursor** option from the **Tools** menu of the KVM Console window. If nothing happens when you press **F2**, select the **Session Options** from the **Tools** menu and click **OK**. Usually this causes the mouse to be captured, and then the functions keys will make it through to the console. If you want the mouse back, you can press **F12**.

5. Press **F2** again to view the login window.
6. Log in to the host. The default username is **root** and the password is **password**.

   Select the **Configure Password** option and reconfigure the root password after you log in.
7. Using the arrow keys, select the **Configure Management Network** option and press **Enter**.
8. **Configuring IP**

   For IP configuration:

   - Use the arrow keys to select **IP Configuration** and press **Enter**.
   - Use the arrow keys to select **Set Static IP address and Network Configuration**.
   - Use the space bar to enable this selection.
   - Use the arrow keys to select **IP Address** and enter the IP address.
   - Use the arrow keys to select **Subnet Mask** and enter the subnet mask.
   - Use the arrow keys to select **Default Gateway** and enter the gateway address.
   - Press **Enter** to accept the IP Configuration updates.

Note If you want to use IPv6 with Cisco Prime Network Registrar, use the arrow keys to select IPv6 Configuration and enter the information requested on that screen.

9. **Configuring DNS Servers**

   To configure the DNS Servers:

   - Use the arrow keys to select **DNS Configuration** and press Enter.
   - Use the arrow keys to select **Primary DNS Server** and enter the IP address of the primary DNS server.
   - Use the arrow keys to select **Alternate DNS Server** and enter the IP address of the alternate DNS server.
   - Use the arrow keys to select **Hostname** and enter the hostname.

   Note Ensure that you enter the entire hostname, including the domain name.

   - Press **Enter** to accept the DNS Configuration updates.

10. If you have a VLAN configured on the switch to which the ESXi is connected, use the arrow keys to select **VLAN (optional)** and press Enter.

    Enter the VLAN for this network connection and press **Enter** to accept the change.

    Press **Esc** to exit the **Configure Management Network** window which you are in now.

11. Use the arrow keys to select **Test Management Network** and press **Enter**.

    You can see the addresses to be pinged and the hostname to be resolved. Use the arrow keys and select the address to be pinged and press **Enter**. The test pings your default gateway and DNS servers and tests the connectivity. Press **Enter** when the test is complete.

    At this point, ESXi listens on the IP address that you configured.

12. Use a browser to connect to the IP address configured for ESXi.

    A window displaying **VMware ESXi 6.5 Welcome** appears.

Note If a warning message about an untrusted SSL certificate appears, select the appropriate action based on your security policy.

Configuring Cisco Prime Network Registrar Virtual Appliance

The Cisco Prime Network Registrar Virtual Appliance is delivered as a virtual machine installed on the ESXi hypervisor. The virtual machine names as shipped from Cisco are “Cisco Prime Network Registrar Local” and “Cisco Prime Network Registrar Regional”.

Note You may change the virtual machine name as per your choice, however, the underlying disk storage will remain under the name originally used to deploy the OVA (for example, Cisco Prime Network Registrar Local).

To manage the virtual machine containing Cisco Prime Network Registrar, as well as manage any other virtual machines which you may deploy on the Jumpstart, use the VMware web client to connect to http://esxip, where esxip is the IP address designated to the ESXi hypervisor.

To configure the Cisco Prime Network Registrar Virtual Appliance:

1. After deploying the OVA files, click the virtual machine name and click the **Console** link.

Note To deploy the OVA files, see the "Deploying the Regional Cluster OVA or Local Cluster OVA" subsection of *Cisco Prime Network Registrar 10.0 Installation Guide.*

2. You will be prompted to enter a root (system) password, which is not the Cisco Prime Network Registrar password.

Note This is the root password for the underlying Linux operating system on which the Cisco Prime Network Registrar 10.0 application is installed. You will be asked to enter this password twice. You will need root access to the underlying Linux operating system later on, so make sure that you remember this password.

