



Managing Pod Through Cisco VIM Unified Management

The following are the naming conventions used in the Cisco VIM UM

1. Super Administrator (UM Admin): User having access to UM Admin profile
2. POD Administrator: User having access to register a Pod in the system(Only UM can add new Pod Admin in the system)
3. Pod users (Normal users):
 - o All the users which are associated with the Pod. Full-pod-access: Role assigned to user which gives full access of a specific Pod(This has nothing to do with Pod Admins)

The following are the Key Points

- User who are UM admin or Pod admin but not associated with any Pod are not counted in UM admin dashboard user count section
- Only Pod Admins can register a new Pod
- Every Pod must a user with “Full-pod-Access” role.
- User cannot be revoked/delete if the users is the last user on the pod with “Full-Pod-Access” role.
- User cannot be delete if user is a Pod admin or UM admin.

The following topics tell you how to install and replace Cisco Virtual Infrastructure Manager (VIM) nodes using Cisco VIM Insight.

- [Monitoring Pod Status, on page 1](#)
- [Managing Hardware, on page 2](#)
- [Power Management, on page 10](#)
- [Managing Software, on page 13](#)
- [Pod User Administration, on page 28](#)

Monitoring Pod Status

The unified management application manages the pods and displays the pod management action status with a cloud icon.

The following table displays a summary of the pod operation, the corresponding cloud-icon color, and the pod status.

Table 1: Pod Operation Status

Pod Operation	UM Icon-Color	Pod Status
Active cloud with no failures	Green	Active
Cloud installation or pod management operation is in progress	Blue	In-progress
Software update (auto) rollback is failed	Red	Critical Warnings
Pending commit post software update	Amber	Warning
Reconfigure failed (for any operation)	Red	Critical Warning
Update, commit, or Rollback failed	Red	Critical Warning
Power management operation fails	Amber	Warning
Management not reachable	Red	Not Reachable

Managing Hardware

Management of your Cisco VIM pods includes adding, removing, or replacing the nodes.

In a pod, multiple nodes cannot be changed at the same time. For example, if you want to replace two control nodes, you must successfully complete the replacement of the first node before you begin to replace the second node. Same restriction applies for addition and removal of storage nodes. Only, in case of Compute Nodes you can add or remove multiple nodes together. However, there must always be one active compute node in the pod at any given point. VNF manager stays active and monitors the compute nodes so that moving the VNFs accordingly as compute node management happens.

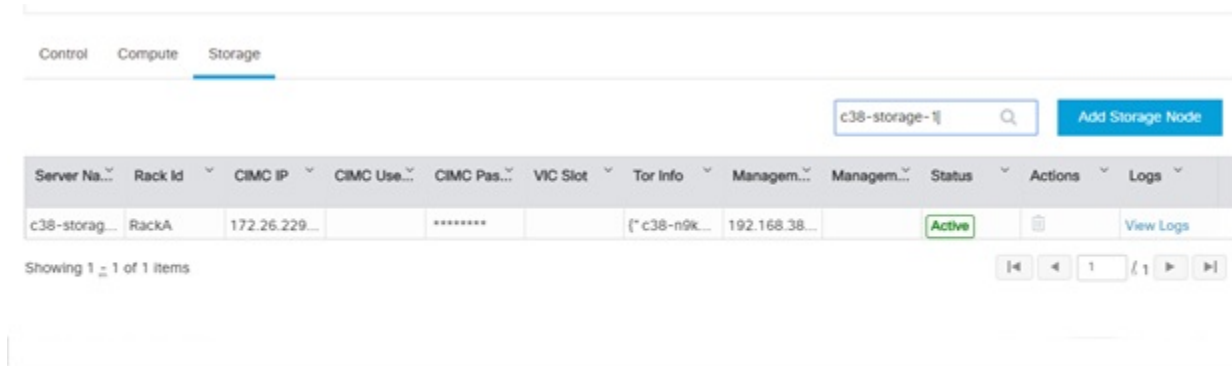


Note When you change a control, storage, or compute node in a Cisco VIM pod using Insight, it automatically updates the server and role in the active blueprint, as a result, your OpenStack deployment changes. When a node is removed from Cisco VIM, sensitive data may remain on the drives of the server. Administrator advice you to use Linux tools to wipe the storage server before using the same server for another purpose. The drives that are used by other application server must be wiped out before adding to Cisco VIM.

Searching Compute and Storage Nodes

This functionality allows you to search the Compute and Storage nodes by server names only. The search result is generated or shows an empty grid if there are no results.

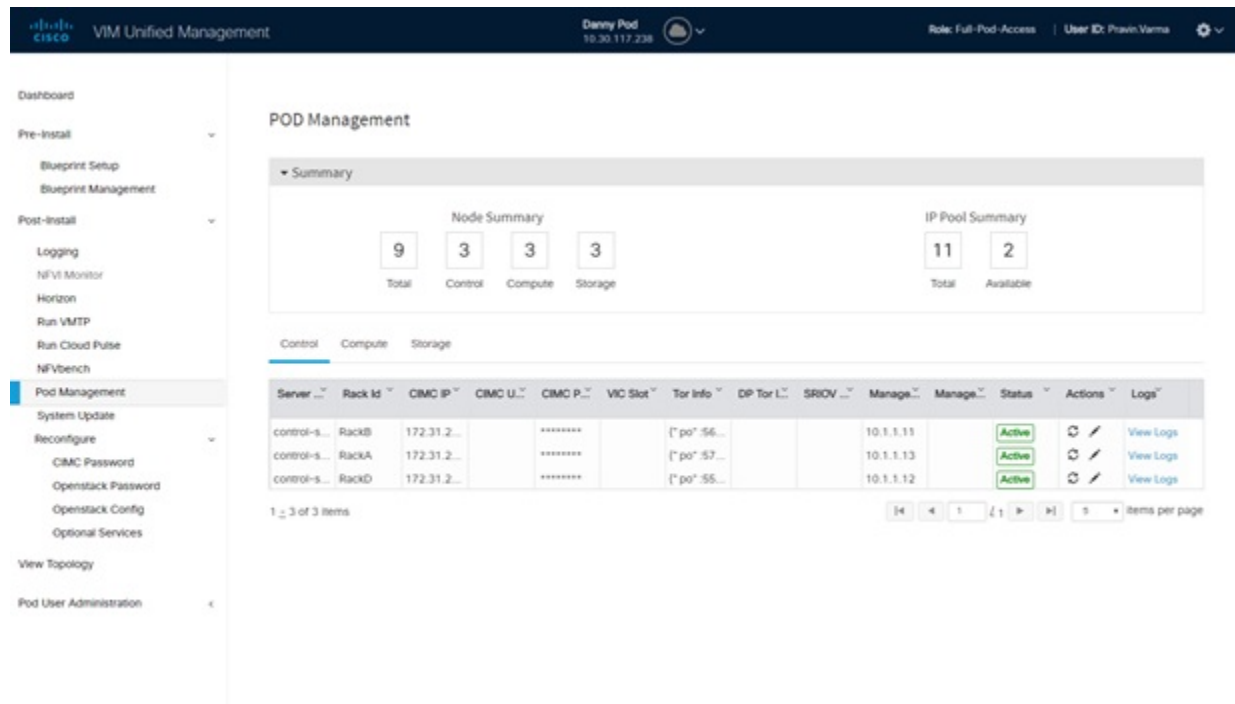
Figure 1: Search Storage Nodes



POD Management

Cisco VIM allows the admin to perform pod life-cycle management from a hardware and software perspective. Cisco VIM provides the ability to power on/off compute node, add, remove or replace nodes based on the respective roles when the nodes of a given pod corrupts at times.

