Integrating with Prime Service Catalog

This chapter consist of the following topics:

Overview

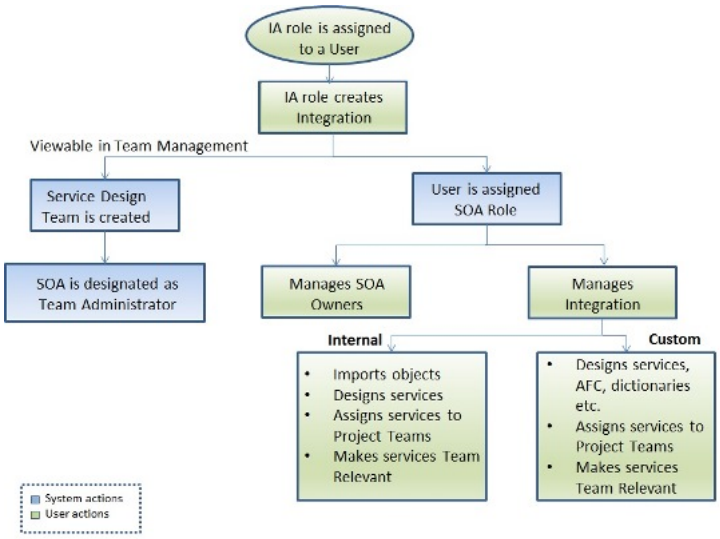
The integrations module is a one stop for all integrations with Prime Service Catalog. The home page of the integrations module offers two tabs, Internal and Custom:

- The **Internal** tab allows you to connect with and manage the third party applications integrated with Prime Service catalog such as UCSD, CloudCenter, Process Orchestrator, AMQP, Web Services, Guacamole servers, Solr and so on. For details on integrating Prime Service Catalog with each of the supported applications see section Integrating with Third Party Applications.
- The **Custom** tab allows you to create and manage service groups and Service Item Groups. For detailed information on creating and managing custom Integrations see Creating Custom Integrations, on page 7.

Note Service Groups and Service Item Groups can no longer be created from Service Designer module.

The approach to managing services from new integrations and SIBD services is revamped to support Team Management with enhanced user experience. The below image depicts the entire workflow of the user roles involved in integrations, system actions, and capabilities of the users.

Figure 1: Workflow of Managing Services



Site Administrator can create and manage all integrations in the system. However, the site administrator can choose to delegate this responsibility to another user. To create an integration, the user must be assigned the Integrations Administrator (IA) role. See section Creating Integrations Administrator, on page 3 to assign IA role to a user. A user with IA role can now access Integrations module. On the Integrations page, only those connections are displayed that are owned by the logged in user.

Using the New Integrations option IA can create a new internal or custom integration. On creation of an integration, the IA user is assigned System Operations Administrator (SOA) role automatically and can manage that particular integration. This implies, SOA role is specific to the integration and all the operations within that connection. The SOA can now perform operations such as Manage SOA Owner, on page 5, Assign Services to Project Teams, on page 6, and Make Services Team Relevant, on page 7. For more details on each of these roles see section Understanding Roles and Capabilities, on page 3.

For each Integration, the system generates a corresponding Service Design team and the SOA is designated as Team Administrator of this team. If Team Management is activated, the Service Design team details is viewable in Team Management module. The purpose of Service Design team is to provide the SOA and members of the team a comprehensive view of all the data pertaining to the integration in one place. For more details on Service Design teams see section Service Design Teams.

Understanding Roles and Capabilities

This section covers the roles and capabilities of all the roles within the scope of Integrations module.

Site Administrator

This module is mainly used by the Integrations Administrator and Service Operations Administrator to create and manage the integrations (internal and custom). However, some integrations can be created and managed only by the Site Administrator, such as AMQP, Web Services, and Apache Solr.

Creating Integrations Administrator

As a Site Administrator you must create an Integrations Administrator, who is well aware of the applications to be integrated with Prime Service Catalog. The Integrations Administrator role creates and manages UCSD, CloudCenter, Process Orchestrator, and UCS PM Integrations. This role can also create and manage custom integrations such as Service groups and Service item group.

The very first Integrations Administrator must be created by ordering the service *Create Integrations Administrator* from Service Catalog. Assign a user in the system as Integrations Administrator from the Search for Recipient pop up and click **Submit**.

In case you have upgraded from previous version of Prime service Catalog, for all existing integrations you must manually map the user who manages those integrations with the Service Operations Administrator role.

Note The Service Administrator role in Prime Service Catalog 12.0 release has been deprecated in the 12.1 release. In case you are upgrading from Prime Service Catalog 12.0 to 12.1 release, all users who were granted Service Administrator role will automatically be granted the role of Integrations Administrator.

Integrations Administrator (IA)

The Integrations Administrator (IA) role creates connection with third party applications such as UCSD, CloudCenter, UCS PM, and so on. The IA also has capabilities to create custom integrations. When an IA creates a connection, the SOA role specific to the connection or Service Group is automatically assigned to the IA. In addition, for every connection a corresponding Service Design Team and Service Groups are created. The SOA is assigned as the team admin for the Service Design Team.

Initially, the IA is allowed to access Integrations and Order Management modules. Once the IA creates a connection and imported the objects, the IA gains access to the Service Designer and Service Item Manager modules as well.

Service Operations Administrator (SOA)

SOA role is a integration specific role i.e., the SOA can access and manage only the integration owned by the SOA. As a result SOA can also view service items and orders of entire integration in the Service Designer module. SOA user is allowed access to the Integrations, Service Designer, User Management, Service Manager and Service Item Manager modules. This user has the capability to assign or unassign the services of the

connection to project teams. Only the assigned services will be available for the team administrator to make them orderable for the users.

The SOA has the following permissions:

- Service Group Level
  - View services and other information in this service group
  - Assign rights
  - Design Services and change data in this group
  - Order Services
- Read and write permission on all roles, groups, people, teams, and OUs
- Service item Instance- Create New Instance data
- Standard-create new Standard Instance data

Integrating with Third Party Applications

The **New Integration** option lets you to integrate Prime Service Catalog with other applications. The below table lists the supported integrations and reference to the detailed information in the Prime Service Catalog documents:

Application	Permissions	Reference to sections
Cisco UCS Director	IA- Create integration SOA- Manage integration	Integrating UCS Director (UCSD) or VACS with Prime Service Catalog, on page 12
Cisco CloudCenter	IA- Create integration SOA- Manage integration	Integrating CloudCenter with Prime Service Catalog, on page 29
Cisco UCS Performance Manager	IA- Create integration SOA- Manage integration	Integrating Performance Manager with Prime Service Catalog, on page 32
Cisco Process Orchestrator	IA- Create integration SOA- Manage integration	Integrating Process Orchestrator with Prime Service Catalog, on page 35
AMQP	Only Site Administrator can create and manage the integration	Managing AMQP Connections, on page 41
Generic Web Service	IA- Create integration SOA- Manage integration	Managing Webservices Connections, on page 44
Single Sign-On such as SAML	Only Site Administrator can create and manage the integration	SAML Configurations, on page 38

Application	Permissions	Reference to sections
Generic Guacamole server	IA- Create integration SOA- Manage integration	Integrating Guacamole Server with Prime Service Catalog, on page 45
Apache Solr	Only Site Administrator can create and manage the integration	Integrating Apache Solr Search Platform, on page 47

Note The **Manage Connection** option in Administration module has been deprecated. If you have upgraded from a previous version of Prime Service Catalog, all existing connections will show up on the Integrations page.

Manage Integrations

Once the new integration is added, depending on the type of applications it offers different options to manage the integration. The below explained tasks may not be applicable for all types of integrations.

The Manage Integration option allows the SOA of the connections to modify the connection and handle connection specific tasks.

Manage SOA Owner

Once the IA has created a connection he assumes the role of SOA for that connection automatically. This person can, however, choose to share or transfer the SOA role for this connection with any other user. This option is available only for the connections with UCSD, CloudCenter, Process Orchestrator, and Performance Manager and custom integrations.

The Manage Integration Owners page lists all the SOAs for this connection.

To share or transfer SOA role:

Step 1 Go to the Integrations page and choose the **Manage SOA Owners** from the settings icon.

Step 2 Click **Associate SOA** .

Step 3 Click on the search icon to search for users, select the users from the list and click **Add** to available on added users list .

The added users are displayed in the panel below. To remove the SOA privilege from user, select the user and click **Remove**.

Step 4 Choose Share or Transfer based on your requirement.

- Share-SOA privilege is shared with the chosen users. All the SOAs of the connection have equal privilege on the connection.
- Transfer-the user loses the SOA privilege and transfers the privileges to some other user. The user then cannot access the connection.

Step 5 Click **Submit**.

Note
- The SOA of any connection can share the SOA privilege to any other user.
- The transfer option is disabled for the Site Administrator. Site administrator can only share the SOA privilege.

Show Log

The show log option displays the status logs pertaining to the connection. These logs help you analyze the status of the services imported and the time of the last sync. **Refresh** triggers sync between Prime Service Catalog and the application, and updates any changes in the services imported.

Test Connectivity

Once the connection is created, use the **Test Connectivity** option to authenticate the credentials.

Remove

You can delete a integration by selecting the **Remove** option. This will delete the integration along with:

- Its imported entities such as virtual machines, VDCs, containers, templates, catalogs, and workflows.
- All SOA roles of the integration.
- All permissions on the services related to the integration for a custom role.

Note As an exception, when a CloudCenter connection is deleted, all the associated entities pertaining to this connection would remain in the system.

Launch VM Client

When this option is selected you can access the VMs on the web browser without any SSH Client. This option is available only if Guacamole or VMRC Server is configured in Prime Service Catalog.

Assign Services to Project Teams

Once the services are imported to Prime Service Catalog, you must manually assign the services to teams that are authorized to avail these services. Only the assigned services can be ordered by the project team members. Assigning services to project teams alone will not allow the team members to order the services. The team administrator of the Project team, however, can use their discretion to choose from these assigned services and makes them orderable to the team members.

To assign services to teams:

Step 1 For the selected connection, select Manage Integrations.

Step 2 From the Discovered panel, select the Services tab.

Step 3 Choose the services that you want to assign a team and click **Assign to Teams**.
From the Select Teams pop-up, choose the teams that are authorized to order this service and click **OK**.

The selected teams and their assigned services are displayed in the *Teams with Assigned Services* panel.

To remove the assigned services:

From the Teams with Assigned Services panel, choose the services to be unassigned from the team and click **Remove**.

Make Services Team Relevant

You can configure how the services can be ordered for teams. Marking the services or Service Groups as Team Relevant makes it easier for the user to order services for only those teams that have the permission to order the service. Depending on the services granted to the user (directly or inherited) you can allow the user to choose for which team the service is being ordered.

If a service is marked team relevant, means that when ordering that service, it must be ordered for a specific team. The order form displays an additional field called *Team Name*. This field displays only those teams to which the user belongs and also has permission to order this service.

Some services may have been marked as Team Relevant by default but this feature comes into affect only when Team management is activated. This setting can be modified at Service Group level or at individual service level from the Service Designer module. For more information see section *Making Services Team Relevant* in Cisco Prime Service Catalog Designer Guide.

Creating Custom Integrations

Service Groups and Service Item Group can now be created only as a Custom integration. However, the service groups and service item groups must be configured in Service Designer module. Service Groups and Service Item Group are logically grouped and assigned to the SOA role.