3. Read the end user license agreement and if you agree with the terms stated, accept the agreement by entering y (Yes).
4. Log in to the server as the root user.
5. To configure the network for the Virtual Appliance, see "Configuring Network Access on RHEL/CentOS 7.x using nmcli" section.

Configuring Network Access on RHEL/CentOS 7.x Using nmcli

The **NetworkManager** command-line tool (**nmcli**) provides a command line way to configure networking by controlling NetworkManager. This section provides only an overview with some examples to help you learn how to use nmcli to configure network access on the virtual appliance.

In a departure from previous approaches to network interface configuration, NetworkManager deals with both connections and interfaces (also known as devices). Connections are configured with IP addresses, gateways, DNS servers, and then applied to interfaces (devices). This is a critical change from the past way of configuring network access on CentOS Linux.

First, there are two nmcli commands that are of general usefulness:

- The **nmcli d** command lists all available network interfaces (devices).
- The **nmcli c** command lists all available configurations.

Use the above two commands frequently as you are learning to use nmcli.

Follow the steps below to configure an IP address for an interface on your virtual appliance. Typically these commands are typed directly into the console of the virtual appliance. If you are already connected through the network (for example, by **ssh**), then making changes to the network interface configuration can be problematic, as you may also lose network connectivity (and thereby your ability to issue nmcli commands) at any point in the process.

1. Make sure that the interface does not block nmcli. The **nmcli d** command lists the existing interfaces. If the interface you want to configure is listed as **unmanaged**, then NetworkManager has been explicitly blocked from configuring this interface. Until you remove this blockage, no `nmcli` command will have any effect on this interface. Note that you may not need to perform this procedure unless the interface is listed as **unmanaged**. Follow the steps below to allow it to be managed by NetworkManager:
   1. Remove the line NM_CONTROLLED-no from the **file /etc/sysconfig/network-scripts/ifcfg-<interface>**, where `interface` is the interface name listed in the `nmcli d` command. If there is no file with this name, then you do not need to perform this procedure.
   2. NetworkManager must be told to read the configuration files again. To do this, give the following command:

      ```
      nmcli connection reload
      ```

Note Manual changes to any **ifcfg** file will not be noticed by NetworkManager until the following command is issued:

```
nmcli connection reload
```

2. Make sure that there is no current configuration for the interface that you want to configure. If you want the configuration that you create to be the default for the interface and there are multiple configurations associated with an interface, it may lead to confusion when the system reboots. The `nmcli c` command lists the existing configurations. If you see any existing configurations, examine them to see if they apply to the interface you want to configure. An easy way to do this is to use the following command:

   ```
   nmcli con show <config> | grep <interface>
   ```

   If you see any output, you should remove the configuration `<config>` with the command:

   ```
   nmcli con delete <config>
   ```

Note There is often a configuration called "Wired connection 1" which needs to be deleted.

3. Create the configuration and associate it with the interface (device) in one command. This command only creates the configuration and associates it with the interface, it does not apply it to the interface.

   ```
   nmcli con add type ethernet con-name <config> ifname <interface> ip4 <ip>/<netmaskwidth>
    gw4 <gateway>
   ```

   where `<config>` is the name of the configuration, which can be anything (including the name of the interface), `<interface>` is the name of the interface (device), `<ip>` is the IPv4 address, `<netmaskwidth>` is the network mask width, and `<gateway>` is the IPv4 gateway address.

   Example (type all in one line):

   ```
   nmcli con add type ethernet con-name my-office ifname ens160 ip4 10.10.24.25/24 gw4
   10.10.20.174
   ```

4. Add the DNS server to the configuration for the interface (device):

```
nmcli con mod <config> ipv4.dns <dnsip>
```

where `<dnsip>` is the IPv4 address of the DNS server and `<config>` is the name of the configuration.