Figure 2: POD Management



Pod Management page has two sections—

1. **Node Summary:** This section shows how many nodes are available and the detailed count of Control, Compute and Storage type.

2. IP Pool Summary: This section shows the Total Pool Summary and the current available pool count.

The operations performed on the running pod are:

Replace Control Nodes: Double fault scenario is not supported. Only the replacement of one controller at a time is supported.



Note If the TOR type is Cisco NCS 5500, an additional popup is displayed to enable the user to update splitter configuration before replacing the control node.

Add Computes/Storage Nodes: N-computes nodes can be replaced simultaneously; however at any given point, at least one compute node has to be active.



Note If the TOR type is Cisco NCS 5500, an option is available to update the splitter cable configuration.

Power On/ Off compute Nodes: You can Power On or Power Off compute node. At least one compute node must be powered on.

Remove Compute/Storage Nodes: You can add one node at a time, when Ceph is run as a distributed storage offering.



Note If TOR type is Cisco NCS 5500, an additional popup is displayed to enable the user to update the splitter cable configuration, before the removal of compute or storage node.

Add Pool: You can increase pool size at any time.

Managing Storage Nodes

Before you add or remove a storage node, review the following guidelines for Managing Storage Nodes.

- **Required Number of Storage Nodes:** A Cisco VIM pod must have a minimum of three and a maximum of 20 storage nodes. If your pod has only two storage nodes, you cannot delete a storage node until you add another storage node. If you have fewer than three storage nodes, you can add one node at a time until you get to 20 storage nodes.
- **Validation of Nodes:** When you add a storage node to a pod, Cisco VIM Insight validates that all the nodes in the pod meet the minimum requirements and are in active state. If you have a control or compute node in a faulty state, you must either correct, delete or replace that node before you can add a storage node.
- **Update Blueprint:** When you add or delete a storage node, Insight updates the blueprint for the Cisco VIM pod.
- **Storage Node Logs:** You can access the logs for each storage node from the link in the Log column on the **Storage Nodes** tab.

Adding Storage Node

Complete the following instructions to add a storage node:



Note You cannot add more than one storage node at a time.

Before you begin

- Remove the non-functional storage node from the pod. You can have maximum 20 storage nodes in a Cisco VIM pod.
- Ensure that the server for the new storage node is in powered state in OpenStack for C Series.

Step 1 In the navigation pane, choose **Post-Install > Pod Management > Storage**.

Step 2 Click on Add Storage node button on the Storage tab. A popup will open where you can provide information about the new Storage node.

Step 3 For C Series, add the following details:

- **Server Name:** Name for the Storage Server to be added.
- **Rack ID:** Enter the Rack ID. (Accepts String format).
- **CIMC IP:** Enter the CIMC IP.
- **CIMC User Name:** User name for the CIMC.
- **CIMC Password:** Enter the password for the CIMC
- **VIC Slot:** Enter the VIC Slot (Optional).
- **ToR switch info:** Mandatory if ToR is configured as True
 - **Management IPv6:** Enter IPv6 Address.

Step 4 For B Series, add the following details:

- **Server Name:** Name for the Storage Server to be added.
- **Rack ID:** Enter the Rack ID. (Accepts String format).
- **Rack Unit ID:** Enter the Rack Unit ID.
- **Management IPv6:** Enter IPv6 Address.

Note Cancel will discard the changes and popup will be closed

If all mandatory fields are filled in correctly then **Add Storage** button will be enabled.

Step 5 Click **Initiate Add Storage**. Add node initialized message will be displayed.

Step 6 To view logs, click **View logs** under Logs column.
The status of the POD will change to Active.

Step 7 Two kinds of failure may occur:

- **Add Node Pre-Failed:** When addition of node failed before the bare-metal stage (step 4) the Active Blueprint will be modified but the Node is not yet added in the Cloud. If you press **X** Icon, then Insight will delete the node information from the Blueprint and the state would be restored.
- **Add Node Post-Failed:** When addition of node failed after the bare-metal stage (step 4) the Active Blueprint will be modified and the node is registered in the cloud. If you press **X** Icon, then Insight will first delete the node from the Blueprint and then node removal from cloud would be initiated.

You can view the logs for this operation under **Logs** column.

Deleting Storage Node

You cannot delete more than one storage node at a time.

Step 1 In the Navigation pane, choose **Post-Install > POD Management > Storage**.

Step 2 Click **X** adjacent to the storage node you want to delete.

Step 3 **Node Removal Initiated successfully** message will be displayed.

To view logs, click **View logs** under logs column.

- If the Storage Node is deleted successfully, the storage node will be removed from the list under **Add/Remove storage Node**.
- In deletion failed, a new button **Clear Failed Nodes** will be displayed. Click **Clear Failed Nodes** to remove the node from cloud and Blueprint.

Managing Compute Nodes

Before you add or remove a compute node, review the following guidelines:

- **Required Number of Compute Nodes:** Cisco VIM pod must have a minimum of one compute node and a maximum of 61 compute nodes (with 3 ceph nodes). If your pod has only one compute node, you cannot delete that node until you add another compute node.
- **Update Blueprint:** When you add or remove a compute node, Insight updates the blueprint for the Cisco VIM pod.
- **Compute Node Logs:** You can access the Logs for each compute node from the link in the Log column on the Compute Nodes table.

Adding Compute Node

Add IP Pool

If all the existing pool size is already used, then you need to increase the pool size. On the Add compute or Add storage popup, Click **Expand Management IP pool** to add a new Pool.

Complete the instructions, to add a compute node:

Before you begin

Ensure that the server for the new compute node is in powered state in OpenStack. You can add more than one compute node at a time.

-
- Step 1** In the navigation pane, click **Post-Install > Pod Management > Compute**.
- Step 2** Click **Add Compute Node** on the Compute tab a popup opens . Add the required information in the popup. To add another node click **Add Another Node** if you planned to add another compute node OR hit Initiate Add Compute if you so not plan to add any more compute node. If you hit “Add Another Node” button, the existing form will be emptied. You will have to fill the information for the new compute node and then repeat step 1. You may use Previous and Next button to navigate among different added node information.
- Step 3** For C Series, add the following details:
- **Server Name:** Name for the Compute Server.
 - **Rack ID:** Enter the Rack ID. (Accepts String format).
 - **CIMC IP:** Enter the CIMC IP.
 - **CIMC User Name:** User name for the CIMC.
 - **CIMC Password:** Enter the password for the CIMC.
 - **VIC Slot:** Enter the VIC Slot (Optional).
 - **ToR switch info:** Mandatory if configured ToR is true.
 - **DP ToR switch info:** Enter input as string format.
 - **SRIVO ToR info :** Enter input as string format.
 - **Management IPv6 :** Enter IPv6 Address.

Step 4 For B Series, add the following details:

- **Server Name:** Name for the Storage Server to be added.
- **Rack ID:** Enter the Rack ID. (Accepts String format).
- **Rack Unit ID:** Enter the Rack Unit ID.
- **Chassis ID:** Enter the Chassis ID. Range for Chassis ID is 1-24.
- **Blade ID:** Enter the Blade ID. Range for Blade ID is 1-8.
- **CIMC Password:** Enter the CIMC Password.
- **Management IPv6:** Enter IPv6 address.