Service groups are created to group similar services. At the service group level you can configure authorization processes, ordering permissions, and escalation notifications. These configurations are inherited by all the services in the group. You can also set whether the service group is Team Relevant or not at Service group level or at service level. For detailed information on configuring service groups, see section *Configuring a Service Group of* Cisco Prime Service Catalog Designer Guide.

Service Item group is a logical grouping of various service items. You must create a service item group to add related service items. For example, create a service item group called hardware to be able to add various service items like laptop, mouse, and so on. On the custom integration page only those integrations are displayed that are owned by the logged in user. For detailed information on configuring service Item groups, see section *Managing the Services and Attributes* in Cisco Prime Service Catalog Designer Guide.

To create a service group:

Before You Begin

- Choose an Organizational Unit (OU) or people who will review a service request, approve service request and also handle escalations.
- You must have Service Lifecycle Management roles assigned and appropriate permissions to access Service Item manager.

Step 1 Choose Custom tab in the Integrations module.

Step 2 Click **New Custom Integration.**

Step 3 Enter a Name and Description for the Service Group and Service Item Group and click **Add**.
The name for the Service Group should be specific to your organization and needs. End users do not see this name, and the name is editable after service group creation. Sample names include "End User IT Desktop Support," "End User IT Desktop Software," or "Identity Management". A brief description for the service group; optional but recommended.

The Service Group that you created is displayed as one of the custom integration under the Custom tab. On each Custom Integration you can perform tasks such as, Manage Integration, Manage SOA Owners, Remove, and Navigate to Service Designer.

Manage Integrations

Manage Integrations option from the settings allows you to edit the service group. This page displays the general details of the group, whether the group is marked as relevant or not, and displays the services belonging to the service group.

To edit a service group:

Step 1 Choose Custom tab in the Integrations module.

Step 2 Select the Service Group that needs to be edited and choose **Manage Integration** option from the settings.

Step 3 Click **Edit** to update the general details and to set 'Team Relevant' status at group level. For more information on team relevant services see section Make Services Team Relevant, on page 7.
To set only certain services within the service group as team relevant, you would need to navigate to service designer module. For more information see section Setting Services as Team Relevant in Cisco Prime Service catalog Designer Guide.

Step 4 Click **Update**.

Manage SOA Owners for Custom Integrations

The manage SOA is similar to managing SOA for internal connections. For more details see section Manage SOA Owner.

To share or transfer SOA role for Custom Integrations:

Step 1 Choose connection and select **Manage SOA Owners** option from the settings icon.

Step 2 Click **Associate SOA**.

Step 3 Choose *Share* or *Transfer* based on your requirement and click **Submit**.

- In case of share SOA role, all the SOAs of the connection have equal privilege on the connection.
- In case of transfer SOA role, the IA loses the SOA privilege and assigns the privileges to some other user. The IA then cannot access the connection. This option is available only for an IA user.

Note The SOA of any connection can share the SOA privilege to any other user.

Assigning Services to teams

Assigning Services to team for custom integrations is similar to the internal integration. For detailed procedure see section Assign Services to Project Teams.

Remove

To delete a Service group:

Step 1 Choose connection and select **Remove** option from the settings icon.

Step 2 Click **OK** on the confirmation message.

Navigate to Service Designer

To proceed further with tasks listed below click on the **Navigate to Service Designer** module.

- Configuring authorization and escalation processes for services in the group
- Configuring permission to order services in the group
- Assigning functional positions that are used by the group
- Creating service items
- Creating services that delivers them
- Making these services orderable

Providing Infrastructure as a Service (IaaS) using Prime Service Catalog

Cisco Prime Service Catalog integrated with UCS Director provides single self-service ITaaS catalog for the self-service provisioning and lifecycle management of VMs in the private and hybrid cloud workloads. You can provide services such as provisioning virtual machines on a private cloud using UCS Director and perform the lifecycle operations on these public and private VMs. This section covers the infrastructure services such as virtual machines, fenced containers, Virtual Application Container Services (VACS), and APIC Container Catalog on UCS Director.

Note

- VACS containers are verified and certified only on UCS Director 5.2 platform.
- The public cloud operations are verified and certified on Amazon Web Services (AWS).

Prime Service Catalog also supports Advanced Catalogs from UCS Director. These advanced catalogs are a wrapper around workflows defined in the UCS Director. Prime Service Catalog creates services for these advance catalogs during the UCS Director discovery process. Out of box, these Advanced Catalog-based services can only create requests or objects in UCS Director and do not have any service item dictionary associated with them. However, these generated services can be customized to manage life cycle of objects created through Advanced Catalogs. These services can be customized by adding a service item dictionary, and populating the dictionary with conditional rules. Then, lifecycle operations for the service item can be added via associated services for the service item.

Note Prime Service Catalog currently does not support the popup table input type for UCS Director advance catalog workflow.

Using Prime Service Catalog for Cloud IaaS, you can:

- Create orderable services for VMs and infrastructure containers in hybrid cloud using a unified web interface after integrating with UCS Director. For more information, see Integrating UCS Director (UCSD) or VACS with Prime Service Catalog.
- Create orderable services for VACS bound VMs and containers.
- Create orderable services for UCS Director based advance catalogs.
- Provide multi-tenant IaaS based on ACI using UCS Director. For more information, see Providing Multi-Tenant IaaS.

Configuring Email Notification on VDC Creation

You receive an email notification when you create a VDC or a standard virtual machine. A VDC can be an APIC, fenced, or VACS container, and a virtual machine can be a standard virtual machine or a cloned virtual machine. You also get an email notification while adding a virtual machine to a Fenced and VACS container.

When you order a new VDC successfully, an email notification is sent out, which includes VDC service item details, VDC subscription data, and specific details of the VDCs such as name, display name, description,

cloud name, and status of the VDC with its corresponding virtual machines. You can view the details of all the virtual machines of a particular VDC.

For information on VDC creation, see the "Virtual Data Centers" section in the Cisco Prime Service 11.1.1 User Guide.

For the email notification to work, the following settings must be done:

1. Set the SMTP properties in the **Administration** module. These properties are, "Mail Server Address", "Mail Server Port", and "Support Email Address".
2. FTL files must adhere to the following guidelines:
   - FTL files are well formed. This includes naming the tags properly, ensuring that every opening tag has a closing tag, ensuring that at least one "to" address exists, in addition to the other precautions mentioned above.
   - FTL files must be placed in some custom template folder and the fully qualified path name to the folder must be specified in **Administration > Settings > Path of the folder containing the FTL files**. The path should navigate to the folder containing the FTL files and not the files itself. By default, these FTL files are available in the "RequestCenter.war/WEB-INF/classes/config/templates/ folder.
   - The FTL file path must be in Linux convention (which is a/b/c/d and not a\b\c\d) andmust mandatorily end with '/'.
   - For clustered environments, the URL *ObjectCache.Application.URL* must be hardcoded in the *Newscale.properties* file.
   - For clustered environments, each node must have the FTL files in the same folder, and this folder must exist in every node.
   - FTL files naming convention must not be changed. The FTL files should remain as follows:
     - create_vdc_fen.ftl—For creating Fenced Container VDC
     - create_vdc_apic.ftl—For creating APIC Container VDC
     - create_vdc_vacs.ftl—For creating VACS Container VDC
     - add_vm_fen.ftl—For adding a VM of a Fenced container
     - add_vm_vacs.ftl—For adding a VM to a VACS container
     - vm_operation.ftl—For cloning a VM of a Fenced container and an APIC container, and creating a Standard VM.
3. You can view, modify, show, hide, or remove the FTL file according to your requirement, but do not change the naming convention of the FTL files, as mentioned above. You can view all the details that are included in the email notification.

You can add more than one email address in the **To** field separated by a comma. This field can also contain namespaces, the supported namespaces are: #Requisition.Customer.Email#, #Requisition.Submitter.Email#, #Requisition.Customer.Supervisor.Email#. The To field can also contain a combination of email address and namespace separated by comma. The **From** field is optional. If used, this field can contain only one email address and must not be empty. By default, it is Support Email Address mentioned in the **Administration > Settings** tab. The **Subject** field of the email template can also be customized with a custom subject line for the email. The Subject field of Email Templates can now store up to 2000 characters.

Note By default, the <from> field has ToBeFilled as the value. If you want to use the <from> field, edit this field with an appropriate and valid email address. If you do not want to use the <from> field, remove this field or comment it out in the FTL. If the FTL is used as is as provided out of the box, then it would result in an error, since ToBeFilled is not a valid email address.

Apart from the customizations mentioned above, you can also add any static text inside of the FTL template. For this, no special tags need to be used. You can just mention the static text as is. The "subject" field of the email template can also be customized with a custom subject line for the email.

Generating Orderable Services for UCS Director Entities

For creating orderable services for provisioning VMs in cloud, you must perform the following steps:

	Steps	Topics
Step 1	Integrate UCS Director with Prime Service Catalog.	Integrating UCS Director (UCSD) or VACS with Prime Service Catalog, on page 12
Step 2	Discover the IaaS entities from UCS Director.	
Step 3	Set up automatic or manual synchronization with UCS Director.	Managing UCS Director Synchronization
Step 4	• Configure search facets, permissions, and presentation for hybrid cloud provisioning services in Prime Service Catalog. • Set up the display category for these cloud services.	• Configuring Permissions and Presentation for Private and Hybrid Cloud Services • Configuring Display Categories for Private Cloud Services

Based on the permissions, end users can now order the hybrid cloud services and perform lifecycle operations on the provisioned containers and virtual machines. For more information on ordering these services, and on the available lifecycle operations for the UCS Director entities, see Cisco Prime Service Catalog 12.1 User Guide.

Integrating UCS Director (UCSD) or VACS with Prime Service Catalog

Using Prime Service Catalog, you can provide infrastructure resources as services and application stack as a service by integrating with Cisco UCS Director (UCSD) and Cisco Virtual Application Container Services (VACS) application. You can manage VMs in hybrid cloud using a unified web interface in Prime Service Catalog after integrating with UCS Director. After integrating with UCS Director and VACS, the types of infrastructure services available in Prime Service Catalog are:

- Container templates, container catalogs, standard catalogs, and advance catalogs from UCS Director

- Container catalog services and container template services from VACS. VACS template services includes a CSR Virtual Machine, VSG Virtual Machine, and application Virtual Machines.

Prerequisites

- To establish an SSL connection, you must add an SSL certificate to the UCS Director or VACS. You can use:
  - A self-signed certificate that matches the hostname or IP address of the UCS Director or VACS server.
  - (Recommended) An SSL certificate that matches the Fully Qualified Domain Name (FQDN) of the UCS Director server signed by a trusted certificate authority.
- If LDAP is integrated, Prime Service Catalog and UCS Director must be integrated with the same LDAP to support single sign-on.
- If you are planning to connect to a UCS Director instance that is integrated with an LDAP, do the following in Prime Service Catalog :
  1. Go to **Administration module > Directories tab > Mappings**.
  2. Map the **Login ID** and **Person Identification** attributes to userPrincipalName.

  Failing to map the above attributes may result in duplicate user accounts in Prime Service Catalog after the UCS Director import.
- Make sure the UCS Director is configured in English.

Step 1 Login to Prime Service Catalog as the Integration Admin user.

Step 2 From the main menu, choose **Advanced Configuration > Integrations** and click **New Integrations**.