Example:

```
nmcli con mod my-office ipv4.dns 72.63.128.140
```

You can add two DNS addresses as given below:

```
nmcli con mod my-office ipv4.dns "72.63.128.140 72.63.111.120"
```

Note This will replace any previously set DNS servers. To add to an previously set DNS entry, use the + before ipv4.dns as shown below:

```
nmcli con mod test-lab +ipv4.dns "72.63.128.140 72.63.111.120"
```

5. Apply the configuration to the interface, which will bring up the interface if it was not already running:

   ```
   nmcli con up <config>
   ```

   where `<config>` is the name of the configuration.

6. Use the following command to examine information about a connection. You may examine information about a connection by using this command:

   ```
   nmcli -p con show <config>
   ```

   This will typically scroll off of the console screen, leaving the beginning unreadable. To allow you to move back and forth and examine the output easily, use this command:

   ```
   nmcli -p con show <config> | less
   ```

   From this, you can see the entire configuration. You can modify things in the configuration with:

   ```
   nmcli con mod <config> <something>.<other> <new-value>
   ```

   Example:

   ```
   nmcli con mod my-office wifi-min.key-cntl wpa-psk
   ```

7. Use the command `set-hostname` to set the hostname for the system:

   ```
   hostnamectl set-hostname <hostname>.<domain>
   ```

Note This must be done before registering the local to the regional, otherwise an error will result about "localhost" already existing.

where `<hostname>` is the hostname you want to use and `<domain>` is the domain name, ending with .com, .org, and so on. It is important to include the domain name (along with the .com, .org, or whatever ending is appropriate), since this is used as the default for DNS lookups.

Example

```
hostnamectl set-hostname my-server.gooddomain.com
```

8. After you configure the networking you **must** restart CPNR in order for the interfaces to be properly discovered by CPNR. Use the following commands to restart: **/etc/init.d/nwreglocal restart** (for Local RHEL/CentOS 6.x) or **systemctl restart nwreglocal** (for Local RHEL/CentOS 7.x), **/etc/init.d/nwregregion restart** (for Regional RHEL/CentOS 6.x) or **systemctl restart nwregregion** (for Regional RHEL/CentOS 7.x). If you fail to restart, it will result in a misconfigured registration at the regional.

   To develop a complete understanding of the usage of nmcli, search the internet for online resources on nmcli and CentOS 7.5.

Configuring Cisco Prime Network Registrar to Automatically Power Up

There are several layers of processing involved in running the Cisco Prime Network Registrar application. Each layer has choices it can make about what to do when it is first powered up after power failures.

You can configure the Cisco Prime Network Registrar to start automatically when power is restored to the Jumpstart.

The two places where you have to change the configurations to make this possible are:

- UCS Hardware—The UCS hardware has to be configured to power up the ESXi hypervisor when power is restored.
- ESXi Hypervisor—The ESXi hypervisor has to be configured to power up the Cisco Prime Network Registrar virtual appliance when power is restored to the ESXi hypervisor layer.

To configure the UCS Hardware to automatically power up the ESXi hypervisor:

1. Connect to the CIMC UCS Management Console at http://*cimcip* using a browser and log in. *cimcip* is the address of the CIMC port.
2. Click the **Navigation** toggle button on the upper left.
3. In the **Compute** tab on the left pane, click the **Power Policies** tab.
4. Select **Power On** from the Power Restore Policy drop-down list in the **Power Restore Policy** area.

   If you want, you can enter a delay value in the Power Delay Value field.
5. Click **Save Changes** to save the updates.

To configure the ESXi hypervisor to automatically power up the Cisco Prime Network Registrar virtual appliance when power is restored to the ESXi hypervisor layer, see the “Configuring the Virtual Appliance to Automatically Power Up” section of *Cisco Prime Network Registrar10.0 Installation Guide*.