If all mandatory fields are filled in correctly then click **Save**

Note Add Compute process can initiate multiple add of compute nodes. Fill in the mandatory fields to save new compute node or press cancel to exit message will be displayed.

Fields of Pod management will remain mandatory for user input based on setup-data.

Step 5 You may perform one among these steps mentioned below:

- Clicking **Cancel** displays the compute node information listed in the table and **Add Compute Node** button is enabled.
- If you feel you have filled in a wrong entry for the compute node information, click **Delete**. This will delete the entry from the table as this information is not added in the Blueprint.
- Click **Initiate Add Compute**, displays Add node initialized message.

Step 6 To view logs, click **View logs** under Logs column. The status of the POD will change to Active.

Step 7 Two kinds of failure may occur:

- **Add Node Pre-Failed:** When addition of node failed before the bare-metal stage (step 4) the Active Blueprint will be modified but the Node is not yet added in the Cloud. If you press **X** Icon, then Insight will delete the node information from the Blueprint and the state would be restored.
- **Add Node Post-Failed:** When addition of node failed after the bare-metal stage (step 4) the Active Blueprint will be modified and the node is registered in the cloud. If you press **X** Icon, then Insight will first delete the node from the Blueprint and then node removal from cloud would be initiated.

You can view the logs for this operation under **Logs** column.

Deleting Compute Node

Compute node is deleted due to a hardware failure. You can delete one compute node at a time.



Note If your pod has only one compute node, you cannot delete that node until you add another compute node.

-
- Step 1** In the navigation pane, choose **Post-Install > POD Management > Compute**.
- Step 2** Click **X** for the compute node to be deleted. To remove multiple compute nodes, choose the target compute nodes which is on the extreme left column, then click **Trash** Icon to remove multiple computes. Node Removal Initiated successfully message is displayed.
- Step 3** To view the Logs, click **View logs** under Logs column.
- If compute nodes are deleted successfully, you cannot view the compute node in the list under **Add or Remove Compute Node**.
 - If Compute Note is deleted, a new button **Clear Failed Nodes** is displayed.
- Step 4** Click **Clear Failed Nodes** to remove the node form Cloud and Blueprint.
-

Managing Control Nodes

Before you replace a control node, review the following guidelines:

- **Required Number of Control Nodes:** A Cisco VIM pod must have three control nodes and you can only replace one node at a time.
- **Validation of Nodes:** When you replace a control node, Cisco VIM Insight validates if all the other nodes in the pod meet the minimum requirements and are in active state. If you have a storage or a compute node in a faulty state, you must correct the faulty state or delete or replace that node before you can replace the control node.
- **Update Blueprint:** When you replace a control node, Insight updates the Active blueprint for the Cisco VIM pod.
- **Control Node Logs:** You can access the logs for each control node from the link in the **Logs** column of Control Nodes table.

Replacing Control Node

You can replace only one control node at a time.

-
- Step 1** In the navigation pane, click **Post-Install > Pod Management > Control**.
- Step 2** Click (Spin) icon. A confirmation pop-up appears, Click proceed to continue.
- Step 3** If you want to edit a specific control node before replace, click **Edit** to update the changes.
- Step 4** On success, **Replace Node Initiated** successfully message is displayed.
- Step 5** You can view the logs in the **Logs** column on the Control Nodes table.
-

What to do next

If the replacement of the control node fails, do the following:

- Click the link in the Logs column.

- Check the logs to determine the cause of the failure.
- Correct the issue and attempt to replace the control node again.

Power Management

Compute node can be powered on or powered off from the Compute Tab in Pod Management section. There is a power button associated with each compute with information provided as tooltip when you hover on that icon.

Following are the steps to power on/off multiple compute node:

1. Click **Power** button located to the left of delete button.
2. Choose the compute nodes by selecting the check box, the corresponding power button gets enabled.

Power On a Compute Node

Following are the steps to power on the compute node:

1. Click the **Compute** tab.
2. In the Pod Management area, check the check box corresponding to the Compute node that you want to power on.



Note The **Power** button of a Compute node is enabled only after you select the Compute node.

Figure 3: Powering On a Compute Node

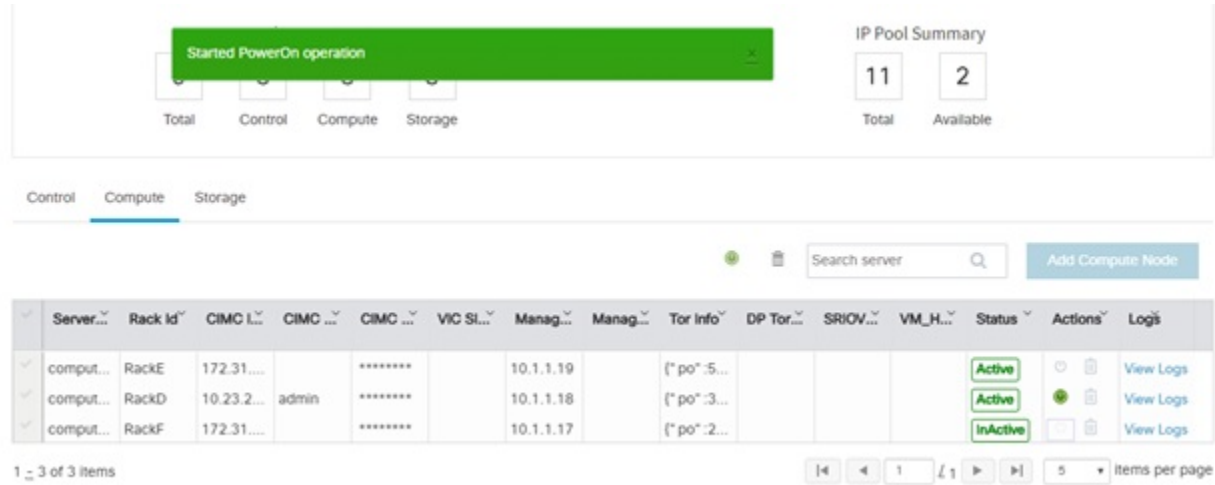
Server...	Rack Id	CIMC L...	CIMC ...	CIMC ...	VIC SL...	Manag...	Manag...	Tor Info	DP Tor...	SRIOV...	VM_H...	Status	Actions	Logi
✓ comput...	RackE	172.31...		*****		10.1.1.19		[* po*:5...				Active	⊞ ⊞ View Logs	
✓ comput...	RackD	10.23.2...	admin	*****		10.1.1.18		[* po*:3...				Active	⊞ ⊞ View Logs	
✓ comput...	RackF	172.31...		*****		10.1.1.17		[* po*:2...				InActive	⊞ ⊞ Power On. Click to Power Off	

1 - 3 of 3 items

5 items per page

3. Under the Actions column, click the **Power** button of the Compute node. It may take a few minutes for the Compute node to power on. The tooltip of the power button displays the status of the Compute node. Once the compute node is powered on, the Power button stops blinking and its color changes to green.

Figure 4: Power On Operation



You can add a Compute node only once a power on task is complete.