Note To integrate Prime Service Catalog with VACS, follow the same procedure, which is used to integrate Prime Service Catalog with the UCS Director. However, in this case, you will need to provide the VACS connection details in the **UCS Director** tab.

Step 3 Select **Cisco UCS Director**.
The client/server side validation happens, on successful creation it navigates to Manage Integrations page.

Step 4 Enter the details to connect to the server where UCS Director is installed.
For https connections, import the root CA certificate of the UCS Director server. Copy the content of the root CA certificate of the server and paste it in the text area. If the root certificate is a chain of certificates, paste the content one below the other. The connection would fail, in case the SSL certificate of the server becomes invalid or untrusted. You can skip the certificate validation by selecting the **Skip Certificate Validation** option.

Step 5 Check **Sync User with IaaS** option to sync this user with IaaS.

Step 6 Check **Enable Poller** if you want to configure automatic polling for the subsequent connections with UCS Director connections.

Note This option is disabled for UCS Director connection that is in Managed Service Provider mode. Manual synchronization is recommended in the UCS Director Managed Service Provider mode.

Step 7 Click **Create Integration**.

Step 8 Select the connection from the Integrations page and choose **Test Connectivity** option from **Manage Integration** drop-down to authenticate the credentials.

Step 9 After the connection is successful, click **Import all Objects** option from **Manage Integration** drop-down. The system starts to discover the data from UCS Director. For more information on data discovered from UCS Director, see Cisco Prime Service Catalog 12.1 Designer Guide.
You can now set the timeout period for UCS Director synchronization initiated using the Connect and Import option. Set the `ucsddata.killSession` parameter in the newscale.properties file to set the timeout. The UCS Director synchronization will end after this set period is elapsed.

Note The UCSD scheduler in the Prime Service Catalog automatically polls UCS Director entities. You can also manually discover these entities using the web interface in Prime Service Catalog. For more information on discovering UCS Director entities in Prime Service Catalog, see Managing UCS Director Synchronization.

Note Once the user is imported to Prime Service Catalog from UCS Director, to login to Prime Service Catalog, the password used must be same as the username.

Step 10 On the **Discovered Panel**, you can:

- View all the discovered entities in the **Objects** tab.
- View the services created for the imported catalog and container entities in the **Services** tab.

  Note Use the **Overwrite Workflow Form Definition** field in the **Discovered Services** > **Advance Catalog Services** > **General** tab to update advance catalog service form on the Prime Service Catalog side.
- Select a service and configure the category, presentation, facets, and permissions for these services. For more information, see Configuring Permissions and Presentation for Private and Hybrid Cloud Services.

Note
- Be sure to re-run import, if you add any additional Templates on UCS Director. For example, the Gateway and the Application Server Templates.
- Check the Organization Designer on Prime Service Catalog to see whether the **Service End User** from UCS Director is discovered and is present in Prime Service Catalog.

Deleting a UCS Director connection

As a Service Operations Administrator, you can delete a UCS Director connection by selecting the **Remove** option either from Integrations > Setting drop down or Manage Integrations page > Manage Integrations drop down. This option will delete the connection along with its imported entities such as virtual machines, VDCs, containers, templates, catalogs, and workflows.

Note
- If a UCS Director connection is in the MSP mode, all the associated workflows for that UCS Director instance will also get deleted.
- The templates and catalogs are deleted only when there is no requisition associated with these services.

However, entities such as users, user groups, images, template definitions, and organization units will remain in Prime Service Catalog.

Enabling Single Sign-On in Prime Service Catalog

If you are using Prime Service Catalog in the Cisco ONE Enterprise Cloud Suite, you must enable single Sign-on (SSO) when integrating Prime Service Catalog with UCS Director.

Caution You cannot configure both LDAP and SAML configured for SSO login in Prime Service Catalog. If you wish to use LDAP SSO, the SAML SSO must be manually disabled, failing which will lead to incorrect login behavior. To disable SAML login, go to **Integrations > Single Sign-On Integration** and uncheck **Enable SSO For SAML** and click **Save**.

Prime Service Catalog and UCS Director use LDAP authentication to handle permissions for catalog items and service items. With LDAP integration, group permissions for the catalog items and virtual machines in UCS Director are synchronized with the service items and catalog items in Prime Service Catalog. For example, if a specific group owns a virtual machine in UCS Director, the users in that group can view the same virtual machine in Prime Service Catalog. In addition, if a specific group can access a catalog item in UCS Director, the users in that group can order the same catalog item from Prime Service Catalog.

Use the procedure below to enable the single sign-on:

Step 1 Set up LDAP integration in Prime Service Catalog. For more information, see the *Configuring LDAP integration* section in Cisco Prime Service Catalog 12.1 Integration Guide.

Step 2 Set up LDAP integration in UCS Director. For more information, see the *LDAP Integration* section in Cisco UCS Director 5.3 Administration Guide.

Note Ensure that the LDAP groups that you are using are imported from Prime Service Catalog to UCS Director. After importing to UCS Director, ensure that you manually synchronize the users and user groups in UCS Director.

Step 3 Integrate UCS Director with Prime Service Catalog. For instructions on integrating UCS Director with Prime Service Catalog, see Integrating UCS Director (UCSD) or VACS with Prime Service Catalog, on page 12.

Note In Prime Service catalog, ensure that the Sync User with IaaS option is checked in the UCSD connection, so that only the users and groups with LDAP authentication are exported from UCS Director.

Managing UCS Director Synchronization

Scheduling UCS Director Synchronization

You can automatically discover UCS Director instances at scheduled intervals using the scheduler. Use the below procedure to configure the scheduler.

Step 1 Edit the following properties files. These files can be located in the **RequestCenter.war/WEB-INF/classes/config** directory.

- In the **newscale.properties** file, change the interval of polling, as shown in the example below:

```
########################################
#Data Poller
########################################
#Cron Expression wakes up poller every 10 minutes of an hour
ucsddata.poller.cron=0 0/10 * * * ?
#Cron Expression wakes up health check for 3rd min and 5 mins thereafter of the hour ex: 03,08,13
 minutes
uscddata.poller.health.check.cron=0 3/5 * * * ?
#High Availability Health checks threshold, this should be greater than Poller cron time specified
 in minutes
ucsddata.healthCheck.threshold=15
# Number of minutes after which button to kill poller shows up on the manage connections UI
uscddata.killSession=30
```

- In the **support.properties** file, set the poller value as “true”, as shown below:

```
###### Data Poller Settings ##################
# In non-cluster mode: this should be enabled for the Requisitions Data script to be run from
the Poller
# In clustered mode: this can be either enabled on all nodes in the cluster OR on a specific
node in the cluster
# - only 1 node in the cluster will run at any given time, even if this is enabled on multiple
 nodes in a cluster (which ever node starts it first)
ucsdData.poller.enable=true
########################################
```

Step 2 In **Administration** > **Settings** page, select the **UCSD Scheduler** option.

Note
- The following step is critical for automatic synchronization.
- All entities except Users will be automatically synchronized if you have enabled the Scheduler. Any change in User on UCS Director should be manually synchronized in Prime Service Catalog. For more information on manual synchronization, see Manually Importing UCS Director Synchronization, on page 16.

Manually Importing UCS Director Synchronization

If Prime Service Catalog and UCS Director are integrated with LDAP, it is recommended to manually poll users information using the web interface whenever the user roles are changed in UCS Director. This is to ensure synchronization of the user’s RBAC permission to Prime Service Catalog services with the changes made in UCS Director.

You can manually import UCS Director instances using the UCS Director Integration page. When you perform this process, all entities including users and roles are synchronized.

This process is used in the following scenarios:

- If you do not want to use a Scheduler.
- If you are using a Scheduler and UCS Director and Prime Service Catalog are integrated with LDAP. To improve the performance, the Scheduler does not synchronize users and roles. Because of this behavior, if an administrator makes changes to users and roles in UCS Director, these changes are not

communicated to Prime Service Catalog. To synchronize these changes with Prime Service Catalog, you must manually import UCS Director instances, which in turn synchronizes the users and roles.

Step 1 Choose **Advanced Configuration > Integrations** (Integrations) page.

Step 2 Select the UCSD instance and select **Manage Integration** option from **Settings** drop down.

Step 3 Click **Import All Objects** option from **Manage Integration** drop-down.

Scheduling the Collection of Reporting Data from UCS Director

You can discover the reporting data for all VMs from the UCS Director at scheduled intervals, using the scheduler, automatically. You can also configure the number of days, months, weeks and beginner of the week for which the data needs to be imported and displayed in the Prime Service Catalog. Use the following procedure to configure the scheduler and the reporting data settings.

Edit the following properties files. These files are located in the **RequestCenter.war/WEB-INF/classes/config** directory.

- In the **newscale.properties** file, change the interval of polling, as shown in the example below:

```
########################################
#Resource Reporting Data Poller
########################################
#Cron Expression wakes up poller every 43 minutes of an hour
• reportsdata.poller.cron=0 10/20 * * * ?
#Cron Expression wakes up health check for 13th min and 15th min thereafter of the hour ex:
13,28,43,58 minutes
reportsdata.poller.health.check.cron=0 17/20 * * * ?
#High Availability Health checks threshold, this should be greater than Poller cron time specified
 in minutes
reportsdata.healthCheck.threshold=127
```

- In the **newscale.properties** file, add the number of months, days, weeks, and set the beginner of week, as shown in the example below:

```
########################################
#Resource Reporting Import Data Settings
########################################
#This property is configurable setting to fetch monthly usage data for first import.
#This is max value. If any value more than 12 is overwritten with 12.
• reportsdata.import.numberofmonths=12
#This property is configurable setting to fetch daily usage data for first import.
#This is max value. If any value more than 365 is overwritten with 365.
• reportsdata.import.numberofdays=365
#This property is configurable setting to fetch weekly usage data for first import.
#This is max value. If any value more than 52 is overwritten with 52.
• reportsdata.import.numberofweeks=52
#This property is configurable setting to fetch weekly usage data for first import.
#Only Monoday or Sunday or the values for this property. Otherwise Monday will be picked
```

```
#for any other day provided here.
• reportsdata.import.beginnerofweek=Monday
```

• In the **support.properties** file, set the poller value as “true”, as shown below:

```
###### Reporting Data Poller Settings ###################
# In non-cluster mode: this should be enabled for the Requisitions Data script to be run from
the Poller
# In clustered mode: this can be either enabled on all nodes in the cluster OR on a specific
node in the cluster
# - only 1 node in the cluster will run at any given time, even if this is enabled on multiple
 nodes in a cluster (which ever node starts it first)
reportsData.poller.enable=true
########################################
```

Configuring Permissions and Presentation for Private and Hybrid Cloud Services

Based on the permissions granted to an end user, the discovered services from UCS Director becomes orderable in the **Service Catalog** module.

To understand the UCS Director groups and roles mapping to Prime Service Catalog groups and roles, see Prime Service Catalog System Defined Roles for UCS Director Integration and Users and User Groups Imported from UCS Director.

Depending on the UCS Director integration, you can discover standard catalogs, container catalogs, and container templates services for end-user provisioning and maintenance of VMs on private and public cloud. Using these services, end users can:

Order services created based on service container catalog, standard catalog, advanced catalog, and fenced container templates from UCS Director.

Before You Begin

Discover the Services from UCS Director by integrating with the UCS Director instance. For more information on integrating UCS Director, see Integrating UCS Director (UCSD) or VACS with Prime Service Catalog.