Licensing the ESXi Host

The VMWare ESXi host will run on a 60-day Evaluation Mode license once it is powered up. The host license that you receive when purchasing a Jumpstart must be applied to license the server. It will be in the following format:

NX61M-43JE6-78J4W-0VB7H-9XHJ4

To license the ESXi host:

1. Connect to the ESXi host using the VMware web client.
2. In the navigation pane on the left, choose **Manage** under **Host**, and then click the **Licensing** tab.
3. Click the **Assign license** button and enter the License key in the pop-up dialog.

How to Recover Cisco Prime Network Registrar Jumpstart

This section describes how to recover Cisco Prime Network Registrar Jumpstart 10.0. It includes the following sections:

- Prerequisites
- Downloading the Recovery Kit
- Recovery Procedures

Prerequisites

To start the recovery process, make sure that you have:

- Internet connectivity—Internet connectivity is required to download the recovery images and to request Cisco Prime Network Registrar replacement licenses from Cisco.com. Ensure that you have the licenses with you before you start the recovery process.
- Recovery kit—The Recovery kit is comprised of three files which must be downloaded from www.cisco.com to your local client. For more information, see “Downloading the Recovery Kit” section.
- Connection to CIMC UCS Management Console—Ensure that the CIMC port is configured on the Cisco Prime Network Registrar Jumpstart appliance. This allows you to configure and manage the ESXi layer. For more information, see “Configuring Cisco Prime Network Registrar Jumpstart” section.

Downloading the Recovery Kit

To download the Cisco Prime Network Registrar Jumpstart recovery kit:

1. From the appropriate server host or client workstation, do the following:

To download	Go to the following URL
Cisco Prime Network Registrar 10.0 Jumpstart Appliance Recovery—approximately 334 MB (cpnr_10_0_jumpstart_appliance_recovery.iso)	https://software.cisco.com/download/home/286322720/type/284561914/release/10.0
Cisco Prime Network Registrar 10.0 Local Virtual Appliance for VMWare—approximately 1690 MB (cpnr_10_0_local.ova)	https://software.cisco.com/download/home/286322716/type/284240043/release/10.0
Cisco Prime Network Registrar 10.0 Regional Virtual Appliance for VMWare—approximately 1566 MB (cpnr_10_0_regional.ova)	

2. To download the recovery kit, click the **Download** button.
3. Sign in with your Cisco.com user ID and password.
4. Read the Cisco End User License Agreement and accept the conditions by clicking **Accept License Agreement.**
5. Download the .iso and .ova files to a location that can be browsed from the host that will be used to recover the Cisco Prime Network Registrar Jumpstart.

Recovery Procedures

This section explains the following recovery procedures:

- Recovering Cisco Prime Network Registrar Jumpstart
- Recovering the Licenses

Recovering Cisco Prime Network Registrar Jumpstart

To recover the Cisco Prime Network Registrar Jumpstart:

1. Use a browser to connect to the IP address of the CIMC console and log in to the console.
2. On the **Chassis Summary** page, click **Launch KVM**. Choose Java or HTML. You will be asked to approve the running of the application, as this operation downloads code to run on your system. After some delay, the KVM Console window is displayed.
3. Click the **Virtual Media** tab.
4. Click **Activate Virtual Devices**.
5. Click the **Virtual Media** tab and choose the connected device that contains the ESXi installation ISO file (cpnr_10_0_jumpstart_appliance_recovery.iso).

   Depending on what devices are attached, the choices are usually “Map CD/DVD”, “Map Removable Disk”, and “Map Floppy”.
6. After selecting the required option, click the **Map Drive** button.

   Ensure that the ISO file is attached and the same status is displayed in the Virtual Media tab.