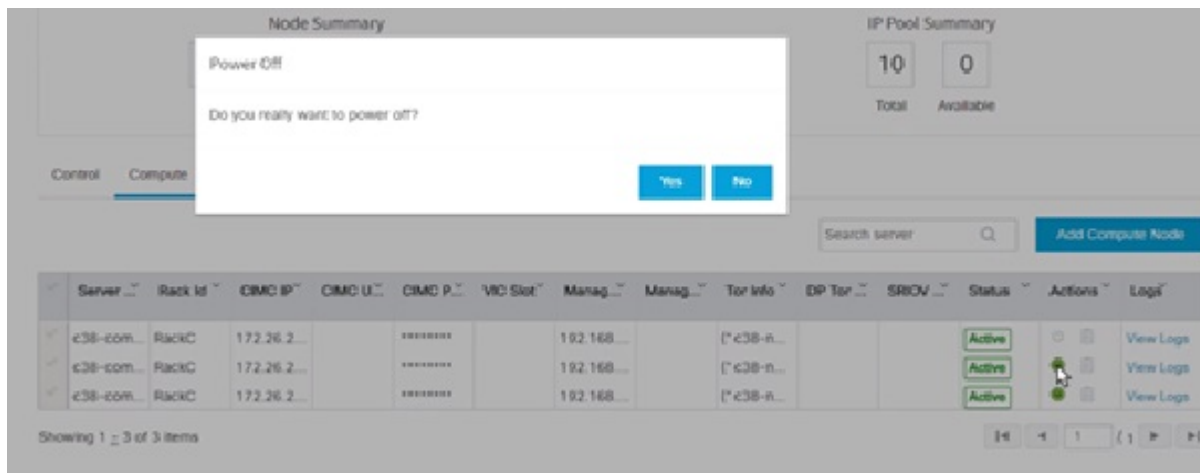
Powering Off Compute Node



Note You cannot power off all the Compute nodes. There must be at least one Compute node that is in the On state.

Follow these steps to power off a Compute node:

1. Click the **Compute** tab.
2. In the Pod Management area, under the Actions column, click the **Power** button of the Compute node that you want to power off.



3. Click **Yes** in the confirmation dialog box.

The screenshot shows the 'Node Summary' section with a green bar indicating 'Started PowerOff operation'. The 'IP Pool Summary' shows 10 Total and 0 Available. Below, a table lists three compute nodes, all with 'Active' status.

Server	Rack Id	CIMC IP	CIMC U	CIMC P	VIC Slot	Manag	Manag	Tor Info	DP Tor	SRIOV	Status	Actions	Logs
c38-com...	RackC	172.26.2...		*****		192.168...		[*c38-n...			Active	[Power Off]	View Logs
c38-com...	RackC	172.26.2...		*****		192.168...		[*c38-n...			Active	[Power Off]	View Logs
c38-com...	RackC	172.26.2...		*****		192.168...		[*c38-n...			Active	[Power Off]	View Logs

It may take a few minutes for the Compute node to power off. The tooltip of the power button displays the status of the Compute node. Once the compute node is powered off, the Power button stops blinking and its color changes to grey.



Note

If there is only one compute node in the grid, and you try to power off it, a message *Last compute node can't be powered off* is displayed. Also, when you power off the last available compute node in the list of nodes, then the message *At least one compute node should be powered on* is displayed.

Multiple compute power/ delete/ reboot operation

You can perform power, delete, and reboot operation on multiple compute nodes using the global buttons located at the top of grid. To enable this operation, select at least one compute node.

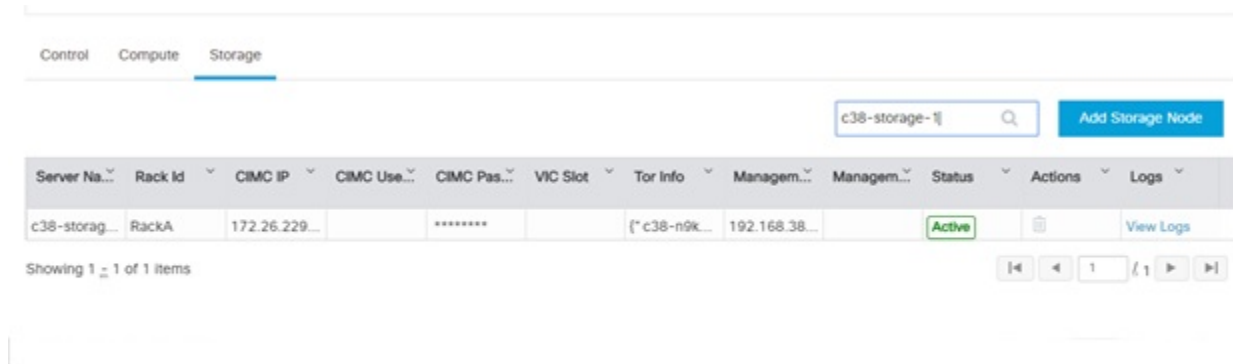
The screenshot shows the 'POD Management' section with a 'Summary' card. The 'Node Summary' shows 8 Total, 3 Control, 2 Compute, and 3 Storage. The 'IP Pool Summary' shows 10 Total and 2 Available. Below, a table lists two compute nodes, both with 'Active' status.

Server	Rack Id	CIMC IP	CIMC U	CIMC P	VIC Slot	Manag	Manag	Tor Info	DP To	SRIOV	VM_H	Sta	Actions	Logs
comput...	RackF	172.31...		*****		10.1.1.17		[*po*_2...				Acti	[Power Off]	View Logs
comput...	RackD	10.23.2...	admin	*****		10.1.1.18		[*po*_3...				Acti	[Power Off]	View Logs

Searching Compute and Storage Nodes

This functionality allows you to search the Compute and Storage nodes by server names only. The search result is generated or shows an empty grid if there are no results.

Figure 5: Search Storage Nodes



Managing Software

Software management of your Cisco VIM pods includes software update, reconfigure of openstack services and password, etc.

VIM Software Update

As part of the lifecycle management of the cloud, VIM has the ability to bring in patches (bug fixes related to code, security, etc.), thereby providing cloud management facility from software point of view. Software update of the cloud is achieved by uploading a valid tar file, following initiation of a System Update form the Insight as follows:

-
- Step 1** In the Navigation pane, click **Post-Install > System Update**.
 - Step 2** Click **Browse** and select the valid tar file.
 - Step 3** Click **Open**.
 - Step 4** Click **Upload and Update**.
Update started Successfully message will be displayed.
 - Step 5** Update status will be shown as **ToUpdate**.
Click the hyperlink to view the reconfigure logs for install logs.
Reconfigure status will be available on the page or the dashboard under **POD Operation** details.
-

What to do next

System Update has been initiated message will be displayed. Logs front-ended by hyperlink will be in the section below in-front of **Update Logs** which shows the progress of the update. During the software update, all other pod management activities will be disabled. Post-update, normal cloud management will commence. Once update has completed you will see the status of update in the box below.

If log update fails, **Auto-RollBack** will be initiated automatically.

If log update is successful, you will have two options to be performed:

1. **Commit**—To proceed with the update.
2. **RollBack**—To cancel the update.

If Auto-rollback fails during software update fails through Insight UI, it is advised that the administrator contact Cisco TAC for help. Do not re-try the update or delete the new or the old installer workspace.