Step 1 Select the connection from the Integrations page and select **Manage Integration** option from **Settings** drop down.

Step 2 Click **Services** button in **Discovered** panel.

Step 3 Double-click on the service to be customized.

Step 4 In the **Details** panel, enter Service Name, Description, and add Categories.

Note Private Cloud Iaas will be selected as the default service category for UCS Director services. You can remove the default category and associate the generated services to another category. A service can also be associated with multiple categories.

Note New Categories can also be created and one category image can also be associated with that newly created category and this new category can be associated with existing service.

For an advance catalog services, select **Yes** in the **Overwrite Form Definition** field, if you want to overwrite Custom Form Rules, Display Properties, and Dictionary Names for these services. And click **Save**.

Step 5 In the **Presentation** panel, click **Attach**, to select an image to be associated with the service or select **Image URL** to enter the URL of the image. Default option selected is **Image File**.

Step 6 Select an image from the list of **Select Image** window and click **Add**.
Cisco provides a number of images out-of-box that you can assign to the service. You can also upload an image to be used for the service.

Step 7 Enter a description for the service by selecting the **Overview** or **Service Form** options, and click **Save**.

Step 8 In the **Facets** panel, choose the required options and click **Save**.

Step 9 In the **Permissions** panel, do the following:

- Select the roles from the list and click **Remove Selected** to remove the permission.
- Select from the **Add Permissions** drop-down list to add or select the roles from the list who can deploy these services.
- **For container templates, container catalogs, standard catalogs, and advance catalogs services created in Prime Service Catalog for UCS Director**:
  - If these services are associated to a group in UCS Director, users in the corresponding group in Prime Service Catalogs can only order services that the group has access to.
  - If the services are associated to All Groups in UCS Director, users in the corresponding group in Prime Service Catalog can order the services that All Groups have access to.

Step 10 Click **Save**.
The new service will be displayed in the **Service Catalog** module based on the category you have selected.

Mapping Templates for UCSD Services

Prime Service Catalog provides out-of-box templates using which you can map to the UCSD services. The template service defines the way the entities of UCSD appear as a service in Service Catalog module. In UCSD, templates can be mapped at catalogs or templates level.

Custom templates can be created based on the out-of-box UCSD templates provided by Prime Service Catalog and used for mapping to the UCSD services. For more information on creating custom templates see, *Create Custom Templates* in Cisco Prime Service Catalog Designer Guide.

To map a template:

Step 1 Select the connection from the Integrations page, choose **Manage Connection** from the settings.

Step 2 Click **Objects** in the **Discovered** panel.

Step 3 Choose the *Template* or *Catalog* from the left hand side and for the selected entry, choose the custom template from the **Select Base Template** drop-down list.

Step 4 You can do one of the following from the settings option:

a) Click **Regenerate Service**, to regenerate the existing service with the selected new template.
b) Click **Generate Service Variant**, to create a service variant corresponding to the UCSD entities with the new custom template.
   Note If this service variant already exists for the selected template, then it will be regenerated.

Users and User Groups Imported from UCS Director

Note In a single pane of glass, where Prime Service Catalog, UCS Director are connected to LDAP:

- The Home OU of a user is always determined by LDAP mapping .
- The User gets group membership of UCS Director if the user belongs to UCS Director imported groups.
- If the User data that is imported (discovered) does not exist in Prime Service Catalog, the same is created in Prime Service Catalog and the normal flow for OU, Group and Role is executed.

When Prime Service Catalog connects to a UCS Director for the first time, Prime Service Catalog creates a:

- **UCSD ::<ID>::All Groups:**

Where <ID> is the 3-letter identifier of the UCS Director server. This group will be the parent group for all groups imported from this UCS Director server.

- **UCSD ::<ID>::<Group Name>**:

Where <ID> is the 3-letter identifier of the UCS Director server. There will be group for each group in the UCS Director. All such groups are grouped under the parent group. Users belonging to various groups in the UCS Director are imported to the respective groups in Prime Service Catalog.

- **Default group**. The default group is grouped under the parent group. Users without a group in the UCS Director are imported to this group.

All the imported users from the UCS Director are assigned an Organizational Unit (OU) in Prime Service Catalog. During the subsequent connections, Prime Service Catalog checks for group membership changes and updates the records accordingly.

Note For container templates, container catalogs, standard catalogs, and advance catalogs services created in Prime Service Catalog for UCS Director:

- If these services are associated to a group in UCS Director, users in the corresponding group in Prime Service Catalogs can only order services that the group has access to.
- If the services are associated to All Groups in UCS Director, users in the corresponding group in Prime Service Catalog can order the services that All Groups have access to.

For those users who are not imported from UCSD, the user must be manually be added to any one of the UCSD imported groups to be able to order UCSD services. Also in order to perform life cycle operations on the VMs that is provisioned by the user, the user must be granted *UCSD End User* role.

Prime Service Catalog System Defined Roles for UCS Director Integration

Prime Service Catalog creates the following system-defined roles for the UCS Director roles it discovers. The following table lists the mapping of the UCS Director to Prime Service Catalog system-defined roles.

Table 1: Prime Service Catalog Roles Mapping with UCS Director Roles

UCS Director Roles	Prime Service Catalog System Defined Roles	Description
System Admin	UCSD Sys Admin	UCSD Sys Admin user can view the details of Containers, vDC's and VM's as service items in My Products and Services based on the Group permissions assigned to each of the UCS Director Service Item in Service Item Manager. Only users with this role can order Container Template Services.
All Policy Admin		
Computing Admin		
Service End-User, Group Admin, Operation roles	UCSD End User	UCSD End User can view the details of Containers, vDC's and VM's as service items in My Stuff based on the Group permissions assigned to each of the UCS Director Service Item in Service Item Manager. Users with this role can order services based on the group to which user belongs and catalogs which are assigned to a group in UCS Director.
All other roles	UCSD Operator	Users with this role can only view and use the self-service portal but cannot order the services.

Note In a single pane of glass, where Prime Service Catalog, UCS Director are connected to LDAP:

- The Home OU of a user is always determined by LDAP mapping.
- The User gets group membership of UCS Director if the user belongs to UCS Director imported groups.
- If the User data that is imported (discovered) does not exist in Prime Service Catalog, the same is created in Prime Service Catalog and the normal flow for OU, Group and Role is executed.

Configuring Display Categories for Private Cloud Services

The new service will be displayed in the **Service Catalog** module based on the category you have selected.

Before You Begin

Discover the Services from UCS Director by integrating with the UCS Director instance. For more information, see Integrating UCS Director (UCSD) or VACS with Prime Service Catalog.

Step 1 Choose **Advanced Configuration > Integrations** and select the connection from the Integrations page.

Step 2 Click **Manage Integration** option from drop down and click on the **Services** tab in the Discovered panel double-click on the service.

Step 3 In the **Details** panel, do the following:

a) Enter a service name and description for the selected service.

b) Select an existing category or create a new category by clicking on the **New** option.

Step 4 Click **Save**.

Providing Multi-Tenant IaaS

This feature enables service providers to use **Cisco ONE Enterprise Cloud Suite** to provide multi-tenant Infrastructure as a Service (IaaS) on ACI. The components required for this functionality are: Prime Service Catalog, UCS Director (in **Managed Service Provider** mode), and ACI.

The **Tenant Management** module in Prime Service Catalog provides infrastructure services to multiple tenants quickly and efficiently. Using this module, tenants can manage their own set of services, and offer these infrastructure services to their end users. A tenant can contain several organizations and each organization can contain several users.

Using **Tenant Management** module:

- A tenant administrator can manage tenant users, define quotas on computing resources and virtual machines for a tenant user, and delegate management of firewalls and load balancers.
- An end user can self-service provision and manage VMs.

The tenant workflow (for example: create, update, and delete tenants), VDC, and VM operations are executed through Advanced and Service Container Catalog workflow in UCS Director. Prime Service Catalog creates services for these advance and service container catalog workflows during the UCS Director discovery process. For this feature to work seamlessly, a site administrator must map these UCS Director discovered services to the Tenant Management workflow in Prime Service Catalog. For more information, see Setting Up Tenant Management Module and Mapping Tenant, VDC, and Firewall Rule Workflows from UCS Director .

Tenant Workflow Configurations in UCS Director for Multi-Tenant IaaS

For seamless multi-tenant IaaS operations, an administrator must ensure that multi-tenant IaaS-related objects are created and configured in UCS Director. An administrator need to configure only four of these multi-tenant IaaS workflows. Remaining workflow are pre-defined and configured during the installation process.

This section covers the list of fields or attributes that must be configured for these workflows in the UCS Director. For more information on how to create these advance and container catalog workflow, see Cisco UCS Director 6.0 Administration Guide.

Note Do not use hyphen in UCS Director Advance Catalog name. This is to avoid the synchronization issues after integrating with Prime Service Catalog.

Table 2: Configurations for Multi-Tenant IaaS Workflows on UCS Director

UCS Director Workflow	UCS Director Advance or Service Container Catalog Fields
VNX Tenant Onboarding	• **CPU Reservation (MHz) - (Sample Value - 10000):** Value for this attribute must be derived by an Analyst or an Administrator. • **Capacity (EMCSizeUnit) (Sample Value - GB)** • **Tenant Profile** : Application caters to only one profile. • **Service offering** : Application caters to only one offering. • **Service Profile** : It is a mandatory value. Map this to an existing profile in the system. • **Physical Server Reserved Space** • **Datastore Size Limit (GB)** • **VM Over Subscription** • **L2 VLan ID** • **L2 IP Subnet**

UCS Director Workflow	UCS Director Advance or Service Container Catalog Fields
Update Tenant	• **Tenant Profile Name:** Application caters to only one profile. This field should be same as specified in VNX Tenant Onboarding workflow. • **Service Offering:** Application caters to only one service offering. This field should be same as specified in VNX Tenant Onboarding workflow • **CPU Reservation (MHz):** Value for this attribute must be derived by an Analyst or an Administrator. • **Service Profile Identity:** It is a mandatory value. Map this to an existing profile in the system. • **Capacity (GB)** • **Datastore Limit**
APIC Service Container catalog	No specific fields to configure for APIC Service Container catalog. Make sure an APIC Service Container catalog is available in UCS Director for VDC workflows.
Firewall Rule Action Configuration	• **Firewall ID** • **Protocol** • **Entry Name** • **Order** • **Service Param** • **Source Address** • **Source Any** • **Source Port** • **Tag**

Setting Up Tenant Management Module

A site administrator must perform the following steps for seamless multi-tenant IaaS operations.

Before You Begin

- Connect to a UCS Director instance that is in the Service Provider mode.
- In Prime Service Catalog, **Service Link** module, verify that **UCSD Agent** is up and running.

- Verify that tenant management-related objects are created and configured in UCS Director. For information on the advance and container catalog workflow inputs that are configured on the UCS Director, see Tenant Workflow Configurations in UCS Director for Multi-Tenant IaaS.

Step 1 Integrate Prime Service Catalog with UCS Director and discover the infrastructure entities from UCS Director. For instructions, see Integrating UCS Director (UCSD) or VACS with Prime Service Catalog.

Step 2 Map the Advanced Catalog/Container Catalog services from UCS Director to the Prime Service Catalog workflow. For more information, see Mapping Tenant, VDC, and Firewall Rule Workflows from UCS Director .

Step 3 Invoke workflow for creating tenants in Prime Service Catalog. For more information, see Onboarding a Tenant.

