Managing Cisco VIM through Unified Management

This funcationality brings in clear separation of roles. It does not store any pod related details obtained directly through Rest API from the pods locally, except for RBAC information.

UI Administrators Privileges and Responsibilities

The Unified Management UI Admin has the following privileges and responsibilities:

1. Unified Management UI Admin(s) can only add Pod Admin. The Pod Admin can be added in two ways:
   - Local database
   - LDAP with registration type as mail, uid, cn or group.
2. Unified Management UI Admin can manage all the users in Unified Management from **Manage Pod Users**.
   - UI Admin can revoke permission of Users: If UI Admin wants to revoke a user from a Pod, click **Revoke permission** icon under Action column.
   - UI Admin can delete a User: If UI Admin wants to delete a user from the UM, Click **Delete** icon under Action column. If there is only one user associated with a Pod then UI Admin needs to delete the pod and then delete or revoke the user permission.
3. Unified Management UI Admin can manage Pod Admin(s) from **Manage Pod Admin**.
   - UI Admin can add a new Pod Admin in Unified Management.
   - UI Admin can revoke permission of a user or LDAP group from being a Pod Admin.

4. Unified Management UI Admin can manage Pods from Manage Pods.
   - UI Admin can delete a Pod from Unified Management.
   - UI Admin can also update password for the REST incase there was a system update on the pod and REST password was changed in that process.
5. Unified Management UI Admin can manage other UI Admin(s) from **Manage UI Admin Users**.
   - Unified Management UI Admin can add another UI Admin.
   - Unified Management UI Admin can revoke permission of the user from being an UI Admin.

Note If there is only one UI Admin for Unified Management, the revoke permission icon is disabled for the user.

Pod UI Privileges and Responsibilities

As Cisco VIM is Rest API based, you can manage a pod through CLI, Rest API or UI. You can always bring in a partial or fully functional Pod and register with VIM UM. UM queries the pod status through Rest API and reflect the same.

Note We recommend the admin to choose only one path to manage the pod.

Adding Cisco VIM Pod

Before you begin

Complete the following pre-requisites to add a Cisco VIM pod:

- Bootstrap of VIM Unified Management must be complete and successful.
- UI and Pod Admin must be available.

Step 1 Navigate to https://br_api:9000

Step 2 Click **Register Management Node** link. Options for selecting IPv4, IPv6, and FQDN are displayed. Checking one of these options displays the corresponding input fields for IPv4, IPv6 and FQDN respectively.

- Enter the endpoint IP (IPv4/IPv6) which is the **br_api** of your pod, or add FQDN address.

  Note Perform the runtime validation to check if the endpoint IP is already registered to Unified Management. No validation is available for IPv6 and FQDN.

- Give a name or tag for the pod you are registering.
- Enter the REST API password for the Pod.

- You can locate the REST API password on the pod you are registering.
- The path to locate REST API password is : /opt/cisco/ui_config.json.

- A brief description about management node. Description field is optional and can be left blank.
- Enter the email ID of the Pod Admin.
  - Run time validation to check if the email ID is Pod admin or not.
  - If False, the Unified Management gives an error that the User is not registered as Pod Admin.
  - If True, the User Name is auto-populated and the **Register** button is enabled.

Step 3 Click **Browse** to upload restapi server CA Certificate. This is enabled once the Pod Admin validation is successful.

- Navigate to `/var/www/mercury/mercury-ca.crt` of the management node.
- Download the Certificate to the local machine and upload the certificate using Unified Management.

Validation check for file size and extension is done as a part of upload and in case of failure the Certificate is deleted and you need to upload the valid certificate again.

If the Certificate is uploaded successfully then **Register** button is enabled. To do a management node health check click **Register**.

- If the REST API service is down on the management node then a failure message will be displayed as : Installer REST API service not available. The certificate will not be deleted.
- If the Certificate is invalid and there is a SSL connection problem with the management node then certificate is deleted and message is displayed to upload the certificate again.
- If the Certificate is valid user is redirected to the login page with a message- management node registered successfully.

Step 4 Click **Register** to redirect the user to the landing or login page. Pod Admin receives the notification mail that the management node is registered successfully.

Note If UM_ADMIN_AS_POD_ADMIN is set to True, all UM-Admins are added as pod-users with **Full-Pod-Access** during pod registration.

Step 5 If you encounter an error stating **Certificate file size is more than allowed limit** during pod registration, use a script to change the default value of the size of your certificate file to 4000 bytes. To change the default value, follow the below procedure:

a) Navigate to Insight installer directory on the UM node: `/root/insight-<tag_if>/tools/`
b) Execute the script: insight_cert_size_change.sh:

```
/insight_cert_size_change.sh -s <pass the size in bytes>
```

Note Ensure that you pass the value in bytes as it might decrease the limit from the default value.

.

c) Once the script is executed, Insight service is restarted automatically with the new file size check.
d) Follow the above steps to register the management node again.

Editing Pod from Cisco VIM Unified Management

You can edit the pod by following the below steps:

Step 1 Log in as the UM UI Admin

Step 2 In the navigation pane, click **PODS**

Step 3 Choose the pod that you want to EDIT in the **Action** column.

Step 4 In the **Edit Pod** popup window, you can edit the **Node name** and **Description**.

Step 5 Click **Save** to update the Pod.

Deleting Pod from Cisco VIM Unified Management

When you delete a Pod from Cisco VIM UM, you are not deleting the Pod from your OpenStack deployment.