If the update is successful and reboot is required for at least one compute node:

- Only commit or rollback is allowed.
- Following operations are not permitted:
 - Reconfigure
 - System update
 - Pod management

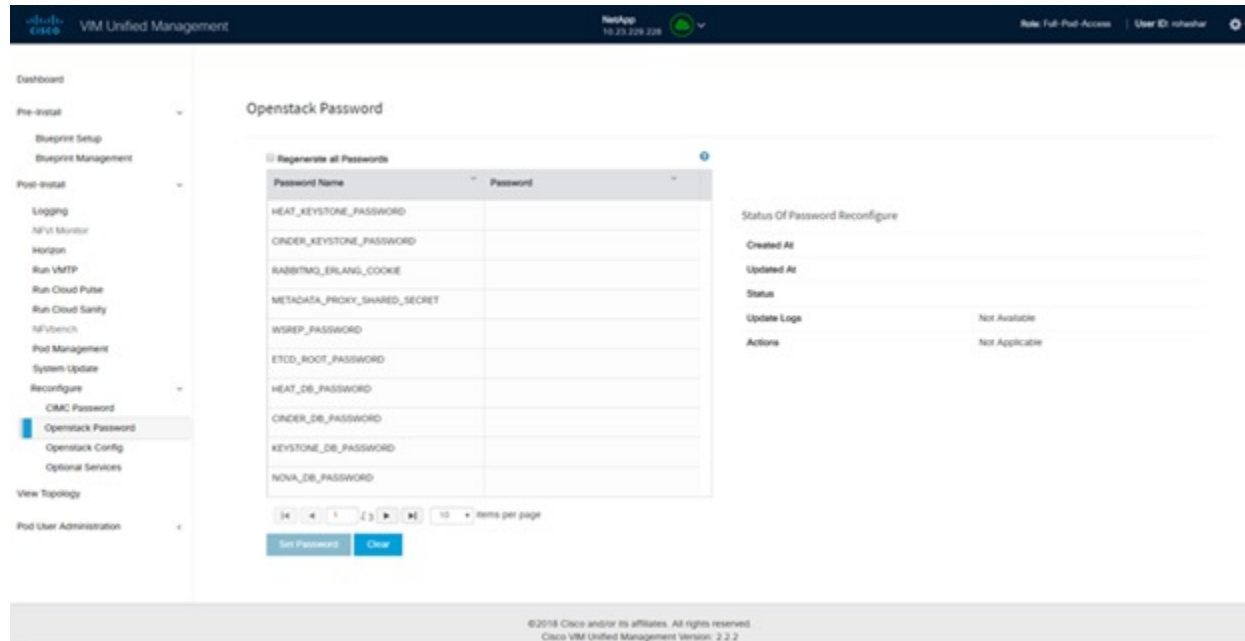


Note You can reboot the node, only after the commit or rollback operation.

Reconfigure Openstack Passwords

There are two options to regenerate the passwords:

- **Regenerate all passwords:** Click **Regenerate all passwords** checkbox and click **Set Password**. This will automatically regenerate all passwords in alphanumeric format.
- **Regenerate single or more password:** This will set a specific password by doing an inline edit for any service like Horizon's ADMIN_USER_PASSWORD. Double click on the field under Password and enter the password to enable **Set Password** button.



During the reconfiguration of password, all other pod management activities will be disabled. Post-update, normal cloud management will commence. If the reconfigure of the password fails, all subsequent pod management operations will be blocked. It is advised to contact Cisco TAC to resolve the situation through CLI.

Reconfigure OpenStack Services, TLS Certificates, and ELK Configurations

Cisco VIM supports the reconfiguration of OpenStack log level services, TLS certificates, and ELK configuration. Following are the steps to reconfigure the OpenStack and other services:

-
- Step 1** In the navigation pane, click **Post-Install > Reconfigure Openstack Config**.
 - Step 2** Click the specific item that you want to change and update. For example: to update the TLS certificate click the path to the certificate location.
 - Step 3** Enter **Set Config** to commence the process.
-

What to do next

During the reconfiguration process, all other pod management activities are disabled. Post-update, normal cloud management commences. If reconfigure of OpenStack Services fails, all subsequent pod management operations are blocked. Contact, Cisco TAC to resolve the situation through CLI.

Reconfiguring CIMC Password through Unified Management

Cisco VIM allows you to Update the cimc_password in the CIMC-COMMON section, and/or the individual cimc_password for each server and then run the update password option.

You need to match the following Password rule to update the Password:

- Must contain at least one lower case letter.
- Must contain at least one upper case letter.
- Must contain at least one digit between 0 to 9.
- One of these special characters !\$#@%^_+*=&
- Your password has to be 8 to 14 characters long.

Before you begin

You must have a C-series pod up and running with Cisco VIM to reconfigure CIMC password.



Note Reconfigure CIMC password section will be disabled if the pod is in failed state as indicated by `ciscovim install-status`.

-
- Step 1** Log-in to **CISCO VIM Insight**.
- Step 2** In the navigation pane, select **Post-Install**.
- Step 3** Click **Reconfigure CIMC Password**.
- Step 4** You can reconfigure the CIMC Password at global level by adding new CIMC_COMMON Password or to reconfigure CIMC Password for individual servers double click the server password you want to edit.
- Step 5** Click **Reconfigure** to initiate reconfigure process.
-

Reconfigure Optional Services

Cisco VIM offers optional services such as heat, migration to Keystone v3, NFVBench, NFVIMON, etc, that can be enabled post-pod deployment. These services can be enabled in one-shot or selectively.

Listed below are the steps to enable optional services:

-
- Step 1** In the Navigation pane, click **Post-Install > Reconfigure Optional Services**.
- Step 2** Choose the right services and update the fields with the right values.
- Step 3** Click **Offline validation**. Once offline validation is successful.
- Step 4** Click **Reconfigure** to commence the process.

During the reconfiguration process, all other pod management activities will be disabled. Post-update, normal cloud management will commence.

If reconfigured OpenStack Services fail, all subsequent pod management operations are blocked. Contact Cisco TAC to resolve the situation through CLI.

Note All reconfigure operation feature contains repeated deployment true or false.

- Repeated re-deployment true - Feature can be re-deployed again.
- Repeated re-deployment false- Deployment of feature allowed only once.

Deployment Status :

Optional Features	Repeated re-deployment Option
APICINFO	True
EXTERNAL_LB_VIP_FQDN	False
EXTERNAL_LB_VIP_TLS	False
INSTALL_MODE	True
HTTP_PROXY & HTTPS_PROXY	True
LDAP	True
NETWORKING	True
NFVBENCH	False
NFVIMON	False
PODNAME	False
PROVIDER_VLAN_RANGES	True
SWIFTSTACK	True
SYSLOG_EXPORT_SETTINGS	False
TENANT_VLAN_RANGES	True
TORSWITCHINFO	False
VIM _ ADMINS	True
VMTP	False
VTS_PARAMETERS	False
AUTOBACKUP	True
Heat	False
Keystone v3	False

Reconfiguring Optional Features Through Unified Management

Step 1 Log-in to Cisco VIM UM.

Step 2 In the **Navigation** pane, expand the **Post-Install Section**.

Step 3 Click **Reconfiguring Optional Feature through UM**.

Step 4 On the **Reconfiguring Optional Feature through UM** page of the Cisco VIM UM, complete the following fields:

Name	Description
Heat check box	<ul style="list-style-type: none"> • Enable Heat. • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process..
Keystone v3 check box	<ul style="list-style-type: none"> • Enable Keystone v3. • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process.
ENABLE_ESC_PRIV	<ul style="list-style-type: none"> • Enable ENABLE_ESC_PRIV . • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process.
Autobackup check box	<ul style="list-style-type: none"> • Enable/Disable Autobackup. • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process.
External LB VIP TLS check box	<ul style="list-style-type: none"> • Enable External LB VIP TLS. • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process.
External LB VIP FQDN check box	<ul style="list-style-type: none"> • Enter Input as a string. • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process.
Pod Name	<ul style="list-style-type: none"> • Enter Input as a string. • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process.