Mapping Tenant, VDC, and Firewall Rule Workflows from UCS Director

When Prime Service Catalog is integrated with UCS Director, the discovery process creates services based on UCS Director Advanced Catalogs and APIC service container catalog. The advance and the APIC service container catalogs in UCS Director are used for publishing workflow for creating, managing a tenant and creating a VDC respectively.

For a seamless multi-tenant IaaS operations, a site administrator must map these services with the UCS Director workflows.

Note Only four of the Prime Service Catalog tenant management workflows need mapping from an administrator. The remaining workflows are pre-defined and are configured during the installation process. For information on the workflows that needs mapping in Prime Service Catalog, see the table below.

Before You Begin

Integrate Prime Service Catalog with UCS Director instance that is in the Service Provider mode. For more information, see Integrating UCS Director (UCSD) or VACS with Prime Service Catalog.

Step 1 Discover the UCS Director entities in Prime Service Catalog.

Step 2 On the discovery page in Prime Service Catalog, select a workflow from the **Manage Workflows** section and click to open manage workflow page. , and select an advance or a service container catalog service from the **Services** drop down on the right-hand side. For information on which services to select in this drop down, see the table below.

Step 3 Based on the type of advance or service container catalog service selected in the previous step, select the values for the remaining workflow attributes and click **Save**.

Note
- Most of the attribute mappings are self explanatory except Organizational Unit. Organizational Unit should be mapped to GroupName.
- You can introduce custom attributes in the PSC service to map any new workflows in UCSD Advance or Service Container Catalogs using the **Add Attribute** option. If the new catalogs are not mapped to the PSC service, requisition is not created and an error is displayed. The custom attributes can be modified or deleted if the catalogs are not in use.

Step 4 Navigate to **Tenant Management** module and invoke workflow for creating tenants. For VDC and Firewall Rule Workflows, navigate to **Service Catalog** module **My Products & Services** > **Virtual Data Centers** to create VDC and add Firewall Rule.
The status of the service request is displayed as Completed, if the operation on UCS Director is successful.

Note If the attributes are not mapped properly, requisition is not created and an error is displayed.

Prime Service Catalog Workflow	UCSD Advance/Service Container Catalogs
Create Tenant	Advance Catalog based on **VNX Tenant Onboarding** workflow
Manage Tenant	Advance Catalog based on **Update Tenant** workflow
Create VDC	Advance Catalog based on any **APIC Service Container Catalog**
Create Firewall	Advance Catalog based on **Firewall Rule Action Configuration** workflow

Onboarding a Tenant

As a site administrator, you can create a tenant administrator. A Tenant administrator can create and manage users, Organization Units (OUs), and VDCs. In addition, the tenant administrator can specify which tasks the users can perform on their virtual machines and services, and can place quotas on computing resources and virtual machines.

When you create a Tenant Admin, the Organization and Tenant User dashlets are automatically created and associated for that Tenant.

The following prerequisites must be met before the site administrator creates a tenant:

Note These prerequisites are also applicable for creating a VDC.

Before You Begin

- Add a UCS Director connection that is in the Manage Service Provider (MSP) mode. You can connect to a UCS Director instance in **Advanced Configuration** > **Integrations** and click **New Integrations**.
- Map the advance/service container catalog services with the Prime Service Catalog workflows. For more information, see Mapping Tenant, VDC, and Firewall Rule Workflows from UCS Director .

- UCSD Agent must be up and running in the Service Link module.

Step 1 Log in as Site Administrator.

Step 2 Go to **Tenant Management**.

Step 3 Click **Add Tenant** from the **Tenant Management Dashboard**.

Step 4 In the **Tenant Information** tab, enter details such as name of the tenant, address, disaster recovery protection information, L2 VLAN ID, L2 IP Subnet, Tenant IP Pool, and Resource Selection (For ND).

Note
- L2 VLAN ID, L2 IP Subnet, and Tenant IP Pool attributes are required to map the appropriate subnet inside a container. Enter the L2 VLAN ID, L2 IP Subnet, and Tenant IP Pool in the recommended format as shown on the web interface.
- Editing tenant details after the tenant is created will cause the L2 VLAN ID, L2 IP Subnet, and Tenant IP Pool fields to be in a read only state.
- If you choose the Provision New Resources option from the Resource Selection (For ND) drop-down list, you must enter the details for RAM (For ND), vCPU (For ND), and Storage (For ND).

Step 5 Specify the reservation details for vDC in the **Quota Management** tab (based on the vDC template).
UCS Director uses this information for resource allocation and to provision that tenant. The Tenant Administrator can then create and manage OUs, vDC, and users for each of the associated Tenant.

When the Tenant is in the **Being provisioned** status, the Tenant Admin icon will be disabled on Tenant Dashboard restricting the user (site admin) to view the User Management. An information icon 'i' is displayed in Status in the Tenant Dashboard and when clicked, displays an overlay of requisition, provisioning workflow summary, comments with date and timestamp.

You can also search and edit only the quota/capacity details (and not any other details associated to a VDC) by navigating to **Tenant Management** > **Find a Tenant**. The Tenant Administrator can navigate to Organization, Users, and VDCs from the User Dashboard.

Note
- The Tenant Admin icon (next to Status column) is enabled or disabled based on the Status of the Tenant. If the Tenant is Active, you can navigate to User Management by clicking the Tenant Admin icon to perform necessary tasks.

Deleting a Tenant

The following instructions are specific only to the customers who have access to the Tenant Management module.

To delete a tenant from the **Tenant Management** dashboard, make sure that you delete all the physical servers, VMs, VDCs, Organization users, or any service items associated with that tenant. Follow the steps in the same sequence as listed below.

There might be slight variations in steps depending on the database you are using.

Step 1 (As a Tenant Administrator) Go to **Service Item Manager > Manage Service Items**, then click the delete icon to delete physical servers for the tenant.

Step 2 Go to **My Products & Services > Virtual Data Center**, then select the VDCs corresponding to the tenant.

Step 3 Delete the load balancer. To delete, select the Load Balancer from the **Load Balancer** tab and click the delete icon.

Step 4 Delete the Firewall rule. To delete, select the **Firewall rule** from the **Firewall Rule** tab and click the delete icon.

Step 5 Delete the VMs. To delete, click the **Virtual Machines** corresponding to the VDC. On the right of each VM, click the gear icon to delete it.

Step 6 Delete the VDCs. Click the delete icon on the existing VDC to delete it.

Step 7 (For Oracle only) Go to the **Administration > Utilities** and purge all the requisitions for the specific users.

Step 8 Go to the **Organisation Designer** module and do the following:

1. Move all the OUs to some other parent OU, which is not a tenant.
2. Remove the additional OUs (Other than Home OU) for users and then delete users.
3. Delete the users by clicking the **Remove** button.

Step 9 (As a Site Administrator) Go to the **Tenant Management** module and click the delete icon next to the tenant, which you want to delete.

Providing CloudCenter Applications as a Service

Cisco Prime Service Catalog offers a direct integration with Cisco CloudCenter. You can set up the connection from Prime Service Catalog to CloudCenter, resulting in the automated import of the application deployment workflows, ready to be published to the catalog.

CloudCenter lets users define cloud-agnostic blueprints of their multi-tier applications and then deploy them to private, public, or hybrid clouds based on cost and performance metrics provided by CloudCenter. CloudCenter can manage the lifecycle of an application with auto-aging policy and the ability to scale-out and scale-in individual tiers of a multi-tier app based on application performance.

Generating Orderable Services for CloudCenter Applications

For creating orderable services for deploying CloudCenter applications in cloud, you must perform the following steps:

	Steps	Topics
Step 1	Integrate CloudCenter with Prime Service Catalog.	Integrating CloudCenter with Prime Service Catalog, on page 29
Step 2	Discover application profiles.	

	Steps	Topics
Step 3	Configure search facets, permissions, and presentation for hybrid cloud provisioning services in Prime Service Catalog.	Configuring Permissions and Presentation for CloudCenter Services, on page 30

Based on the permissions, end users can now deploy the application services.

Integrating CloudCenter with Prime Service Catalog

As a Integrations Administrator you can add a connection to CloudCenter server, and import Application Profiles and Activation Profiles from CloudCenter database. For each CloudCenter application profile, Prime Service Catalog automatically creates a service.
To integrate CloudCenter with Prime Service Catalog follow the below procedure:

Step 1 Login to Prime Service Catalog as the Integrations Administrator (or Site Administrator) user.

Step 2 From the main menu, choose **Advanced Configuration** > **Integrations** and click **New Integrations**.

Step 3 Select **Cisco CloudCenter**.

Step 4 Enter the details and click **Create Integration** to connect to the CloudCenter server.

1. For https connections, import the root CA certificate of the CloudCenter server. Copy the content of the root CA certificate of the server and paste it in the text area. If the root certificate is a chain of certificates, paste the content one below the other. The connection would fail, in case the SSL certificate of the server becomes invalid or untrusted. You could Skip the certificate validation by selecting the **Skip Certificate Validation** option.
2. API Key is a mandatory field, you must obtain the username and API key from CloudCenter to connect to the CloudCenter server.
3. By default, a base template is mapped to the connection. However, you can use other templates available in the drop-down list. For more information on Service Templates see section Mapping Application Templates for CloudCenter, on page 31.

Step 5 Choose **Test Connectivity** option from **Manage Integration** drop-down to validate the credentials and the server details.

Step 6 After the connection is successful, click **Import all Objects** option from **Manage Integration** drop-down. The system starts to discover and import the published CloudCenter application profile.

Step 7 In the **Discovered** panel, you can:

- View all the discovered entities in the **Objects** tab.
- View the services created for the Application in the **Services** tab.
- Select a service and configure the category, presentation, facets, and permissions for these services. For more information, see Configuring Permissions and Presentation for CloudCenter Services, on page 30.

Deleting a CloudCenter Connection

You can delete a CloudCenter connection by choosing **Remove** option from **Manage Integration** or by choosing **Remove** option from **Settings** drop down in the Integrations page. This option will delete the connection along with its imported entities such as applications and activation profiles.

Note Even if the connection is deleted, all the associated entities pertaining to the connection is retained in the system.

Configuring Permissions and Presentation for CloudCenter Services

Based on the permissions granted to the user, the discovered application services become available in the **Service Catalog** module. Using the options described in the below procedure you can grant deploying permission of these services to OUs, users, groups or roles in prime Service Catalog, or customize the services by adding more presentation details, descriptions, categories, etc. However, the services are ready to be deployed as is without any additional definitional changes.

Before You Begin

Discover the Application Profiles from CloudCenter by integrating with the CloudCenter. For more information on integrating, see Integrating CloudCenter with Prime Service Catalog, on page 29.

Step 1 Select the connection from the Integrations page and click **Services** in the **Discovered** panel or select **Manage Integration** option from **Settings** drop down and click **Services** in the **Discovered** panel.

Step 2 Select the service to be customized.

Step 3 In the **Details** panel, enter Service Name, Description, and add Categories. And click **Save**.
Select **Yes** in the **Overwrite Form Definition field**, if you want to overwrite Custom Form Rules, Display Properties, and Dictionary Names for these services. And click **Save**.

Note CloudCenter Applications will be selected as the default service category for CloudCenter services. You can remove the default category and associate the generated services to another category. A service can also be associated with multiple categories.

Step 4 In the **Presentation** panel, click **Attach**, to select an image to be associated with the service or select **Image URL** to enter the URL of the image. Default option selected is **Image File**.