7. In the **Compute** tab on the left pane, click the **BIOS** tab.
8. Click the **Configure Boot Order** tab and then click the **Configure Boot Order** button.
9. Click the **Advanced** tab.
10. Click **Add Virtual Media**, select Sub Type **KVM MAPPED DVD**, and enter a name for the device.
11. Save the changes and close the Configure Boot Order dialog box.
12. Choose **Configured one time boot device** and select the device created in the previous step.
13. Save the changes.
14. Click the **Host Power** link and then choose **Power Cycle**. Monitor the process via the KVM.
15. Follow the on-screen instructions in the KVM Console window to install ESXi 6.5. This step could take several to many minutes depending on the network connection from the client where the install is being run to the server.

    You may be presented with a choice to upgrade or re-install and re-partition, depending on the situation. Choose the option appropriate for your situation.

    ESXi is always installed in the evaluation mode which will run for 60 days. If you do not have the ESXi 6.5 license key, call the Cisco Technical Assistance Center (TAC) and ask for the Licensing Team. For your local Cisco TAC phone number, see the Cisco Worldwide Contacts page at:

    http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html
16. After the installation completes, unmap the **Virtual Media** drive by clicking Virtual Media and selecting the **Activate Virtual Devices** menu.
17. After the server reboots, configure ESXi 6.5 via the KVM Console window. For more information on how to configure the ESXi layer, see "*Configuring Network Information for ESXi*" section.
18. Using VMware web client, connect to the IP address or hostname of the UCS (ESXi) host.
19. In the navigation pane on the left, click **Virtual Machines**.
20. Click the **Create / Register VM** link.
21. Choose **Deploy a virtual machine from an OVF or OVA file.**
22. Click **Next**.
23. Enter a name for the virtual machine.
24. Click the blue box and navigate to the .ova file.
25. Click **Next** and follow the on-screen instructions.
26. On the **Deployment Options** page, select the **Thick** Disk Provisioning radio button.

    See the "Deploying the Regional Cluster OVA or Local Cluster OVA on VMware" subsection of *Cisco Prime Network Registrar 10.0 Installation Guide* for details.

Note You might want to resize the data disk before starting the virtual machine since the Recovery DVD has the standard OVAs. For details regarding increasing the disk size, see the "Increasing the Size of Disk on VMware" procedure in the "Introduction to Cisco Prime Network Registrar Virtual Appliance" chapter of the *Cisco Prime Network Registrar 10.0 Administration Guide*.

27. Click the name of the virtual machine and click the **Console** link. For more information, see "Configuring Cisco Prime Network Registrar Virtual Appliance" section.
28. Connect to Cisco Prime Network Registrar using http://. It prompts you to create an admin user and password for Cisco Prime Network Registrar.

Recovering the Licenses

You can now restore your original license or request a replacement license at http://www.cisco.com/go/license.

Troubleshooting

If you encounter any issue for which you are not able to find a solution, contact the Cisco Technical Assistance Center (TAC) for help.

For assistance in troubleshooting, the appliance comes with a secure FTP server and a TAC tool.

Ensure that you send the data gathered by the TAC tool to the TAC team in case of issues. For more details regarding the TAC tool, see the *Cisco Prime Network Registrar 10.0 Administration Guide*.

You can use the FTP server (vsftpd) to transfer files to and from the virtual appliance. You have to create a user to log in to the vsftpd because the 'root' user cannot be used for logging in. The vsftpd will not be up and running when you power on the appliance, so you have to manually start it.

You can start the vsftpd using the command:

```
/etc/init.d/vsftpd start
```

You can stop the vsftpd using the command:

```
/etc/init.d/vsftpd stop
```

-

Related Documentation

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

The following is a list of documentation that you can refer to:

Hardware Documents

Go to the following page to see the documentation for UCS server hardware:

https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c220-m5-rack-server/model.html

Platform-Specific Documents

The following is a list of sites with platform-specific documentation:

- For VMware ESXi specific documentation, go the VMware website.
- For CentOS specific documentation, go to the CentOS website.

Software Documents

The following document gives the list of documents available for Cisco Prime Network Registrar 10.0:

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/network_registrar/10-0/doc_overview/guide/CPNR_Doc_Overview.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.