Name	Description
Tenant Vlan Ranges	<ul style="list-style-type: none"> • Augment tenant vlan ranges input. For Example: 3310:3315. • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process.
Provider VLAN Ranges	<ul style="list-style-type: none"> • Enter input to tenant vlan ranges. For Example: 3310:3315. • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process.
Install Mode	<ul style="list-style-type: none"> • Select Connected or Disconnected, any one form the drop-down list. • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process.
Registry Setup Settings checkbox	<p>For Registry Setup:</p> <ul style="list-style-type: none"> • Enter the Registry User Name. It is a mandatory field • Enter the Registry Password. The minimum length of the password is three. • Enter the Registry Email. It is a mandatory field. • Enter the Registry Name. For example, Registry FQDN name. It is a mandatory field, only when SDS is enabled. • Click Offline Validation • If offline validation is successful, click Reconfigure to commence the process.

Name	Description	
Syslog Export Settings	Following are the options for Syslog Settings:	
	Remote Host	Enter Syslog IP Address.
	Facility	Defaults to local5
	Severity	Defaults to debug
	Clients	Defaults to ELK
	Port	Defaults to 514 but is modified by the User.
	Protocol	Supports only UDP
Configure ToR checkbox	Click Offline Validation . <ul style="list-style-type: none"> • When Offline Validation is successful, click Reconfigure to commence the process. True or False . Default is false.	

Name	Description		
<p>ToR Switch Information</p>	<p>Click + to add information for ToR Switch.</p>		
	<table border="1"> <thead> <tr> <th data-bbox="902 352 1214 386">Name</th> <th data-bbox="1221 352 1523 386">Description</th> </tr> </thead> </table>	Name	Description
	Name	Description	
	<p>Name</p>	<p>ToR switch name.</p>	
	<p>Username</p>	<p>ToR switch username.</p>	
	<p>Password</p>	<p>ToR switch Password.</p>	
	<p>SSH IP</p>	<p>ToR switch SSH IP Address.</p>	
	<p>SSN Num</p>	<p>ToR switch ssn num. output of show license host-id.</p>	
	<p>VPC Peer Keepalive</p>	<p>Peer Management IP. You need not define if there is no peer.</p>	
	<p>VPC Domain</p>	<p>Need not define if there is no peer.</p>	
	<p>VPC Peer port</p>	<p>Interface for vpc peer ports.</p>	
	<p>VPC Peer VLAN Info</p>	<p>vlan ids for vpc peer ports (optional).</p>	
	<p>BR Management Port Info</p>	<p>Management interface of the build node.</p>	
<p>BR Management PO Info</p>	<p>Port channel number for the management interface of the build node.</p>		
<p>Click Save</p> <ul style="list-style-type: none"> • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process. 			

Note When setup data is ACI VLAN with TOR then reconfigure options are:

<p>TORSwitch Information mandatory table if you want to enter ToR information</p>	<p>Click + to add information for ToR Switch.</p> <table border="1" data-bbox="862 281 1487 590"> <thead> <tr> <th data-bbox="862 281 1175 338">Name</th> <th data-bbox="1175 281 1487 338">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="862 338 1175 394">Host Name</td> <td data-bbox="1175 338 1487 394">ToR switch name.</td> </tr> <tr> <td data-bbox="862 394 1175 451">VPC Peer Keepalive</td> <td data-bbox="1175 394 1487 451">Peer Management IP.</td> </tr> <tr> <td data-bbox="862 451 1175 508">VPC Domain</td> <td data-bbox="1175 451 1487 508">Do not define if there is no</td> </tr> <tr> <td data-bbox="862 508 1175 590">Node ID</td> <td data-bbox="1175 508 1487 590">Integer, unique across all switches</td> </tr> </tbody> </table> <p>Click Save</p> <ul style="list-style-type: none"> • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process. 	Name	Description	Host Name	ToR switch name.	VPC Peer Keepalive	Peer Management IP.	VPC Domain	Do not define if there is no	Node ID	Integer, unique across all switches
Name	Description										
Host Name	ToR switch name.										
VPC Peer Keepalive	Peer Management IP.										
VPC Domain	Do not define if there is no										
Node ID	Integer, unique across all switches										
<p>NFV Bench</p>	<p>Enable check box which by default is false.</p> <p>Add Tor info connected to switch:</p> <ul style="list-style-type: none"> • Select a TOR Switch and Enter the Switch name. • Enter the port number. For example: eth1/5 • NIC Ports: INT1 and INT2 optional input, enter the 2 port numbers of the 4-port 10G Intel NIC at the management node used for NFVBench. • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process. <p>Note If ToR is already present in Setup-data or already deployed. Then no need add Tor info, by default ToR info switchname is mapped in NFV bench.</p>										

<p>Swiftstack</p> <p>SwiftStack is only supported with Keystone v2. If you select Keystone v3, swiftstack will not be available for configuration.</p>	<p>Cluster End Point</p>	<p>IP address of PAC (proxy-account-container) endpoint.</p>
	<p>Admin User</p>	<p>Admin user for swift to authenticate in keystone.</p>
	<p>Admin Tenant</p>	<p>The service tenant corresponding to the Account-Container used by Swiftstack.</p>
	<p>Reseller Prefix</p>	<p>Reseller_prefix as configured for Keystone Auth,AuthToken support in Swiftstack E.g KEY_</p>
	<p>Admin Password</p>	<p>swiftstack_admin_password</p>
	<p>Protocol drop-down list</p>	<p>http or https</p>
	<ul style="list-style-type: none"> • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process. 	

LDAP with Keystone v3	Domain Name field	Enter the Domain name.
	Object Class for Users field	Enter a string as input.
	Object Class for Groups	Enter a string.
	Domain Name Tree for Users	Enter a string.
	Domain Name Tree for Groups field	Enter a string.
	Suffix for Domain Name field	Enter a string.
	URL field	Enter a URL with port number.
	Domain Name for Bind User field	Enter a string.
	Password field	Enter Password as string format.
	User Filter	Enter filter name as string.
	User ID Attribute	Enter a string.
	User Name Attribute	Enter a string.
	User Mail Attribute	Enter a string.
Group Name Attribute	Enter a string.	
<ul style="list-style-type: none"> • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process. 		