Step 5 Select an image from the list of **Select Image** window and click **Add**. Cisco provides a number of images out-of-box that you can assign to the service. You can also upload an image to be used for the service.

Step 6 Enter a description for the service by selecting the **Overview** or **Service Form** options, and click **Save**.

Step 7 In the **Facets** panel, choose the required options and click **Save**.

Step 8 In the **Permissions** panel, do the following:

- Select the roles from the list and click **Remove Selected** to remove the permission.
- Select from the **Add Permissions** drop-down list to add or select the roles from the list who can then deploy these services.

Step 9 Click **Save**.

The new service will be displayed in the **Service Catalog** module based on the category you have selected.

Mapping Application Templates for CloudCenter

You can set a base template for the services for a chosen connection or the application profile. This template defines the way the application appears as a service in Service Catalog module.

The templates can be mapped at two levels:

- **Connection level**: You can map the template when you add a new connection or modify the connection later to map a new template. On import all the applications associated with that connection inherit the template assigned at the connection level.

Note Only those template will continue to inherit connection level template which were inheriting before connection level template is changed.

- **Application Profile level**: Templates can also be assigned at application profile level. You can create custom templates in Service Designer based on the out-of-box template for CloudCenter, these custom templates will then be available for mapping to the Application Profiles. For more information, see Cisco Prime Service Catalog Designer Guide.

Note It is recommended to apply the custom templates at application profile level only in the case current template for that application profile is updated and you want the service to have those changes.

To map templates at application profile level follow the below procedure:

Step 1 Select the connection from the Integrations page and click **Objects** in the **Discovered** panel.

Step 2 Choose the Application Profile from the list and select the new template from the **Select Base Template** drop-down list.

Step 3 You can do one of the following from the settings option:

a) Click **Regenerate Service**, to regenerate the existing service with the selected new template.

b) Click **Generate Service Variant**, to create a service variant corresponding to the application profile with the new base template.

Note If this service variant already exists for the selected template, then it will be regenerated.

User Management in Prime Service Catalog and CloudCenter Integration

In Prime Service catalog 12.0, user was pushed in to CloudCenter and associated to the default Activation Profile only when the user joined or created a Team for the first time. However, from 12.1 release onwards, the behavior has been changed such that the user need not be part of the team for the user to be pushed to CloudCenter. Users are pushed into CloudCenter when the user is imported from LDAP or SAML on login event or users are created manually by importing through Catalog Deployer, Organization Designer or NSAPI. This will allow Prime Service Catalog-CloudCenter integration to operate independent of the Prime Service Catalog Team Management module.

Supported CloudCenter Features

Prime Service Catalog now supports the following features of CloudCenter:

Multiple CloudCenter Connections

You can now add more than one CloudCenter connection. In case of multi CloudCenter connections, users are pushed into multiple CloudCenter environments when imported on to Prime Service Catalog.

Prime Service Catalog imports application profile for every connection and generate service for each application profile by default. If two connections are having the same application profile, Prime Service Catalog generates two services one for each connection with short name appended in the Service Name to distinguish them.

Governance Mode

Prime Service Catalog supports CloudCenter system tags, aging policies, and rules-based governance. It means that the tags created in CloudCenter when associated with the deployment takes various automatic actions based on the tags that are associated with resources and the system tag matching rules that are defined. This is applicable only if rules-based governance is enabled on CloudCenter. In case aging policy is defined for an application in CloudCenter, after the set duration the new status of application is updated. For example, if an application is set to terminate or suspend after certain duration, the same application will be deleted or suspended in Prime Service Catalog. However, the status of the application may not reflect right away in Prime Service Catalog. The status of the application syncs with Prime Service Catalog based on the poller settings. By default this cron job is set to run every day at 1 a.m.

The poller property cloudcenterdata.poller.cron in *newscale.properties* file allows you to set the frequency of the data sync between Prime Service Catalog and CloudCenter.

For detailed information on system tags, aging policies, and rules-based governance see Cisco CloudCenter Documentation.

Integrating Performance Manager with Prime Service Catalog

As a Integrations Administrator you can add a connection to Performance Manager server. Data points for performance reports are generated in UCS Performance Manager. Prime Service Catalog imports these data points through an API call functionality. For each Performance Manager application profile, Prime Service Catalog automatically creates a service. You can view the performance report for a vDC for an hour, 6 hours, and 1 week. You can also customize the time interval for which you need the performance report. For more

information on performance reports, see section *Viewing Performance reports* in Cisco Prime Service Catalog User Guide.

Before You Begin

Ensure to have UCSD connection established and VMs created by UCSD user in Prime Service Catalog.

SUMMARY STEPS

1. Login to Prime Service Catalog as the Integrations Administrator user.
2. From the main menu, choose **Advanced Configuration > Integrations** and click **New Integrations**.
3. Select **Cisco UCS Performance Manager**.
4. Enter the details to connect to the server where UCS Performance Manager is installed.
5. Click **Create Integration**.
6. Select the connection from the Integrations page to and choose **Test Connectivity** option from **Manage Integration** drop-down to authenticate the credentials.

DETAILED STEPS

Step 1 Login to Prime Service Catalog as the Integrations Administrator user.

Step 2 From the main menu, choose **Advanced Configuration > Integrations** and click **New Integrations**.

Step 3 Select **Cisco UCS Performance Manager**.

Step 4 Enter the details to connect to the server where UCS Performance Manager is installed.
For https connections, import the root CA certificate of the UCS Performance Manger server. Copy the content of the root CA certificate of the server and paste it in the text area. If the root certificate is a chain of certificates, paste the content one below the other. The connection would fail, in case the SSL certificate of the server becomes invalid or untrusted. You can skip the certificate validation by selecting the **Skip Certificate Validation** option.

Step 5 Click **Create Integration**.

Step 6 Select the connection from the Integrations page to and choose **Test Connectivity** option from **Manage Integration** drop-down to authenticate the credentials.

Note The UCSPM scheduler in the Prime Service Catalog automatically polls UCS Performance Manager entities.

Configuring Performance Reports

Performance is a real time data and it's not stored in the Prime Service Catalog tables. Using the **Performance** tab, you can view the line charts representation of the performance of the resources under a vDC. Data points for performance reports are generated in UCS Performance Manager. Prime Service Catalog imports these data points through an API call functionality. You can view the performance report for a vDC for an hour, 6 hours, and 1 week. You can also customize the time interval for which you need the performance report.

Poller connects to a UCS Performance Manager instance, ensures automatic synchronization and collection of reporting data for all VMs from the UCS Performance Manager at scheduled intervals. The polling interval can be configured in the newscale.properties file. You can edit the newscale.properties file located at `RequestCenter.war/WEB-INF/classes/config` directory to configure the polling interval.

- In the support.properties file, set the poller value as “true” as shown in the example below:

```
###### UCSPM Data Poller Settings ###################
# In non-cluster mode: this should be enabled for the Requisitions Data script to be run
from the Poller
# In clustered mode: this can be either enabled on all nodes in the cluster OR on a specific
 node in the cluster
# - only 1 node in the cluster will run at any given time, even if this is enabled on
multiple nodes in a cluster (which ever node starts it first)
ucspmData.poller.enable=true
########################################
```

- In the newscale.properties file, change the interval of polling, as shown in the example below:

```
########################################
#UCSPM Data Poller
########################################
#Cron Expression wakes up poller every 5, 35 minutes of an hour
ucspmdata.poller.cron=0 5/30 * * * ?
#Cron Expression wakes up health check 12 minute thereafter of the hour ex: 12, 42
minutes
ucspmdata.poller.health.check.cron=0 12/30 * * * ?
#High Availability Health checks threshold, this should be greater than Poller cron
time specified in minutes, Poller will be killed if its running more than 2 hours 7
minutes
ucspmdata.healthCheck.threshold=127
########################################
```

  For more information on configuring the polling interval and data import settings, see *Scheduling the Collection of Reporting Data from UCS Director* section of Cisco Prime Service Catalog 12.1 Administration and Operation Guide.

For information on UCSPM integration, see *Integrating Performance Manager with Prime Service Catalog* section of Cisco Prime Service Catalog 12.1 Administration and Operation Guide.

For more information on the charts and description for Performance Report on the , see section *Viewing Performance Reports* of Cisco Prime Service Catalog User Guide.

Deleting a UCS Performance Manager Connection

As a Service Administrator, you can delete a UCS Performance Manager connection by selecting the **Remove** option either from Integrations > Setting drop down or Manage Integrations page > Manage Integrations drop down. This option will delete the connection along with its imported entities such as application and activation profiles, clouds, and deployment environments..

Integrating with Process Orchestrator

Cisco Process Orchestrator is an automation pack that is included with the Cisco Prime Service Catalog license. These packs are designed to further enhance Cisco Prime Service Catalog's automation capabilities as well as integrate with available workplace and data center services. Cisco Process Orchestrator can help with IT process automation processes and tasks that IT staff would otherwise perform manually. The integration of these two solutions greatly improves alignment with best practices and security, quality, and productivity functions when integrated with other IT automated processes. With the Integration feature, the workflows exposed from Process Orchestrator are imported to Prime Service Catalog. Prime Service Catalog also supports the features on Process Orchestrator.

Generating Orderable Services for Process Orchestrator Applications

For creating orderable services for deploying Process Orchestrator applications in cloud, you must perform the following steps:Integrating with Process Orchestrator, on page 34

Step 1 Integrate Process Orchestrator with Prime Service Catalog.

Step 2 Discover workflows.

Step 3 Configure search facets, permissions, and presentation for hybrid cloud provisioning services in Prime Service Catalog.

Integrating Process Orchestrator with Prime Service Catalog

As an Integrations Administrator, you can add a connection to Process Orchestrator server, and import Process Orchestrator work flows from Process Orchestrator. For each Process Orchestrator workflow, Prime Service Catalog automatically creates a service.

To integrate Process Orchestrator with Prime Service Catalog follow the below procedure:

Before You Begin

1. On Prime Service Catalog, configure and set up AMQP connection For more information see Managing AMQP Connections, on page 41.
2. On Cisco Process Orchestrator configure the following settings:
   1. Go to **File > Env properties** and check **Enable Cisco Prime Service Catalog Integration**.
   2. Go to **New process > PSC Integration** tab and check the option **Import into Cisco Prime Service Catalog Integration**.
   3. Enable rest Webservices.

   For more details on these settings, see Cisco Process Orchestrator User Guide 3.5.

Step 1 Login to Prime Service Catalog as the Integrations Administrator user.

Step 2 From the main menu, choose **Advanced Configuration** > **Integrations** and click **New Integrations**.

Step 3 Select **Cisco Process Orchestrator**.

Step 4 Enter the details and click **Create Integration** to connect to the Process Orchestrator server.

a) For https connections, import the root CA certificate of the PO server. Copy the content of the root CA certificate of the server and paste it in the text area. If the root certificate is a chain of certificates, paste the content one below the other. The connection would fail, in case the SSL certificate of the server becomes invalid or untrusted. You could Skip the certificate validation by selecting the **Skip Certificate Validation** option.

b) Choose the Authentication Type. Keep in mind that the Authentication type used in Process Orchestrator and Prime Service Catalog must match.

c) By default, a base template is mapped to the connection. However, you can use other templates available in the drop-down list. For more information on Service Templates see section Mapping Workflow Templates for Process Orchestrator Services.