Before you begin

Following the steps to delete a Cisco VIM Pod:

- Bootstrap of VIM Unified Management is complete and successful as per the install guide.
- At least one UI and Pod Admin exists as per the install guide.
- The UM manages the targeted Pod.

Step 1 Log in as the **UM UI Admin**.

Step 2 In the navigation pane, click **Manage Pods**.

Step 3 Choose the pod that you want to delete in the Action column and click **Delete**.

Step 4 Click **Proceed**, to confirm the deletion.

Context Switching Within Unified Management

Cisco VIM UM has permissions to switch between two or more pods for a particular node. The user can be a admin for one or more pods, and a normal user for some other pod, simultaneously. Ability to access multiple pods, provides the user to maintain context and yet scale from a pod management point of view.

There are two ways a user can switch to another pod.

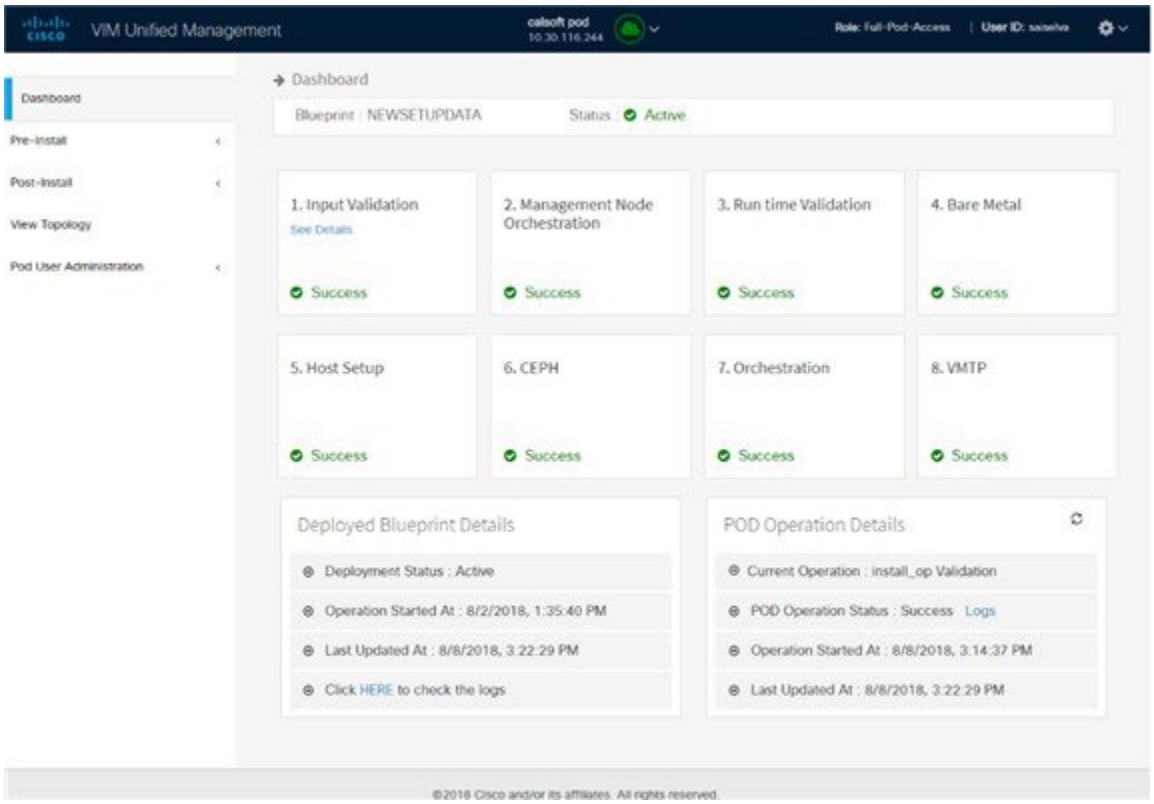
- **Context Switching Icon**: Context Switching Icon is situated on the top right corner and is the third icon from the right tool tip of the UI. Click **Context Switching** Icon to view all the pods that you can access. Pod with a red dot indicates that the REST Password that is entered during registration of the Management node does not match with the current REST Password for that of particular node. In such a situation the

Pod admin or User has to reach out to UI admin to update the password for that Node. UI admin updates the password from Manage Pods in Unified Management UI admin Portal.

- **Switch Between Management Nodes**: Switch Between Management Nodes is available in the Dashboard. The user can see all the pods in the table and can navigate to any Pod using a single click. If mouse pointer changes from hand or cursor to a red dot sign it indicates that the REST Password entered during registration of Management node does not match with the current REST Password for that particular node.

Dashboard

After selecting a Pod from landing page, you will be redirected to the **Dashboard** of that particular Pod.



Blueprint Name

Blueprint section provides the name of the Blueprint, the health status of the blueprint and the various installation stages with the status. The different status is Success, Failed or Not Run.

Click **Next and Previous**, you can navigate between various installation stages.

Deployed Cloud Status

This section highlights the cloud status on the Pod.

- Active (Green): If the cloud is deployed without any failures.
- Failed (Red): If the cloud deployment fails.
- Not Available (Gray): If the cloud is not deployed on the Pod.

Deployed Blueprint Details

In this section you get information about deployed blueprint which includes Deployment Status, Operation start time, Operation update time, and a link to the log of last operation. In case of the failure of cloud installation, the name with keyword regarding component failure is visible as Deployment Status.

Pod Operation Details

The Pod operation details table provides information regarding the current and last operation which includes Current operation details, Pod operation status and information about the operation start time and update time. Refresh icon facilitates the user to fetch latest operation status from the Pod.