<p>NFV Monitoring</p>	<p>Followings are the field values for NFV Monitoring:</p> <table border="1"> <tr> <td data-bbox="901 285 1214 338">Master Admin IP field.</td> <td data-bbox="1219 285 1518 338">Enter Input as IP format.</td> </tr> <tr> <td data-bbox="901 344 1214 428">Collector Management IP field</td> <td data-bbox="1219 344 1518 428">Enter Input as IP format.</td> </tr> <tr> <td colspan="2" data-bbox="901 434 1518 480">Collector VM1 info</td> </tr> <tr> <td data-bbox="901 487 1214 533">Host Name field</td> <td data-bbox="1219 487 1518 533">Enter Host Name as a string.</td> </tr> <tr> <td data-bbox="901 539 1214 592">CCUSER password field</td> <td data-bbox="1219 539 1518 592">Enter Password.</td> </tr> <tr> <td data-bbox="901 598 1214 644">Password field</td> <td data-bbox="1219 598 1518 644">Enter password.</td> </tr> <tr> <td data-bbox="901 651 1214 697">Admin IP field</td> <td data-bbox="1219 651 1518 697">Enter Input as IP format.</td> </tr> <tr> <td data-bbox="901 703 1214 756">Management IP field</td> <td data-bbox="1219 703 1518 756">Enter Input as IP format.</td> </tr> <tr> <td colspan="2" data-bbox="901 762 1518 808">Collector VM2 info</td> </tr> <tr> <td data-bbox="901 814 1214 867">Host Namefield</td> <td data-bbox="1219 814 1518 867">Enter a string.</td> </tr> <tr> <td data-bbox="901 873 1214 926">CCUSER field</td> <td data-bbox="1219 873 1518 926">Enter Password.</td> </tr> <tr> <td data-bbox="901 932 1214 984">Management IP field</td> <td data-bbox="1219 932 1518 984">Enter Input as IP format.</td> </tr> <tr> <td colspan="2" data-bbox="901 991 1518 1037">Dispatcher</td> </tr> <tr> <td data-bbox="901 1043 1214 1127">Rabbit MQ Username Field</td> <td data-bbox="1219 1043 1518 1127">Enter a string.</td> </tr> </table> <ul style="list-style-type: none"> • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process. 	Master Admin IP field.	Enter Input as IP format.	Collector Management IP field	Enter Input as IP format.	Collector VM1 info		Host Name field	Enter Host Name as a string.	CCUSER password field	Enter Password.	Password field	Enter password.	Admin IP field	Enter Input as IP format.	Management IP field	Enter Input as IP format.	Collector VM2 info		Host Namefield	Enter a string.	CCUSER field	Enter Password.	Management IP field	Enter Input as IP format.	Dispatcher		Rabbit MQ Username Field	Enter a string.
Master Admin IP field.	Enter Input as IP format.																												
Collector Management IP field	Enter Input as IP format.																												
Collector VM1 info																													
Host Name field	Enter Host Name as a string.																												
CCUSER password field	Enter Password.																												
Password field	Enter password.																												
Admin IP field	Enter Input as IP format.																												
Management IP field	Enter Input as IP format.																												
Collector VM2 info																													
Host Namefield	Enter a string.																												
CCUSER field	Enter Password.																												
Management IP field	Enter Input as IP format.																												
Dispatcher																													
Rabbit MQ Username Field	Enter a string.																												
<p>VTS Parameter</p>	<p>Following are the fields to reconfigure for VTS parameters</p> <table border="1"> <tr> <td data-bbox="901 1369 1214 1415">VTC SSH Username field.</td> <td data-bbox="1219 1369 1518 1415">Enter the string.</td> </tr> <tr> <td data-bbox="901 1421 1214 1474">VTC SSH Username field.</td> <td data-bbox="1219 1421 1518 1474">Enter the password.</td> </tr> </table> <ul style="list-style-type: none"> • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process. 	VTC SSH Username field.	Enter the string.	VTC SSH Username field.	Enter the password.																								
VTC SSH Username field.	Enter the string.																												
VTC SSH Username field.	Enter the password.																												

VMTP	<p>Check one of the check boxes to specify a VMTP network:</p> <ul style="list-style-type: none"> • Provider Network • External Network <p>For the Provider Network complete the following:</p>	
	Network Name field.	Enter the name for the external network.
	IP Start field.	Enter the starting floating IPv4 address.
	IP End field.	Enter the ending floating IPv4 address.
	Gateway field	Enter the IPv4 address for the Gateway.
	DNS Server field.	Enter the DNS server IPv4 address.
	Segmentation ID field.	Enter the segmentation ID.
	Subnet	Enter the Subnet for Provider Network.
	For External Network fill in the following details:	
	Network Name field.	Enter the name for the external network.
	Network IP Start field.	Enter the starting floating IPv4 address.
	Network IP End field.	Enter the ending floating IPv4 address.
	Network Gateway field	Enter the IPv4 address for the Gateway.
	DNS Server field.	Enter the DNS server IPv4 address.
	Subnet	Enter the Subnet for External Network.
<ul style="list-style-type: none"> • Click Offline Validation . • When Offline Validation is successful, click Reconfigure to commence the process. 		

<p>Networking</p> <p>In Reconfigure optional services networking, you can reconfigure IP tables, or add http_proxy/https_proxy.</p>	<p>To reconfigure networking, update the relevant information:</p> <table border="1" data-bbox="901 283 1521 688"> <tr> <td data-bbox="901 283 1214 415">IP Tables</td> <td data-bbox="1219 283 1521 415">Click Add(+) to add a table. Enter input as subnet format. E.g. 12.1.0.1/2</td> </tr> <tr> <td data-bbox="901 415 1214 548">http_proxy_server</td> <td data-bbox="1219 415 1521 548">Enter HTTP_PROXY_SERVER E.g. <a.b.c.d:port></td> </tr> <tr> <td data-bbox="901 548 1214 688">https_proxy_server</td> <td data-bbox="1219 548 1521 688">Enter HTTP_PROXY_SERVER E.g. <a.b.c.d:port></td> </tr> </table> <ul style="list-style-type: none"> • Click Save. • Click Offline Validation. • When Offline Validation is successful, click Reconfigure to commence the process. 	IP Tables	Click Add(+) to add a table. Enter input as subnet format. E.g. 12.1.0.1/2	http_proxy_server	Enter HTTP_PROXY_SERVER E.g. <a.b.c.d:port>	https_proxy_server	Enter HTTP_PROXY_SERVER E.g. <a.b.c.d:port>
IP Tables	Click Add(+) to add a table. Enter input as subnet format. E.g. 12.1.0.1/2						
http_proxy_server	Enter HTTP_PROXY_SERVER E.g. <a.b.c.d:port>						
https_proxy_server	Enter HTTP_PROXY_SERVER E.g. <a.b.c.d:port>						
<p>APICINFO</p> <p>Note Reconfigure optional services only APIC hosts can be reconfigure.</p>	<p>To reconfigure APICINFO, follow the process:</p> <ul style="list-style-type: none"> • Enter input for APIC hosts format. <ip1 host1>:[port] or eg.12.1.0.12 • Click Save. • Click Offline Validation. • When Offline Validation is successful, click Reconfigure to commence the process. <p>Note APIC hosts can be reconfigure minimum 1 host and max 3 but not 2 hosts.</p>						
<p>Vim_admins</p>	<p>To reconfigure vim_admins, follow the process:</p> <ul style="list-style-type: none"> • To add a new root user, Click + and add the Username and admin hash password (Starting with \$6). • To remove the existing user, Click -. • When Offline Validation is successful, click Reconfigure to commence the process. 						

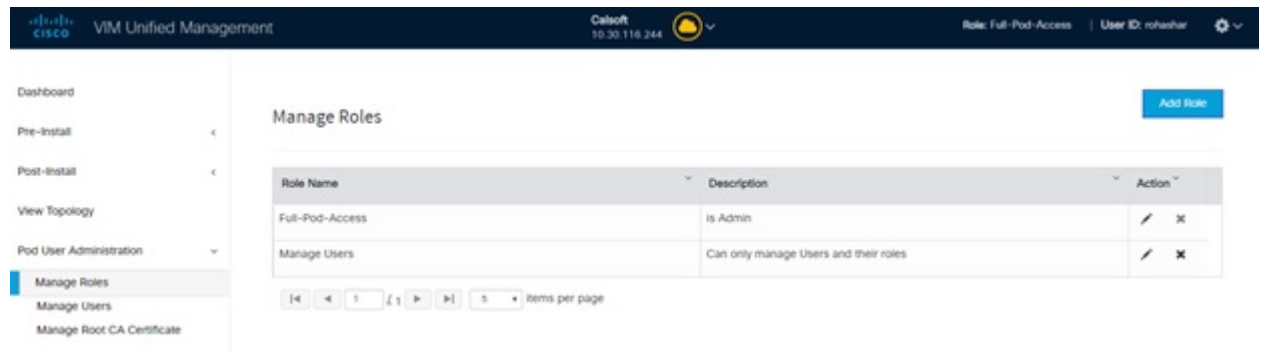
Pod User Administration

Cisco VIM UM offers Users (Pod Admins or Pod Users) to manage Users and roles that are associated with them.