Step 5 Choose **Test Connectivity** option from **Manage Integration** drop-down to validate the credentials and the server details.

Step 6 After the connection is successful, click **Import all Objects** option from **Manage Integration** drop- down. The system starts to discover and import the published workflow.

Step 7 In the **Discovered** panel, you can:

- View all the discovered entities in the **Objects** tab.
- View the services created for the Application in the **Services** tab.
- Select a service and configure the category, presentation, facets, and permissions for these services. For more information, see Configuring Permissions and Presentation for Process Orchestrator Services.

Deleting a Process Orchestrator Connection

You can delete a Process Orchestrator connection by choosing **Remove** option from **Manage Integration** or by choosing **Remove** option from **Settings** drop down in the Integrations page. This option will delete the connection along with its imported workflows.

Configuring Permissions and Presentation for Process Orchestrator Services

After you have completed the Integrating Process Orchestrator with Prime Service Catalog, you can grant deploying permission of these services to OUs, users, groups or roles in prime Service Catalog, or customize the services by adding more presentation details, descriptions, categories, etc. The procedure is similar to customizing the CloudCenter services, for the detailed steps see, section Configuring Permissions and Presentation for CloudCenter Services, on page 30.

Mapping Workflow Templates for Process Orchestrator Services

A base template for the services allows you to maintain a uniform style and presentation for the services from a particular connection. You can set a base template for the services for a chosen connection. This template defines the way the application appears as a service in Service Catalog module.

Note Custom templates are not supported in workflow definitions.

To map templates to the workflow follow the below procedure:

Step 1 Select the connection from the Integrations page and click **Objects** in the **Discovered** panel.

Step 2 Choose the workflow from the list and select the new template from the **Select Base Template** drop-down list.

Step 3 You can do one of the following from the settings option:

a) Click **Regenerate Service**, to regenerate the existing service with the selected new template.

b) Click **Generate Service Variant**, to create a service variant corresponding to the workflow with the new base template.

Note If this service variant already exists for the selected template, then it will be regenerated. All the services now appear under service Items tab.

Modifying Form Presentation Process Orchestrator Workflow Service

Prime Service Catalog supports the below features of Process Orchestrator that can be used to configure the presentation of the Process Orchestrator Workflow Service :

1. Creating CPO Workflow Attribute Metadata Template. For more details see section Workflow Attribute Metadata, on page 37.
2. CPO table Type-These are treated as grid dictionaries in Prime Service Catalog.
3. Rearranging the variables of the Process using Move Up and Move Down options.

Workflow Attribute Metadata

Using the variable metadata options in Process Orchestrator you can configure the presentation of the workflow attribute. If the variables are not configured, all the attributes appear as plain text boxes in Prime Service Catalog Service Items page. Variable metadata templates allows you to represent Process Orchestrator workflow attribute fields as combos, radio options, check-box selection, multi-select options, text area, hide attribute, password, or read-only. For information on adding variable metadata to a process see section *Adding Variables to a Process* of Cisco Process 3.5 Orchestrator User Guide.

Table 3: Variable Metadata Templates

Display Type	Sample Template
Silgle Select	[{"DisplayType":"select","Values":[{"label":"Meher","value":"Meher"},{"label":"Gary","value":"Gary"},{"label":"David","value":"David"}],"EndPoint":"","OptionLabelColumn":"","OptionValueColumn":""}]
Radio	[{"DisplayType":"radio","Values":[{"label":"RTP","value":"RTP"},{"label":"SJC","value":"SJC"},{"label":"IND","value":"IND"}],"EndPoint":"","OptionLabelColumn":"","OptionValueColumn":""}]
Checkbox	[{"DisplayType":"checkbox","Values":[{"label":"8080","value":"8080"},{"label":"9010","value":"9010"},{"label":"8088","value":"8088"}],"EndPoint":"","OptionLabelColumn":"","OptionValueColumn":""}]
Multi-select	[{"DisplayType":"multiselect","Values":[{"label":"Meraki-1","value":"Meraki-1"},{"label":"APICEM-2","value":"APICEM-2"},{"label":"CDO-1","value":"CDO-1"}],"EndPoint":"","OptionLabelColumn":"","OptionValueColumn":""}][{"DisplayType":"hidden"}][{"DisplayType":"textarea"}]
Password	[{"DisplayType":"password"}]
Hidden	[{"DisplayType":"hidden"}]
Textarea	[{"DisplayType":"textarea"}]

Workflow-level Metadata Templates

Variable metadata can also be added at workflow-level. Below is an example:

```
[  {"AttributeName": "Employee", "EndPoint":
"/api/v1/GlobalVariables/QueryTable?nameOrId=Employee&filterExpression=[Department] like
'#Department#' ",
   "OptionLabelColumn": "FirstName", "OptionValueColumn": "Department"  },
   {"AttributeName": "FirstName", "EndPoint":
"/api/v1/GlobalVariables/QueryTable?nameOrId=EmpService&filterExpression=[FirstName] like
'*' ",
   "OptionLabelColumn": "FirstName",    "OptionValueColumn": "EmpID"  }]
```

Limitations

- Attributes and service names created in Prime Service Catalog must not consist ".".
- Prime Service Catalog grid dictionaries do not support Boolean value.

SAML Configurations

The Security Assertion Markup Language (SAML) is an XML based open standard data format for exchanging authentication and authorization across domain and product. SAML 2.0 protocol offers SSO across Prime Service Catalog and CloudCenter, and enables federation between Prime Service Catalog and an Identity provider (IDP).

Note The Prime Service Catalog supports only one IDP connection to authenticate a user at login.

The SAML Configurations includes the following:

- SAML Configuration
- Enabling SAML Authentication for API, on page 40
- Configuring IDP Mappings
- Refresh MetaData

For detailed information on SAML Configurations, see the Configuring SSO Using SAML chapter of Cisco Prime Service Catalog Integration Guide.

SAML Configuration

This section provides information on how to configure the SAML configuration in the Prime Service Catalog:

Before You Begin

Ensure to configure your IDP.

Step 1 Login to Prime Service Catalog as the Integrations Administrator user.

Step 2 From the main menu, choose **Advanced Configuration** > **Integrations**, and click **New Integrations**.

Step 3 Choose **Single Sign-on** and check the **Enable SSO for SAML** check-box.

Step 4 (Optional) Choose **Enable SAML Authentication for API** to authenticate the APIs with SAML. For more information see section, Enabling SAML Authentication for API, on page 40.

Step 5 Select **SAML Configuration** to configure SAML and click **Configure**.

Step 6 In the **Configuration Details** area, click **Edit** and enter the following mandatory information:

- EntityID—Enter entity identity to identify the SAML configuration.
- Certificate(B64Encoded)—Paste the certificate contents here.
- Private Key(B64Encoded)—Enter the private key details here.

These field are automatically populated with the Prime Service Catalog certificate and private key once the server boots up. However, you could use a CA or Self-Signed certificates generated from the Open-SSL or Java Key tool. Certificates should be in Bas-64 encoded format.

Step 7 Click **Save**.

Note You must restart the server for the changes to take effect. In a cluster set up, you must restart every individual nodes for the settings to take effect.

Step 8 To download the metadata, click **Manage Integration** > **Download MetaData**.
Download metadata is an XML file that contains the SP entity ID and certificate. This metadata is used to register into the respective IDP so that IDP can identity the SP when the request comes from SP.

Enabling SAML Authentication for API

Use this option to restrict only SAML authentication on Prime Service Catalog REST APIs. If this setting is disabled and SAML is enabled for the Prime Service Catalog, then it means that user can make nsapi call by providing header authentication or SAML token based authentication.

Configuring IDP Mappings

This section provides information on how to configure the SAML mappings in the Prime Service Catalog:

Step 1 Login to Prime Service Catalog as the Integrations Administrator user.

Step 2 From the main menu, choose **Advanced Configuration** > **Integrations**, and click **New Integrations**.

Step 3 Choose **Single Sign-on** and check the **Enable SSO for SAML** check-box.

Step 4 Click **Configure** to configure SAML settings.

Step 5 In the IDP Mappings panel, click **Add IDP** to add a mapping in SAML Dashboard.

Step 6 Enter the following information in the **Mapping Information** page:

- Name—Enter unique name to identify the IDP configuration. This name cannot be edited once you save the mapping.
- MetaData—Paste the MetaData contents of IDP that is downloaded from the IDP.
  You must download the IDP metadata from the respective IDP. For example, for ADFS you can download the Metadata from the following URL:
  https://<server_domain_Name>/FederationMetadata/2007-06/FederationMetadata.xml.

Step 7 Configure the **Mapping Information** attributes based on the requirements documented in the Mapping Worksheet. The mappings prefixed with an asterisk (*), shown in the Mapping Information section, are mandatory. Additional (optional) attributes are available under **Optional** tab.

- The attributes on the left hand side are person profile irrespective of the users roles or capabilities. Any user on successful login would use the right hand side attributes from IDP to match it to Left hand side attributes of Prime Service Catalog.
- The SAML assertion attributes on the right hand side is passed from IDP to SP (Service Catalog) on successful authentication.
- In case you wish to add the supervisor information which is not available in the Prime Service Catalog database then, from the optional attributes enter the Supervisor details such as, Login ID, First Name, Last Name, Email, and Organization Unit.

Step 8 Click **Save**.

Note
- You must restart the server for the changes to take effect. In a cluster set up, you must restart every individual nodes for the settings to take effect.
- Once you enable SAML, you can access the Prime Service Catalog only from the IDP login page.
- To perform housekeeping activates after configuring the SAML SSO you can access the Prime Service Catalog from backdoor URL *http://<ipaddress>:<port>/RequestCenter?Astalavista=true*.

Refresh MetaData

Click the gear icon and select the option **Refresh Metadata**, to refresh the node on cluster before it kicks off the scheduled refresh activity every 24 hours.

Managing AMQP Connections

The AMQP username and password along with other AMQP settings can be used to establish connection with the RabbitMQ server. From this release onwards, multiple AMQP Connections are supported. The AMQP Public Key is used to secure the sensitive field using the public key and this secure field will be decrypted by the external system by using the corresponding private key. The AMQP Secure String Format is the format in which the data is encrypted. The default secure string format is Bytes. For information on configuring AMQP tasks for publishing service request to an external system, see Cisco Prime Service Catalog Designer Guide.

Connecting to RabbitMQ Server

RabbitMQ connection is automatically added when Prime Service Catalog node is installed from the Virtual Appliance. From the Integrations module, you can establish communication with another RabbitMQ server by providing the AMQP credentials, under **Advanced Configuration** > **Integrations**, click **New Integration** and select **AMQP**. After you provide the details ensure to save your setting and click **Test AMQP Connection** to validate.

When you click **Test AMQP Connection**, the AMQP connection information is directly inserted into the database without going through the UI. The connection is saved only if AMQP connection authentication is successful. For more details, refer to **REST-based nsAPIs** section of the **Integrating with AMQP** chapter in *Cisco Prime Service Catalog Integration Guide*.

Table 4: AMQP Settings

Field	Description
Identifier	Enter a unique identifier for the connection.
Name	Enter a name for the connection.
Host Name or IP Address	Enter the IP address or the host name of the server where RabbitMQ is installed. If you are using cluster, enter the IP address or the host name of the server where RabbitMQ HA proxy is installed.
Protocol	Select the supported protocol from the drop-down, TCP or SSL.

Field	Description
Port	Displays the port number for RabbitMQ to connect with Prime Service Catalog. This field is auto populated based on the port number you select in **AMQP Port Type**. Default is 5672. **Note** If the ports configured are different than what is defaulted, Users can change it and click the 'Update' button to save the same.
Root CA Certificate	If you are using the protocol as SSL, then click on the **Certificate** option to add a valid SSL certificate. In case of AMQP cluster, if you select this option, you can connect to the HA proxy only if the user has a valid SSL certificate. **Note** If you do not click this option, then you will not be able to connect to SSL.
Skip Certificate Validation	Check this check box to skip the certificate validation .
User Name	Enter the username to connect to the RabbitMQ server.
Password	Enter the password to connect to the RabbitMQ server.
Virtual Host	Enter the virtual host to connect to the RabbitMQ Server, either locally or via remote client. Default corresponds to '/' in RabbitMQ server.
Public Key	The AMQP Public Key is used to secure the sensitive field using the public key and this secure field is decrypted by the external system by using the corresponding private key.
Secure String Format	The AMQP Secure String Format is the format in which the data is encrypted. The default secure string format is Bytes.
Server Down Notification	Select an e-mail template to notify one or more users if the AMQP cluster nodes goes down when a service request is ordered. The system will generate e-mail notifications for any of the following tasks: pre, post, or main tasks.
Recovery Interval	The AMQP recovery Interval is the interval between recovery attempts in minutes for AMQP Connection. Default value is 5 and value range is 1 to 60.
Inbound Queue	Enter the queue to which Service Catalog listens to for inbound messages. For inbound messages a dedicated queue *psc_inbound_queue* is created in RabbitMQ. This name can be modified if required.
Message Type	Select the message type format from the drop-down. This defines the default message processing format for all the outbound and inbound messages for the particular connection.

Note Prime Service Catalog assumes that the RabbitMQ server is installed with a username and password.

- If SSL is supported, the required configuration changes must be done and the ports must be enabled on SSL. For more information on enabling SSL for RabbitMQ server, refer to RabbitMQ documentation.
- AMQP tasks, configured in the Service Definition, use the connection information provided in the Administration module for message publishing. In addition, this information is used by the Overview API to return RabbitMQ details to the caller.
- When the particular connection is saved successfully, a persistent AMQP connection from Prime Service Catalog to the AMQP Server is established to do the following:
  - Republishing of outbound AMQP message when the AMQP server goes down and comes back again.
  - Processing of inbound messages.
- The AMQP Public Key created in the **Administration** > **Settings** > **Public/Private Keys** will be available for selection for every new AMQP connection that is created.

Managing AMQP Tasks and Queue on RabbitMQ Server

Prime Service Catalog includes an administrative utility that allows you access the AMQP tasks queue on RabbitMQ Server instead of managing them on the RabbitMQ Server. You can access this console from **Administration > Utilities> AMQP Topics**. You can view all the available tasks for the chosen connection and delete any unwanted tasks. You can filter the available tasks for the selected connection based on one of the following criteria:

- All Exchanges: List all exchanges on RabbitMQ server
- In Used Exchanges: Exchanges for service requests that are in progress or are in active state and exchanges at service definition time.
- Orphan Exchanges. Exchanges that do not have references to any service definitions or are created by an external system.

Republishing AMQP Messages on RabbitMQ Server

Prime service Catalog offers an administrative utility that allows you to manually republish the AMQP messages to the RabbitMQ Server for the services that you have ordered.

Step 1 Go to **Administration** > **Utilities** > **AMQP Message Republish**.

Step 2 Enter the requisition id for the service for which you want to republish the message, and then click **Fetch Tasks**.

Step 3 Select the task and then click **Resend Message**.

Managing Webservices Connections

The Webservices allows you to access the services and functions defined by the Webservices. The Integrations page contains all information of the Webservices connection details that can be used in the Service Designer Active Form Components DDRs. The connection details are moved from the Dynamic Data Retrieval (DDR) to a centralized place, from which the details can be reused in the service designer. Prime Service Catalog supports multiple webservice connections. To add a webservice connection perform the following procedure and you will need to provide the connection details for the Webservice:

Step 1 Choose **Advanced Configuration** > **Integrations**, click **New Integration** and select **Generic Web Services**.

Step 2 Enter the following details to connect to the server.

Table 5: Integrating Webservices

Identifier	Enter a unique identifier for the webservice connection.
Name	Enter a name for the Service.
Host Name or IP Address	Enter a host name or the IP address of the server.
Protocol	Enter the required protocol, HTTP or HTTPS.
Port	Enter the port number of this Host name or IP address, default is 80 for http and 443 for https.
Root CA Certificate	Enter a valid certificate to connect to the server.
Skip Certificate Validation	Check this check-box to skip the certificate validation.
User Name	Enter the user name of the connection to the corresponding IP address or Host name.
Password	Enter the password of the Host name or IP address.
Authentication Mechanism	Select the required authentication, Session or Header.
Basic Authentication	Check this check box for basic authentication.
UserName Params	Enter the user name parameters, this entry is not mandatory.
Password Params	Enter the password parameters, this entry is not mandatory.
Login URL	Enter the URL to get the authentication/session token for API calls.
Authentication TokenParameter	Enter the authentication token parameter.

Step 3 Click **Save** and click **Test Connection** to authenticate the credentials.

Note

1. If the service with webservices DDR connection is exported and imported on different instances of Prime Service Catalog of same release, the Identifier and Name is displayed as the same name provided by you while creating the service.
2. If the service is imported from the previous release, the Identifier and Name for the webservice is created as I1, l2, and so on.

   Where, I indicates Import and the number changes incrementally as you import new services.
3. If the service with webservices DDR connection is upgraded by running the installer from the previous release, the Identifier and Name is created as W1, W2, and so on.

   Where, W indicates Upgrade and the number changes incrementally as we upgrade new services.

Note For more information on how to export and import of a service, see *Exporting and Importing a Service* in Cisco Prime Service Catalog 12.1 Designer Guide.

Enabling Web Based SSH or RDP to VMs

Prime Service Catalog uses a Guacamole or VMRC server to enable web based SSH or RDP to application VMs launched during the application lifecycle process. These are optional components that you may choose to configure. Guacamole server supports VMs from both UCSD and CloudCenter. Whereas, VMRC supports VMs only from UCSD.

Once the parameters are updated, you can access all the imported VMs on the web browser using the Launch VM action in the Service Items page.

Integrating Guacamole Server with Prime Service Catalog

Apache Guacamole is a clientless remote desktop gateway. In order to access the VMs imported as part of UCSD or CloudCenter Integration, you must integrate with the Guacamole Server from the Integrations module. Once the Guacamole server is configured, you can launch the VMs on the web browser from the Service Items page.

To integrate Guacamole Server with Prime Service Catalog, configure Guacamole server using Prime Service Catalog Virtual Appliance. Once the configuration is complete, a Guacamole server integration appears in the Integrations module automatically. However, you can edit this connection or add a new Guacamole connection from the integrations UI. For information on configuration see section *Installing Guacamole node* in Cisco Prime Service Catalog Virtual Appliance Quick Start Guide.

Note Apache Guacamole server can be configured only on Prime Service Catalog Virtual Appliance and is not supported on the standard installer.

To add a new guacamole connection:

Before You Begin

End user whose going to perform action called "Launch VM Action" should have permission on this Standard Table Data.

Step 1 Login to Prime Service Catalog as the Integrations Administrator user.

Step 2 From the main menu, choose **Advanced Configuration > Integrations** and click **New Integrations**.

Step 3 Select **Generic Guacamole server**.

Step 4 Enter the details to connect to the Guacamole server. Click **Create Integration**.

Step 5 Select the connection from the Integrations page to and choose **Test Connectivity** option from **Manage Integration** drop-down to authenticate the credentials.

Step 6 Choose **Refresh** option from **Manage Integration** drop-down to update the parameters of the UCSD and CloudCenter connections.

Configuring VMRC Server

VMware Remote Console (VMRC) is a remote desktop application that can be used in conjunction with VMware vSphere Web Client to access VMs. VMRC connects to an instance of Virtual Server and provides access to its virtual machines remotely. VMRC is supported only for UCS Director VMs.

To configure VMRC:

Before You Begin

1. User must have appropriate permissions on standard table data.
2. User must be aware of the vSphere credentials.

Step 1 Go to **Service Item Manager** module > **Manage Standards**.

Step 2 Choose *UCSD Cloud Information* from the **UCS Director** group and enter the vSphere credentials.

Step 3 Navigate to **Design Service Items > UCS Director > Virtual Machine** and select the Associated Services tab.

Step 4 Add service called **Launch VM Client**.

Once the connection is successful, go to **Service Catalog** > **Service Items**, for UCSD Virtual Machine a new option **Launch VM** is available. Click this option to launch the VM in VMRC console.

Integrating Apache Solr Search Platform

Solr search enhances the search user experience when configured on any Web site. Apache Solr can index and search multiple sites and return recommendations for related content based on the search query's taxonomy. Integrate Prime Service Catalog with Solr to improve the performance of the Service Catalog search functionality. Currently, Prime Service Catalog supports Solr integration only for Microsoft SQL Server databases.

For Prime Service Catalog to connect to Solr, you must first enable Solr from the Administration module. This will add the option to create a Solr connection on the Integrations module. Once a connection to a running Solr server has been added, Service Catalog search uses the Solr platform. If Solr search is disabled or Solr server is unreachable for some reason, Prime Service Catalog will automatically fall back to querying the database for search results.

Configuring Apache Solr

In preparation of Solr integration with Prime Service catalog, follow the below procedure to configure the Solr server.

To configure Apache Solr:

Before You Begin

Ensure to create Solr Core before proceeding with the configuration.

Step 1 Stop the Apache Solr server

Step 2 Copy the configuration files located under the <PSC_Install_Directory>/solr/sqlserver directory to the conf directory inside your Solr core location <Solr_Install_Directory>/server/solr/{core_name}/conf, overwriting the existing files.

Step 3 Update the overwritten solr-data-config.xml file to specify the database connection details.

Step 4 Start the Solr server.

Step 5 Access the Solr administrative console and select the particular core from the Core Selector drop-down. Navigate to the Data Import tab, and click **Execute** to import the Service Catalog data into Solr.

Step 6 Once the import is complete, navigate to the Query tab and query the engine to ensure that the data is correctly populated.

Note Any changes made to service definitions and localization data, including associations with keywords and categories, require re-importing the data into Solr.

Connecting to Solr Server

The Manage Integrations option for Solr allows you to review and edit the server connection details.

To integrate Prime Service Catalog with Solr:

Before You Begin

1. Configure Apache Solr for Prime Service Catalog. For more information see section Configuring Apache Solr.
2. Enable **Solr Search** option from Administration > Settings > Common Settings.

Step 1 Login to Prime Service Catalog as Site Administrator user.

Step 2 From the main menu, choose **Advanced Configuration** > **Integrations** and click **New Integrations**.

Step 3 Select **Apache Solr**.

Step 4 Specify the server details and the name of your Solr core.
For https connections, import the root CA certificate of the Solr server. Copy the content of the root CA certificate of the server and paste it in the text area. If the root certificate is a chain of certificates, paste the content one below the other. The connection would fail, in case the SSL certificate of the server becomes invalid or untrusted. You could Skip the certificate validation by selecting the **Skip Certificate Validation** option.

Step 5 Click **Create Integration** to connect to the Apache Solr server.