Managing Roles

User can create multiple Roles and assign them to other pod users. System has a default role that is named as Full-Pod-Access which is assigned to the person who registers the Pod.

Manage Roles



Step 1 Click **Login as POD User**.

Step 2 Navigate to **Pod User Administration** and click **Manage Roles**. By default you see full-pod-access role in the table.

Step 3 Click **Add New Role** to create a new role.

Step 4 Complete the following fields in the **Add Roles** page in Cisco VIM UM:

Field Name	Field Description
Role	Enter the name of the role.
Description	Enter the description of the role.
Permission	Check the Permission check box to select the permission.
Click Save .	Once the Blueprint is in Active state all the permissions are same for C-series and B-series Pods other than Reconfigure CIMC Password which is missing for B-series Pod.

Note Permissions are divided in the granular level where viewing **Dashboard** is the default role that is implicitly added while creating a role.

Note Permissions are divided in the granular level where viewing **Dashboard** is the default role that is implicitly added while creating a role.

Managing Users

This section allows you to add the users. It shows all the users associated with the Pod. You can check the online status of all the user. Click **Refresh** on upper right corner to check the status.

User Name	Email ID	Role Name	Is Registered	Online	Action
Rohan R	rohanshar@cisco.com	Full-Pod-Access	YES	Online	[Edit] [Delete]
Aniket C	achothte@cisco.com	Manage Users	NO	Offline	[Edit] [Delete]

To add a new user:

- Step 1** Click **Login as POD User**.
- Step 2** Navigate to **POD User Administration** and click **Manage Users**.
- Step 3** Click **Add Users** to add a new user.
- Step 4** Complete the following fields in the **Add Users** pane of the Cisco VIM Insight:

Field Name	Field Description
Email ID	Enter the Email ID of the User.
User Name	Enter the User Name if the User is new. If the User is already registered to the Insight the User-Name gets auto-populated.
Role	Select the Role from the drop-down list.

- Step 5** Click **Save** Once the Blueprint is in Active state all the permissions are same for C-series and B-series Pods other than Reconfigure CIMC Password which is missing for B-series Pod.

Revoke Users

User with Full-Pod-Access or Manage Users permission can revoke other users from the specific Pod.

To revoke users:

- Step 1** Click **Undo** icon. A confirmation pop up will appear.
- Step 2** Click **Proceed** to continue.

Note Self revoke is not permitted. After revoking the another user, if the user is not associated with any other pod then the revoked user will be auto deleted from the system.

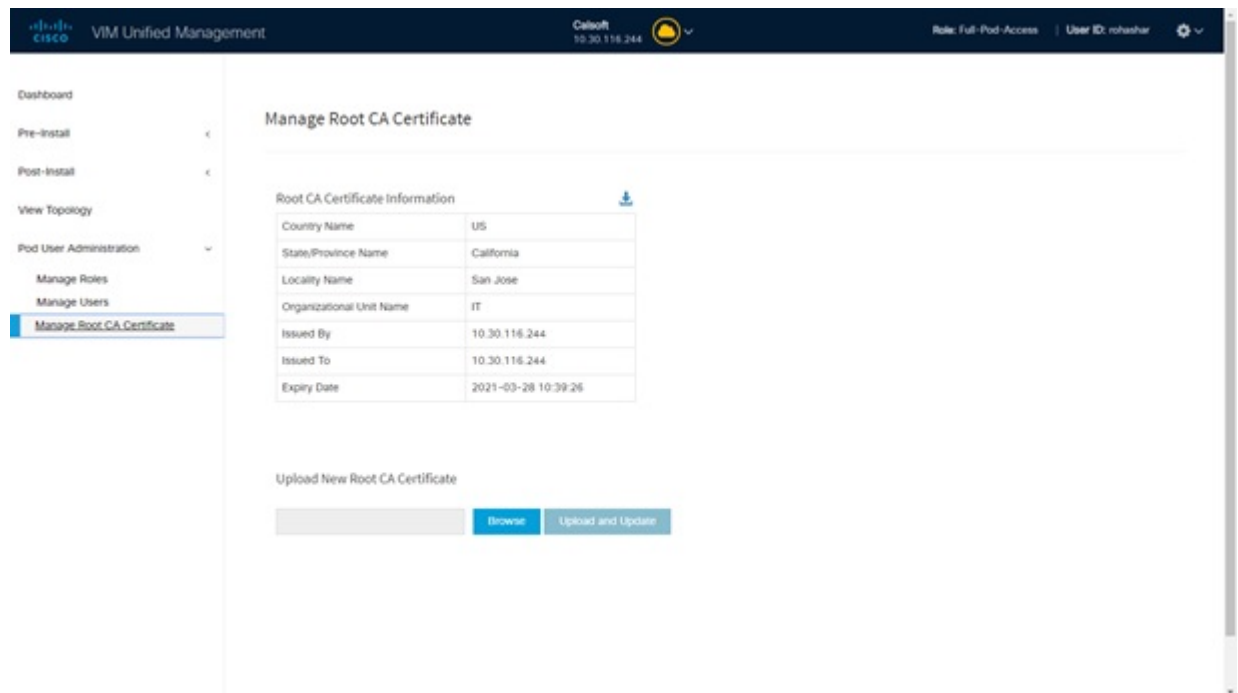
Edit Users

User with Full-Pod-Access or Manage Users permission can edit other user's permission for that specific Pod.
To edit user's permission

- Step 1** Click **Edit** icon.
- Step 2** Update the permission.
- Step 3** Click **Save**. The Grid will get refreshed automatically.

Managing Root CA Certificate

You can update the CA Certificate during the registration of the POD. Once, logged in as POD User and if you have the permission to update the certificate you can view under POD User Administration>> Manage Root CA Certificate.



The screenshot shows the 'Manage Root CA Certificate' page in the Cisco VIM Unified Management interface. The page includes a sidebar with navigation options like 'Dashboard', 'Pre-install', 'Post-install', 'View Topology', and 'Pod User Administration'. The main content area displays the following information:

Root CA Certificate Information	
Country Name	US
State/Province Name	California
Locality Name	San Jose
Organizational Unit Name	IT
Issued By	10.30.116.244
Issued To	10.30.116.244
Expiry Date	2021-03-28 10:39:26

Below the table, there is a section titled 'Upload New Root CA Certificate' with a file input field, a 'Browse' button, and an 'Upload and Update' button.

To update the Certificate:

- Step 1** Click **Login as POD User**

Step 2 Navigate to **POD User Administration>>Manage Root CA certificate**.

Step 3 Click **Browse** and select the certificate that you want to upload.

Step 4 Click **Upload**.

- If the certificate is Invalid, and does not matches with the certificate on the management node located at (var/www/mercury/mercury-ca.crt) then Insight reverts the certificate which was working previously.
- If the Certificate is valid, Insight runs a management node health check and then update the certificate with the latest one.

Note The CA Certificate which is uploaded should be same as the one which is in the management node.
